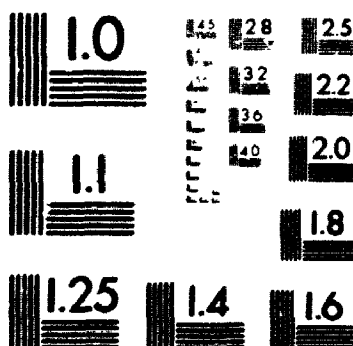


1

PM-1 3½" x 4" PHOTOGRAPHIC MICROCOPY TARGET  
NBS 1010a ANSI/ISO #2 EQUIVALENT



PRECISION<sup>SM</sup> RESOLUTION TARGETS



National Library  
of Canada

Acquisitions and  
Bibliographic Services Branch

395 Wellington Street  
Ottawa, Ontario  
K1A 0N4

Bibliothèque nationale  
du Canada

Direction des acquisitions et  
des services bibliographiques

395, rue Wellington  
Ottawa (Ontario)  
K1A 0N4

Your file - Votre référence

Our file - Notre référence

## NOTICE

## AVIS

The quality of this microform is heavily dependent upon the quality of the original thesis submitted for microfilming. Every effort has been made to ensure the highest quality of reproduction possible.

If pages are missing, contact the university which granted the degree.

Some pages may have indistinct print especially if the original pages were typed with a poor typewriter ribbon or if the university sent us an inferior photocopy.

Reproduction in full or in part of this microform is governed by the Canadian Copyright Act, R.S.C. 1970, c. C-30, and subsequent amendments.

La qualité de cette microforme dépend grandement de la qualité de la thèse soumise au microfilmage. Nous avons tout fait pour assurer une qualité supérieure de reproduction.

S'il manque des pages, veuillez communiquer avec l'université qui a conféré le grade.

La qualité d'impression de certaines pages peut laisser à désirer, surtout si les pages originales ont été dactylographiées à l'aide d'un ruban usé ou si l'université nous a fait parvenir une photocopie de qualité inférieure.

La reproduction, même partielle, de cette microforme est soumise à la Loi canadienne sur le droit d'auteur, SRC 1970, c. C-30, et ses amendements subséquents.

# Local global methods in number theory

by

Vincenzo Acciaro, M.C.S.

A thesis submitted to  
the Faculty of Graduate Studies and Research  
in partial fulfillment of  
the requirements for the degree of  
Doctor of Philosophy

Ottawa-Carleton Institute for Computer Science

School of Computer Science

Carleton University

Ottawa, Ontario

May 29, 1995

© Copyright

1995, Vincenzo Acciaro



National Library  
of Canada

Acquisitions and  
Bibliographic Services Branch

395 Wellington Street  
Ottawa, Ontario  
K1A 0N4

Bibliothèque nationale  
du Canada

Direction des acquisitions et  
des services bibliographiques

395, rue Wellington  
Ottawa (Ontario)  
K1A 0N4

Your file    Votre référence

Our file    Notre référence

**The author has granted an irrevocable non-exclusive licence allowing the National Library of Canada to reproduce, loan, distribute or sell copies of his/her thesis by any means and in any form or format, making this thesis available to interested persons.**

**L'auteur a accordé une licence irrévocable et non exclusive permettant à la Bibliothèque nationale du Canada de reproduire, prêter, distribuer ou vendre des copies de sa thèse de quelque manière et sous quelque forme que ce soit pour mettre des exemplaires de cette thèse à la disposition des personnes intéressées.**

**The author retains ownership of the copyright in his/her thesis. Neither the thesis nor substantial extracts from it may be printed or otherwise reproduced without his/her permission.**

**L'auteur conserve la propriété du droit d'auteur qui protège sa thèse. Ni la thèse ni des extraits substantiels de celle-ci ne doivent être imprimés ou autrement reproduits sans son autorisation.**

ISBN 0-612-08831-6

**Canada**

Name

VINCENTO ACCIARO

Dissertation Abstracts International is arranged by broad, general subject categories. Please select the one subject which most nearly describes the content of your dissertation. Enter the corresponding four-digit code in the spaces provided.

COMPUTER SCIENCE

SUBJECT TERM

0000

SUBJECT CODE

U·M·I

## Subject Categories

## THE HUMANITIES AND SOCIAL SCIENCES

## COMMUNICATIONS AND THE ARTS

Architecture 0729  
Art History 0377  
Cinema 0900  
Dance 0378  
Fine Arts 0357  
Information Science 0723  
Journalism 0391  
Library Science 0399  
Mass Communications 0708  
Music 0413  
Speech Communication 0459  
Theater 0465

## EDUCATION

General 0515  
Administration 0514  
Adult and Continuing 0516  
Agricultural 0517  
Art 0273  
Bilingual and Multicultural 0282  
Business 0688  
Community College 0275  
Curriculum and Instruction 0727  
Early Childhood 0518  
Elementary 0524  
Finance 0277  
Guidance and Counseling 0519  
Health 0680  
Higher 0745  
History of 0520  
Home Economics 0278  
Industrial 0521  
Language and Literature 0279  
Mathematics 0280  
Music 0522  
Philosophy of 0998  
Physical 0523

Psychology 0525  
Reading 0535  
Religious 0527  
Sciences 0714  
Secondary 0533  
Social Sciences 0534  
Sociology of 0340  
Special 0529  
Teacher Training 0530  
Technology 0710  
Tests and Measurements 0288  
Vocational 0747

## LANGUAGE, LITERATURE AND LINGUISTICS

Language  
General 0679  
Ancient 0289  
Linguistics 0290  
Modern 0291  
Literature  
General 0401  
Classical 0294  
Comparative 0295  
Medieval 0297  
Modern 0298  
African 0316  
American 0591  
Asian 0305  
Canadian (English) 0352  
Canadian (French) 0355  
English 0593  
Germanic 0311  
Latin American 0312  
Middle Eastern 0315  
Romance 0313  
Slavic and East European 0314

## PHILOSOPHY, RELIGION AND

## THEOLOGY

Philosophy 0422  
Religion  
General 0318  
Biblical Studies 0321  
Clergy 0319  
History of 0320  
Philosophy of 0322  
Theology 0469

## SOCIAL SCIENCES

American Studies 0323  
Anthropology  
Archaeology 0324  
Cultural 0326  
Physical 0327  
Business Administration  
General 0310  
Accounting 0272  
Banking 0770  
Management 0454  
Marketing 0338  
Canadian Studies 0385  
Economics  
General 0501  
Agricultural 0503  
Commerce-Business 0505  
Finance 0508  
History 0509  
Labor 0510  
Theory 0511  
Folklore 0358  
Geography 0366  
Gerontology 0351  
History  
General 0578

Ancient 0579  
Medieval 0581  
Modern 0582  
Black 0328  
African 0331  
Asia, Australia and Oceania 0332  
Canadian 0334  
European 0335  
Latin American 0336  
Middle Eastern 0333  
United States 0337  
History of Science 0585  
Law 0398  
Political Science  
General 0615  
International Law and Relations 0616  
Public Administration 0617  
Recreation 0814  
Social Work 0452  
Sociology  
General 0626  
Criminology and Penology 0627  
Demography 0938  
Ethnic and Racial Studies 0631  
Individual and Family Studies 0628  
Industrial and Labor Relations 0629  
Public and Social Welfare 0630  
Social Structure and Development 0700  
Theory and Methods 0344  
Transportation 0709  
Urban and Regional Planning 0999  
Women's Studies 0453

## THE SCIENCES AND ENGINEERING

## BIOLOGICAL SCIENCES

Agriculture  
General 0473  
Agronomy 0285  
Animal Culture and Nutrition 0475  
Animal Pathology 0476  
Food Science and Technology 0359  
Forestry and Wildlife 0473  
Plant Culture 0479  
Plant Pathology 0480  
Plant Physiology 0817  
Range Management 0777  
Wood Technology 0746

## Biology

General 0306  
Anatomy 0287  
Biostatistics 0308  
Botany 0309  
Cell 0379  
Ecology 0329  
Entomology 0353  
Genetics 0369  
Limnology 0793  
Microbiology 0410  
Molecular 0307  
Neuroscience 0317  
Oceanography 0416  
Physiology 0433  
Radiation 0821  
Veterinary Science 0778  
Zoology 0472  
Biophysics  
General 0786  
Medical 0760

## EARTH SCIENCES

Biogeochemistry 0425  
Geochemistry 0996

Geodesy 0370  
Geology 0372  
Geophysics 0373  
Hydrology 0388  
Mineralogy 0411  
Paleobotany 0345  
Paleoecology 0426  
Paleontology 0418  
Paleozoology 0985  
Palynology 0427  
Physical Geography 0368  
Physical Oceanography 0415

## HEALTH AND ENVIRONMENTAL SCIENCES

Environmental Sciences 0768  
Health Sciences  
General 0566  
Audiology 0300  
Chemotherapy 0992  
Dentistry 0567  
Education 0350  
Hospital Management 0769  
Human Development 0758  
Immunology 0982  
Medicine and Surgery 0564  
Mental Health 0347  
Nursing 0569  
Nutrition 0570  
Obstetrics and Gynecology 0380  
Occupational Health and Therapy 0354  
Ophthalmology 0381  
Pathology 0571  
Pharmacology 0419  
Pharmacy 0572  
Physical Therapy 0382  
Public Health 0573  
Radiology 0574  
Recreation 0575

Speech Pathology 0460  
Toxicology 0383  
Home Economics 0386

## PHYSICAL SCIENCES

## Pure Sciences

Chemistry  
General 0485  
Agricultural 0749  
Analytical 0486  
Biochemistry 0487  
Inorganic 0488  
Nuclear 0738  
Organic 0490  
Pharmaceutical 0491  
Physical 0494  
Polymer 0495  
Radiation 0754  
Mathematics 0405  
Physics  
General 0605  
Acoustics 0986  
Astronomy and Astrophysics 0606  
Atmospheric Science 0608  
Atomic 0748  
Electronics and Electricity 0607  
Elementary Particles and High Energy 0798  
Fluid and Plasma 0759  
Molecular 0609  
Nuclear 0610  
Optics 0752  
Radiation 0756  
Solid State 0611  
Statistics 0463

## Applied Sciences

Applied Mechanics 0346  
Computer Science 0984

Engineering  
General 0537  
Aerospace 0538  
Agricultural 0539  
Automotive 0540  
Biomedical 0541  
Chemical 0542  
Civil 0543  
Electronics and Electrical 0544  
Heat and Thermodynamics 0348  
Hydraulic 0545  
Industrial 0546  
Marine 0547  
Materials Science 0794  
Mechanical 0548  
Metallurgy 0743  
Mining 0551  
Nuclear 0552  
Packaging 0549  
Petroleum 0765  
Sanitary and Municipal 0554  
System Science 0790  
Geotechnology 0428  
Operations Research 0796  
Plastics Technology 0795  
Textile Technology 0994

## PSYCHOLOGY

General 0621  
Behavioral 0384  
Clinical 0622  
Developmental 0620  
Experimental 0623  
Industrial 0624  
Personality 0625  
Physiological 0989  
Psychobiology 0349  
Psychometrics 0632  
Social 0451



The undersigned hereby recommend to  
The Faculty of Graduate Studies and Research  
acceptance of the thesis,

**Local global methods in number theory**  
submitted by

Vincenzo Acciario, M.C.S.

in partial fulfilment of the requirements  
for the degree of Doctor of Philosophy



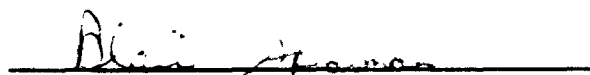
---

Director, School of Computer Science



---

Thesis Supervisor



External Examiner

Carleton University

July 13, 1995

# Abstract

The main results of this thesis are the following:

(i) Let  $F$  be an arbitrary field, and  $f(x)$  a polynomial in one variable over  $F$  of degree  $\geq 1$ . Given a polynomial  $g(x) \neq 0$  over  $F$  and an integer  $m > 1$  we give necessary and sufficient conditions for the existence of a polynomial  $z(x) \in F[x]$  such that  $z(x)^m \equiv g(x) \pmod{f(x)}$ . We show how our results can be specialized to  $\mathbf{R}$ ,  $\mathbf{C}$  and to finite fields. Since our proofs are constructive it is possible to translate them into an effective algorithm when  $F$  is a computable field (e.g. a finite field or an algebraic number field).

(ii) Let  $L = \mathbf{Q}[\alpha]$  be a cyclic number field of prime degree  $q$ , and let  $a$  be a nonzero rational number. We give an algorithm which takes as input  $a$  and the minimal polynomial of  $\alpha$  over  $\mathbf{Q}$ , and determines if  $a$  is the norm of an element of  $L$ . The algorithm runs in time polynomial in the size of the input, assuming the use of an oracle in order to obtain a complete factorization of  $a$  and a complete factorization of the discriminant  $d_L(\alpha)$  of  $\alpha$ . A generalization of the algorithm to cyclic number fields of squarefree degree is also presented. As an application, we give an algorithm to test if a cyclic algebra  $A = (E, \sigma, a)$  over  $\mathbf{Q}$  is a division algebra.

## Acknowledgements

I would like to express my most profound gratitude to Prof. J.D. Dixon, my thesis supervisor, for his patience, his invaluable advice and for everything that I learnt from him.

I would like to thank Prof. K.S. Williams for his many suggestions and his crucial support.

I would like to thank Prof. V.L. Plantamura, at the University of Bari, for his sincere and constant support.

Finally, I would like to thank my friends William and Elena Anselmi, Angelo Mingarelli, Marisol Montpetit, Lilli Nanni, Nicola Santoro and everyone else who made my permanence in Ottawa delightful.

*This thesis is dedicated to my parents Adamo and Laura Acciaro, my sister Anna and my little nephew Stefano.*



# Contents

<b>Abstract</b>	<b>iii</b>
<b>Acknowledgements</b>	<b>iv</b>
<b>List Of Tables</b>	<b>vi</b>
<b>List Of Figures</b>	<b>vii</b>
<b>1 Introduction</b>	<b>1</b>
1.1 From Local to Global . . . . .	3
1.2 Our contribution . . . . .	7
<b>2 Basic Definitions and Preliminary Results</b>	<b>12</b>
2.1 Basic Notation . . . . .	12
2.2 Some Preliminaries on Valuations . . . . .	13
2.3 Localization of a Dedekind Domain . . . . .	16
2.4 The Chinese Remainder Theorem . . . . .	18
2.5 Hensel's Lemma . . . . .	19
2.6 Some Results from Local Class Field Theory . . . . .	20
2.7 Some Results from Global Class Field Theory . . . . .	22
2.8 Encoding Data . . . . .	24

<b>3</b>	<b>Power roots of polynomials over arbitrary fields</b>	<b>25</b>
3.1	The method . . . . .	26
3.1.1	Lifting of zero . . . . .	31
3.1.2	The exponent $m$ is a multiple of $\text{char}(F)$ . . . . .	33
3.2	The complex case . . . . .	35
3.3	The real case . . . . .	36
3.4	Finite fields . . . . .	37
3.5	Arithmetic complexity . . . . .	37
3.6	Concluding remarks . . . . .	39
3.6.1	Factorization of polynomials over algebraic number fields . . . . .	40
3.6.2	A simple algorithm for extracting $m^{\text{th}}$ roots in $\mathbf{Q}[\alpha]$ . . . . .	43
3.6.3	Factorization of polynomials over finite fields . . . . .	45
3.6.4	Finding $m^{\text{th}}$ roots in finite fields . . . . .	46
<b>4</b>	<b>Norm equations over cyclic number fields of prime degree</b>	<b>52</b>
4.1	The unramified case . . . . .	54
4.2	The totally ramified case . . . . .	54
4.3	The finite primes: summarizing . . . . .	56
4.4	The case of infinite primes . . . . .	58
4.5	The complete algorithm . . . . .	58
<b>5</b>	<b>Recognizing the decomposition type of a rational prime</b>	<b>63</b>
5.1	Integral basis known . . . . .	63
5.1.1	Recognizing the inert primes . . . . .	64
5.1.2	Finding Eisenstein Elements . . . . .	67
5.2	Integral basis unknown . . . . .	70
5.2.1	Implementation and complexity issues . . . . .	77
5.3	Computational examples . . . . .	84
5.3.1	Discriminant of the form $p^{q-1}$ or $q^{2^r-2}$ . . . . .	84

5.3.2	Some computed examples . . . . .	87
<b>6</b>	<b>Norm equations over cyclic number fields of squarefree degree</b>	<b>90</b>
6.1	Reduction to the prime degree case . . . . .	90
6.1.1	Computation of the minimal subfields of $E$ . . . . .	93
6.1.2	The complete test . . . . .	94
6.1.3	Implementation issues. . . . .	97
<b>7</b>	<b>Test of cyclic algebras over <math>\mathbb{Q}</math> for zero divisors</b>	<b>100</b>
<b>8</b>	<b>On the discriminant of cyclic number fields of odd prime degree</b>	<b>105</b>
8.1	Eisenstein polynomials . . . . .	106
8.2	Finding Eisenstein elements . . . . .	108
8.3	$p$ is totally and tamely ramified . . . . .	109
8.4	$p$ is totally and wildly ramified . . . . .	111
8.5	Some remarks . . . . .	115
8.6	Computational examples . . . . .	115
8.6.1	Discriminant of the form $p^{q-1}$ with $p \neq q$ . . . . .	117
8.6.2	Discriminant of the form $q^{2q-2}$ . . . . .	118
8.6.3	Discriminant of the form $p^{q-1}q^{2q-2}$ with $p \neq q$ . . . . .	122
8.7	Concluding remarks . . . . .	124
	<b>References</b>	<b>125</b>

## List of Tables

3.1	Roots of cyclotomic polynomials from $C_3$ to $C_{15}$ . . . . .	50
3.2	Roots of cyclotomic polynomials from $C_{16}$ to $C_{20}$ . . . . .	51
5.1	First 100 positive integers which are norms from $L = \mathbb{Q}[\alpha]$ , where $\alpha$ is a root of $x^5 + x^4 - 4x^3 - 3x^2 + 3x + 1$ . . . . .	87
5.2	First 100 positive integers which are norms from $L = \mathbb{Q}[\alpha]$ , where $\alpha$ is a root of $x^3 - x^2 - 82x + 311$ . . . . .	88

## List of Figures

4.1	The algorithm NORM. . . . .	62
5.1	The algorithm DECOMPOSE. . . . .	85
5.2	Auxiliary procedure used by DECOMPOSE. . . . .	89
6.1	The algorithm NORMSQF. . . . .	99
7.1	The algorithm SKEWFIELD. . . . .	104
8.1	The algorithm CONSTRUCT. . . . .	112
8.2	The algorithm TAME. . . . .	112
8.3	The algorithm WILD. . . . .	116
8.4	A Maple program to construct wild examples. . . . .	123

## Chapter 1 -

# Introduction

This thesis is about computational methods in number theory that rely heavily upon localization.

Why a thesis in computational number theory? In order to answer this question, we will spend some words to illustrate what are the two major trends in this area today.

On the one hand researchers in number theory are interested in practical algorithms that they can run on their computers in order to test some hypothesis or just for the sake of mathematical curiosity. Hence they need good algorithms, where good means practical. We think that in this context the following sentence, pronounced by H.P.F. Swinnerton-Dyer at his lecture at the Brighton Conference [19] in 1965, is still pertinent (although the figures may have changed in thirty years).

*A calculation that takes  $10^6$  operations is trivial, and is worth doing even if its results will probably be useless. A calculation that takes  $10^9$  operations is substantial, but not unreasonable. It is worth doing in pursuit of any serious idea, but not just in the hope that something may turn up; moreover, the method of calculation should now be reasonably efficient, whereas for a smaller problem one chooses the simplest possible method*

*in order to minimize the effort of writing a program. Finally a calculation that takes  $10^{12}$  operations is close to the limit of what is physically possible; it can only be justified by a major scientific advance such as landing a man on the moon.*

The trend of research that puts its emphasis on practical algorithms is well represented by the book of M. Pohst and H. Zassenhaus [78] and by the recent book of H. Cohen [23]. In fact, the algorithms described in [78] ‘yield good to excellent results for number fields of small degree and not too large discriminant’ [78, Preface], and the algorithms described in [23] have been implemented in the package PARI [11], developed in France by Prof. H. Cohen and his collaborators.

Another trend of research considers algorithms in algebraic number theory for their own sake rather than with any view toward applications. This trend is well represented by H.W. Lenstra’s survey paper [58]. Here an algorithm is considered better than another if ‘for each positive real number  $N$  it is at least  $N$  times as fast for all but finitely many values of the input data’, in other words if its asymptotic complexity is better. However, in the same paper [58] Lenstra points out that an algorithm which is good according to his definition might not be good for practical purposes.

In some areas of computer science an algorithm is considered just an object of mathematical research, rather than a tool to use. This point of view may produce algorithms that are asymptotically polynomial in time and space, but that cannot be tested even on very small examples because of the large constants involved in the function that describes their temporal behavior.

On the contrary, the objective of our research has been the design of algorithms which are at the same time *asymptotically good*, i.e. whose running time is polynomial in the size of the input, and *practical*, i.e. really work.

The algorithms described here have been implemented using the number theory package PARI [11]. Our tests show that they yield good results, as far as it concerns the execution time, with inputs of very large size. Needless to say, part of the merit goes to the high efficiency of the package PARI.

Before discussing our contribution to the research, we would like to spend some words about the local to global method in number theory.

## 1.1 From Local to Global

The concept of localization is common, often with different meanings, in the natural sciences.

We will take for granted the fact that generally it is quite easy to tackle a problem locally, whereas it is more difficult if not impossible to tackle the same problem globally. We have many examples of this behavior in mathematics, e.g. in the theory of optimization, where finding a local minimum of a function is generally easier than finding a global minimum.

If we restrict our attention to algebra and number theory, we have a classical extreme example: consider the equation

$$x^n + y^n + z^n = 0 \quad (n > 2) \quad (1.1)$$

It is well known that, for a given  $n$ , the problem of determining the solvability of (1.1) in the integers is extremely difficult. On the other hand, the solvability of (1.1) modulo a given prime  $p$  (a local problem), can be determined, if not easily, at least in a finite number of steps.

Fortunately in many cases it is possible to gather together the local solutions of a given problem, in order to deduce some properties of the original solution, which we call for this reason the 'global' solution – in some cases we are able to obtain complete informations about the global solution.

We will call this process the *local to global method*. It is easily seen that, from a problem solving point of view, we have just rediscovered the idea of 'divide and conquer' familiar to researchers in design and analysis of algorithms.

In this section we will illustrate some successful examples of the application of the local to global method in number theory, in order to give a concrete motivation to our approach to the subject.



The archetype in the universe of our discourse is certainly the Chinese Remainder Theorem, which has been known for at least fifteen centuries – according to D.E. Knuth [49, p. 271], a special case of this theorem was stated by the Chinese mathematician Sun Tsu, between 280 and 473 A.D.

The Chinese Remainder Theorem is one of the nicest examples of constructive mathematics, since its proof is really an algorithm.

In its most classical formulation this theorem states that, given  $r$  integers  $m_1, \dots, m_r$  relatively prime, and  $r$  arbitrary integers  $l_1, \dots, l_r$ , it is always possible to find an integer  $m$  such that  $m \equiv l_i \pmod{m_i}$  for  $i = 1, \dots, r$ . The integer  $m$  is uniquely defined modulo the product  $m_1 \cdots m_r$ .

Let us consider the class of mathematical problems whose solution is an integer. Very often it is easier to obtain a solution of a given problem in this class modulo a prime  $p$ , rather than modulo an arbitrary integer  $m$ . The reason lies in the fact that the residue classes of the integers modulo  $p$  form a field, and so ‘division is possible’. The transition from a solution modulo  $p$  to a solution modulo  $p^n$ , where  $n$  is a positive integer, is in some cases made possible by Newton’s method.

Given a simple root  $a_1$  of a polynomial equation modulo  $p$ , Newton’s method allows one to ‘lift’ it to a root  $a_2$  of the same polynomial equation modulo  $p^2$ , and then again lift  $a_2$  to a root  $a_3$  modulo  $p^3$ , and so on ... forever! Moreover  $a_i \equiv a_{i+1} \pmod{p^i}$ , for  $i = 1, 2, \dots$ .

The nice thing about Newton’s method is that at each step, we are only required to work modulo  $p$ , that is in the finite field  $\mathbb{F}_p$  of  $p$  elements. This process of ameliorating an initial solution is called  $p$ -adic lifting, or  $p$ -adic refinement.

It is natural at this point to introduce the following notion. For a fixed prime  $p$ , consider the sequence of rings  $\{\mathbb{Z}/p^i\mathbb{Z}\}_{i=0,1,\dots}$  together with the natural mappings  $\mathcal{N}_i : \mathbb{Z}/p^i\mathbb{Z} \rightarrow \mathbb{Z}/p^{i-1}\mathbb{Z}$ , which are clearly surjective. Form all the possible infinite sequences  $a = (a_0, a_1, a_2, \dots)$ , with  $a_i \in \mathbb{Z}/p^i\mathbb{Z}$  ( $i = 0, 1, \dots$ ) and  $a_{i-1} = \mathcal{N}_i(a_i)$  ( $i = 1, 2, \dots$ ). Since each  $\mathcal{N}_i$  is surjective, given an element  $a_i \in \mathbb{Z}/p^i\mathbb{Z}$  we can always find an element  $a_{i+1} \in \mathbb{Z}/p^{i+1}\mathbb{Z}$  such that  $a_i = \mathcal{N}_{i+1}(a_{i+1})$ , and so such sequences exist. Define the two operations of addition and multiplication on these sequences

componentwise. Then these sequences form a ring, called the projective limit of the rings  $\mathbb{Z}/p^i\mathbb{Z}$  and denoted by  $\lim(\mathbb{Z}/p^i\mathbb{Z})$ . It is usual to write  $\mathbb{Z}_p$  for the ring  $\lim(\mathbb{Z}/p^i\mathbb{Z})$  and call it the ring of  $p$ -adic integers.

It is clear that Newton's method, when applicable, produces a solution of the original polynomial equation in  $\lim(\mathbb{Z}/p^i\mathbb{Z})$ .

Note that some authors [24, Definition 14.49, p. 153] use Newton's method to define the ring of  $p$ -adic integers, although we think that it is more natural to proceed the other way around.

Newton's method and the Chinese Remainder Theorem are two ubiquitous ingredients of computational number theory. Together, they have been successfully applied to solve computationally the most disparate problems in number theory (see [60] and [96] for an overview of their applications). See [28] for an example of their application for finding the exact rational solution of a regular system  $Ax = b$  of linear equations with integral coefficients.

Given the ring  $\lim(\mathbb{Z}/p^i\mathbb{Z})$ , which turns out to be an integral domain, we can form its field of quotients, denoted by  $\mathbb{Q}_p$  and called the field of  $p$ -adic numbers, by adjoining the rational number  $1/p$ .  $\mathbb{Q}_p$  is a *local field*, that is a locally compact non discrete topological field, and in this sense it shares many properties of the field  $\mathbb{R}$  of reals and of the field  $\mathbb{C}$  of complex numbers, which are local fields as well.

However,  $\mathbb{Q}_p$  is totally disconnected, while  $\mathbb{R}$  and  $\mathbb{C}$  are connected. Moreover,  $\mathbb{Z}_p$  is embedded in  $\mathbb{Q}_p$  as a compact, open subring, while no such subrings exist for  $\mathbb{R}$  or  $\mathbb{C}$ .

Although  $\mathbb{Q}_p$  is an infinite and uncountable extension of  $\mathbb{Q}$ , it is conceptually easy to handle, since a  $p$ -adic number is simply a  $p$ -adic integer divided by a suitable power of  $p$ .

The introduction of the  $p$ -adic numbers [44] opened new and unexplored horizons to mathematical research, and allowed number theorists to solve elegantly some problems which had been open for long time.

An early and striking result in this direction is the Theorem of Hasse-Minkowski about the zeroes of quadratic forms. It states that a quadratic form with rational

coefficients admits a nontrivial zero over the rationals if and only if it admits a nontrivial zero over  $\mathbb{Q}_p$ , for all the primes  $p$ , and over  $\mathbb{R}$ . A variant of this theorem asserts that two quadratic forms with rational coefficients are equivalent over the rationals if and only if they are equivalent over  $\mathbb{Q}_p$ , for all the primes  $p$ , and over  $\mathbb{R}$ .

The ideas discussed above can be generalized to other rings. The rings of most interest to number theorists are the Dedekind Domains: the class of Dedekind Domains is quite large, since it includes amongst others the Principal Ideal Domains. We recall here that a Dedekind Domain is a ring which is Noetherian, integrally closed, and where each prime ideal is maximal. Dedekind Domains arise naturally in number theory as the ring of integers of algebraic number fields. The unique factorization of integers into the product of primes is replaced in Dedekind Domains by the unique factorization of ideals into the product of prime ideals.

In this thesis we will deal with rings of integers of algebraic number fields and also with the following instances of Dedekind Domains, which by chance happen to be Principal Ideal Domains as well:

- The ring  $F[x]$  of polynomials in one variable over a field  $F$ ;
- The localization of the ring of integers of an algebraic number field at a prime ideal;
- The ring of integers of a field complete with respect to a nonarchimedean valuation.

For the class of Dedekind Domains there is a corresponding version of the Chinese Remainder Theorem and of Hensel's Lemma – now, of course, the role of the prime integers is played by the prime ideals. Again, given a Dedekind Domain  $\mathcal{O}$ , it is possible to define the ring of the  $\mathcal{P}$ -adic integers, where  $\mathcal{P}$  is a prime ideal of  $\mathcal{O}$ , as the projective limit  $\lim(\mathcal{O}/\mathcal{P}^i\mathcal{O})$ , and then define the field of  $\mathcal{P}$ -adic numbers as its field of quotients.

In the next section we describe the main results that we obtain in this thesis.

## 1.2 Our contribution

In this thesis we present algorithmic solutions to some problems in computational number theory. Our algorithms, or their proofs of correctness, rely heavily upon the local to global principle discussed above.

In Chapter 3 we consider the following problem:

### **Power roots of polynomials.**

*Let  $F$  be an arbitrary field,  $m$  an integer greater than one,  $f(x)$  a polynomial in one variable over  $F$  of degree  $\geq 1$ , and  $g(x) \neq 0$  a polynomial over  $F$ . Find necessary and sufficient conditions for the existence of a polynomial  $z(x) \in F[x]$  such that  $z(x)^m \equiv g(x) \pmod{f(x)}$ . If  $z(x)$  exists, find it.*

This problem originated from a paper of J.B. Miller [69], where the author gives some sufficient conditions for the existence of a polynomial  $z(x) \in F[x]$  such that  $z(x)^m \equiv g(x) \pmod{f(x)}$ , when  $F$  is the field  $\mathbf{R}$  of real numbers or the field  $\mathbf{C}$  of complex numbers. Miller explicitly states in [69] that the conditions given are not necessary.

Using standard tools (Newton's method and the Chinese Remainder Theorem) we extend Miller's results by giving both *necessary and sufficient* conditions for the existence of an  $m^{\text{th}}$  root in  $F[x]/(f(x))$ , when  $F$  is any field, not necessarily  $\mathbf{C}$  or  $\mathbf{R}$ . While the methods used by Miller in [69] are analytical, ours are purely algebraic. In particular, we show how our theoretical results can be specialized to the field  $\mathbf{R}$  of real numbers, the field  $\mathbf{C}$  of complex numbers, and to finite fields. Moreover, since our proofs are constructive, our method can be directly translated into a computer program when  $F$  is any computable field (e.g. an algebraic number field or a finite field).

In Chapter 4 we consider the following problem:

### **Norm group membership I.**

*Let  $L = \mathbf{Q}[\alpha]$  be a cyclic number field of prime degree  $q$ , given by the*

*minimal polynomial  $m_\alpha(x)$  of  $\alpha$  over  $\mathbb{Q}$ , and let  $a$  be a nonzero rational number. Decide if  $a$  is the norm of some element of  $L$ .*

In Chapters 4 and 5 we give an algorithm to solve this problem. Under the assumption that we have a complete factorization of  $a$  and a complete factorization of the discriminant  $d_L(\alpha)$  of  $\alpha$ , our algorithm runs in time polynomial in the size of the input.

The theoretical solution to the norm membership problem stated above lies in a very elegant result in number theory, known as Hasse's Norm Theorem, from H. Hasse who formulated it in 1926. This theorem states that, given a cyclic extension  $K/k$  of global fields, a nonzero element of  $k$  is a norm of an element of  $K$  if and only if it is a local norm everywhere, that is at all the possible completions, including the archimedean ones. In our case  $k = \mathbb{Q}$ , and  $K = L$ .

In Chapter 4 we prove that the set of finite primes that must be taken into consideration in order to apply the Hasse Norm Theorem to our problem is actually finite, and that the infinite primes play a role only in the case of quadratic fields.

In order to translate the Hasse Norm Theorem into an efficient algorithm, we need a polynomial time algorithm to solve the following subproblem:

#### **Decomposition of a rational prime.**

*Determine if a rational prime  $p$  is inert, splits or else ramifies in  $L$ . If  $p$  ramifies, then find an element  $\pi \in L$  whose minimal polynomial  $m_\pi(x)$  is Eisenstein at  $p$ .*

We consider the problem 'Decomposition of a rational prime' in Chapter 5. We develop two algorithms to solve the problem, depending whether an integral basis for  $L$  is known, or not. We recall here that there is an algorithm due to M. Pohst and H. Zassenhaus [77] that finds an integral basis of an algebraic number field in polynomial time, assuming the use of oracles for factoring integers and factoring polynomial over finite fields. In practice, the algorithm of Pohst and Zassenhaus is 'good' for fields of small degree and discriminant of moderate size.

The first algorithm takes as input  $p$  and an integral basis  $\Gamma$  for  $L$ , and it solves the problem stated above in time polynomial in the size of the input.

The second algorithm takes as input  $p$  and the minimal polynomial  $m_\alpha(x)$  of  $\alpha$  and it solves the problem stated above again in time polynomial in the size of the input.

Needless to say it, the first algorithm is conceptually much easier than the second one.

In Chapter 6 we extend the algorithm given in Chapter 4 to cyclic number fields of squarefree degree, that is we give an algorithm to solve the following problem:

### **Norm group membership II.**

*Let  $E = \mathbb{Q}[\nu]$  be a cyclic number field of squarefree degree  $n$ , given by the minimal polynomial  $m_\nu(x)$  of  $\nu$  over  $\mathbb{Q}$ , and let  $a$  be a nonzero rational number. Decide if  $a$  is the norm of some element of  $E$ .*

We prove that it is enough to consider the same problem over all the minimal subfields of  $E$ , which turn out to be cyclic of prime degree, and we show how to compute these.

If we assume that we are allowed to call an oracle in order to obtain a complete factorization of  $a$  and a complete factorization of the discriminant  $d_L(\nu)$  of  $\nu$ , then we can prove that the extended algorithm runs again in time polynomial in the size of the input.

In Chapter 7 we give an application of the algorithms developed in Chapters 4 and 5 to a computational problem on finite dimensional associative algebras over the rationals.

Before stating the problem let us recall some definitions from the theory of finite dimensional associative algebras.

Let  $A$  be a finite dimensional associative algebra over a field  $F$ . An element  $a \in A$  is called a *divisor of zero* if there is a nonzero element  $b \in A$  such that  $ab = 0$ ; an algebra without nonzero divisors of zero is called a *division algebra*. An algebra  $A$  is said to be *simple* if it does not possess any nontrivial two sided ideal, and *central*

if its center is equal to the base field. An algebra  $A$  of dimension  $n$  over a field  $F$  is said to be *cyclic* if it is central simple over  $F$ , and it has a cyclic subfield of degree  $\sqrt{n}$  over  $F$ . There is a standard way of presenting a cyclic algebra [76, p. 277] as a triple  $(M, \sigma, a)$ , where  $M$  is the cyclic subfield of degree  $\sqrt{n}$  over  $F$ ,  $\sigma$  is a generator of the Galois group of  $M/F$ , and  $a$  is a nonzero element of  $F$ .

L. Rónyai in a series of papers [80, 81, 83, 46, 84, 85] considered the problem of deciding if a finite dimensional central simple algebra over an arbitrary number field has zero divisors. Rónyai assumes that the algebra is given by a set of structure constants, and he attacks the problem using sophisticated tools from noncommutative number theory (i.e. the theory of maximal orders in noncommutative domains). Rónyai's algorithm is very powerful, since it computes the *index* of the algebra (for the definition of 'index' see Chapter 7), thus allowing one to get a lot of information about the structure of the algebra. Rónyai's algorithm runs in time polynomial in the size of the input, assuming the use of oracles for factorization.

Note that, giving an algebra by a set of structure constants, or what is the same by its regular representation, is no doubt a very inefficient way. Often, other *presentations* and/or *representations* of an algebra are preferred, either because they arise as the natural choice, or because they are much more compact. For example, in order to give the group algebra over a field  $F$  of a group  $G$ , it is enough to specify a description of  $F$  and a presentation of  $G$ .

Now, by the theorem of Albert-Hasse-Brauer-Noether [76, p. 359], if  $F$  is a number field then the class of cyclic algebras over  $F$  coincides with the class of central simple algebras over  $F$ . In particular, every central simple algebra  $A$  over  $\mathbb{Q}$  is cyclic, and hence  $A$  admits a very compact presentation as a triple  $(M, \sigma, a)$ .

To our knowledge, the problem of deciding algorithmically if a cyclic algebra  $A = (M, \sigma, a)$  over the rationals has zero divisors has not been considered so far. This will be the last problem considered in this thesis, that we state as

### **Test for divisors of zero.**

*Let  $A = (M, \sigma, a)$  be a cyclic algebra over the rationals. Assume that the field  $M$  is given by the minimal polynomial  $m_c(x)$  of a primitive element*

*c for  $M/\mathbb{Q}$ , the automorphism  $\sigma$  is given as a polynomial  $i(x)$  over  $\mathbb{Q}$ , such that  $i(c) = \sigma(c)$ , and  $a$  is a nonzero rational number. Decide if  $A = (M, \sigma, a)$  is a division algebra.*

In Chapter 7 we present our algorithmic solution to this problem. We prove that, if we assume that we are allowed to call an oracle in order to obtain a complete factorization of  $a$  and a complete factorization of the discriminant  $d_M(c)$  of  $c$ , then the algorithm runs in time polynomial in the size of the input.

A theorem of A.A. Albert allows us to reduce this problem to the problem of deciding if the rational number  $a$  is a norm from any minimal subfield of  $M$ . Since all the minimal subfields of  $M$  are cyclic of prime degree, we can then exploit the algorithms developed in Chapters 4 and 5.

In Chapter 8 we will consider the following problem:

### **Decomposition of a rational prime II.**

*Let  $L = \mathbb{Q}[\alpha]$  be a cyclic number field of odd prime degree  $q$ , given by the minimal polynomial  $m_\alpha(x)$  of  $\alpha$  over  $\mathbb{Q}$ . Decide if a rational prime  $p$  ramifies in  $L$ . If  $p$  ramifies, then find an element  $\pi \in L$  whose minimal polynomial  $m_\pi(x)$  is Eisenstein at  $p$ .*

We show that, if we do not require to know if a non ramified prime  $p$  splits or it is inert, then it is possible to devise a very simple algorithm to solve the problem.

The algorithm takes as input  $p$  and the minimal polynomial  $m_\alpha(x)$  of  $\alpha$ . Experiments show that the running time of this algorithm is slightly better than the running time of the algorithm described in Chapter 5, although the minimal polynomial  $m_\pi(x)$  of the element  $\pi$  found by the algorithm might have a larger size.



## Chapter 2

# Basic Definitions and Preliminary Results

In this chapter we recall some basic definitions from algebraic number theory and class field theory, and we state without proof some basic results needed in the proof of our theorems.

## 2.1 Basic Notation

If  $B$  is a subgroup of a group  $A$ ,  $(A : B)$  will denote the index of  $B$  in  $A$ . When  $m$  is a positive integer,  $A^m$  will denote the subgroup of  $A$  generated by the  $m^{\text{th}}$  powers of the elements of  $A$ .

The symbol  $\deg f(x)$  will denote the degree of the polynomial  $f(x)$ .

If  $k$  is a subfield of a field  $K$ ,  $[K : k]$  will denote the degree of the field extension  $K/k$ , and  $K^* = K \setminus \{0\}$  will denote the multiplicative group of  $K$ .

As usual  $\mathbf{Q}$  will denote the field of rational numbers,  $\mathbf{R}$  the field of real numbers,  $\mathbf{C}$  the field of complex numbers,  $\mathbf{Z}$  the ring of integers and  $\mathbf{N}$  the natural integers. When  $m$  is a prime power, the symbol  $\mathbf{F}_m$  will denote the finite field of  $m$  elements.

When  $K$  is a normal separable extension of a field  $k$  the symbol  $\text{Gal}(K/k)$  will denote the Galois group of  $K$  over  $k$ .

When  $\alpha$  is an algebraic number, the minimal polynomial of  $\alpha$  over  $\mathbf{Q}$  will be denoted simply by  $m_\alpha(x)$ .

Let  $K$  be an algebraic number field, of degree  $n$  over  $\mathbb{Q}$ . The symbol  $\mathcal{O}_K$  will denote the ring of integers of  $K$ , that is the algebraic closure of  $\mathbb{Z}$  in  $K$ . The symbol  $d_K$  will denote the discriminant of  $K$ . If  $\beta \in K$ , then the symbol  $d_K(\beta)$  will denote the discriminant of the  $n$ -tuple  $(1, \beta, \dots, \beta^{n-1})$ .

Let us assume now that  $\mathcal{O}_k$  is a Dedekind Domain, with quotient field  $k$ . Recall that a *Dedekind Domain* is a ring which is Noetherian, integrally closed, and such that every nonzero prime ideal is maximal.

Given a finite extension  $K$  of  $k$ , then the integral closure of  $\mathcal{O}_k$  in  $K$  is a Dedekind Domain as well, denoted by  $\mathcal{O}_K$ .

If  $\mathcal{Q}$  is a prime ideal of  $\mathcal{O}_K$ , then  $\mathcal{P} = \mathcal{Q} \cap k$  is a prime ideal of  $k$ , and we say that  $\mathcal{Q}$  lies above  $\mathcal{P}$  or that  $\mathcal{Q}$  divides  $\mathcal{P}$ .

The field  $\mathcal{O}_k/\mathcal{P}$  is naturally embedded in the field  $\mathcal{O}_K/\mathcal{Q}$ . The degree  $[\mathcal{O}_K/\mathcal{Q} : \mathcal{O}_k/\mathcal{P}]$  is called the inertial degree of  $\mathcal{Q}$  over  $\mathcal{P}$  and is denoted by  $f(\mathcal{Q}|\mathcal{P})$ . The exact power of  $\mathcal{Q}$  dividing  $\mathcal{P}\mathcal{O}_K$  is called the ramification index of  $\mathcal{Q}$  over  $\mathcal{P}$  and is denoted by  $e(\mathcal{Q}|\mathcal{P})$ .

When  $K$  is a Galois extension of  $k$ , and  $\mathcal{P}$  is a prime ideal of  $\mathcal{O}_k$ , then the Galois group  $\text{Gal}(K/k)$  permutes transitively the prime ideals of  $\mathcal{O}_K$  lying above  $\mathcal{P}$ . From this it follows that all the prime ideals above  $\mathcal{P}$  have the same ramification index, denoted by  $e(\mathcal{P})$ , and the same inertial degree, denoted by  $f(\mathcal{P})$ . If we denote by  $g(\mathcal{P})$  the number of prime ideals lying above  $\mathcal{P}$  then the equality  $e(\mathcal{P})f(\mathcal{P})g(\mathcal{P}) = [K : k]$  holds.

## 2.2 Some Preliminaries on Valuations

In this section we recall the definition of valuation of a field and of completion of a field with respect to a given valuation. For a very elegant account of the theory of valuations we refer the reader to [7].

A function  $x \mapsto |x|$  from a field  $K$  to the reals is called a *valuation* if

- (i).  $|x| \geq 0$  for all  $x \in K$ , and  $|x| = 0$  if and only if  $x = 0$ ;

$$(ii). |x| \cdot |y| = |xy|;$$

$$(iii). |x + y| \leq |x| + |y|.$$

If in addition the valuation satisfies the stronger inequality:

$$|x + y| \leq \max(|x|, |y|)$$

then we say that the valuation is *non-archimedean*, otherwise the valuation is called *archimedean*. For a non-archimedean valuation the set  $\{x \in K \mid |x| \leq 1\}$  is a ring, called the *valuation ring* of  $K$ .

A valuation endows the field  $K$  with the structure of a metric space, by defining the distance  $d$  between two points as follows:

$$d(x, y) = |x - y| \quad x, y \in K$$

Two valuations are said to be equivalent if they induce the same topology on  $K$ . We define a *prime* of  $K$  to be a set of equivalent valuations of  $K$ .

When  $K$  is an algebraic number field we distinguish between the *finite primes* of  $K$  and the *infinite primes* of  $K$ , depending on the non-archimedean or archimedean nature of the corresponding valuations.

The finite primes are in one to one correspondence with the prime ideals of  $\mathcal{O}_K$ , the ring of integers of  $K$ . We will use the same symbol to denote a finite prime of  $K$  and the corresponding prime ideal of  $\mathcal{O}_K$ .

The infinite primes are in one to one correspondence with the embeddings  $\sigma$  of  $K$  into  $\mathbb{C}$ , the field of complex numbers. Namely, a real infinite prime is an embedding  $\sigma : K \rightarrow \mathbb{R}$ , and a non-real (complex) infinite prime is a pair of complex conjugate embeddings  $\sigma, \bar{\sigma}$  of  $K$  into  $\mathbb{C}$ , with  $\sigma \neq \bar{\sigma}$ .

Let  $\mathcal{P}$  be a finite prime of  $K$ . If  $\beta \in K$  and  $\beta \neq 0$ , we will denote by  $\nu_{\mathcal{P}}(\beta)$  the order of  $\beta$  at  $\mathcal{P}$ , that is, the power of  $\mathcal{P}$  in the factorization of the fractional ideal  $\beta\mathcal{O}$ . We define  $\nu_{\mathcal{P}}(0)$  to be  $\infty$ .

All the equivalent valuations of  $K$  belonging to the finite prime  $\mathcal{P}$  are of the form

$$\beta \mapsto c^{\nu_{\mathcal{P}}(\beta)}$$

where  $0 < c < 1$  is a fixed constant. We call any of them a  $\mathcal{P}$ -adic valuation of the field.

**Remark.** When  $K = \mathbb{Q}$  and  $p$  is a rational prime, by abuse of language we will write  $p$  for the prime corresponding to the ideal  $p\mathbb{Z}$ . If  $b \in \mathbb{Q}$  and  $b \neq 0$ , then  $\nu_p(b)$  will denote the order of  $b$  at  $p$ , that is, the power of the ideal  $p\mathbb{Z}$  in the factorization of the fractional ideal  $b\mathbb{Z}$ . We define  $\nu_p(0)$  to be  $\infty$ .

In the set of equivalent valuations determined by a prime of  $K$ , we select a canonical one as follows.

The *normalized valuation* of  $K$  with respect to a finite prime  $\mathcal{P}$  is defined to be the function

$$j \mapsto \mathcal{N}(\mathcal{P})^{-\nu_{\mathcal{P}}(j)}$$

where  $\mathcal{N}(\mathcal{P})$  denotes the absolute norm of  $\mathcal{P}$ , that is the number of elements in the quotient ring  $\mathcal{O}_K/\mathcal{P}$ .

The *normalized valuation* of  $K$  with respect to a real infinite prime  $\sigma$  is defined to be the function

$$a \mapsto |\sigma(a)|$$

where  $|\sigma(a)|$  denotes the ordinary absolute value of the real number  $\sigma(a)$ .

The *normalized valuation* of  $K$  with respect to a non-real infinite prime  $\sigma$  is defined to be the function

$$a \mapsto |\sigma(a)|^2$$

where  $|\sigma(a)|$  denotes the modulus of the complex number  $\sigma(a)$ .

Since a valuation endows  $K$  with the structure of a metric space, given a prime  $\mathcal{D}$  of  $K$  we can form the completion  $K_{\mathcal{D}}$  of  $K$  with respect to the normalized valuation determined by  $\mathcal{D}$ .

When  $\sigma$  is an infinite prime, then  $K_{\sigma}$  can be given the structure of a field, isomorphic either to  $\mathbb{R}$  or to  $\mathbb{C}$ .

When  $\mathcal{P}$  is a finite prime, then  $K_{\mathcal{P}}$  can be given the structure of a field, called the field of  $\mathcal{P}$ -adic numbers. In this case, the set  $\{x \in K_{\mathcal{P}} \mid \nu_{\mathcal{P}}(x) \geq 0\}$  is a subring

of  $K_{\mathcal{P}}$ , denoted by  $\mathcal{O}_{\mathcal{P}}$  and called the ring of  $\mathcal{P}$ -adic integers. The group of units of  $\mathcal{O}_{\mathcal{P}}$  will be denoted by  $U_{\mathcal{P}}$ .

Moreover, when  $p$  is a rational prime, the symbol  $\mathbb{Q}_p$  will denote the field of  $p$ -adic numbers,  $\mathbb{Z}_p$  the ring of  $p$ -adic integers, and  $U_p$  the group of units of  $\mathbb{Z}_p$ .

Let  $K/k$  be an extension of algebraic number fields. If  $\mathcal{Q}$  is a finite prime of  $K$  and  $\mathcal{P}$  is the unique prime of  $k$  lying below  $\mathcal{Q}$ , then  $k_{\mathcal{P}}$  can be embedded algebraically and topologically in  $K_{\mathcal{Q}}$ . To simplify matters, we identify  $k_{\mathcal{P}}$  with its embedding in  $K_{\mathcal{Q}}$ .

The following theorem shows that the property of an extension of number fields of being Galois is preserved by the completions at the finite primes.

**Theorem 2.1** *Let  $K$  be a finite Galois extension of an algebraic number field  $k$ . Let  $\mathcal{P}$  be a finite prime of  $k$  and  $\mathcal{Q}$  be a prime of  $K$  lying above  $\mathcal{P}$ . Then  $K_{\mathcal{Q}}/k_{\mathcal{P}}$  is also Galois, and the Galois groups  $\text{Gal}(K_{\mathcal{Q}}/k_{\mathcal{P}})$  and  $\text{Gal}(K/K \cap k_{\mathcal{P}})$  are isomorphic.*

*Proof.* See [76, p. 347, Corollary c].  $\square$

## 2.3 Localization of a Dedekind Domain

In this section we recall the concept of *localization* of a ring, and we state some theorems for future reference.

Although localization can be defined for general rings, and even for non integral domains (see [8, p. 36]), here we will restrict our attention to Dedekind Domains.

Let  $\mathcal{O}$  be a Dedekind Domain with quotient field  $k$ . We say that a subset  $S$  of  $\mathcal{O}$  is a multiplicative set if it contains the unity of  $\mathcal{O}$  and it is closed under multiplication.

The set  $S^{-1}\mathcal{O}$  of quotients  $r/s$  with  $r \in \mathcal{O}$  and  $s \in S$  is a subring of  $k$  called the *localization* of  $\mathcal{O}$  at  $S$ . The ring  $\mathcal{O}$  is naturally embedded in  $S^{-1}\mathcal{O}$  by the map  $x \mapsto x/1$ .

When  $\mathcal{P}$  is a prime ideal of  $\mathcal{O}$ , it is easy to check that the set  $S = \mathcal{O} \setminus \mathcal{P}$  is a multiplicative subset of  $\mathcal{O}$ . In this case, by abuse of language, we call  $S^{-1}\mathcal{O}$  the *localization* of  $\mathcal{O}$  at  $\mathcal{P}$ .

Although it is quite common to denote the localization of  $\mathcal{O}$  at a prime ideal  $\mathcal{P}$  by the symbol  $\mathcal{O}_{\mathcal{P}}$ , to avoid confusion we will retain this symbol for the ring of integers of the field of  $\mathcal{P}$ -adic numbers, where  $\mathcal{P}$  is an ideal of an algebraic number field.

When  $S = \mathcal{O} \setminus \mathcal{P}$ , the ring  $S^{-1}\mathcal{O}$  is *local*, i.e. it has a unique maximal ideal, namely  $\mathcal{P} S^{-1}\mathcal{O}$ .

In addition,  $S^{-1}\mathcal{O}$  is a principal ideal domain, and so every ideal must be a power of its unique maximal ideal.

A local principal ideal domain is called a *discrete valuation ring*. The valuation ring of a non archimedean valuation of a field  $k$  is a typical example of a discrete valuation ring. The valuation ring of the field of  $\mathcal{P}$ -adic numbers is simply the ring of  $\mathcal{P}$ -adic integers.

We state the following theorems concerning discrete valuation rings for future reference.

**Theorem 2.2** *Let  $S$  be a multiplicative set in a ring  $\mathcal{O}$ , and let  $\mathcal{B}$  be the integral closure of  $\mathcal{O}$  in a field extension  $K$  of the field of quotients  $k$  of  $\mathcal{O}$ . Then, the integral closure of  $S^{-1}\mathcal{O}$  in  $K$  is given by  $S^{-1}\mathcal{B}$ .*

*Proof.* See [52, Proposition 8, p. 8].  $\square$

**Theorem 2.3** *The integral closure of a ring  $\mathcal{O}$  in a finite extension  $K$  of its quotient field  $k$  is equal to the intersection of all the valuation rings of  $K$  containing  $\mathcal{O}$ .*

*Proof.* See [53, Proposition 3.6, p. 351].  $\square$

This last theorem assumes a particularly neat form when  $R = S^{-1}\mathcal{O}$ , with  $S = \mathcal{O} \setminus \mathcal{P}$  as above. In this case, if we denote by  $\mathcal{Q}_1, \dots, \mathcal{Q}_r$  the prime ideals of  $\mathcal{B}$  above  $\mathcal{P}$ , and by  $T_i$  the multiplicative set  $\mathcal{B} \setminus \mathcal{Q}_i$ , then the valuation rings above  $S^{-1}\mathcal{O}$  are just the rings  $T_i^{-1}\mathcal{B}$ .

In particular, when there is only one prime ideal  $\mathcal{Q}$  of  $\mathcal{B}$  above  $\mathcal{P}$ , the integral closure of  $S^{-1}\mathcal{O}$  in  $K$  is just  $T^{-1}\mathcal{B}$ , with  $T = \mathcal{B} \setminus \mathcal{Q}$ , and so it is a discrete valuation ring as well. In this case, we have

**Theorem 2.4** *Let  $\mathcal{O}$  be a Dedekind Domain, with quotient field  $k$ . Let  $\mathcal{B}$  be the integral closure of  $\mathcal{O}$  in a finite separable extension  $K$  of  $k$ . Let  $\mathcal{P}$  be a prime ideal of  $\mathcal{O}$ , and assume that there is only one prime ideal  $\mathcal{Q}$  of  $\mathcal{B}$  lying above  $\mathcal{P}$ . Let  $S$  denote the multiplicative set  $\mathcal{O} \setminus \mathcal{P}$ . Let  $\pi \in \mathcal{Q} S^{-1}\mathcal{B} \setminus (\mathcal{Q} S^{-1}\mathcal{B})^2$ , and let  $\beta \in S^{-1}\mathcal{B}$  be a primitive element for  $S^{-1}\mathcal{B}/\mathcal{Q} S^{-1}\mathcal{B}$  over  $S^{-1}\mathcal{O}/\mathcal{P} S^{-1}\mathcal{O}$ . Then  $S^{-1}\mathcal{O}[\beta, \pi] = S^{-1}\mathcal{B}$*

*Proof.* See [52, Proposition 23, p. 26]  $\square$

## 2.4 The Chinese Remainder Theorem

Although it is possible to find many different versions of the Chinese Remainder Theorem in the literature, we will need only the following basic version.

**Theorem 2.5** *Let  $R$  be a commutative ring with unity, and  $\mathcal{I}_1, \dots, \mathcal{I}_r$  ideals such that  $\mathcal{I}_i + \mathcal{I}_j = R$  for all  $i \neq j$ . Given elements  $x_1, \dots, x_r \in R$ , there is an  $x \in R$  such that  $x \equiv x_i \pmod{\mathcal{I}_i}$  for all  $i$ .*

*Proof.* See [53, p. 94].  $\square$

We will use the Chinese Remainder Theorem in Chapter 3, where  $R$  will be the ring  $F[x]$  of polynomials in one indeterminate over a field  $F$ .

Since  $F[x]$  is a Principal Ideal Domain, in this ring the Chinese Remainder Theorem admits a very simple formulation:

**Theorem 2.6** *Let  $F$  be a field, and  $f_1(x), \dots, f_r(x)$  pairwise coprime polynomials over  $F$ . Given polynomials  $g_1(x), \dots, g_r(x)$  over  $F$ , it is possible to find a polynomial  $f(x) \in F[x]$  such that  $f(x) \equiv g_i(x) \pmod{f_i(x)}$  for all  $i$ .*

The construction of the polynomial  $f(x)$  is implicit in the proof of the theorem.

## 2.5 Hensel's Lemma

Hensel's Lemma is a method, due to the German mathematician Hensel, for lifting approximate factorizations of polynomials over valuation rings. According to B. Mazur [64] this method was already implicit in the work of Kummer. The name 'Lemma' must not mislead: Hensel's Lemma is capable of many generalizations. In fact, quoting J.W.S. Cassels [19, p. 83] 'in the literature there is a variety of results that go under this name'.

Hensel's Lemma has its roots in Newton's method for finding the roots of a polynomial equation by successive refinements of an initial approximate solution. It takes an approximate factorization in a valuation ring and produces a new approximate factorization, which is better with respect to the given valuation.

Although some authors [97] consider Hensel's Lemma a special case of Newton's method, it is nowadays quite common to consider Newton's method as a corollary of Hensel's Lemma. This will be our approach in this section, following J. von zur Gathen [38].

Let  $K$  denote a field complete with respect to a nonarchimedean valuation,  $\mathcal{O}_K$  its ring of integers, and  $\mathcal{P}$  its maximal ideal. In addition, let  $\overline{K}$  denote the residue class field of  $K$ , that is  $\mathcal{O}_K/\mathcal{P}$ . We have a canonical homomorphism

$$\mathcal{O}_K \rightarrow \mathcal{O}_K/\mathcal{P} = \overline{K}$$

which extends to the polynomial ring  $\mathcal{O}_K[x]$  as follows:

$$g(x) = \sum_{i=0}^m c_i x^i \mapsto \sum_{i=0}^m \bar{c}_i x^i = \bar{g}(x)$$

where  $\bar{c}$  denotes the residue class mod  $\mathcal{P}$  of an element  $c \in \mathcal{O}_K$ .

**Theorem 2.7 (Hensel's Lemma)** *Let  $K$  be a field complete with respect to a nonarchimedean valuation, and let  $\mathcal{O}_K$  be its ring of integers. Let  $f(x)$  be a primitive polynomial in  $\mathcal{O}_K[x]$  which factors in the residue class field  $\overline{K}$  of  $K$  as*

$$\overline{f(x)} = G(x)H(x)$$



where  $G(x)$  and  $H(x)$  are nonzero relatively prime polynomials in  $\overline{K}[x]$ . Then

$$f(x) = g(x)h(x)$$

where  $g(x), h(x) \in K[x]$  and  $\deg g(x) = \deg G(x)$ , and  $G(x)$  and  $H(x)$  are the images of  $g(x)$  and  $h(x)$ , respectively, in  $\overline{K}[x]$ .

*Proof.* See [14, pp. 275–276].  $\square$

We mention only a few consequences of Hensel's Lemma.

**Corollary 2.1 (Newton's method)** *With the same notation as above, suppose that  $\overline{f}(x)$  has a root in  $\overline{K}[x]$  with multiplicity one. Then  $f(x)$  has a root in  $\mathcal{O}_K$  with multiplicity one.*

*Proof.* See [47, p. 83].  $\square$

**Corollary 2.2** *Let  $f(x)$  be a primitive polynomial in  $\mathcal{O}_K[x]$  which is irreducible in  $K[x]$ . If  $K$  is complete, then  $\overline{f}(x)$  is a power of an irreducible polynomial in  $\overline{K}[x]$ .*

*Proof.* See [65, Lemma 3, p. 95].  $\square$

## 2.6 Some Results from Local Class Field Theory

In this section and in the next one we recall some results from local and global class field theory, needed later on in this thesis. For a brief summary of class field theory we refer the reader to [37].

The objective of local class field theory is to describe all the abelian extensions of a local field.

A local field is defined to be a locally compact, nondiscrete topological field. It is known that a local field is either a finite extension of the field  $\mathbb{Q}_p$ , for some prime  $p$  of  $\mathbb{Q}$  (including the infinite prime), or the field of formal power series over a finite field. In this thesis we will be concerned only with the first case.

The main theorem of local class field theory establishes a one to one correspondence between the abelian extensions of a local field  $K$  and the open subgroups of finite index in  $K^*$ .

More precisely, for a fixed local field  $K$ , to each abelian extension  $L$  of  $K$  there corresponds uniquely the norm subgroup  $N_{L/K}(L^*)$  of  $K^*$ , and conversely, any open subgroup of finite index in  $K^*$  is the norm subgroup of some abelian extension  $L$  of  $K$ .

Moreover, for a given abelian extension  $L$  of  $K$ , there is a canonical isomorphism

$$\psi : \text{Gal}(L/K) \rightarrow K^*/N_{L/K}(L^*)$$

called the main isomorphism of local class field theory.

After these remarks we can state the results from local class field theory that we will use in the next chapters.

The first theorem tells us that the norm map behaves in the expected way with respect to the operation of composition of fields.

**Theorem 2.8** *Let  $L_1, \dots, L_r$  be abelian extensions of a local field  $K$ . Let  $L = L_1 \cdots L_r$  be their composite. Then  $N_{L/K}(L^*) = \cap_{i=1, \dots, r} N_{L_i/K}(L_i^*)$ .*

*Proof.* See [86, Lemma 15, p. 168].  $\square$

The next theorem characterizes completely the norm group of the unramified extensions of  $\mathbb{Q}_p$ .

**Theorem 2.9** *Let  $L_p$  be an unramified extension of  $\mathbb{Q}_p$  of degree  $f$  over  $\mathbb{Q}_p$ . Let  $\beta = p^m u \in \mathbb{Q}_p^*$ , with  $u \in U_p$ ,  $m \in \mathbb{Z}$ . Then  $\beta \in N_{L_p/\mathbb{Q}_p}(L_p^*)$  if and only if  $f \mid m$ . In particular every unit of  $\mathbb{Q}_p$  is the norm of a unit in  $L_p$ .*

*Proof.* See [5, Theorem 19, p. 141] and [47, p. 153].  $\square$

The last result from local class field theory that we need is known as the *fundamental equality of local class field theory*. It is valid for any local field, and hence in particular for any  $p$ -adic field.

**Theorem 2.10** *Let  $L/K$  be a cyclic extension of local fields, with ramification index  $e$ . Let  $U_L$  (resp.  $U_K$ ) denote the group of units of  $L$  (resp.  $K$ ). Then  $(U_K : N_{L/K}(U_L)) = e$  and  $(K^* : N_{L/K}(L^*)) = [L : K]$ .*

*Proof.* See [52, Corollary, p. 221] and [52, Theorem 3, p. 219].  $\square$

## 2.7 Some Results from Global Class Field Theory

Global class field theory describes all the abelian extensions of a global field. A global field is either an algebraic number field, that is a finite extension of the field  $\mathbb{Q}$  of rationals, or a field of algebraic functions in one variable over a finite field. In this thesis we will be concerned only with the first case.

In global class field theory the role of the multiplicative group of the field  $K^*$  is played by the idele class group  $C_K$ , defined as follows. Let  $M_K$  denote the set of inequivalent valuations of  $K$ . The idele group  $J_K$  of a field  $K$  is the restricted topological product of the multiplicative groups  $K_v^*$  with respect to the units  $U_v$  of  $K_v$ : by this we mean the subgroup of the direct product

$$\prod_{v \in M_K} K_v^*$$

consisting of elements all but a finite number of whose components lie in  $U_v$ .

From a topological point of view  $J_K$  is made into a locally compact group by decreeing that each group

$$\prod_{v \in S} K_v^* \prod_{v \in M_K \setminus S} U_v$$

is an open subgroup of  $J_K$ , where  $S$  ranges over all the finite subsets  $M_K$ . Given an idele  $a$  of  $J_L$  we define its norm  $N_{L/K}(a)$  to be the idele of  $J_K$  whose  $v$ -component is

$$\prod_{w|v} N_{K_w/K_v}(a_w)$$

The group  $L^*$  is embedded in  $J_L$  as a discrete subgroup called the group of principal ideles, and the quotient group

$$C_L = J_L / L^*$$

with the quotient topology, is called the idele class group. It is possible to extend the norm map to the idele class group.

The main theorem of global class field theory states that given a finite extension  $L/K$  of a global field  $K$ , the norm subgroup  $N_{L/K}(C_L)$  of  $C_K$  uniquely determines the field  $L$ , and conversely, any open subgroup  $N$  of finite index in  $C_K$  is the norm subgroup  $N_{L/K}(C_L)$  for some finite abelian extension  $L$  of  $K$ . We call  $L/K$  the class field to  $N$ .

After these preliminaries, we state the results from global class field theory that we will use in the next chapters.

The most striking result, around which our thesis winds, is certainly the following celebrated theorem of H. Hasse:

**Theorem 2.11 (Hasse Norm Theorem)** *Let  $L/K$  be a cyclic extension of global fields. An element  $a \in K^*$  is a norm from  $L^*$  if and only if  $a$  is a local norm at every prime (including the infinite primes) of  $K$ .*

*Proof.* See [47, Theorem 4.5, p. 156].  $\square$

We note here that the Hasse Norm Theorem is strictly limited to cyclic extensions (see [19, p. 360] for counterexamples). In other words, for a noncyclic extension  $L$  of a global field  $K$  it may happen that an element which is a local norm everywhere is not a global norm, although the converse is always true.

The next theorem tells us that in the application of the Hasse Norm Theorem we can leave out a particular prime.

**Theorem 2.12** *If  $L/K$  is an abelian extension of global fields and  $a \in K^*$  is a local norm at all the primes of  $K$  with the possible exception of one particular prime, then  $a$  is a local norm at that prime as well.*

*Proof.* See [47, p. 190].  $\square$

## 2.8 Encoding Data

In order to discuss the *time* complexity of our algorithms we have to define how the size of an object, and therefore the size of the input, is measured.

We define the size of a sequence of nonnegative integer as the number of bits needed to represent the sequence in binary.

Negative integers are represented by adding a sign bit to their binary representation.

A rational number  $c$  is encoded as a sequence  $r, s$  with  $r$  and  $s$  coprime integers such that  $r/s = c$ .

When  $n$  is a positive integer, the elements of the ring  $\mathbb{Z}/n\mathbb{Z}$  are encoded as nonnegative integers smaller than  $n$ . This implies that the size of any element of  $\mathbb{Z}/n\mathbb{Z}$  is bounded by  $\log(n + 2)$ .

A compound object (polynomial, vector, matrix) is encoded in the dense representation, by giving the sequence of *all* its coefficients. Then the size of the compound object is just the sum of the sizes of its simple constituents.

In particular, the degree of a polynomial is bounded by the size of the sequence of its coefficients. This implies that, when  $\alpha$  is an algebraic number then the degree  $[\mathbb{Q}[\alpha] : \mathbb{Q}]$  is bounded by the size of the minimal polynomial  $m_\alpha(x)$  of  $\alpha$  over  $\mathbb{Q}$ .

## Chapter 3

# Power roots of polynomials over arbitrary fields

Let  $F$  be an arbitrary field, of characteristic  $\text{char}(F)$ ,  $f(x)$  a polynomial in one variable over  $F$  of degree  $\geq 1$ ,  $g(x)$  a nonzero polynomial over  $F$  and  $m > 1$  an integer.

In [69] J.B. Miller gives some sufficient conditions for the existence of a polynomial  $z(x) \in F[x]$  such that  $z(x)^m \equiv g(x) \pmod{f(x)}$ , when  $F$  is  $\mathbf{R}$  or  $\mathbf{C}$ . Miller explicitly states in his paper that the conditions given are not necessary.

In this chapter we extend Miller's results by giving necessary and sufficient conditions for the existence of an  $m^{\text{th}}$  root in  $F[x]/(f(x))$ , when  $F$  is any field, not necessarily  $\mathbf{C}$  or  $\mathbf{R}$ . While the methods used by Miller in [69] are analytical, ours are purely algebraic, for they rely on the power of the combination Hensel's Lemma - Chinese Remainder Theorem.

Moreover, since all the proofs given here are constructive, it is possible to translate them into an effective algorithm when  $F$  is a computable field (e.g. an algebraic number field or a finite field). The results of this chapter have been published in [1].

When  $\text{char}(F) \nmid m$ , we can summarize our results in the following theorem:

**Theorem 3.1** *Let  $F$  be a field, and  $m > 1$  a positive integer,  $\text{char}(F) \nmid m$  if  $\text{char}(F) > 0$ . Let  $g(x), f(x)$  be polynomials over  $F$ , with  $g(x) \neq 0$  and  $\deg f(x) \geq 1$ .*

In  $F[x]$  the congruence

$$z(x)^m \equiv g(x) \pmod{f(x)} \quad (3.1)$$

admits a solution if and only if for every irreducible factor  $p(x)$  of  $f(x)$ :

if  $l \geq 0$  denotes the highest exponent to which  $p(x)$  divides  $g(x)$  and  $k \geq 1$  denotes the highest exponent to which  $p(x)$  divides  $f(x)$ , then either

(i).  $k \leq l$ , or

(ii).  $m \mid l$  and  $y(x)^m \equiv g(x)/p(x)^l \pmod{p(x)}$  is solvable for  $y(x)$ .

When  $\text{char}(F) \mid m$  the conditions for the solvability of the congruences  $z_i(x)^m \equiv g(x) \pmod{p_i(x)^{k_i}}$  are more involved – we will consider this case in Section 3.1.2.

What we show essentially in this chapter is that we can reduce the problem of solving (3.1) to the problem of solving simpler equations, of the form  $z(x)^m \equiv g(x)$

$\pmod{p(x)}$ , with  $p(x)$  irreducible over  $F$ . But, as we will show in Section 3.1, solving these simpler congruences is equivalent to extracting  $m^{\text{th}}$  roots in some algebraic extension of  $F$ .

We will prove Theorem 3.1 in Section 3.1. In Sections 3.2, 3.3 and 3.4 we will show how to specialize Theorem 3.1 to  $\mathbb{C}$ ,  $\mathbb{R}$  and to finite fields.

### 3.1 The method

When  $n$  and  $y$  are arbitrary integers and  $m$  is a positive integer greater than one, it is well known how to solve the congruence

$$x^m \equiv y \pmod{n}$$

using the combination Hensel's Lemma – Chinese Remainder Theorem (see [71, pp. 79–90] for a nice exposition of the technique). Our aim here is to extend this method to the ring  $F[x]$  of polynomials in one variable over a field  $F$ , in order to solve the congruence (3.1).

Let us assume without loss of generality that  $f(x)$  is monic, since if  $z(x)^m \equiv g(x) \pmod{f(x)}$  holds, then  $z(x)^m \equiv g(x) \pmod{cf(x)}$  holds for any  $c \in F$ . Our method can be summarized as follows:

- (i). Factor  $f(x)$  into monic irreducibles obtaining  $f(x) = p_1(x)^{k_1} \dots p_n(x)^{k_n}$  where the  $p_i(x)$  are distinct irreducibles and each  $k_i \geq 1$ :
- (ii). Solve each of the congruences  $z_i(x)^m \equiv g(x) \pmod{p_i(x)}$  for  $z_i(x)$ ,  $i \in \{1, \dots, n\}$ ;
- (iii). Lift the solutions obtained in the previous step from  $F[x]/(p_i(x))$  to  $F[x]/(p_i(x)^{k_i})$ ;
- (iv). Combine the solutions of the previous step using the Chinese Remainder Theorem to obtain a solution of the original congruence.

Step (iv) does not present any technical difficulty, since it relies on the well known isomorphism [53, page 95]:

$$F[x]/(f(x)) \cong F[x]/(p_1(x)^{k_1}) \times \dots \times F[x]/(p_n(x)^{k_n})$$

When  $p(x)$  is a monic irreducible polynomial  $F[x]/(p(x)) \cong F(\alpha)$  where  $\alpha$  is any root of  $p(x)$ : the actual isomorphism is given by  $k(x) + (p(x)) \mapsto k(\alpha)$ . It follows that Step (ii), that is the extraction of an  $m^{\text{th}}$  root of  $g(x)$  modulo  $p(x)$ , is equivalent to the extraction of an  $m^{\text{th}}$  root of  $g(\alpha)$  in  $F(\alpha)$ .

Therefore, most of the rest of this section will be devoted to explaining how Step (iii), i.e. the lifting process, can be accomplished.

Fundamental to the entire process is the concept of the  $p(x)$ -adic expansion of a polynomial  $f(x)$  [53, page 189]. Given  $f(x), p(x) \in F[x]$ , with  $\deg p(x) \geq 1$ , there exist unique polynomials

$$g_0(x), g_1(x), \dots, g_t(x) \in F[x]$$

such that  $\deg g_i(x) < \deg p(x)$  and

$$f(x) = g_0(x) + g_1(x)p(x) + g_2(x)p(x)^2 + \dots + g_t(x)p(x)^t$$



The polynomials  $g_i(x)$  can be computed recursively as follows:

- $g_0(x) := f(x) \bmod p(x)$
- $g_{i+1}(x) := (f(x) - \sum_{k=0}^i g_k(x)p(x)^k)/p(x)^{i+1} \bmod p(x)$ .

The lifting method is based on the following instance of Hensel's Lemma.

**Lemma 3.1** *Let  $p(x)$  be an irreducible element of  $F[x]$ . Let  $G(y)$  be a polynomial with coefficients in  $F[x]$ . Assume that there is an element  $f_0(x) \in F[x]$ , with  $\deg f_0(x) < \deg p(x)$ , such that  $G(f_0(x)) \equiv 0 \pmod{p(x)}$  and  $G'(f_0(x)) \not\equiv 0 \pmod{p(x)}$ . Given any positive integer  $k$  there is a unique polynomial  $f_{k-1}(x) \in F[x]$  of degree less than  $\deg p(x)^k$  such that  $G(f_{k-1}(x)) \equiv 0 \pmod{p(x)^k}$  and  $f_{k-1}(x) \equiv f_0(x) \pmod{p(x)}$ .*

*Proof.* Our proof is freely adapted from the proof of Hensel's Lemma given in [50, page 16]. We show how to construct a sequence of polynomials  $f_1(x), \dots, f_{k-1}(x) \in F[x]$  such that for all  $n \in \{1, \dots, k-1\}$ :

- (i).  $G(f_n(x)) \equiv 0 \pmod{p(x)^{n+1}}$
- (ii).  $f_n(x) \equiv f_{n-1}(x) \pmod{p(x)^n}$
- (iii).  $\deg f_n(x) < \deg p(x)^{n+1}$

We prove that the sequence  $(f_n(x))$  exists and is unique by induction on  $n$ . If  $f_1(x)$  satisfies (ii) and (iii) then it must be of the form

$$f_0(x) + b_1(x)p(x)$$

with  $\deg b_1(x) < \deg p(x)$ . When we expand  $G(f_1(x))$  we obtain

$$G(f_1(x)) = G(f_0(x) + b_1(x)p(x)) = G(f_0(x)) + G'(f_0(x))b_1(x)p(x) + w(x)$$

where  $w(x)$  is a polynomial divisible by  $p(x)^2$ . Since  $p(x) \mid G(f_0(x))$  by assumption, we can write

$$G(f_0(x)) \equiv a_0(x)p'(x) \pmod{p(x)^2}$$

where  $\deg a_0(x) < \deg p(x)$ . So, in order to get  $G(f_1(x)) \equiv 0 \pmod{p(x)^2}$  we must have

$$a_0(x)p(x) + G'(f_0(x))b_1(x)p(x) \equiv 0 \pmod{p(x)^2}$$

that is

$$a_0(x) + G'(f_0(x))b_1(x) \equiv 0 \pmod{p(x)}$$

The last congruence has a unique solution  $\pmod{p(x)}$  for  $b_1(x)$  since by hypothesis  $G'(f_0(x)) \not\equiv 0 \pmod{p(x)}$ . Then

$$f_1(x) = f_0(x) + b_1(x)p(x)$$

is the unique polynomial satisfying (i), (ii) and (iii) with  $n = 1$ .

Next, assume that

$$f_1(x), f_2(x), \dots, f_{n-1}(x)$$

are known, and we want to find  $f_n(x)$ . By (ii) and (iii) we need

$$f_n(x) = f_{n-1}(x) + b_n(x)p(x)^n$$

with  $\deg b_n(x) < \deg p(x)$ . We expand  $G(f_n(x))$  obtaining

$$\begin{aligned} G(f_n(x)) &= G(f_{n-1}(x) + b_n(x)p(x)^n) \\ &\equiv G(f_{n-1}(x)) + G'(f_{n-1}(x))b_n(x)p(x)^n \pmod{p(x)^{n+1}} \end{aligned}$$

Since

$$G(f_{n-1}(x)) \equiv 0 \pmod{p(x)^n}$$

by the inductive hypothesis, we obtain

$$G(f_{n-1}(x)) \equiv a_{n-1}(x)p(x)^n \pmod{p(x)^{n+1}}$$

and the condition

$$G(f_n(x)) \equiv 0 \pmod{p(x)^{n+1}}$$

becomes

$$a_{n-1}(x)p(x)^n + G'(f_{n-1}(x))b_n(x)p(x)^n \equiv 0 \pmod{p(x)^{n+1}}$$

that is

$$a_{n-1}(x) + G'(f_{n-1}(x))b_n(x) \equiv 0 \pmod{p(x)}$$

Since

$$f_{n-1}(x) \equiv f_0(x) \pmod{p(x)}$$

it follows that

$$G'(f_{n-1}(x)) \equiv G'(f_0(x)) \not\equiv 0 \pmod{p(x)}$$

and so the previous congruence has a unique solution  $\pmod{p(x)}$  for  $b_n(x)$ . Then

$$f_n(x) = f_{n-1}(x) + b_n(x)p(x)^n$$

is the unique polynomial satisfying (i), (ii) and (iii).  $\square$

Our objective is to solve the congruence:

$$y(x)^m \equiv g(x) \pmod{p(x)^k} \tag{3.2}$$

where  $p(x)$  is a monic irreducible factor of  $f(x)$ .

Let  $y_0(x)$  be a solution of  $y(x)^m \equiv g(x) \pmod{p(x)}$ : clearly if such an element  $y_0(x)$  does not exist then (3.2) cannot admit any solution.

If

$$my_0(x)^{m-1} \not\equiv 0 \pmod{p(x)}$$

we can use the construction given in Lemma 3.1 with  $G(y) := y(x)^m - g(x)$  to obtain a sequence of polynomials

$$y_1(x), y_2(x), \dots$$

such that

$$y_i(x)^m \equiv g(x) \pmod{p(x)^{i+1}}$$

A solution of (3.2) is then given by  $y_{k-1}(x)$ , and this solution is unique, modulo  $p(x)^k$ .

If

$$my_0(x)^{m-1} \equiv 0 \pmod{p(x)}$$

the lifting argument can not be applied, although (3.2) may still have a solution.

Let us assume therefore that

$$my_0(x)^{m-1} \equiv 0 \pmod{p(x)}$$

Since  $F[x]/(p(x))$  is a field this may happen only in two cases: if  $y_0(x) \equiv 0 \pmod{p(x)}$  or if  $\text{char}(F) \mid m$ . We discuss the first case in Section 3.1.1 and the second case in Section 3.1.2.

**Remark.** Let  $s_i$  denote the number of solutions of the congruence

$$z_i(x)^m \equiv g(x) \pmod{p_i(x)^{k_i}}$$

It is easy to see that the number of solution of (3.1) is given by  $\prod_{i=1}^n s_i$ . In the case when  $\gcd(f(x), g(x)) = 1$  and  $\text{char}(F) \nmid m$ , Lemma 3.1 shows that the lifting process is unique and so  $s_i$  is also the number of  $m^{\text{th}}$  roots of  $g(x) \pmod{p_i(x)}$ .

### 3.1.1 Lifting of zero

It is easy to see that the zero polynomial is a solution of  $y(x)^m \equiv g(x) \pmod{p(x)}$  if and only if  $p(x) \mid g(x)$ . The following lemma deals with this case.

**Lemma 3.2** *Assume that  $p(x) \mid g(x)$ . Let  $l$  be the highest exponent to which  $p(x)$  divides  $g(x)$ . If  $k \leq l$  the zero polynomial is a solution of (3.2). If  $k > l$  then (3.2) admits a solution if and only if  $m \mid l$  and*

$$y(x)^m \equiv g(x)/p(x)^l \pmod{p(x)^{k-l}} \quad (3.3)$$

*admits a solution. In this case if  $\hat{y}(x)$  denotes a solution of (3.3) then  $\hat{y}(x)p(x)^{l/m}$  is a solution of (3.2).*

*Proof.* If  $k \leq l$  the zero polynomial is obviously a solution of (3.2), so we will suppose that  $k > l$ .

Assume that

$$\hat{y}(x)^m \equiv g(x)/p(x)^l \pmod{p(x)^{k-l}}$$

This is equivalent to

$$p(x)^k \mid \hat{y}(x)^m p(x)^l - g(x)$$

Thus, if  $m \mid l$  we can write the last relation as

$$p(x)^k \mid \dot{y}(x)^m p(x)^{(l/m)m} - g(x)$$

and so  $\dot{y}(x)p(x)^{l/m}$  is a solution of (3.2).

On the other hand, suppose that  $k > l$  and (3.2) admits a solution. Let the  $p(x)$ -adic expansion of  $g(x)$  be

$$a_1(x)p(x)^l + a_2(x)p(x)^{l+1} + \dots$$

with  $a_1(x) \neq 0$ . Let

$$\bar{y}(x) = b_1(x)p(x)^r + \dots$$

be a solution of (3.2), with  $b_1(x) \neq 0$ . Then the  $p(x)$ -adic expansion of  $\bar{y}(x)^m$  is

$$(b_1(x)^m \bmod p(x))p(x)^{rm} + \dots$$

Since  $b_1(x) \neq 0$  and  $\deg b_1(x) < \deg p(x)$  it follows that

$$b_1(x) \not\equiv 0 \pmod{p(x)}$$

and therefore

$$b_1(x)^m \not\equiv 0 \pmod{p(x)}$$

since  $p(x)$  is prime.

Now

$$\bar{y}(x)^m \equiv g(x) \pmod{p(x)^k}$$

if and only if

$$(b_1(x)^m \bmod p(x))p(x)^{rm} + \dots$$

and

$$a_1(x)p(x)^l + \dots$$

coincide up to the term in  $p(x)^{k-1}$ . Since  $a_1(x) \neq 0$  and  $b_1(x)^m \bmod p(x) \neq 0$  it follows that  $l = rm$  and so  $m \mid l$  as asserted.  $\square$

**Corollary 3.1** *Under the assumptions of the previous lemma, if  $\text{char}(F) \nmid m$  and  $k > l$  then (3.2) admits a solution if and only if  $m \mid l$  and  $y(x)^m \equiv g(x)/p(x)^l \pmod{p(x)}$  admits a solution.*

*Proof.* The Corollary follows immediately from Lemma 3.2 since the right hand side of (3.3) is not divisible by  $p(x)$ .  $\square$

Note that if  $p(x) \mid g(x)$  and at the same time  $\text{char}(F) \mid m$ , we can use Lemma 3.2 to reduce this case to the case  $p(x) \nmid g(x)$  and  $\text{char}(F) \mid m$ , which is handled in the next section.

### 3.1.2 The exponent $m$ is a multiple of $\text{char}(F)$

In this section we will assume that  $p(x) \nmid g(x)$ . When  $q = \text{char}(F) > 0$  the map  $a \mapsto a^q$  is always an endomorphism of  $F$ . It follows that if

$$a(x) = a_0 + a_1x + \dots + a_nx^n$$

is a polynomial over  $F$  then

$$a(x)^q = a_0^q + a_1^q x^q + \dots + a_n^q x^{nq}$$

We will use this fact frequently in this section.

**Lemma 3.3** *Let  $q = \text{char}(F)$ ,  $q \neq 0$ . Assume that  $m = q^l$  for some positive integer  $l$ , and  $m \geq k$ . If (3.2) admits a solution, then every solution of  $y(x)^m \equiv g(x) \pmod{p(x)}$  is a solution of (3.2).*

*Proof.* Let us assume that (3.2) admits a solution  $y_1(x)$ . Let  $y_0(x)$  be a solution of  $y(x)^m \equiv g(x) \pmod{p(x)}$ . Then

$$(y_0(x) - y_1(x))^m = y_0(x)^m - y_1(x)^m \equiv 0 \pmod{p(x)}$$

Since  $p(x)$  is prime and  $k \leq m$  it follows that

$$p(x)^k \mid (y_0(x) - y_1(x))^m$$

and therefore

$$y_0(x)^m \equiv y_1(x)^m \pmod{p(x)^k}$$

that is

$$y_0(x)^m \equiv g(x) \pmod{p(x)^k}$$

□

**Remark.** Therefore, when  $m = q^t$  and  $m \geq k$ , to test if (3.2) is solvable, it is enough to find *any* solution of  $y(x)^m \equiv g(x) \pmod{p(x)}$  and check if it satisfies (3.2). Clearly if  $y(x)^m \equiv g(x) \pmod{p(x)}$  does not admit any solution then (3.2) does not admit any solution.

**Lemma 3.4** *Let  $q = \text{char}(F)$ ,  $q \neq 0$ . Assume that  $m = q^t$  for some positive integer  $t$ .*

*If  $m \mid k$  then (3.2) admits a solution if and only if  $g(x) \pmod{p(x)^k}$  is a polynomial in  $x^m$  and all its coefficients have an  $m^{\text{th}}$  root in  $F$ .*

*If  $m \nmid k$  let  $w := \lfloor k/m \rfloor$ , let  $s := k \bmod m$ , let  $z(x) := g(x) \bmod p(x)^{mw}$  and  $r(x) := (g(x) - z(x))/(p(x)^{mw}) \bmod p(x)^s$ . Then (3.2) admits a solution if and only if  $z(x)$  is a polynomial in  $x^m$ , all its coefficients have an  $m^{\text{th}}$  root in  $F$  and  $j(x)^m \equiv r(x) \pmod{p(x)^s}$  admits a solution.*

*Proof.* Let

$$g_0(x) + g_1(x)p(x)^m + \dots$$

be the  $p(x)^m$ -adic expansion of  $g(x)$ .

If  $y(x)$  is an  $m^{\text{th}}$  root of  $g(x)$  modulo  $p(x)^k$  and

$$y_0(x) + y_1(x)p(x) + \dots$$

is its  $p(x)$ -adic expansion then

$$y(x)^m = y_0(x)^m + y_1(x)^m p(x)^m + \dots$$

and this expression must coincide with the  $p(x)^m$ -adic expansion of  $y(x)^m$ .

Let us assume first that  $m \mid k$ . It can be seen that in this case (3.2) is satisfied if and only if

$$\begin{aligned} y_0(x)^m + y_1(x)^m p(x)^m + \dots + y_{k/m-1}(x)^m p(x)^{m(k/m-1)} = \\ g_0(x) + g_1(x)p(x)^m + \dots + g_{k/m-1}(x)p(x)^{m(k/m-1)} \end{aligned}$$

Therefore  $g_i(x)$  must be the  $m^{\text{th}}$  power of  $y_i(x)$ , for  $i = 0, \dots, k/m - 1$ . But then  $g(x) \bmod p(x)^k$  is the  $m^{\text{th}}$  power of a polynomial  $y(x)$ , i.e. it must be a polynomial in  $x^m$  and each of its coefficients must have an  $m^{\text{th}}$  root in  $F$  - it is easy at this point to find the actual polynomial  $y(x)$ .

Assume next that  $m \nmid k$ . The argument used above tells us that

$$g_i(x) = y_i(x)^m$$

for  $i = 0, \dots, \lfloor k/m \rfloor - 1$ , and

$$g_i(x) \equiv y_i(x)^m \pmod{p(x)^s}$$

for  $i = \lfloor k/m \rfloor$ , as asserted. Since  $s < m$ , the last congruence can be handled using Lemma 3.3.  $\square$

Note that Lemma 3.3 and Lemma 3.4 are valid for any field of characteristic  $q > 0$ .

**Remark.** When  $q \mid m$  but  $m$  is not a power of  $q$ , write  $m$  as  $q^t r$ , with  $q \nmid r$ . Write (3.2) as  $(y(x)^{q^t})^r \equiv g(x) \pmod{p(x)^k}$ .

Set  $z(x) := y(x)^{q^t}$  and solve  $z(x)^r \equiv g(x) \pmod{p(x)^k}$  for  $z(x)$ . Finally solve  $y(x)^{q^t} \equiv z(x) \pmod{p(x)^k}$  for  $y(x)$  to obtain a solution of (3.2).

## 3.2 The complex case

In  $\mathbb{C}[x]$  an irreducible polynomial  $p(x)$  can have only degree 1, and therefore we can take  $p(x) = x - \alpha$ , with  $\alpha \in \mathbb{C}$ . We recall here that  $\mathbb{C}[x]/(x - \alpha) \cong \mathbb{C}$  under the isomorphism

$$g(x) + (x - \alpha) \mapsto g(\alpha)$$



If  $p(x) \nmid g(x)$ , the congruence  $y(x)^m \equiv g(x) \pmod{p(x)}$  always admits a (nonzero) solution, since  $\mathbf{C} \cong \mathbf{C}[x]/p(x)$  is algebraically closed, and this solution can be lifted to a solution modulo  $p(x)^k$ , since  $m$  does not divide the characteristic of  $\mathbf{C}$ .

If  $g(x) \equiv 0 \pmod{p(x)}$  then (3.2) admits a solution if and only if the conditions imposed by Lemma 3.2 are satisfied. We summarize our results in the following theorem:

**Theorem 3.2** *In  $\mathbf{C}[x]$  the congruence (3.1) admits a solution if and only if for every common root  $\alpha$  of  $f(x)$  and  $g(x)$  either the multiplicity of  $\alpha$  in  $g(x)$  is greater than or equal to the multiplicity of  $\alpha$  in  $f(x)$  or else  $m$  divides the multiplicity of  $\alpha$  in  $g(x)$ .*

### 3.3 The real case

In  $\mathbf{R}[x]$  an irreducible polynomial  $p(x)$  can have only degree 1 or 2. Assume first that  $p(x) \nmid g(x)$ .

If  $\deg p(x) = 1$ , then we can take  $p(x) = x - \alpha$ , with  $\alpha \in \mathbf{R}$ ; then  $\mathbf{R}[x]/(p(x)) \cong \mathbf{R}$  under the isomorphism

$$g(x) + (p(x)) \mapsto g(\alpha)$$

Then  $y(x)^m \equiv g(x) \pmod{p(x)}$  admits a solution unless  $g(\alpha) < 0$  and  $m$  is even. Moreover this solution can always be lifted to a solution modulo  $p(x)^k$ .

If  $\deg p(x) = 2$ , then  $\mathbf{R}[x]/(p(x)) \cong \mathbf{C}$ . In this case  $y(x)^m \equiv g(x) \pmod{p(x)}$  admits a nonzero solution and this solution can be lifted to a solution modulo  $p(x)^k$ .

Assume next that  $p(x) \mid g(x)$ . If  $\deg p(x)$  is 1 or 2 then (3.2) admits a solution if and only if the conditions imposed by Lemma 3.2 are satisfied. We summarize our results in the following theorem:

**Theorem 3.3** *In  $\mathbf{R}[x]$  the congruence (3.1) admits a solution if and only if the following holds for every (real or complex) root  $\alpha$  of  $f(x)$ : if  $l$  denotes the multiplicity of  $\alpha$  in  $g(x)$  and  $k$  the multiplicity of  $\alpha$  in  $f(x)$ , then either*

(i).  $k \leq l$ , or

(ii).  $m \mid l$ , and whenever  $\alpha$  is real either  $(g/p^l)(\alpha) > 0$  or else  $m$  is odd.

### 3.4 Finite fields

When  $K$  is a finite field there is an easy criterion to decide if an element  $a$  has an  $m^{\text{th}}$  root in it, namely let

$$e = \frac{(|K| - 1)}{\gcd(m, |K| - 1)}$$

and test if  $a^e$  is equal to 1 or not: in the first case  $a$  has exactly  $\gcd(m, |K| - 1)$  roots in the field, in the second case it has no roots. We summarize our results in the following theorem:

**Theorem 3.4** *Let  $F$  be a finite field of characteristic  $q$ . Write  $m$  as  $q^l r$  with  $q \nmid r$ . In  $F[x]$  the congruence (3.1) admits a solution if and only if the following holds for every irreducible factor  $p(x)$  of  $f(x)$ : if  $d := \deg p(x)$ ,  $e := (|F|^d - 1) / \gcd(r, |F|^d - 1)$ ,  $l$  is equal to the highest exponent to which  $p(x)$  divides  $g(x)$  and  $k$  is equal to the highest exponent to which  $p(x)$  divides  $f(x)$ , then either*

(i).  $k \leq l$ , or

(ii).  $m \mid l$  and  $(g(x)/p(x)^l)^e \equiv 1 \pmod{p(x)}$ .

### 3.5 Arithmetic complexity

In this section we will discuss briefly the arithmetic complexity of our algorithm, i.e. we will be concerned only with the number of arithmetic operations (sometimes called 'field operations') carried out.

We will postpone the discussion of the two problems of factoring  $f(x)$  over  $F$  and finding  $m^{\text{th}}$  roots in  $F[x]/(p(x))$  to the next section. A standard reference for the problems discussed in this section is [4].

Let  $M(n)$  denote the number of arithmetic steps needed to multiply two polynomials of degree  $n$ . Note that  $M(n)$  is related by a multiplicative constant to the cost  $D(n)$  of dividing (with remainder) a polynomial of degree at most  $2n$  by a polynomial of degree  $n$ .

The choice of the multiplication algorithm depends to a great extent on the degree of the polynomials being multiplied. When the degree  $n$  is small we can use the classical schoolboy algorithm which requires  $\mathcal{O}(n^2)$  arithmetic steps.

When the degree  $n$  has moderate size we can use a simple algorithm due to A. Karatsuba and Y. Ofman [48], that requires only  $\mathcal{O}(n^{1.58})$  arithmetic steps [4, Section 8.3, p. 286]. According to experiments conducted by R.J. Fateman [33], this method is convenient only for polynomials of degree larger than 40.

Finally, when the degree  $n$  is very large we can use the multiplication algorithm based on the Fast Fourier Transform [4, Section 7.4, p. 269], which requires only  $\mathcal{O}(n \log n)$  arithmetic steps. However, according to experiments conducted by R.T. Moenck [70], this method is convenient only for polynomials of degree larger than 300.

Let us keep up for the rest of this section with the notation introduced in Section 3.1.

It is clear that, in the lifting process, the quantity  $G'(y_0(x)) = my_0(x)^{m-1}$  and its inverse modulo  $p(x)$  must be computed only once. Now, we can compute  $y_0(x)^{m-1}$  modulo  $p(x)$  using the binary powering algorithm. Since each intermediate result is again a polynomial of degree at most  $\deg p(x)$ , it follows that we can compute  $y_0(x)^{m-1}$  modulo  $p(x)$  in  $\mathcal{O}(M(\deg p(x)) \log m)$  arithmetic operations. The multiplication by  $m$  requires only  $\mathcal{O}(\deg p(x))$  multiplications, and hence its cost is dominated by the cost of the previous step.

The computation of the multiplicative inverse of  $G'(y_0(x))$  modulo  $p(x)$  is carried out using the extended euclidean algorithm, and this can be done in  $\mathcal{O}(M(\deg p(x)) \log \deg p(x))$  arithmetic operations [4, Theorem 8.19, p. 308]. Let  $\text{Inv}(x)$  denote the unique polynomial of degree less than  $\deg p(x)$  such that  $\text{Inv}(x) G'(y_0(x)) \equiv 1 \pmod{p(x)}$ .

At the  $j^{\text{th}}$  step ( $j = 1, \dots, k-1$ ) of the lifting process we compute

$$y_j(x) = -\text{Inv}(x) (y_{j-1}(x)^m - g(x)) + y_{j-1}(x) \bmod p(x)^{j+1}$$

The result is a polynomial of degree at most  $(j+1) \deg p(x)$ .

In order to compute  $y_j(x)$  we compute first  $y_{j-1}(x)^m \bmod p(x)^{j+1}$  using the binary powering algorithm. This requires  $\mathcal{O}(M((j+1) \deg p(x)) \log m)$  arithmetic operations. It is clear that the multiplication by  $-\text{Inv}(x)$  and the addition of  $y_{j-1}(x)$  are dominated by this cost.

Finally we have to consider the cost of step ((iv)) of Section 3.1, i.e. combining the local solutions using the Chinese Remainder Theorem. Let us assume that

$$k_1 \deg p_1(x) \leq \dots \leq k_n \deg p_n(x) = d$$

Let  $r_i(x)$  denote, in this section, a solution of the congruence  $y(x)^m \equiv g(x) \pmod{p_i(x)^{k_i}}$ . Then, it is possible to compute the unique polynomial  $z(x)$  of degree less than  $\deg f(x)$  such that

$$z(x) \equiv r_1(x) \pmod{p_1(x)}, \dots, z(x) \equiv r_n(x) \pmod{p_n(x)}$$

in  $\mathcal{O}(M(nd) \log n)$  arithmetic steps [4, Theorem 8.13, p. 298].

### 3.6 Concluding remarks

From what has been said so far, it is clear that in order to solve efficiently the equation (3.1) we need

- (i). a good algorithm to factor polynomials over  $F$ ; and
- (ii). a good algorithm to extract  $m^{\text{th}}$  roots in some finite extension  $F[\alpha]$  of  $F$ .

Let us point out, first, that it is not obvious that these tasks can be accomplished in a finite number of steps, when  $F$  is an arbitrary constructible field. In other words, before talking about the complexity of an algorithm, one should be sure that the algorithm terminates.

It is clear that when  $F$  is a finite field, the two tasks mentioned above can be accomplished in a finite number of steps.

For the case of the rationals, F. von Schubert showed in 1793 how to find all the factors of degree  $n$  of a given polynomial in a finite number of steps; the method was rediscovered about 90 years later by L. Kronecker (see [49, p. 431] for an historical perspective). Note that the running time of von Schubert's algorithm is exponential in the size of the polynomial to be factored. Moreover, the extraction of an  $m^{\text{th}}$  root of a rational number  $a = r/s$  (with  $\gcd(r, s) = 1$ ) over  $\mathbb{Q}$  is trivial if we know a complete factorization of  $r$  and  $s$ , otherwise it can be carried out by applying the Newton-Raphson method to the polynomials  $x^m - r$  and  $x^m - s$ .

In the next sections we will discuss briefly what is known about the complexity of the problems (i) and (ii) when  $F$  is an algebraic number field or a finite field.

### 3.6.1 Factorization of polynomials over algebraic number fields

H. Zassenhaus [99] was the first to propose the use of Hensel's Lemma for factoring a polynomial with rational coefficients. His method requires factoring the given polynomial modulo some prime  $p$  and then lifting, if possible, the known factorization from  $\mathbb{Z}/p\mathbb{Z}$  to  $\mathbb{Z}$ . Unfortunately, no polynomial time algorithm is known for factoring a polynomial over a finite field.

In 1982 A.K. Lenstra, H.W. Lenstra and L. Lovasz [54] proved that it is possible to factor a polynomial with rational coefficients in polynomial time, and they gave an algorithm to perform the task. Now, by Gauss Lemma we can always assume that the polynomial  $f(x)$  to be factored has integral coefficients and is primitive, that is  $f(x) = \sum_{i=0}^n a_i x^i$  with  $a_i \in \mathbb{Z}$  and  $\gcd(a_0, \dots, a_n) = 1$ . The running time of the algorithm, measured in bit operations is  $\mathcal{O}(n^{12} + n^9(\log |f(x)|)^3)$ , where  $n$  denotes the degree of  $f(x)$ , and  $|f(x)|$  denotes the ordinary Euclidean length of  $f(x)$ , that is

$$|\sum_{i=0}^n a_i x^i| = \left( \sum_{i=0}^n a_i^2 \right)^{1/2}$$

In [57] A.K. Lenstra extended this algorithm to handle polynomials over algebraic number fields. The idea, common to [54] and [57], is to regard the sought for irreducible factor as an element of a certain integral lattice, and then prove that it is actually the smallest element of this lattice. This enables us to compute this factor by using the basis reduction algorithm for lattices developed by the author in [54]. Let  $\alpha$  be a root of a monic irreducible polynomial  $F(y) \in \mathbb{Z}[y]$ . Let  $f(x)$  be a monic polynomial of degree  $n$  in  $\mathbb{Q}[\alpha][x]$  to be factored, and let  $d$  be a rational integer such that  $f(x) \in (1/d)\mathbb{Z}[\alpha][x]$ . Write

$$f(x) = \frac{1}{d} \sum_{i=0}^n \left( \sum_{j=0}^{\deg F-1} a_{i,j} \alpha^j \right) x^i$$

Define  $f_{\max}$  to be the height of  $f$ , that is  $f_{\max} = \max |a_{i,j}|$ , and  $|F|$  to be the Euclidean length of  $F$ . Then, it is shown [57, Theorem 4.5] that Lenstra's algorithm computes the irreducible factorization of  $f(x)$  in

$$O(n^6(\deg F)^6 + n^5(\deg F)^6 \log(\deg F |F|) + n^5(\deg F)^5 \log(d f_{\max}))$$

operations on integers of binary length

$$O(n^3(\deg F)^3 + n^2(\deg F)^3 \log(\deg F |F|) + n^2(\deg F)^2 \log(d f_{\max}))$$

Hence the running time is polynomial in the size of the input.

Another method for factoring polynomials over algebraic number fields (see [78, pp. 346–347] and [23, pp. 142–144]) was developed by B. Trager [89] by improving an idea that was proposed by Kronecker in 1882. Let  $\mathbb{Q}[\alpha]$  be as above, and let  $\sigma_i$  denote the  $\deg F$  distinct embeddings of  $\mathbb{Q}[\alpha]$  into  $\mathbb{C}$ . For a polynomial  $f(x) \in \mathbb{Q}[\alpha][x]$ , let  $\sigma_i(f(x))$  be the polynomial obtained by applying  $\sigma_i$  to the coefficients of  $f(x)$ . Define the norm of  $f(x)$  to be

$$N(f(x)) = \prod_{i=1}^{\deg F} \sigma_i(f(x))$$

Then  $N(f(x))$  is invariant under all the  $\sigma_i$ , and hence by Galois theory it belongs to  $\mathbb{Q}[x]$ . Let us assume first that  $N(f(x))$  is squarefree. If  $N(f(x)) = \prod_i G_i(x)$  is a

complete factorization into irreducibles over  $\mathbb{Q}$ , then  $f(x) = \prod_i \gcd(f(x), G_i(x))$  is a complete factorization into irreducibles over  $\mathbb{Q}[\alpha][x]$ . If  $N(f(x))$  is not squarefree then there are at most  $(n \deg F)^2$  integers  $k$  such that  $N(f(x - k\alpha))$  is not squarefree, and hence we can modify  $f(x)$  suitably in order to obtain a polynomial with squarefree norm. A.L. Chistov and D.Y. Grigoriev [20] proved that the reduction to factoring polynomials over  $\mathbb{Q}$  is polynomial time, and hence, by the result of Lenstra, Lenstra and Lovasz the overall algorithm runs in time polynomial in the size of the input. Unfortunately, the norm of a polynomial of degree  $n$  computed over an extension field of  $\mathbb{Q}$  of degree  $\deg F$  is a polynomial of degree  $n \deg F$ , and this is a serious drawback of the algorithm.

Our experience in experiments conducted with PARI and Maple suggests that none of the algorithms implemented in these packages for factoring polynomials over finite nontrivial extensions of  $\mathbb{Q}$  can be used to solve real problems. In fact, the running time may be extremely large even when factoring a cyclic polynomial of degree 5 over its splitting field.

It is clear that the same factorization algorithms can be used to extract the  $m^{\text{th}}$  roots of an element  $a \in \mathbb{Q}[\alpha]$ , by factoring the polynomial  $x^m - a$  over  $\mathbb{Q}[\alpha]$  and looking for linear factors. However, we have a strong feeling that the problem of extracting  $m^{\text{th}}$  roots in  $\mathbb{Q}[\alpha]$  should be computationally and conceptually easier than the factorization problem.

The problem of extracting an  $m^{\text{th}}$  root  $\beta$  of an element  $a \in \mathbb{Q}[\alpha]$ , has been investigated by J. Blömer [13]. His main result is the following [13, Theorem 18, p. 675]: *There is a probabilistic Monte Carlo algorithm with error probability less than  $2^{-t}$  that decides whether there exists a number  $\beta \in \mathbb{Q}[\alpha]$  such that  $\beta^m = a$ . The running time of the algorithm is polynomial in  $t$ ,  $\log m$  and the input size of  $a$ . If the algorithm returns that there exists a number  $\beta$  with this property, the coefficients of  $\beta$  are computed.*

Recently, G. Ge [40, Theorem 1.1, p. 422] removed the randomness from Blömer's algorithm using diophantine approximation techniques.

In the next section we propose a very simple algorithm to extract an  $m^{\text{th}}$  root  $\beta$

of an element  $a \in \mathbb{Q}[\alpha]$ , which works well when for some integer  $b$  the element  $b\beta$  can be expressed as a linear combination of  $1, \alpha, \dots, \alpha^{n-1}$  with small integer coefficients.

### 3.6.2 A simple algorithm for extracting $m^{\text{th}}$ roots in $\mathbb{Q}[\alpha]$

Let  $a \in \mathbb{Q}[\alpha]$  as above, and let  $m_\alpha(x)$  be the minimal polynomial of  $\alpha$  over  $\mathbb{Q}$ , say of degree  $n$ . If  $\beta$  is an  $m^{\text{th}}$  root of  $a$  then the other  $m^{\text{th}}$  roots of  $a$  are given by  $\omega^j \beta$  ( $j = 0, 1, \dots, m-1$ ) where  $\omega$  is a primitive  $m^{\text{th}}$  root of unity.

Let  $\hat{\beta} \in \mathbb{C}$  be an approximation of  $\beta$ , say with precision  $\epsilon$ , obtained for example using Newton's method (as it is done in PARI). Let  $\hat{\alpha} \in \mathbb{C}$  be an approximation of  $\alpha$ , using the same precision  $\epsilon$ .

If  $\beta \in \mathbb{Q}[\alpha]$  then it is possible to write

$$\beta = \frac{a_0}{b} + \frac{a_1}{b}\alpha + \dots + \frac{a_{n-1}}{b}\alpha^{n-1} \quad (3.4)$$

with  $a_i \in \mathbb{Z}$  ( $i = 0, 1, \dots, n-1$ ) and  $b \in \mathbb{Z}$ . Now, we can rewrite (3.4) as

$$-b\beta + b_0 + b_1\alpha + \dots + b_{n-1}\alpha^{n-1} = 0$$

In particular, if we replace  $\beta$  with  $\hat{\beta}$  and  $\alpha$  with  $\hat{\alpha}$ , then we expect the expression

$$-b\hat{\beta} + b_0 + b_1\hat{\alpha} + \dots + b_{n-1}\hat{\alpha}^{n-1} \quad (3.5)$$

to be close to zero, where the closeness depends on the precision  $\epsilon$  chosen. Hence, for a fixed  $\hat{\beta}$  and  $\hat{\alpha}$  in (3.5), the integers  $b, b_0, \dots, b_{n-1}$  determine a  $\mathbb{Z}$ -linear dependence relation among the elements of the set

$$S = \{-\hat{\beta}, 1, \hat{\alpha}, \dots, \hat{\alpha}^{n-1}\}$$

Such a dependence relation can be discovered, if the precision  $\epsilon$  is adequate, using the following method, described in [23, p. 99]. Let us assume for simplicity that the elements of  $S$  are all reals, and hence rationals. Consider the quadratic form

$$Q(c, c_0, \dots, c_{n-1}) = c_0^2 + \dots + c_{n-1}^2 + d(-c\hat{\beta} + c_0 + c_1\hat{\alpha} + \dots + c_{n-1}\hat{\alpha}^{n-1})^2 \quad (3.6)$$



where  $d$  is a fixed constant. This form defines a scalar product on  $\mathbf{R}^n$ . If  $d$  is large, then a short vector of  $\mathbf{Z}^n$  for this form forces

$$|-c\hat{\beta} + c_0 + c_1\hat{\alpha} + \dots + c_{n-1}\hat{\alpha}^{n-1}|$$

to be small, as well as the integers  $c_0, \dots, c_{n-1}$ . Such a short vector is found using the Lenstra-Lenstra-Lovasz algorithm. If the constant  $d$  and the precision  $\epsilon$  are chosen with caution, then we have

$$c = b, c_0 = b_0, \dots, c_{n-1} = b_{n-1}$$

H. Cohen [23, p. 99] suggests to take the constant  $d$  between  $\epsilon^{-1}$  and  $\epsilon^{-2}$ , and  $\epsilon < a^{-n}$  if we expect the terms  $b_i$  to be of the order of  $a$  (in particular Cohen suggests the choice  $\epsilon = a^{-1.5n}$ ).

The method described above has been implemented in PARI and tested on a SPARCSTATION 10.

We used the PARI procedure *roots* to find an approximation of  $\alpha$ , and the standard exponentiation operator to find an approximation of  $\beta$ . The procedure *lindep2* was used to find a  $\mathbf{Z}$ -linear dependence among the elements of the set  $S$ . The procedure *lindep2* is controlled by a parameter *prec* which determines the constant  $d$  specified above.

As an example of our computations, consider  $\mathbf{Q}[\alpha]$  where  $\alpha$  satisfies the irreducible polynomial

$$p(x) = x^7 + x^6 - 12x^5 - 7x^4 + 28x^3 + 14x^2 - 9x + 1$$

The 4<sup>th</sup> power of

$$f(x) = 34x^3 + 12x + 555$$

modulo  $p(x)$  is

$$\begin{aligned} g(x) = & 2687965064x^6 + 9192876208x^5 + 3355426880x^4 \\ & -1964618456x^3 - 10686231184x^2 + 15800701376x + 94021741105 \end{aligned}$$

Using the default precision of 28 digits, and the maximum value allowed for the parameter *prec*, a 4<sup>th</sup> root of  $g(\alpha)$  over  $\mathbb{Q}[\alpha]$  was found in 660 milliseconds.

For a comparison, the factorization of the polynomial  $x^4 - g(\alpha)$  over the field  $\mathbb{Q}[\alpha]$  took 192 seconds, resulting in

$$x^4 - g(\alpha) = (x - f(\alpha))(x + f(\alpha))(x^2 - t(\alpha))$$

where

$$t(x) = 1156x^6 + 816x^4 + 37740x^3 + 144x^2 + 13320x + 308025$$

For a more interesting class of examples, let  $C_n$  be the  $n^{\text{th}}$  cyclotomic field, that is the field obtained by adjoining to  $\mathbb{Q}$  a primitive  $n^{\text{th}}$  root of the unity.

Using the method described above we found all the  $n^{\text{th}}$  roots of the unity in  $C_n$ , for  $n = 3, \dots, 20$ . The  $n^{\text{th}}$  cyclotomic polynomial was obtained using the standard PARI function *cyclo*( $n$ ). We used the standard precision of 28 digits for finding the complex roots of  $C_n$  and the complex roots of the polynomial  $x^n - 1$ . The parameter *prec* that controls the procedure *lindep2* was set equal to 15.

In Table 3.1 and Table 3.2 we list for each cyclotomic field  $C_n$  the execution time in milliseconds and the symbolic roots of the unity found, expressed as a polynomial in  $x$ , where  $x$  is a primitive  $n^{\text{th}}$  root of the unity.

**Remark.** Without loss of generality we can assume that  $S$  is a set of integers, by multiplying the elements of  $S$  by the least common multiple of their denominators. In this case it is possible to use a different approach for finding small integral relations among the elements of  $S$ , due to J. Hastad *et al* [43], which is based on ideas from the Lattice Basis Reduction algorithm. Hastad's algorithm accepts as input a vector  $\vec{x} = (x_1, \dots, x_n)$  of integers and computes a basis for the  $(n - 1)$ -dimensional lattice of integer relations for  $\vec{x}$ . The algorithm requires at most  $\mathcal{O}(n^3 \log \|\vec{x}\|)$  arithmetic steps using  $\mathcal{O}(n + \log \|\vec{x}\|)$ -bit integers.

### 3.6.3 Factorization of polynomials over finite fields

When  $F = \mathbb{F}_q$  is a finite field, the situation is quite different. Although so far no deterministic polynomial time algorithm for factoring polynomials over finite

fields is known, in practice we have very efficient probabilistic algorithms to perform this task. These algorithms use randomization in the course of the computation. Two classic algorithms are due to E.R. Berlekamp [12] and to E.G. Cantor and H. Zassenhaus [18]. Both these algorithms are typical examples of polynomial time Las Vegas algorithms. Depending on the random string received as part of the input, a Las Vegas algorithm either outputs a correct result or reports failure, where the probability of failure is  $\leq 1/2$ . By running the algorithm  $t$  times, the probability of failure reduces to  $\leq 2^{-t}$ . As opposed to a Monte Carlo algorithm, a Las Vegas algorithm never outputs erroneous results (the term ‘Las Vegas’ to designate this type of algorithm was introduced by L. Babai in [9]). The algorithm of Cantor and Zassenhaus takes about  $\mathcal{O}(n^3 + n^2(\log n)(\log p)^3)$  expected steps to factor a polynomial  $f(x)$  of degree  $n$  over  $\mathbb{F}_p$ , where  $p$  is a prime number.

A new deterministic algorithm for factoring polynomials over finite prime fields has been recently introduced by H. Niederreiter [72]. The algorithm has been subsequently extended to arbitrary finite fields [73]. These algorithms are of great practical value for fields of small characteristics. However, according to H. Niederreiter [74, p. 267] ‘the Holy Grail of polynomial factorization over finite fields, namely a deterministic polynomial time algorithm for solving this problem, is still out of reach’.

### 3.6.4 Finding $m^{\text{th}}$ roots in finite fields

Suppose that  $F = \mathbb{F}_q$  is the finite field with  $q$  elements. As we remarked in the discussion preceding Theorem 3.4, it is easy to decide if an element  $a \in \mathbb{F}_q$  is an  $m^{\text{th}}$  root in  $\mathbb{F}_q$ . However, no polynomial time deterministic algorithm is known for finding an  $m^{\text{th}}$  root in a finite field, unless we assume the Extended Riemann Hypothesis (see for example [3] and [45]).

On the other hand there are very efficient probabilistic algorithms [79] for finding the roots of polynomial equations over finite fields: clearly, the  $m^{\text{th}}$  roots of an element  $a \in \mathbb{F}_q$  are simply the solutions in  $\mathbb{F}_q$  of the polynomial equation  $x^m - a = 0$ .

Without loss of generality we can assume for the rest of this section that  $m$  is prime, since the extraction of a root of arbitrary order can be always accomplished through a sequence of extractions of roots of prime order. Moreover let us assume that  $a^{(q-1)/m} = 1$ , for otherwise there are no solutions in  $\mathbf{F}_q$ .

A general method for extracting  $m^{\text{th}}$  root in  $\mathbf{F}_q$  goes back essentially to Gauss [39, Sections 67–68]. A nice description of the algorithm can be found in [68, Section 5.3, pp. 261–264]. Rather than presenting the algorithm here, we limit ourselves to state the main results concerning its complexity. With the assumption that  $m$  is prime, it is proved in [68, Proposition 1.10, p. 264] that

- If  $m \nmid q - 1$  then the unique  $m^{\text{th}}$  root of  $a$  can be computed in  $\mathcal{O}(\log q)$  operations in  $\mathbf{F}_q$ .
- If  $m \mid q - 1$  then we can compute all the  $m^{\text{th}}$  roots of  $a$  in  $\mathbf{F}_q^*$  in  $\mathcal{O}(m^r \log q)$  operations in  $\mathbf{F}_q$ , assuming that we know an element  $y$  of  $\mathbf{F}_q^*$  of order  $m^r$ , where  $m^r$  is the highest power of  $m$  dividing  $q - 1$ .

In order to apply Gauss' algorithm we need an efficient way to produce an element  $y$  of  $\mathbf{F}_q^*$  of the required order  $m^r$ . One way to achieve this requires one to know an  $m^{\text{th}}$  nonresidue  $g$  in  $\mathbf{F}_q^*$ . In fact, if we let  $s = (q - 1)/m^r$  then the equation that  $g$  satisfies, namely

$$g^{(q-1)/m} \neq 1$$

becomes

$$g^{sm^{r-1}} \neq 1 \tag{3.7}$$

If we let  $y = g^s$  then

$$y^{m^{r-1}} \neq 1 \tag{3.8}$$

Since  $y^m = 1$  it follows that  $y$  belongs to the unique subgroup of  $\mathbf{F}_q^*$  of order  $m^r$ . On the other hand, by (3.8)  $y$  does not belong to the unique subgroup of  $\mathbf{F}_q^*$  of order  $m^{r-1}$ , and therefore its order is exactly  $m^r$ .

**Finding  $m^{\text{th}}$  nonresidues in  $\mathbf{F}_q^*$ .** Equation (3.7) tells us that  $g$  does not belong to the unique subgroup of  $\mathbf{F}_q^*$  of order

$$s \ m^{r-1} = \frac{q-1}{m}$$

Hence, there are

$$q-1 - \frac{q-1}{m}$$

elements in  $\mathbf{F}_q^*$  which are  $m^{\text{th}}$  nonresidues in  $\mathbf{F}_q^*$ . Therefore an  $m^{\text{th}}$  nonresidue  $g$  can be found by random sampling in  $\mathbf{F}_q^*$  in

$$\frac{q-1}{q-1 - \frac{q-1}{m}}$$

expected trials.

The problem of finding deterministically an  $m^{\text{th}}$  nonresidue in  $\mathbf{F}_q^*$  has only been solved conditionally on the assumption of the Extended Riemann Hypothesis. Let us state the main results.

In [10] E. Bach proved, extending a previous result of N.C. Ankeny [6], that if we assume the Extended Riemann Hypothesis then the least  $m^{\text{th}}$  nonresidue mod  $p$ , with  $p$  and  $m$  primes and  $p \equiv 1 \pmod{m}$ , is bounded by  $c \log^2 p$ , where  $c$  is an effectively computable constant independent of  $p$  and  $m$ .

In [45] M.A. Huang extended Bach's result to finite fields of  $p^o$  elements, where  $o$  stands for the order of  $p \bmod m$ , with  $p$  and  $m$  primes as above. He proved that, if we assume the Extended Riemann Hypothesis then there is an absolute effectively computable constant  $c$  such that there exists an  $m^{\text{th}}$  non residue in  $\mathbf{F}_{p^o}$  that can be written as  $a_0 + a_1 w + \dots + a_{o-1} w^{o-1}$  with the absolute values of  $a_i$  bounded above by  $cm^2 \log^2 pm$  and  $\mathbf{F}_p[w] = \mathbf{F}_{p^o}$ , with  $w$  being a root of the  $m^{\text{th}}$  cyclotomic polynomial over  $\mathbf{F}_p$ .

To our knowledge, so far the best deterministic algorithms for finding nonresidues in finite fields, is due to J. Buchmann and V. Shoup [17]. They give an algorithm to find  $m^{\text{th}}$  nonresidues in  $\mathbf{F}_{p^n}$ , which works with any positive integer  $n$ . Assuming again the Extended Riemann Hypothesis, the authors prove that the algorithm runs in polynomial time for a fixed  $n$  and  $p \rightarrow \infty$ .

**Finding primitive roots in  $F_q^*$ .** It is clear that the element  $y$  required by Gauss' algorithm can be found easily if we know a primitive element for  $F_q^*$ .

Since there are exactly  $\phi(q-1)$  primitive elements in  $F_q^*$ , and, for all  $n \geq 3$  we have  $\phi(n)/n \geq c(\log \log n)^{-1}$ , for some positive constant  $c$  (see [68, Exercise 1, p. 266]), it follows that a primitive element can be found by random sampling, in an expected number of  $\mathcal{O}(\log \log q)$  trials.

In [88] V. Shoup investigated the existence of a deterministic polynomial time search procedure for primitive elements in an arbitrary finite field. In particular, he proved that the problem of constructing a primitive polynomial over  $F_p$  ( $p$  prime) of degree  $n$  can be reduced in deterministic time  $(np)^{\mathcal{O}(1)}$  to the problem of testing primitivity. This result is particularly useful when  $p$  is small, e.g.  $p = 2$ . In the same paper Shoup proved that, if we assume the Extended Riemann Hypothesis, then the least primitive root mod  $p$  is  $\mathcal{O}(r^4(\log r + 1)^4(\log p)^2)$ , where  $r$  stands for the number of distinct prime divisors of  $p-1$ , and so  $r = \mathcal{O}(\log p)$ .

**Finding  $m^{\text{th}}$  roots in finite fields of prime order.** If we restrict our finite field to have a prime number  $p$  of elements, then it is possible to give some sharper results.

In [94] H.C. Williams gave an ad hoc algorithm for solving the equation

$$x^m \equiv a \pmod{p} \quad (3.9)$$

assuming that  $p$  and  $m$  are primes, with  $p \equiv 1 \pmod{m}$ , and that  $a^{(p-1)/m} \equiv 1 \pmod{p}$ , that is the congruence 3.9 is solvable. If we define a step to be an arithmetic operation modulo  $p$  or an arithmetic operation on  $m$ -bit integers, then the algorithm runs in  $\mathcal{O}(m^3 \log p)$  steps, assuming that an integer  $b$  has been found such that  $(b^m - a)^{(p-1)/m} \not\equiv 0, 1 \pmod{p}$ .

In [95] K.S. Williams and K. Hardy present a refinement of this algorithm which finds a solution in  $\mathcal{O}(m^4) + \mathcal{O}(m^2 \log p)$  steps, assuming again that the required integer  $b$  has been already determined. This algorithm, suitably modified, can be used to compute  $m^{\text{th}}$  roots in the finite field of  $p^n$  elements, when  $m$  divides  $p^n - 1$ .

field	time ms.	symbolic roots
$C_3$	60	$-x - 1, x, 1$
$C_4$	70	$-x, x, 1, -1$
$C_5$	370	$x^2, x^3, -x^3 - x^2 - x - 1, x, 1$
$C_6$	140	$-x + 1, x, -x, x - 1, 1, -1$
$C_7$	1,240	$x^4, x^3, x^2, x^5, -x^5 - x^4 - x^3 - x^2 - x - 1, x, 1$
$C_8$	550	$-x^2, x^2, -x^3, x, -x, x^3, 1, -1$
$C_9$	1,660	$-x^4 - x, x^2, x^4, x^5, -x^5 - x^2, x, x^3, -x^3 - 1, 1$
$C_{10}$	730	$-x, x^3 - x^2 + x - 1, -x^3 + x^2 - x + 1, x, -x^3, x^2, -x^2, x^3, 1, -1$
$C_{11}$	8,510	$x^6, x^5, x^2, x^9, x^7, x^4, x^3, x^8, -x^9 - x^8 - x^7 - x^6 - x^5 - x^4 - x^3 - x^2 - x - 1, x, 1$
$C_{12}$	820	$-x, x^3 - x, -x^3 + x, x, -x^2, x^2 - 1, -x^2 + 1, x^2, -x^3, x^3, 1, -1$
$C_{13}$	16,140	$x^3, x^{10}, x^{11}, x^2, x^4, x^9, x^7, x^6, x^8, x^5, -x^{11} - x^{10} - x^9 - x^8 - x^7 - x^6 - x^5 - x^4 - x^3 - x^2 - x - 1, x, 1$
$C_{14}$	2,500	$-x^2, x^5, -x^3, x^4, -x^5 + x^4 - x^3 + x^2 - x + 1, x, -x, x^5 - x^4 + x^3 - x^2 + x - 1, -x^5, x^2, -x^4, x^3, 1, -1$
$C_{15}$	6,710	$-x^6 - x, x^4, -x^5 - 1, x^5, x^7 - x^6 - x^3 + x^2 - 1, x^6, -x^7 + x^6 - x^4 + x^3 - x^2 + 1, x, x^7 - x^5 + x^4 - x^3 + x - 1, x^7, -x^7 + x^5 - x^4 - x + 1, x^2, -x^7 - x^2, x^3, 1$

**Table 3.1:** Roots of cyclotomic polynomials from  $C_3$  to  $C_{15}$

field	time ms.	symbolic roots
$C_{16}$	5,810	$-x^5, x^3, -x^2, x^6, -x^6, x^2, -x^4, x^4, -x,$ $x^7, -x^7, x, -x^3, x^5, 1, -1$
$C_{17}$	55,190	$x^7, x^{10}, x^5, x^{12}, x^{15}, x^2, x^{14}, x^3,$ $x^{13}, x^4, x^8, x^9, x^6, x^{11}, -x^{15} - x^{14} - x^{13} - x^{12} -$ $x^{11} - x^{10} - x^9 - x^8 - x^7 - x^6 - x^5 - x^4 - x^3 -$ $x^2 - x - 1, x, 1$
$C_{18}$	3,490	$-x^3 + 1, x^3, x^5 - x^2, -x, -x^5, x^4,$ $-x^4, x^5, -x^3, x^3 - 1, -x^5 + x^2, x, x^4 -$ $x, -x^2, -x^4 + x, x^2, 1, -1$
$C_{19}$	93,730	$x^{13}, x^6, x^{17}, x^2, x^{11}, x^8, x^{15}, x^4,$ $x^{10}, x^9, x^{16}, x^3, x^{14}, x^5, x^{12}, x^7, -x^{17} - x^{16} -$ $x^{15} - x^{14} - x^{13} - x^{12} - x^{11} - x^{10} - x^9 - x^8 -$ $x^7 - x^6 - x^5 - x^4 - x^3 - x^2 - x - 1, x, 1$
$C_{20}$	8,470	$-x^4, x^6, -x^6 + x^4 - x^2 + 1, x^2, -x^2, x^6 -$ $x^4 + x^2 - 1, -x^7, x^3, -x, x^7 - x^5 + x^3 -$ $x, -x^6, x^4, -x^5, x^5, -x^3, x^7, -x^7 + x^5 - x^3 +$ $x, x, 1, -1$

Table 3.2: Roots of cyclotomic polynomials from  $C_{16}$  to  $C_{20}$



## Chapter 4

# Norm equations over cyclic number fields of prime degree

H. W. Lenstra, in a survey paper on algorithms in algebraic number theory [58] wrote:

*Among the many other algorithmic questions in algebraic number theory that merit attention we mention (...), problems from class field theory such as the calculation of Artin symbols, (...)*

In this chapter we consider the following problem, which belongs naturally to class field theory:

*Let  $L = \mathbf{Q}[\alpha]$  be a cyclic extension of the rationals of prime degree  $q$ , and let  $a \in \mathbf{Q}^*$ . Does the equation*

$$N_{L/\mathbf{Q}}(\lambda) = a \tag{4.1}$$

*admit any solution  $\lambda$  in  $L$ ?*

Note that we are not asking how to find a solution  $\lambda$ , but simply determining whether a solution exists. Without loss of generality we can assume that  $a \in \mathcal{O}$ , the ring of algebraic integers of  $L$ .

If we assume that  $a \in \mathbf{Z}$ , the rational integers, and we ask for solutions of (4.1) in the algebraic integers, then we can use an algorithm, due to U. Fincke and M. Pohst

[78, p. 336], based on methods borrowed from the geometry of numbers, which works for any finite extension of  $\mathbb{Q}$  (the problem of determining algebraic integers of given norm arises in class number and class group computations). However, even if (4.1) is not solvable in the algebraic integers, it may still be solvable in  $\mathbb{Q}[\alpha]$ .

In this chapter we give an algorithm to determine if (4.1) is solvable, based on methods from class field theory. The input to our algorithm consists of  $a$  and the minimal polynomial  $m_\alpha(x)$  of  $\alpha$  over  $\mathbb{Q}$ . We show that, if we assume that we are allowed to call an oracle in order to obtain a complete factorization of  $a$  and a complete factorization of  $d_L(\alpha)$ , the discriminant of the  $q$ -tuple  $(1, \alpha, \dots, \alpha^{q-1})$ , then the algorithm runs in time polynomial in the size of the input.

Otherwise stated, in our complexity analysis we are assuming that we are allowed to call an oracle for factoring integers. However we think that this is not a limitation of our algorithm, since we call the oracle only twice, to factor  $a$  and to factor  $d_L(\alpha)$ .

Our algorithm is based on Theorem 2.11, the celebrated Hasse Norm Theorem, which in this context reads as follows:

*A nonzero rational number  $a$  is a norm from  $L$  if and only if it is a local norm at every prime of  $L$ , including the infinite primes.*

We will show below that it is possible to list a finite set of primes, such that these are the only finite primes that must be taken into consideration in applying the Hasse Norm Theorem.

Then, in Section 4.4 we will show that the infinite primes play a role only in the quadratic case.

Finally, in Section 4.5 we present the complete algorithm and discuss its complexity.

An important role in the following discussion is played by Lemma 2.1, which guarantees us that the property of a global field extension of being Galois is preserved by the completions at the finite primes.

Since  $L/\mathbb{Q}$  is Galois, all the ideals lying above a rational prime  $p$  must have the same ramification index  $e(p)$  and the same inertial degree  $f(p)$ . Therefore, the

degree  $[L_{\mathcal{P}} : \mathbb{Q}_p]$ , which is equal to  $e(p)f(p)$ , is independent of the prime ideal  $\mathcal{P}$  lying above  $p$ . Let  $g(p)$  be the number of distinct prime ideals lying above  $p$ . From the formula

$$e(p)f(p)g(p) = [L : \mathbb{Q}]$$

and the primality of  $q$  it follows that either  $e(p) = 1$  or  $e(p) = q$ .

Our first task is to recognize the decomposition type of a rational prime  $p$  in  $L$ . In the next chapter we will develop two polynomial time algorithms to accomplish this task, depending whether an integral basis for  $L$  is known or not.

## 4.1 The unramified case

In this section we deal with the case  $e(p) = 1$ , that is we assume that the prime  $p$  is *unramified* in  $L$ .

The case when  $f(p) = 1$ , that is when  $p$  *splits completely* in  $L$ , is uninteresting, since we have  $L_{\mathcal{P}} = \mathbb{Q}_p$ , and so any  $a \in \mathbb{Q}_p^*$  is the norm of itself in the trivial extension of  $\mathbb{Q}_p$ .

Hence we will restrict our attention to the case  $f(p) = q$ , that is when  $p$  is *inert* in  $L$ . Then  $L_{\mathcal{P}}$  is a nontrivial unramified extension of  $\mathbb{Q}_p$  of degree  $q$ , so we can apply Theorem 2.9 to obtain a complete characterization of the norm group of  $L_{\mathcal{P}}/\mathbb{Q}_p$ .

In our case Theorem 2.9 tells us that, if we express  $a$  as  $p^t u$ , with  $t \in \mathbb{Z}$  and  $u \in U_p$ , then  $a \in N_{L_{\mathcal{P}}/\mathbb{Q}_p}(L_{\mathcal{P}}^*)$  if and only if  $q|t$ .

## 4.2 The totally ramified case

For the totally ramified extensions of  $\mathbb{Q}_p$ , the problem of deciding whether an element of  $\mathbb{Q}_p^*$  is a local norm is harder. We need a preliminary lemma

**Lemma 4.1** *Let  $u = \sum_{i=0}^{\infty} u_i p^i \in U_p$ , with  $u_i$  integers,  $0 \leq u_i < p$  and  $u_0 \neq 0$ . If  $q \neq p$  is a prime, then  $u \in U_p^q$  if and only if  $u_0$  is a  $q^{\text{th}}$  power modulo  $p$ . The index  $(U_p : U_p^q)$  is equal to  $q$  if  $q \mid p-1$ , and it is equal to 1 otherwise.*

*Proof.* Clearly, if  $u$  is a  $q^{\text{th}}$  power in  $\mathbb{Q}_p$  then  $u_0$  is a  $q^{\text{th}}$  power modulo  $p$ . Conversely, let  $g(x) = x^q - u$ . Consider the equation

$$g(x) = 0 \quad (4.2)$$

in  $\mathbb{Q}_p$ . Assume that

$$\hat{x}^q \equiv u_0 \pmod{p}$$

where  $\hat{x} \not\equiv 0 \pmod{p}$ , since  $u_0 \not\equiv 0 \pmod{p}$ . Now

$$g'(\hat{x}) = q\hat{x}^{q-1} \not\equiv 0 \pmod{p}$$

and therefore, by Hensel's lemma [47, Proposition 3.5, p. 83], we can lift  $\hat{x}$  to a solution of the equation (4.2) in  $U_p$ .

If  $q \nmid p-1$  then every integer not divisible by  $p$  has a  $q^{\text{th}}$  root  $\pmod{p}$ . Therefore the argument given above shows that every element of  $U_p$  has a  $q^{\text{th}}$  root in  $U_p$ , and so  $(U_p : U_p^q) = 1$ .

If  $q \mid p-1$ , choose an integer  $w$  which is not a  $q^{\text{th}}$  root  $\pmod{p}$ . Since the group of units of  $\mathbb{Z}/p\mathbb{Z}$  is cyclic, the first part of the lemma shows that the set  $\{1, w, \dots, w^{q-1}\}$  is a set of coset representatives for  $U_p^q$  in  $U_p$ , and therefore  $(U_p : U_p^q) = q$ .  $\square$

Next, using Theorem 2.10, the so called *fundamental equality of class field theory* we are able to characterize the norm groups of the totally ramified extensions of  $\mathbb{Q}_p$  of prime degree.

**Theorem 4.1** *Let  $L_p$  be a totally ramified cyclic extension of  $\mathbb{Q}_p$ , of prime degree  $q$ , where  $q \mid p-1$ . An element  $u \in U_p$  is a norm of a unit in  $L_p$  if and only if  $u$  is a  $q^{\text{th}}$  power in  $U_p$ .*

*Proof.* Let  $U_p$  denote the group of units of  $L_p$ . It is easy to see that

$$N_{L_p/\mathbb{Q}_p}(U_p) \supset U_p^q$$

since for any  $x \in U_p$  we have

$$N_{L_p/\mathbb{Q}_p}(x) = x^q$$

By Lemma 4.1 the index  $(U_p : U_p^q)$  is equal to  $q$ . Then Theorem 2.10, with  $K = L_{\mathcal{P}}$ ,  $k = \mathbb{Q}_p$  and  $e(p) = q = [L_{\mathcal{P}} : \mathbb{Q}_p]$ , gives us the desired equality

$$N_{L_{\mathcal{P}}/\mathbb{Q}_p}(U_{\mathcal{P}}) = U_p^q$$

□

**Remark.** The case  $p \neq q$  and  $q \nmid p-1$ , with  $L_{\mathcal{P}}$  a totally ramified cyclic extension of  $\mathbb{Q}_p$  of degree  $q$  can never happen. Indeed, we certainly have  $N_{L_{\mathcal{P}}/\mathbb{Q}_p}(U_{\mathcal{P}}) \supset U_p^q$ , and Lemma 4.1 implies that  $U_{\mathcal{P}} = U_p^q$ . This contradicts Theorem 2.10 (for a different proof of this statement see [90]).

**Remark.** The remaining case  $p = q$  can be ignored, without incurring the risk of being incomplete. In fact, by Theorem 2.12 if  $a \in \mathbb{Q}^*$  is a  $p$ -local norm for all the primes  $p$ , with the possible exception of one particular prime, then  $a$  must be a local norm at that prime also. Thus, if  $a$  is not a local norm at the prime  $p = q$ , then there is a prime  $p' \neq q$  for which  $a$  is not a local norm. Hence we can avoid consideration of the case  $p = q$ .

### 4.3 The finite primes: summarizing

Let  $p$  be a rational prime and  $\mathcal{P}$  be a prime ideal of  $\mathcal{O}$  lying above  $p$ . We want to determine whether  $a \in N_{L_{\mathcal{P}}/\mathbb{Q}_p}(L_{\mathcal{P}}^*)$ .

If  $p$  splits completely in  $\mathcal{O}$  then every  $a \in \mathbb{Q}_p^*$  is a norm, and so this case is not interesting.

The case where  $p$  is inert is also easily dealt with, as it has been shown in Section 4.1.

It remains to consider the case where  $p$  divides  $d_L$ , the discriminant of  $L/\mathbb{Q}$ , that is when  $L_{\mathcal{P}}$  is a totally ramified extension of  $\mathbb{Q}_p$  of degree  $q$ . We have seen that we can ignore the case  $p = q$ , so suppose  $p \neq q$ . Assume that we know an element  $u_1 \in U_{\mathcal{P}}$  such that

$$pu_1 \in N_{L_{\mathcal{P}}/\mathbb{Q}_p}(L_{\mathcal{P}}^*) \quad (4.3)$$

If  $a = p^t u$  with  $u \in U_p$ , then we can write

$$a = \frac{(pu_1)^t u}{u_1^t}$$

and so  $a \in N_{L_p/Q_p}(L_p^*)$  if and only if

$$\frac{u}{u_1^t} \in N_{L_p/Q_p}(L_p^*) \quad (4.4)$$

Now Theorem 4.1 tells us that (4.4) holds precisely when

$$\frac{u}{u_1^t} \in U_p^q \quad (4.5)$$

Thus we want to construct an element  $u_1 \in U_p$  which satisfies (4.3). For this purpose, take any  $\pi \in \mathcal{P} \setminus \mathcal{P}^2$ . Then  $\nu_p(\pi) = 1$ , and

$$\nu_p(N_{L/Q}(\pi)) = \nu_p(\pi) = 1$$

Since  $[L : Q] = [L_p : Q_p] = q$ , and  $q$  is prime, therefore

$$N_{L_p/Q_p}(\pi) = N_{L/Q}(\pi)$$

Hence can take

$$u_1 = \frac{N_{L_p/Q_p}(\pi)}{p}$$

**Remark.** In order to decide if (4.5) is satisfied we proceed as follows. We know that  $u/u_1^t \in Q^*$  and  $\nu_p(u/u_1^t) = 0$  by construction. We write  $u/u_1^t$  as  $j/k$  with  $j, k \in \mathbb{Z}$  and  $\gcd(j, k) = 1$ , and then we compute  $m, n \in \mathbb{Z}$  such that  $mk + np = 1$ . Now  $jm \in \mathbb{Z}$ , and it can be shown (see [50, p. 12]) that

$$\nu_p\left(\frac{u}{u_1^t} - jm\right) \geq 1$$

Lemma 4.1 then tells us that  $u/u_1^t$  is a  $q$ -th power in  $U_p$  if and only if  $jm$  is a  $q$ -th residue modulo  $p$ , and it is well known (see [75, Theorem 2.27, p. 64]) that this holds if and only if

$$(jm)^{(p-1)/\gcd(q, p-1)} \equiv 1 \pmod{p}$$

that is, if and only if

$$(jm)^{(p-1)/q} \equiv 1 \pmod{p}$$

since  $q \mid p-1$ .

**Remark.** The following example shows that a ramified prime  $p$  might not be a norm at  $p$ , and hence the construction of the element  $u_1$  given above is unavoidable. Consider the cyclic field  $L$  of degree 3 over  $\mathbf{Q}$  generated by the roots of the polynomial  $x^3 - x^2 - 82x + 311$ . The discriminant of  $L$  is  $13^2 \cdot 19^2$ . Now

$$13^{(19-1)/3} \equiv 11 \pmod{19}$$

and hence by Theorem 4.1 the element 13 can not be a norm at 19. Since 13 is clearly a norm at all the unramified primes, if it was a norm at 13 then by Theorem 2.12 it would be a norm at 19 as well, which is a contradiction.

## 4.4 The case of infinite primes

Since  $L = \mathbf{Q}[\alpha]$  is Galois over  $\mathbf{Q}$ , then either  $L$  is *totally real*, that is all the possible embeddings of  $L$  in  $\mathbf{C}$  are real, or  $L$  is *totally complex*, that is all the embeddings are non-real (see [23, Def. 4.1.9]).

Since  $[L : \mathbf{Q}] = q$  is a prime number, if  $q \neq 2$  then  $q$  is odd, and hence  $L$  must necessarily be totally real. If  $[L : \mathbf{Q}] = 2$ , then  $L$  is complex precisely when  $d_L(\alpha) < 0$ .

Given any infinite prime  $\infty$ , if  $L$  is totally real then  $L_\infty = \mathbf{R}$ , and if  $L$  is totally complex then  $L_\infty = \mathbf{C}$ . The completion of  $\mathbf{Q}$  at its unique infinite prime is  $\mathbf{R}$ .

In the totally real case, any element of  $\mathbf{R}$  is the norm of itself in the trivial extension of  $\mathbf{R}$ . In the totally complex case we have  $N_{\mathbf{C}/\mathbf{R}}(\mathbf{C}) = \mathbf{R}^+$ , the nonnegative reals. The latter case can only arise when  $q = 2$ .

## 4.5 The complete algorithm

We now describe an algorithm to decide if  $a \in \mathbf{Q}^*$  is a norm from  $L$ .

Write  $a$  as  $r/s$ , with  $r \in \mathbb{Z}$ ,  $s \in \mathbb{Z} \setminus \{0\}$ , and  $\gcd(r, s) = 1$ . The considerations in Section 4.3 show that the only finite primes that must be taken into account are those which divide  $r$ , those which divide  $s$ , and those which divide the field discriminant  $d_L$ , and that we may ignore the prime  $q$ .

Let us assume first that an integral basis  $\Gamma = \{\omega_1, \dots, \omega_q\}$  for  $L$  is known. Then it is easy to construct the list of ramified primes, since these are exactly those primes dividing the field discriminant  $d_L$ , which can be computed using the formula

$$d_L = \det(\text{Tr}_{L/\mathbb{Q}}(\omega_i \omega_j))$$

In practice, if the integral basis has been obtained using the Pohst-Zassenhaus algorithm, we do not need to construct the list of ramified primes, since this list is returned by the algorithm, together with the integral basis.

In order to decide if a non-ramified prime  $p$  is inert we use the algorithm to be described in Section 5.1.1, whose execution time is polynomial in the size of  $p$  and in the size of  $\Gamma$ . For the other subproblem, i.e. given a ramified prime  $p$  find an element  $\pi \in \mathcal{O}$  whose norm has  $p$ -order 1, we will show in Section 5.1.2 that  $\pi$  can be found in the set

$$\{\text{Tr}_{L/\mathbb{Q}}(\omega) - q\omega \mid \omega \in \Gamma\}$$

and so  $\pi$  can be found in polynomial time.

Let us assume next that an integral basis for  $L$  is not known. In Section 5.2 we will develop an algorithm, called DECOMPOSE, that takes as input  $m_\alpha(x)$  and a rational prime  $p$  and determines the decomposition type of  $p$  in  $L$  in time polynomial in the size of the input. Moreover, if  $p$  is ramified, it returns an element  $\pi \in \mathcal{O}$  whose norm has  $p$ -order 1.

Recall that  $d_L \mid d_L(\alpha)$ , and  $d_L(\alpha)$  can be computed by the formula

$$d_L(\alpha) = (-1)^{q(q-1)/2} N_{L/\mathbb{Q}}(m'_\alpha(\alpha)) \quad (4.6)$$

where  $m'_\alpha(x)$  denotes the formal derivative of  $m_\alpha(x)$ . Once a complete factorization of  $d_L(\alpha)$  is known, we can use the algorithm DECOMPOSE to determine the prime



divisors  $p$  of  $d_L$ , and for each of them a corresponding element  $\pi$  whose norm has  $p$ -order 1. The following result, due to B.M. Urazbaev [90] can be used to save some work:

**Theorem 4.2** *The discriminant  $d_L$  of a cyclic extension  $L/\mathbb{Q}$  of odd prime degree  $q$  has the form:*

$$d_L = q^a \prod p_i^{q-1}$$

where the  $p_i$  are distinct rational primes of the form  $nq+1$ , and  $a = 0$  or  $a = 2(q-1)$ .

Clearly, by Theorem 4.2, we can ignore those primes  $p$  dividing  $d_L(\alpha)$  for which either  $p \not\equiv 1 \pmod{q}$  or  $\nu_p(d_L(\alpha)) < q-1$ .

The complete algorithm NORM is shown in Figure 4.1. It takes as input  $a$  and  $m_\alpha(x)$ , and returns *TRUE* if  $a \in N_{L/\mathbb{Q}}(L^*)$ , *FALSE* otherwise.

In analyzing the complexity of the algorithm NORM, we will ignore the cost of factoring  $a$  and  $d_L(\alpha)$ .

Using the encoding described in Section 2.8 we want to show that the algorithm NORM runs in time polynomial in the size of the input. For this purpose it is enough to bound the size and the number of the primes involved in the test.

Now, the size of each prime divisor of  $a$  is at most equal to  $\text{size}(a)$ . Moreover, since a rational integer  $n > 2$  has at most  $1 + \log n$  factors, it follows that  $a$  has at most  $1 + \text{size}(a)$  prime divisors.

Using a bound due to Mahler [62, Corollary to Theorem 1, p. 261] we obtain

$$|d_L(\alpha)| < q^q (1 + |a_{q-1}| + \dots + |a_0|)^{2q-2} \quad (4.7)$$

Define  $H = \max(|a_i|)_{i=0, \dots, q-1}$  to be the height of  $m_\alpha(x)$ .

The same argument used above shows that  $d_L(\alpha)$  has at most

$$q \log q + 2(q-1) \log(1 + |a_{q-1}| + \dots + |a_0|)$$

factors, that is at most  $q \log q + 2(q-1) \log(qH)$  factors. The size of each factor is bounded by  $q \log q + 2(q-1) \log(qH)$ . Asymptotically,

$$q \log q + 2(q-1) \log(qH) = \mathcal{O}(q \log q + q \log H)$$

The algorithm DECOMPOSE is called to determine the decomposition type of each prime divisor of  $a$  and of each prime divisor of  $d_L(\alpha)$ , hence it is called at most  $\mathcal{O}(\log a + q \log q + q \log H)$  times.

In the next chapter we will determine the execution time of the algorithm DECOMPOSE.

**On the number of ramified primes.** It is interesting to give an upper bound on the number of ramified primes in  $L = \mathbb{Q}[\alpha]$ . Since  $d_L \mid d_L(\alpha)$ , it follows that if  $p \neq q$  is a positive prime divisor of  $d_L$ , by Theorem 4.2 we must have  $p \leq \sqrt[q]{d_L(\alpha)}$ , and therefore, by (4.7)

$$p < q^{q/(q-1)}(1 + |a_{q-1}| + \dots + |a_0|)^2$$

which in turn implies that

$$\begin{aligned} \text{size}(p) &< \frac{q}{q-1} \log q + 2 \log(1 + |a_{q-1}| + \dots + |a_0|) \\ &< \frac{q}{q-1} \log q + 2 \log(qH) \end{aligned}$$

Now,  $d_L \mid d_L(\alpha)$  and so  $p^{q-1} \mid d_L(\alpha)$  for each ramified prime  $p \neq q$ . Therefore the product of all the ramified primes not equal to  $q$  divides  $\sqrt[q]{d_L(\alpha)}$ . Hence the number of ramified primes  $p \neq q$  to take into consideration is bounded above by  $\log \sqrt[q]{d_L(\alpha)}$ , that is by

$$\frac{q}{q-1} \log q + 2 \log(qH)$$

```

procedure NORM( $a, m_\alpha(x)$ ):
  if ( $[L : \mathbf{Q}] = 2$  and  $d_L(\alpha) < 0$  and  $a < 0$ ) then
    return FALSE
  endif
  construct the set  $RP$  of ramified primes;
  express  $a$  as  $r/s$ , with  $r, s \in \mathbf{Z}$  and  $\gcd(r, s) = 1$ ;
  let  $NP$  be the set of positive primes dividing  $r$ ;
  let  $DP$  be the set of positive primes dividing  $s$ ;
  for all the  $p$  in  $RP \cup NP \cup DP$ , with  $p \neq q$  do
    let  $t = \nu_p(a)$ ;
    if  $p \notin RP$  then
      if ( $p$  is inert and  $q \nmid t$ ) then
        return FALSE
      endif
    else
      let  $\pi \in L$  be such that  $\nu_p(N_{L/\mathbf{Q}}(\pi)) = 1$ ;
      let  $u = a/(N_{L/\mathbf{Q}}(\pi)^t)$ ;
      express  $u$  as  $j/k$ , with  $j, k \in \mathbf{Z}$  and  $\gcd(j, k) = 1$ ;
      compute  $m, n \in \mathbf{Z}$  such that  $mk + np = 1$ ;
      let  $z = (p - 1)/q$ ;
      if  $(jm)^z \not\equiv 1 \pmod{p}$  then
        return FALSE
      endif
    endif
  endfor
  return TRUE

```

Figure 4.1: The algorithm NORM.

## Chapter 5

# Recognizing the decomposition type of a rational prime

:

Let  $L$  be a cyclic number field of prime degree  $q$  over  $\mathbb{Q}$ , and let  $\mathcal{O}$  denote the ring of integers of  $L$ . In this chapter we consider the following two problems

- (i). Recognize the decomposition type of a rational prime  $p$  in  $L$ , with  $p$  not equal to  $q$ ;
- (ii). If  $p$  is a ramified prime not equal to  $q$ , find an Eisenstein element  $\pi$  at  $p$ , that is an element  $\pi \in \mathcal{O}$  whose minimal polynomial  $m_\pi(x)$  is Eisenstein at  $p$ .

In Section 5.1 we show that these problems admit a relatively simple solution when an integral basis  $\Gamma = \{\omega_1, \dots, \omega_q\}$  for  $L$  over  $\mathbb{Q}$  is known.

Since it is expensive to compute an integral basis, in Section 5.2 we develop a fast algorithm to solve the problems stated above when an integral basis for  $L$  over  $\mathbb{Q}$  is not known.

## 5.1 Integral basis known

Let  $\Gamma = \{\omega_1, \dots, \omega_q\}$  be an integral basis for  $L$  over  $\mathbb{Q}$ . Now, the discriminant of  $L/\mathbb{Q}$  is given by the formula

$$d_L = \det(\text{Tr}_{L/\mathbb{Q}}(\omega_i \cdot \omega_j))$$

and so the ramified primes are easily found, since these are exactly those primes dividing the discriminant.

We recall once again that there is a very general algorithm for computing the integral basis of a number field, due to M. Pohst and H. Zassenhaus (see [77], [23, Chapter 6, Section 1, pp. 297–306]). The input of the Pohst-Zassenhaus algorithm consists of the minimal polynomial over  $\mathbb{Q}$  of a primitive element for the field; the algorithm runs in time polynomial in the size of the input, assuming the use of oracles for factoring integers and factoring polynomials over finite fields. The algorithm of Pohst and Zassenhaus has been improved by D.J. Ford in [34]. Recently A.L. Chistov [21] was able to prove that computing maximal orders is polynomial time equivalent to computing the largest square dividing a positive integer (see also [16, Theorem 1, p. 40] and [58, Theorem 4.4]). Unfortunately, no good algorithms are known for the problem of finding the largest square factor of a given integer [58, Section 2.3, p. 6] which seems to be as difficult as integer factorization.

Moreover, if an integral basis for  $L/\mathbb{Q}$  is known, it is possible to solve the problems stated at the beginning of this chapter using a very general algorithm for decomposing a rational prime in a number field, due to J. Buchmann and H.W. Lenstra [15]. A nice description of the Buchmann-Lenstra algorithm can be found in [23, Section 6.2.2, p. 309].

Rather than taking this route, we exploit the Galois structure of  $L$  to obtain a very simple and much more efficient solution of our problem.

### 5.1.1 Recognizing the inert primes

Our first task is to recognize if the unramified rational prime  $p$  splits completely in  $L$  or it is inert. Let  $\mathcal{O}$  denote the ring of integers of  $L$ . It is clear that the  $\mathbb{F}_p$ -algebra  $\mathcal{O}/p\mathcal{O}$  is a field if and only if  $p\mathcal{O}$  is a maximal ideal (or, equivalently a prime ideal, since  $\mathcal{O}$  is a Dedekind domain) of  $\mathcal{O}$ , that is if  $p$  does not split. Otherwise, from the primality of  $q$  and the fact that  $L/\mathbb{Q}$  is Galois, it follows that  $\mathcal{O}/p\mathcal{O}$  decomposes into the direct product of  $q$  fields isomorphic to  $\mathbb{F}_p$ .

The problem of decomposing a separable commutative algebra over a finite field has been studied extensively (see [30, Section 2.4] and [23, p. 313]), and there are efficient algorithms to accomplish this task. In our case all we need is to recognize if  $\mathcal{O}/p\mathcal{O}$  is a field. For this purpose we prove the following lemma:

**Lemma 5.1** *Let  $L$  be an algebraic number field and  $p$  be a rational prime. Let  $\mathcal{O}$  be the ring of integers of  $L$ . Let  $\phi : \mathcal{O}/p\mathcal{O} \rightarrow \mathcal{O}/p\mathcal{O}$  be the (linear) map given by  $x \mapsto x^p - x$ . Then  $\mathcal{O}/p\mathcal{O}$  is a field if and only if the dimension of the kernel of  $\phi$  is equal to 1.*

*Proof.* We know that  $\mathcal{O}/p\mathcal{O}$  is a finite separable algebra over  $\mathbb{F}_p$ , and more precisely it is the direct product of fields, and  $\phi$  is linear because  $\mathbb{F}_p$  has characteristic  $p$ . Write  $\mathcal{O}/p\mathcal{O}$  as  $A_1 \times \cdots \times A_r$ , where each  $A_i$  is a finite extension of the base field  $\mathbb{F}_p$ . An element  $(\alpha_1, \dots, \alpha_r)$  is in the kernel of  $\phi$  if and only if each  $\alpha_i$  belongs to  $\mathbb{F}_p$ . It follows that the dimension of  $\ker(\phi)$  is equal exactly to  $r$ , and this proves the assertion.  $\square$

In order to apply Lemma 5.1 we need an efficient way to compute the kernel of the linear map  $\phi$ . Let us assume that the elements  $\{\omega_1, \dots, \omega_q\}$  of the integral basis  $\Gamma$  are given as

$$\omega_i = \frac{\sum_{j=0}^{q-1} z_{ij} \alpha^j}{d} \quad (1 \leq i \leq q)$$

where  $d, z_{ij} \in \mathbb{Z}$ , and the matrix  $(z_{ij})$  is in Hermite Normal Form (this is a common assumption, e.g. in Cohen's book [23], since it allows one to reduce drastically the amount of computations required in many number theoretical algorithms).

Clearly the matrix  $A = (\frac{z_{ij}}{d})$  takes the original basis  $\{1, \alpha, \dots, \alpha^{q-1}\}$  for  $L$  as a vector space over  $\mathbb{Q}$  into the new basis  $\Gamma = \{\omega_1, \dots, \omega_q\}$ .

Let us compute first a set  $S$  of  $q^3$  elements  $\eta_{ijk}$  such that

$$\omega_i \omega_j = \sum_{k=1}^q \eta_{ijk} \omega_k \quad (1 \leq i, j \leq q) \quad (5.1)$$

Clearly  $\eta_{ijk} \in \mathbb{Z}$  ( $1 \leq i, j, k \leq q$ ); moreover, since

$$\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Q} = L$$

it follows that  $S$  is a set of structure constants for  $L$  as an algebra over  $\mathbb{Q}$ .

Generally, a set of structure constants for an algebra over a field can be computed by solving a (eventually very large) system of linear equations, and it can be shown that the number of arithmetic operations required is polynomial in the dimension of the algebra (see [30] for an accurate analysis of algorithms dealing with finite dimensional associative algebras).

In our case we proceed as follows: since the algebra is commutative, we need to compute only  $q(q+1)/2$  products  $\omega_i \omega_j$ , namely those products with  $1 \leq i \leq j \leq q$ . Let us express each product  $\omega_i \omega_j$  as a polynomial in  $\alpha$  with rational coefficients, that is

$$\omega_i \omega_j = \sum_{k=0}^{q-1} g_{ijk} \alpha^k \quad (5.2)$$

Now, we can easily recover the coefficients  $\eta_{ijk}$  in (5.1) from the coefficients  $g_{ijk}$  in (5.2) by exploiting the fact that the matrix  $(\frac{\alpha^j}{d})$  is triangular.

Once we have computed  $S$ , the set

$$\bar{S} = \{\bar{\eta}_{ijk} = \eta_{ijk} \bmod p \mid 1 \leq i, j, k \leq q\}$$

gives us a set of structure constant for  $\mathcal{O}/p\mathcal{O}$  as an algebra over  $\mathbb{F}_p$ . In other words, there is a basis  $\bar{\omega}_1, \dots, \bar{\omega}_q$  for  $\mathcal{O}/p\mathcal{O}$  as an algebra over  $\mathbb{F}_p$  such that

$$\bar{\omega}_i \bar{\omega}_j = \sum_{k=1}^q \bar{\eta}_{ijk} \bar{\omega}_k \quad (1 \leq i, j \leq q)$$

In order to compute the matrix  $M$  which represents the linear transformation  $\phi$  we determine the effect of  $\phi$  on the basis elements of  $\mathcal{O}/p\mathcal{O}$  as follows.

For each  $i$  ( $1 \leq i \leq q$ ) we compute  $\bar{\omega}_i^p$  using the binary powering algorithm [23, p. 8], which requires only  $\mathcal{O}(\log p)$  steps. Clearly we need to consider only the cost of squaring at each step, since this cost dominates the overall complexity. Now, in order to square an expression of the form  $c_1 \bar{\omega}_1 + \dots + c_q \bar{\omega}_q$  we use the knowledge of the structure constants of the  $\mathbb{F}_p$ -algebra  $\mathcal{O}/p\mathcal{O}$ . It is easily seen that squaring the above expression requires  $\mathcal{O}(q^3)$  operations in  $\mathbb{F}_p$ . Hence the computation of  $\bar{\omega}_i^p$  requires  $\mathcal{O}(q^3 \log p)$  arithmetic operations in  $\mathbb{F}_p$ . This has to be done for all the basis elements, for a total of  $\mathcal{O}(q^4 \log p)$  arithmetic operations in  $\mathbb{F}_p$ .

Next, if we write

$$\overline{\omega_i^p} - \overline{\omega_i} = \sum_{k=1}^q \overline{b_{ik} \omega_k}$$

then  $M = (\overline{b_{ik}})$  is the required matrix.

Finally, the computation of the kernel of  $\phi$  or, what is the same, of  $M$ , requires only  $\mathcal{O}(q^3)$  arithmetic operations (see [23, pp. 56–58]) in the field  $\mathbb{F}_p$ .

*Remark.* The requirement for the integral basis  $\Gamma$  to be in the Hermite Normal Form allows one to compute easily the structure constants for  $L$  as an algebra over  $\mathbb{Q}$ . However, it might happen that the structure constants found in this naïve way have very large size, and therefore their computation could be very expensive. In order to overcome this problem H.W. Lenstra suggests in [58] to use a basis  $\Gamma$  which has been LLL reduced. In this case it is possible to prove [58, p. 11] that  $\eta_{ijk} = |d_L|^{\mathcal{O}(q)}$  for all  $i, j, k$  ( $1 \leq i, j, k \leq q$ ), where  $d_L$  denotes the discriminant of  $L$ , and so  $\text{size}(\eta_{ijk}) = \mathcal{O}(q(2 + \log |d_L|))$ .

### 5.1.2 Finding Eisenstein Elements

Given a ramified prime  $p$ , the following lemma allows one to find an element  $\pi \in \mathcal{P} \setminus \mathcal{P}^2$ .

**Lemma 5.2** *Let  $L$  be a cyclic extension of  $\mathbb{Q}$  of prime degree  $q$ . Let  $\mathcal{B}$  be an integral basis for  $L/\mathbb{Q}$ . If  $p$  is a ramified rational prime not equal to  $q$ , and  $\mathcal{P}$  denotes the unique prime ideal of  $\mathcal{O}$  lying above  $p$ , then  $\nu_{\mathcal{P}}(\text{Tr}_{L/\mathbb{Q}}(\omega) - q\omega) = 1$  for some  $\omega \in \Gamma$ .*

*Proof.* Let  $\sigma$  be a generator of  $\text{Gal}(L/\mathbb{Q})$ . The uniqueness of  $\mathcal{P}$  shows that  $\sigma(\mathcal{P}) = \mathcal{P}$  and  $\mathcal{O} = \mathbb{Z} + \mathcal{P}$ . Thus

$$\sigma(\theta) - \theta \in \mathcal{P} \quad \text{for all } \theta \in \mathcal{O}$$

Hence for each  $\theta \in \mathcal{O}$  we must have

$$\text{Tr}_{L/\mathbb{Q}}(\theta) - q\theta = \sum_{i=1}^q (\sigma^i(\theta) - \theta) \in \mathcal{P}$$



Now suppose that  $\gamma \in \mathcal{P} \setminus \mathcal{P}^2$ . Since  $\text{Gal}(L/\mathbf{Q})$  fixes  $\mathcal{P}$ , we must have

$$\text{Tr}_{L/\mathbf{Q}}(\gamma) = \sum_{i=1}^q \sigma^i(\gamma) \in \mathcal{P} \cap \mathbf{Z} = p\mathbf{Z} \subseteq p\mathcal{O} = \mathcal{P}^q$$

and so

$$\text{Tr}_{L/\mathbf{Q}}(\gamma) - q\gamma \in \mathcal{P} \setminus \mathcal{P}^2$$

because  $q\gamma \in \mathcal{P} \setminus \mathcal{P}^2$ . Since the map

$$\theta \mapsto \text{Tr}_{L/\mathbf{Q}}(\theta) - q\theta$$

is  $\mathbf{Z}$ -linear, it follows that

$$\text{Tr}_{L/\mathbf{Q}}(\omega) - q\omega \in \mathcal{P} \setminus \mathcal{P}^2$$

for some  $\omega \in \Gamma$ .  $\square$

Since  $\mathcal{P}$  is the only prime ideal lying above  $p$  and its inertial degree is 1, then

$$\nu_p(N_{L/\mathbf{Q}}(\beta)) = \nu_p(\beta) \text{ for all } \beta \in L$$

(see [14, p. 197]). Hence, by Lemma 5.2 it is sufficient to find an  $\omega \in \Gamma$  such that

$$\nu_p(N_{L/\mathbf{Q}}(\text{Tr}_{L/\mathbf{Q}}(\omega) - q\omega)) = 1$$

Then

$$\text{Tr}_{L/\mathbf{Q}}(\omega) - q\omega \in \mathcal{P} \setminus \mathcal{P}^2$$

as desired.

Let us show now that the search for an Eisenstein element can be done in time polynomial in  $q$ , in the size of  $m_\alpha(x)$ , and in the size of  $\Gamma$ .

Let  $m_\alpha(x) = x^q + a_{q-1}x^{q-1} + \dots + a_1x + a_0$ , with  $a_i \in \mathbf{Z}$  ( $i = 0, \dots, q-1$ ), and define the height of  $m_\alpha(x)$  to be  $H = \max_{i=1, \dots, q}(|a_i|)$ .

Let us assume that we have computed in advance the traces of  $\alpha, \alpha^2, \dots, \alpha^{q-1}$ , using for example Newton's formulas [23, Proposition 4.3.3, p. 161], and let

$$B = \max(|\text{Tr}_{L/\mathbf{Q}}(\alpha^j)|)_{j=0, \dots, q-1}$$

Let us also assume that an algebraic number  $\beta$  is represented as

$$\beta = \frac{b_{q-1}\alpha^{q-1} + \dots + b_1\alpha + b_0}{d}$$

with  $d > 0$ ,  $b_{q-1}, \dots, b_1, b_0, d \in \mathbb{Z}$  and  $\gcd(b_{q-1}, \dots, b_1, b_0, d) = 1$ . We call the  $(q+1)$ -tuple

$$(b_{q-1}, \dots, b_1, b_0, d)$$

the *standard representation* of  $\beta$ . We define  $\text{size}(\beta)$  to be the sum of the sizes of the components of its standard representation. For an algebraic number  $\beta$  represented as above, define  $|\beta|_{\max}$  to be  $\max(|b_i|)_{i=0, \dots, q-1}$ .

Then, the computation of  $\text{Tr}_{L/\mathbb{Q}}(\omega)$  is done by just computing the trace of the numerator of  $\omega$ , in its standard representation. This requires  $\mathcal{O}(q)$  operations on integers which are bounded in absolute value by  $\max(B, |\omega|_{\max})$ . The trace computation can be done in  $\mathcal{O}(q (\log \max(B, |\omega|_{\max}))^2)$  elementary operations. The result is an integer  $l$ , bounded in absolute value by  $qB|\omega|_{\max}$ . By linearity,  $\text{Tr}_{L/\mathbb{Q}}(\omega) = l/d$ , however we do not reduce this fraction.

The multiplication of  $\omega$  by  $q$  requires  $\mathcal{O}(q)$  multiplications of  $q$  times integers which are bounded in absolute value by  $|\omega|_{\max}$ . This can be done in  $\mathcal{O}(q \log(q) \log(|\omega|_{\max}))$  elementary operations. Clearly  $|q\omega|_{\max} = q|\omega|_{\max}$ .

The construction of  $\delta = \text{Tr}_{L/\mathbb{Q}}(\omega) - q\omega$  requires just one subtraction, which can be performed in  $\mathcal{O}(\log \max(q|\omega|_{\max}, qB|\omega|_{\max}))$  elementary operations, that is in  $\mathcal{O}(\log q + \log B + \log |\omega|_{\max})$  elementary operations. The result is written as

$$\delta = \frac{c_{q-1}\alpha^{q-1} + \dots + c_1\alpha + c_0}{d}$$

where, eventually,  $\gcd(c_{q-1}, \dots, c_1, c_0, d) \neq \pm 1$ . Note that  $\max(|c_i|)_{i=0, \dots, q-1} = qB|\omega|_{\max}$ .

Finally,  $N_{L/\mathbb{Q}}(\delta)$  is obtained (see [23, Proposition 4.3.4, p. 162]) by computing the following resultant:

$$N_{L/\mathbb{Q}}(\delta) = d^{-q} \text{Res}(m_\alpha(x), c_{q-1}x^{q-1} + \dots + c_1x + c_0)$$

This can be done in

$$\mathcal{O}(q^3 \log(qB|\omega|_{\max}) + (\log(qB|\omega|_{\max}))^2)$$

elementary operations, using the modular resultant algorithm of G.E. Collins [25].

We are left with the problem of determining  $B$ , that is an upper bound on the absolute values of the traces of  $\alpha, \alpha^2, \dots, \alpha^{q-1}$ . A quick way to proceed is the following: let  $M_\alpha$  be the companion matrix of  $\alpha$ . Clearly  $M_\alpha$  has integral coefficients, and, if we denote by  $|M_\alpha^j|_{\max}$  the maximum of the absolute values of the entries of  $M_\alpha^j$ , we have

$$\begin{aligned} |M_\alpha^j|_{\max} &\leq q |M_\alpha^{j-1}|_{\max} |M_\alpha|_{\max} \\ &\leq q^{j-1} |M_\alpha|_{\max}^j \\ &= q^{j-1} H^j \end{aligned}$$

where  $H = |M_\alpha|_{\max}$  is the height of  $m_\alpha(x)$ . Then we can take

$$B = q^{q-2} H^{q-1}$$

The overall complexity is dominated by the resultant calculation, so we need

$$\mathcal{O}(q^3 \log(q^{q-1} H^{q-1} |\omega|_{\max}) + (\log(q^{q-1} H^{q-1} |\omega|_{\max}))^2)$$

elementary operations. Since we have to check in the worst case all the elements of the basis  $\Gamma$ , we require at most

$$\mathcal{O}(q^4 \log(q^{q-1} H^{q-1} |\omega|_{\max}) + q(\log(q^{q-1} H^{q-1} |\omega|_{\max}))^2)$$

elementary operations.

## 5.2 Integral basis unknown

In this section we develop a fast algorithm to find the decomposition type of a rational prime  $p$  in  $L$  as well as to find an Eisenstein element at a ramified prime

$p$ , assuming that an integral basis for  $L$  over  $\mathbf{Q}$  is not known (an algorithm for computing the discriminant of a cyclic number field of prime degree, which uses totally different ideas, is described in Chapter 8).

So, let us assume that  $L = \mathbf{Q}[\alpha]$ , where  $\alpha$  is an algebraic integer given by its minimal polynomial  $m_\alpha(x)$  over  $\mathbf{Q}$ . Clearly  $m_\alpha(x) \in \mathbf{Z}[x]$ .

In the following lemma we relate the decomposition of the minimal polynomial  $m_\alpha(x)$  of  $\alpha$  over  $\mathbf{Q}_p$  to the decomposition of  $p$  in  $L$ .

**Lemma 5.3** *Let  $L = \mathbf{Q}[\alpha]$  be a cyclic number field of prime degree  $q$ , with  $\alpha$  an algebraic integer, and let  $p$  be a rational prime. If  $p$  is inert or totally ramified in  $L$  then  $m_\alpha(x)$  is irreducible over  $\mathbf{Q}_p$ .*

*Proof.* Let  $K = \mathbf{Q}[\beta]$  be an arbitrary number field. It can be shown (see [47, Exercise 1, p. 92]) that if  $\mathcal{P}_i$  ( $i = 1, \dots, r$ ) are the prime ideals lying above a rational prime  $p$ , with inertial degree  $f(\mathcal{P}_i|p)$  and ramification index  $e(\mathcal{P}_i|p)$ , then  $m_\beta(x)$  splits into  $r$  factors in  $\mathbf{Q}_p$ , with respective degrees

$$e(\mathcal{P}_1|p)f(\mathcal{P}_1|p), \dots, e(\mathcal{P}_r|p)f(\mathcal{P}_r|p)$$

In our case we have  $r = 1$  and so  $m_\alpha(x)$  is irreducible over  $\mathbf{Q}_p$ .  $\square$

The following corollary to Lemma 5.3 is an immediate consequence of Corollary 2.2 of Hensel's Lemma (Theorem 2.7).

**Corollary 5.1** *Let  $L = \mathbf{Q}[\alpha]$  be a cyclic number field of prime degree  $q$ , with  $\alpha$  an algebraic integer, and let  $p$  be a rational prime. If  $p$  does not split in  $L$ , then  $m_\alpha(x)$  is either irreducible over  $\mathbf{F}_p$  or it is the  $q^{\text{th}}$  power of a linear polynomial over  $\mathbf{F}_p$ .*

The next lemma exploits the Galois structure of  $L$  to obtain more information about the decomposition of the rational primes in  $L$ .

**Lemma 5.4** *Let  $L = \mathbf{Q}[\alpha]$  be a cyclic number field of prime degree  $q$ , with  $\alpha$  an algebraic integer, and let  $p$  be a rational prime. If  $p$  splits completely in  $L$ , then  $m_\alpha(x)$  splits into (possibly equal) linear factors over  $\mathbf{F}_p$ . Conversely, if  $m_\alpha(x)$  has at least two distinct linear factors over  $\mathbf{F}_p$ , then  $p$  splits completely in  $L$ .*

*Proof.* If  $p$  splits completely in  $L$  then the Frobenius automorphism of  $p$  is trivial. Hence any root of  $m_\alpha(x)$  has only one conjugate in the algebraic closure of  $\mathbf{F}_p$ , namely itself. This proves the first assertion.

To prove the second assertion assume that  $p$  does not split in  $L$  and  $m_\alpha(x) \equiv g(x)h(x) \pmod{p}$ , with  $g(x)$  and  $h(x)$  relatively prime. This clearly contradicts Corollary 5.1.  $\square$

The next lemma gives us a partial converse of Corollary 5.1.

**Lemma 5.5** *Let  $K = \mathbf{Q}[\beta]$  be an algebraic number field, with  $\beta$  integral over  $\mathbf{Z}$ , and let  $p$  be a rational prime. If the minimal polynomial  $m_\beta(x)$  of  $\beta$  over  $\mathbf{Q}$  is irreducible over  $\mathbf{F}_p$ , then  $p$  is inert in  $K$ .*

*Proof.* See [26, Proposition 5.11, p. 102].  $\square$

Combining the results obtained so far we obtain the following.

**Lemma 5.6** *Let  $L = \mathbf{Q}[\alpha]$  be a cyclic extension of  $\mathbf{Q}$  of prime degree  $q$ , where  $\alpha$  is an algebraic integer. Then its minimal polynomial  $m_\alpha(x)$  is either irreducible over  $\mathbf{F}_p$  or it splits into linear factors over  $\mathbf{F}_p$ . If  $m_\alpha(x)$  has at least two distinct roots in  $\mathbf{F}_p$ , then  $p$  splits completely in  $L$ . If  $m_\alpha(x)$  has no roots in  $\mathbf{F}_p$  then  $p$  is inert in  $L$ .*

The value of Lemma 5.6 lies in the fact that it is possible to check very efficiently whether its hypotheses are fulfilled. For this purpose we compute

$$l(x) = \gcd(x^p - x, m_\alpha(x))$$

over  $\mathbf{F}_p$ ; then  $m_\alpha(x)$  has no roots in  $\mathbf{F}_p$  precisely when  $\deg l(x) = 0$ , and it is a  $q^{\text{th}}$  power over  $\mathbf{F}_p$  precisely when  $\deg l(x) = 1$ . In practice we compute

$$j(x) = x^p \bmod m_\alpha(x)$$

over  $\mathbf{F}_p$ , using the binary powering algorithm (see [23, p. 8]); then

$$l(x) = \gcd(j(x) - x, m_\alpha(x))$$

Before proving the main theorem of this section, we need a last lemma

**Lemma 5.7** *Let  $L = \mathbf{Q}[\alpha]$  be a cyclic number field of prime degree  $q$  with  $\alpha \in \mathcal{O}$ , the ring of integers of  $L$ , and let  $p$  be a rational prime.*

*If  $p$  ramifies in  $L$  and  $\pi \in \mathcal{P} \setminus \mathcal{P}^2$ , where  $\mathcal{P}$  denotes the unique prime ideal of  $\mathcal{O}$  above  $p$ , then the minimal polynomial  $m_\pi(x)$  of  $\pi$  is Eisenstein at  $p$ . Conversely, if the minimal polynomial  $m_\pi(x)$  of some  $\pi \in \mathcal{O}$  is Eisenstein at  $p$ , then  $p$  ramifies in  $L$ .*

*Proof.* See [52, Proposition 11, p. 52]).  $\square$

Now we can state the main theorem of this section.

**Theorem 5.1** *Let  $L = \mathbf{Q}[\alpha]$  be a cyclic number field of prime degree  $q$  with  $\alpha \in \mathcal{O}$ , the ring of integers of  $L$ , and let  $p$  be a rational prime. Then:*

(i). *If  $p$  is inert or totally ramified, then there exist  $m, h \in \mathbf{Z}$ , with  $h \geq 0$ , such that*

$$\gamma = \frac{\alpha - m}{p^h} \in \mathcal{O} \quad (5.3)$$

*but no integers  $h', m'$  with  $h' > h$  such that*

$$\gamma' = \frac{\alpha - m'}{p^{h'}} \in \mathcal{O}$$

(ii). *If  $p$  is inert in  $L$  then  $m_\gamma(x)$  is irreducible over  $\mathbf{F}_p$ .*

(iii). *If  $p$  ramifies in  $L$  then  $m_\gamma(x) \equiv (x - c)^q \pmod{p}$ , with  $q \nmid r = \nu_p(N_{L/\mathbf{Q}}(\gamma - c))$ . Let  $s \in \mathbf{N}$  and  $l \in \mathbf{Z}$  be such that  $rs + ql = 1$ . Then  $\pi = (\gamma - c)^s p^l$  satisfies an Eisenstein polynomial at  $p$ .*

*Proof.* By assumption  $\alpha \in \mathcal{O} \setminus \mathbf{Z}$ . Assertion (i) comes from the fact that when  $p$  does not split completely  $\alpha \notin \mathbf{Q}_p$  by Lemma 5.3 and so we must have  $\mathcal{O} \cap \mathbf{Z}_p = \mathbf{Z}$ . Note that  $L = \mathbf{Q}[\gamma]$ .

To prove (ii) assume that  $p$  is inert and  $m_\gamma(x)$  is not irreducible over  $\mathbf{F}_p$ . Then, by Corollary 5.1 we would have

$$m_\gamma(x) \equiv (x - c)^q \pmod{p}$$

for some  $c \in \mathbf{Z}$ . Hence  $\gamma - c \in p\mathcal{O}$  and so

$$\frac{\alpha - m - cp^h}{p^{h+1}} \in \mathcal{O}$$

contradicting the choice of  $h$ .

To prove (iii) assume that  $p$  ramifies, and so  $p\mathcal{O} = \mathcal{P}^q$ , where  $\mathcal{P}$  denotes the unique prime ideal of  $\mathcal{O}$  above  $p$ . Since  $m_\gamma(x)$  cannot be irreducible over  $\mathbf{F}_p$  by Lemma 5.6, we must have

$$m_\gamma(x) \equiv (x - c)^q \pmod{p}$$

for some  $c \in \mathbf{Z}$ . Then

$$(\gamma - c)^q \in p\mathcal{O}$$

and so  $\gamma - c \in \mathcal{P}$ . We claim that

$$\gamma - c \notin \mathcal{P}^q$$

For otherwise, reasoning as above we would have

$$\frac{\alpha - m - cp^h}{p^{h+1}} \in \mathcal{O}$$

contradicting the choice of  $h$ . Therefore

$$\gamma - c \in \mathcal{P}^r \setminus \mathcal{P}^{r+1}$$

with  $0 < r < q$ . Let  $s \in \mathbf{N}$  and  $l \in \mathbf{Z}$  be such that  $rs + ql = 1$ . It can be easily seen that

$$\pi = (\gamma - c)^s p^l \in \mathcal{P} \setminus \mathcal{P}^2$$

and therefore by Lemma 5.7 the polynomial  $m_\pi(x)$  must be Eisenstein at  $p$ .  $\square$

The next lemma shows that the integer  $h$  given by (5.3) is 'small'.

**Lemma 5.8** *Let us assume the notation of Theorem 5.1.*

*If  $p$  is inert, then*

$$h = \frac{\nu_p(d_L(\alpha))}{q(q-1)}$$

*If  $p$  is totally ramified then*

$$h \leq \frac{\nu_p(d_L(\alpha))}{q(q-1)}$$

*Proof.* Let us assume first that  $p$  is inert. Let  $S$  denote the multiplicative set  $\mathbf{Z} \setminus p\mathbf{Z}$ , and let  $T$  denote the multiplicative set  $\mathcal{O} \setminus \mathcal{P}$ .

Now, by Theorem 2.2 the integral closure of  $S^{-1}\mathbf{Z}$  in  $L$  is equal to  $S^{-1}\mathcal{O}$ .

However, by Theorem 2.3 the integral closure of  $S^{-1}\mathbf{Z}$  in  $L$  is the intersection of all the valuation rings of  $L$  containing  $S^{-1}\mathbf{Z}$ . Since  $\mathcal{P}$  is the unique prime ideal of  $\mathcal{O}$  lying above  $p$ , it follows that the integral closure of  $S^{-1}\mathbf{Z}$  in  $L$  is equal to  $T^{-1}\mathcal{O}$ , and so it is a local ring.

Since  $\gamma$  is a primitive element for  $\mathcal{O}/\mathcal{P}$  over  $\mathbf{Z}/p\mathbf{Z}$  and  $T^{-1}\mathcal{O}$  is a local ring, by Theorem 2.4 it follows that the set  $\{1, \gamma, \dots, \gamma^{q-1}\}$  is an integral basis for  $T^{-1}\mathcal{O}$  over  $S^{-1}\mathbf{Z}$ . Since  $p$  is inert this implies that  $\nu_p(d_L(\gamma)) = 0$ .

Now in general, when  $\delta \in \mathcal{O}$  and  $b \in \mathbf{Z}$ , we have

$$d_L(p\delta) = p^{q(q-1)}d_L(\delta)$$

and

$$d_L(p\delta + b) = d_L(p\delta)$$

and therefore

$$d_L(\alpha) = p^{q(q-1)h}d_L(\gamma)$$

that is

$$\nu_p(d_L(\alpha)) = q(q-1)h$$

This proves the first part of the lemma.

Assume next that  $p$  ramifies. We have seen that in this case

$$m_\gamma(x) \equiv (x - c)^q \pmod{p}$$

for some  $c \in \mathbf{Z}$ , with

$$\gamma - c \in \mathcal{P}^r \setminus \mathcal{P}^{r+1} \quad (0 < r < q)$$

Clearly

$$\nu_p(d_L(\gamma - c)) \geq \nu_p(d_L(\gamma))$$



Now, by Theorem 4.2 when  $q$  is odd we have

$$\nu_p(d_L) = \begin{cases} q-1 & \text{if } p \neq q \\ 0 \text{ or } 2(q-1) & \text{if } p = q \end{cases}$$

Moreover, it can be shown (see [23, Proposition 5.1.1, p. 218]) that when  $q = 2$  we have

$$\nu_p(d_L) = \begin{cases} 1 & \text{if } p \neq 2 \\ 2 \text{ or } 3 & \text{if } p = 2 \end{cases}$$

The same argument as above shows that

$$\nu_p(d_L(\alpha)) = q(q-1)h + \nu_p(d_L(\gamma - c))$$

and so

$$\nu_p(d_L(\alpha)) \geq q(q-1)h + \nu_p(d_L)$$

It follows that

$$h \leq \frac{\nu_p(d_L(\alpha)) - \nu_p(d_L)}{q(q-1)}$$

and hence

$$h \leq \frac{\nu_p(d_L(\alpha))}{q(q-1)}$$

□

**Remark.** Assuming that  $p$  is inert, we claim that if

$$u \in \mathbf{Z} \text{ and } i < h = \frac{\nu_p(d_L(\alpha))}{q(q-1)}$$

then the minimal polynomial of  $(\alpha - u)/p^i$  cannot be irreducible over  $\mathbf{F}_p$ . In fact, if  $\omega = (\alpha - u)/p^i$ , with  $i < h$  and  $u \in \mathbf{Z}$ , then the argument used in the proof of Lemma 5.8 shows that  $\nu_p(d_L(\omega)) > 0$ . But then the set  $\{1, \omega, \dots, \omega^{q-1}\}$  cannot be an integral basis for  $T^{-1}\mathcal{O}$  over  $S^{-1}\mathbf{Z}$ , hence  $\omega$  cannot be a primitive element for  $\mathcal{O}/\mathcal{P}$  over  $\mathbf{Z}/p\mathbf{Z}$ , and so  $m_\omega(x)$  must be a  $q^{th}$  power over  $\mathbf{F}_p$ .

The computation of the algebraic integer  $\gamma$  that satisfies (5.3) is carried out by  $p$ -adic lifting. For this purpose we compute iteratively a sequence of algebraic numbers  $\gamma_1, \gamma_2, \dots$  as follows: if

$$m_{\gamma_{i-1}}(x) \equiv (x - c_i)^q \pmod{p}$$

where  $\gamma_0 = \alpha$ , then we let

$$\gamma_i = \frac{\gamma_{i-1} - c_i}{p}$$

From what has been said in this section it is clear that the process can stop as soon as either one of the following conditions is satisfied:

- (i).  $i = \nu_p(d_L(\alpha))/(q(q-1))$ . By applying Theorem 5.1 to  $\gamma = \gamma_i$  we are able to verify if  $p$  ramifies or it is inert in  $L$ . If neither the cases are true then  $p$  splits completely in  $L$ .
- (ii).  $\gamma_i \notin \mathcal{O}$  for  $i < \nu_p(d_L(\alpha))/(q(q-1))$ . The note above shows that  $p$  cannot be inert, and so we have to check if  $p$  is ramified, by applying Theorem 5.1 to  $\gamma = \gamma_{i-1}$ . If  $p$  is not ramified then it splits completely.
- (iii). The minimal polynomial of  $\gamma_i$ , with  $i \leq \nu_p(d_L(\alpha))/(q(q-1))$ , has at least two distinct roots in  $\mathbf{F}_p$ . In this case  $p$  splits completely in  $L$ .

The algorithm DECOMPOSE, shown in Figure 5.1, implements the ideas described above. It takes as input  $p$  and  $\alpha$ , and returns *INERT* if  $p$  is inert in  $L = \mathbf{Q}[\alpha]$ , *SPLITS* if it splits, and *RAMIFIES* plus an Eisenstein element  $\pi$  if  $p$  ramifies.

**Remark.** When  $p \nmid d_L(\alpha)$ , then  $m_\alpha(x)$  is either irreducible over  $\mathbf{F}_p$  or it has distinct roots in  $\mathbf{F}_p$ , depending whether  $p$  is inert or it splits in  $L$ . In order to check whether  $m_\alpha(x)$  has roots in  $\mathbf{F}_p$  it is enough to compute  $l(x) = \gcd(x^p - x, m_\alpha(x))$ , over  $\mathbf{F}_p$ ; if  $\deg l(x) \neq 0$  then  $p$  is inert otherwise it splits in  $L$ .

### 5.2.1 Implementation and complexity issues

In this section we will show that the algorithm DECOMPOSE runs in time polynomial in the size of the input.

Let  $\beta$  be as in Figure 5.1. Since  $\beta$  is always an algebraic integer during the execution of the program DECOMPOSE, we can write  $\beta$  as

$$\beta = \frac{c_{q-1}\alpha^{q-1} + \dots + c_1\alpha + c_0}{d_L(\alpha)} \quad (5.4)$$

with  $c_i \in \mathbb{Z}$  ( $i = 0, \dots, q-1$ ).

The main problem in the complexity analysis comes from the fact that it is quite hard to estimate accurately the size of the coefficients  $c_i$  during the execution of the program. Hence, we take another approach, namely we estimate the size of  $m_\beta(x)$  from time to time.

It can be shown that the size of the coefficients  $c_i$  is bounded by a function of the sizes of  $m_\beta(x)$  and of  $m_\alpha(x)$  (see [92, Lemma 8.3]). However, we will never need to know  $\beta$  in the form (5.4), since for the application that we have in mind (i.e. in the NORM algorithm) it is enough to know  $m_\beta(x)$ . In fact, we have seen that the algorithm NORM needs to know only the ramification type of  $p$ , and whenever  $p$  ramifies it needs  $N_{L/\mathbb{Q}}(\pi)$ , for some Eisenstein element  $\pi$  at  $p$ .

Moreover it is easy to see that, whenever  $\pi$  is needed we can easily recover it from  $\alpha$ , from the sequence  $c_1, c_2, \dots, c_k$  (where  $c_i$  stands for the element  $c$  constructed at the  $i^{\text{th}}$  iteration, in the algorithm DECOMPOSE), and from the values of  $s$  and  $l$  found in the algorithm CONSTRUCT\_EISENSTEIN, using the simple formula:

$$\pi = \left( \frac{\alpha - c_1 p^k - c_2 p^{k-2} - \dots - c_k}{p^k} \right)^s p^l \quad (5.5)$$

**An upper bound for the number of iterations.** We have shown in Lemma 5.8 that the internal loop of the algorithm DECOMPOSE is executed at most  $h = \nu_p(d_L(\alpha))/(q(q-1))$  times. The greatest value of  $h$  is attained when  $p = 2$ . In this case, using Mahler's bound (4.7) we get

$$\nu_2(d_L(\alpha)) < q \log q + (2q-2) \log(1 + |a_{q-1}| + \dots + |a_0|)$$

Let  $H = \max(|a_r|)_{r=0, \dots, q}$  be again the height of  $m_\alpha(x)$ , and take  $\log H$ , as a measure of our input size. This measure will prove in the sequel more useful than the usual measure  $\text{size}(m_\alpha(x)) = \sum_{r=0}^q \log(|a_r| + 2)$ . Then, from the formula above we obtain

$$\begin{aligned} \nu_2(d_L(\alpha)) &< q \log q + (2q-2) \log(qH) \\ &= q \log q + 2(q-1)(\log q + \log H) \end{aligned}$$

This shows that the number of iterations is bounded above by

$$h = \frac{\log q}{q-1} + \frac{2(\log q + \log H)}{q}$$

that is

$$h = \mathcal{O}\left(\frac{\log q + \log H}{q}\right)$$

**The cost of computing  $\gcd(x^p - x, m_\alpha(x))$ .** The argument following Lemma 5.6 shows that it is possible to check if  $m_\alpha(x)$  has no roots, at least two distinct roots or just one root in  $\mathbf{F}_p$  – and in the last case compute the unique root, which has multiplicity  $q$  – by computing  $\gcd(x^p - x, m_\alpha(x))$ .

Let us show that this computation can be performed in time polynomial in the size of  $p$  and in the degree  $q$  of  $m_\alpha(x)$ .

In fact, we can compute  $x^p \bmod m_\alpha(x)$  using  $\mathcal{O}(\log p)$  multiplications modulo  $m_\alpha(x)$ . Each multiplication costs, using the standard algorithms,  $\mathcal{O}(q^2)$  operations in  $\mathbf{F}_p$ , for a total of  $\mathcal{O}(q^2 \log p)$  operations in  $\mathbf{F}_p$ .

Next, the computation of  $\gcd((x^p \bmod m_\alpha(x)) - x, m_\alpha(x))$  can be performed in  $\mathcal{O}(q^2)$  operations in  $\mathbf{F}_p$  (see [49, p. 427]) using Euclid's algorithm.

It is clear that we can consider each operation in  $\mathbf{F}_p$  as an operation on  $p$ -bit integers, and so we can assume an upper bound of  $\mathcal{O}((\log p)^2)$  bit operations per operation in  $\mathbf{F}_p$ . This gives an overall complexity of  $\mathcal{O}(q^2(\log p)^3)$ .

**An upper bound for the size of  $m_\beta(x)$ .** Next let us show that, during the execution of the main loop of the algorithm DECOMPOSE, shown in Figure 5.1, the size of the minimal polynomial of the algebraic integer  $\beta$  is bounded by a polynomial in the size of  $m_\alpha(x)$ .

By looking at Figure 5.1 it can be seen that at the  $k^{\text{th}}$  iteration of the internal loop, the algebraic integer  $\beta$  can be expressed as

$$\beta = \frac{\alpha - m_k}{p^k}$$

where  $m_k$  is an integer such that  $0 \leq m_k < p^k$ , and  $m_h = m$  in the notation of Lemma 5.1.

If  $\sigma$  denotes a generator of  $\text{Gal}(L/\mathbf{Q})$ , we can write

$$\begin{aligned}
 m_\beta(x) &= \prod_{i=1}^q (x - \sigma^i(\frac{\alpha - m_k}{p^k})) \\
 &= \prod_{i=1}^q (x - p^{-k} \sigma^i(\alpha - m_k)) \\
 &= \prod_{i=1}^q p^{-k} (p^k x - \sigma^i(\alpha - m_k)) \\
 &= p^{-kq} \prod_{i=1}^q (p^k x - \sigma^i(\alpha) + m_k) \\
 &= p^{-kq} m_\alpha(p^k x + m_k)
 \end{aligned}$$

Next, we expand symbolically  $m_\alpha(p^k x + m_k)$  around  $m_k$  using Taylor's formula, obtaining

$$m_\alpha(p^k x + m_k) = \sum_{i=0}^q \frac{m_\alpha^{(i)}(m_k) \cdot (p^k x)^i}{i!}$$

where  $m_\alpha^{(i)}(m_k)$  denotes the  $i^{\text{th}}$  derivative of  $m_\alpha(x)$  evaluated at  $m_k$ . It follows that the coefficient  $b_i$  of  $x^i$  in  $m_\beta(x)$  is given by

$$b_i = \frac{m_\alpha^{(i)}(m_k) \cdot p^{k(i-q)}}{i!}$$

We want to show that  $b_i$  is not 'too large'. Since  $b_i \in \mathbf{Z}$ , it is enough to show that  $m_\alpha^{(i)}(m_k)$  is not too large. Let

$$m_\alpha(x) = a_q x^q + a_{q-1} x^{q-1} + \dots + a_1 x + a_0$$

with  $a_i \in \mathbf{Z}$  ( $i = 0, \dots, q$ ) and  $a_q = 1$ . Then

$$\begin{aligned}
 m'_\alpha(x) &= q a_q x^{q-1} + (q-1) a_{q-1} x^{q-2} + \dots + 2 a_2 x + a_1 \\
 m_\alpha^{(2)}(x) &= q(q-1) a_q x^{q-2} + (q-1)(q-2) a_{q-1} x^{q-3} + \dots + 2 a_2
 \end{aligned}$$

and more generally

$$m_\alpha^{(i)}(x) = \sum_{r=i}^q \left( \prod_{j=r+1-i}^r j \right) a_r x^{r-i}$$

Clearly

$$\begin{aligned}
 |m_{\alpha}^{(i)}(m_k)| &= \left| \sum_{r=1}^q \left( \prod_{j=r+1-i}^r j \right) a_r m_k^{r-i} \right| \\
 &\leq \sum_{r=1}^q \left( \prod_{j=r+1-i}^r j \right) |a_r| |m_k|^{r-i} \\
 &< \frac{q!}{(q-i)!} \sum_{r=1}^q |a_r| |m_k|^{r-i} \\
 &\leq \frac{q!}{(q-i)!} H \sum_{r=1}^q |m_k|^{r-i} \\
 &< \frac{q!}{(q-i)!} H 2 |m_k|^{q-i}
 \end{aligned}$$

and hence

$$|b_i| < \frac{2q!}{i!(q-i)!} p^{k(i-q)} H |m_k|^{q-i}$$

Now,  $|m_k| < p^k$  by construction, and so we obtain

$$\begin{aligned}
 |b_i| &< \frac{2q!}{i!(q-i)!} p^{k(i-q)} H p^{k(q-i)} \\
 &= \frac{2q!}{i!(q-i)!} H
 \end{aligned}$$

Hence there is an *effective bound* for the size of the  $i^{\text{th}}$  coefficient of  $m_{\beta}(x)$  which is *independent of the iteration number*, namely

$$\text{size}(b_i) < \log\left(\frac{2q!}{i!(q-i)!}\right) + \log H \quad (5.6)$$

where  $b_i$  stands for the coefficient of  $x^i$  in  $m_{\beta}(x)$ .

**Computing the Taylor shift.** At each iteration in the procedure DECOMPOSE we need to compute the minimal polynomial of  $(\beta - c)/p$ , where  $c$  is an integer between 0 and  $p - 1$  included. In order to estimate the overall complexity of the algorithm, we need an upper bound for the time spent in the execution of this step. Let  $\delta = (\beta - c)/p$ . Applying Taylor's shift as before, we can write the coefficient of  $x$  in  $m_{\beta-c}(x)$  as

$$\frac{m_{\beta}^{(i)}(c)}{i!}$$

and hence the coefficient of  $x^i$  in  $m_\varepsilon(x)$  as

$$v_i = \frac{m_\beta^{(i)}(c)}{i!} \cdot \frac{1}{p^{q-i}}$$

The problem of computing efficiently the coefficients of the Taylor's shift has been investigated by M. Shaw and J.F. Traub [87]. Let  $p(x)$  be a polynomial of degree  $n$ , and let  $c_0$  be a constant. An algorithm to compute  $p(x + x_0)$  which makes use of Horner's rule requires  $n(n - 1)/2$  multiplications and the same number of additions. Shaw and Traub give in [87] an algorithm which requires only  $2n - 1$  multiplications and  $n - 1$  divisions.

We have proved above that the height of  $m_\beta(x)$  is bounded above by  $2q!H$ , and that the same bound holds for the height of  $m_\varepsilon(x)$  as well. Hence, the height of  $m_{\beta-c}(x)$  is bounded above by  $p^q 2q!H$ .

Let us make the following *simplifying assumption*: during the execution of the algorithm of Shaw and Traub each multiplication and/or division is carried out on integers bounded in absolute value by  $p^q 2q! H$ . Since  $\log(p^q 2q! H) < q \log p + q \log q + \log H$ . It is clear that the algorithm of Shaw and Traub requires then

$$\mathcal{O}(q(q \log p + q \log q + \log H)^2)$$

elementary operations for computing  $m_{\beta-c}(x)$ .

In order to obtain  $m_\varepsilon(x)$  we need to divide the coefficients of  $m_{\beta-c}(x)$  by a suitable power of  $p$  (namely, divide the coefficient of  $x^i$  by  $p^{q-i}$ , for  $i = 0, \dots, q-1$ ). However, the cost of this operation is dominated by the cost of the Taylor's shift.

**The cost of computing  $m_\pi(x)$ .** It remains to bound the size of  $m_\pi(x)$ , the minimal polynomial of  $\pi = (\beta)^s p^l$ , constructed in the procedure CONSTRUCT\_EISENSTEIN.

Equation (5.6) above shows that when the procedure CONSTRUCT\_EISENSTEIN is called the size of the norm of  $\beta$ , which is simply the coefficient  $b_0$  of  $m_\beta(x)$ , is quite small, namely:

$$\text{size}(N_{L/\mathbb{Q}}(\beta)) < \log(2) + \log H$$

In particular, the value of  $r = \nu_p(N_{L/Q}(\beta))$  is bounded above by  $1 + \log H$  (this bound is attained when  $p = 2$ ).

Now, elementary number theory tells us that the integer  $s$  such that  $rs + ql = 1$  can be always taken between 1 and  $q - 1$  included. This forces the integer  $l$ , for which the relation  $rs + ql = 1$  holds, to be negative. Again, elementary number theory tells us that  $l$  can be always taken between 0 and  $-r + 1$  included, that is

$$-\log H = -r + 1 < l \leq 0$$

In particular, from the consideration of the extreme case ( $s = q - 1$ ) we obtain the following lemma, which shows that there is a bound on the size of  $N_{L/Q}(\pi)$  which is approximately equal to the size of  $m_\alpha(x)$ .

**Lemma 5.9** *The size of the norm of the Eisenstein element  $\pi$  found by the algorithm DECOMPOSE is bounded above by  $(q - 1)(1 + \log H)$ , where  $H$  denotes the height of  $m_\alpha(x)$ .*

Since on entering the procedure CONSTRUCT\_EISENSTEIN the minimal polynomial of  $\beta$  is known, we can compute the minimal polynomial of  $\beta^s$  as follows [61, Theorem 7, p. 182]:

$$m_{\beta^s}(y) = \text{Res}_x(x^s - y, m_\beta(x))$$

where  $\text{Res}$  denotes the resultant of the two polynomials.

Given two bivariate polynomials over  $\mathbb{Z}$ , say  $f(x, y)$  and  $g(x, y)$ , with

$$\deg_x f(x, y), \deg_x g(x, y), \deg_y f(x, y), \deg_y g(x, y) \leq n$$

and whose coefficients size is bounded by  $B$ , it is possible to compute  $\text{Res}_x(f(x, y), g(x, y))$  in time  $\mathcal{O}(n^6 B^2)$  using the subresultant algorithm [61], or else in time  $\mathcal{O}(n^5 B + n^4 B^2)$  using the modular resultant algorithm developed by G.E. Collins [25]. Now, the argument above shows that the largest coefficient of  $m_\beta(x)$  in absolute value is bounded above by  $2 q! H$ , and hence by  $q^q H$ . Therefore we can take

$$B = q \log q + \log H$$



and so we can compute the minimal polynomial of  $\beta^q$  in time

$$\mathcal{O}(q^5(q \log q + \log H) + q^4(q \log q + \log H)^2) \quad (5.7)$$

Then, from

$$m_{\beta^q}(x) = x^q + b_{q-1}x^{q-1} + \dots + b_1x + b_0$$

we can obtain  $m_{\beta^{q^l}}(x)$  as follows

$$m_{\beta^{q^l}}(x) = x^q + (b_{q-1}p^l)x^{q-1} + \dots + (b_1p^{l(q-1)})x + (b_0p^{lq})$$

It is clear that the complexity of the resultant calculation dominates the complexity of the algorithm `CONSTRUCT_EISENSTEIN`, hence we can take (5.7) as an upper bound on the complexity of the algorithm `CONSTRUCT_EISENSTEIN` itself.

### 5.3 Computational examples

The algorithm `DECOMPOSE` described in this chapter and the algorithm `NORM` described in Chapter 4 have been coded in PARI. In this section we will show some examples of computations which have actually been performed. Before doing this, however, we will discuss the case in which there is only one ramified prime, which is less interesting from a computational point of view, but is capable of a very nice theoretical characterization.

#### 5.3.1 Discriminant of the form $p^{q-1}$ or $q^{2q-2}$

Let us assume that  $d_L = p^{q-1}$  with  $p \neq q$ , or  $d_L = q^{2q-2}$ . In this case it is possible to give a nice characterization of the norm elements in  $\mathbb{Q}^*$ . We begin by proving the following

**Lemma 5.10** *Let  $L$  be a cyclic field of prime degree  $q$ . Assume that there is only one rational prime  $p$  which ramifies in  $L$  (possibly  $p = q$ ). Then*

- (i).  $p$  is a norm from  $L$ ;

```

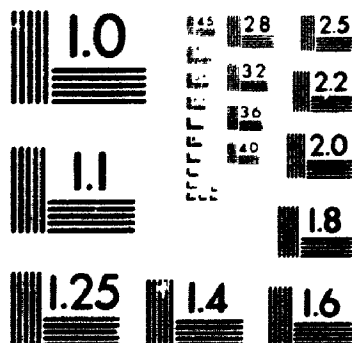
procedure DECOMPOSE( $p, \beta$ ):
  if  $p \nmid d_L(\beta)$ 
    then if  $m_\beta(x)$  has no roots in  $\mathbf{F}_p$ 
      then return INERT
    else return SPLITS
  endif
endif
  let  $h = \lfloor \nu_p(d_L(\beta)) / (q(q-1)) \rfloor$ ,
  for  $i = 1$  to  $h$  do
    if  $m_\beta(x)$  has exactly one root  $c$  in  $\mathbf{F}_p$ 
      then let  $\beta = (\beta - c)/p$ ;
      if  $m_\beta(x) \notin \mathbf{Z}[x]$ 
        then let  $\beta = p\beta$ ;
      return CONSTRUCT_EISENSTEIN( $p, \beta$ )
    endif
  else return SPLITS
endif
endfor
if  $m_\beta(x)$  has exactly one root  $c$  in  $\mathbf{F}_p$ 
  then let  $\beta = \beta - c$ 
else if  $m_\beta(x)$  has no roots in  $\mathbf{F}_p$ 
  then return INERT
else return SPLITS
endif
endif
return CONSTRUCT_EISENSTEIN( $p, \beta$ )

```

Figure 5.1: The algorithm DECOMPOSE.

# 2 OF 2

PM-1 3½"x4" PHOTOGRAPHIC MICROCOPY TARGET  
NBS 1010a ANSI/ISO #2 EQUIVALENT



PRECISION<sup>SM</sup> RESOLUTION TARGETS

(ii). If  $r$  is a rational prime which splits in  $L$ , then  $r$  is a norm from  $L$ ;

(iii). If  $r$  is a rational prime which is inert in  $L$ , then  $r$  is not a norm from  $L$ .

In particular, if  $p \neq q$  then a rational prime  $r \neq p$  splits in  $L$  if and only if  $r^{(p-1)/q} \equiv 1 \pmod{p}$ .

*Proof.* Let  $p$  be the unique rational prime which ramifies in  $L$ . By Theorem 2.9  $p$  is a norm at all the unramified primes, and hence by Theorem 2.12  $p$  must be a norm at itself as well. Therefore, by the Hasse Norm Theorem  $p$  is a global norm.

Let  $r$  be a rational prime that splits in  $L$ . Again, by Theorem 2.9  $r$  is a norm at all the primes that split in  $L$ , and a norm at all the primes which are inert in  $L$ . Hence by Theorem 2.12  $r$  must be a norm at  $p$  as well, and therefore by the Hasse Norm Theorem  $r$  must be a global norm.

Next, let  $r$  be a rational prime which is inert in  $L$ . Then by Theorem 2.9  $r$  can not be a norm at  $r$ , and hence  $r$  can not be a global norm.

Finally, assume that  $p \neq q$ . If a prime  $r$  splits in  $L$  then we have just proved that  $r$  is a norm from  $L$ , and hence by Theorem 4.1 and Lemma 4.1 we must have  $r^{(p-1)/q} \equiv 1 \pmod{p}$ . If a prime  $r$  is inert in  $L$ , then we have just proved that  $r$  is not a norm at  $r$ , although by Theorem 2.9  $r$  is a norm at all primes that split and at all the other primes that are inert in  $L$ . Hence, by Theorem 2.12  $r$  can not be a norm at  $p$  and therefore  $r^{(p-1)/q} \not\equiv 1 \pmod{p}$ .  $\square$

The previous lemma gives us a fast criterion to recognize if a rational number  $a$  is a norm from  $L$  when there is only one ramified prime  $p \neq q$ , namely

**Corollary 5.2** *Let  $L$  be a cyclic field of prime degree  $q$  and discriminant  $p^{q-1}$ , with  $p \neq q$  prime, and let  $a$  be a rational number. Write  $a$  as  $p^s \prod p_j^{e_j}$ , where the elements  $p_j$  are distinct primes and  $s, e_j \in \mathbf{Z}$ . Then  $a$  is a norm from  $L$  if and only if  $q \mid e_j$  for all the  $j$  such that  $p_j^{(p-1)/q} \not\equiv 1 \pmod{p}$ .*

Note that Lemma 5.10 does not hold when there is more than one ramified prime. Consider for example the cyclic field  $L$  of discriminant  $13^2 19^2$  generated by the polynomial  $x^3 - x^2 - 82x + 311$ . The prime 43 splits in  $L$ , but  $43^{(13-1)/3} \equiv 9 \pmod{13}$ , and also  $43^{(19-1)/3} \equiv 7 \pmod{19}$ .

### 5.3.2 Some computed examples

To test the performance of our algorithms, we applied the algorithm NORM to each positive integer  $1, 2, 3, \dots$  in turn until 100 norms were found, and we recorded the running time.

In Table 5.1 we consider the polynomial  $x^5 + x^4 - 4x^3 - 3x^2 + 3x + 1$  whose discriminant, which turns out to be the field discriminant as well, is  $11^4$ . The first 100 positive integers which are norms from  $L$  were computed in 2 minutes and 4,710 ms.

For a comparison, consider the polynomial  $x^5 - 6663x^4 + 608627x^3 - 13160932x^2 + 2524039x + 283999$  which generates the same field as the polynomial  $x^5 + x^4 - 4x^3 - 3x^2 + 3x + 1$ . The discriminant of this polynomial is  $11^4 23^{12} 43^2 331^2 461^2 505031^2$ . All the primes dividing the discriminant, except 11, split in  $L$ . Using this polynomial, we computed the first 100 positive integers which are norms from  $L$  in 20 minutes and 18,540 ms.

1	11	23	32	43	67	89	109	121	131
197	199	241	243	253	263	307	331	352	353
373	397	419	439	461	463	473	529	571	593
617	659	661	683	727	736	737	769	857	859
881	947	967	979	989	991	1013	1024	1033	1123
1187	1199	1231	1277	1297	1319	1321	1331	1376	1409
1429	1441	1451	1453	1541	1583	1607	1627	1693	1759
1783	1847	1849	1871	1913	1979	2003	2047	2069	2089
2111	2113	2144	2167	2179	2189	2221	2243	2267	2287
2309	2311	2333	2377	2399	2441	2507	2531	2551	2617

**Table 5.1:** First 100 positive integers which are norms from  $L = \mathbb{Q}[\alpha]$ , where  $\alpha$  is a root of  $x^5 + x^4 - 4x^3 - 3x^2 + 3x + 1$

For an example of a cyclic field with more than one ramified primes consider the polynomial  $x^3 - x^2 - 82x + 311$ . Its discriminant, which turns out to be the

field discriminant as well, is  $13^2 19^2$ . Using this polynomial, we computed the first 100 positive integers which are norms from  $L$  in 3 minutes and 20,390 milliseconds. These integers are shown in Table 5.2.

For a comparison, we performed the same test using the polynomial  $x^3 - 26566x^2 + 105638441x - 103601453623$ , which generates the same field. Note that the discriminant of this polynomial is  $13^2 19^2 229^2 1747^2 5851^2$ , and all the primes except 13 and 19 split in  $L$ . This time the test took 6 minutes and 40,490 milliseconds.

1	8	27	31	64	83	103	125	151	216
221	229	239	247	248	311	343	391	437	463
467	493	512	521	551	559	571	577	619	664
677	729	733	767	824	837	863	911	923	961
989	1000	1019	1091	1139	1171	1208	1217	1223	1247
1261	1273	1331	1357	1399	1451	1481	1483	1513	1559
1607	1633	1691	1711	1717	1721	1728	1741	1747	1768
1832	1873	1912	1919	1937	1949	1976	1984	2003	2053
2059	2159	2197	2231	2241	2249	2287	2393	2413	2488
2573	2621	2699	2729	2744	2781	2813	2839	2861	2881

**Table 5.2:** First 100 positive integers which are norms from  $L = \mathbb{Q}[\alpha]$ , where  $\alpha$  is a root of  $x^3 - x^2 - 82x + 311$

```
procedure CONSTRUCT_EISENSTEIN( $p, \beta$ ):  
  let  $\tau = \nu_p(N_{L/\mathbb{Q}}(\beta))$ ;  
  if  $q \mid \tau$   
    then return SPLITS  
  endif  
  find  $s \in \mathbb{N}$  and  $l \in \mathbb{Z}$  such that  $\tau s + ql = 1$ ,  
  with  $1 \leq s \leq q - 1$ ;  
  let  $\pi = (\beta)^s p^l$ ;  
  if  $m_\pi(x)$  is Eisenstein at  $p$   
    then return RAMIFIES and  $\pi$   
    else return SPLITS  
endif
```

Figure 5.2: Auxiliary procedure used by DECOMPOSE.

## Chapter 6

# Norm equations over cyclic number fields of squarefree degree

Let  $E = \mathbb{Q}[\nu]$  be a cyclic number field  $E$  of squarefree degree  $n$  over  $\mathbb{Q}$ , and let  $a$  be a nonzero rational number. In this chapter we give an algorithm to decide if the equation

$$N_{E/\mathbb{Q}}(\lambda) = a \tag{6.1}$$

is solvable in  $E$ , by generalizing the algorithm NORM described in Chapter 4. Theorem 2.8, stated in Chapter 2, will play a major role in this chapter, for it will enable us to reduce the problem over  $E$  to the same problem over all the cyclic subfields of  $E$  of prime degree over  $\mathbb{Q}$ .

We will show that the generalized algorithm runs again in time polynomial in the size of the input, assuming that we are allowed to call an oracle to obtain a complete factorization of  $a$  and a complete factorization of the discriminant  $d_E(\nu)$  of  $\nu$ .

## 6.1 Reduction to the prime degree case

Let  $\mathcal{P}$  be a prime of  $E$ . The next lemma tells us how to obtain all the minimal subfields of  $E_{\mathcal{P}}$ , the  $\mathcal{P}$ -adic completion of  $E$ .



**Lemma 6.1** *Let  $E$  be a cyclic number field of squarefree degree  $n$ . Let  $p$  be a rational prime, and  $\mathcal{P}$  be a prime lying above  $p$  in  $E$ . Let  $E_{\mathcal{P}}$  be the completion of  $E$  with respect to  $\nu_{\mathcal{P}}$ . Let  $\hat{M}$  be a minimal subfield of  $E_{\mathcal{P}}$  over  $\mathbb{Q}_p$ . Then*

- (i). *The degree of  $\hat{M}$  over  $\mathbb{Q}_p$  is a prime number  $q$ ;*
- (ii).  *$\hat{M}$  is the composite in  $E_{\mathcal{P}}$  of  $\mathbb{Q}_p$  and  $M$ , where  $M$  is the unique minimal subfield of  $E$  over  $\mathbb{Q}$  of the same degree  $q$ .*

*Proof.* By Lemma 2.1 the extension  $E_{\mathcal{P}}/\mathbb{Q}_p$  is cyclic of degree  $m$ , with  $m \mid n$ . Therefore if  $\hat{M}$  is a minimal subfield of  $E_{\mathcal{P}}$  over  $\mathbb{Q}_p$ , its degree must be a prime number  $q$ , with  $q \mid n$ . We show next that  $\hat{M} = M\mathbb{Q}_p$ , where  $M$  is the unique minimal subfield of  $E$  over  $\mathbb{Q}$  of degree  $q$ . Suppose that the assertion were false. By the primality of  $q$  this would be possible if and only if  $M\mathbb{Q}_p = \mathbb{Q}_p$ . Since  $[E : \mathbb{Q}]$  is squarefree, this would imply that  $q \mid [E_{\mathcal{P}} : \mathbb{Q}_p]$  but  $q \nmid [E : M]$ , contradicting the fact that  $[E_{\mathcal{P}} : M\mathbb{Q}_p]$  must divide  $[E : M]$ .  $\square$

In the following lemma we characterize the global norms in terms of the local norms.

**Lemma 6.2** *Let  $E$  be a cyclic number field of squarefree degree  $n$ , and  $a \in \mathbb{Q}^*$ . Then  $a \in N_{E/\mathbb{Q}}(E^*)$  if and only if*

- (i). *if  $E$  is totally complex then  $a > 0$ ;*
- (ii). *for each minimal subfield  $M$  of  $E$  and for each finite prime  $\mathcal{D}$  of  $M$  lying above  $p$  we have  $a \in N_{M_{\mathcal{D}}/\mathbb{Q}_p}(M_{\mathcal{D}}^*)$ .*

*Proof.* For a subfield  $K$  of  $E$  and a divisor  $\mathcal{P}$  of  $E$  let us denote the restriction of  $\mathcal{P}$  to  $K$  by  $\mathcal{P} \cap K$ . By Theorem 2.11,  $a \in N_{E/\mathbb{Q}}(E^*)$  if and only if  $a \in N_{E_{\mathcal{P}}/\mathbb{Q}_p}(E_{\mathcal{P}}^*)$  for all the prime divisors  $\mathcal{P}$  of  $E$ .

Let us consider the infinite primes first. If  $\mathcal{P}$  is an infinite prime of  $E$ , then  $\mathcal{P} \cap \mathbb{Q} = \infty$ , the unique infinite prime of  $\mathbb{Q}$ , and  $\mathbb{Q}_{\infty} = \mathbb{R}$ . Then, either  $E_{\mathcal{P}} = \mathbb{R}$ , and because  $E$  is Galois this is equivalent to saying that  $E$  is totally real, or  $E_{\mathcal{P}} = \mathbb{C}$ ,

and because  $E$  is Galois this is equivalent to saying that  $E$  is totally complex (see Section 4.4). We have seen that in the first case

$$N_{E_{\mathcal{P}}/\mathbf{Q}_{\infty}}(E_{\mathcal{P}}^*) = N_{\mathbf{R}/\mathbf{R}}(\mathbf{R}) = \mathbf{R}$$

while in the second case

$$N_{E_{\mathcal{P}}/\mathbf{Q}_{\infty}}(E_{\mathcal{P}}^*) = N_{\mathbf{C}/\mathbf{R}}(\mathbf{C}) = \mathbf{R}^+$$

Let us consider next the finite primes. By Theorem 2.8, if we fix a finite prime  $\mathcal{P}$  of  $E$ , then  $a \in N_{E_{\mathcal{P}}/\mathbf{Q}_p}(E_{\mathcal{P}}^*)$  if and only if  $a \in N_{\hat{M}/\mathbf{Q}_p}(\hat{M}^*)$  for all the minimal subfields  $\hat{M}$  of  $E_{\mathcal{P}}$ .

Therefore  $a \in N_{E/\mathbf{Q}}(E^*)$  if and only if (i) holds and for each prime  $\mathcal{P}$  of  $E$  we have  $a \in N_{\hat{M}/\mathbf{Q}_p}(\hat{M}^*)$  for all the minimal subfields  $\hat{M}$  of  $E_{\mathcal{P}}$ .

Note that, when  $M$  is a minimal subfield of  $E$  and  $\mathcal{P}$  is a finite prime of  $E$ , then the composite  $M \cdot \mathbf{Q}_p$  (in  $E_{\mathcal{P}}$ ) is either  $\mathbf{Q}_p$  or a proper minimal subfield of  $E_{\mathcal{P}}$  of prime degree  $q$ . Moreover, by Lemma 6.1 each minimal subfield  $\hat{M}$  of  $E_{\mathcal{P}}$  is obtained in this way, that is by composing  $\mathbf{Q}_p$  with a minimal subfield of  $E$  of the same degree  $q$  (the composition taking place in  $E_{\mathcal{P}}$ ).

Since  $\hat{M}$  is the completion of  $M$  with respect to the valuation determined by the finite prime  $\mathcal{P} \cap M$ , we can write  $M_{\mathcal{P} \cap M}$  instead of  $\hat{M}$ .

But then  $a \in N_{E/\mathbf{Q}}(E^*)$  if and only if (i) holds and for each minimal subfield  $M$  of  $E$  we have

$$a \in N_{M_{\mathcal{P} \cap M}/\mathbf{Q}_p}(M_{\mathcal{P} \cap M}^*)$$

for all the finite primes  $\mathcal{P}$  of  $E$ .

Next note that, for each finite prime  $\mathcal{P}$  of  $E$  there is exactly one prime of  $M$  below  $\mathcal{P}$ , which we denoted by  $\mathcal{P} \cap M$ , and conversely, for each finite prime  $\mathcal{D}$  of  $M$  there is (at least) one finite prime  $\mathcal{P}$  of  $E$  such that  $\mathcal{P} \cap M = \mathcal{D}$ .

But then  $a \in N_{E/\mathbf{Q}}(E^*)$  if and only if (i) holds and for each minimal subfield  $M$  of  $E$  we have  $a \in N_{M_{\mathcal{D}}/\mathbf{Q}_p}(M_{\mathcal{D}}^*)$  for all the finite primes  $\mathcal{D}$  of  $M$ . This proves the lemma.  $\square$

Since  $E/\mathbb{Q}$  is cyclic of squarefree degree, it follows that  $E$  is the composite of *all* its minimal subfields. Therefore  $E$  is real if and only if all its minimal subfields are real. In other words, if  $E$  is complex then it has at least one minimal subfield which is complex.

The following theorem is now an easy consequence of Lemma 6.2.

**Theorem 6.1** *Let  $E$  be a cyclic number field of squarefree degree  $n$ , and  $a \in \mathbb{Q}^*$ . Then  $a \in N_{E/\mathbb{Q}}(E^*)$  if and only if  $a \in N_{M/\mathbb{Q}}(M^*)$  for each minimal subfield  $M$  of  $E$ .*

### 6.1.1 Computation of the minimal subfields of $E$

In order to apply Theorem 6.1 we must be able to compute all the minimal subfields of  $E = \mathbb{Q}[\nu]$ .

We recall here that there are very general algorithms to compute the lattice of subfields of a general algebraic number field [29], but in our case we do not need the full power of these algorithms, since a very simple ad hoc method will turn out to be more than adequate.

For this purpose we need to know a generator  $\tau$  for the (cyclic) Galois group of  $E/\mathbb{Q}$ .

Let  $m_\nu(x)$  be the minimal polynomial of  $\nu$  over  $\mathbb{Q}$ . An algorithm due to Lenstra [57] allows one to factor a polynomial over an algebraic number field, in time polynomial in the size of the input. If we apply this algorithm to  $m_\nu(x)$  over the field  $E$  itself, then  $m_\nu(x)$  factors into linear factors, and any other root of  $m_\nu(x)$  will be expressed as a polynomial

$$g_i(\theta) \quad (i = 1, \dots, n)$$

in the symbolic root  $\theta$ , corresponding to the complex root  $\nu$ . We can now choose  $g_i$  such that

$$\nu \mapsto g_i(\nu)$$

determines an automorphism  $\tau$  generating  $\text{Gal}(E/\mathbb{Q})$ .

Once  $\tau$  is known we can compute the minimal subfields of  $E$ , since these are in one to one correspondence with the maximal subgroups of  $\text{Gal}(E/\mathbb{Q})$ .

For each prime  $q$  dividing  $n$ , let  $H_{d/q} = \langle \tau^q \rangle$  denote the unique maximal subgroup of  $\text{Gal}(E/\mathbb{Q})$  of order  $d/q$ , and let  $L_q$  denote the unique minimal subfield of  $E$  of degree  $q$  corresponding to it. To find  $L_q$ , compute the following polynomial, of degree  $n/q$ :

$$h_q(x) = (x - \tau^q(\nu))(x - \tau^{2q}(\nu)) \cdots (x - \tau^n(\nu)) \quad (6.2)$$

It is a standard fact from Galois theory (see [91, p. 169]) that the coefficients of  $h_q(x)$  lie in  $L_q$  and they generate  $L_q$  over  $\mathbb{Q}$ . From the minimality of  $L_q$  it follows that any coefficient of  $h_q(x)$  which does not lie in  $\mathbb{Q}$  is a primitive element for  $L_q$  over  $\mathbb{Q}$ .

### 6.1.2 The complete test

Using the results of the previous sections, we are now able to describe the main algorithm of this chapter. Let  $E$  be a cyclic number field of squarefree degree  $n$  over  $\mathbb{Q}$ . The algorithm NORMSQF, described in Figure 6.1, takes as input a nonzero rational number  $a$  and the minimal polynomial for an algebraic integer  $\nu$  which generates  $E$  over  $\mathbb{Q}$ , and returns *TRUE* if  $a$  belongs to the norm group of  $L/\mathbb{Q}$ , *FALSE* otherwise.

We will show next that the algorithm NORMSQF runs in time polynomial in the size of the input, assuming that we are allowed to call an oracle to factor  $a$ , and to factor the discriminant of the primitive element of each minimal subfield of  $E$ .

Clearly the procedure NORM is called at most  $\text{size}(n)$  times, since  $\lfloor \log n \rfloor$  is an upper bound for the number of prime divisors of  $n$ , and  $\text{size}(n)$  is equal to  $\lfloor \log n \rfloor + 1$ .

For each prime factor  $q$  of  $n$ , the coefficients of the polynomial  $h_q(x)$  are algebraic integers, and they are represented as polynomials in  $\nu$ .

In order to show that the entire test runs in time polynomial in the size of the input it is necessary to bound the size of  $m_\alpha(x)$ , where  $\alpha$  is any non rational coefficient of  $h_q(x)$ , for each prime factor  $q$  of  $n$ .

**Lemma 6.3** *Let  $h_q(x)$  and  $m_\nu(x)$  be as in (6.2). Then the size of  $h_q(x)$  is bounded by a polynomial in the size of  $m_\nu(x)$ .*

*Proof.* Note that  $h_q(x)$  is a factor of  $m_\nu(x)$ . Now, we can factor  $m_\nu(x)$  completely over  $\mathbb{Q}[\nu]$  in time polynomial in the size of  $m_\nu(x)$ , using Lenstra's algorithm [57] for factoring polynomials over arbitrary number fields. This implies that the size of each conjugate of  $\nu$  is bounded by a polynomial in the size of  $m_\nu(x)$ . Since  $m_\nu(x)$  is given in its dense representation, then  $n$  is bounded above by the size of  $m_\nu(x)$ . Therefore the size of the coefficients of  $h_q(x)$ , which are just the elementary symmetric functions in

$$\{\tau^q(\nu), \tau^{2q}(\nu), \dots, \tau^n(\nu)\}$$

is bounded by a polynomial in the size of  $m_\nu(x)$ .  $\square$

An intuitive argument to prove that the size of  $m_\alpha(x)$  is bounded by a polynomial in the size of  $m_\nu(x)$  runs as follows. By Lemma 6.3 the size of each coefficient  $\alpha$  of  $h_q(x)$  is bounded by a polynomial in the size of  $m_\nu(x)$ . Since  $m_\alpha(x)$  can be computed in time polynomial in the size of  $\alpha$ , using standard methods from linear algebra (see [23, Section 4.3, p. 160]), then necessarily the size of  $m_\alpha(x)$  must be bounded by a polynomial in the size of  $m_\nu(x)$ .

We present now a rigorous proof. Recall that the height  $f(x)_{\max}$  of a polynomial  $f(x)$  with complex coefficients is defined as the maximum of the moduli of its coefficients.

**Corollary 6.1** *Let  $h_q(x)$  and  $m_\nu(x)$  be as in (6.2). If  $\alpha$  is a non rational coefficient of  $h_q(x)$ , then the size of  $m_\alpha(x)$  is bounded by a polynomial in the size of  $m_\nu(x)$ .*

*Proof.* By hypothesis  $m_\nu(x)$  is monic with integral coefficients. A classical theorem due to Cauchy [68, p. 146] states that the roots of  $m_\nu(x)$  are bounded in modulus by  $M = 1 + m_\nu(x)_{\max}$ . By construction,  $\alpha$  is the  $j^{\text{th}}$  elementary symmetric function of  $n/q$  of the roots of  $m_\nu(x)$ , for some  $j \in \mathbb{N}$  ( $1 \leq j \leq n/q$ ). Hence, the maximum  $|\alpha|$  of the moduli of the conjugates of  $\alpha$  satisfies the inequality

$$|\alpha| \leq \binom{n/q}{j} M^j$$

Since the coefficient  $a_i$  of  $x^i$  in  $m_\alpha(x)$  is the  $(q-i)$ -th elementary symmetric function of the conjugates of  $\alpha$ , we can bound it as follows:

$$\begin{aligned} |a_i| &\leq \binom{q}{i} |\alpha|^i \\ &\leq \binom{q}{i} \left( \binom{n/q}{j} M^j \right)^i \end{aligned}$$

Hence

$$m_\alpha(x)_{\max} < q! ((n/q)! (1 + m_\nu(x)_{\max})^{n/q})^q$$

and

$$\begin{aligned} \log m_\alpha(x)_{\max} &\leq \log(q! ((n/q)! (1 + m_\nu(x)_{\max})^{n/q})^q) \\ &= q \log q + q \log((n/q)! (1 + m_\nu(x)_{\max})^{n/q}) \\ &< q \log q + q((n/q) \log(n/q) + (n/q) \log(1 + m_\nu(x)_{\max})) \\ &= q \log q + n \log(n/q) + n \log(1 + m_\nu(x)_{\max}) \end{aligned}$$

It follows that

$$\begin{aligned} \text{size}(m_\alpha) &\leq q \log m_\alpha(x)_{\max} \\ &= q(q \log q + n \log(n/q) + n \log(1 + m_\nu(x)_{\max})) \end{aligned}$$

Now,  $\log(1 + m_\nu(x)_{\max})$  is clearly bounded by  $\text{size}(m_\nu(x))$ , and by hypothesis  $m_\nu(x)$  is given in its dense representation, which implies that  $q < n \leq \text{size}(m_\nu(x))$ . This proves our assertion.  $\square$

**Remark on the execution time.** We can derive an upper bound for the time needed to factor  $m_\nu(x)$  over its splitting field, simply referring to the results in [57]. If we denote by  $|m_\nu(x)|$  the Euclidean length of  $m_\nu(x)$ , that is the square root of the sum of the squares of its coefficients, then Theorem 4.5 in [57] shows that Lenstra's algorithm computes the irreducible factorization of  $m_\nu(x)$  over its splitting field in

$$\mathcal{O}(n^{12} + n^{11} \log(n |m_\nu(x)|) + n^{10} \log m_\nu(x)_{\max})$$

operations on integers of binary length

$$O(n^6 + n^5 \log(n |m_\nu(x)|) + n^4 \log m_\nu(x)_{\max})$$

**Remark.** Bounds for the height of the irreducible factors of  $f(x)$  over  $\mathbb{Q}$  have been studied by M. Mignotte ([66],[67], [41]). These bounds are extremely useful in the design and analysis of algorithms for factoring polynomials over  $\mathbb{Q}$ , or over an algebraic number field.

### 6.1.3 Implementation issues.

In practice, the factorization of  $m_\nu(x)$  over its splitting field is unfeasible even when the degree of  $m_\nu(x)$  is small, say 15, with the known algorithms and the current computer technology. As a practical alternative we suggest the use of the polynomial reduction algorithm POLRED developed by H. Cohen and F. Diaz y Diaz [22]. Given a polynomial  $f(x)$  defining a number field  $K$  of degree  $n$ , the algorithm POLRED produces smaller polynomials which define the same number field  $K$ . In addition, the algorithm may produce minimal polynomials of elements defining subfields of  $K$ . Note however that it is not guaranteed that all the subfields will be found, since POLRED returns at most  $n$  polynomials, while the number of subfields of  $K$  may be much larger (note however that this problem does not arise for cyclic extensions). The great advantage of the algorithm POLRED over the (known) polynomial factorization algorithms is that POLRED applies the Lattice Reduction Algorithm of Lenstra, Lenstra and Lovasz to a lattice of dimension  $n$ , rather than  $n^2$ .

We tested the implementation of POLRED in PARI, on a SPARCSTATION 10, using the following polynomial which defines a cyclic number field  $E$  of degree 15:

$$\begin{aligned} m_\nu(x) = & x^{15} + 3x^{14} - 24x^{13} - 66x^{12} + 201x^{11} + 501x^{10} \\ & - 710x^9 - 1659x^8 + 975x^7 + 2413x^6 - 261x^5 - 1329x^4 \\ & - 249x^3 + 84x^2 + 12x - 1 \end{aligned}$$

POLRED found in 66 seconds the following polynomials:

- $x^5 - x^4 - 4x^3 + 3x^2 + 3x - 1$ , defining the unique subfield of  $E$  of degree 5;
- $x^3 - 3x - 1$  defining the unique subfield of  $E$  of degree 3;
- $x - 1$  defining  $\mathbb{Q}$ ; and
- $x^{15} - 27x^{13} - 4x^{12} + 252x^{11} + 60x^{10} - 976x^9 - 288x^8 + 1473x^7 + 384x^6 - 755x^5 - 168x^4 + 150x^3 + 27x^2 - 9x - 1$ , defining  $E$ .

For a comparison, we were not able to factor  $m_\nu(x)$  over its splitting field using the factorization algorithm implemented in PARI.



```

procedure NORMSQF( $a, m_\nu(x)$ ):
  compute a generator  $\tau$  of the Galois group of  $E/\mathbb{Q}$ ;
  for all the distinct prime factors  $q$  of  $n$  do
    compute  $h_q(x) = (x - \tau^q(\nu))(x - \tau^{2q}(\nu)) \cdots (x - \tau^n(\nu))$ ;
    let  $\alpha$  be any non rational coefficient of  $h_q(x)$ ;
    compute the minimal polynomial  $m_\alpha(x)$  of  $\alpha$  over  $\mathbb{Q}$ ;
    if NORM( $a, m_\alpha(x)$ ) = FALSE then
      return(FALSE)
    endif
  return(TRUE);

```

Figure 6.1: The algorithm NORMSQF.

## Chapter 7

# Test of cyclic algebras over $Q$ for zero divisors

In this chapter we show how the algorithm NORM described in Chapter 4 can be exploited to test if a cyclic algebra over  $Q$  has zero divisors.

Let us recall first some basic definitions from the theory of finite dimensional associative algebras. For some of the computational aspects of the theory we refer to [36], [80], [81], [82], [85] and to [30, Chapt. 2].

Let  $A$  be a finite dimensional associative algebra over a field  $F$ . An element  $a \in A$  is called a *divisor of zero* if there is a nonzero element  $b \in A$  such that  $ab = 0$ ; an algebra without nonzero divisors of zero is called a *division algebra*. An algebra  $A$  is said to be *simple* if it does not possess any nontrivial two sided ideal, and *central* if its center is equal to the base field.

Let  $A$  be a central simple algebra of finite dimension  $n$  over  $Q$ . Recall that the dimension  $n$  of a central simple algebra  $A$  over the base field is always a square number; the positive integer  $d = \sqrt{n}$  is called the *degree* of  $A$ .

By the Wedderburn Structure Theorem [76, p. 49], any central simple algebra  $A$  over a field  $F$  is isomorphic to a full matrix algebra over a, possibly noncommutative, finite extension  $D$  of  $F$ . The degree of  $D$  over  $F$  (as an algebra) is called the (*Schur*) *index* of  $A$ . Clearly,  $A$  is a division algebra if and only if its index and its degree are the same.

On the other hand it is known from Brauer's theory (see [76, p. 260]) that, for some finite number  $h$ , the tensor product  $A \otimes \dots \otimes A$  ( $h$  times) is isomorphic to a full matrix algebra over  $F$ . The smallest such  $h$  is called the *exponent* of  $A$ .

An important class of central simple algebras is given by the *cyclic algebras*. They were discovered by L.E. Dickson and named 'Dickson's algebras' after him by J.H.M. Wedderburn [27, p. 66].

Following Pierce [76, p. 276] they can be defined in a concise way as follows:

**Definition 7.1** *An associative algebra  $A$  of dimension  $n$  over a field  $F$  is called cyclic if it is central simple over  $F$ , and it has a cyclic subfield  $M$  of degree  $\sqrt{n}$  over  $F$ .*

In a more concrete way cyclic algebras can be defined as follows (see [76, p. 277]):

**Definition 7.2** *A finite dimensional associative algebra  $A$  over a field  $F$  is called cyclic if it is generated over  $F$  by two elements  $c$  and  $b$  such that:*

- (i). *The subalgebra  $F[c]$  of  $A$  generated by  $c$  is a cyclic extension field  $M$  of  $F$  of degree  $d$ , say;*
- (ii).  *$b$  is invertible and  $b^{-1}cb = \sigma(c)$ , where  $\sigma$  is a generator of the Galois group  $\text{Gal}(M/F)$ ;*
- (iii).  *$b^d \in F^*$ .*

It follows from this characterization that  $A$  is a central simple algebra of dimension  $d^2$  over  $F$  with basis  $\{c^i b^k | 0 \leq i, k < d\}$ . Let  $a = b^d$ . We denote the algebra  $A$  by  $(M, \sigma, a)$ .

Although cyclic algebras have an uncomplicated structure, as the next theorem shows they are quite general (see [76, p. 359] for a proof).

**Theorem 7.1 (Brauer-Hasse-Noether)** *Every central simple algebra over an algebraic number field is cyclic, and its index is equal to its exponent.*

In particular, every division algebra over  $\mathbf{Q}$  is cyclic. The theorem that follows is basic for our construction - for its proof we refer to [5, p. 98].

**Theorem 7.2 (Albert)** *Let  $M/F$  be a cyclic extension of commutative fields of degree  $d$ . Then the cyclic algebra  $(M, \sigma, a)$  has exponent  $d$  if and only if  $a \notin N_{L/F}(L^*)$  for each minimal subfield  $L$  of  $M$  over  $F$ .*

Note that when  $F$  is an algebraic number field, Theorems 7.1 and 7.2 give a criterion for  $(M, \sigma, a)$  to be a division algebra.

Given a cyclic algebra  $A = (M, \sigma, a)$ , we can use the algorithm NORM developed in the previous sections to check if the conditions of Theorem 7.2 are satisfied.

The minimal subfields of  $M$  are in one to one correspondence with the maximal subgroups of  $\text{Gal}(M/\mathbf{Q})$ . For each prime  $q$  dividing  $d$ , let  $H_{d/q} = \langle \sigma^{(q)} \rangle$  denote the unique maximal subgroup of  $\text{Gal}(M/\mathbf{Q})$  of order  $d/q$ , and let  $L_q$  denote the unique minimal subfield of  $M$  of degree  $q$  corresponding to it. To find  $L_q$ , compute

$$h_q(x) = (x - \sigma^q(c))(x - \sigma^{2q}(c)) \cdots (x - \sigma^d(c)) \quad (7.1)$$

It is a standard fact from Galois theory (see [91, p. 169]) that the coefficients of  $h_q(x)$  lie in  $L_q$  and they generate  $L_q$  over  $\mathbf{Q}$ . From the minimality of  $L_q$  it follows that any coefficient of  $h_q(x)$  which does not lie in  $\mathbf{Q}$  is a primitive element for  $L_q$  over  $\mathbf{Q}$ . Note that the number of subfields which must be considered is bounded by  $\text{size}(d) = \text{size}(n)/2$ , since  $\lfloor \log d \rfloor$  is an upper bound for the number of prime divisors of  $d$ , and  $\text{size}(d)$  is equal to  $\lfloor \log d \rfloor + 1$ .

The algorithm SKEWFIELD, shown in Figure 7.1, implements the ideas discussed above.

It takes as input a primitive element  $c$  for  $M$  over  $\mathbf{Q}$ , a generator  $\sigma$  of  $\text{Gal}(M/\mathbf{Q})$ , and a nonzero rational number  $a$ , and returns *TRUE* if  $A = (M, \sigma, a)$  has no zero divisors, *FALSE* otherwise.

The same considerations about the complexity of the algorithm NORMSQF show that the test runs in time polynomial in the size of the input, assuming that we are allowed to call an oracle in order to obtain a complete factorization of  $a$  and a

complete factorization of the discriminant of the primitive element of each minimal subfield of  $M$ .

```

procedure SKEWFIELD( $c, \sigma, a$ )
  let  $d = \sqrt{n}$ ;
  for all the distinct prime factors  $q$  of  $d$  do
    compute  $h_q(x) = (x - \sigma^q(c))(x - \sigma^{2q}(c)) \cdots (x - \sigma^d(c))$  ;
    let  $\alpha$  be any non rational coefficient of  $h_q(x)$ ;
    compute the minimal polynomial  $m_\alpha(x)$  of  $\alpha$  over  $\mathbb{Q}$ ;
    if  $\text{NORM}(a, m_\alpha(x)) = \text{TRUE}$ 
      then return FALSE
    endif
  endfor
  return TRUE

```

Figure 7.1: The algorithm SKEWFIELD.

## Chapter 8

# On the discriminant of cyclic number fields of odd prime degree

Let  $L = \mathbb{Q}[\alpha]$  be a cyclic number field of odd prime degree  $q$  over  $\mathbb{Q}$ , where  $\alpha$  is given by its minimal polynomial  $m_\alpha(x)$  over  $\mathbb{Q}$ . Without loss of generality assume that  $\alpha \in \mathcal{O}$ , the ring of algebraic integers of  $L$ .

Once again we recall that the discriminant of  $L$  can be computed using a very general algorithm due to M. Pohst and H. Zassenhaus ([77], [98], [23, p. 297]): this algorithm indeed computes an integral basis  $\mathcal{B} = \{\omega_1, \dots, \omega_q\}$  for the extension  $L/\mathbb{Q}$ , and hence the discriminant  $d_L$ .

In this chapter we show that, if we do not need an integral basis for  $L/\mathbb{Q}$  for other reasons, then the full power of the Pohst-Zassenhaus' algorithm is not required.

Indeed we give an algorithm to compute the discriminant  $d_L$  of  $L$ , which relies upon a fast method to find Eisenstein elements in  $L$ . The algorithm accepts as input the minimal polynomial of  $\alpha$  over  $\mathbb{Q}$  and a rational prime  $p$ , and decides if  $p$  ramifies in  $L$ . If it does, then the algorithm returns an algebraic integer  $\pi$  whose minimal polynomial is Eisenstein at  $p$ . It is easy to see that such an element  $\pi$  generates the value group of the unique valuation that extends the  $p$ -adic valuation from  $\mathbb{Q}$  to  $L$ ;  $\pi$  is sometimes called a *prime element* or a *local uniformizer*.

The algorithm described in this chapter is conceptually simpler than the algorithm described in Chapter 5. The reason lies in the fact that now we are not asking

for the decomposition type of a rational prime  $p$ , but simply whether  $p$  ramifies or not. The results of this chapter will appear in [2].

Let  $d_L(\alpha)$  denote once again the discriminant of  $\alpha$ . For each  $p \mid d_L(\alpha)$  we have to decide if  $p \mid d_L$ .

Firstly, by Urazbaev's criterion (Theorem 4.2), we can ignore those primes  $p \neq q$  for which either  $p \not\equiv 1 \pmod{q}$  or  $\nu_p(d_L(\alpha)) < q - 1$ . Moreover, we can ignore the prime  $q$  if  $\nu_q(d_L(\alpha)) < 2(q - 1)$ .

Secondly, we take into account the fact that  $L/\mathbb{Q}$  is Galois. As we have seen in Chapter 4, this implies that if  $p$  is a rational prime then either  $p$  splits completely in  $L$ , or  $p$  is inert in  $L$ , or  $p$  is totally ramified in  $L$ .

By assumption  $\alpha \in \mathcal{O}$ , and therefore the coefficients of  $m_\alpha(x)$  lie in  $\mathbb{Z}$ . The next lemma, which relates the decomposition of a prime  $p$  in  $L$  to the factorization of  $m_\alpha(x)$  over  $\mathbb{F}_p$ , is a simple consequence of Corollary 5.1 and Lemma 5.5.

**Lemma 8.1** *Let  $L$  be a cyclic extension of  $\mathbb{Q}$ , of odd prime degree  $q$ . Let  $p$  be a rational prime, and  $\alpha$  be an algebraic integer in  $L \setminus \mathbb{Z}$ . If  $p$  ramifies in  $L$ , then the minimal polynomial  $m_\alpha(x)$  of  $\alpha$  over  $\mathbb{Q}$  splits into the product of  $q$  identical linear factors over  $\mathbb{F}_p$ .*

It is easy to apply Lemma 8.1 following the method described in Section 5.2: the polynomial  $m_\alpha(x)$  is a  $q^{\text{th}}$  power over  $\mathbb{F}_p$  precisely when the degree of  $l(x) = \gcd(x^p - x, m_\alpha(x))$  is equal to one (the gcd is computed over  $\mathbb{F}_p$ ). Moreover  $l(x)$  can be computed very efficiently using the binary powering algorithm.

Unfortunately, the previous lemma gives only a necessary condition for a prime  $p$  to ramify in  $L$ . In the next section we will develop some necessary and sufficient conditions.

## 8.1 Eisenstein polynomials

Let us assume that  $p$  is totally ramified, and let  $\mathcal{P}$  be the unique prime ideal lying above  $p\mathbb{Z}$ . Since there is only one extension of the  $p$ -adic valuation from  $\mathbb{Q}$  to



$L$ , if  $\theta \in L$  we must have  $\nu_p(\theta) = \nu_p(N_{L/Q}(\theta))$ . In particular, if  $\theta \in \mathcal{P} \setminus \mathcal{P}^2$ , then  $\nu_p(N_{L/Q}(\theta)) = \nu_p(\theta) = 1$ . This shows that if  $p$  is ramified, then  $\mathcal{O}$  contains elements whose norms have  $p$ -order equal to 1. On the other hand

**Lemma 8.2** *If a rational prime  $p$  is inert in  $L$  then there is no  $\theta \in \mathcal{O} \setminus \mathbb{Z}$  whose norm has  $p$ -order 1.*

*Proof.* Assume that  $\theta \in \mathcal{O} \setminus \mathbb{Z}$  is an element whose norm has  $p$ -order 1. If  $\theta_1, \theta_2, \dots, \theta_q$  denote the conjugates of  $\theta$ , with  $\theta = \theta_1$  say, then  $N_{L/Q}(\theta) = \theta_1 \theta_2 \cdots \theta_q$ . Since  $p$  is inert,  $p\mathcal{O}$  is the only prime ideal of  $\mathcal{O}$  lying above  $p\mathbb{Z}$ . By assumption  $\theta_1 \theta_2 \cdots \theta_q \in p\mathbb{Z} \subset p\mathcal{O}$ , and hence, since  $p\mathcal{O}$  is a prime ideal, some conjugate of  $\theta$  must lie in  $p\mathcal{O}$ . But then, since  $p\mathcal{O}$  is  $\sigma$ -invariant, all the conjugates of  $\theta$  must lie in  $p\mathcal{O}$ , and therefore  $N_{L/Q}(\theta) \in p^q \mathcal{O} \cap \mathbb{Z} = p^q \mathbb{Z}$ , against our assumption.  $\square$

The next theorem is an immediate consequence of Lemma 8.2 and of Lemma 5.7.

**Theorem 8.1** *Let  $p$  be a rational prime. Assume that there is an element  $\theta \in \mathcal{O} \setminus \mathbb{Z}$  whose norm has  $p$ -order 1. Then  $p$  ramifies in  $L$  if and only if  $m_\theta(x)$  is Eisenstein at  $p$ .*

In order to apply Theorem 8.1, we need an efficient algorithm to solve the following problem: find an element of  $\mathcal{O}$  whose norm has  $p$ -order 1. The next lemma shows that it is enough to find any algebraic integer whose norm has  $p$ -order not divisible by  $q$ .

**Lemma 8.3** *Let  $p$  be a ramified prime. Given  $\gamma' \in \mathcal{O}$  with  $q \nmid \nu_p(N_{L/Q}(\gamma'))$ , we can construct an element  $\gamma \in \mathcal{O}$  with  $\nu_p(N_{L/Q}(\gamma)) = 1$ .*

*Proof.* Let  $r = \nu_p(N_{L/Q}(\gamma'))$ . Since  $p$  is ramified by hypothesis, we must have  $\gamma' \in \mathcal{P}^r \setminus \mathcal{P}^{r+1}$ . Since  $q \nmid r$ , we can find an  $s \in \mathbb{N}$  such that  $rs + ql = 1$  ( $l \in \mathbb{Z}$ ). If we let  $\gamma = (\gamma')^s p^l$ , then

$$\gamma \in \mathcal{P}^{rs+ql} \setminus \mathcal{P}^{rs+ql+1}$$

that is,  $\gamma \in \mathcal{P} \setminus \mathcal{P}^2$ , which proves our assertion.  $\square$

## 8.2 Finding Eisenstein elements

We will continue to assume that  $p$  is ramified. Let  $\sigma$  be a generator of  $\text{Gal}(L/\mathbb{Q})$ . The uniqueness of  $\mathcal{P}$  shows that  $\sigma(\mathcal{P}) = \mathcal{P}$  and  $\mathcal{O} = \mathbb{Z} + \mathcal{P}$ . Thus

$$\sigma(\beta) - \beta \in \mathcal{P} \quad \text{for all } \beta \in \mathcal{O}$$

We will use this fact often, in the following.

Let us consider the embedding  $\mathcal{O} \hookrightarrow \mathcal{O}_{\mathcal{P}}$ . For this purpose, we fix, *once for all*, an element  $\pi \in \mathcal{P} \setminus \mathcal{P}^2$ , and we take  $R = \{0, 1, \dots, p-1\}$  to be a set of representatives of  $\mathcal{O}/\mathcal{P}$  in  $\mathcal{O}$ . Every  $\beta \in \mathcal{O}_{\mathcal{P}}$  can be written as a convergent series (in the  $\mathcal{P}$ -adic metric)

$$\beta = \sum_{i=0}^{\infty} \sum_{j=0}^{q-1} a_{i,j} p^i \pi^j \quad (a_{i,j} \in R)$$

where the coefficients  $a_{i,j}$  are uniquely determined by  $\beta$ .

Moreover, if  $\beta \in \mathcal{O} \setminus \mathbb{Z}$ , then for some  $h, k \in \mathbb{N}$ , with  $0 < k < q$  we must have

- (i).  $a_{h,k} \neq 0$ ; and
- (ii).  $a_{i,j} = 0$  whenever  $(i < h \text{ and } 0 < j < q)$  or  $(i = h \text{ and } 0 < j < k)$ .

for otherwise, using the fact that  $ef = [L_{\mathcal{P}} : \mathbb{Q}_p] = q = [L : \mathbb{Q}]$ , the element  $\beta$  would be a  $p$ -adic integer in  $\mathcal{O}$ , and therefore an element of  $\mathbb{Z}$ .

We define now a function  $\Lambda : \mathcal{O} \rightarrow \mathcal{O}$  as follows: if  $\beta, h, k$  are as above, then

$$\Lambda(\beta) = \sum_{j=k}^{q-1} a_{h,j} p^h \pi^j + \sum_{i=h+1}^{\infty} \sum_{j=0}^{q-1} a_{i,j} p^i \pi^j$$

Since  $\sigma$  fixes  $p$  and any element of  $R$ , clearly we have

**Lemma 8.4** *Let  $\beta \in \mathcal{O}$ . If  $\sigma \in \text{Gal}(L/\mathbb{Q})$  then  $\sigma(\beta) - \beta = \sigma(\Lambda(\beta)) - \Lambda(\beta)$ .*

### 8.3 $p$ is totally and tamely ramified

In this section we assume that  $p$  is ramified and  $p \neq q$ , and we let  $\mathcal{P}$  denote the unique ideal of  $\mathcal{O}$  above  $p\mathbb{Z}$ .

**Lemma 8.5** *Let  $\sigma$  be a generator of  $\text{Gal}(L/\mathbb{Q})$ . Then  $\nu_{\mathcal{P}}(\sigma(\pi) - \pi) = 1$ .*

*Proof.* Since  $\{1, \pi, \dots, \pi^{q-1}\}$  is a local basis at  $p$ , we must have (see [93, Proposition 4.8.18, p.164])

$$\nu_p(d_L(\pi)) = \nu_{\mathcal{P}}(d_L) = q - 1$$

But  $d_L(\pi) = N_{L/\mathbb{Q}}(m'_\pi(\pi))$ , and

$$\nu_p(N_{L/\mathbb{Q}}(m'_\pi(\pi))) = \nu_{\mathcal{P}}(m'_\pi(\pi)) = \nu_{\mathcal{P}}((\sigma(\pi) - \pi) \cdots (\sigma^{q-1}(\pi) - \pi))$$

Each factor on the right hand side has  $\mathcal{P}$ -order greater than zero, there are  $q - 1$  factors, and so by the pigeon hole principle  $\nu_{\mathcal{P}}(\sigma(\pi) - \pi)$  must be 1.  $\square$

**Lemma 8.6** *Let  $\sigma$  be a generator of  $\text{Gal}(L/\mathbb{Q})$ .*

*If  $0 < r < q$  then  $\nu_{\mathcal{P}}(\sigma(\pi^r) - \pi^r) = r$ .*

*Proof.* Since  $\mathcal{P}$  and all its powers are  $\sigma$ -invariant, it follows that

$$\sigma(\pi) \equiv a\pi \pmod{\mathcal{P}^2}$$

with  $0 < a < p$ . Then

$$\sigma^2(\pi) \equiv a\sigma(\pi) \pmod{\mathcal{P}^2}$$

that is,

$$\sigma^2(\pi) \equiv a^2\pi \pmod{\mathcal{P}^2}$$

and more generally

$$\sigma^i(\pi) \equiv a^i\pi \pmod{\mathcal{P}^2}$$

But  $\sigma^q(\pi) = \pi$ , and so  $a^q \equiv 1 \pmod{p}$ . Therefore the order of  $a$  in  $\mathbb{F}_p^*$  must divide  $q$ . Since  $q$  is prime and  $a \not\equiv 1 \pmod{p}$  by Lemma 8.5, the order of  $a$  in  $\mathbb{F}_p^*$  must be equal to  $q$ . If  $0 < r < q$ , then

$$\sigma(\pi^r) - \pi^r = \sigma(\pi)^r - \pi^r \equiv a^r\pi^r - \pi^r \pmod{\mathcal{P}^{r+1}}$$

with  $a^r \not\equiv 1 \pmod{p}$ , which proves the assertion.  $\square$

**Corollary 8.1** *Let  $\sigma$  be a generator of  $\text{Gal}(L/\mathbb{Q})$ . If  $\beta \in \mathcal{O} \setminus \mathbb{Z}$ , then*

$$\nu_{\mathcal{P}}(\sigma(\Lambda(\beta)) - \Lambda(\beta)) = \nu_{\mathcal{P}}(\Lambda(\beta))$$

*In particular,  $q \nmid \nu_{\mathcal{P}}(\sigma(\Lambda(\beta)) - \Lambda(\beta))$ .*

*Proof.* Define a function  $F : L \rightarrow L$  by

$$F(x) = \sigma(x) - x$$

Note that  $\nu_{\mathcal{P}}(\sigma(x)) = \nu_{\mathcal{P}}(x)$ , and so  $\nu_{\mathcal{P}}(F(x)) \geq \nu_{\mathcal{P}}(x)$ . Since  $F$  is  $\mathbb{Z}$ -linear, we have

$$\begin{aligned} F(\Lambda(\beta)) &= F\left(\sum_{j=k}^{q-1} a_{h,j} p^h \pi^j + \sum_{i=h+1}^{\infty} \sum_{j=0}^{q-1} a_{i,j} p^i \pi^j\right) \\ &= \sum_{j=k}^{q-1} F(a_{h,j} p^h \pi^j) + F(t) \end{aligned}$$

with

$$t = \sum_{i=h+1}^{\infty} \sum_{j=0}^{q-1} a_{i,j} p^i \pi^j$$

Now,

$$\nu_{\mathcal{P}}(t) \geq (h+1)q$$

and so

$$\nu_{\mathcal{P}}(F(t)) \geq (h+1)q$$

Note that

$$\nu_{\mathcal{P}}(F(a_{h,j} p^h \pi^j)) = qh + j \quad (j = k, \dots, q-1)$$

if  $0 < a_{h,j} < p$ , and

$$\nu_{\mathcal{P}}(F(a_{h,j} p^h \pi^j)) = \infty$$

if  $a_{h,j} = 0$ . Clearly  $0 < a_{h,k} < p$ , by the definition of the function  $\Lambda$ , and so

$$\nu_{\mathcal{P}}\left(\sum_{j=k}^{q-1} F(a_{h,j} p^h \pi^j)\right) = hq + k$$

Therefore

$$\nu_{\mathcal{P}}(F(\Lambda(\beta))) = hq + k = \nu_{\mathcal{P}}(\Lambda(\beta))$$

□

**Theorem 8.2** *If  $\beta \in \mathcal{O} \setminus \mathbb{Z}$  then  $q \nmid \nu_{\mathcal{P}}(m'_{\beta}(\beta))$ .*

*Proof.* By Lemma 8.4, if  $\sigma$  denotes a generator of  $\text{Gal}(L/\mathbb{Q})$ , we have

$$\begin{aligned} m'_{\beta}(\beta) &= (\sigma(\beta) - \beta) \cdots (\sigma^{q-1}(\beta) - \beta) \\ &= (\sigma(\Lambda(\beta)) - \Lambda(\beta)) \cdots (\sigma^{q-1}(\Lambda(\beta)) - \Lambda(\beta)) \end{aligned}$$

By Corollary 8.1, then

$$\nu_{\mathcal{P}}(m'_{\beta}(\beta)) = (q-1)\nu_{\mathcal{P}}(\Lambda(\beta))$$

Since  $q \nmid \nu_{\mathcal{P}}(\Lambda(\beta))$ , it follows that  $q \nmid \nu_{\mathcal{P}}(m'_{\beta}(\beta))$ .  $\square$

The algorithm TAME, shown in Figure 8.2, implements the ideas described above. It takes as input a prime  $p \neq q$  and  $\alpha$  and returns *RAMIFIES* plus an Eisenstein element  $\pi$  if  $p$  ramifies in  $L = \mathbb{Q}[\alpha]$ , otherwise it returns *DOES\_NOT\_RAMIFY*.

## 8.4 $p$ is totally and wildly ramified

In this section we assume that  $p$  is ramified and  $p = q$ , and we denote by  $\mathcal{P}$  the unique ideal of  $\mathcal{O}$  above  $q\mathbb{Z}$ , and by  $\pi$  an element of  $\mathcal{P} \setminus \mathcal{P}^2$ . Define a function  $G : L \rightarrow L$  by

$$G(x) = \text{Tr}_{L/\mathbb{Q}}(x) - qx$$

Clearly,  $G$  is  $\mathbb{Z}$ -linear and it vanishes on  $\mathbb{Q}$ .

**Lemma 8.7** *Let  $0 < r < q$ . Then*

$$G(\pi^r) \equiv aq - q\pi^r \pmod{\mathcal{P}^{2q}}$$

with  $0 \leq a < q$ .

*Proof.* Since  $\text{Tr}_{L/\mathbb{Q}}(\pi^r) \in q\mathbb{Z}$ , we can write

$$\text{Tr}_{L/\mathbb{Q}}(\pi^r) \equiv aq \pmod{q^2}$$

with  $0 \leq a < q$ . This proves the assertion.  $\square$

```

procedure CONSTRUCT( $\gamma, p$ ):
  let  $r = \nu_p(N_{L/Q}(\gamma))$ ;
  find  $s \in \mathbf{N}$  and  $l \in \mathbf{Z}$  such that  $rs + ql = 1$ ;
  let  $\epsilon = \gamma^s p^l$ ;
  if  $m_\epsilon(x)$  is Eisenstein at  $p$ 
    then return  $\epsilon$ 
    else return 0
  endif

```

Figure 8.1: The algorithm CONSTRUCT.

```

procedure TAME( $p, \alpha$ ):
  if  $p \not\equiv 1 \pmod{q}$ 
    then return DOES_NOT_RAMIFY
  endif
  if  $\nu_p(d_L(\alpha)) < q - 1$ 
    then return DOES_NOT_RAMIFY
  endif
  compute  $c(x) = \gcd(x^p - x, m_\alpha(x))$  over  $\mathbf{F}_p$ ;
  if  $\deg(c(x)) \neq 1$ 
    then return DOES_NOT_RAMIFY
  endif
  let  $\gamma = m'_\alpha(\alpha)$ ;
  let  $\pi = \text{CONSTRUCT}(\gamma, p)$ ;
  if  $\pi \neq 0$ 
    then return RAMIFIES and  $\pi$ 
    else return DOES_NOT_RAMIFY
  endif

```

Figure 8.2: The algorithm TAME.

**Theorem 8.3** Assuming the notation of Section 8.2, if  $\beta \in \mathcal{O} \setminus \mathbf{Z}$ , then  $G(\beta) = G(\Lambda(\beta))$  and

$$G(\beta) \equiv bq^{h+1} - cq^{h+1}\pi^k \pmod{\mathcal{P}^{(h+1)q+k+1}}$$

with  $0 \leq b < q$  and  $0 < c < q$ .

*Proof.* Since the function  $G$  is  $\mathbf{Z}$ -linear, and it vanishes on  $\mathbf{Q}$ , we have

$$\begin{aligned} G(\beta) &= G(\Lambda(\beta)) \\ &= G\left(\sum_{j=k}^{q-1} a_{h,j} q^h \pi^j + \sum_{i=h+1}^{\infty} \sum_{j=0}^{q-1} a_{i,j} q^i \pi^j\right) \\ &= \sum_{j=k}^{q-1} G(a_{h,j} q^h \pi^j) + G\left(\sum_{i=h+1}^{\infty} \sum_{j=0}^{q-1} a_{i,j} q^i \pi^j\right) \\ &= \sum_{j=k}^{q-1} G(a_{h,j} q^h \pi^j) + \sum_{j=0}^{q-1} G(a_{h+1,j} q^{h+1} \pi^j) + G(t) \end{aligned}$$

with

$$t = \sum_{i=h+2}^{\infty} \sum_{j=0}^{q-1} a_{i,j} q^i \pi^j$$

Now,

$$\nu_{\mathcal{P}}(t) \geq (h+2)q$$

and so

$$\nu_{\mathcal{P}}(G(t)) \geq (h+2)q$$

Also, by Lemma 8.7,

$$\nu_{\mathcal{P}}(G(a_{h+1,j} q^{h+1} \pi^j)) \geq q(h+2) \quad (j = 0, \dots, q-1)$$

and

$$G(a_{h,k} q^h \pi^k) \equiv b_k q^{h+1} - c_k q^{h+1} \pi^k \pmod{\mathcal{P}^{(h+2)q}}$$

with  $c_k \not\equiv 0 \pmod{q}$ , since  $a_{h,k} \not\equiv 0 \pmod{q}$  by the definition of the function  $\Lambda$ .

Moreover, if  $a_{h,s} \not\equiv 0 \pmod{q}$  ( $s = k+1, \dots, q-1$ ) then

$$G(a_{h,s} q^h \pi^s) \equiv b_s q^{h+1} - c_s q^{h+1} \pi^s \pmod{\mathcal{P}^{(h+2)q}}$$

This shows that

$$G(\beta) \equiv q^{k+1} \left( \sum_{i=k}^{q-1} b_i \right) - q^{h+1} c_k \pi^k \pmod{\mathcal{P}^{(h+1)q+k+1}}$$

with  $c_k \not\equiv 0 \pmod{q}$ . To prove our assertion, let  $b = \sum_{i=k}^{q-1} b_i \pmod{q}$ , and  $c = c_k$ .  
□

We show next how Theorem 8.3 can be used to obtain an algebraic integer whose norm has  $q$ -order not divisible by  $q$ . Let  $w = \nu_q(N_{L/\mathbb{Q}}(G(\beta)))$ .

If  $q \nmid w$  then  $b \equiv 0 \pmod{q}$ , and  $G(\beta)$  is the desired element.

Otherwise,  $w = q(h+1)$ , and if we let  $v = w/q$  then

$$G(\beta)/q^v \equiv b - c\pi^k \pmod{\mathcal{P}^{k+1}}$$

Note that  $G(\beta)/q^v \in \mathcal{O}$ , since  $\nu_{\mathcal{P}}(G(\beta)/q^v) = 0$  and  $\nu_{\mathcal{Q}}(G(\beta)/q^v) = \nu_{\mathcal{Q}}(G(\beta)) \geq 0$ , when  $\mathcal{Q}$  is any prime ideal of  $\mathcal{O}$  not equal to  $\mathcal{P}$ . Let  $\rho = G(\beta)/q^v$ . It is easily seen that, if

$$m_{G(\beta)}(x) = x^q + b_{q-1}x^{q-1} + \dots + b_1x + b_0$$

then

$$m_{\rho}(x) = x^q + (b_{q-1}/q^v)x^{q-1} + \dots + (b_1/q^{v(q-1)})x + (b_0/q^{vq})$$

Since  $q$  is assumed to be ramified, then

$$m_{\rho}(x) \equiv (x - \hat{s})^q \pmod{q}$$

Let  $s$  be a representative of the residue class of  $\hat{s}$ , with  $0 \leq s < q$ . Then  $(\rho - s)^q \in q\mathcal{O}$ . Hence  $s = b$  and

$$\rho - s \equiv -c\pi^k \pmod{\mathcal{P}^{k+1}}$$

Therefore  $\rho - s$  is the desired element.

The algorithm WILD, shown in Figure 8.3, implements the ideas described above. It takes as input  $q$  and  $\alpha$  and returns *RAMIFIES* plus an Eisenstein element  $\pi$  if  $q$  ramifies in  $L = \mathbb{Q}[\alpha]$ , otherwise it returns *DOES NOT RAMIFY*.



## 8.5 Some remarks

In this chapter we have shown how to determine if a rational prime  $p$  ramifies in  $L$ , and if this is the case, how to find an Eisenstein element at  $p$ . The algorithms TAME and WILD given here are conceptually simpler than the algorithm DECOMPOSE given in Chapter 5. However, they do not tell us if a nonramified prime  $p$  is inert or splits in  $L$ .

It is natural to ask if there is some general algorithm to accomplish the task of recognizing the decomposition type of a rational prime  $p$  in a number field  $K = \mathbb{Q}[\beta]$ , with ring of integers  $\mathcal{O}$ , without having to compute the prime ideal decomposition. The trivial case, when  $p$  does not divide the module index  $[\mathcal{O} : \mathbb{Z}[\beta]]$  is dealt with using a classical theorem of Kummer [47, Theorem 7.6, p. 32]. For the abelian case, we state the following general result due to M.A Huang [45, Theorem 1.3].

**Theorem 8.4** *Let  $K$  be an abelian number field and  $p$  a rational prime non dividing  $[K : \mathbb{Q}]$ . Assuming the Extended Riemann Hypothesis, it is possible to compute the ramification index and the residue class degree of  $p$  relative to  $K$  in deterministic polynomial time.*

Assume that  $[K : \mathbb{Q}] = q$  is prime, and let  $\epsilon$  be a primitive  $q^{\text{th}}$  root of unity. Huang's algorithm works by translating the original problem to the Kummer extension  $K[\epsilon]/\mathbb{Q}[\epsilon]$ . However Huang's method appears to be of theoretical rather than practical interest, since it requires application of the Lenstra-Lenstra-Lovasz algorithm [54] in various constructions of fields and groups (see [45, p. 123]).

## 8.6 Computational examples

The algorithms described in this chapter have been implemented in PARI and tested on a SPARCSTATION 10. Since the running time is negligible, we report for each field the Eisenstein elements found, in order to compare them with the Eisenstein elements found using the algorithm DECOMPOSE.

```

procedure WILD( $q, \alpha$ ):
  if  $\nu_q(d_L(\alpha)) < 2(q - 1)$ 
    then return DOES_NOT_RAMIFY
  endif
  if  $m_\alpha(x)$  is not a  $q^{th}$  power over  $\mathbb{F}_q$ 
    then return DOES_NOT_RAMIFY
  endif
  let  $\delta = \text{Tr}_{L/\mathbb{Q}}(\alpha) - q\alpha$ ;
  let  $w = \nu_q(N_{L/\mathbb{Q}}(\delta))$ ;
  if  $q \nmid w$  then let  $\gamma = \delta$ 
  else
    let  $v = w/q$ ; let  $\rho = \delta/q^v$ ;
    if  $m_\rho(x) \notin \mathbb{Z}[x]$ 
      then return DOES_NOT_RAMIFY
    endif
    compute  $c(x) = \gcd(x^q - x, m_\rho(x))$  over  $\mathbb{F}_q$ ;
    if  $c(x) \neq x - s$ 
      then return DOES_NOT_RAMIFY
    endif
    let  $\gamma = \rho - s$ ;
    if  $q \mid \nu_q(N_{L/\mathbb{Q}}(\gamma))$ 
      then return DOES_NOT_RAMIFY
    endif
  endif
  let  $\pi = \text{CONSTRUCT}(\gamma, q)$ ;
  if  $\pi \neq 0$ 
    then return RAMIFIES and  $\pi$ 
    else return DOES_NOT_RAMIFY
  endif

```

Figure 8.3: The algorithm WILD.

### 8.6.1 Discriminant of the form $p^{q-1}$ with $p \neq q$

The algorithm TAME was tested using the following polynomials found in H.Cohen's book [23, p. 327]:

$$p_3(x) = x^3 + x^2 - 2x - 1$$

$$p_5(x) = x^5 + x^4 - 4x^3 - 3x^2 + 3x + 1$$

$$p_7(x) = x^7 + x^6 - 12x^5 - 7x^4 + 28x^3 + 14x^2 - 9x + 1$$

The corresponding field discriminants are  $7^2$ ,  $11^4$ ,  $29^6$ .

Below we list the Eisenstein polynomials  $w_{i,p}(x)$ , corresponding to the polynomial  $p_i(x)$  and to the prime  $p$ , which were found using the algorithm TAME:

$$w_{3,7}(x) = x^3 - 7x^2 + 14x - 7$$

$$w_{5,11}(x) = x^5 - 88x^4 + 660x^3 - 627x^2 + 154x - 11$$

$$\begin{aligned} w_{7,29}(x) = & x^7 - 1104572330073x^6 + 4722139878230826133194x^5 \\ & - 279772708771873219858337478x^4 \\ & + 5345395959971537411317679411x^3 \\ & - 3009073955331456639517564210x^2 + 14368312908084136906477x \\ & - 16896044879663069 \end{aligned}$$

For a comparison, we list below the Eisenstein polynomials  $u_{i,p}(x)$ , corresponding to the polynomial  $p_i(x)$  and to the prime  $p$ , which were found using the algorithm DECOMPOSE:

$$u_{3,7}(x) = x^3 - 14x^2 + 63x - 91$$

$$u_{5,11}(x) = x^5 - 44x^4 + 770x^3 - 6699x^2 + 28974x - 49841$$

$$\begin{aligned} u_{7,29}(x) = & x^7 - 174x^6 + 12963x^5 - 536007x^4 + 13285103x^3 \\ & - 197372086x^2 + 1627442416x - 5745350399 \end{aligned}$$

### 8.6.2 Discriminant of the form $q^{2q-2}$

In this section we show that it is quite easy to produce cyclic fields of prime degree  $q$  in which the only ramified prime is  $q$ , and we give some examples below.

Recall that, by the Kronecker-Weber theorem [47, p. 165] every abelian number field can be embedded in a cyclotomic field of suitable degree.

In particular, if a cyclic field  $L$  of odd prime degree  $q$  has  $q$  as its only ramified prime, then [63, Exercise 37, p. 129] it can be shown that  $L$  is contained in the  $q^2$ -th cyclotomic field. Now, the Galois group of the  $q^2$ -th cyclotomic field is isomorphic to the multiplicative group of the ring  $\mathbb{Z}/q^2\mathbb{Z}$ , and hence it is cyclic of order  $q(q-1)$ . It is well known how to produce all the subfields of the  $q^n$ -th cyclotomic field [91, p. 176], where  $q$  is prime and  $n$  is a positive integer – let us recall briefly the construction, when  $n = 2$ .

Let  $\zeta$  be a primitive  $q^2$ -th root of unity. Then the minimal polynomial of  $\zeta$  over  $\mathbb{Q}$  is the  $q^2$ -th cyclotomic polynomial, which is given by

$$x^{q(q-1)} + x^{q(q-2)} + \dots + x^q + 1$$

Let  $r$  be an integer such that its image in the ring  $\mathbb{Z}/q^2\mathbb{Z}$  generates the multiplicative group of  $\mathbb{Z}/q^2\mathbb{Z}$ . Then the Galois group of  $\mathbb{Q}[\zeta]/\mathbb{Q}$  is generated by the automorphism  $\tau$  such that

$$\tau(\zeta) = \zeta^r$$

It can be proved that the term

$$\xi = \zeta + \tau^q(\zeta) + \tau^{2q}(\zeta) + \dots + \tau^{(q-2)q}(\zeta)$$

belongs to the unique subfield  $L$  of degree  $q$  of  $\mathbb{Q}[\zeta]$ , and moreover  $\xi$  is a primitive element for  $L$  over  $\mathbb{Q}$ . The minimal polynomial  $m_\xi(x)$  of  $\xi$  over  $\mathbb{Q}$  is the desired polynomial needed to test the algorithm WILD.

The following polynomials have been computed using the method described above:

$$p_3(x) = x^3 - 3x + 1$$

$$\begin{aligned}
p_5(x) &= x^5 - 10x^3 + 5x^2 + 10x + 1 \\
p_7(x) &= x^7 - 21x^5 - 21x^4 + 91x^3 + 112x^2 - 84x - 97 \\
p_{11}(x) &= x^{11} - 55x^9 + 33x^8 + 825x^7 - 396x^6 \\
&\quad - 4972x^5 + 1287x^4 + 12760x^3 - 924x^2 - 10989x + 243
\end{aligned}$$

Below we list the Eisenstein polynomials  $w_i(x)$ , corresponding to the polynomials  $p_i(x)$ , which were found using the algorithm WILD (resp. in 10, 25, 45, 80 milliseconds):

$$\begin{aligned}
w_3(x) &= x^3 - 6x^2 + 9x - 3 \\
w_5(x) &= x^5 - 20x^4 + 150x^3 - 525x^2 + 850x - 505 \\
w_7(x) &= x^7 - 42x^6 + 735x^5 - 6909x^4 + 37387x^3 \\
&\quad - 115150x^2 + 183456x - 112511 \\
w_{11}(x) &= x^{11} - 110x^{10} + 5445x^9 - 160083x^8 + 3105465x^7 \\
&\quad - 41729754x^6 + 396251768x^5 - 2658133687x^4 + 12340722240x^3 \\
&\quad - 37.48534076x^2 + 68437746531x - 55682227953
\end{aligned}$$

For a comparison, we list below the Eisenstein polynomials  $u_i(x)$ , corresponding to the polynomials  $p_i(x)$ , which were found using the algorithm DECOMPOSE (resp. in 20, 20, 60, 105 milliseconds):

$$\begin{aligned}
u_3(x) &= x^3 - 3x^2 + 3 \\
u_5(x) &= x^5 - 5x^4 + 25x^2 - 25x + 5 \\
u_7(x) &= x^7 - 7x^6 + 49x^4 - 98x^2 - 49x + 7 \\
u_{11}(x) &= x^{11} - 11x^{10} + 363x^8 - 1089x^7 - 1089x^6 + 6413x^5 \\
&\quad + 242x^4 - 11616x^3 - 2178x^2 + 6534x + 2673
\end{aligned}$$

Our experiments with this construction on a SPARCSTATION 10 using PARI have been limited to  $q \leq 11$ , and failed for larger primes. The bottleneck lies in the computation of the minimal polynomial of  $\xi$  over  $\mathbb{Q}$ , which essentially reduces to the computation of the minimal polynomial of a  $q(q-1) \times q(q-1)$  matrix with integer

coefficients. The function *char()* implemented in PARI computes the characteristic polynomial of a  $n \times n$  matrix  $M$  by computing the adjoint matrix  $M^{adj}$  of  $M$ , and it is known [23, p. 52] that this method requires  $\mathcal{O}(n^4)$  operations in the straight line model of computation.

Hence, in order to construct larger examples, we have to avoid the computation of the minimal polynomial of  $\xi$ . This can be done by estimating numerically a primitive  $q^2$ -th root of unity, and then estimating  $\xi$  and all its conjugates say  $\hat{\xi}_1, \dots, \hat{\xi}_q$ . This is easily done, since we know the action of the Galois group of  $C_{q^2}$  on  $\xi$ . It is clear that the polynomial

$$m_{\hat{\xi}}(x) = (x - \hat{\xi}_1) \dots (x - \hat{\xi}_q)$$

is an approximation of  $m_{\xi}(x)$ , the minimal polynomial of  $\xi$ . If we carried out the computations using an adequate precision, then  $m_{\xi}(x)$  is obtained by rounding the coefficients of  $m_{\hat{\xi}}(x)$  to the nearest integer. A Maple procedure that implements the ideas discussed above is shown in Figure 8.4. The procedure is called as follows

$$\text{collect}(\text{elem}(n), x, i \rightarrow \text{round}(i));$$

where  $n$  is the (prime) degree of the desired cyclic field. Using this program we constructed the following polynomials

$$\begin{aligned} p_{13}(x) &= x^{13} - 78x^{11} - 65x^{10} + 2080x^9 + 2457x^8 \\ &\quad - 24128x^7 - 27027x^6 + 137683x^5 + 110214x^4 - 376064x^3 \\ &\quad - 128206x^2 + 363883x - 12167 \\ p_{17}(x) &= x^{17} - 136x^{15} + 85x^{14} + 6154x^{13} - 6545x^{12} \\ &\quad - 119680x^{11} + 168555x^{10} + 998835x^9 - 1749300x^8 \\ &\quad - 2783546x^7 + 6581040x^6 - 678725x^5 - 3813882x^4 \\ &\quad + 770593x^3 + 616267x^2 - 82620x - 577 \\ p_{19}(x) &= x^{19} - 171x^{17} - 133x^{16} + 11476x^{15} + 15580x^{14} \\ &\quad - 385833x^{13} - 673436x^{12} + 6916190x^{11} + 13391960x^{10} \\ &\quad - 66283229x^9 - 126730380x^8 + 339213156x^7 + 582575340x^6 \end{aligned}$$

$$\begin{aligned}
& -861915924x^5 - 1264657480x^4 + 868638105x^3 + 1138104275x^2 \\
& -137550709x - 221874931
\end{aligned}$$

The corresponding Eisenstein polynomials which were found using the algorithm WILD (resp in 88, 110, 125 milliseconds) are

$$\begin{aligned}
w_{13}(x) &= x^{13} - 156x^{12} + 11154x^{11} - 483847x^{10} + 14202760x^9 \\
& -297813321x^8 + 4587719968x^7 - 52547195181x^6 + 447305133691x^5 \\
& -2793444538794x^4 + 12432720042496x^3 - 37317982335218x^2 \\
& +67654117212955x - 55893361285021 \\
w_{17}(x) &= x^{17} - 272x^{16} + 34680x^{15} - 2752725x^{14} \\
& +152345194x^{13} - 6238381455x^{12} + 195716959168x^{11} \\
& -4804939712619x^{10} + 93449986408595x^9 - 1447942780998268x^8 \\
& +17872066460817606x^7 - 174719193199899088x^6 \\
& +1336162045976908987x^5 - 7824879897977436278x^4 \\
& +33883949327735099809x^3 - 102221649203474911611x^2 \\
& +191796224112178399652x - 168488758269952339199 \\
w_{19}(x) &= x^{19} - 342x^{18} + 55233x^{17} - 5598749x^{16} + 399325204x^{15} \\
& -21291694804x^{14} + 880056115575x^{13} - 28854510538714x^{12} \\
& +761500599861254x^{11} - 16317905187968636x^{10} + 285073842730166683x^9 \\
& -4059926571594316938x^8 + 46937897320989445908x^7 \\
& -436643544083067734340x^6 + 3220444160178689126124x^5 \\
& -18400938925820506096160x^4 + 78535649477687333418873x^3 \\
& -235628045690362587415769x^2 + 443231717937172714093283x \\
& -393221801447722764394343
\end{aligned}$$

The corresponding Eisenstein polynomials which were found using the algorithm DECOMPOSE (resp in 100, 120, 140 milliseconds) are

$$u_{13}(x) = x^{13} - 13x^{12} + 507x^{10} - 845x^9 - 7605x^8 + 14872x^7$$

$$\begin{aligned}
& +56615x^6 - 100724x^5 - 217841x^4 + 288314x^3 + 380926x^2 \\
& - 268203x - 158171 \\
u_{17}(x) = & x^{17} - 17x^{16} + 1445x^{14} - 6936x^{13} - 23120x^{12} \\
& + 234668x^{11} - 232934x^{10} - 2255645x^9 + 6539492x^8 \\
& + 2044386x^7 - 31812253x^6 + 39958007x^5 + 14934653x^4 \\
& - 74809095x^3 + 67717324x^2 - 25975320x + 3684767 \\
u_{19}(x) = & x^{19} - 19x^{18} + 1805x^{16} - 5776x^{15} - 67868x^{14} \\
& + 295659x^{13} + 1304293x^{12} - 6563702x^{11} - 13483350x^{10} \\
& + 76176054x^9 + 69810180x^8 - 467936864x^7 - 125336312x^6 \\
& + 1371428531x^5 - 135767407x^4 - 1370374050x^3 + 224419621x^2 \\
& + 182716540x - 28492267
\end{aligned}$$

### 8.6.3 Discriminant of the form $p^{q-1}q^{2q-2}$ with $p \neq q$

Finally, let us consider a mixed example, namely the splitting field of the polynomial

$$p_3 = x^3 - 6x^2 - 27x + 44$$

This polynomial generates the same field as the polynomial  $x^3 - 39x - 26$ , which was found in the number fields tables recently released by The Computational Number Theory group in Bordeaux. These tables contain the description of more than 55000 number fields of degrees 3,4,5,6 and 7, and are available by anonymous ftp at the address [megrez.math.u-bordeaux.fr](http://megrez.math.u-bordeaux.fr). The discriminant of the splitting field of  $p_3$  is  $3^4 \cdot 13^2$ . The Eisenstein polynomial at 13, which was found using the algorithm TAME is

$$x^3 - 1053x^2 + 303264x - 21835008$$

The Eisenstein polynomial at 13, which was found using the algorithm DECOMPOSE is

$$x^3 - 39x^2 + 468x - 1716$$



```

with(numtheory);
fred(elem);
elem := proc(p)
    local g,h,k,h1,k1,c,i,j,l,f;
    g := primroot(1,p2);
    h := gp mod p2; k := g(p-1) mod p2;
    k1 := 1; c := array(0..p-1);
    for i from 0 to p-1 do
        c[i] := 0.0; h1 := 1;
        for j from 1 to p-1 do
            c[i] := c[i] + cos(2*Pi*h1*k1/(p*p));
            h1 := h1*h mod p2;
        od;
        k1 := k1*k mod p2;
    od;
    f := expand(evalf(product (x-c[l],l=0..p-1)));
end:

```

Figure 8.4: A Maple program to construct wild examples.

The Eisenstein polynomial at 3, which was found using the algorithm WILD is

$$x^3 - 6x^2 - 27x + 96$$

The Eisenstein polynomial at 3, which was found using the algorithm DECOMPOSE is

$$x^3 - 12x^2 + 9x + 66$$

## 8.7 Concluding remarks

The computational examples given in the previous sections show that the size of the minimal polynomial  $m_\pi(x)$  of the Eisenstein element  $\pi$  found by the algorithm TAME (or WILD) is generally larger than the size of the corresponding minimal polynomial  $m_\tau(x)$  found by the algorithm DECOMPOSE.

In the case of the algorithm TAME it is possible to give a very simple explanation of this behavior. When the procedure CONTRUCT is called,  $\gamma$  is equal to  $m'_\alpha(\alpha)$ , and so  $|N_{L/Q}(\gamma)| = |d_L(\alpha)|$ . Hence, from Mahler's bound (4.7) we get

$$\text{size}(N_{L/Q}(\gamma)) < q \log q + 2(q-1)(\log q + \log H)$$

where  $H$  stands for the height of  $m_\alpha(x)$ .

Now, elementary number theory tells us that the integer  $s$  such that  $rs + ql = 1$  can be always taken between 1 and  $q-1$  included. This forces the integer  $l$ , for which the relation  $rs + ql = 1$  holds, to be negative.

In particular, from the consideration of the extreme case ( $s = q-1$ ,  $l = 0$ ) we obtain the following lemma (compare it with Lemma 5.9):

**Lemma 8.8** *The size of the norm of the Eisenstein element  $\pi$  found by the algorithm TAME is bounded above by  $(q-1)q \log q + 2(q-1)^2(\log q + \log H)$ , where  $H$  denotes the height of  $m_\alpha(x)$ .*

## References

- [1] V. Acciario, *Power roots of polynomials over arbitrary fields*, Bull. Austral. Math. Soc. 50 (1994), 327–335.
- [2] V. Acciario, *Finding Eisenstein elements in cyclic number fields of odd prime degree*, to appear in Bull. Austral. Math. Soc.
- [3] L. Adleman, K. Manders, and G. Miller. *On taking roots in finite fields*, Proceedings of the 18<sup>th</sup> IEEE Symposium on Foundations of Computer Science, 1977, 175–177.
- [4] A.V. Aho, J.E. Hopcroft, and J.D. Ullman. *The Design and Analysis of Computer Algorithms*, Addison-Wesley, Reading, Massachusetts, 1974.
- [5] A.A. Albert, *Structure of Algebras*, A.M.S. Colloquium Publications vol. 24, 1961.
- [6] N.C. Ankeny. *The least quadratic non residue*, Annals of Math. 55 (1952), 65–72.
- [7] E. Artin. *Theory of Algebraic Numbers*, Notes by G. Wurges, translated by G. Striker, Göttingen, 1956.
- [8] M. Atiyah and I. Macdonald, *Introduction to Commutative Algebra*, Addison-Wesley Publishing Company, 1969.
- [9] L. Babai. *Monte Carlo algorithms in graph isomorphism testing*, Tech. Rep. 79–10, Department of Mathematics and Statistics, University of Montreal, 1979.

- [10] E. Bach, *Fast algorithms under the Extended Riemann Hypothesis: a concrete estimate*, Proceedings of the 14<sup>th</sup> ACM Symp. on Theory of Computing (1982), 290-295.
- [11] C. Batut, D. Bernardi, H. Cohen and M. Olivier, *User's Guide to PARI-GP, version 1.39*, Université Bordeaux I, 1995.
- [12] E.R. Berlekamp, *Factoring polynomials over large finite fields*, Math. Comp. 24 (1970), 713-735.
- [13] J. Blömer, *Computing sums of radicals in polynomial time*, Proceedings of the 32<sup>nd</sup> IEEE Symposium on Foundations of Computer Science, 1991, 670-677.
- [14] Z.I. Borevich and I.R. Shafarevich, *Number Theory*, Academic Press, New York and London, 1966.
- [15] J. Buchmann and H.W. Lenstra, *Computing maximal orders and factoring over  $\mathbb{Z}_p$* , preprint, 1993.
- [16] J. Buchmann, *Complexity of algorithms in algebraic number theory*, Proceedings of the first conference of the Canadian Number Theory Association (R.A. Mollin, ed.), De Gruyter, Berlin, 1990, 37-53.
- [17] J. Buchmann and V. Shoup, *Constructing nonresidues in finite fields and the Extended Riemann Hypothesis*, in Proceedings of the 23<sup>th</sup> ACM Symposium on Theory of Computing 1991, 72-79.
- [18] D.G. Cantor and H. Zassenhaus, *A new algorithm for factoring polynomials over finite fields*, Math. Comp. 36 (1981), 587-592.
- [19] J.W.S. Cassels and A. Frohlich, *Algebraic Number Theory*, Academic Press, London and New York, 1967.
- [20] A.L. Chistov and D.Y. Grigoriev, *Polynomial time factoring of the multivariate polynomials over a general field*, USSR Academy of Sciences, Steklov Mathematical Institute, Leningrad, 1982.

- [21] A.L. Chistov, *The complexity of constructing the ring of integers of a global field*, Soviet Math. Dokl. 39 (1989), 597-600.
- [22] H. Cohen and F. Diaz y Diaz, *A polynomial reduction algorithm*, Seminaire de Theorie de Nombres de Bordeaux (Serie 2) 3 (1991), 351-360.
- [23] H. Cohen, *A Course in Computational Algebraic Number Theory*, Springer-Verlag, New York, 1993.
- [24] H. Cohn, *A Classical Introduction to Algebraic Numbers and Class Fields*, Springer-Verlag, New York, 1978.
- [25] G.E. Collins, *The calculation of multivariate polynomial resultants*, JACM 19 (1971), 515-532.
- [26] D.A. Cox, *Primes of the Form  $x^2 + ny^2$* , John Wiley and Sons, New York, 1989.
- [27] L.E. Dickson, *Algebras and their Arithmetic*, Dover Publications, Inc., New York, 1960.
- [28] J.D. Dixon, *Exact solution of linear equations using p-adic expansions*, Numer. Math. 40 (1982), 137-141.
- [29] J.D. Dixon, *Computing subfields in algebraic number fields*, J. Austral. Math. Soc. 49 (1990), 434-448.
- [30] W. Eberly, *Computations for Algebras and Group Representations*, Ph.D. Thesis, University of Toronto, 1989.
- [31] W. Eberly, *Decomposition of algebras over finite fields and number fields*, Comput. Complexity 1 (1991), 179-206.
- [32] W. Eberly, *Decomposition of algebras over  $\mathbf{R}$  and  $\mathbf{C}$* , Comput. Complexity 1 (1991), 207-230.
- [33] R.J. Fateman, *Polynomial multiplication, powers and asymptotic analysis: some comments*, SIAM J. Comp. 3 (1974), 196-213.

- [34] D.J. Ford, *On the computation of the maximal order in a Dedekind Domain*, Ph.D. Thesis, Ohio State University, 1978.
- [35] K. Friedl, *Algorithms in algebra*, Diploma Thesis, Eötvös University, Budapest, 1983.
- [36] K. Friedl and L. Ronyai, *Polynomial time solutions of some problems in computational algebra*. Proceedings of the 17<sup>th</sup> ACM Symposium on Theory of Computing, Providence, 1985, 153–162.
- [37] D. Garbanati, *Class field theory summarized*, Rocky Mountain J. Math. 11 (1981), 195–225.
- [38] J. von zur Gathen, *Hensel and Newton methods in valuation rings*, Math. Comp. 42 (1984), 637–661.
- [39] K.F. Gauss, *Disquisitiones Arithmeticae*. Fleischer, Leipzig, 1801.
- [40] G. Ge, *Testing equalities of multiplicative representations in polynomial time*, Proceedings of the 34<sup>th</sup> IEEE Symposium on Foundations of Computer Science, 1993, 422–426.
- [41] P. Glesser and M. Mignotte, *An inequality about irreducible factors of integer polynomials II*, in 'Applied Algebra, Algebraic Algorithms and Error Correcting Codes' (S. Sakata ed.), Lecture Notes in Comput. Sci., vol. 508, Springer-Verlag, New York, 1990, 260–266.
- [42] L.J. Goldstein, *Analytic Number Theory*, Prentice-Hall, Inc., Englewood Cliffs, New Jersey, 1971.
- [43] J. Haslrad, B. Just, J.C. Lagarias, and C.P. Schnorr, *Polynomial time algorithms for finding integer relations among real numbers*, Siam J. Comput. 18 (1989), 859–881.
- [44] K. Hensel, *Über eine neue Begründung der Theorie der algebraischen Zahlen*, Jber. Deutsch. Math. Verein. 6 (1897), 83–88.

- [45] M.A. Huang, *Riemann hypothesis and finding roots over finite fields*, Proceedings of the 17<sup>th</sup> ACM Symposium on Theory of Computing, 1985, 121–130.
- [46] G. Ivanyos and L. Rónyai, *Finding maximal orders in semisimple algebras over  $\mathbb{Q}$* , Comput. Complexity 3 (1993), 245–261.
- [47] G.J. Janusz, *Algebraic Number Fields*, Academic Press, New York, 1973.
- [48] A. Karatsuba and Y. Ofman, *Multiplication of multidigit numbers by automata*, Soviet Physics-Doklady 7 (1963), 595–596.
- [49] D. E. Knuth, *The Art of Computer Programming*, vol. 2. Seminumerical Algorithms, Addison-Wesley Publishing Company, Reading, Massachusetts, 1981.
- [50] N. Koblitz,  *$p$ -adic Numbers,  $p$ -adic Analysis and Zeta Functions*, Springer-Verlag, New York, 1984.
- [51] S. Landau, *Factoring polynomials over algebraic number fields*, SIAM J. Comput. 14 (1985), 184–195.
- [52] S. Lang, *Algebraic Number Theory*, Springer-Verlag, New York, 1986.
- [53] S. Lang, *Algebra*, 3rd ed., Addison-Wesley Publishing Company, Reading, Massachusetts, 1993.
- [54] A.K. Lenstra, H.W. Lenstra and L. Lovasz, *Factoring polynomials with rational coefficients*, Math. Ann. 261 (1982), 515–534.
- [55] A.K. Lenstra, *Lattices and factorization of polynomials over algebraic number fields*, EUROCAM '82 (Jacques Calmet, ed.), Lecture Notes in Computer Science, vol. 144, Springer-Verlag, New York, 1982, 32–39.
- [56] A.K. Lenstra, *Factoring polynomials over algebraic number fields*, Report TW 213/82, Mathematisch Centrum, Amsterdam 1982

- [57] A.K. Lenstra, *Factoring polynomials over algebraic number fields*, EUROCAL '83 (J. A. van Hultzen, ed.), Lecture Notes in Comput. Sci., vol. 162, Springer-Verlag, New York, 1983, 245–254.
- [58] H.W. Lenstra, *Algorithms in algebraic number theory*, Bull. Amer. Math. Soc. 26 (1992), 211–244.
- [59] R. Lidl and H. Niederreiter, *Finite Fields*, Encyclopedia of Math. and its Applications vol. 20, Addison-Wesley Publishing Company, Reading, Massachusetts, 1983.
- [60] J.D. Lipson, *Newton's Method: a Great Algebraic Algorithm*, Proceedings of the 1976 ACM Symposium on Symbolic and Algebraic Computation, 1976, 260–270.
- [61] R. Loos, *Computing in algebraic extensions*, in 'Computer algebra, symbolic and algebraic computation' (B. Buchberger, G.E. Collins, and R. Loos editors), Springer-Verlag, Wien, 1982.
- [62] K. Mahler, *An inequality for the discriminant of a polynomial*, Michigan Math. J. 11 (1964), 257–262.
- [63] D.A. Marcus, *Number Fields*, Springer-Verlag, New York, 1977.
- [64] B. Mazur, *On the passage from local to global in number theory*, Bull. Amer. Math. Soc. 29 (1993), 14–34.
- [65] P.J. McCarthy, *Algebraic Extensions of Fields*, Dover Publications, Inc., New York, 1991.
- [66] M. Mignotte, *An inequality about factors of polynomials*, Math. Comp. 28 (1974), 1153–1157.
- [67] M. Mignotte, *An inequality about irreducible factors of integer polynomials*, J. Number Theory 30 (1988), 156–166.



- [68] M. Mignotte, *Mathematics for Computer Algebra*, Springer-Verlag, New York, 1992.
- [69] J.B. Miller, *Power roots of polynomials*, Bull Austral. Math. Soc. 47 (1993), 163–168.
- [70] R.T. Moenck, *Practical fast polynomial multiplication*, in Proceedings SYM-SAC'76 (R.D. Jenks ed.), ACM Press (1976), 136–145.
- [71] T. Nagell, *Introduction to Number Theory*, Chelsea Publishing Company, New York, 1964.
- [72] H. Niederreiter, *A new efficient factorization algorithm for polynomials over small finite fields*, Appl. Algebra Engrg. Comm. Comput. 4 (1993), 81–87.
- [73] H. Niederreiter, *Factorization of polynomials and some linear algebra problems over finite fields*, Linear Algebra Appl. 192 (1993), 301–328.
- [74] H. Niederreiter, *New deterministic factorization algorithms for polynomial over finite fields*, Contemporary Mathematics 168 (1994), 251–268.
- [75] I. Niven and H.S. Zuckerman. *An Introduction to the Theory of Numbers*, John Wiley and Sons, New York, 1980.
- [76] R.S. Pierce, *Associative Algebras*, Springer-Verlag, New York, 1982.
- [77] M.E. Pohst, *Three principal tasks of computational algebraic number theory*, Number Theory and Applications, (R.A. Mollin ed.), Kluwer Academic Publisher, Dordrecht, 1989, 123–133.
- [78] M.E. Pohst and H. Zassenhaus, *Algorithmic Algebraic Number Theory*, Cambridge University Press, Cambridge, 1989.
- [79] M.O. Rabin, *Probabilistic algorithms in finite fields*, SIAM J. Comp. 9 (1980), 273–280.

- [80] L. Rónyai, *Simple algebras are difficult*, Proceedings of the 19<sup>th</sup> ACM Symposium on Theory of Computing, New York, 1987, 398–408.
- [81] L. Rónyai, *Zero divisors in quaternion algebras*, J. Algorithms 9 (1988), 494–506.
- [82] L. Rónyai, *Computing the structure of finite algebras*, J. Symb. Comp. 9 (1990), 355–373.
- [83] L. Rónyai, *Algorithmic properties of maximal orders in simple algebras over  $\mathbf{Q}$* , Comput. Complexity 2 (1992), 225–243.
- [84] L. Rónyai, *Computations in associative algebras*, DIMACS Series in Discrete Mathematics and Theoretical Computer Science, vol. 11, 1993.
- [85] L. Rónyai, *A deterministic algorithm to compute splitting elements in simple algebras over  $\mathbf{Q}$* , J. Algorithms 16 (1994), 24–32.
- [86] O.F.G. Schilling, *The Theory of Valuations*, A.M.S. Mathematical Surveys, vol. 4, 1950.
- [87] M. Shaw and J.F. Traub, *On the number of multiplications for the evaluation of a polynomial and some of its derivatives*, JACM 21 (1974), 161–167.
- [88] V. Shoup, *Searching for primitive roots in finite fields*, Math. Comp. 58 (1992), 369–380.
- [89] B. Trager, *Algebraic factoring and rational function integration*, Proceedings of SYMSAC '76, (1976) 219–226.
- [90] B.M. Urazbaev, *On the discriminant of a cyclic number field of prime degree*, Izvestiya Akad. Nauk Kazah. SSR 97, (1950).
- [91] B.L. van der Waerden, *Algebra*, 7th ed., vol. 1. Springer-Verlag, New York, 1991.

- [92] P.J. Weinberger and L.P. Rothschild, *Factoring polynomials over algebraic number fields*, ACM Transactions on Mathematical Software 2 (1976), 335–350.
- [93] E. Weiss, *Algebraic Number Theory*, McGraw-Hill, New York, 1963.
- [94] H.C. Williams, *Some algorithms for solving  $x^q \equiv N \pmod{p}$* , Proceedings of the 3<sup>rd</sup> Southeastern Conference on Combinatorics, Graph Theory, and Computing, Florida Atlantic University (1972), 451–462.
- [95] K.S. Williams and K. Hardy, *A refinement of H.C. Williams'  $q$ -th root algorithm*, Math. Comp. 61 (1993), 475–483.
- [96] D.Y.Y. Yun, *Algebraic algorithms using  $p$ -adic constructions*, Proceedings of the 1976 ACM Symposium on Symbolic and Algebraic Computation, 1976, 248–259.
- [97] D.Y.Y. Yun, *Hensel meets Newton – Algebraic constructions in an analytic setting*, Analytic Computational Complexity. (J.F. Traub ed.), Academic Press, New York, 1976.
- [98] H. Zassenhaus, *Ein Algorithmus zur Berechnung einer Minimalbasis über gegebener Ordnung*, Funktionalanalysis, Approximationstheorie, numerische Mathematik, Oberwolfach 1965 (L. Collatz, G. Meinardus, and H. Unger, eds.), Birkhäuser, Basel, 1967, 90–103.
- [99] H. Zassenhaus, *On Hensel factorization I*, J. Number Theory 1 (1969), 291–311.
- [100] R. Zippel, *Effective Polynomial Computation*, Kluwer Academic Publisher, Boston Dordrecht London, 1993.

**END**

**3 1 - 0 5 - 9 | 6**

**FIN**