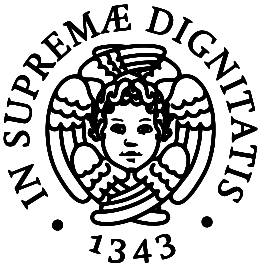


Università di Pisa

Corso di Laurea Magistrale in Matematica
Tesi di Laurea Magistrale

Factoring polynomials over $\mathbb{Z}/(n)$

Candidato:
Carlo Sircana

Relatori:
Prof.ssa Patrizia Gianni
Dott. Enrico Sbarra

Controrelatore:
Prof. Roberto Dvornicich

Anno Accademico 2015/2016

Contents

Introduction

The problem of factoring polynomials is one of the main issues of computational algebra and has been successfully solved for polynomials with coefficients in rings such as the integers $\mathbb{Z}$ and the finite fields $\mathbb{F}_q$. In this thesis, we deal with the problem of factoring polynomials over quotient rings of $\mathbb{Z}$. This topic has applications in coding theory, in some generalizations of cyclic codes, but it is also interesting for its own sake. For instance, it is linked by means of Hensel's lemma to the factorization of polynomials over p-adic fields and some other main issues of algebraic number theory. We deal with this connection in the first chapter. First of all, we clarify what being irreducible means over $\mathbb{Z}/(n)$ and we reduce ourselves, using the Chinese Remainder Theorem, to the case of a polynomial over $\mathbb{Z}/(p^l)$, where p is a prime factor of n. Then we give a constructive proof of the famous Hensel's lemma, that allows us to lift a factorization with coprime factors over $\mathbb{Z}/(p)$ to a factorization over $\mathbb{Z}/(p^l)$. We show that Hensel's lemma allows us to reduce factorization to the case of a monic polynomial. Another important consequence of Hensel's lemma is the uniqueness of the factorization it provides, even if the factors are not necessarily irreducible. Moreover, since the splitting obtained in this way coincides with the irredundant primary decomposition of the ideal generated by the polynomial, we can also assume that f is a primary polynomial, i.e. a (monic) polynomial of the form $f \equiv \phi^k \pmod{p}$ where ϕ is irreducible modulo p.

These first theorems present a relation between factorization over $\mathbb{Z}/(p^l)$ and over the p-adic integers. This leads us, in the second chapter, to the study of one of the main tools for p-adic factorization: Newton polygons. p-adic fields are naturally endowed with a discrete valuation and Newton polygons exploit this property to relate the values of the coefficients of a polynomial to its irreducibility. The values of the coefficients are used to construct a polygon in $\mathbb{R}^2$; if this polygon has two different sides, the polynomial splits over the p-adics and hence over $\mathbb{Z}/(p^l)$. Indeed, the roots of an irreducible polynomial have all the same valuations and the slope of the sides are related to the valuation of the roots. In the last section of the chapter, we give a brief description of the algorithm for factoring polynomials to obtain a deeper understanding of how Newton polygons are used in this context. The idea lying behind the algorithm is to find a sequence of polynomials in order to give a certificate for the irreducibility. The certificate for the irreducibility of a polynomial f is given by an integral basis of the ring of integers of the field generated by one of the roots of f. Given this background information, in the third chapter we describe the state of the art for factoring polynomials over $\mathbb{Z}/(n)$. In particular, we illustrate the ideas of the algorithm by Von Zur Gathen and Hartlieb [10] and

the improvements made by Cheng and Labahn [6] to find all the factorizations over $\mathbb{Z}/(n)$, assuming some conditions on n depending on the discriminant of the polynomial. The algorithm is based on the fact that all the factorizations of f over $\mathbb{Z}/(p^l)$ with l sufficiently large can be obtained from the computation of the factorization of f over the ring of the p-adic integers. Indeed, the refined form of Hensel's lemma presented in the first chapter assures that all the factorizations can be lifted; the main additional ingredient of this algorithm is the computation of a Smith normal form, which is used to compute the kernel of a matrix over $\mathbb{Z}/(p^l)$.

However, in the algorithm given by Von Zur Gathen and Hartlieb [10] the factors of f are processed two at a time. The improvements given in [6] address this problem; the authors present a generalized form of the resultant in order to process all factors at once. In spite of the efficiency of this method, it does not provide a complete solution because of the restrictions on the discriminant of the polynomial.

A different approach was presented by Sălăgean [21], who gives an algorithm to compute a factorization of a polynomial over $\mathbb{Z}/(p^2)$, where $p \in \mathbb{N}$ is a prime number, with no restrictions on the discriminant of the polynomial. First of all, she gives an easy irreducibility criterion and then she notices that every primary reducible polynomial over $\mathbb{Z}/(p^2)$ admits a particular kind of factorization which has at most 2 distinct factors. She shows that this factorization has the maximum number of total factors and the minimum number of distinct irreducible factors over all possible factorizations. Exploiting this fact, she finds all the factorizations of a polynomial having the maximum number of factors.

Her point of view has inspired our work, presented in the fourth chapter. We generalize the results of her article with two different interpretations of the irreducibility criterion for polynomials over $\mathbb{Z}/(p^2)$, and we present two other independent proofs of the criterion, one using the theory of Newton polygons, the other using Dedekind's Criterion. Our work on the first approach consists of a generalization of Newton polygons to the ring $\mathbb{Z}/(p^l)$. Whenever the valuation of the constant term of the polynomial is lower than l, all the results about Newton polygons still hold. We then give a necessary condition for the shape of a Newton polygon of an irreducible polynomial over $\mathbb{Z}/(p^l)$ and a partial criterion for determining whether or not a polynomial is irreducible over $\mathbb{Z}/(p^l)$. Furthermore, we speed up the computation of the lifting method given by Von Zur Gathen and Hartlieb in [11] by detecting the degrees of some of the factors before starting the computations.

Our second approach is related to Dedekind's criterion, which gives a necessary and sufficient condition for a ring to be integrally closed. This relation leads us to the study of a link between the index of an order and irreducibility over $\mathbb{Z}/(p^l)$. Specifically, we identify the index as the main cause of the non uniqueness of the factorization, noticing that the index is related to the discriminant of the order and this provides a deeper understanding of irreducibility over $\mathbb{Z}/(p^l)$. Using Krasner's lemma, we find a formula to upper bound the minimum $l \in \mathbb{N}$ such that a polynomial irreducible over the p-adics is irreducible over $\mathbb{Z}/(p^l)$ and we apply these results to polynomials over $\mathbb{Z}/(p^3)$, combining the two different approaches.

Finally we remark that, although we were primarily interested in factoring polynomial over $\mathbb{Z}/(n)$, and we connected the search for factors to the factorization over the p-adics, many of the intermediate results can be generalized

from quotients of the p-adics to quotients of more general p-adic fields and so we decided to present those results in this more general setting.

CHAPTER 1

Factoring modular polynomials

Factoring polynomials is one of the main issues of computational algebra, as it is essential for solving problems such as computing the normalization and the decomposition of primes in integral extensions. It is also interesting from a theoretical point of view, since some invariants strictly related to polynomials are involved in problems of algebraic number theory. However, it is not an easy task; while the problem has already been solved over $\mathbb{Z}$, finite extensions of $\mathbb{Q}$ and over finite fields, there is still a lot to do for local fields and, unexpectedly, quotients of $\mathbb{Z}$. In this work, we will focus on the latter, presenting all the results already achieved and giving our contribution. More specifically, we will deal with the problem of finding all the factorizations of a univariate polynomial over such rings, exploiting the information given by the reduction in the residue field and in the completion, which is the reason why we are going to recall later in this chapter all the main results about valuations and completions that we will use in this work. Summarizing, the aim of the thesis is the following:

Given a polynomial $f \in \mathbb{Z}[x]$ and a positive integer $n \in \mathbb{N}$, find one or all the factorizations into irreducible factors of f over $\mathbb{Z}/(n)$

At first glance, this problem may seem easier than factoring over the other rings listed before since $\mathbb{Z}/(n)$ is a finite ring, but this is not the case because these rings are not UFDs and not domains. This is why the purpose of this work is not only to find one factorization but of all of them. Dealing with this problem, the presence of more than one factorization is only one of the issues that can occur, as the following example shows:

Example 1.1 (Shamir [22])**.** *Let $p, q \in \mathbb{N}$ be distinct prime numbers and consider the polynomial*

$$f = x \in \mathbb{Z}[x]$$

Unexpectedly, f is not irreducible mod pq and it can be factored as

$$f \equiv \frac{1}{p^2+q^2}(px+q)(qx+p) \pmod{pq}$$

because p^2+q^2 is invertible (neither p nor q divide it). This shows that the degree of each factor can be equal to the degree of the polynomial we are factoring.

To avoid problems such as the one in the example, we take advantage of the Chinese Remainder theorem. Indeed, consider the factorization into prime numbers of n

$$n = \prod_{i=1}^{r} p_i^{e_i}$$

Then, by the Chinese Remainder theorem, the coprimality of the p_i gives the isomorphism

$$\mathbb{Z}/(n)[x] \simeq \mathbb{Z}/(p_1^{e_1})[x] \times \ldots \times \mathbb{Z}/(p_r^{e_r})[x]$$

In order to find the factorizations of a polynomial over $\mathbb{Z}/(n)$, we can therefore reduce ourselves to find them over the factors $\mathbb{Z}/(p^l)$ by virtue of the following lemma:

Lemma 1.2. *Let $R_1, \ldots, R_n$ be commutative rings and let $f = (f_1, \ldots, f_n)$ be an element of their product $R_1 \times \cdots \times R_n$. f is irreducible if and only if there exists an index j such that f_j is irreducible in R_j and f_i is a unit in R_i for $i \neq j$.*

Proof. Assume that f is irreducible. If there are two indices j_1, j_2 such that f_{j_1} and f_{j_2} are not units, then we can split f as the product of

$$f = (1, 1, \ldots, f_{j_1}, 1, \ldots, 1) \cdot (f_1, \ldots, f_{j_1-1}, 1, f_{j_1+1}, \ldots, f_n)$$

and both factors are not invertible, contradicting the irreducibility of f. Therefore, all the components of f must be units except one, which must be irreducible in R_i. Otherwise, let i be the index corresponding to the non-unit component and let $f_i = gh$; then

$$f = (f_1, \ldots, f_{i-1}, g, f_{i+1}, \ldots, f_n) \cdot (1, \ldots, 1, h, 1, \ldots, 1)$$

To show the converse, it is enough to prove that an element satisfying the hypothesis is irreducible. Assume by contradiction that

$$f = (g_1, \ldots, g_n) \cdot (h_1, \ldots, h_n)$$

and let f_j be the non-unit component of f, which is by hypothesis irreducible. Then $f_j = g_j h_j$ and by the irreducibility of f_j we can assume without loss of generality that g_j is a unit. All the other components must be units and so the vector $(g_1, \ldots, g_n)$ is a unit, giving a contradiction. □

This lemma allows us to reduce to the case of a local ring, where the problem of factoring polynomials is less chaotic, because it is possible to bring the problem to the completion of $\mathbb{Z}$ with respect to a prime number p.

Remark 1.3. *As Shamir points out ([22]), this reduction depends on the possibility of factoring the integer n into prime powers. This is equivalent to find a factorization of n, which is a hard problem if n is large, even using efficient algorithms such as quadratic sieve, number field sieve and Lenstra's elliptic curve method. See [7] for further information.*

There is only one issue that can occur in this approach. Indeed, if the projection of the polynomial f on one of the factors is zero, f does not admit a factorization, as it follows from the characterization of the irreducible elements given in the lemma.

Example 1.4. *Consider the polynomial $f = 3x$ in the ring $\mathbb{Z}/(6)[x]$. By the Chinese Remainder theorem, we have the isomorphism:*

$$\begin{array}{ccc} \mathbb{Z}/(6)[x] & \longrightarrow & \mathbb{Z}/(2)[x] \times \mathbb{Z}/(3)[x] \\ 3x & \longmapsto & (x, 0) \end{array}$$

By the lemma above, $(x, 0)$ can not be written as a product of irreducible factors and therefore f does not admit a factorization. The cause of this problem is the number 3, which can be written as $3 = 3 \cdot 3$ and therefore it is not irreducible (and it can't be written as a product of irreducible factors).

When this happens, we can not solve our problem directly. Nevertheless, it is possible to return a partial factorization by considering the integer n' obtained by increasing the power of some of the primes dividing n, factoring f over $\mathbb{Z}/(n')$ and reducing the factorization mod n. More precisely, assume that $n = \prod_{i=1}^{s} p_i^{e_i}$ is the factorization of n into distinct prime numbers and write

$$f = g \cdot \prod_{i=1}^{s} p_i^{l_i}$$

where $l_i = 0$ if $p_i^{e_i} \nmid f$ and $l_i \geq e_i$ otherwise. Then consider

$$n' = \prod_{i=1}^{s} p_i^{\max\{l_i+1, e_i\}}$$

factor f mod n' and return this factorization reduced mod n.

Fortunately, when none of the projections of f mod $p_i^{e_i}$ is zero, then f admits a factorization into irreducible elements. It is enough to show that this happens in $\mathbb{Z}/(p^l)$, where $p \in \mathbb{N}$ is a prime number and $l \in \mathbb{N}$.

Observation 1.5. *In $\mathbb{Z}/(p^l)[x]$, for $l \geq 2$, the element p is both irreducible and prime. Indeed, the quotient by p is an integral domain and this proves that p is prime. Moreover, being irreducible means to be maximal among the principal ideals, and this clearly holds for p.*

Given an element f in $\mathbb{Z}/(p^l)$, let p^m be the maximum power of p that divides it and write $f = p^m g$, where g is a polynomial having at least one coefficient which is not divisible by p. Therefore g is not a zero divisor and this implies, by noetherianity, that g has an expression as a product of irreducible elements (see [2]). Hence

Proposition 1.6. *Let $f \in \mathbb{Z}/(n)[x]$ be a polynomial and let*

$$n = \prod_{i=1}^{s} p_i^{e_i}$$

be the factorization into prime numbers of n. If the projection of f on $\mathbb{Z}/(p_i^{e_i})[x]$ is not zero for every i, then f can be expressed as a product of irreducible factors (non necessarily unique).

1.1 Completions and p-adic fields

As we will use this language later, we recall some well-known results about completions and discrete valuations.

Definition 1.7. *Let R be a ring and let I be an ideal of R. We define the I-adic completion of R as the ring*

$$\hat{R}_I = \left\{ (a_0, a_1, \dots) \in \prod_{n \in \mathbb{N}} {}^{A}\!/_{I^n} \;\middle|\; a_i \equiv a_j \pmod{I^j} \ \forall i > j \right\}$$

We say that R is complete with respect to the I-adic topology if the natural map $R \to \hat{R}_I$ is an isomorphism (both algebraically and topologically).

In this work, we will deal mainly with the ring of p-adic integers and its integral extensions:

Definition 1.8. *Let $p \in \mathbb{N}$ be a prime number. We define the ring of p-adic integers $\mathbb{Z}_p$ as the completion of $\mathbb{Z}$ with respect to the ideal (p).*

Henceforth, we will consider only the ring of p-adic integers and its integral complete extensions. These rings are naturally endowed with a sort of "distance". $\mathbb{Z}_p$ and the other rings we will encounter are integral domains and we can consider their quotient fields. We endow them with a valuation:

Definition 1.9. *Let K be a field. A valuation v on K is a homomorphism from the multiplicative group of the field to the additive group of $\mathbb{R}$*

$$\begin{array}{rccc} v\colon & K^* & \longrightarrow & \mathbb{R} \\ & \alpha & \longmapsto & v(\alpha) \end{array}$$

such that $v(\alpha+\beta) \geq \min\{v(\alpha), v(\beta)\}$ for all $\alpha, \beta \in K^*$. In addition, if the image of the valuation is a discrete subgroup of $\mathbb{R}$, the valuation is called discrete.

Observation 1.10. *Let K be a field endowed with a discrete valuation v and let $\alpha, \beta \in K$. It is easy to see that, if $v(\alpha) > v(\beta)$, then $v(\alpha + \beta) = v(\beta)$.*

Example 1.11. *We describe a family of discrete valuations on $\mathbb{Q}$. Let $p \in \mathbb{N}$ be a prime number; given an element $\alpha \in \mathbb{Q}$, we express it as*

$$\alpha = p^s \frac{a}{b}$$

with $(a, p) = (b, p) = 1$ and $s \in \mathbb{Z}$. Choose $\lambda \in \mathbb{R}$; we define $v_{p,\lambda}(\alpha) = s \cdot \lambda$. These are essentially all the possible discrete valuations on $\mathbb{Q}$ (see [17]).

Given a discrete valuation, we can consider the subring of K given by element of K with positive valuation

$$\mathcal{O}_K = \{\alpha \in K^* \mid v(\alpha) \geq 0\} \cup \{0\}$$

This is usually called a discrete valuation ring (DVR) and it is a well-known fact that it is a one-dimensional local ring. The maximal ideal of $\mathcal{O}_K$ is always principal and we call one of its generator a uniformizing parameter. A discrete subgroup of $\mathbb{R}$ is a lattice, isomorphic to $\mathbb{Z}$ and a uniformizing parameter corresponds to an element such that its image under the valuation generates $v(K^*)$ and has non-negative valuation. If the field K is complete, then its valuation rings are too.

Definition 1.12. *Let K be a field endowed with a discrete valuation and let $\mathcal{O}_K$ be the corresponding discrete valuation ring. We define the residue field of $\mathcal{O}_K$ as the field obtained as the quotient of $\mathcal{O}_K$ by its maximal ideal.*

Example 1.13. *The ring $\mathbb{Z}_p$ of p-adic integer is a discrete valuation ring of its quotient field $\mathbb{Q}_p$. One of the valuations of $\mathbb{Q}_p$ whose ring is $\mathbb{Z}_p$ is the one that, given an element $\alpha \in \mathbb{Q}_p$ and considered its expression*

$$\alpha = \sum_{i \geq -n} a_i p^i \qquad\qquad a_i \in \{0, \dots, p-1\}$$

such that $a_{-n} \neq 0$, then $v(\alpha) = -n$. A uniformizing parameter is p, which is clearly an element with minimum positive valuation.
The same valuations restricted to $\mathbb{Q}$ give rise to the localizations $\mathbb{Z}_{(p)}$ of $\mathbb{Z}$, that are discrete valuation rings but not complete.

Remark 1.14. *Henceforth, we will always consider the valuation v on $\mathbb{Q}_p$ such that $v(p) = 1$.*

As we said before, we will consider finite (integral) extensions of $\mathbb{Z}_p$ and this is why we define the following

Definition 1.15. *A field K is a p-adic field if $K/\mathbb{Q}_p$ is a finite extension of fields.*

Let K be a p-adic field. The valuation considered on $\mathbb{Q}_p$ extends to a valuation on K, and this extension is unique:

Proposition 1.16. *Let L be an algebraic extension of a p-adic field K and let v be a discrete valuation on K. There is a unique extension of v to a valuation w on L such that $w|_K = v$. If in addition L/K is finite, then w is discrete and, given $\alpha \in K$,*

$$w(\alpha) = \frac{1}{n} v\Big(N_{L/K}(\alpha)\Big)$$

where $N_{L/K} \colon L \to K$ is the norm map.

Proof. See [17]. □

This proposition has a remarkable consequence. Given a p-adic field K, let $f \in K[x]$ be an irreducible polynomial and denote by $\alpha_1, \dots, \alpha_n$ its roots. Each root generates a p-adic field $K(\alpha_i)$ and there is an extension v_i of the valuation

v to each of these fields. Since the polynomial is irreducible, we know that for each pair of roots α_i, α_j there exists a K-automorphism τ_{ij} of $\overline{K}$ such that $\tau_{ij}(\alpha_i) = \alpha_j$. The composition $v_j \circ \tau_{ij}$ is an extension of v to $K(\alpha_i)$ and therefore $v_i = v_j \circ \tau_{ij}$ by the uniqueness of the extension. In particular, $v_i(\alpha_i) = v_j(\alpha_j)$; in other words, calling $\bar{w}$ the (unique) extension of v to $\overline{\mathbb{Q}}_p$, $\bar{w}(\alpha_i) = \bar{w}(\alpha_j)$ for all i, j.

Example 1.17. *One of the easiest application of this fact is that, if* $f = x^n + \sum_{i=0}^{n-1} a_i x^i$ *is an irreducible polynomial, then* $\bar{w}(a_0) = n\bar{w}(\alpha)$*, where* α *is one of the roots of* f*.*

The extension property allows us to define a numerical invariant related to every extension of fields. Indeed, given a field K with a discrete valuation v and a finite extension L, we know that there is a unique extension w of v and w is still discrete. Therefore we obtain in this way two different discrete subgroup of $\mathbb{R}$, both isomorphic to $\mathbb{Z}$. The cardinality of the quotient must be finite and we get the following definition:

Definition 1.18. *Let* K *be a* p*-adic field with a discrete valuation* v *and let* L/K *be a finite field extension. If* w *is the extension of* v *to* L*, we define the ramification index* $e(L/K)$ *as*

$$e(L/K) = [w(L^*) : v(K^*)]$$

where L^*, K^* *are the multiplicative groups of* L *and* K *respectively.*

Another numerical invariant that we can associate with a finite extension of p-adic fields is the inertia degree. Let K be a p-adic field and let L/K be a finite extension of fields; denote by $\mathcal{O}_K$ and $\mathcal{O}_L$ their valuation rings. The extension of their residue fields is necessarily finite. Indeed, given linearly independent elements $\bar{\alpha}_1, \ldots, \bar{\alpha}_n$ on the residue fields, any of their lifts to L are still independent. This means that the degree of the extension is bounded by $[L : K]$.

Definition 1.19. *Let* K *be a* p*-adic field and* L/K *be a finite extension of fields. Let* k_L *and* k_K *be the residue fields of* L *and* K*. We define the inertia degree* $f(L/K)$ *as the degree of the extension of the residue fields:*

$$f(L/K) = [k_L : k_K]$$

Observation 1.20. *With the same notations as above,* $L/\mathbb{Q}_p$ *is a finite extension and therefore the residue field of* L *is a finite extension of* $\mathbb{Z}/(p)$*. In particular, the residue field of any* p*-adic field is finite and every finite* p*-adic extension of fields corresponds to an extension of finite fields, which is always separable. This fact allows us to use the primitive element theorem on the residue fields.*

The numerical invariants we have just defined are strictly related to the degree of the extension and the following theorem shows that they generalize the ramification theory for finite extensions of $\mathbb{Q}$ (see [14]).

Theorem 1.21. *Let* L/K *be a finite extension of* p*-adic fields. Let* $\alpha \in L$ *be a uniformizing parameter of* L *and let* $\beta \in L$ *be a lift of a primitive element of*

the extension of the residue fields. Calling $\mathcal{O}_K$ and $\mathcal{O}_L$ the valuation rings of K and L, it holds

$$\mathcal{O}_L = \mathcal{O}_K[\alpha, \beta]$$

and $\mathcal{O}_L$ is integral over $\mathcal{O}_K$. Furthermore,

$$[L : K] = e(L/K) \cdot f(L/K)$$

Proof. $\mathcal{O}_L$ is integral and finite over $\mathcal{O}_K$ by [17], Chap. 2, Th. 4.8. We show that the set $\alpha^i \beta^j$ for $i = 0, \dots, e(L/K)-1$ and $j = 0, \dots, f(L/K)-1$ is a free set of generators for $\mathcal{O}_L$ as a $\mathcal{O}_K$-module. The formula about degree, ramification index and inertia degree follows easily. Let M be the $\mathcal{O}_K$-module generated by the elements $\alpha^i \beta^j$ and denote by N the module generated by the β^j. Notice that $\mathcal{O}_L = N + \alpha\mathcal{O}_L$. Indeed, modulo α every element can be written as a linear combination of the β^j and therefore we get the equality. If $e = e(L/K)$, then iteratively

$$\begin{aligned} \mathcal{O}_L &= N + \alpha\mathcal{O}_L \\ &= N + \alpha(N + \alpha\mathcal{O}_L) \\ &= \dots \\ &= N + \alpha N + \dots + \alpha^{e-1}N + \alpha^e\mathcal{O}_L \end{aligned}$$

By the definition of M, the latter is equal to $M + \alpha^e\mathcal{O}_L$. Now we notice that $\alpha^e\mathcal{O}_L = \pi\mathcal{O}_L$, where π is a uniformizing parameter of $\mathcal{O}_K$. Indeed, $e \cdot v(\alpha) = v(\pi)$ and this means that there exists $\omega \in \mathcal{O}_L^*$ such that $\omega\alpha^e = \pi$, so that $\pi\mathcal{O}_L = \alpha^e\mathcal{O}_L$. Then

$$\mathcal{O}_L = M + \pi\mathcal{O}_L$$

and Nakayama's Lemma implies that $\mathcal{O}_L = M$, as desired. □

Definition 1.22. *By virtue of the theorem above, we call the valuation ring of a p-adic field K the ring of integers of K. Furthermore, we call an integral basis of $\mathcal{O}_L$ over $\mathcal{O}_K$ any basis of $\mathcal{O}_L$ as a $\mathcal{O}_K$-module.*

The previous theorem tells us that, working in p-adic field, the ring of integers can always be generated by 2 elements. However, we can show that a better result can be achieved:

Proposition 1.23. *Let L/K be a finite p-adic field extension and let $\mathcal{O}_K$ and $\mathcal{O}_L$ be the rings of integers of L and K. Then there exists $\gamma \in \mathcal{O}_L$ such that $\mathcal{O}_L = \mathcal{O}_K[\gamma]$.*

Proof. By the previous theorem, we know that $\mathcal{O}_L = \mathcal{O}_K[\alpha, \beta]$, where α is a uniformizing parameter of L and β is a lift of a primitive element of the extension of the residue fields. Let $f \in \mathcal{O}_K[x]$ be a monic lift of the minimal polynomial of $\bar{\beta}$. Then

$$f(\alpha + \beta) \equiv f(\beta) + \alpha f'(\beta) \pmod{\alpha^2}$$

Notice that $f'(\beta) \not\equiv 0 \pmod{\alpha}$ because f is separable and that $f(\beta) \equiv 0 \pmod{\alpha}$ and therefore $f(\beta)$ is not invertible. We distinguish two cases:

- if $f(\beta)$ has the same valuation of α, then $f(\beta)$ is a uniformizer and $\mathcal{O}_K[\alpha, \beta] = \mathcal{O}_K[\beta]$. It is enough to choose $\gamma = \beta$.

- if $f(\beta)$ has greater valuation, then $f(\beta) \equiv 0 \pmod{\alpha^2}$ and

$$f(\beta + \alpha) \equiv \alpha f'(\beta) \pmod{\alpha^2}$$

This means that $f(\alpha+\beta)$ is a uniformizer (its valuation is the same as α) and the projection of $\alpha+\beta$ on the residue field is β, so $\gamma = \alpha+\beta$ generates $\mathcal{O}_L$.

□

One of the most important theorem that holds in the context of ring of integers is Hensel's Lemma, which gives a sufficient condition to lift a factorization from the residue field to the ring.

Theorem 1.24 (Hensel's Lemma)**.** *Let (R, m) be a complete local ring with residue field k and $f \in R[x]$ be a monic polynomial. Let $g, h \in k[x]$ be monic polynomials such that $(g, h) = 1$ and*

$$f \equiv gh \pmod{m}$$

Then there exist unique monic polynomials $G, H \in R[x]$ such that $(G, H) = 1$, $f = GH$ and

$$G \equiv g \pmod{m} \qquad\qquad H \equiv h \pmod{m}$$

This theorem is crucial in understanding what happens over the p-adic integers and provides an easy tool to obtain a factorization over the p-adics and $\mathbb{Z}/(p^n)$. The proof is constructive and the coprimality requirement plays a key role in it: the idea is to lift a factorization over R/m^n to one over R/m^{n+1}. Uniqueness follows from the fact that the ring is complete with respect to the topology induced by the maximal ideal. We will prove the theorem with the additional hypothesis that the maximal ideal of R is principal, generated by an element π. The proof without this assumption is conceptually the same, but notations become heavy.

Proof. We give an inductive method in order to obtain the desired factorization. Assume that a factorization

$$f \equiv G_n \cdot H_n \pmod{\pi^n}$$

is given, such that $(G_n, H_n) = 1$ over $R/(\pi^n)$. We want to lift this factorization mod π^{n+1}, preserving the same properties. Let $G_{n+1}, H_{n+1} \in R/(\pi^{n+1})[x]$ be polynomials such that

$$G_{n+1} \equiv G_n + \pi^n u \pmod{\pi^{n+1}} \qquad H_{n+1} \equiv H_n + \pi^n r \pmod{\pi^{n+1}}$$

We want to determine $u \in R/(\pi^{n+1})[x]$ and $r \in R/(\pi^{n+1})[x]$ in order to obtain $f \equiv G_{n+1}H_{n+1} \pmod{\pi^{n+1}}$:

$$f - G_{n+1}H_{n+1} \equiv f - G_nH_n - \pi^n(uH_n + rG_n) \pmod{\pi^{n+1}}$$

Let $\gamma \in R/(\pi^{n+1})[x]$ such that $\pi^n\gamma \equiv f - G_nH_n \pmod{\pi^{n+1}}$. The equation

$$\gamma \equiv uH_n + rG_n \pmod{\pi}$$

admits solutions since by hypothesis H_n, G_n are coprime and therefore we have lifted the factorization.
Now, we show that these lifts are coprime. We know that G_n, H_n are coprime over $R/(\pi^n)$, so there exist $s, t \in R/(\pi^n)[x]$ such that

$$s \cdot G_n + t \cdot H_n \equiv 1 \pmod{\pi^n}$$

Let $\xi \in R/(\pi^{n+1})[x]$ such that

$$s \cdot G_n + t \cdot H_n \equiv 1 + \pi^n \xi \pmod{\pi^{n+1}}$$

We want to show that we can lift s, t in order to obtain the Bezout's identity between G_{n+1} and H_{n+1}, so to determine $\delta, \eta \in R/(\pi^{n+1})[x]$ such that

$$(s + \pi^n \delta)G_{n+1} + (t + \pi^n \eta)H_{n+1} \equiv 1 \pmod{\pi^{n+1}}$$

Substituting the expression for G_{n+1} and H_{n+1}, we get

$$1 + \pi^n \xi + \pi^n \delta G_n + \pi^n us + \pi^n \eta H_n + \pi^n rt \equiv 1 \pmod{\pi^{n+1}}$$

Therefore

$$\delta G_n + \eta H_n \equiv -\xi - us - rt \pmod{\pi}$$

and the equation has solution since G_n, H_n are coprime.
Using this inductive procedure, we can construct coherent sequences $G_i \in R/(\pi^i)[x]$, $H_i \in R/(\pi^i)[x]$ which have limits $G, H \in R[x]$ by the definition of completion, as desired.
We need to prove the uniqueness of G, H. Assume that $\widetilde{G}, \widetilde{H} \in R[x]$ are other polynomials that satisfy the hypotheses. There exist $a, b \in R[x]$ such that

$$\widetilde{G} = G + \pi a \qquad\qquad \widetilde{H} = H + \pi b$$

with $\deg a < \deg G$ and $\deg b < \deg H$. By these expressions,

$$GH = \widetilde{G}\widetilde{H} = GH + \pi(aH + bG) + \pi^2 ab \Rightarrow aH + bG + \pi ab = 0$$

In particular, $aH + bG \equiv 0 \pmod{\pi}$ and the degree conditions imply $a \equiv 0 \pmod{\pi}$ and $b \equiv 0 \pmod{\pi}$. We have shown that $G \equiv \widetilde{G} \pmod{\pi^2}$ and $H \equiv \widetilde{H} \pmod{\pi^2}$; by induction, we get the thesis. □

Example 1.25. *We consider the polynomial $f = x^2 + 5x + 2$ over $\mathbb{Z}/(4)$. Notice that this ring is trivially complete and so Hensel's Lemma holds. We want to find a factorization of f by means of Hensel's Lemma. Over the residue field (which is $\mathbb{Z}/(2)$), f projects to the polynomial*

$$f \equiv x^2 + 5x + 2 \equiv x^2 + x \equiv x(x + 1) \pmod{2}$$

We have to lift this factorization to $\mathbb{Z}/(4)$, so we need to find s, t such that

$$(x + 1 + 2s)(x + 2t) \equiv x^2 + 5x + 2 \pmod{4}$$

Therefore,

$$x^2 + x + 2(xs + (x+1)t) \equiv x^2 + 5x + 2 \pmod{4} \Rightarrow\ xs + (x+1)t \equiv 1 \pmod{2}$$

We solve this equation by means of Bezout's identity:

$$(x+1)+x \equiv 1 \pmod 2$$

which tells us that $s = 1$ *and* $t = 1$ *are solutions. We have obtained the following factorization:*

$$f \equiv (x-1)(x+2) \pmod 4$$

as desired.

We still have two concepts to recall that we will use in the following chapters: the different and the discriminant. These tools are essential in the study of ramification:

Definition 1.26. *Let* L/K *be a finite* p*-adic field extension of degree* n *and let* $p \in \mathbb{N}$ *be the characteristic of the residue field of* K*. We say that* L/K *is*

- *unramified if* $f(L/K) = n$ *(so that* $e(L/K) = 1$*)*
- *totally ramified if* $e(L/K) = n$
- *tamely ramified if* $(e(L/K), p) = 1$
- *wildly ramified if* $p \mid e(L/K)$

Observation 1.27. *Notice that being tamely or wildly ramified does not imply that the extension is totally ramified.*

Example 1.28. *Let* K *be the* 3*-adic field obtained by adding a root of the polynomial* $f = x^2 + 1$ *to* $\mathbb{Q}_3$*.* f *is irreducible mod* 3 *so the extension of the residue fields has degree* 2*, i.e.* $f(K/\mathbb{Q}_p) = 2$*. Therefore the extension* $K/\mathbb{Q}_p$ *is unramified.*

Example 1.29. *Let* $n \in \mathbb{N}$ *and consider the* 2*-adic field* K_n *obtained by adding a root of the polynomial* $f_n = x^n + 2$ *to* $\mathbb{Q}_2$*. Notice that* f_n *is irreducible for all* $n \in \mathbb{N}$ *by Eisenstein's criterion. If we consider the normalized valuation on* $\mathbb{Q}_2$ *(*$v(2) = 1$*) and its unique extension to the algebraic closure, the valuation of the constant term is* 1 *and, by proposition 1.16, the valuation of each root of* f_n *is* $1/n$*. The definition of index of ramification implies that* $n \mid e(L/K)$ *and by degree reasons equality holds. This means that the extension generated by a root of* f_n *is always totally ramified. Furthermore, if* $2 \mid n$*, the extension is wildly ramified, while if* $2 \nmid n$*, the extension is tamely ramified.*

Given an extension of p-adic fields L/K, it is always possible to split it in three parts:

Proposition 1.30. *Let* L/K *be an extension of* p*-adic fields. There exist* U*,* F *subextensions of* L/K

$$\begin{array}{l} L \\ \Big| \ \textit{wild and totally ramified} \\ F \\ \Big| \ \textit{tame and totally ramified} \\ U \\ \Big| \ \textit{unramified} \\ K \end{array}$$

such that U/K is unramified, F/U is totally and tamely ramified and L/F is totally and wildly ramified.

Definition 1.31. *Let R be a Dedekind domain with fraction field K. A R-module $M \subseteq K$ is a fractional ideal if there exists $d \in R\backslash\{0\}$ such that $d \cdot M \subseteq R$.*

Fractional ideals of a Dedekind domain form a group with respect to the product; this follows directly from the unique decomposition of the ideals into a product of prime ideals in a Dedekind domain (see [2]).
Given an extension of p-adic fields L/K, we consider the set

$$(\mathcal{O}_L)^* = \left\{ \alpha \in L \;\middle|\; \mathrm{Tr}_{L/K}(\alpha \mathcal{O}_L) \subseteq \mathcal{O}_K \right\}$$

This $\mathcal{O}_L$-module is a fractional ideal and $(\mathcal{O}_L)^* \supseteq \mathcal{O}_L$. Therefore, its inverse is a proper ideal of $\mathcal{O}_L$:

Definition 1.32. *Let L/K be a p-adic field extension. We define the different $\mathcal{D}_{L/K}$ as the inverse of the fractional ideal $(\mathcal{O}_L)^*$.*

The different is an ideal of the ring $\mathcal{O}_L$, which is a discrete valuation ring. Therefore, if $\alpha \in \mathcal{O}_L$ is a uniformizing parameter, $\mathcal{D}_{L/K}$ coincides with an ideal generated by α^s for a certain $s \in \mathbb{N}$. We can relate this number to the type of ramification:

Proposition 1.33. *Let L/K be a p-adic field extension of degree n and let α be a uniformizer element of $\mathcal{O}_L$. Let $s \in \mathbb{N}$ such that $\mathcal{D}_{L/K} = (\alpha^s)$. Denoting by e the ramification index of L/K, it holds:*

- *if L/K is tamely ramified, $s = e - 1$*
- *if L/K is wildly ramified, then $e \leq s \leq e - 1 + v_P(e)$*

In particular, if L/K is unramified then $\mathcal{D}_{L/K} = (1)$.

Proof. See [17] or [23]. □

The other numerical invariant that we define is the discriminant:

Definition 1.34. *Let L/K be a separable field extension of degree n and let $\alpha_1, \ldots, \alpha_n \in L$. Consider all the embeddings $\sigma_1, \ldots, \sigma_n \colon L \to \overline{L}$ of L over K, so that $\sigma_i|_K = \mathrm{Id}$. We define the discriminant of $\alpha_1, \ldots, \alpha_n$ as*

$$\begin{aligned} \mathrm{disc}(\alpha_1, \ldots, \alpha_n) &= \det \begin{pmatrix} \sigma_1(\alpha_1) & \sigma_2(\alpha_1) & \ldots & \sigma_n(\alpha_1) \\ \sigma_1(\alpha_2) & \sigma_2(\alpha_2) & \ldots & \sigma_n(\alpha_2) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_1(\alpha_n) & \sigma_2(\alpha_n) & \ldots & \sigma_n(\alpha_n) \end{pmatrix}^2 \\ &= \det \begin{pmatrix} \mathrm{Tr}(\alpha_1^2) & \mathrm{Tr}(\alpha_1\alpha_2) & \ldots & \mathrm{Tr}(\alpha_1\alpha_n) \\ \mathrm{Tr}(\alpha_1\alpha_2) & \mathrm{Tr}(\alpha_2^2) & \ldots & \mathrm{Tr}(\alpha_2\alpha_n) \\ \vdots & \vdots & \ddots & \vdots \\ \mathrm{Tr}(\alpha_1\alpha_n) & \mathrm{Tr}(\alpha_2\alpha_n) & \ldots & \mathrm{Tr}(\alpha_n^2) \end{pmatrix} \end{aligned}$$

The separability assumption is crucial, since it is the necessary condition for the trace to be non-zero (see [4]). We notice that the discriminant is zero if and only if $\alpha_1, \ldots, \alpha_n$ are linearly dependent over K.

Example 1.35. *We consider the splitting field K of $f = x^2 + 1$ and the field extension $K/\mathbb{Q}_3$. We denote by ζ_4 a 4-th primitive root of unity, so that $K = \mathbb{Q}_3(\zeta_4)$. We want to compute the discriminant of $1, \zeta_4$. By definition,*

$$\operatorname{disc}(1, \zeta_4) = \det \begin{pmatrix} 1 & 1 \\ \zeta_4 & -\zeta_4 \end{pmatrix}^2 = (-2\zeta_4)^2 = -4$$

Now we want to relate the discriminants of two different n-tuples of linearly independent elements $\alpha_1, \ldots, \alpha_n$ and $\beta_1, \ldots, \beta_n$. We can find a linear combination of the β_i such that

$$\alpha_j = \sum_{i=1}^{n} m_{ij}\beta_i$$

Denote by M the matrix

$$\begin{pmatrix} m_{11} & m_{12} & \ldots & m_{1n} \\ m_{21} & m_{22} & \ldots & m_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ m_{n1} & m_{n2} & \ldots & m_{nn} \end{pmatrix}$$

Then

$$\begin{pmatrix} \sigma_1(\alpha_1) & \sigma_2(\alpha_1) & \ldots & \sigma_n(\alpha_1) \\ \sigma_1(\alpha_2) & \sigma_2(\alpha_2) & \ldots & \sigma_n(\alpha_2) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_1(\alpha_n) & \sigma_2(\alpha_n) & \ldots & \sigma_n(\alpha_n) \end{pmatrix} = M \cdot \begin{pmatrix} \sigma_1(\beta_1) & \sigma_2(\beta_1) & \ldots & \sigma_n(\beta_1) \\ \sigma_1(\beta_2) & \sigma_2(\beta_2) & \ldots & \sigma_n(\beta_2) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_1(\beta_n) & \sigma_2(\beta_n) & \ldots & \sigma_n(\beta_n) \end{pmatrix}$$

so that

$$\operatorname{disc}(\alpha_1, \ldots, \alpha_n) = \det M^2 \cdot \operatorname{disc}(\beta_1, \ldots, \beta_n) \tag{1.1}$$

This formula has important consequence; indeed, let $\alpha_1, \ldots, \alpha_n$ and $\beta_1, \ldots, \beta_n$ be two integral basis of $\mathcal{O}_L$ over $\mathcal{O}_K$. The determinant of M is invertible in $\mathcal{O}_K$ and therefore the discriminants of the two n-tuples generate the same ideal.

Definition 1.36. *Let L/K be a finite extension of p-adic fields. We define the discriminant* $\operatorname{disc}(L/K)$ *as the ideal generated by the discriminant of an integral basis of $\mathcal{O}_L$ over $\mathcal{O}_K$.*

By the change of basis formula, the discriminants of any two n-tuples of linearly independent integral elements differ by a square. This fact is sometimes useful in order to prove that a set of n elements is an integral basis.

Example 1.37. *Over $\mathbb{Q}_5$, consider the polynomial $f = x^2 + 5$, which is irreducible by Eisenstein's criterion, and let K be its splitting field over $\mathbb{Q}_5$. Called α one of the roots of f,*

$$\operatorname{disc}(1, \alpha) = \det \begin{pmatrix} 1 & 1 \\ \alpha & -\alpha \end{pmatrix}^2 = -4 \cdot 5$$

4 is invertible and we can ignore it (we are interested in the ideal, not in the number!). Consequently, $\mathbb{Z}_p[\alpha]$ is integrally closed since 5 is not a square in $\mathbb{Q}_5$.

Definition 1.38. *Let L/K be a p-adic field extension and let $\alpha_1, \dots, \alpha_n \in \mathcal{O}_L$. Let $\beta_1, \dots, \beta_n \in \mathcal{O}_L$ an integral basis of $\mathcal{O}_L$. We define the index* $\mathrm{ind}(M)$ *of the $\mathcal{O}_K$-module M generated by $\alpha_1, \dots, \alpha_n$ in $\mathcal{O}_L$ as the ideal generated by the determinant of the change of coordinates matrix. In other words, it is the only ideal such that*

$$\mathrm{disc}(\alpha_1, \dots, \alpha_n) = \mathrm{ind}(M)^2 \, \mathrm{disc}(L/K)$$

The index controls how much a ring is near to be integrally closed and it is the main criterion in the algorithms for computing the normalization over a PID to understand when an integral basis has been found.

Definition 1.39. *Let L/K be an extension of p-adic fields of degree n and let $\mathcal{O}_K$ and $\mathcal{O}_L$ be their valuations ring. A ring $\mathcal{O}$ is an order if $\mathcal{O}_K \subseteq \mathcal{O} \subseteq \mathcal{O}_L$ and $\mathcal{O}$ is a free $\mathcal{O}_K$-module of rank n.*

Example 1.40. *Let $\mathcal{O}_K$ be the valuation ring of a p-adic field. Let $f \in \mathcal{O}_K[x]$ be a monic irreducible polynomial and denote by $\alpha \in \overline{\mathbb{Q}_p}$ one of its roots. Then $\mathcal{O}_K[x]/(f) \simeq \mathcal{O}_K[\alpha]$ is an order. In the next chapters, we will show when such an order coincides with the valuation ring and we will estimate its index.*

There exists a relation between discriminant and different:

Proposition 1.41. *Let L/K be a p-adic field extension. Then*

$$\mathrm{disc}(\mathcal{O}_L) = N_{L/K}(\mathcal{D}_{L/K})$$

Proof. See [23]. □

Example 1.42. *Consider the polynomial $f_n = x^n + p$ in $\mathbb{Q}_p[x]$ with $(n, p) = 1$. We have already seen that the extension K generated by one of its roots α is totally ramified. We want to compute the discriminant of the extension; in particular, it is enough to understand its valuation. Since the extension is totally ramified and the valuation of α is $1/n$ (with respect to the normalized valuation), $\mathcal{O}_K = \mathbb{Z}_p[\alpha]$. The extension is tamely ramified and we know that $\mathcal{D}_{K/\mathbb{Q}_p} = (\alpha^{n-1})$. To compute the discriminant, we use the last proposition and the norm map:*

$$v(N_{K/\mathbb{Q}_p}(\alpha^{n-1})) = (n-1)v(N_{K/\mathbb{Q}_p}(\alpha)) = (n-1)v(a_0) = (n-1)$$

This means that $\mathrm{disc}(K/\mathbb{Q}_p) = (p^{n-1})$.

The last relevant fact that we recall is the famous Krasner's lemma:

Theorem 1.43 (Krasner's Lemma)**.** *Let K be a p-adic field endowed with a discrete valuation v and let α, β be algebraic over K. Assume that for every immersion $\sigma\colon K(\alpha) \to \overline{K}$ such that $\sigma \neq Id$ holds*

$$v(\beta - \alpha) > v(\sigma(\alpha) - \alpha)$$

Then $K(\alpha) \subseteq K(\beta)$.

The proof of this lemma is essentially a consequence of the uniqueness of the extension of a valuation:

Proof. We want to show that every embedding $\sigma\colon K(\alpha,\beta) \to \overline{K}$ such that $\sigma|_{K(\beta)} = Id$ fixes α, i.e. $\sigma(\alpha) = \alpha$. We notice that, by the uniqueness of the extension of a valuation,

$$v(\beta - \sigma(\alpha)) = v(\sigma(\beta - \alpha)) = v(\beta - \alpha)$$

On the other hand,

$$v(\sigma(\alpha) - \alpha) = v(\sigma(\alpha) - \beta + \beta - \alpha) \geq \min\{v(\sigma(\alpha) - \beta), v(\beta - \alpha)\}$$

By hypothesis, if $\sigma \neq Id$, then $v(\beta - \alpha) > v(\sigma(\alpha) - \beta)$ and therefore, since they have different valuations, the equality holds:

$$v(\sigma(\alpha) - \alpha) = v(\sigma(\alpha) - \beta) = v(\beta - \alpha)$$

This gives a contradiction, so there can not exist a non-identical embedding. This means that $K(\alpha) \subseteq K(\beta)$, as desired. □

1.2 Hensel's Lemma and Factorization over $\mathcal{O}_K/(\pi^l)$

In this section, we are going to exploit some of the results we have presented about p-adic fields in order to obtain some basic facts about factorization over $\mathbb{Z}/(p^l)$. In particular, Hensel's Lemma will be use extensively in order to obtain a pre-processing algorithm for polynomials over these rings.

In the first part of this section, we show that it is always possible to reduce the problem to monic polynomials. To obtain this result, we need to strengthen Hensel's lemma. This generalization can be found in [10] but we are going to prove it in a more general setting, assuming that the ring R is a discrete valuation ring (not necessarily complete) with uniformizing parameter π such that its completion coincides with the ring of integers of a p-adic field.
A tool that we will use extensively is the resultant. Let $g, h \in R[x]$ be two polynomials over an integral domain, of degree n, m respectively. We write $g = \sum a_i x^i$ and $h = \sum b_i x^i$ and we consider the matrices

$$M_g = \overbrace{\begin{pmatrix} a_n & 0 & \dots & 0 \\ a_{n-1} & a_n & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ \vdots & \vdots & & a_n \\ \vdots & \vdots & & \vdots \\ a_0 & \vdots & & \vdots \\ & a_0 & & \vdots \\ & & \ddots & \vdots \\ & & & a_0 \end{pmatrix}}^{m} \qquad M_h = \overbrace{\begin{pmatrix} b_m & 0 & \dots & 0 \\ b_{m-1} & b_m & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ \vdots & \vdots & & b_m \\ \vdots & \vdots & & \vdots \\ b_0 & \vdots & & \vdots \\ & b_0 & & \vdots \\ & & \ddots & \vdots \\ & & & b_0 \end{pmatrix}}^{n}$$

obtained by writing the coordinates of the polynomial $x^i g$, $x^j h$ for $i = 0, \dots, m-1$ and $j = 0, \dots, n-1$ with respect to the basis $x^{n+m-1}, \dots, x, 1$.

Definition 1.44. *Let R be an integral domain and let $g, h \in R[x]$ be two polynomials of degree n, m respectively. We define the resultant* $\mathrm{Res}(g,h)$ *as the determinant of the following matrix*

$$S(g,h) = \left(\begin{array}{c|c} M_g & M_h \end{array} \right)$$

which is called the Sylvester matrix of g and h.

The resultant provides an easy method to compute the discriminant of an order generated by the root of a polynomial:

Proposition 1.45. *Let $f \in \mathcal{O}_K[x]$ be a monic irreducible polynomial of degree n and let α be one of its roots in an algebraic closure. Then*

$$\mathrm{disc}(1, \alpha, \ldots, \alpha^{n-1}) = \mathrm{Res}(f, f')$$

Proof. See [14]. □

Remark 1.46. *Henceforth, we will assume that R is a discrete valuation ring with uniformizing parameter π and $\hat{R}$ is its completion with respect to its maximal ideal.*

Since we are going to exploit the properties of the resultant in the cases of p-adic fields, we are interested in its valuation more than its precise value. As a matter of notation, we denote the valuation of the resultant $\mathrm{Res}(g,h)$ as r_{gh}.

Definition 1.47. *Let R be a discrete valuation ring and let M be a matrix with entries in R. We define the valuation $v(M)$ of M as the minimum of the valuations of its components.*

Definition 1.48. *Let R be a discrete valuation ring and let $g, h \in R[x]$ be two polynomials such that* $\det(S(g,h)) \neq 0$. *We define the reduced resultant s_{gh} of g, h as the opposite of the valuation of $S(g,h)^{-1}$*

$$s_{gh} = -v(S(g,h)^{-1})$$

Clearly, the reduced discriminant can be computed directly by the definition but it requires to invert a matrix. There is a more convenient method to determine it, using the Smith normal form:

Proposition 1.49. *Let $g, h \in R[x]$ be two polynomials of degrees n, m respectively such that* $\det(S(g,h)) \neq 0$ *and let D be the diagonal matrix*

$$D = \begin{pmatrix} d_1 & & & \\ & d_2 & & \\ & & \ddots & \\ & & & d_{n+m} \end{pmatrix}$$

obtained as the Smith normal form of $S(g,h)$ (so $d_1 \mid d_2 \mid d_3 \mid \cdots \mid d_{n+m}$). Then $s_{gh} = v(d_{n+m})$.

Proof. Let $P, Q \in GL(n, R)$ be two matrices such that

$$P \cdot D \cdot Q = S(g, h)$$

Then

$$S(g, h)^{-1} = Q^{-1} \cdot D^{-1} \cdot P^{-1}$$

Notice that Q^{-1}, P^{-1} have entries that lie in R and therefore their valuations are ≥ 0. Furthermore, there is an element in the last column of Q^{-1} not divisible by π because Q must be still invertible mod π; denote by i be the row index of this element. In the same way, there exists an element in the last row of P^{-1} not divisible by π; call j its column index. Then the element of $S(g, h)^{-1}$ in position (i, j) is such that its valuation is equal to $-v(d_{n+m})$. This proves that $s_{gh} \geq v(d_{n+m})$.
The other inequality is trivial, since every element of $S(g, h)^{-1}$ has valuation greater than $-v(d_{n+m})$ (notice that $-v(d_{n+m}) \leq -v(d_i)$ for all $i \leq n + m$) and therefore we get the equality. □

Proposition 1.50. *Let $g, h \in R[x]$ be two polynomials of degree n, m respectively and assume that the resultant $\operatorname{Res}(g, h)$ is different from zero. Let $b \in R$ such that $\operatorname{Res}(g, h) = \pi^{r_{gh}} b$. For all $\nu \in R[x]$ of degree $\deg \nu < n + m$ there exist unique $A, B \in R[x]$ such that*

$$\pi^{s_{gh}} b\nu = Ag + Bh$$

and $\deg A < m$, $\deg B < n$.

Proof. Write

$$\nu = \sum_{i=0}^{n+m-1} \nu_i x^i \qquad A = \sum_{i=0}^{m-1} A_i x^i \qquad B = \sum_{i=0}^{n-1} B_i x^i$$

We can consider the coefficients of A and B as the solution of the linear system

$$S(g, h) \begin{pmatrix} A_{m-1} \\ \vdots \\ A_0 \\ B_{n-1} \\ \vdots \\ B_0 \end{pmatrix} = \pi^{s_{gh}} b \begin{pmatrix} \nu_{n+m-1} \\ \vdots \\ \nu_0 \end{pmatrix}$$

By hypothesis, the determinant of $S(g, h)$ is non-zero and so the matrix is invertible in the quotient field of R. The relation becomes

$$\begin{pmatrix} A_{m-1} \\ \vdots \\ A_0 \\ B_{n-1} \\ \vdots \\ B_0 \end{pmatrix} = \pi^{s_{gh}} b S(g, h)^{-1} \begin{pmatrix} \nu_{n+m-1} \\ \vdots \\ \nu_0 \end{pmatrix}$$

Now, we notice that the entries of the matrix $\pi^{s_{gh}} S(g,h)^{-1}$ are in R since their valuation is equal or greater than zero by the definition of s_{gh} and therefore the same holds for the solution of the linear system, the coefficients of A, B. The uniqueness follows from the fact that $S(g,h)$ is invertible. □

Corollary 1.51. *Let $g, h \in R[x]$ be two polynomials of degree n, m respectively and assume that the resultant $\operatorname{Res}(g,h)$ is different from zero. For all $\nu \in \hat{R}[x]$ of degree $\deg \nu < n+m$ there exist unique $A, B \in \hat{R}[x]$ such that*

$$\pi^{s_{gh}} \nu = Ag + Bh$$

and $\deg A < m$, $\deg B < n$.

Proof. It is enough to use the same argument of the proof and notice that, in the same notations as the proposition, b is invertible in the completion. □

The corollary tells us that there exist $A, B \in \hat{R}[x]$ such that $Ag + Bh = \pi^{s_{gh}}$ and therefore s_{gh} gives us information about the elimination ideal of (g,h) in $\hat{R}[x]$. The following lemma shows that this information is sufficient to determine it:

Lemma 1.52. *Let $g, h \in R[x]$ be two polynomials such that $\operatorname{Res}(g,h) \neq 0$ and either $lc(g)$ or $lc(h)$ is not divisible by π. Then s_{gh} is minimal with respect to the property that there exist $A, B \in \hat{R}[x]$ such that*

$$Ag + Bh = \pi^{s_{gh}}$$

Proof. As we said before, we only need to prove the minimality of s_{gh}. Let $n = \deg g$ and $m = \deg h$ and assume by contradiction that there exist $A', B' \in \hat{R}[x]$ such that

$$A'g + B'h = \pi^{\sigma}$$

with $0 \leq \sigma < s_{gh}$. Without loss of generality, we can assume that the leading coefficient of g is not divisible by π, so that $lc(g)$ is a unit in $\hat{R}[x]$. Furthermore, we can assume that $\deg A' < m$ and $\deg B' < n$. Indeed, if $\deg B' \geq \deg g$, we can divide B' by g and $B' = qg + B''$ and $\deg B'' < \deg g = n$. Substituting,

$$A'g + (qg + B'')h = \pi^{\sigma} \implies (A' + qh)g + B''h = \pi^{\sigma}$$

and setting $A'' = A' + qh$, we reduce to the case that $\deg B'' < \deg h$. Since $\hat{R}[x]$ is an integral domain and the degree is additive, it must hold $\deg A'' < \deg g$. Exploiting this relation, for every $\nu \in \hat{R}[x]$ of degree $< n+m$ there exist $A_\nu, B_\nu \in \hat{R}[x]$ such that

$$A_\nu g + B_\nu h = \pi^{\sigma} \nu$$

with $\deg A_\nu < \deg h$ and $\deg B_\nu < \deg g$. We write

$$A_\nu = \sum_{i=0}^{m-1} A_{\nu,i} x^i \qquad B_\nu = \sum_{i=0}^{n-1} B_{\nu,i} x^i \qquad \nu = \sum_{i=0}^{n+m-1} \nu_i x^i$$

with $A_{\nu,i}, B_{\nu,i}, \nu_i \in \hat{R}$ and we get the linear system

$$S(g,h)\begin{pmatrix} A_{\nu,m-1} \\ \vdots \\ A_{\nu,0} \\ B_{\nu,n-1} \\ \vdots \\ B_{\nu,0} \end{pmatrix} = \pi^\sigma \begin{pmatrix} \nu_{n+m-1} \\ \vdots \\ \nu_0 \end{pmatrix}$$

Inverting $S(g,h)$, we get the relation

$$\begin{pmatrix} A_{\nu,m-1} \\ \vdots \\ A_{\nu,0} \\ B_{\nu,n-1} \\ \vdots \\ B_{\nu,0} \end{pmatrix} = \pi^\sigma S(g,h)^{-1} \begin{pmatrix} \nu_{n+m-1} \\ \vdots \\ \nu_0 \end{pmatrix}$$

If we set $\nu = x^i$, we get that the i-th column of $\pi^\sigma S(g,h)^{-1}$ has entries in $\hat{R}$. This means that $s_{gh} \leq \sigma$, as desired. □

Lemma 1.53. *Let $g, h, G, H \in R[x]$ be monic polynomials such that* $\operatorname{Res}(g,h) \neq 0$ *and*

$$g \equiv G \pmod{\pi^{s_{gh}+1}} \qquad h \equiv H \pmod{\pi^{s_{gh}+1}}$$

Then $s_{GH} = s_{gh}$.

Proof. Let $\sigma = s_{gh}$ and let $g_0, h_0 \in R[x]$ such that

$$G = g + \pi^{\sigma+1} g_0 \qquad H = h + \pi^{\sigma+1} h_0$$

First, we show that $\operatorname{Res}(G,H) \neq 0$. Indeed, if this is not the case, $S(G,H)$ is not invertible and there exist $A, B \in R[x]$ such that

$$AG + BH = 0$$

with $\deg(A) < \deg(G)$ and $\deg(B) < \deg(H)$ and either A or B not zero mod π. Then, using the expressions of G, H with respect to g, h we get

$$\begin{aligned} 0 &= AG + BH \\ &= A(g + \pi^{\sigma+1} g_0) + B(h + \pi^{\sigma+1} h_0) \\ &= Ag + Bh + \pi^{\sigma+1}(g_0 A + h_0 B) \end{aligned}$$

This means that there exists a polynomial $\mu \in R[x]$ of degree $\deg \mu < \deg g + \deg h$ such that $Ag + Bh = \pi^{\sigma+1}\mu$. However, the uniqueness of the coefficients A, B of proposition 1.50 implies that $A \equiv B \equiv 0 \pmod{\pi}$, contradicting the hypotheses. Consequently, we can suppose that $\operatorname{Res}(G,H) \neq 0$.
We know by the previous proposition that there are polynomials $A', B' \in \hat{R}[x]$ such that

$$A'g + B'h = \pi^\sigma$$

with $\deg A' < \deg h$ and $\deg B' < \deg g$. Therefore, substituting g, h with G, H, there is a polynomial $\nu \in \hat{R}[x]$ such that

$$A'G + B'H = \pi^\sigma + \pi^{\sigma+1}\nu = \pi^\sigma(1 + \pi\nu)$$

Since $(1+\pi\nu)$ is invertible over $R/(\pi^k)$ for every $k \geq 1$, we can find $A_0, B_0 \in R[x]$ such that

$$A_0G + B_0H \equiv \pi^\sigma \pmod{\pi^{s_{GH}+1}}$$

Assume by contradiction that $\sigma < s_{GH}$. By the last equation, we get

$$\pi^{s_{GH}-\sigma}A_0G + \pi^{s_{GH}-\sigma}B_0H \equiv \pi^{s_{GH}} \pmod{\pi^{s_{GH}+1}}$$

and there exists $\nu \in R[x]$ such that

$$\pi^{s_{GH}-\sigma}A_0G + \pi^{s_{GH}-\sigma}B_0H = \pi^{s_{GH}}(1 + \pi\nu)$$

Calling a_i, b_i, ν_i the coefficients of A_0, B_0, ν respectively, we can read into the relation the following linear system

$$\pi^{s_{GH}-\sigma}S(G,H)\begin{pmatrix} a_{m-1} \\ \vdots \\ a_0 \\ b_{n-1} \\ \vdots \\ b_0 \end{pmatrix} = \pi^{s_{GH}}\begin{pmatrix} \pi\nu_{n+m-1} \\ \vdots \\ \pi\nu_1 \\ 1+\pi\nu_0 \end{pmatrix}$$

Inverting $S(G,H)$ we get

$$\pi^{s_{GH}-\sigma}\begin{pmatrix} a_{m-1} \\ \vdots \\ a_0 \\ b_{n-1} \\ \vdots \\ b_0 \end{pmatrix} = \pi^{s_{GH}}S(G,H)^{-1}\begin{pmatrix} \pi\mu_{n+m-1} \\ \vdots \\ \pi\mu_1 \\ 1+\pi\mu_0 \end{pmatrix}$$

We want to show that the last column of $\pi^{s_{GH}}S(G,H)^{-1}$ is not divisible by π. Assume by contradiction that π divides every element of the last column of $\pi^{s_{GH}}S(G,H)^{-1}$. Then, the right-hand side is not divisible by π whereas the left is, giving a contradiction and proving that $\sigma \geq s_{GH}$. The same argument shows that $\sigma \leq s_{GH}$, proving the equality.
Suppose that the last column of $\pi^{s_{GH}}S(G,H)^{-1}$ is divisible by π; then

$$\pi^{s_{GH}-1}S(G,H)^{-1}e_n = \begin{pmatrix} \gamma_{m-1} \\ \vdots \\ \gamma_0 \\ \delta_{n-1} \\ \vdots \\ \delta_0 \end{pmatrix} \in \hat{R}^{n+m}$$

where e_n is the vector with 1 in the n-th position and 0 elsewhere. If $\gamma = \sum_{i=0}^{m-1} \gamma_i x^i$ and $\delta = \sum_{i=0}^{n-1} \delta_i x^i$, we get

$$\gamma G + \delta H = \pi^{s_{GH}-1}$$

and this gives a contradiction, because we stated in the previous lemma that $(G, H) \cap \mathcal{O}_K = (\pi^{s_{GH}})$. □

Theorem 1.54. *[Hensel's Lemma] Let $f, \mu, \nu \in R[x]$ be polynomials of degrees $n+m, n, m$ respectively such that*

- $f \equiv \mu\nu \pmod{\pi^l}$
- $lc(f) = lc(\mu\nu)$
- $lc(\mu) \not\equiv 0 \pmod{\pi}$
- $\mathrm{Res}(\mu, \nu) \neq 0$
- $k > 2s_{\mu\nu}$

Then there exist unique polynomials $g, h \in \hat{R}[x]$ (the completion of R with respect to the maximal ideal of R) such that

- $f = gh$ *in* $\hat{R}[x]$
- $g \equiv \mu \pmod{\pi^{l-s_{gh}}}$ *and* $h \equiv \nu \pmod{\pi^{l-s_{gh}}}$
- $lc(g) = lc(\mu)$ *and* $lc(h) = lc(\nu)$

Proof. Let $\sigma = s_{\mu\nu}$. We want to construct inductively a coherent sequence of polynomials A_i, $B_i \in R[x]$ such that

- $\deg(A_i) < m$, $\deg(B_i) < n$
- given a factorization $f \equiv GH \pmod{\pi^{l+i-1}}$ satisfying the hypothesis, then
$$f \equiv (G + \pi^{l-\sigma+i-1}B_i)(H + \pi^{l-\sigma+i-1}A_i) \pmod{\pi^{l+i}}$$

In these assumptions, we can write $f = GH + \pi^{l+i-1}\eta$, with $\eta \in R[x]$ and $\deg \eta < n+m$, because the leading coefficient of f coincides with the leading coefficient of GH. By the lemma, $s_{\mu\nu} = s_{GH}$ and we denote this quantity by σ. We know by proposition 1.50 that there are two polynomials $A_i, B_i \in R[x]$ such that

$$GA_i + HB_i \equiv \pi^\sigma \eta \pmod{\pi^{\sigma+1}}$$

Therefore, denoting by $\tau = l - \sigma + i - 1$, we get

$$\begin{aligned}(G + \pi^\tau B_i)(H + \pi^\tau A_i) &\equiv GH + \pi^\tau(GA_i + HB_i) + \pi^{2\tau}A_iB_i \\ &\equiv GH + \pi^\tau\pi^\sigma\eta + \pi^{2\tau}A_iB_i \\ &\equiv GH + \pi^{l+i-1}\eta = f \pmod{\pi^{2\tau}}\end{aligned}$$

Notice that by hypothesis, $2\tau \geq l + i$ and so we have constructed the sequence we wanted.

Summarizing, we have constructed two Cauchy sequences that give two polynomials $g, h \in \hat{R}[x]$ such that $f = gh$,

$$g = \mu + \sum_{i\geq 1} \pi^{l-\sigma+i-1} B_i \qquad\qquad h = \nu + \sum_{i\geq 1} \pi^{l-\sigma+i-1} A_i$$

and that satisfy the requirements.
We need to prove uniqueness. Assume that g, h and g', h' are two pairs of polynomials in $\hat{R}[x]$ fulfilling the requirements. Then we can write

$$g' = g + \pi^{l-s_{\mu\nu}} a \qquad\qquad h' = h + \pi^{l-s_{\mu\nu}} b$$

where $a, b \in \hat{R}[x]$. Using these relations,

$$\begin{aligned} gh = g'h' &= (g + \pi^{l-s_{\mu\nu}} a)(h + \pi^{l-s_{\mu\nu}} b) \\ &= gh + \pi^{l-s_{\mu\nu}}(bg + ah) + \pi^{2l-2s_{\mu\nu}} ab \end{aligned}$$

so that $(bg + ah) + \pi^{l-s_{\mu\nu}} ab = 0$. Therefore $bg + ah \equiv 0 \pmod{\pi^{l-s_{\mu\nu}}}$ and by the previous proposition $a \equiv b \equiv 0 \pmod{\pi^{l-2s_{\mu\nu}}}$. This means that $g \equiv g' \pmod{\pi^{2l-3s_{\mu\nu}}}$ and $h \equiv h' \pmod{\pi^{2l-3s_{\mu\nu}}}$. Since $2l - 3s_{\mu\nu} > l - s_{\mu\nu}$ by hypothesis, inductively we get the equality $g = g'$ and $h = h'$, as desired. □

Observation 1.55. *Notice that $2s_{\mu\nu} \leq v(\mathrm{disc}(f))$. Indeed,*

$$\begin{aligned} v(\mathrm{disc}(f)) &= v(\mathrm{Res}(f, f')) \\ &= v(\mathrm{Res}(\mu\nu, \mu'\nu + \mu\nu')) \\ &= v(\mathrm{Res}(\mu, \mu'\nu)) v(\mathrm{Res}(\nu, \mu\nu')) \\ &= v(\mathrm{Res}(\mu, \mu')) + v(\mathrm{Res}(\mu, \nu)) + v(\mathrm{Res}(\nu, \mu)) + v(\mathrm{Res}(\nu, \nu')) \\ &= v(\mathrm{disc}(\mu)) + v(\mathrm{disc}(\nu)) + 2 \cdot v(\mathrm{Res}(\mu, \nu)) \end{aligned}$$

By proposition 1.49, it follows that $v(\mathrm{Res}(\mu, \nu)) \geq s_{\mu\nu}$ and therefore it holds $v(\mathrm{disc}(f)) \geq 2s_{\mu\nu}$.

This general version of Hensel's lemma allows us to prove that we can reduce the problem of factoring polynomials over $R/(\pi^l)$ to monic polynomials:

Theorem 1.56. *Let $f \in R[x]$ be a polynomial of positive degree and let $k \in \mathbb{N}$. Then there exist $k \in \mathbb{N}$, $\nu, F \in R[x]$ such that*

- *the image of ν in $R/(\pi^l)[x]$ is a unit*
- *F is monic*
- *$f \equiv \pi^k \nu F \pmod{\pi^l}$*

Furthermore, the irreducible factors of f are the irreducible factors of F and, if $k \geq 1$, π.

Proof. First of all, we write $f \equiv \pi^k g \pmod{\pi^l}$ with $g \not\equiv 0 \pmod{\pi}$. Let $n = \deg g$ and m be the degree of its reduction mod π. Assume first that $n \neq m$. In this case, we set $\nu_0 = lc(g)x^{n-m} + g_m$ where g_m is the coefficient of the term of degree m of g, so that ν_0 is a unit mod π. With this choice, there exists a monic polynomial $F_0 \in R[x]$ such that $g \equiv \nu_0 F_0 \pmod{\pi}$, $\deg g = \deg \nu_0 + \deg F_0$ and $lc(g) = lc(\nu_0 F_0)$. Since ν_0 is a unit, $s_{F_0\nu_0} = 0$ and we can use Hensel's lemma 1.54 to get lifts ν, F that satisfy the requirements.
If $n = m$, the same argument works, considering $\nu_0 = lc(g)$. □

Therefore, given a polynomial $f \in R[x]$, we can always assume that f is monic and restrict the factors to be monic. Working with monic polynomials gives the advantage of the additivity law for the degree, so we will not encounter issues like the one in the Shamir's example presented at the beginning of this chapter. In particular, the maximum number of factors of a monic polynomial over $R/(\pi^l)$ is bounded by its degree and every linear monic polynomial is irreducible, assuming the factors are monic.
Having solved this first issue, we focus on the use of Hensel's lemma in order to factor a monic polynomial $f \in R[x]$. Fix a positive integer $l \in \mathbb{N}$ and assume that we want to factor the reduction of f mod π^l. Using Hensel's lemma 1.24 or 1.54, we reduce f mod π and factor it over the residue field, then we lift this factorization mod π^l. The proof of Hensel's lemma we gave before 1.54 is constructive and to obtain the corresponding factorization it is enough to repeat the same procedure of the proof. In the case of three or more factors, it is enough to the repeat the procedure for every factor inductively. For further information, see [7].

Example 1.57. *We consider the polynomial*

$$f = x^6 - 18x^5 - 280x^4 + 2x^3 - 35x^2 - 578x - 280 \in \mathbb{Z}[x]$$

We want to apply Hensel's lemma in order to factor f in $\mathbb{Z}/(27)[x]$. First of all, we factor f mod 3:

$$f \equiv (x^2+1)^2(x+1)(x-1) \pmod 3$$

Then, we lift this factorization to $\mathbb{Z}/(27)$ by virtue of Hensel's Lemma:

$$f \equiv (x^2+1)^2(x+10)(x-1) \pmod{27}$$

getting a factorization.

This factorization corresponds exactly to the irredundant primary decomposition of the ideal (f) in $R/(\pi^l)[x]$. We recall the fundamental facts about it, starting from the definition:

Definition 1.58. *Let R be a ring and $I \subseteq R$ an ideal. A primary decomposition of I is the expression of I as the intersection of primary ideals $Q_1, \ldots, Q_r$*

$$I = \bigcap_{i=1}^{r} Q_i$$

If $\sqrt{Q_i} \neq \sqrt{Q_j}$ for $i \neq j$ and $Q_i \not\supseteq \cap_{j\neq i} Q_j$ for all i, the decomposition is called minimal or irredundant.

Given a primary decomposition of an ideal I and taking radicals, we obtain prime ideals whose intersection is $\sqrt{I}$. We can distinguish two different types of such prime ideals:

Definition 1.59. *Let $I = \cap_{i=1}^{r} Q_i$ be an irredundant primary decomposition of an ideal I and let $P_i = \sqrt{Q_i}$. We say that P_i is minimal if it is minimal in the set of the prime ideals containing I, embedded otherwise.*

Furthermore, the following uniqueness result holds:

Theorem 1.60. *Let I be an ideal of a noetherian ring R. The primary components associated with the minimal prime ideals of I are uniquely determined.*

Proof. See [2]. □

We know that $R/(\pi^l)[x]$ is a noetherian ring and, under this hypothesis, a primary decomposition exists for every ideal. In order to use effectively the uniqueness theorem, we need to recall a relevant property of the primary decomposition due to the fact the dimension of the ring is one. More specifically, $R/(\pi^l)[x]$ is a one-dimensional ring and every ideal generated by an element which is not a zero-divisor can not have an embedded component. Indeed, denote by I the ideal generated by such an element. Then all the minimal primes of I are maximal ideals (Krull's Hauptidealsatz, [2]) and therefore every embedded prime ideal would properly contain a maximal ideal and this is a contradiction.

Now we want to prove that the factorization of f given by Hensel's lemma corresponds exactly to the primary decomposition of the ideal (f). First of all, we need to show that the polynomial obtained in this way generates a primary ideal.

Lemma 1.61. *Let $f \in R/(\pi^l)[x]$ be a monic polynomial such that $f \equiv \phi^k \pmod{\pi}$, where $\phi \in R/(\pi^l)[x]$ is irreducible over the residue field. Then the ideal generated by f in $R/(\pi^l)[x]$ is primary and its radical is $(\pi, \phi(x))$.*

Proof. We recall that an ideal whose radical is a maximal ideal is primary (see [2]). By virtue of this fact, it is enough to show that the radical of f is a maximal ideal. Clearly, the element π is contained in the radical of (f) since it is a nilpotent element. Then we can consider the quotient for the ideal generated by π; here, we notice that $(\pi, f) = (\pi, \phi^k)$ and its radical is (π, ϕ), which is maximal, proving the thesis. □

Let $f \in R/(\pi^l)[x]$ and let $F_1, \ldots, F_m \in R/(\pi^l)[x]$ be the factors of f obtained by Hensel's lemma. The projections of $F_1, \ldots, F_m$ to the residue field are different by construction and the characterization of the radical given in the lemma implies that $\sqrt{f_i} \neq \sqrt{f_j}$ if $i \neq j$. This shows the following:

Theorem 1.62. *Let $f \in R/(\pi^l)[x]$ be a monic polynomial and let $F_1, \ldots, F_m \in R/(\pi^l)[x]$ be the factors of f obtained by means of Hensel's Lemma. Then*

$$(f) = \bigcap_{i=1}^{m} (F_i) = \prod_{i=1}^{m} (F_i)$$

is the irredundant primary decomposition of (f).

Proof. We have already shown that $(f) = \prod_{i=1}^{m}(F_i)$. We only need to prove that $\prod_{i=1}^{m}(F_i) = \cap_{i=1}^{m}(F_i)$ and this follows from the coprimality of $F_1, \ldots, F_m$ and the Chinese Remainder theorem. □

However, as we know, being primary does not imply being irreducible (while an irreducible polynomial always generates a primary ideal) and therefore the factorization found in this way is not satisfactory from the algorithmic point of view, even if it provides a good pre-processing for the polynomials.
The uniqueness of this factorization is important. Even if we have not remarked this fact yet, the factorization into irreducible element is far from being unique

even if f is a monic polynomial over $R/(\pi^l)$ and the number of factorizations could be exponential (see [10]).

Example 1.63. *Let $f = x^4 \in \mathbb{Z}[x]$ and we want to find a factorization of f mod 4. Clearly, x is irreducible and so f is already expressed as a product of irreducible factors. However,*

$$f \equiv (x^2+2)^2 \pmod 4 \qquad\qquad f \equiv (x+2)^4 \pmod 4$$

are other factorizations into irreducible factors. Furthermore, even the number of factors changes.

Even if such issues can occur, the uniqueness of the primary decomposition implies the following result:

Theorem 1.64. *Let $f \in R/(\pi^l)[x]$ be a monic polynomial such that f splits completely into a product of distinct irreducible factors over the residue field*

$$f \equiv \prod_{i=1}^{n} F_i \pmod \pi$$

with $(F_i, F_j) = 1$ for every pair of indices $i \neq j$. Then the factors of f in $R/(\pi^l)[x]$ obtained by means of Hensel's lemma are irreducible and this is the only factorization into irreducible factors of f.

Proof. The fact that the factorization given by Hensel's lemma $f \equiv F_1 F_2 \dots F_n \pmod{\pi^l}$ is a factorization into relatively prime irreducible factors is obvious, since the projection of each $F_i \bmod \pi$ is irreducible. We have to prove uniqueness. Let

$$f \equiv \prod_i G_i^{e_i} \pmod{\pi^l}$$

be a factorization of f into monic irreducible factors. Every irreducible factor generates a primary ideal and, by the uniqueness of the primary decomposition, the primary components of every irredundant primary decomposition must be the same. By virtue of this uniqueness, for every index i there is a set of indices $\{i_1, \dots, i_k\}$ such that

$$\left(G_{i_1}^{e_1} \dots G_{i_k}^{e_k}\right) = (F_i)$$

and both generators are monic. Therefore equality between the given generators must hold, the irreducibility of F_i and of the G_j implies that I contains only one index and the corresponding factor has multiplicity one. Repeating the same argument for all indices, we get the thesis. □

In [10] and [6], the authors do not notice that this theorem can be used to reduce the problem to the primary components, as we are going to show in the following proposition:

Proposition 1.65. *Let $f \in R/(\pi^l)[x]$ be a monic polynomial and let*

$$f \equiv \prod_{i=1}^{s} F_i \pmod{\pi^l}$$

be the factorization into monic primary polynomials given by Hensel's lemma. Consider a factorization into monic irreducible polynomials of f

$$f \equiv \prod_{i=1}^{t} G_i^{e_i} \pmod{\pi^l}$$

and denote by $J_i = \{j_{i,1} \ldots, j_{i,k_i}\}$ the set of all the indices such that $\sqrt{G_{j_{i,l}}} = \sqrt{F_i}$. Then

$$F_i \equiv \prod_{j \in J_i} G_j^{e_j} \pmod{\pi^l}$$

Proof. The primary ideal of an irredundant primary decomposition is unique and (F_i) and $(\prod_{j\in J_i} G_j^{e_j})$ are primary components corresponding to the same prime ideal. Therefore the ideals must coincide; since the generators are both monic, equality must hold. □

This result provides an easy tool that can often speed up the algorithms as we will see in the third chapter.

Example 1.66. *Consider the polynomial $f = (x-1)(x+4)(x+2) \in \mathbb{Z}[x]$. We want to find all the factorizations of f mod 25. First, we use Hensel's lemma, so we factor f mod 5:*

$$f \equiv (x-1)^2(x-2) \pmod{5}$$

We lift this factorization to $\mathbb{Z}/(25)$, obtaining

$$f \equiv (x^2+3x-4)(x-2) \pmod{25}$$

By the previous proposition, the factor $(x-2)$ appears in every factorization. We have to discuss all the factorizations of (x^2+3x-4). Clearly, every factorization reduced modulo 5 must coincide with $(x+1)^2$. We have to find s, $t \in \mathbb{Z}[x]$ such that

$$(x-1+5s)(x-1+5t) \equiv (x^2+3x-4) \pmod{25}$$

We get

$$x-1 \equiv (x-1)(s+t) \pmod{5} \Rightarrow s+t \equiv 1 \pmod{5}$$

Therefore, all the factorizations of x^2+3x-4 are

$$x^2+3x-4 = (x-1+5t)(x+4-5t)$$

for $t \in \{0, \ldots 4\}$. Notice that some of them coincide. Summarizing, all the factorizations of f are

$$f \equiv (x-1)(x+4)(x-2) \pmod{25}$$
$$f \equiv (x+9)(x-6)(x-2) \pmod{25}$$
$$f \equiv (x+14)(x-11)(x-2) \pmod{25}$$

All the reductions shown in this part have an immediate algorithmic application, because they allow us to assume the the polynomials we take into account are monic and that their projections to the residue field is the power of an irreducible polynomial. We can achieve a better result in the setting of a

p-adic field K with uniformizing parameter π. Specifically, let $f \in \mathcal{O}_K[x]/(\pi^l)$ be a monic polynomial , let $\phi \in \mathcal{O}_K[x]$ be a monic irreducible mod π and assume that $f \equiv \phi^k \pmod{\pi}$. We denote by U the unramified extension of K generated by one of the roots of ϕ; this is a Galois extension of K and the residue field of U is a finite extension of the residue field of K on which ϕ splits completely. Therefore, by Hensel's Lemma, we can find a factorization of $f = F_1 \dots F_d$ over $\mathcal{O}_U$, where $d = \deg \phi$. There is a relation between the irreducibility of these factors and $f \bmod \pi^l$. Over a p-adic field K, the following holds:

Lemma 1.67. *Let K be a p-adic field and let $f \in \mathcal{O}_K[x]$ be a monic polynomial such $f \equiv \phi^k \pmod{\pi}$, where $\phi \in \mathcal{O}_K[x]$ is a monic polynomial of degree d irreducible mod π. Let U be the unramified extension of K generated by the roots of ϕ and let $F_1, \dots, F_d \in \mathcal{O}_U[x]$ be the factors of f obtained by means of Hensel's lemma. Then f is irreducible in $\mathcal{O}_K[x]$ if and only if $F_1, \dots, F_d$ are irreducible in $\mathcal{O}_U[x]$.*

Proof. Assume first that f is irreducible. Then, it holds $N_{U/K}(F_i) = f$. Indeed,

$$f = F_1 \dots F_d \Rightarrow f^d = N_{U/K}(F_1) \dots N_{U/K}(F_d)$$

Since the norm of every F_i is non trivial and f is irreducible, it must hold $N_{U/K}(F_i) = f$.
By contradiction, suppose that one of the F_i is reducible, so $F_i = GH$. The norm is multiplicative and so

$$f = N_{U/K}(F_i) = N_{U/K}(G) N_{U/K}(H)$$

and this gives a proper factorization of f, which is impossible.
Vice versa, suppose that F_i is irreducible for all i and assume by contradiction that f is reducible, so that there exist $g, h \in \mathcal{O}_K[x]$ such that $f = gh$. Denote by $G_1, \dots, G_d \in \mathcal{O}_U[x]$ and $H_1, \dots, H_d \in \mathcal{O}_U[x]$ the factors given by Hensel's Lemma of g, h respectively. Then, in $\mathcal{O}_U[x]$,

$$F_1 F_2 \dots F_d = G_1 G_2 \dots G_d H_1 H_2 \dots H_d$$

Since $\deg G_i > 0$, $\deg H_i > 0$ for all indices i, this means that at least one F_i is not irreducible, giving a contradiction. □

The same holds in our settings, as we are going to show in the following proposition.

Observation 1.68. *If L/K is an unramified extension of p-adic fields, a uniformizing parameter for K is a uniformizing parameter for U too.*

Proposition 1.69. *Let $f \in \mathcal{O}_K[x]$ be a monic irreducible polynomial and let U be the unramified extension as above. Let $F_1, \dots, F_d \in \mathcal{O}_U[x]$ be the polynomials obtained by Hensel's Lemma applied to the factors of f over $\mathcal{O}_U/(\pi)$. Then f is irreducible over $\mathcal{O}_K/(\pi^l)$ if and only if $F_1, \dots, F_d$ are irreducible over $\mathcal{O}_U/(\pi^l)$.*

Proof. Assume first that f is irreducible mod π^l. By contradiction, suppose that one of the F_i is reducible. Reordering the factors, we can assume that F_1 splits in $\mathcal{O}_U[x]/(\pi^l)$, so that $F_1 \equiv G_1 G_2 \pmod{\pi^l}$. Since f is irreducible, we know that $N(F_1) = f$. Consider the polynomial $\widetilde{F_1} \in \mathcal{O}_U[x]$ obtained as the

product $\widetilde{G}_1\widetilde{G}_2$, where $\widetilde{G}_1$, $\widetilde{G}_2$ are monic lifts of G_1, G_2. Then, since $F_1 \equiv \widetilde{F}_1 \pmod{\pi^l}$, it holds

$$f = N_{U/K}(F_1) \equiv N_{U/K}(\widetilde{F}_1) = N_{U/K}(\widetilde{G}_1)N_{U/K}(\widetilde{G}_2) \pmod{\pi^l}$$

and this gives a contradiction.
Vice versa, assume $f \equiv G_1G_2 \pmod{\pi^l}$. We can consider the polynomial $\widetilde{f} \in \mathcal{O}_K[x]$ obtained as the product of two lifts of G_1, G_2. $\widetilde{f}$ is clearly reducible over $\mathcal{O}_K$ and then the polynomials $\widetilde{F}_1, \ldots, \widetilde{F}_d$ obtained by Hensel's Lemma must be reducible over $\mathcal{O}_U$ by the previous lemma. We notice that

$$F_1 \ldots F_d \equiv f \equiv \widetilde{f} \equiv \widetilde{F}_1 \ldots \widetilde{F}_d \pmod{\pi^l}$$

and so $F_i \equiv \widetilde{F}_i \pmod{\pi^l}$ by the uniqueness of the lift of the factorization provided by Hensel's lemma. Since $\widetilde{F}_1$ is reducible over $\mathcal{O}_U$, it is also reducible over $\mathcal{O}_U/(\pi^l)$. As a consequence, F_1 is reducible over $\mathcal{O}_U/(\pi^l)$, as desired. □

Summarizing the results of this chapter, we have shown that, given a polynomial $f \in \mathbb{Z}[x]$, in order to find the factorizations of f over $\mathbb{Z}/(n)$ we can reduce ourselves, by means of the Chinese Remainder theorem, to the case of $n = p^l$, where $p \in \mathbb{N}$ is a prime number. Then, we have studied the properties of p-adic fields and of their rings of integers. In particular, since the factor rings of the rings of integers of p-adic fields have the same properties of $\mathbb{Z}/(p^l)$, we have considered polynomials over these rings. In these settings, we can use Hensel's lemma in order to find all the primary components of (f) in $\mathcal{O}_K/(\pi^l)[x]$ and the corresponding factorization is unique. This method does not assure to find a factorization into irreducible monic polynomial, but it is enough to reduce our problem to finding all the factorization of a polynomial such that its projection mod p is a power of an irreducible polynomial. Furthermore, extending the field, we can also assume that this irreducible polynomial has degree one.

Achievements:

- Reduction to factorization in $\mathbb{Z}/(p^l)[x]$
- Generalization of the problem to a discrete valuation ring R such that its completion is the ring of integers of a p-adic field K
- Reduction to polynomials having a unique irreducible factors mod π
- Reduction to irreducible linear factor mod π

The effectiveness of Hensel's lemma suggests examining in depth the factorization of polynomials in the completion in order to obtain further information in our context and we will achieve this in the next chapter.

CHAPTER 2

Factoring over p-adic fields

In this chapter, we will deal with the problem of factoring polynomials over $\mathbb{Q}_p$ and over p-adic fields in general. There are mainly two tools that are extensively used in these algorithms. We have already seen one of them, Hensel's lemma, and we are now going to introduce the second one: Newton polygons. Our exposition will be based mainly on the articles [12], [19], [20], [9] and on the book [17].

2.1 Newton polygons

Newton polygons rise naturally when dealing with polynomials having coefficients in the ring of integers of a p-adic field and give a criterion for determining whether or not a polynomial is irreducible which can be easily implemented. We give at first an intuitive motivation for introducing such a concept.

Let $p \in \mathbb{N}$ be a prime number and consider a p-adic field K with its ring of integers $\mathcal{O}_K$. We have seen in the previous chapter that, if $f \in \mathcal{O}_K[x]$ is an irreducible polynomial, the valuation of all its roots is the same (1.16). More specifically, assume that $f \in \mathcal{O}_K[x]$ is a monic polynomial, let $\alpha_1, \ldots, \alpha_n$ be the roots of f in an algebraic closure of $\mathbb{Q}_p$ and call a_i the coefficients of f, so that

$$f = x^n + \sum_{i=0}^{n-1} a_i x^i$$

We know that $v(a_0) = n \cdot v(\alpha_1)$. What can we say about the other coefficients? They are symmetric functions of the roots of f and so we can use the property of discrete valuations in order to bound their values. For example, estimating in this way the valuation of the coefficient of the degree one term we get the following relation

$$\begin{aligned} v(a_1) &= v\Big(\sum_{1 \le i_1 < \cdots < i_{n-1} \le n} \alpha_{i_1} \ldots \alpha_{i_{n-1}} \Big) \\ &\ge \min_{1 \le i_1 < \cdots < i_{n-1} \le n} v(\alpha_{i_1} \ldots \alpha_{i_{n-1}}) \\ &= (n-1) v(\alpha_1) \end{aligned}$$

and more generally

$$v(a_i) \geq (n-i)v(\alpha_1)$$

These short computations suggest that, if we draw in the plane the points $(i, v(a_i))$, they all lie on or above the line L passing through $(0, v(a_0))$ and $(n, 0)$. Furthermore, L can be considered as the lower convex hull of these points. This argument gives rise to the following definition:

Definition 2.1. *Let K be a p-adic field endowed with a discrete valuation v and denote by $\mathcal{O}_K$ its ring of integers. Given a monic polynomial $f = \sum_{i=0}^{n} a_i x^i \in \mathcal{O}_K[x]$ such that $a_0 \neq 0$, we define the Newton Polygon of f as the lower convex hull of the points $(i, v(a_i)) \in \mathbb{R}^2$. We denote it by $N(f)$.*

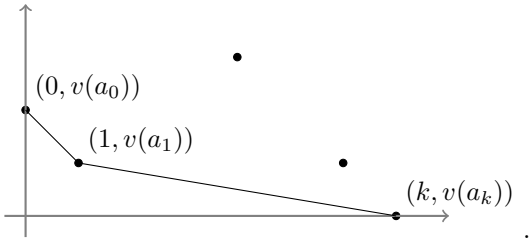


Figure 2.1: The Newton polygon of a reducible polynomial

Some authors do not require any condition on the constant term and admit considering points on the convex hull lying at infinity and even the requirements about the leading term can be dropped. However, we prefer assuming these hypotheses since in our context we can always reduce to this case. In particular, we are interested in factoring polynomials and if the constant term is zero, it is clear that we can factor out a positive power of x from the polynomial. Moreover, we have shown in the first chapter that we can reduce the factorization of a polynomial over $\mathbb{Z}/(n)$ to the monic case. Since our aim is to exploit p-adic factorization in order to get some information about factorization over $\mathbb{Z}/(n)$, it makes sense to restrict to these cases.

Definition 2.2. *Let $f \in \mathcal{O}_K[x]$ a monic polynomial and let $N(f)$ be its Newton polygon. We call*

- *sides the segments composing $N(f)$*
- *length of a side the lenght of its projection on the x-axis*
- *vertices of $N(f)$ the endpoints of the sides of $N(f)$*
- *points of $N(f)$ the points belonging to one of the side of $N(f)$.*

Our intuitive introduction provides the following result, which relates the irreducibility of a polynomial to the shape of its Newton polygon:

Theorem 2.3. *Let $f \in \mathcal{O}_K[x]$ be a monic irreducible polynomial. Then the Newton polygon of f has a single side with slope $-v(\alpha)$, where α is one of the roots of f.*

In the same manner, considering the valuations of the roots, it is possible to show that every side of the Newton polygon of a polynomial f corresponds to one of its factors.

Theorem 2.4. *Let K be a p-adic field and $f \in \mathcal{O}_K[x]$ be a polynomial. Assume that its Newton Polygon is composed of n sides with increasing slope $\lambda_1 < \lambda_2 < \ldots < \lambda_n$. Then f splits into the product*

$$f(x) = \prod_{i=1}^{n} f_i(x)$$

where each f_i has degree equal to the length of the i-th side and the Newton Polygon of f_i has a unique side, with slope λ_i.

We will prove this theorem later, in a more general setting. The theorem states that every side of a Newton Polygon corresponds to a factor (non necessarily irreducible) of f but we need to check whether or not a polynomial whose Newton polygon is one-sided is irreducible. Unfortunately, this is false, as the following example shows:

Example 2.5. *Set $K = \mathbb{Q}_2$ and consider the polynomials in $\mathbb{Z}_2[x]$*

$$f = x^2 + 8x + 12 \qquad\qquad g = x^2 + 8x + 28$$

We draw their Newton polygons: the coefficient of f and g have the same valuation and they share the same Newton Polygon, which is one-sided:

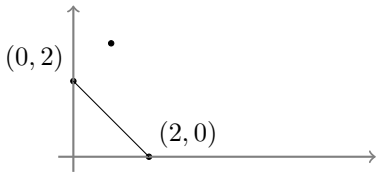


Figure 2.2: The Newton polygons of f and g

However, f can be expressed as a product of linear factors $f = (x+2)(x+6)$ and so it is reducible, while g is irreducible, since it has no roots in $\mathbb{Z}/32\,\mathbb{Z}$.

Sometimes it is possible to say something more and with additional hypotheses we can obtain an irreducibility criterion:

Corollary 2.6. *Let $f \in \mathcal{O}_K[x]$ be a monic polynomial and assume that its Newton polygon is composed by n sides with non-increasing slope. Then the number of irreducible factors of f is bounded by n. In particular, if a_0 is the constant term of f, $(n, v(a_0)) = 1$ and the Newton Polygon of f has a unique side, then f is irreducible.*

This corollary, which we will prove later, can be interpreted as a generalized Eisenstein's criterion. Indeed, the Newton polygon of a polynomial satisfying Eisenstein's criterion has a one-sided Newton polygon. Furthermore, the degree is trivially coprime to its valuation proving irreducibility.

This criterion is powerful but it is completely useless when the projection of the polynomial to the residue field is a power of an irreducible polynomial of

degree greater than one because in this case the valuation of the constant term is 0. The Newton polygon of such a polynomial does not provide any information about its irreducibility and even the criterion on the number of factors is trivial (every polynomial of degree n has at most n factors...). To include these cases in the theory, there are mainly two possibilities:

- Extend the base field to the unramified extension given by the splitting field of the irreducible factors of $f \bmod \pi$
- Generalize the notion of Newton Polygon in order to consider effectively these cases

The first option is computationally unconvenient in our case, since implementing unramified extensions requires to work with polynomials having coefficients in a factor ring of $\mathcal{O}_K[x]$. Therefore we pursue the second plan, which was first presented by Ore ([18]). We emphasize that the two choices are identical from a theoretical point of view, as we will show later.

The idea of this generalization consists in a change of the basis. In the case of standard Newton polygon, we have considered the natural expression of a polynomial as the sum of its monomials. We choose a polynomial $\phi \in \mathcal{O}_K[x]$ and define a reduced ϕ-development:

Definition 2.7. *Consider a polynomial $\phi \in \mathcal{O}_K[x]$ of degree d. We define a reduced ϕ-development of a polynomial $f \in \mathcal{O}_K[x]$ of degree n as an expression*

$$f(x) = \sum_{i=0}^{\lfloor n/d \rfloor} a_i(x)\phi(x)^i$$

such that $\deg(a_i(x)) < n$ *for all* $i = 0, \ldots, \lfloor n/d \rfloor$.

The reduced ϕ-development is unique. Indeed, consider two reduced ϕ-development of the same polynomial f

$$f = \sum_{i=0}^{s} a_i(x)\phi(x)^i = \sum_{i=0}^{s} b_i(x)\phi(x)^i$$

The remainder of the division by ϕ are $a_0(x)$ and $b_0(x)$, which are consequently equal. Then, the remainder of the division of $f - a_0(x)$ by ϕ^2 are $a_1(x)\phi(x)$ and $b_1(x)\phi(x)$, so that $a_1(x) = b_1(x)$. By induction, we get the equality of all the coefficients.

Clearly, the usual expression of the polynomial can be considered as the reduced x-development; in this sense it is a generalization of the standard concept. The uniqueness discussion provides an easy method to find the reduced ϕ-development as the sequence of the remainder of the division by ϕ^i.

In order to define a generalization of the Newton polygon, we have to clarify what the valuation of a polynomial is:

Definition 2.8. *Let K be a p-adic field endowed with a discrete valuation v. Given a polynomial $f = \sum_{i=0}^{n} a_i x^i \in \mathcal{O}_K[x]$, we define the valuation of f as*

$$v(f) = \min_{i=0,\ldots,n} v(a_i)$$

Now we are ready to define the ϕ-polygon of a polynomial.

Definition 2.9. *Let $f, \phi \in \mathcal{O}_K[x]$ be monic polynomials such that $\phi \nmid f$. We consider the reduced ϕ-development of f*

$$f = \sum_{i=0}^{k} a_i(x)\phi(x)^i$$

The generalized Newton ϕ-polygon of f or the ϕ-polygon of f is the lower convex hull of the points $(i, v(a_i(x))) \in \mathbb{R}^2$. We denote it by $N_\phi(f)$.

We clarify the construction of the generalized Newton ϕ-polygon with the following example:

Example 2.10. *We consider the polynomial $f = x^4 + 5x^2 + 9x + 4$ in $\mathbb{Z}_3[x]$. We want to find the ϕ-polygon of f, where $\phi = x^2 + 1$. Firstly, we compute the reduced ϕ-development. Dividing f by ϕ,*

$$f(x) = \phi(x) \cdot (x^2 + 4) + 9x$$

Therefore $a_0(x) = 9x$. Now we divide $(x^2 + 4)$ by $x^2 + 1$ and

$$x^2 + 4 = 1 \cdot \phi(x) + 3$$

Substituting,

$$f(x) = \phi(x)^2 + 3\phi(x) + 9x$$

is the reduced ϕ-development of f. Now, we consider the valuations of the coefficients. In this case,

$$v(a_0) = 2 \qquad v(a_1) = 1 \qquad v(a_2) = 0$$

and the ϕ-polygon is one-sided:

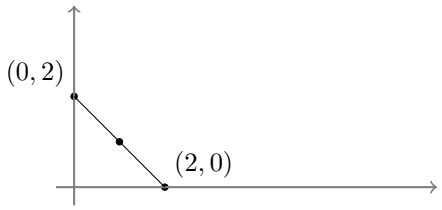


Figure 2.3: Newton polygons of f

This generalization is far from being intuitive unlike the standard Newton polygon; this is the reason why we introduced at first the standard case. Now we need to prove that the same results we stated before still hold. The proofs are quite technical and we need to introduce some notations and some formalisms about polygons.

Definition 2.11. *Let $\lambda = a/b \in \mathbb{Q}$ be a negative rational number, $(a, b) = 1$. We denote by $S(\lambda)$ the set of segments in $\mathbb{R}^2$ with slope λ and non-negative integers ending points.*
Given an element $S \in S(\lambda)$, we define

- *the length $l(S)$ of S as the length of its projection on the x-axis*
- *the height $h(S)$ of S as the length of its projection on the y-axis*
- *the degree $d(S)$ of S as $l(S)/b = a/h(S)$.*

In other words, the degree of a side S measures how many shorter sides $S_i \in S(\lambda)$ are contained in S.

The sets $S(\lambda)$ contain the "bricks" of which polygons are made and we can define a sum on them. We proceed inductively:

- Assume first that we want to sum two sides $S_1 \in S(\lambda_1)$, $S_2 \in S(\lambda_2)$. Let P_0, Q_0 be the endpoints of S_1 and P_1, Q_1 be the endpoints of S_2. If $\lambda_1 < \lambda_2$, we define $S_1 + S_2$ as the polygon having vertices $P_0 + P_1$, $Q_0 + P_1$, $Q_0 + Q_1$. if $\lambda_2 < \lambda_1$, we define $S_1 + S_2$ as the polygon having vertices $P_0 + P_1$, $P_0 + Q_1$, $Q_0 + Q_1$.
- Assume that we want to sum $n+1$ sides $S_1 \in S(\lambda_1), \ldots, S_{n+1} \in S(\lambda_{n+1})$. Order them in a way such that $\max \lambda_i = \lambda_{n+1}$. Let $P_0, \ldots P_n$ be the vertices of the polygon obtained as the sum of the first n sides ordered by increasing abscissa and let P_{n+1}, Q_{n+1} be the endpoints of S_{n+1}. We define the sum $S_1 + \cdots + S_{n+1}$ as the polygon having vertices

$$P_0 + P_{n+1}, \ldots, P_n + P_{n+1}, P_n + Q_{n+1}$$

Example 2.12. *Consider the sides $S_1 \in S(-1)$ and $S_2 \in S(-1/2)$ such that their initial points are $(0,1)$ and $(0,2)$ and their ending points are $(1,0)$ and $(2,1)$ respectively. The sum is the polygon having initial point $(0,3)$, having $(1,2)$ as a vertex and ending in $(3,1)$.*

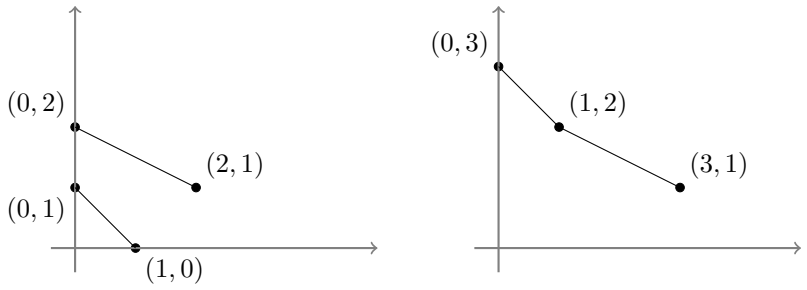


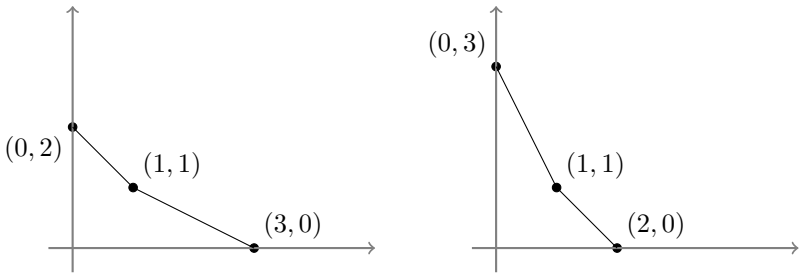
Figure 2.4: The sum of S_1 and S_2

We are not interested in all the possible polygons, but only in the ones composed of sides with negative slopes, since these sides carry the information we are interested in. In fact, our aim is to consider a monic polynomial $f \in \mathcal{O}_K[x]$ and the Newton polygon of such a polynomial has only sides with non-positive slopes. The horizontal sides do not carry information and if the polygon is not one-sided they correspond to factors that can be easily removed using Hensel's lemma, as we will see. Therefore, we are only interested in the following concept:

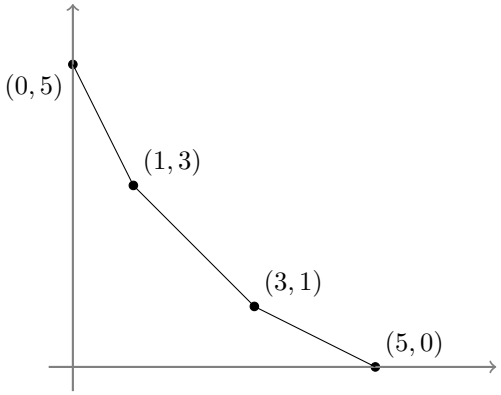
Definition 2.13. *We define a principal polygon $P \subseteq \mathbb{R}^2$ as an open convex polygon obtained as a finite sum of sides with negative slope.*

In the same way as the case of the set of all segments (with arbitrary slopes), the set of principal polygons is endowed with a sum operation. More specifically, the sum of two principal polygons is the sum of all their sides. The result is still a principal polygon since the sides of the resulting polygon have the same slopes as the summands.

Example 2.14. *Consider the following polygons:*



By the definition given above, the sum of these polygons is



Back to our ϕ-polygons, our assumptions do not assure that the ϕ-polygon of a polynomial is always a principal polygon, because there can be a final horizontal side. Removing that side, we can easily associate one to f:

Definition 2.15. *Let $f \in \mathcal{O}_K[x]$ be a monic polynomial and let $\phi \in \mathcal{O}_K[x]$ be a monic polynomial such that $\phi \nmid f$. We define the principal ϕ-polygon $N_\phi^-(f)$ as the principal polygon obtained as the sum of the sides with negative slope of the ϕ-polygon of f.*

Our aim is to relate the shape of the ϕ-polygon of a polynomial to a factorization; it is essential to understand how the product of polynomial affects the shape of the Newton polygons. Surprisingly, given two polynomials $f, g \in \mathcal{O}_K[x]$, the sum of the principal polygons $N_\phi^-(f)$ and $N_\phi^-(g)$ as defined coincides to the ϕ-polygon $N_\phi^-(fg)$:

Theorem 2.16 (Theorem of the Product)**.** *Let $f, g \in \mathcal{O}_K[x]$ be monic polynomials and $\phi \in \mathcal{O}_K[x]$ be a monic polynomial such that ϕ is irreducible mod π and $\phi \nmid fg$. Then*

$$N_\phi^-(fg) = N_\phi^-(f) + N_\phi^-(g)$$

In order to prove this theorem, we prove some lemmas and introduce the notion of an admissible development. Clearly, the extremal points of a polygon play a crucial role and they motivate the following definition:

Definition 2.17. *Let N be a polygon and $P = (i, y) \in \mathbb{R}^2$ be a point with integer abscissa. Let $Q = (i, \widetilde{y}) \in N$. We say that P lies on or above N if $y \geq \widetilde{y}$.*

We would like to understand the behaviour of these points under the sum of polygons. Given a principal polygon N, let μ_i be the slope of the segment joining $(i-1, y_{i-1}) \in N$ and $(i, y_i) \in N$. If there exists a point of N with abscissa $i \in \mathbb{N}$, we denote by $U_i(N)$ the set $\{\mu_1, \ldots, \mu_i\}$.

Lemma 2.18. *Let N, N' be principal polygons and let $P = (i, \eta)$ and $P' = (j, \xi)$ be points lying on or above N and N' respectively. Then $P + P'$ lies on or above $N + N'$. Furthermore, $P + P' \in N + N'$ if and only if $P \in N$, $P' \in N'$ and $U_{i+j}(N + N') = U_i(N) \cup U_j(N')$.*

Proof. Denote by $y_i(N)$ the ordinate of the point of N of abscissa i. By definition of sum of principal polygons, it is immediate to see that $y_i(N) + y_j(N') \geq y_{i+j}(N + N')$ and the equality holds if and only if $U_i(N) \cup U_j(N') = U_{i+j}(N + N')$. Furthermore, $\eta + \xi \geq y_i(N) + y_j(N')$. The thesis follows immediately. □

In order to obtain the ϕ-polygon of f, it is not necessary to consider its reduced ϕ-development, but under certain hypotheses on the coefficients, we can relax this condition, as we are going to show.
We consider a ϕ-development of f (not necessarily the reduced one)

$$f(x) = \sum_{i \geq 0} a_i'(x)\phi(x)^i$$

and the principal polygon N' generated by the lower convex hull of the points $(i, v(a_i'))$. We define the coefficients

$$c_i = \begin{cases} 0 & \text{if } (i, v(a_i')) \text{ lies above } N' \\ \frac{a_i'(x)}{\pi^{v(a_i')}} \pmod{(\pi, \phi(x))} & \text{if } (i, v(a_i')) \text{ lies on } N' \end{cases}$$

Definition 2.19. *We define a ϕ-development of f*

$$f(x) = \sum a_i'(x)\phi(x)^i$$

admissible if $c_i \not\equiv 0 \pmod{(\pi, \phi)}$ for all i such that $(i, v(a_i'))$ is a vertex of N'.

The definition seems quite obscure but the following lemma gives a light on it:

Lemma 2.20. *Let $f \in \mathcal{O}_K[x]$ be a monic polynomial and let*

$$f(x) = \sum a_i'(x)\phi(x)^i$$

be an admissible ϕ-development of f. Then the principal part N' of the polygon associated with this development coincides with $N_\phi^-(f)$.

Proof. Consider the reduced ϕ-development of f:

$$f(x) = \sum a_i(x)\phi(x)^i$$

Then, we write down the reduced ϕ-development of each a_i':

$$a_i(x)' = \sum_{k\geq 0} b_{i,k}(x)\phi(x)^k \tag{2.1}$$

Substituting these coefficients in the expression of f, we get

$$\begin{aligned} f(x) &= \sum_i a_i(x)\phi(x)^i \\ &= \sum_i a_i'(x)\phi(x)^i \\ &= \sum_i \phi(x)^i \sum_k b_{i,k}(x)\phi(x)^k \\ &= \sum_i \sum_{k\leq i} b_{i-k,k}(x)\phi(x)^i \end{aligned}$$

The uniqueness of the reduced ϕ-development implies the following equality

$$a_i(x) = \sum_{0\leq k\leq i} b_{i-k,k}(x) \tag{2.2}$$

Now, we look at valuations. We notice the following facts:

- It holds that $v(b_{i,k}(x)) \geq v(a_i'(x))$. Indeed, $a_i'(x)/\pi^{v(a_i'(x))}$ is an integral element (because its valuation is 0) and we can consider its reduced ϕ-development
$$\frac{a_i'(x)}{\pi^{v(a_i'(x))}} = \sum l_k(x)\phi(x)^k$$
which has the property that $l_k(x) \in \mathcal{O}_K[x]$. In particular, $v(l_k(x)) \geq 0$. Multiplying for $\pi^{v(a_i'(x))}$, we get
$$a_i'(x) = \sum \pi^{v(a_i'(x))} l_k(x)\phi(x)^k$$
and by the uniqueness of the reduced ϕ-development $\pi^{v(a_i'(x))}l_k(x) = b_{i,k}(x)$. Passing to valuations, $v(a_i'(x)) + v(l_k(x)) = v(b_{i,k}(x))$ and therefore $v(b_{i,k}(x)) \geq v(a_i'(x))$.

- The points $(i, v(a_i(x)))$ lie on or above N'. By (2.2),
$$v(a_i(x)) \geq \min_k v(b_{i-k,k}(x))$$
If k_0 is the index corresponding to the minimum, then $v(b_{i-k_0,k_0}(x)) \geq v(a_{i-k_0}'(x))$ by the previous point. By definition, $v(a_{i-k_0}'(x))$ is the ordinate of one of the points of whom N' is the lower convex hull and, denoting by $y_j(N')$ the ordinate of the polygon at abscissa j, we get
$$v(a_i(x)) \geq v(a_{i-k_0}'(x)) \geq y_{i-k_0}(N') \geq y_i(N') \tag{2.3}$$
where the last inequality holds because N' is a principal polygon and the slopes are strictly increasing by definition.

The second point shows that all the vertices of the polygon $N_\phi^-(f)$ lie on or above N'.
Let now $(i, v(a_i'(x)))$ be a vertex of N'. By hypothesis, $c_i' \neq 0$ and by (2.1)

$$0 \not\equiv c_i' \equiv \frac{a_i(x)'}{\pi^{v(a_i'(x))}} \equiv \frac{b_{i,0}(x)}{\pi^{v(a_i'(x))}} \pmod{\pi, \phi}$$

since all the other terms are divisible by ϕ. This means that $v(b_{i,0}) = v(a_i'(x))$. We want now to show that $v(a_i(x)) = v(b_{i,0}(x))$. Notice that, if $k \neq 0$, we get, repeating the same argument as relation 2.3, the following inequalities:

$$v(b_{i-k,k}(x)) \geq v(a_{i-k}'(x)) \geq y_{i-k}(N') > y_i(N') \tag{2.4}$$

since N' is a principal polygon and the slope of each edge is negative, while $v(b_{i,0}(x)) = y_i(N')$. As a consequence,

$$v(a_i(x)) = \min_k v(b_{i-k,k}(x)) = v(b_{i,0}(x))$$

where the first equality holds because all the other terms of the reduced ϕ-development of a_i' are greater (see 1.10). Therefore we have shown that if $(i, v(a_i'(x)))$ is a vertex of N', $v(a_i(x)) = v(a_i'(x))$.
Summarizing, the principal polygon $N_\phi^-(f)$ associated with f coincides with N' in the abscissas corresponding to vertices and the valuations of the the terms of the reduced ϕ-development are greater. Therefore $N' = N_\phi^-(f)$, as desired. □

Now, we are ready to prove the theorem of the product:

Proof of the theorem of the product 2.16. Let $f, g \in \mathcal{O}_K[x]$ and consider their reduced ϕ-development

$$f(x) = \sum a_i(x)\phi(x)^i \qquad\qquad g(x) = \sum b_i(x)\phi(x)^i$$

Then we can express their product as

$$f(x)g(x) = \sum A_i(x)\phi(x)^i \qquad\qquad A_k(x) = \sum_{i+j=k} a_i(x)b_j(x)$$

Let N' be the polygon associated with this ϕ-development of fg. We want to show that this development is admissible and that N' coincides with the sum of the ϕ-polygons of f and g.
Clearly, the sum of points lying on or above $N_\phi^-(f)$ and $N_\phi^-(g)$ lies on or above $N_\phi^-(f) + N_\phi^-(g)$. Furthermore, using the property of discrete valuations,

$$v(A_k(x)) \geq \min_{i+j=k} v(a_i(x)) + v(b_j(x))$$

This means that the points $(i, v(A_k(x)))$ lie on or above $N_\phi^-(f)+N_\phi^-(g)$, proving that the whole N' lies on or above $N_\phi^-(f)+N_\phi^-(g)$. We now want to show that the vertices of the two polygons coincide. Let $P_k = (k, y_k)$ be a vertex of $N_\phi^-(f)+N_\phi^-(g)$, so that P_k is the end point of $S_1 + \ldots S_\gamma + T_1 + \cdots + T_\sigma$ for S_i and T_j sides of $N_\phi^-(f)$ and $N_\phi^-(g)$ respectively. By virtue of lemma 2.18, for all the pairs i, j such that $i + j = k$, the points $(i, v(a_i(x))) + (j, v(b_j(x)))$ lie above $N_\phi^-(f) + N_\phi^-(g)$ except from the one obtained as the sum of the two vertices of

$N_\phi^-(f)$ and $N_\phi^-(g)$ corresponding to $S_1+\cdots+S_\gamma$ and $T_1+\cdots+T_\sigma$. We denote by i_0 and j_0 the corresponding abscissas and $(i_0, v(a_{i_0}(x))) + (j_0, v(b_{j_0}(x))) = P_k$. As a consequence, $a_{i_0}(x)b_{j_0}(x)$ is the term in the defining sum for A_k having minimum valuation and so $v(A_k(x)) = v(a_{i_0}(x))+v(b_{j_0}(x))$, proving the equality $N' = N_\phi^-(f) + N_\phi^-(g)$.
Now, we show that the ϕ-developed we have considered is admissible:

$$\frac{A_k(x)}{\pi^{y_k}} \equiv \frac{a_{i_0}(x)b_{j_0}(x)}{\pi^{y_k}} \equiv \frac{a_{i_0}(x)}{\pi^{y_{i_0}(N_\phi(f))}} \cdot \frac{b_{j_0}(x)}{\pi^{y_{j_0}(N_\phi(g))}} \not\equiv 0 \pmod{\pi, \phi(x)}$$

and so the considered development is admissible. By the previous lemma, $N_\phi^-(fg) = N' = N_\phi^-(f) + N_\phi^-(g)$, as desired. □

Finally, we prove the theorem of the polygon, which is the most relevant theoretical result concerning polygons. It is the generalization of theorem 2.4 we stated at the beginning of this section, the key result about standard Newton polygons. We split the proof into two parts:

Lemma 2.21. *Let $f \in \mathcal{O}_K[x]$ be a monic irreducible polynomial and $\phi \in \mathcal{O}_K[x]$ be a monic polynomial such that $f \equiv \phi^k \pmod{\pi}$ and ϕ is irreducible over the residue field. If $\phi \nmid f$, then the ϕ-polygon of f has a unique side with slope equal to $-v(\phi(\alpha)) < 0$, where α is one of the roots of f in $\overline{\mathbb{Q}_p}$.*

Proof. First of all, we notice that, by the uniqueness of the extension of a valuation, $v(\phi(\alpha))$ is independent of the choice of α. Then, α is an integral element since it is a root of a monic polynomial, so $v(\phi(\alpha)) \geq 0$. Moreover, $f(x) \equiv \phi(x)^k \pmod{\pi}$, so $\phi(\alpha)$ can not be invertible and and $v(\phi(\alpha)) > 0$.
Let $\mu(x) = x^k + \sum b_i x^i$ be the minimal polynomial of $\phi(\alpha)$ and consider the polynomial $q(x) = \phi(x)^k + \sum b_i \phi(x)^i$. Since the coefficients of μ are the symmetric functions of $\phi(\alpha)$ and its conjugates, we have

$$v(b_0) = k \cdot v(\phi(\alpha)) \qquad\qquad v(b_i) \geq (k-i) \cdot v(\phi(\alpha))$$

These relations imply that $N_\phi(q)$ has a unique side with slope $-v(\phi(\alpha))$. Notice that α is a root of q and since f is the minimal polynomial of α, $f \mid q$. By the theorem of the product it follows that $N_\phi(f)$ has a unique side with slope $-v(\phi(\alpha))$, as desired. □

Theorem 2.22 (Theorem of the Polygon)**.** *Let $f \in \mathcal{O}_K[x]$ be a monic polynomial and $\phi \in \mathcal{O}_K[x]$ be a monic polynomial such that $f \equiv \phi^k \pmod{\pi}$ and ϕ is irreducible over the residue field. Assume that $\phi \nmid f$. If $S_1, \ldots, S_l$ are all the sides with different slopes of $N_\phi(f)$, f admits a factorization*

$$f(x) = F_1(x) \ldots F_l(x)$$

such that

- *$N_\phi(F_i)$ is one-sided and equal to S_i up to a translation*
- *For every root α of F_i, we have $v(\phi(\alpha)) = -\lambda_i$, where λ_i is the slope of S_i.*

Proof. Fixing a slope λ, we can consider the set of irreducible factors of f, h_j such that $N(h_j)$ has slope λ. The product of these factors is a monic polynomial F_i that divides f, $N_\phi(F_i)$ coincides (up to a translation) with the side with slope λ of $N_\phi(f)$ and by the lemma the statement about the slope holds too. Repeating this procedure for every side, we get the thesis. □

Corollary 2.23. *With the same notation of the previous theorem, the number of factors of F_i is bounded by the degree of $N_\phi(F_i)$.*

Proof. By the theorem of the product, every irreducible factor of F_i corresponds to a side of $N_\phi(F_i)$ having endpoints with integers coordinates. The maximum number of such sides of $N_\phi(F_i)$ is, by definition, its degree. □

Corollary 2.24. *Let $f \in \mathcal{O}_K[x]$ be a monic irreducible polynomial, α be one of its roots and consider $L = K(\alpha)$. Then*

- *the ramification index $e(L/K)$ is divisible by s, where $\lambda = -r/s$ is the slope of the side of $N_\phi(f)$ and $(r, s) = 1$.*
- *the inertia degree $f(L/K)$ is divisible by* $\deg(\phi)$.

Therefore, in order to detect the irreducibility of a polynomial $f \in \mathcal{O}_K[x]$, a partial criterion is the following:

- project f to $\mathcal{O}_K[x]/(\pi)$; if the projection splits into two coprime factors , f is reducible.
- lift the irreducible factor of f mod π to $\mathcal{O}_K[x]$; denote by ϕ this lift
- construct the ϕ-polygon of f
- if the ϕ-polygon has two or more sides with different slopes, then f is reducible.

There is a problem in this method, given by the choices of the lift of the irreducible factor of f mod π. Indeed, different lifts give different polygons:

Example 2.25. *Let $f = (x^2 + 4)^2$ be a polynomial over $\mathbb{Z}_3$. Two different lifts of the irreducible factor of f over $\mathbb{F}_3$ are $\phi_1 = x^2 + 1$ and $\phi_2 = x^2 + 9x + 4$. Then*

$$f = \phi_1^2 + 6\phi_1 + 9 = \phi_2^2 + \phi_2(-18x + 81) - 729x - 324$$

Therefore the ϕ_1-polygon of f is one-sided with ends $(0, 2)$, $(2, 0)$, while the ϕ_2-polygon of f is one-sided with ends $(0, 4)$, $(2, 0)$.

The choice of the lift can influence the shape of the polygon; however, understanding in advance which lift is more convenient is not easy.

Unramified extensions and Newton polygons Before introducing the notion of ϕ-polygon, we said that working over an unramified extension we would have obtained the same results. This follows from the following theorem:

Theorem 2.26. *Let $f, \phi \in \mathcal{O}_K[x]$ be monic polynomials such that $f \equiv \phi^k \pmod{\pi}$ and ϕ is irreducible over the residue field. Let α be one of the roots of f and U, $K \subseteq U \subseteq K(\alpha)$, be the unramified extension of degree equal to $\deg \phi$. Consider the minimal polynomial μ of α over $\mathcal{O}_U$ and let ν be a monic lift of its unique irreducible factor over the residue field of U. Then*

$$N_\phi^-(f) = N_\nu^-(f)$$

Proof. Since $\nu \mid \phi$, we can write $\phi(x) = \nu(x) \cdot \rho(x)$ in $\mathcal{O}_U[x]$. Consider the reduced ϕ-development of f:

$$f(x) = \sum a_i(x)\phi(x)^i$$

Substituting the factorization,

$$f(x) = \sum a_i(x)\rho(x)^i\nu(x)^i$$

We want to show that this ν-development of f is admissible. This fact would imply the thesis since we have seen that the principal polygon of an admissible development coincide with the ν-polygon. Our aim is to prove that, if $(i, v(a_i'))$ is a vertex of the polygon,

$$c_i = \frac{a_i(x)\rho(x)^i}{\pi^{v(a_i(x)\rho(x)^i)}} \not\equiv 0 \pmod{\pi, \nu}$$

and this is trivial, since $(\rho(x), \nu(x)) = 1$ and $v(\rho(x)) = 0$. □

There is an interesting consequence of this theorem. As in the statement of the theorem, let μ be the minimal polynomial of α over the unramified extension U. Since $\mu \mid f$ in $\mathcal{O}_U[x]$, there exists $h \in \mathcal{O}_U[x]$ such that $f = \mu \cdot h$. By the theorem of the product 2.16 and the previous theorem, $N_\nu^-(\mu) + N_\nu^-(h) = N_\nu^-(f) = N_\phi^-(f)$. The projection of the monic polynomial h to the residue field is coprime to ν. So, if we write the reduced ν-development of h,

$$h(x) = \sum_{i=0}^{t} b_i(x)\nu(x)^i$$

it must hold that $v(b_0) = 0$ and $v(b_t) = 0$. This means that $N_\nu(h)$ is a horizontal line, proving the following corollary:

Corollary 2.27. *In the hypothesis of the previous theorem,*

$$N_\nu^-(\mu) = N_\phi^-(f)$$

We summarize all the properties:

Properties of Newton polygons:

- If the Newton polygon of f is composed of two sides with different slopes, f factors.

- If the Newton polygon of f is one-sided and does not contain points with integer coordinates, f is irreducible.
- The number of factors of f is bounded by the sum of the degrees of the sides in the polygon.
- The slope of a side of the ϕ-polygon is the inverse of the valuation of $\phi(\alpha)$, where α is a root of f.

2.1.1 Computing the slope factorization

Newton polygons provide a simple tool to detect irreducibility and they also give a method to factor polynomials. Now we deal with the problem of finding the factorization given by theorems 2.22 and 2.4. We call this factorization the "slope" factorization, since each factor corresponds to a side with different slope in the Newton polygon of f. There are some different methods to compute it; we are going to show the easiest one, which is, from a theoretical point of view, the clearest.
Let $f \in \mathcal{O}_K[x]$ be the monic polynomial we want to factor and let $\alpha_1, \dots, \alpha_n$ be its roots in an algebraic closure $\overline{\mathbb{Q}}_p$ of $\mathbb{Q}_p$.

Definition 2.28. *Let $\mu(x) \in K[x]$ be a polynomial. We define the characteristic polynomial of μ as*

$$\chi_\mu^{(f)}(t) = \prod_{i=1}^{n}(t - \mu(\alpha_i)) = \mathrm{Res}_x(f(x), t - \mu(x))$$

Characteristic polynomials play a crucial role in all algorithms for factoring polynomials over the p-adics, since by definition they are polynomials that split completely over the splitting field of f. In this sense, characteristic polynomials provide some non-trivial relations among the roots of f; more precisely, if a characteristic polynomial splits into coprime factors, we can factor f. Indeed, let $\mu \in K[x]$ be a polynomial such that $\chi_\mu^{(f)} \in \mathcal{O}_K[x]$ and assume that $\chi_\mu^{(f)}(t) = \chi_1(t)\chi_2(t)$ with $(\chi_1, \chi_2) = 1$. Then, reordering the roots,

$$h_1(t) = \prod_{i=1}^{s}(t - \mu(\alpha_i)) \qquad h_2(t) = \prod_{i=s+1}^{n}(t - \mu(\alpha_i))$$

In particular, $f(x) \mid h_1(\mu(x))h_2(\mu(x))$, since $\chi_\mu^{(f)}(\mu(\alpha_i)) = 0$ for all i, and

$$\begin{aligned} f(x) &= \gcd(f(x), h_1(\mu(x))h_2(\mu(x))) \\ &= \gcd(f(x), h_1(\mu(x))) \cdot \gcd(f(x), h_2(\mu(x))) \end{aligned}$$

where the last equality follows from the coprimality of h_1, h_2. Both of them are non-trivial polynomials and so we have found a proper factorization of f:

Proposition 2.29. *With the same notations as the definition, assume that the characteristic polynomial $\chi_\mu^{(f)} \in \mathcal{O}_K[x]$ splits into coprime factors over $\mathcal{O}_K$. Then f splits over $\mathcal{O}_K$.*

We want to exploit this observation in order to obtain the slope factorization of a polynomial $f \in \mathcal{O}_K[x]$. We assume that $f \equiv \phi^k \pmod{\pi}$, where $\phi \in \mathcal{O}_K[x]$ is a monic polynomial of degree d and irreducible mod π.
For clarity, we discuss at first the case of the standard Newton polygon, in which we consider $\phi = x$. Let $\lambda_1 < \lambda_2 < \ldots < \lambda_n$ be the slopes of the Newton polygon of f.

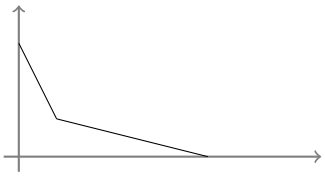


Figure 2.5: A Newton polygon with two lines

The idea is to find a polynomial μ such that its characteristic polynomial $\chi_\mu^{(f)}$ "flattens" the side with greatest slope of the polygon of f, as we are going to explain. More precisely, we know that the slope of a side corresponds to the valuation of some of the roots of f and therefore we would like to make a change of variables in order to have that that the valuations of the roots corresponding to that side is 0. After such a change, the polynomial splits over the residue field by construction and so we are able to factor f and repeat the procedure on the other sides. This change of variables can be done by the computation of a characteristic polynomial. Assume that the slope of the last side of the Newton polygon is $\lambda_n = -r/s$, where $(r, s) = 1$. We consider then the polynomial $\mu(x) = x^s/\pi^r$ and we compute the characteristic polynomial:

$$\chi_\mu^{(f)}(t) = \prod_{i=1}^{n}(t - \mu(\alpha_i)) = \prod_{i=1}^{n}\left(t - \frac{\alpha_i^s}{\pi^r}\right)$$

In this way, the roots of f having minimal valuations correspond to the roots of $\chi_\mu^{(f)}$ having valuation 0. So this polynomial splits over the residue field and so in $\mathcal{O}_K[x]$ using Hensel's Lemma. The preliminary observation allows us to split f, as desired.

The same procedure works in the case of the generalized Newton polygon. In this case, if the side has slope $-r/s$, we have to consider the polynomial $\mu(x) = \phi(x)^s/\pi^r$ and the same argument about valuations shows that the polynomial must split over the residue field and so over $\mathcal{O}_K[x]$.

Computation of the GCD There is a crucial point in this algorithm: the computation of the greatest common divisor over $\mathcal{O}_K$. Indeed, we need to make all the computations over the p-adics, where the coefficients are series. Consequently, they are usually represented truncating the representation and there are problems of approximations. Fortunately, in the settings we described before we have additional information. Specifically, we have a monic polynomial $f \in \mathcal{O}_K[x]$ and two polynomials $g, h \in \mathcal{O}_K[x]$ such that $f \mid gh$ and we want to compute both $G_1 = \gcd(f, g)$ and $G_2 = \gcd(f, h)$. The idea is quite easy. Consider the Sylvester matrices $S(f, g)$ and $S(f, h)$. We know that the column-reduction of these matrices over K gives the coefficients of G_1 and G_2 in their

last non-zero columns, because column-reduction corresponds to the Euclidean algorithm. Instead, the column-reduction over $\mathcal{O}_K$ gives the coefficients of $\pi^{j_1}G_1$ and $\pi^{j_2}G_2$ for some $j_1, j_2 \in \mathbb{N}$ (because π is not invertible in $\mathcal{O}_K$). We need to upper bound these exponents in order to get the precision needed in the computation. We define

$$G_1(x) = \gcd(f(x), g(x)) \qquad G_2(x) = \gcd(f(x), h(x))$$

so that $f(x) = G_1(x)G_2(x)$, and $H_1(x) = g(x)/G_1(x)$ and $H_2(x) = h(x)/G_2(x)$. We consider the ideals

$$(\pi^{s_{G_2H_1}}) = (G_2, H_1) \cap \mathcal{O}_K \quad (\pi^{s_{G_1H_2}}) = (G_1, H_2) \cap \mathcal{O}_K \quad (\pi^{s_{gh}}) = (g, h) \cap \mathcal{O}_K$$

which coincide with the reduced resultants we considered in the first chapter and that can be computed directly by the Smith normal forms of the Sylvester matrices. Clearly, there is a relation between the exponents, explicitly $s_{G_2H_1} \leq s_{gh}$ and $s_{G_1H_2} \leq r$ because $g = G_1H_1$ and $h = G_2H_2$. Furthermore, if we denote by $\pi^{j_1}G_1$ and $\pi^{j_2}G_2$ the polynomials obtained by the column-reduction of the Sylvester matrix $S(f, g)$ and $S(f, h)$ respectively, we get

$$\pi^{j_1}G_1 \in (f, g) \qquad \pi^{j_2}G_2 \in (f, h)$$

Notice that $s_{G_2H_1} \leq j_1$. Indeed, $\pi^{j_1}G_1 \in (f, g)$ and so

$$\pi^{j_1} \in \Big(\frac{f(x)}{G_1(x)}, \frac{g(x)}{G_1(x)}\Big) \cap \mathcal{O}_K = (G_2(x), H_1(x)) \cap \mathcal{O}_K = (\pi^{s_{G_2H_1}})$$

Furthermore, we know that $\pi^{s_{G_2H_1}}G_1 \in (f, g)$ and therefore we get $s_{G_2H_1} = j_1$; in the same way, $s_{G_1H_2} = j_2$.
This means that if $m > s_{gh}$, we can find an approximation of the greatest common divisor. Indeed, in this case $m > s_{G_2H_1}$ and $m > s_{G_1H_2}$. Let $\pi^{s_{G_1H_2}}\widetilde{G}_1$ the polynomial obtained by the coefficients of last non-zero column of the column-reduction applied to the Sylvester matrix $S(f, g) \bmod \pi^m$. Then

$$\pi^{s_{G_2H_1}}G_1 \equiv \pi^{s_{G_2H_1}}\widetilde{G}_1 \pmod{\pi^m} \Rightarrow\ G_1 \equiv \widetilde{G}_1 \pmod{\pi^{m-s_{gh}}}$$

and the same holds for G_2. Therefore, if we want to know the greatest common divisor mod π^n, we need to do the computation mod $\pi^{n+s_{gh}}$.

We summarize this argument in the following theorem:

Theorem 2.30. *Let $f \in \mathcal{O}_K[x]$ be a monic polynomial and let $g, h \in \mathcal{O}_K[x]$ be two monic polynomials such that*

$$f(x) \mid g(x)h(x)$$

Let $m \in \mathbb{N}$ be an integer such that $m > s_{gh}$. We consider the polynomial $\pi^{s_1}G_1$ given by the last non-zero column of the matrix obtained by column reduction of $S(f, g)$ over $\mathcal{O}_K/(\pi^m)$. Then

$$G_1 \equiv \gcd(f, g) \pmod{\pi^{m-s_{gh}}}$$

Example 2.31. *Consider the following polynomial f with coefficients in $\mathbb{Q}_2$*

$$f(x) = x^2 + 2x + 8$$

We want to find its slope factorization. The Newton polygon of this polynomial has two sides, with slope -1 *and* -2*, as shown in the figure:*

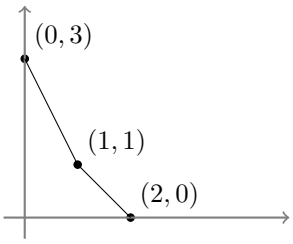


Figure 2.6: Newton diagram of f

We proceed with the computation of the characteristic polynomial of $\mu(x) = x/2$*. The resultant of* $t-(x/2)$ *and* $f(x)$ *with respect to* x *is the determinant of the matrix*

$$S(f(x), t-\mu(x)) = \begin{pmatrix} -\frac{1}{2} & 0 & 1 \\ t & -\frac{1}{2} & 2 \\ 0 & t & 8 \end{pmatrix}$$

which is equal to $\chi_\mu^{(f)} = t^2+t+2$*. As expected,* $\chi_\mu^{(f)}$ *splits over the residue field* $\mathbb{Z}/(2)$ *as a product of two coprime factors,* t *and* $t+1$*. Lifting this factorization to* $\mathbb{Z}/(128)$*, we get*

$$\chi_\mu^{(f)} \equiv (t+91)(t+38) \pmod{128}$$

Therefore, substituting $t = \mu(x)$ *and eliminating the denominators,* $f(x) \mid (x+182)(x+76) \pmod{512}$*. We need to compute the reduced resultant of these factors:*

$$(x+182, x+76) \cap \mathbb{Z}_2 = (2)$$

and this means that $f(x) \equiv (x+182)(x+76) \pmod{256}$*.*

2.2 Factorization algorithm

In this section, we present a complete algorithm for factoring polynomials over a p-adic field. We need to recall some results about characteristic polynomials and their relations with factorization. In what follows, we consider a p-adic field K with a uniformizing parameter π and a monic polynomial $f \in \mathcal{O}_K[x]$, where $\mathcal{O}_K$ denotes the ring of integers as usual.
We have seen that, if a characteristic polynomial $\chi_\mu^{(f)}$ splits over K, then we can obtain a factorization of f. It is crucial to understand whether or not a polynomial can be factored by using Hensel's lemma and the slope factorization:

Definition 2.32. *Let* $\mu \in K[x]$ *be a polynomial such that* $\chi_\mu^{(f)}(t) \in \mathcal{O}_K[t]$*. We say that*

- μ *passes the Hensel test if* $\chi_\mu^{(f)}$ *is a power of an irreducible polynomial mod* π

- *μ passes the Newton test if the Newton polygon of $\chi_\mu^{(f)}$ is one-sided.*

Notice that if a polynomial μ passes the Hensel test and the projection of its characteristic polynomial to the residue field is different from a power of t, then it also passes the Newton test. This follows from the fact that in this case the constant term of $\chi_\mu^{(f)}$ has valuation zero and therefore the Newton polygon has a single horizontal side ($\chi_\mu^{(f)}$ is monic by definition).
Proposition 2.29 can be strengthened: the other implication holds too.

Theorem 2.33. *Let $f \in \mathcal{O}_K[x]$ be a monic polynomial and let $\mu \in K[x]$ be a polynomial such that $\chi_\mu^{(f)}(t)$ is irreducible over K. Then f is irreducible.*

Proof. This result follows from a field theoretical argument. Indeed, if we denote by $\alpha_1, \ldots, \alpha_n$ the roots of f in the algebraic closure $\overline{\mathbb{Q}}_p$, we know that

$$\chi_\mu^{(f)}(t) = \prod_{i=1}^{n} (t - \mu(\alpha_i))$$

It follows immediately that $K(\alpha_i) \supseteq K(\mu(\alpha_i))$. By hypothesis, $K(\mu(\alpha_i))$ has degree n over K and by the containment the same must hold for $K(\alpha_i)$. This means that f is the minimal polynomial of its roots, so it is irreducible. □

This theorem provides an irreducibility criterion which plays a key role in all the factorization algorithms. Usually, they start searching for a polynomial $\mu \in K[t]$ such that $\chi_\mu^{(f)}$ is irreducible; if they find one, the algorithms stop and return an irreducibility certificate, if they do not, they will eventually factor f. This method can seem strange and gives rise to the following two questions:

- How can we determine whether $\chi_\mu^{(f)}$ is irreducible or not? This reduction seems as difficult as the starting problem.
- Why does such an algorithm terminate? It is necessary to find a way that leads to such a μ in a short time.

The answers to the first question determine the main differences between the existing algorithms. We are going to follow the argument given in [9]. We will discuss the second question later. The idea of the authors of this article is to find a polynomial μ such that $\chi_\mu^{(f)}$ has a particular shape:

Definition 2.34. *Let $f \in \mathcal{O}_K[x]$ be a monic polynomial. We say that f is in Eisenstein form if there exist polynomials $\phi, h_1, h_2 \in \mathcal{O}_K[x]$ such that*

$$f(x) = \phi(x)^k + \pi\phi(x)h_1(x) + \pi h_2(x)$$

and

- *ϕ is irreducible mod π*
- $\deg(\phi(x)h_1(x)) < \deg f$
- $(h_2, \phi) = 1 \pmod{\pi}$
- $\deg h_2 < \deg f$

The name of such polynomials comes from the fact that, when $\phi = x$, they coincide with the polyomials satisfying the hypotheses of Eisenstein's criterion. As in that case, it is easy to see that they are irreducible:

Proposition 2.35. *Let $f \in \mathcal{O}_K[x]$ be a polynomial in Eisenstein form. Then f is irreducible.*

Proof. As we said before, the theorems about Newton polygons are a generalization of Eisenstein's criterion and we can use them to prove elegantly this proposition. We consider the normalized valuation on K, so that $v(\pi) = 1$. Since $f = \phi(x)^k + \pi\phi(x)h_1(x) + \pi h_2(x)$ is in Eisenstein form, the ϕ-polygon of f is one-sided, with vertices $(0, 1)$ and $(k, 0)$ and in particular it has degree 1, proving the irreducibility of f by 2.22 and its corollary. □

The algorithm will try to find a polynomial $\mu \in K[x]$ such that $\chi_\mu^{(f)}$ is in Eisenstein form. If such a polynomial exists, f is irreducible:

Definition 2.36. *We say that $\mu \in K[x]$ certifies f is $\chi_\mu^{(f)}(t)$ is in Eisenstein form.*

If there exists a polynomial $\mu \in K[x]$ which certifies f, there exists an infinite number of them:

Proposition 2.37. *Let $\mu \in K[x]$ that certifies f and let $\widetilde{\mu}$ such that $\mu \equiv \widetilde{\mu} \pmod{\pi^2}$. Then $\widetilde{\mu}$ certifies f.*

Proof. We have to show that $\chi_{\widetilde{\mu}}^{(f)}$ is in Eisenstein form. It is enough to prove that $\chi_\mu^{(f)} \equiv \chi_{\widetilde{\mu}}^{(f)} \pmod{\pi^2}$:

$$\chi_\mu^{(f)}(t) = \prod_{i=1}^{n}(t - \mu(\alpha_i)) \equiv \prod_{i=1}^{n}(t - \widetilde{\mu}(\alpha_i)) = \chi_{\widetilde{\mu}}^{(f)}(t) \pmod{\pi^2}$$

Therefore, if $\chi_\mu^{(f)}$ is of Eisenstein form, the same holds for $\chi_{\widetilde{\mu}}^{(f)}$. □

In order to prove that this test is practical, we need to show that every irreducible polynomial has a certificate. The way we are going to prove this is interesting and is related to the monogenicity of the rings of integers of p-adic fields (1.23).

Let $\mu \in K[x]$ be a polynomial such that $\chi_\mu^{(f)}(t) \in \mathcal{O}_K[t]$ and suppose that it passes both the Hensel and Newton tests. We want to understand if we can produce a certificate starting from μ or if we can factor it (and so f). We notice that a partial information about the inertia degree of the algebra generated by f can be obtained:

Definition 2.38. *Let $\mu \in K[x]$ be a polynomial passing both the Hensel and the Newton test. We define the inertia degree F_μ of μ as the degree of the irreducible factor ϕ_μ of $\chi_\mu^{(f)}$ over the residue field.*

In particular, if f is irreducible and L is the field generated by one of its roots, it holds $F_\mu \mid f(L|K)$ ($f(L|K)$ is the inertia degree of the field extension L/K).
Clearly, to factor f it is enough to factor $\chi_\mu^{(f)}$, as we have seen before (2.29).

To factor $\chi_\mu^{(f)}$, we can now take advantage of Newton polygons. We have seen that the Newton polygon is usually inefficient (as in this case: since μ passes the Newton test, it does not provide any useful information) and so we want to understand if its generalized Newton polygon with respect to ϕ_μ ($\chi_\mu^{(f)}$ passes the Hensel test, so has a unique irreducible factor ϕ_μ mod π) provides us more information. In order to do this, we have to consider the polynomial ϕ_μ and its characteristic polynomial $\chi_{\phi_\mu}^{(f)}$. Assume that the latter passes the Newton and the Hensel test (if not, we can factor f). Then we consider the slope of the side of $N_{\phi_\mu}(\chi_\mu^{(f)})$ $\lambda = -U_\mu/E_\mu$, with $(E_\mu, U_\mu) = 1$.

Definition 2.39. *Let $\mu \in K[x]$ be a polynomial passing both the Hensel and the Newton tests and let $\phi_\mu \in \mathcal{O}_K[x]$ be a lift of the irreducible factor of $\chi_\mu^{(f)}$ mod π. If $N_{\phi_\mu}(\chi_\mu^{(f)})$ is one-sided with slope λ, we denote by E_μ the unique positive integer such that $\lambda = -U_\mu/E_\mu$.*

We now want to find a characteristic polynomial in Eisenstein form; in the language of Newton polygons, this means that we want to obtain a polynomial such that the slope of the unique side of its polygon is of the form $1/e$ with $e \in \mathbb{N}$.

Definition 2.40. *We define γ_μ as the polynomial*

$$\gamma_\mu(t) = \frac{\phi_\mu(t)^s}{\pi^r}$$

where $r, s \in \mathbb{Z}$ satisfies $rU_\mu - sE_\mu = 1$ and $0 \leq r \leq E_\mu - 1$.

With these choices, the slope of the side of the Newton polygon of χ_{γ_μ} is $1/E_\mu$.

Proposition 2.41. *Let $f \in \mathcal{O}_K[x]$ be a monic irreducible polynomial and let $\alpha \in \overline{\mathbb{Q}}_p$ be one of its roots. Let $\mu \in K[x]$ be a polynomial such that $\chi_\mu^{(f)} \in \mathcal{O}_K[t]$. The following are equivalent:*

1. *μ certifies f*
2. *$\gamma_\mu(\mu) = \phi_\mu(\mu)$ and $E_\mu F_\mu = n$*
3. *$\mathcal{O}_K[\mu(\alpha)]$ is integrally closed*

Proof.

(1) $\Rightarrow$ (2) If $\chi_\mu^{(f)}$ is irreducible over the residue field then $E_\mu = 1$, $U_\mu = 0$ and $F_\mu = n$ (the polygon is a single horizontal segment). This means that, with the same notations as in the definition, $r = 1$ and $s = 0$ so that

$$\gamma_\mu(\mu) = \phi_\mu(\mu)$$

Otherwise, assume that $\chi_\mu^{(f)}$ is not irreducible mod π. Then the ϕ_μ-polygon is one-sided of slope $1/k$, where k is such that $\chi_\mu^{(f)} = \phi_\mu^k$. So $N_\mu = 1$ and $E_\mu = k$, $F_\mu = n/k$. Furthermore, $r = 1$ and $s = 0$ satisfies the definition of γ_μ, so that

$$\gamma_\mu = \phi_\mu$$

as desired.

(2) ⇒ (3) By the theory of Newton polygons, we get that the order generated by $\mu(\alpha)$ contains an element that generates the residue field (the roots of ϕ_μ, using Hensel's lemma) and an element whose ramification index is $1/E_\mu$ (which is $\phi_\mu(\alpha)$), and therefore it is integrally closed.

(3) ⇒ (1) If $\chi_\mu^{(f)}$ is irreducible over the residue field, μ is trivially a certificate. Assume then that $\chi_\mu^{(f)} \equiv \phi_\mu^k \pmod{\pi}$ and $k > 1$. We can write $\chi_\mu^{(f)}$ as

$$\chi_\mu^{(f)}(t) = \phi_\mu(t)^k + \pi(\phi_\mu(t)h_1(t) + h_2(t))$$

where $\deg h_2 < \deg \phi_\mu$. We want to show that $h_2 \notin \pi\mathcal{O}_K$. Assume that $h_2 \in \pi\mathcal{O}_K$. Then the element

$$\delta = \frac{\phi_\mu(\mu(\alpha))^{k-1}}{\pi}$$

belongs to $\mathcal{O}_L$ but not to $\mathcal{O}_K[\mu(\alpha)]$, giving a contradiction. Indeed, δ is a root of the polynomial

$$x^2 + h_1(\mu(\alpha))x + \frac{\phi_\mu(\mu(\alpha))^{k-2}h_2(\mu(\alpha))}{\pi}$$

and the coefficients lie in $\mathcal{O}_K[\mu(\alpha)]$.

□

Corollary 2.42. *Let $f \in \mathcal{O}_K[x]$ be a monic polynomial. Then f is irreducible if and only if there exists $\mu \in K[x]$ that certifies f.*

Proof. If there exists such a μ, then f is irreducible by Theorem 2.33. Vice versa, assume that f is irreducible. Let α be one of its roots, let $L = K(\alpha)$ and call $\mathcal{O}_L$ the integral closure of $\mathcal{O}_K$ in L. We know by proposition 1.23 that there exists $\beta \in \mathcal{O}_L$ such that $\mathcal{O}_L = \mathcal{O}_K[\beta]$. We can express β as a combination of $1, \dots, \alpha^{n-1}$ because the powers of α form a basis for L over K. Thus there exists $\mu \in K[x]$ such that $\beta = \mu(\alpha)$, so that

$$\mathcal{O}_L = \mathcal{O}_K[\beta] = \mathcal{O}_K[\mu(\alpha)]$$

By the above theorem, we get that μ certifies f, as desired. □

A factorization algorithm Before describing the algorithm, we need a technical lemma, which relates the properties of a polynomial in Eisenstein form to the algebraic properties of the field generated by one of its roots.

Proposition 2.43. *Let L/K be an extension of p-adic fields and let $\mathcal{O}_L$ and $\mathcal{O}_K$ be their rings of integers. Let Π be a uniformizing parameter of $\mathcal{O}_L$ and let $\alpha \in \mathcal{O}_L$ be a primitive element for L over K, so that $L = K(\alpha)$. Consider a polynomial $\phi \in \mathcal{O}_K[x]$ such that ϕ is irreducible mod π and $\phi(\alpha) \in (\Pi)$. The following are equivalent:*

1. *The minimal polynomial of α over K is in Eisenstein form*
2. *$(\phi(\alpha)) = (\Pi)$ and α mod Π is a primitive element for the extension of the residue fields.*

Proof.

(1) ⇒ (2) Assume that the minimal polynomial f of α is in Eisenstein form, so that there exist $\widetilde{\phi}$, h_1, $h_2 \in \mathcal{O}_K[x]$ such that

$$f(x) = \widetilde{\phi}(x)^k + \pi h_1(x)\widetilde{\phi}(x) + \pi h_2(x)$$

Notice that $\widetilde{\phi}(\alpha)$ is a generator of the maximal ideal because of corollary 2.24 applied to the $\widetilde{\phi}$-polygon of f. Therefore, there exists an exponent $s \in \mathbb{N}$ such that $v(\widetilde{\phi}(\alpha)^s) = v(\phi(\alpha))$. Since they are both irreducible mod π, $s = 1$ and $\phi(\alpha)$ is a prime element. Furthermore, $\alpha \bmod \pi$ generates the extension of the residue fields, because $\widetilde{\phi}(\alpha)^k \equiv 0 \pmod{\pi}$ and therefore the image of α coincides with a root of $\widetilde{\phi}$ mod π. Since the splitting field of $\widetilde{\phi}$ is the residue field of $\mathcal{O}_L$, we get the thesis.

(2) ⇒ (1) Choose a set Ω of q representatives of the classes of elements of the residue field of K, where q is its cardinality. We define

$$\Sigma = \{c_0 + c_1\alpha + \ldots + c_{F-1}\alpha^{\deg\phi - 1} \mid c_i \in \Omega\}$$

Since $\alpha \bmod \pi$ generates the extension of the residue fields, Σ is a set of representative of $\mathcal{O}_L/(\phi(\alpha))$ and therefore every element $\gamma \in \mathcal{O}_L$ can be written uniquely as

$$\gamma = \sum a_i \pi^i \quad a_i \in \Sigma$$

By hypothesis, $\phi(\alpha)$ generates the maximal ideal of $\mathcal{O}_L$ and $v(\phi(\alpha)) = 1/e(L|K)$. This means that $\phi(\alpha)^{e(L|K)}/\pi$ is a unit in $\mathcal{O}_L$ and so it can be expressed as follows:

$$\frac{\phi(\alpha)^{e(L|K)}}{\pi} = \sum_{i=0}^{\infty} \pi^i \sum_{j=0}^{e(L|K)-1} \lambda_{i,j}\phi(\alpha)^j$$

where each $\lambda_{i,j}$ lies in Σ and $\lambda_{0,1}$ is a unit. Each $\lambda_{i,j}$ can be written by definition as a combination of $1, \alpha, \ldots, \alpha^{\deg\phi-1}$, so that $\lambda_{i,j} = \epsilon_{i,j}(\alpha)$. Since the degrees of the $\epsilon_{i,j}$ are bounded by $\deg\phi - 1$, the following is a polynomial

$$\mu_\alpha(x) = \phi(x)^{e(L|K)} - \pi \sum_{j=0}^{e(L|K)-1} \Big(\sum_{j=0}^{\infty} \pi^j \epsilon_{i,j}(x)\Big)\phi(x)^i$$

has α as a roots and is in Eisenstein form, proving its irreducibility. Since it is monic, it is the minimal polynomial of α.

□

Now we can give the outline of the algorithm. First, we need a routine to implement the representation given in the previous proposition. More specifically, the routine takes as input two polynomials $g, \phi \in \mathcal{O}_K[x]$ such that

$$g(x) \equiv \phi(x)^s \pmod{\pi}$$

for some $s > 0$, ϕ is irreducible mod π, g is squarefree, $\deg \phi = d$, the ϕ-polygon of g has slope $-1/E$ and $Ed < \deg f = n$. It returns either a proper factorization of g or a polynomial φ such that $E_\varphi F_\varphi > Ed$ and $E_\varphi \geq E$, $F_\varphi \geq d$ (E_φ and F_φ are the invariants defined in 2.38 and 2.39). The routine tries to compute the expansion given in the previous proposition. Since $Ed < n$, the order generated by one of the roots of g is not integrally closed and such an expansion does not exist. Therefore the procedure leads either to a factorization of g or to the construction of a polynomial φ having the properties stated above. In the pseudocode, α will denote a root of g and all the characteristic polynomials are computed with respect to g.

Algorithm 1
Input: The polynomials g, ϕ and s such that $g \equiv \phi^s \pmod{\pi}$.
Output: A factorization of f or a polynomial φ such that $E_\varphi F_\varphi > Ed$.

Find $t(x) \in K[x]$ such that $t(x)\phi(x) \equiv 1 \pmod{g}$
$\mu = \phi^E$
loop
  $j = \lfloor v(\mu(\alpha)) \rfloor$
  $k = (v(\mu(\alpha)) - j)E$
  $\gamma = \pi^{-j} t(x)^k \mu(x) \pmod{g}$
  if γ fails the Hensel test **then**
    return a factorization of g
  end if
  if $F_\gamma \nmid d$ **then**
    Find $\varphi \in \mathcal{O}_K[x, \gamma(x)]$ s.t. $\mathcal{O}_K/(\pi)[\overline{\varphi}] = \mathcal{O}_K/(\pi)[\overline{\alpha}, \overline{\gamma}]$
    if φ or $\phi_\varphi(\varphi)$ fail the Hensel test **then**
      return a factorization of g
    end if
    if $E_\varphi < E$ **then**
      $\varphi = \varphi + \phi_\mu$
    end if
    return φ
  end if
  Find $\delta = \sum_{i=0}^{d-1} c_i x^i$ s.t. $\phi_\gamma(\delta(\alpha)) \equiv 0 \pmod{\pi}$ and $v(\gamma(\alpha_j) - \delta(\alpha_j)) > 0$ for some j
  if $\gamma - \delta$ fails either the Hensel test or the Newton test **then**
    return a factorization of g
  end if
  $\mu = \mu - \pi^j \phi(x)^k \delta(x)$
  if $E_\mu \nmid E$ **then**
    Find $a, b, c \in \mathbb{N}$ s.t. $(aN_\mu - cE_\mu)E + bE_\mu = \gcd(E, E_\mu)$
    $\varphi = x + \frac{\phi_\mu^b \mu(x)^a}{\pi^c} \pmod{g}$
    return φ
  end if
  if μ is sufficiently precise **then**
    return a factorization of g
  end if
end loop

Observation 2.44. *We need to clarify what "μ is sufficiently precise" means. Since we are working on a p-adic field, we need to choose a precision for the representation of every element, since we know that every element is represented as a series. After some iterations of this routine, it can happen that the polynomial μ divides g mod π^l, where l is the precision chosen. Called $\nu \in \mathcal{O}_K[x]$ a polynomial such that $g = \nu \cdot \mu \pmod{\pi^l}$, if $l > s_{\mu\nu}$ then we can lift this factorization to $\mathcal{O}_K$ using Hensel's lemma 1.54 and thus return a proper factorization of g.*

We explain how this procedure works with an example:

Example 2.45. *Assume that Algorithm 1 takes as input the polynomials*

$$g(x) = x^4 + 127x^3 + 43x^2 + 42x - 259 \qquad \phi = x^2 + x + 1$$

over $\mathbb{Z}_5$. We compute the characteristic polynomial of ϕ:

$$\chi_\phi^{(g)}(t) = t^4 - (2^4 \cdot 5 \cdot 199)t^3 + (5^4 \cdot 53)t^2 + (5^3 \cdot 7 \cdot 59)t + (5^4 \cdot 7^2)$$

The Newton polygon of $\chi_\phi^{(g)}$ is one-sided, with vertices $(0,4)$, $(4,0)$. In particular, $v(\phi(\alpha)) = 1$ for every root of g by 2.22. With the notations of the pseudocode, we compute γ, which is a polynomial such that $v(\gamma(\alpha)) = 0$, following the algorithm to compute the slope factorization (see subsection 2.1.1).

$$\gamma(x) = \frac{x^2 + x + 1}{5}$$

Computing the characteristic polynomial $\chi_\gamma^{(g)}$, it can be seen that γ passes the Hensel test

$$\chi_\gamma^{(g)}(t) = t^4 - (2^4 \cdot 199)t^3 + (5^2 \cdot 53)t^2 + (7 \cdot 59)t + 7^2$$

and the irreducible factor of $\chi_\gamma^{(g)}$ mod 5 is $\phi_\gamma(t) = t^2 + 3t + 3$. In particular, the slope factorization is trivial and that the conditions of the "if" clauses are not satisfied. Consequently, we can skip them and go to line 20.
Now, we have to find a polynomial δ satisfying $v(\phi_\gamma(\delta(\alpha))) \geq 1$ and $v((\gamma - \delta)(\alpha)) > 0$. In other words, we are trying to find one of the coefficients $\lambda_{i,j}$ of proposition 2.43. Notice that, called α a root of g, its projection $\overline{\alpha}$ to the residue field is a root of $t^2 + t + 1$. Therefore, on the splitting field of $t^2 + t + 1$, we get the factorization

$$t^3 + 3t + 3 = (t + \overline{\alpha} + 2)(t - \overline{\alpha} + 1)$$

This means that we have two possible choices for δ, namely

$$\delta_1(x) = -x - 2 \qquad \delta_1(x) = x - 1$$

and both satisfy $v((\gamma - \delta)(\alpha)) > 0$. This ambiguity is due to the fact that g is not irreducible. Indeed, $\gamma - \delta_1$ fails the Hensel test

$$\chi_{\gamma-\delta_1}^{(g)}(t) = t^4 - 3065t^3 + 18608t^2 - 34545t + 28950 \equiv t^4 + 3t^2 \equiv t^2(t^2+3) \pmod 5$$

and the same holds for $\gamma - \delta_2$:

$$\chi_{\gamma-\delta_2}^{(g)}(t) = t^4 - 3315t^3 + 12433t^2 - 19770t + 7825 \equiv t^4 + 3t^2 \equiv t^2(t^2+3) \pmod 5$$

and in both cases we can get a factorization of g by 2.29. Notice that if we choose $\delta_1(x)$ and skip this "if" clause, then the approximation given is "sufficiently precise" to give a factorization of g. Indeed, the algorithm sets $\mu = t^2 + t + 1 - 5\delta_1 = x^2 + 6x + 11$ and it holds $\mu \mid g \pmod{5^3}$. In particular, called

$$\nu = x^2 + 121x - 694$$

we have $\chi = \mu \cdot \nu \pmod{5^3}$ and the reduced resultant of μ and ν is $s_{\mu\nu} = 1$. This means that we can use Hensel's lemma 1.54 to lift these factors and get a factorization of g.

Now, we give the pseudocode of the factorization algorithm. It takes as input a polynomial $f \in \mathcal{O}_K[x]$ and returns either a proper factorization or a certificate for f. The algorithm tries to find iteratively a polynomial ν that certifies f. Starting from $\nu(x) = x$, ν is replaced at every iteration by the polynomial φ given in output by the routine. If ν fails the Newton or the Hensel tests, the algorithm returns a proper factorization of f by using Hensel's lemma or the slope factorization. If it passes them and $E_\nu F_\nu = n$, then it gives in output a certificate for f. If these conditions are not satisfied, it applies Algorithm 1 to $(\chi_\nu^{(f)}, \phi_\nu)$ (the characteristic polynomial of ν and a lift of its irreducible factor mod π). If the routine returns a factorization of $\chi_\nu^{(f)}$, we can obtain a factorization of f by the computation of a gcd, while if it returns a polynomial φ we have to iterate the procedure.

Algorithm 2 - Factorization of polynomials over $\mathcal{O}_K$
Input: a monic polynomial $f \in \mathcal{O}_K[x]$
Output: a proper factorization of f or a certificate for f

1: $\nu(x) = x$
2: **loop**
3: **while** $\operatorname{disc}(\chi_\nu^{(f)}) = 0$ **do** ▷ We want $\chi_\nu^{(f)}$ to be separable
4: $\nu(x) = \nu(x) + \pi x$
5: **end while**
6: **if** ν or $\phi_\nu(\nu)$ fail the Hensel test or the Newton test **then**
7: **return** a proper factorization of f
8: **end if**
9: **if** $N_\nu > 1$ **then**
10: $\nu(x) = \nu(x) + \gamma_\nu(\nu(x))$ ▷ Then $N_\nu = 1$
11: **end if**
12: **if** $E_\nu F_\nu = n$ **then**
13: **return** μ is a certificate for f
14: **end if**
15: Apply **Algorithm 1** to the pair $(\chi_\nu^{(f)}, \phi_\nu)$
16: **if** Algorithm 1 returns a factorization of $\chi_\nu^{(f)}$ **then**
17: **return** a proper factorization of f
18: **else**
19: $\nu = \varphi$ ▷ φ is the output of Algorithm 1
20: **end if**
21: **end loop**

To prove that the factorization algorithm terminates, we have to bound the number of iterations needed in Algorithm 1: the following theorem shows that it ends before $v(\mu(\alpha))$ becomes greater than $2 \cdot v(\mathrm{disc}(g))/\deg f$. The valuation of $\mu(\alpha)$ increases during the execution of the algorithm and therefore such a bound will be eventually reached. When this happens, the following theorem implies the irreducibility of g and consequently the irreducibility of f and the algorithm terminates.

Theorem 2.46. *Let $\alpha_1, \dots, \alpha_n$ and $\beta_1, \dots, \beta_s$ be elements of an algebraic closure $\overline{K}$ of K. Assume that*

- $g(x) = \prod_{i=1}^{n}(x - \alpha_i)$ *is a squarefree polynomial in $\mathcal{O}_K[x]$*
- $h(x) = \prod_{i=1}^{s}(x - \beta_i)$ *is a polynomial in $K[x]$*
- $2 \cdot v(\mathrm{disc}(g)) \geq n \cdot v(h(\alpha_i))$ *for all $i = 1, \dots, n$*
- *The degree of any irreducible factor of g is $\geq s$*

Then $s = n$ and g is irreducible over K.

We need some preliminary lemmas.

Lemma 2.47. *Let g as above, let $\alpha \in \overline{K}$ and let $\widetilde{\alpha}$ be one of the roots of f such that $v(\alpha - \widetilde{\alpha})$ is maximal. Then*

$$v(g(\alpha)) = \sum_{i=1}^{n} \min\{v(\alpha - \widetilde{\alpha}), v(\alpha_i - \widetilde{\alpha})\}$$

Proof. Clearly, we have

$$v(g(\alpha)) = \sum_{i=1}^{n} v(\alpha - \alpha_i)$$

By triangular inequality,

$$v(\alpha - \alpha_i) = v(\alpha - \widetilde{\alpha} + \widetilde{\alpha} - \alpha_i) \geq \min\{v(\alpha - \widetilde{\alpha}), v(\widetilde{\alpha} - \alpha_i)\}$$

Since we want to determine an equality, we use observation 1.10 and we study first what happens when $v(\alpha - \widetilde{\alpha}) \neq v(\widetilde{\alpha} - \alpha_i)$. If $v(\alpha - \widetilde{\alpha}) > v(\widetilde{\alpha} - \alpha_i)$, then it holds $v(\alpha - \alpha_i) = v(\widetilde{\alpha} - \alpha_i)$ and so

$$v(\alpha - \alpha_i) = v(\widetilde{\alpha} - \alpha_i) = \min\{v(\alpha - \widetilde{\alpha}), v(\alpha_i - \widetilde{\alpha})\}$$

If $v(\widetilde{\alpha} - \alpha_i) > v(\alpha - \widetilde{\alpha})$, then the same argument shows that $v(\alpha - \alpha_i) = v(\alpha - \widetilde{\alpha})$ and

$$v(\alpha - \alpha_i) = v(\alpha - \widetilde{\alpha}) = \min\{v(\alpha - \widetilde{\alpha}), v(\alpha_i - \widetilde{\alpha})\}$$

We only need to understand what happens when $v(\alpha - \widetilde{\alpha}) = v(\widetilde{\alpha} - \alpha_i)$. If the following equality holds

$$v(\alpha - \alpha_i) = \min\{v(\alpha - \widetilde{\alpha}), v(\widetilde{\alpha} - \alpha_i)\}$$

we are done. Assume then that

$$v(\alpha - \alpha_i) > \min\{v(\alpha - \widetilde{\alpha}), v(\widetilde{\alpha} - \alpha_i)\}$$

By hypothesis, $\widetilde{\alpha}$ is the root of g such that $v(\alpha - \widetilde{\alpha})$ is maximal and therefore we get a contradiction. This means that this last case never holds, proving the thesis. □

Lemma 2.48. *Assume that the same hypotheses of theorem 2.46 hold. Then $h(x) \in \mathcal{O}_K[x]$ and h is irreducible over K. Furthermore, there exist a root α of g and a root β of h such that $K(\alpha) = K(\beta)$. In particular, the minimal polynomial of α over K is an irreducible factor of g of degree s.*

Proof. Let $g = g_1 \dots g_m$ be the factorization of g into monic irreducible factors over K and reorder the roots in the following way:

$$g_i(x) = \prod_{j=1}^{n_i} (x - \alpha_{i,j})$$

Let G_i be the Galois group of the splitting field of g_i over K and Δg_i be the minimal distance between two distinct zeroes of g_i. Denote by $\widetilde{\alpha}_{i,j}$ a root of g_i such that $v(\beta_j - \widetilde{\alpha}_{i,j})$ is maximal. We want to show that we can apply Krasner's lemma (1.43). Assume by contradiction that $v(\beta_j - \widetilde{\alpha}_{i,j}) \leq \Delta g_i$. Then, using the previous lemma, we get

$$\begin{aligned}
v(g_i(\beta_j)) &= \sum_{k=1}^{n_i} v(\beta_j - \alpha_{i,k}) \\
&= \sum_{k=1}^{n_i} \min\{v(\beta_j - \widetilde{\alpha}_{i,j}), v(\widetilde{\alpha}_{i,j} - \alpha_{i,k})\} \\
&\leq \sum_{k=1}^{n_i} \min\{\Delta g_i, v(\widetilde{\alpha}_{i,j} - \alpha_{i,k})\} \\
&= \Delta g_i + \sum_{\alpha_{i,j} \neq \widetilde{\alpha}_{i,j}} \min\{\Delta g_i, v(\widetilde{\alpha}_{i,j} - \alpha_{i,k})\} \\
&= \Delta g_i + \sum_{\alpha_{i,j} \neq \widetilde{\alpha}_{i,j}} v(\widetilde{\alpha}_{i,j} - \alpha_{i,k})
\end{aligned}$$

Reordering the roots, we can assume that $\Delta g_i = v(\alpha_{i,1} - \alpha_{i,2})$. We can choose $\sigma_{i,1}, \dots, \sigma_{i,s} \in G_i$ such that the elements

$$\sigma_{i,1}(\widetilde{\alpha}_{i,1}) \qquad \sigma_{i,2}(\widetilde{\alpha}_{i,1}) \qquad \dots \qquad \sigma_{i,s}(\widetilde{\alpha}_{i,1})$$

are distinct and $\tau_{i,1}, \dots, \tau_{i,s} \in G_i$ such that

$$\tau_{i,1}(\widetilde{\alpha}_{i,1}) \qquad \tau_{i,2}(\widetilde{\alpha}_{i,2}) \qquad \dots \qquad \tau_{i,s}(\widetilde{\alpha}_{i,s})$$

are distinct. With these choices, the following equalities trivially hold

$$\Delta g_i = v(\sigma_{i,j}(\alpha_{i,1}) - \sigma_{i,j}(\alpha_{i,2})) \qquad v(\widetilde{\alpha}_{i,j} - \alpha_{i,k}) = v(\tau_{i,j}(\widetilde{\alpha}_{i,j} - \alpha_{i,k}))$$

Hence we get

$$\begin{aligned}
\sum_{j=1}^{s} g_i(\beta_j) &\geq \sum_{j=1}^{s} \Big(\Delta g_i + \sum_{\alpha_{i,k} \neq \widetilde{\alpha}_{i,j}} v(\widetilde{\alpha}_{i,j} - \alpha_{i,k}) \Big) \\
&= \sum_{j=1}^{s} \Delta g_i + \sum_{j=1}^{s} \sum_{\alpha_{i,k} \neq \widetilde{\alpha}_{i,j}} v(\widetilde{\alpha}_{i,j} - \alpha_{i,k})
\end{aligned}$$

$$
\begin{aligned}
&= \sum_{j=1}^{s} v(\sigma_{i,j}(\alpha_{i,1}) - \sigma_{i,j}(\alpha_{i,2})) + \sum_{j=1}^{s} \sum_{\alpha_{i,k} \neq \widetilde{\alpha}_{i,j}} v(\tau_{i,j}(\widetilde{\alpha}_{i,j} - \alpha_{i,k})) \\
&\leq 2 \cdot v(\mathrm{disc}(g_i))
\end{aligned}
$$

Notice now that

$$
\begin{aligned}
\max_{1 \leq k \leq n} n \cdot v(h(\alpha_k)) &\leq \sum_{k=1}^{n} v(h(\alpha_k)) \\
&= \sum_{j=1}^{s} v(g(\beta_j)) \\
&= \sum_{i=1}^{m} \sum_{j=1}^{s} v(g_i(\alpha_j)) \\
&\leq \sum_{i=1}^{m} 2 \cdot v(\mathrm{disc}(g_i)) \\
&\leq 2 \cdot v(\mathrm{disc}(g))
\end{aligned}
$$

and this contradicts the hypotheses. This means that there are some indices such that $v(\beta_j - \widetilde{\alpha}_{i,j}) > \Delta g_i$. By Krasner's lemma, $K(\widetilde{\alpha}_{i,j}) \subseteq K(\beta_j)$ and, since the degree of every irreducible component of g is greater than s, equality holds. Therefore, $n_i = s$ and h is irreducible. To conclude, we notice that $g \in \mathcal{O}_K[x]$ and $v(\beta_j - \widetilde{\alpha}_{i,j}) > \Delta g_i$: this proves that $h \in \mathcal{O}_K[x]$. □

Lemma 2.49. *Assume that the hypotheses of theorem 2.46 hold. Then $K(\alpha) \simeq K(\alpha)$ for every root α of g and every root β of h.*

Proof. If $n = s$, the statement follows from the previous lemma. Assume that $s < n$. Let g_1 be the irreducible factor of g having the property of the above lemma and let $g_2 = g/g_1$. Denote by $B = \max_{j=1}^{n} v(h(\alpha_j))$, where $\alpha_1, \ldots, \alpha_n$ are the roots of g, by $\alpha_{1,j}$ the roots of g_1 and by $\alpha_{2,j}$ the roots of g_2. We know that $h \in \mathcal{O}_K[x]$ is irreducible by the previous lemma. We notice that

$$
\begin{aligned}
\sum_{i=1}^{s} v(g_1(\beta_i)) &= \sum_{j=1}^{s} v(g(\alpha_{1,j})) \geq nB \\
\sum_{i=1}^{s} v(g_2(\beta_i)) &= \sum_{j=1}^{n-s} v(h(\alpha_{2,j})) \geq (n-s)B
\end{aligned}
$$

and so it follows

$$
v(g_1(\beta_i)) \geq B \qquad\qquad v(g_2(\beta_i)) \geq \frac{n-s}{s} B
$$

for all the roots β_i of h. Furthermore,

$$
v(\mathrm{disc}(g_1)) + v(\mathrm{Res}(g_1, g_2)) = \sum_{i=1}^{s} \Big(\sum_{j \neq i} v(\alpha_{1,i} - \alpha_{i,j}) + \sum_{j=1}^{n-s} v(\alpha_{1,i} - \alpha_{2,j}) \Big)
$$

Let G be the Galois group of the splitting field of g_1; notice that this coincides with the Galois group of the splitting field of h. Denote by $\widetilde{\beta}_i$ one of the roots of h that is closest to $\alpha_{1,i}$ and let $\sigma_{j,i} \in G$ such that $\sigma_{j,i}(\alpha_{1,j}) = \alpha_{1,i}$. Then

$$v(\widetilde{\beta}_i - \alpha_{1,i}) \geq v(\sigma_{j,i}(\widetilde{\beta}_i - \alpha_{1,j})) = v(\widetilde{\beta}_i - \alpha_{i,j})$$

Thus

$$\begin{aligned}
A_i &:= \sum_{j \neq i} v(\alpha_{1,i} - \alpha_{1,j}) + \sum_{j=1}^{n-s} v(\alpha_{1,i} - \alpha_{2,j}) \\
&= \sum_{j \neq i} v(\alpha_{1,i} - \widetilde{\beta}_i + \widetilde{\beta}_i - \alpha_{1,j}) + \sum_{j=1}^{n-s} v(\alpha_{1,i} - \widetilde{\beta}_i + \widetilde{\beta}_i - \alpha_{2,j}) \\
&\geq \sum_{j \neq i} \min\{v(\alpha_{1,i} - \widetilde{\beta}_i), v(\widetilde{\beta}_i - \alpha_{1,j})\} + \sum_{j=1}^{n-s} \min\{v(\alpha_{1,i} - \widetilde{\beta}_i), v(\widetilde{\beta}_i - \alpha_{2,j})\} \\
&= \sum_{j \neq i} v(\widetilde{\beta}_i - \alpha_{1,j}) + \sum_{j=1}^{n-s} \min\{v(\alpha_{1,i} - \widetilde{\beta}_i), v(\widetilde{\beta}_i - \alpha_{2,j})\}
\end{aligned}$$

If $v(\alpha_{1,i} - \widetilde{\beta}_j) \leq v(\widetilde{\beta}_i - \alpha_{2,j})$ for some j then

$$B \leq v(g_1(\widetilde{\beta}_i)) \leq A_i$$

On the other hand, if $v(\alpha_{1,i} - \widetilde{\beta}_j) > v(\widetilde{\beta}_i - \alpha_{2,j})$ for all j then

$$B \leq \frac{n-s}{s} B \leq v(g_2(\widetilde{\beta}_i)) = \sum_{j=1}^{n-s} v(\widetilde{\beta}_i - \alpha_{2,j}) \leq A_i$$

Therefore, we get the following chain of inequalities

$$\begin{aligned}
nB &< 2v(\mathrm{disc}(g)) \\
&= 2v(\mathrm{disc}(g_1)) + 2v(\mathrm{disc}(g_2)) + 4v(\mathrm{Res}(g_1, g_2)) \\
&\leq 2sB \cdot v(\mathrm{disc}(g_2))
\end{aligned}$$

This means that $(n-s)B < 2v(\mathrm{disc}(g_2))$. We have shown that g_2 satisfies the hypotheses of theorem 2.46 and we can apply lemma 2.48 to it. Inductively, g splits into a product of irreducible factors of degree s and for every root α of g and for every root β of h holds $K(\alpha) \simeq K(\beta)$. □

We are now ready to prove the theorem 2.46:

Proof of 2.46. We have shown in the last lemma that, if g splits, all its factors must have degree s. Clearly, if $s = n$ we have the thesis. Suppose that $s < n$. Write $g = g_1 \dots g_{n/s}$ and

$$g_i = \prod_{j=1}^{n} (x - \alpha_{i,j})$$

Denote by $\widetilde{\beta}_{r,i}$ a root of h that is closest to $\alpha_{r,i}$. As done in the previous lemma, we have

$$A_{r,i} = \sum_{j \neq i} v(\alpha_{r,i} - \alpha_{r,j}) + \sum_{s \neq r} \sum_{j=1}^{s} v(\alpha_{r,i} - \alpha_{s,j})$$

$$\begin{aligned}
&\geq \sum_{j\neq i} \min\{v(\alpha_{r,i} - \widetilde{\beta}_{r,i}), v(\widetilde{\beta}_{r,i} - \alpha_{r,j})\} + \sum_{s\neq r}\sum_{j=1}^{s} v(\alpha_{r,i} - \alpha_{s,j}) \\
&\geq \sum_{j\neq i} v(\widetilde{\beta}_{r,i} - \alpha_{r,j}) + \sum_{s\neq r}\sum_{j=1}^{s} \min\{v(\alpha_{r,i} - \widetilde{\beta}_{r,i}), v(\widetilde{\beta}_{r,i} - \alpha_{s,j})\} \\
&\geq \max_{i,j} v(h(\alpha_{i,j}))
\end{aligned}$$

As a consequence,

$$v(\mathrm{disc}(g)) = \sum_{r=1}^{n/s}\sum_{i=1}^{s} A_{r,i} \geq \max_{i,j} v(h(\alpha_{i,j}))^n \geq 2 \cdot v(\mathrm{disc}(g))$$

This gives a contradiction, hence $n = s$, proving that g is irreducible. □

Summarizing,

- We have presented an irreducibility test for a polynomial f over a p-adic field K. This criterion is based on the existence of a polynomial μ whose characteristic polynomial $\chi_\mu^{(f)}$ is in Eisenstein form and, in particular, irreducible. We have proven that the existence of this polynomial is related to the monogenicity of the ring of the integers of a p-adic field; knowing such a polynomial μ, we can construct an integral basis for the ring of integers.
- We have described an algorithm for factoring polynomials over a p-adic field K. The algorithm tries to prove the irreducibility of f, searching for a certificate $\mu \in K[x]$ for f. Given a polynomial μ, it tests if $\chi_\mu^{(f)}$ is in Eisenstein form, constructing an approximation g of $\chi_\mu^{(f)}$. If μ is not a certificate, the construction of g leads to a new μ or to a factorization of $\chi_\mu^{(f)}$ (and consequently a factorization of f). During the execution of the algorithm, the valuation of $g(\beta)$ increases, where β is a root of $\chi_\mu^{(f)}$, and theorem 2.46 proves that the algorithm terminates.

CHAPTER 3

Algorithms

In this chapter, we will study the idea of the algorithm in [10] and the algorithm given in [6] for the computation of all the factorizations of a monic polynomial f in $\mathcal{O}_K/(\pi^l)$ for l sufficiently large (depending on the discriminant of f). These algorithms are quite efficient, because they reduce the problem to p-adic factorization and linear algebra. Then, we will discuss the implementation of a brute-force algorithm in order to find all the factorizations regardless of the discriminant. Finally, we will consider the specific problem of finding the factorizations over $\mathcal{O}_K/(\pi^2)$, following [21].

3.1 Factorization over $\mathcal{O}_K/(\pi^l)$ for large l

We dedicate this section to the study of a method for factoring polynomials over $\mathcal{O}_K/(\pi^l)$ for l sufficiently large. The main tool of this algorithm is Hensel's lemma, that allows us to take advantage of the factorization algorithm over the p-adics to obtain all the factorizations of a polynomial mod π^l.
In the first chapter, we have seen that the effectiveness of Hensel's lemma 1.54 depends on the discriminant of the polynomial. In this section, we will usually assume that K is a p-adic field and $\mathcal{O}_K$ is its ring of integers and we will consider a monic polynomial $f \in R[x]$ such that $\operatorname{disc}(f) \neq 0$, where R is a discrete valuation ring whose completion is $\mathcal{O}_K$. We will consider the normalized valuation on K, so that $v(\pi) = 1$, where π is a uniformizing parameter of R. If $l \in \mathbb{N}$ is a positive integer such that $l > v(\operatorname{disc}(f))$, Hensel's lemma implies that if f splits mod π^l

$$f \equiv gh \pmod{\pi^l}$$

then there exist two polynomials $G, H \in \mathcal{O}_K[x]$ such that $f = GH$ over $\mathcal{O}_K$ and

$$g \equiv G \pmod{\pi^{l-s_{gh}}} \qquad h \equiv H \pmod{\pi^{l-s_{gh}}}$$

where s_{gh} denotes the valuation of the reduced resultant of f, g, defined in 1.48. This means that two different factorizations of f mod π^l must coincide mod $\pi^{l-s_{gh}}$, because $\mathcal{O}_K[x]$ is a UFD. This argument leads to the following:

Theorem 3.1. *Let $f \in R[x]$ be a monic polynomial such that* $\operatorname{disc}(f) \neq 0$ *and*

consider a factorization into monic irreducible polynomials $g_i \in \mathcal{O}_K[x]$

$$f = \prod_{i=1}^{s} g_i$$

Assume that $f \equiv gh \pmod{\pi^l}$ *with* $g, h \in R[x]$ *monic and* $l > v(\mathrm{disc}(f))$*. Then there exists a partition*

$$\{1, \dots, s\} = S_1 \cup S_2$$

such that

$$g \equiv \prod_{i \in S_1} g_i \pmod{\pi^{l - s_{gh}}} \qquad h \equiv \prod_{i \in S_2} g_i \pmod{\pi^{l - s_{gh}}}$$

Proof. By Hensel's lemma 1.54, we can lift the factorization $f \equiv gh \pmod{\pi^l}$ to a factorization $f = GH$ in $\mathcal{O}_K[x]$ such that

$$g \equiv G \pmod{\pi^{l - s_{gh}}} \qquad h \equiv H \pmod{\pi^{l - s_{gh}}}$$

The uniqueness of the factorization over $\mathcal{O}_K$ implies that there exists a partition as in the statement. □

This theorem suggests that, in order to obtain the factorizations of f mod π^l, we can consider the factorization of f over the completion, consider its projection mod $\pi^{l - s_{gh}}$ and then lift this factorization to $\mathcal{O}_K/(\pi^l)$ to find all the factors of f. This is the key part of the algorithms. We investigate first how to deal with this problem in the case of a polynomial $f \in R[x]$ having only two different irreducible factors. In this case, we can give a characterization of these lifts in terms of the resultant.
Specifically, let $f \in R[x]$ be a monic polynomial of degree $n + m$ and let $g, h \in \mathcal{O}_K[x]$ be two polynomials of degree n, m respectively such that

$$f \equiv gh \pmod{\pi^l}$$

Assume that $\mathrm{Res}(g, h) \neq 0$ and let $A, B \in R[x]$ of degrees lower than n, m such that

$$f \equiv (g + \pi^{l - s_{gh}} A)(h + \pi^{l - s_{gh}} B) \pmod{\pi^l}$$

We want to find conditions on the coefficients of $A, B \in \mathcal{O}_K[x]$. Computing the product, we get

$$\pi^{l - s_{gh}}(Ah + Bg) - \pi^{2l - 2s_{gh}} AB \equiv 0 \pmod{\pi^l}$$

Since by hypothesis $l > v(\mathrm{disc}(f))$, it holds $l > 2s_{gh}$ by observation 1.55. Therefore, $2l - 2s_{gh} \geq l$ and we get

$$Ah + Bg \equiv 0 \pmod{\pi^{s_{gh}}}$$

We denote by a_i, b_i the coefficients of A, B, such that

$$A = \sum_{i=0}^{n-1} a_i x^i \qquad B = \sum_{i=0}^{m-1} b_i x^i$$

Then the last relation is equivalent to the linear system

$$S(g,h)\begin{pmatrix} b_{m-1} \\ \vdots \\ b_0 \\ a_{n-1} \\ \vdots \\ a_0 \end{pmatrix} \equiv 0 \pmod{\pi^{s_{gh}}}$$

Therefore all the lifts are characterized as the elements of the kernel of this linear system. To solve this system, we can consider the matrix $S(g,h)$ and its Smith normal form, that exists since $\mathcal{O}_K$ is a PID. Specifically, we know that there exist two matrices $P, Q \in \mathrm{GL}(n+m, \mathcal{O}_K)$ such that

$$P \cdot S(g,h) \cdot Q = \begin{pmatrix} d_1 & & & \\ & d_2 & & \\ & & \ddots & \\ & & & d_{n+m} \end{pmatrix}$$

where $d_i \mid d_{i+1}$ for $i = 1, \ldots, n+m-1$. Let j be the minimum index such that $\pi \mid d_j$ (and so $\pi \mid d_i$ for all $i \geq j$) and let π^{t_i} be the maximum power of π dividing d_i for $i = j, \ldots n+m$. Such an index exists because by hypothesis $\pi \mid \det S(g,h) = d_1 d_2 \ldots d_{n+m}$. Clearly, the kernel of the diagonal matrix over $\mathcal{O}_K/(\pi^{s_{gh}})$ is generated by the elements

$$\begin{cases} \pi^{s_{gh}-t_i} e_i & \text{if } s_{gh} \geq t_i \\ e_i & \text{if } s_{gh} < t_i \end{cases}$$

for $i = j, \ldots, n+m$. Since P and Q are invertible over $\mathcal{O}_K/(\pi^{s_{gh}})$, we get that the kernel of $S(g,h)$ is generated by the elements

$$\begin{cases} \pi^{s_{gh}-t_i} Q e_i & \text{if } s_{gh} \geq t_i \\ Q e_i & \text{if } s_{gh} < t_i \end{cases}$$

Using this method, we can give the outline of an algorithm, with the additional hypothesis that f has only two factors over $\mathcal{O}_K$. In this case, we have shown that all the factorizations of f into irreducible factors coincide mod $\pi^{l-s_{gh}}$. Therefore, the algorithm works in the following way:

- Given the factorization of $f \in R[x]$ in $\mathcal{O}_K[x]$ $f = gh$, compute s_{gh}
- If $s_{gh} = 0$, then f has a unique factorization $f \equiv gh \pmod{\pi^l}$.
- If $s_{gh} > 0$, consider the factorization $f = gh$ over $\mathcal{O}_K/(\pi^{l-s_{gh}})$
- Lift the factors to $\mathcal{O}_K/(\pi^l)[x]$

Generalizing this procedure to the case of a polynomial having more than 2 irreducible factors in $\mathcal{O}_K[x]$ is not easy. An inductive approach has been developed in [10]. We will not follow this article to solve this issue; the method

described can be improved ([6]) in order to process more than 2 factors at the same time by extending the notion of resultant of two polynomials.

Consider a monic polynomial $f \in R[x]$ and its factorization in the completion

$$f = \prod_{i=1}^{s} g_i$$

where every $g_i \in \mathcal{O}_K[x]$ is monic and irreducible of degree $n_i < \deg f = n$. We denote by h_i the polynomials obtained by multiplying all the factors of f except one, namely

$$h_i = \prod_{j \neq i} g_j$$

which have consequently degree $\hat{n}_i = n - n_i$. Denoting by $h_j^{(i)}$ the coefficients of h_i, we can write

$$h_i = \sum_{j=0}^{\hat{n}_i} h_j^{(i)} x^j$$

and consider the related block

$$M_{h_i} = \overbrace{\begin{pmatrix} h^i_{\hat{n}_i} & 0 & \dots & 0 \\ h^i_{\hat{n}_i - 1} & h^i_{\hat{n}_i} & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ \vdots & \vdots & & h^i_{\hat{n}_i} \\ \vdots & \vdots & & \vdots \\ h^i_0 & \vdots & & \vdots \\ & h^i_0 & & \vdots \\ & & \ddots & \vdots \\ & & & h^i_0 \end{pmatrix}}^{n_i}$$

given by stripes having the same entries (the coefficients of h_i).

Definition 3.2. *We define the generalized Sylvester matrix of $h_1, \dots, h_s \in \mathcal{O}_K[x]$ as the matrix*

$$M(h_1, \dots, h_s) = \left(\begin{array}{c|c|c|c} M_{h_1} & M_{h_2} & \dots & M_{h_s} \end{array} \right)$$

which is a $n \times n$ matrix. We define $r(h_1, \dots, h_s)$ as the valuation of the determinant of $M(h_1, \dots, h_s)$,

$$r(h_1, \dots, h_s) = v(\det(M(h_1, \dots, h_s)))$$

Notice that this is a clear generalization of the usual Sylvester matrix, for example $M(h_1, h_2) = S(g_2, g_1)$. Furthermore, even if the matrix depends on the ordering of the polynomials, the valuation of the determinant is independent from it.

We want to recover all the good properties of the Sylvester matrix. In our notations, when it is clear which polynomials $h_1, \ldots, h_s$ we are taking into account, we will denote simply by M the matrix and by r the valuation of its determinant.

Observation 3.3. *We know that in the case of the standard Sylvester matrix of two polynomials $g, h \in R[x]$, the resultant $\operatorname{Res}(g,h)$ belongs to the ideal (g,h); more specifically, there exist $A, B \in R[x]$ such that*

$$Ag + Bh = \operatorname{Res}(g,h)$$

and $\deg A < \deg h$, $\deg B < \deg g$. The same proof shows that the determinant of the generalized Sylvester matrix $M(h_1, \ldots, h_s)$ can be expressed as a combination

$$\det M = \sum_{i=1}^{s} \psi_i h_i$$

where $\deg \psi_i < n_i$.

Proposition 3.4. *In the settings described above, $\det M = 0$ if and only if there are two indices $i \neq j$ such that $\deg(\gcd(g_i, g_j)) > 0$.*

Proof. First, suppose that $\det M = 0$. By observation 3.3, there exists a non-trivial combination of the h_i giving 0:

$$\sum_{i=1}^{s} \psi_i h_i = 0$$

Then

$$-\psi_1 h_1 = \sum_{i=2}^{s} \psi_i h_i$$

Since by definition $g_1 \mid h_i$ for all $i \geq 2$, it holds $g_i \mid \psi_1 h_1$. If $\deg(\gcd(g_i, g_j)) = 0$ for all $i \neq j$, then $\gcd(g_1, h_1) = 1$, hence $g_1 \mid \psi_1$. However, by hypothesis $\deg \psi_1 < \deg g_1$, giving a contradiction.

Vice versa, assume that there are two indices $i \neq j$ such that $\deg \gcd(g_i, g_j) \geq 1$. We call d their common factor; then $d \mid h_i$ for all i and therefore $d \mid \det M$. If $\det M \neq 0$, then $\deg \det M \geq \deg d \geq 1$, giving a contradiction (the determinant lies in $\mathcal{O}_K$). □

This proposition allows us to obtain the same results that hold for the resultant, for instance

Proposition 3.5. *Let $\alpha_{i,j}$ be the roots of g_i in an algebraic closure of $\mathbb{Q}_p$. Then*

$$\det M = \prod_{i=1}^{s-1} \prod_{j=i+1}^{s} \prod_{k=1}^{n_i} \prod_{e=1}^{n_j} (\alpha_{i,k} - \alpha_{j,e})$$

Proof. First of all, we notice that every coefficient of h_i is a symmetric function of the elements $\alpha_{j,e}$ for $j \neq i$. Since $\det M$ is a homogeneous polynomial in the coefficients of h_i, it is a symmetric function of the $\alpha_{i,j}$. Therefore each $\alpha_{i,j}$ has degree at most $n - n_i$ in $\det M$. By the previous proposition, $\det M = 0$ if

and only if there are two indices $i \neq j$ such that $\deg \gcd(g_i, g_j) \geq 1$, which is equivalent to say that they have a common root in the algebraic closure. This means that $\det M$ is divisible by $\alpha_{i,k} - \alpha_{j,e}$ for $1 \leq i < j \leq s$, $1 \leq k \leq n_i$, $1 \leq e \leq n_j$ and therefore the right hand side of the statement divides the left one. However, the right hand side has degree exactly $n - n_i$ in each $\alpha_{i,j}$ and therefore the two sides differ by a constant factor.
We want to show that this factor is one. We notice that, expanding the product, the right hand side contains the term

$$\prod_{i=1}^{s-1} \prod_{k=1}^{n_i} \alpha_{i,k}^{\sum_{j=i+1}^{s} n_j}$$

The same holds for the left hand side. Indeed, using the Laplace formula, the only way to obtain an element of this degree is to choose the last stripe of the first block, the second last stripe of the second block and so on. This element has positive sign and so we get the equality. □

Corollary 3.6. *Let $f \in R[x]$ be a monic polynomial and let $g_1, \ldots, g_s \in \mathcal{O}_K[x]$ be monic irreducible polynomials such that*

$$f = \prod_{i=1}^{s} g_i$$

over $\mathcal{O}_K$. Let $h_1, \ldots, h_s$ as above and let $M = M(h_1, \ldots, h_s)$ be their generalized Sylvester matrix. Then

$$\operatorname{disc}(f) = (\det M)^2 \prod_{i=1}^{s} \operatorname{disc}(g_i)$$

Proof. By the previous proposition,

$$(\det M)^2 = \prod_{i=1}^{s-1} \prod_{j=i+1}^{s} \prod_{k=1}^{n_i} \prod_{e=1}^{n_j} (\alpha_{i,k} - \alpha_{j,e})^2$$

while

$$\operatorname{disc}(f) = \prod_{i=1}^{s-1} \prod_{j=i}^{s} \prod_{k=1}^{n_i} \prod_{e=1}^{n_j} (\alpha_{i,k} - \alpha_{j,e})^2$$

(the only difference is the range of the index j). To conclude, it is enough to notice that

$$\operatorname{disc}(g_i) = \prod_{k=1}^{n_i} \prod_{e=1}^{k-1} (\alpha_{i,k} - \alpha_{i,e})^2$$

and these are exactly the missing elements of the product. □

Now, we prove another constructing version of Hensel's lemma which uses this new concept of resultant. First, we need a lifting method:

Proposition 3.7. *Let $f = \prod_{i=1}^{s} g_i$ be the factorization of a monic polynomial $f \in R[x]$ into monic irreducible factors $g_i \in \mathcal{O}_K[x]$ and let*

$$h_i = \prod_{j \neq i} g_j$$

Given $\delta \in R[x]$ a polynomial of degree $\deg \delta < \deg f = n$, there exist unique polynomials $\psi_i \in R[x]$ such that

$$(\det M)\delta = \sum_{i=1}^{s} \psi_i h_i$$

and $\deg \psi_i < \deg h_i = n_i$.

Proof. The proof is essentially the same as the one given in the first chapter (1.50). We write

$$\delta = \sum_{i=0}^{n-1} \delta_i x^i \qquad\qquad \psi_i = \sum_{i=0}^{n_i-1} \psi_{i,j} x^j$$

The thesis is equivalent to a solution of the linear system

$$M(h_1, \ldots, h_s) \cdot \begin{pmatrix} \psi_{1,n_1-1} \\ \vdots \\ \psi_{1,0} \\ \vdots \\ \psi_{s,n_s-1} \\ \vdots \\ \psi_{r,0} \end{pmatrix} = \det M(h_1, \ldots, h_s) \cdot \begin{pmatrix} \delta_{n-1} \\ \vdots \\ \delta_0 \end{pmatrix}$$

The entries of $\det M(h_1, \ldots, h_s) \cdot M(h_1, \ldots, h_s)^{-1}$ are in $\mathcal{O}_K$ (it follows easily from the adjoint matrix formula) and this gives a solution which is clearly unique. □

Proposition 3.8. *Let $g_1, \ldots g_s, u_1, \ldots, u_s \in \mathcal{O}_K[x]$ be monic polynomials. We call*

$$h_i = \prod_{j \neq i} g_i \qquad\qquad \widetilde{h}_i = \prod_{j \neq i} u_i$$

and assume that $g_i \equiv u_i \pmod{\pi^r}$ for all indices i, where $r = r(h_1, \ldots, h_s)$. Then

$$r(h_1, \ldots, h_s) = r(\widetilde{h}_1, \ldots, \widetilde{h}_s)$$

Proof. It is enough to notice that the multilinearity of the determinant implies that

$$\det M(h_1, \ldots, h_s) \equiv \det M(\widetilde{h}_1, \ldots, \widetilde{h}_s) \pmod{\pi^r}$$

and this gives the thesis. □

Theorem 3.9. *Let $f \in R[x]$ and $g_1, \ldots, g_s \in \mathcal{O}_K[x]$ be monic polynomials. Denote by $h_i \in \mathcal{O}_K[x]$ the polynomial $\prod_{j \neq i} g_j$. Assume that*

- $l > v(\mathrm{disc}(f))$
- $f \equiv \prod_{i=1}^{s} g_i \pmod{\pi^l}$

Then there are monic polynomials $G_i \in \mathcal{O}_K[x]$ such that

$$f = \prod_{i=1}^{s} G_i$$

and $G_i \equiv g_i \pmod{\pi^{l-r}}$, where $r = r(h_1, \ldots, h_s)$.

Proof. Since $l > v(\mathrm{disc}(f))$, the formula for the discriminant given in corollary 3.6 gives us

$$\mathrm{disc}(f) \equiv (\det M(h_1, \ldots, h_s))^2 \prod_{i=1}^{s} \mathrm{disc}(g_i) \pmod{\pi^l}$$

Hence $l \geq v((\det M(h_1, \ldots, h_s))^2 \prod_{i=1}^{s} \mathrm{disc}(g_i))$ and $l > 2r$, where r is the valuation of the determinant of $M(h_1, \ldots, h_s)$.

We show by induction on i that we can find $\psi_{i,j} \in R[x]$ with $\deg \psi_{i,j} < n_j = \deg g_j$ such that, given a factorization

$$f \equiv \prod_{j=1}^{s} \widetilde{G}_j \pmod{\pi^{l+i-1}}$$

such that $\widetilde{G}_j \equiv g_j \pmod{\pi^{l-r}}$ and $\widetilde{G}_j$ is monic, then

$$f \equiv \prod_{j=1}^{s} (\widetilde{G}_j + \pi^{l-r+i-1}\psi_{i,j}) \pmod{\pi^{l+i}}$$

Let $\rho \in R[x]$ be the polynomial such that

$$f = \prod_{i=1}^{s} \widetilde{G}_j + \pi^{l+i-1}\rho$$

in $\mathcal{O}_K[x]$. Since all the polynomials are monic, it holds $\deg \rho < n = \deg f$. The previous lemma implies that the valuation of the determinant of the generalized Sylvester matrix obtained by $g_1, \ldots, g_s$ and by $\widetilde{G}_1, \ldots, \widetilde{G}_s$ is the same. Using proposition 3.7, we can find $\psi_{i,j} \in R[x]$ such that

$$\pi^r \rho \equiv \sum_{j=1}^{s} \psi_{i,j} \prod_{t \neq j} \widetilde{G}_t \pmod{\pi^{r+1}}$$

This means that

$$f \equiv \prod_{j=1}^{s} (\widetilde{G}_j + \pi^{l-r+i-1}\psi_{i,j}) \pmod{\pi^{l+i}}$$

and setting $G_j = g_j + \sum_{i \geq 1} \pi^{l-r+i-1}\psi_{i,j}$ we get the thesis. □

We are now ready to give the outline of the algorithm. Let $f \in R[x]$ be a monic polynomial. The version of the Hensel's lemma just proved implies that, given a factorization of $f \bmod \pi^l$ for $l > v(\mathrm{disc}(f))$,

$$f \equiv \prod_{i=1}^{s} g_i \pmod{\pi^l}$$

all the factorizations are of the form

$$f \equiv \prod_{i=1}^{s}(g_i + \pi^{l-r}\varphi_i) \pmod{\pi^l} \tag{3.1}$$

because they must correspond to the unique factorization existing over the completion. Therefore, finding all the factorizations of $f \bmod \pi^l$ is equivalent to finding all the possible φ_j satisfying the relation 3.1. As in the algorithm described in the case of a polynomial having only two factors over the completion, this problem can be solved via linear algebra. Indeed,

$$\begin{aligned} f \equiv \prod_{i=1}^{s}(g_i + \pi^{l-r}\varphi_i) \pmod{\pi^l} &\iff f \equiv \prod_{i=1}^{s} g_i + \pi^{l-r}\sum_{i=1}^{s}\varphi_i h_i \pmod{\pi^l} \\ &\iff \pi^{l-r}\sum_{i=1}^{s}\varphi_i h_i \equiv 0 \pmod{\pi^l} \\ &\iff \sum_{i=1}^{s}\varphi_i h_i \equiv 0 \pmod{\pi^r} \end{aligned}$$

where as usual $h_i = \prod_{j\neq i} g_j$. Notice that in the second equivalence we have used $2(l-r) > l$. The φ_i satisfying the last equation are exactly the kernel of the matrix $M(h_1,\dots,h_s) \bmod \pi^r$, which can be easily found by computing its Smith normal form over $\mathcal{O}_K$ (which is a PID), as done before. Clearly, if $r(h_1,\dots,h_s) = 0$, the matrix is invertible and there is only one factorization. Assume then that $r(h_1,\dots,h_s) \geq 1$. Then, let $P, Q \in \mathrm{GL}(n, \mathcal{O}_K)$ be two matrix such that

$$P \cdot K(h_1,\dots,h_r) \cdot Q = \begin{pmatrix} d_1 & & & \\ & d_2 & & \\ & & \ddots & \\ & & & d_n \end{pmatrix}$$

where $d_i \in \mathcal{O}_K$ and $d_i \mid d_{i+1}$. Since $\det P$ and $\det Q$ are invertible, the valuations of the diagonal matrix and of $M(h_1,\dots,h_s)$ is the same. Thus there exists the minimum index i such that $\pi \mid d_i$ and $\pi \nmid d_{i-1}$. Denote by Q_i the i-th column of Q and by r_i the valuation of d_i; it is immediate to see that the vectors $\pi^{r-r_i}Q_i$ are a basis for the kernel of $M(h_1,\dots,h_r)$.

As a practical observation, we notice that, since $l > 2r$, we do not need to know precisely the h_i but only the matrix $M(h_1,\dots,h_s) \bmod \pi^{\lfloor l/2 \rfloor}$. We now give the pseudocode of the algorithm, in the setting of the ring of integers of a p-adic field.

Factorizations of a polynomial mod π^l for large l

1: **Input:** $f \in R[x]$ monic, $l \in \mathbb{N}$ such that $l > v(\mathrm{disc}(f))$ and a factorization into irreducible monic polynomials $f = \prod_{i=1}^{s} g_i$ in $\mathcal{O}_K[x]$
2: **if** $s = 1$ **then**
3: **return** f is irreducible
4: **end if**
5: **if** $v(\mathrm{disc}(f)) = 0$ **then**

6: **return** $f \equiv \prod_{i=1}^{s} g_i \pmod{\pi^l}$
7: **end if**
8: Compute $h_i \equiv f/g_i \pmod{\pi^l}$ for all i and form the generalized Sylvester matrix $M(h_1, \ldots, h_s) \pmod{\pi^{\lfloor l/2 \rfloor}}$.
9: Compute $r(h_1, \ldots, h_s)$
10: Compute the kernel of $M(h_1, \ldots, h_s) \pmod{\pi^r}$ using the Smith normal form
11: Using the basis of the kernel found in the previous step, form all the factorizations
12: **return** All the factorization of f obtained.

Example 3.10. *We consider the polynomial* $f = (x^2+3)(x+6)(x^2+9)$ *over* $\mathbb{Z}$. *Notice that this is already a factorization into irreducible factors over* $\mathbb{Z}_3$. *We want to find all the factorizations of* f *over* $\mathbb{Z}/(3^{14})$. *We have* $v(\mathrm{disc}(f)) = 13$ *and therefore we can use the algorithm just described. First of all, we compute* $h_1, h_2, h_3 \in \mathbb{Z}_3[x]$*:*

$$h_1 = \frac{f}{x^2+3} = x^3 + 6x^2 + 9x + 54$$
$$h_2 = \frac{f}{x+6} = x^4 + 12x^2 + 27$$
$$h_3 = \frac{f}{x^2+9} = x^3 + 6x^2 + 3x + 18$$

Then we construct the generalized Sylvester matrix:

$$M(h_1, h_2, h_3) = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 \\ 6 & 1 & 0 & 6 & 1 \\ 9 & 6 & 12 & 3 & 6 \\ 54 & 9 & 0 & 18 & 3 \\ 0 & 54 & 27 & 0 & 18 \end{pmatrix}, r(h_1, h_2, h_3) = 5$$

We compute a basis for the kernel of $M(h_1, h_2, h_3)$ *over* $\mathbb{Z}/(3^5)$, *using the Smith normal form.*

$$P \cdot M(h_1, h_2, h_3) \cdot Q = D$$

$$P = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 1 & -30 & -8 & 0 & 0 \\ -15 & 459 & 120 & -1 & -1 \\ -510 & 15633 & 4076 & -37 & -80 \\ -1161 & 35586 & 9279 & -84 & -181 \end{pmatrix}$$

$$Q = \begin{pmatrix} -1 & -32 & 20 & 170 & -44085 \\ 7 & 191 & -122 & -1029 & 266850 \\ 22 & 641 & -409 & -3450 & 894688 \\ 9 & 256 & -163 & -1376 & 356837 \\ -54 & -1535 & 980 & 8265 & -2143362 \end{pmatrix}$$

$$D = \begin{pmatrix} 1 & & & & & \\ & 1 & & & & \\ & & 3 & & & \\ & & & 3 \cdot 2 & & \\ & & & & 3^3 \cdot 130 & \end{pmatrix}$$

Therefore a basis for the kernel of $M(h_1, h_2, h_3) \pmod{3^5}$ *is given by the last three columns of* Q *multiplied by* $3^4, 3^4$ *and* 3^2 *respectively:*

$$\mathcal{B} = \left\{ 3^4 \cdot \begin{pmatrix} 20 \\ -122 \\ -166 \\ -163 \\ 8 \end{pmatrix}, 3^4 \cdot \begin{pmatrix} 170 \\ -57 \\ -48 \\ -161 \\ 3 \end{pmatrix}, 3^2 \cdot \begin{pmatrix} -102 \\ 36 \\ 205 \\ 113 \\ -102 \end{pmatrix} \right\}$$

where we have reduced the entries of the vectors mod 3^5*. Therefore we can write all the factorizations of* $f = u_1 u_2 u_3$*,*

$$u_1 = x^2 + 3 + 3^9(3^4\alpha_1(20x - 122) + 3^4\alpha_2(170x - 57) + 3^2\alpha_3(-102x + 36))$$
$$u_2 = x + 6 + 3^9(-3^4\alpha_1 \cdot 166 - 3^4\alpha_2 \cdot 48 + 3^2\alpha_3 \cdot 205)$$
$$u_3 = x^2 + 9 + 3^9(3^4\alpha_1(-165x + 8) + 3^4\alpha_2(-161x + 3) + 3^2\alpha_3(113x - 102))$$

where $0 \leq \alpha_1 < 3$*,* $0 \leq \alpha_2 < 3$*,* $0 \leq \alpha_3 < 27$*.*

Observation 3.11. *The factorizations given in output by the algorithm can be redundant; it is possible that different values of the parameters give rise to the same factorization.*

The authors of the article focus on the cost of the algorithm, providing an interesting discussion on how to compute efficiently the kernel of a generalized Sylvester matrix on $\mathcal{O}_K[x]/(\pi^l)$. However, this is far from our purpose and for interested readers we refer to the article.

We should still make a remark about this algorithm, which has not been noticed by the authors. They do not care about the uniqueness of the factorization and they start directly by factoring the polynomial over the completion. This algorithm can be improved: we have seen in the first chapter (1.65) that we can reduce to the primary component of the ideal generated by the polynomial which corresponds to a factor obtained by Hensel's lemma. Instead of forming the generalized Sylvester matrix of all the factors, it is better to reduce to a primary component and process all of them separately. While this is irrelevant in the worst case, this improves the performances of the algorithm in the average case, since computing some Smith normal forms of small matrices is better than one of a big.

3.2 Factorization over $\mathcal{O}_K/(\pi^l)$ for small l

What can be done in the case $\leq v(\mathrm{disc}(f))$? This problem is hard and the only method is, as far as we know, the brute-force algorithm: try to lift the factorization mod π to all the possible factorizations of $f \bmod \pi^l$.

Let $f \in R[x]$ be a monic polynomial such that $f \equiv \phi^k \pmod{\pi}$, where $\phi \in R[x]$ is a monic polynomial irreducible mod π. Finding all the factorizations

with a brute-force method is really expensive, because we need to consider all the possible partition of k and try to lift all the possible factorizations. The relations that arise in this process are, in general, not easily solvable.

Example 3.12. *We want to find all the factorizations of* $f = x^3$ *over* $\mathbb{Z}/(8)$. *First, we try to obtain all the factorizations into linear factors over* $\mathbb{Z}/(4)$. *We want to find* $\alpha, \beta, \gamma \in \mathbb{Z}/(2)$ *such that*

$$x^3 \equiv (x + 2\alpha)(x + 2\beta)(x + 2\gamma) \pmod 4$$

We get the relation $\alpha + \beta + \gamma = 0 \pmod 2$ *and consequently the factorizations*

$$x^3 \equiv x^3 \pmod 4 \qquad x^3 \equiv x(x+2)^2 \pmod 4$$

Now, we lift them mod 8. *In the first case, we want to find* α, β, $\gamma \in \mathbb{Z}/(2)$ *such that*

$$x^3 \equiv (x + 4\alpha)(x + 4\beta)(x + 4\gamma) \pmod 8$$

This means that $\alpha + \beta + \gamma \equiv 0 \pmod 2$ *and therefore we get the factorizations*

$$x^3 \equiv x(x+4)^2 \pmod 8 \qquad x^3 \equiv x^3 \pmod 8$$

In the second case, we want to find α, β, γ *such that*

$$x^3 = (x + 2 + 4\alpha)(x + 2 + 4\beta)(x + 4\gamma) \pmod 8$$

Notice that the only term of degree one is $4x$ *and therefore it is impossible to lift such a factorization.*
Now, we need to consider the factorizations consisting of a factor of degree one and a factor of degree 2. *Firstly, we want to find* α, β *such that*

$$x^3 \equiv (x^2 + 2(\alpha x + \beta))(x + 2\gamma) \pmod 4$$

We get the equations $\alpha + \gamma = 0 \pmod 2$ *and* $\beta = 0 \pmod 2$, *so that all the factorizations mod* 4 *are*

$$x^3 \equiv x^3 \pmod 4 \qquad x^3 \equiv (x^2 + 2x)(x + 2) \pmod 4$$

Now we try to lift them mod 8. *In the first case, we need to find* α, β, γ *such that*

$$x^3 \equiv (x^2 + 4(\alpha x + \beta))(x + 4\gamma) \pmod 8$$

The only solutions give rise to

$$f \equiv (x^2 + 4x)(x + 4) \pmod 8 \qquad f \equiv x^3 \pmod 8$$

Since $x^2 + 4x$ *is reducible, there are no new factorizations.*
In the second case, we want to find α, β, γ *such that*

$$x^3 \equiv (x^2 + 2x + 4(\alpha x + \beta))(x + 2 + 4\gamma) \pmod 8$$

We get $\alpha + \gamma + 1 \equiv 0 \pmod 2$ *and* $\beta \equiv 1 \pmod 2$ *and the corresponding factorizations*

$$x^3 \equiv (x^2 + 6x + 4)(x + 2) \pmod 8 \quad x^3 \equiv (x^2 + 2x + 4)(x + 6) \pmod 8$$

Summarizing, all the factorizations of f *over* $\mathbb{Z}/(8)$ *are:*

$$f \equiv (x^2 + 6x + 4)(x + 2) \pmod 8 \quad f \equiv (x^2 + 2x + 4)(x + 6) \pmod 8$$
$$f \equiv x(x + 4)^2 \pmod 8 \qquad f \equiv x^3 \pmod 8$$

As the example shows, the number of factorizations can increase passing from $\mathcal{O}_K/(\pi^i)$ to $\mathcal{O}_K/(\pi^{i+1})$ and some factorizations mod π^i do not give rise to factorizations mod π^{i+1}. Therefore a criterion to understand whether or not a factorization mod π^i lifts to a factorization mod π^{i+1} would reduce the cost of this algorithm. In [11], it is presented the following proposition:

Proposition 3.13. *Let $f \in R[x]$ be a monic polynomial such that $f \equiv \phi^k \pmod{\pi}$, where $\phi \in R[x]$ is a monic polynomial, irreducible over the residue field. Assume $f \equiv uw \pmod{\pi^l}$ and $u \equiv \phi^m \pmod{\pi}$, $v \equiv \phi^{k-m} \pmod{\pi}$, where $m \leq k/2$. The following are equivalent:*

1. *$\frac{f-uw}{\pi^l}$ is divisible by ϕ^m mod π*
2. *For every $\varphi \in \mathcal{O}_K[x]$ with $\deg\varphi < \deg u$ there exists a polynomial $\psi \in \mathcal{O}_K[x]$ with $\deg(\psi) < \deg(w)$ such that $f \equiv (u+\pi^l\varphi)(w+\pi^l\psi) \pmod{\pi^{l+1}}$*
3. *There exist polynomials $\varphi, \psi \in \mathcal{O}_K[x]$ with $\deg(\varphi) < \deg(u)$ and $\deg(\psi) < \deg(w)$ such that*
$$f \equiv (u + \pi^l\varphi)(w + \pi^l\psi) \pmod{\pi^{l+1}}$$
4. *There exist polynomials $\varphi, \psi \in \mathcal{O}_K[x]$ such that*
$$f \equiv (u + \pi^l\varphi)(w + \pi^l\psi) \pmod{\pi^{l+1}}$$

Proof.

(1) $\Rightarrow$ (2) Let $\gamma \in \mathcal{O}_K[x]$ such that

$$\frac{f - uw}{\pi^l} \equiv \gamma\phi^m \pmod{\pi}$$

Assume that $\varphi \in \mathcal{O}_K[x]$ is a polynomial of degree $\deg\varphi < \deg u$, as in the statement. We consider $\psi \in \mathcal{O}_K[x]$ as a monic lift of $\gamma - \phi^{k-2m}\varphi \pmod{\pi}$. Notice that $\deg\gamma < \deg\phi^{k-m} = \deg w$ and

$$\deg(\phi^{k-2m}\varphi) < \deg(\phi^{k-2m}u) = \deg\phi^{k-m} = \deg w$$

Hence $\deg\psi < \deg w$ and

$$\begin{aligned} f - (u + \pi^l\varphi)(w + \pi^l\psi) &\equiv f - uw - \pi^l(\varphi w + u\psi) \\ &\equiv f - uw - \pi^l(\varphi\phi^{k-m} + \phi^m(\gamma - \phi^{k-2m}\varphi)) \\ &\equiv f - uw - \pi^l(\varphi\phi^{k-m} + \phi^m\gamma - \phi^{k-m}\varphi) \\ &\equiv f - uw - \pi^l\phi^m\gamma \\ &\equiv 0 \pmod{\pi^{l+1}} \end{aligned}$$

and this proves the first implication.

(2) $\Rightarrow$ (3) Trivial.

(3) $\Rightarrow$ (4) Trivial.

(4) $\Rightarrow$ (1) Let $\varphi, \psi \in \mathcal{O}_K[x]$ be polynomials such that such that $f \equiv (u + \pi^l\varphi)(w + \pi^l\psi) \pmod{\pi^{l+1}}$. Then

$$\frac{f - uw}{\pi^l} \equiv \varphi w + \psi u \equiv \varphi\phi^{k-m} + \psi\phi^m \equiv \phi^m(\varphi\phi^{k-2m} + \psi) \pmod{\pi}$$

□

This criterion speeds up the computation, but it is not enough to make the problem effectively solved. We will provide another important criterion in the following chapter.

3.3 Factoring over $\mathcal{O}_K/(\pi^2)$

The algorithm described above is far from being satisfactory from some points of view. Indeed, it requires to know a p-adic factorization and this brings in some precision problems. Furthermore, this approach does not give any information on how to find a factorization into irreducible factors of a polynomial modulo small powers of a prime. In this section, we will deal with the problem of finding a factorization mod π^2 following [21]. First of all, the author notices that the following criterion holds:

Theorem 3.14. *Let $l \geq 2$ and $f \in \mathcal{O}_K[x]/(\pi^l)$ be a monic polynomial and let $\phi \in \mathcal{O}_K[x]$ be a monic polynomial such that ϕ is irreducible mod π and $f \equiv \phi^k \pmod{\pi}$ with $k \geq 2$. Write $f = \phi^k + \pi h$. If f factors, then one of the following holds:*

1. $h \equiv 0 \pmod{\pi}$
2. $\phi \mid h \pmod{\pi}$

Proof. Let $f \equiv f_1 f_2$ be a proper factorization of f in $\mathcal{O}_K[x]/(\pi^l)$. We can write

$$f_1 = \phi^{k_1} + \pi h_1 \qquad\qquad f_2 = \phi^{k_2} + \pi h_2$$

with $0 < k_1 \leq k_2$ and $k_1 + k_2 = k$. Then, computing the product,

$$\begin{aligned} f_1 f_2 &= (\phi^{k_1} + \pi h_1)(\phi^{k_2} + \pi h_2) \\ &= \phi^k + \pi(h_1\phi^{k_2} + h_2\phi^{k_1}) + \pi^2 h_1 h_2 \end{aligned}$$

Therefore, mod π, we have the equality

$$h \equiv h_1\phi^{k_2} + h_2\phi^{k_1} \equiv \phi^{k_1}(h_2 + \phi^{k_2-k_1}h_1) \pmod{\pi}$$

Hence either $h \equiv 0 \pmod{\pi}$ or $\phi \mid h \pmod{\pi}$, as desired. □

Given the difficulty of the problem we are dealing with, it should be clear to the reader that the converse does not hold:

Example 3.15. *We consider the polynomial $f = x^4 + 4x + 4$ in $\mathbb{Z}[x]$. The projection of this polynomial mod 2 is x^4 and therefore, in the notations of the above theorem, we write*

$$f = x^4 + 2(2x + 2)$$

Notice that $2x + 2 \equiv 0 \pmod{2}$; however f is irreducible over $\mathbb{Z}/(8)$. Indeed, it clearly has no roots and by brute force it can be seen that it is impossible to factor it.

The theorem we just proved can be considered as a generalized Eisenstein's criterion. Indeed, it can be restated as follows:

Corollary 3.16. *Let $f \in \mathcal{O}_K[x]$ be a monic polynomial such that $f \equiv \phi^k \pmod{\pi}$, where $\phi \in \mathcal{O}_K[x]$ is a monic polynomial irreducible mod π. Let $h \in \mathcal{O}_K[x]$ be the polynomial satisfying $f = \phi^k + \pi h$. If $h \neq 0$ mod π and $\phi \nmid h$ mod π then f is irreducible.*

Let $f \in \mathcal{O}_K[x]$ be an Eisenstein polynomial (i.e. a monic polynomial which is irreducible by Eisenstein's criterion), $f = \sum a_i x^i$. In the notations of the corollary, we consider

$$\phi = x \qquad\qquad h = \frac{a_{n-1}x^{n-1} + \ldots + a_0}{\pi}$$

Since $a_0 \not\equiv 0 \pmod{\pi^2}$, $h \not\equiv 0 \pmod{\pi}$. Furthermore, $x \nmid h \pmod{\pi}$ because for the same reason h has a non-zero constant term mod π and the corollary proves the irreducibility of f over $\mathcal{O}_K/(\pi^2)$, thus over $\mathcal{O}_K$.

Sălăgean gives a criterion to understand when a primary component is irreducible:

Proposition 3.17. *Let $f \in \mathcal{O}_K[x]/(\pi^l)$ be a monic polynomial such that f is not squarefree mod π. Let $f_1, f_2 \in \mathcal{O}_K[x]/(\pi^l)$ such that $f_1 \mod \pi$ is the squarefree part of $f \pmod{\pi}$ and*

$$f \equiv f_1 f_2 \pmod{\pi}$$

Let $h \in \mathcal{O}_K[x]/(\pi^l)$ such that $\pi h \equiv f - f_1 f_2$. If $h \not\equiv 0 \pmod{\pi}$ and $(h, f_2) \equiv 1 \pmod{\pi}$ then every primary component of f is irreducible.

Proof. We consider a factorization of $f \bmod \pi$

$$f \equiv \prod_{i=1}^{s} g_i^{e_i} \pmod{\pi}$$

Therefore the factorization given by Hensel's lemma in $\mathcal{O}_K[x]/(\pi^l)$ is of the form

$$f \equiv \prod_{i=1}^{s} (g_i^{e_i} + \pi h_i) \pmod{\pi^l}$$

We want to show that each factor is irreducible; by the previous theorem, it is enough to show that $h_i \not\equiv 0 \pmod{\pi}$ and $g_i \nmid h_i \pmod{\pi}$. We write

$$f_1 \equiv \prod_{i=1}^{s} g_i + \pi w_1 \pmod{\pi^l} \qquad f_2 = \prod_{i=1}^{s} g_i^{e_i - 1} + \pi w_2 \pmod{\pi^l}$$

Therefore,

$$f - f_1 f_2 \equiv \pi\Big(\sum_{i=1}^{s} h_i \prod_{j \neq i} g_i^{e_i} - w_1 \prod_{i=1}^{s} g_i^{e_i - 1} - w_2 \prod_{i=1}^{s} g_i\Big) \pmod{\pi^2}$$

This means that

$$h \equiv \sum_{i=1}^{s} h_i \prod_{j \neq i} g_j^{e_j} - w_1 \prod_{i=1}^{s} g_i^{e_i - 1} - w_2 \prod_{i=1}^{s} g_i \pmod{\pi}$$

We have seen in the first chapter (1.65) that if $e_i = 1$ the corresponding primary component is irreducible. Let i be an index such that $e_i \geq 2$. Then, mod g_i,

$$h \equiv h_i \prod_{j \neq i} g_j^{e_j} \pmod{(\pi, g_i)}$$

and since by hypotheses $h \not\equiv 0 \pmod{\pi}$ (h is coprime to f_2 mod π), the same holds for h_i. Furthermore, $g_i \nmid h \pmod{\pi}$ and therefore the same must hold in the right hand side ((π, g_i) is a maximal ideal). The thesis follows. □

Focusing on the case of a polynomial mod π^2, we can see that the previous theorem can be strengthened in order to provide a necessary and sufficient condition for irreducibility:

Theorem 3.18. *Let $f \in \mathcal{O}_K[x]/(\pi^2)$ be a monic polynomial such that $f \equiv \phi^k \pmod{\pi^2}$, where $\phi \in \mathcal{O}_K[x]/(\pi^2)$ is a monic polynomial, irreducible mod π. Assume that $k \geq 2$ and let $h \in \mathcal{O}_K[x]/(\pi^2)$ such that $f \equiv \phi^k + \pi h \pmod{\pi^2}$. Then f factors if and only if one of the following holds:*

1. $h \equiv 0 \pmod{\pi}$
2. $\phi \mid h \pmod{\pi}$

Proof. We need to show that if one of the conditions is satisfied, f factors. Clearly if $h \equiv 0 \pmod{\pi}$ then $\pi h = 0$ and then $f = \phi^k$ is a factorization of f into irreducible factors. Assume now that $h \neq 0 \pmod{\pi}$ and that $\phi \mid h \pmod{\pi}$. Even in this case it is clear that f splits, since we can split out a factor ϕ. However, we want to produce a factorization into irreducible factors of f. Let $k_1 \in \mathbb{N}$ be the maximum power of ϕ dividing h mod π. Then we can write $h \equiv \phi^{k_1} w \pmod{\pi}$ for some $w \in \mathcal{O}_K/(\pi^2)[x]$. This means that $\pi h = \pi \phi^{k_1} w$. Hence, we have the factorization

$$f \equiv \phi^{k_1}(\phi^{k-k_1} + \pi w) \pmod{\pi^2}$$

The factor $\phi^{k-k_1} + \pi w$ is irreducible by the previous corollary and therefore we have found a proper factorization of f into irreducible factors. □

This theorem gives a criterion for determining whether a polynomial is irreducible or not in $\mathcal{O}_K[x]/(\pi^2)$ and provides an algorithm to factor polynomials in such a ring. The spirit of this method is completely different from the one given by von Zur Gathen, since it does not require the knowledge of the factorization of a lift to the p-adic field. Moreover, the results obtained in this way can be used as a part of the algorithm for p-adic factorization in order to determine if a polynomial is irreducible. This is why a similar approach is generally better. However, in their algorithm, Von Zur Gathen and Hartlieb do not find one factorization, but all the possible factorizations. Sălăgean tries to recover some of these factorizations, but finding all of them is much more difficult. Thus, we will focus on the search for all the factorizations having the maximum number of factors.

Example 3.19. *Consider the polynomial $f = x^4$ over $\mathbb{Z}/(4)$. Then the factorizations of f into the maximum number of factors are clearly into linear factors:*

$$x^4 \qquad (x+2)^4 \qquad x^2(x+2)^2$$

while f admits also factorizations into fewer factors, for example $f = (x^2+2)^2$.

We are going now to classify all the possible factorizations into the maximum number of factors.

Proposition 3.20. *Let K be a p-adic field and let $f \in \mathcal{O}_K[x]/(\pi^2)$ be a monic polynomial which is not irreducible and congruent to a power of an irreducible polynomial mod π. f admits a factorization into monic irreducible factors of one (but not both) of the following types:*

1. *$f = \phi^k$ for some $\phi \in \mathcal{O}_K[x]$ irreducible mod π.*
2. *$f = \phi^{k_1}(\phi^{k-k_1} + \pi w)$ for some $\phi, w \in \mathcal{O}_K[x]$ such that ϕ is irreducible mod π, $w \neq 0$ mod π and, if $p \nmid k$, $k - k_1 \geq 2$.*

Proof. By the proof of theorem 3.18, we know that f can be written as in the statement. We need to show that f can not be written in both ways and that, whenever $p \nmid k$ and $k - k_1 = 1$, f can be written as in (1). First, assume that $p \nmid k$ and $f = \phi^{k-1}(\phi + \pi w)$. Let k^{-1} be the inverse of k mod π and let $u \in \mathcal{O}_K[x]/(\pi^2)$ be a lift of $k^{-1}w$. Then $f = (\phi + \pi u)^k$. Indeed,

$$(\phi + \pi u)^k = \phi^k + k\pi\phi^{k-1}u = \phi^k + \pi\phi^{k-1}w = f$$

and so a factorization of type (1). Suppose now that f admits both factorizations (1) and (2), so that

$$f = \phi_1^k = \phi_2^{k_1}(\phi_2^{k-k_1} + \pi w)$$

Clearly there exists $u \in \mathcal{O}_K[x]/(\pi^2)$ such that $\phi_1 = \phi_2 + \pi u$. This means that

$$\phi_2^k + \pi\phi_2^{k_1}w = (\phi_2 + \pi u)^k = \phi_2^k + \pi k\phi_2^{k-1}u$$

Hence, $w = k\phi_2^{k-k_1-1}u \pmod{\pi}$. We need to distinguish two cases:

- If $p \mid k$, then $w = 0 \pmod{\pi}$, and this gives a contradiction by the irreducibility of the factor.
- If $p \nmid k$, then $k - k_1 - 1 \geq 1$ and $\phi_2 \mid w \pmod{\pi}$, this gives a contradiction because the factor $\phi_2 + \pi w$ was supposed to be irreducible.

□

Proposition 3.21. *Assume that the same hypotheses of proposition 3.20 hold. The two types of factorizations have the maximum number of factors among all the existing factorizations. Furthermore, among all the factorizations with the maximum number of factors, they have the minimum number of distinct irreducible factors.*

Proof. With the notations of the above proposition, it is clear that the type (1) is a factorization into the maximum number of factors (it follows from Hensel's lemma). Assume than that f has a factorization of type (2). Let

$$f \equiv \prod_{i=1}^{t}(\phi^{s_i} + \pi w_i) \pmod{\pi^2}$$

be any factorization of f into irreducible factors. We can assume that $s_1 \leq s_2 \leq \ldots \leq s_t$. Computing the product,

$$f \equiv \phi^k + \pi\sum_{i=1}^{t} w_i\phi^{k-s_i} \equiv \phi^k + \pi\phi^{k_1}w \pmod{\pi^2}$$

We deduce that

$$\phi^{k-s_t} \sum_{i=0}^{t} w_i \phi^{s_t - s_i} \equiv \phi^{k_1} w \pmod{\pi}$$

In particular, $k_1 \geq k - s_t$. Notice that

$$\sum_{i=1}^{t-1} s_i = k - s_t \leq k_1$$

and since $s_i \geq 1$ for all indices i, we get $t \leq k_1 + 1$. This proves that $k_1 + 1$ is the maximum number of factors of a polynomial having factorization of type (2). Furthermore, since polynomials having a factorization of type (2) can not have one of type (1), the minimum number of distinct irreducible factors is 2, and this ends the proof. □

In order to provide all the possible factorizations having the properties of the last proposition, we still need to discuss the choice of the irreducible polynomial ϕ. In particular, it is not clear if changing it provides new factorizations. The following proposition solves this problem:

Proposition 3.22. *Assume that the same hypotheses of proposition 3.20 hold. If $p \mid k$, then the irreducible polynomial ϕ is uniquely determined. Otherwise, every lift of the irreducible factor of $f \bmod \pi$ provides a different factorization, but the power k_1 is uniquely determined and there is a unique irreducible polynomial $\phi^{k-k_1} + \pi w$ that gives the factorization.*

Proof. Assume first that f admits a factorization of type (1), so $f = \phi^k$. Let ϕ_1 be another monic lift of the irreducible factor of $f \bmod \pi$. Then there exists u such that $\phi = \phi_1 + \pi u$ and

$$f \equiv (\phi_1 + \pi u)^k \equiv \phi_1^k + \pi k \phi^{k-1} u \pmod{\pi^2}$$

Hence, if $p \mid k$, we have found another factorization of f of type (1), if $p \nmid k$ we have not.
If f has a factorization of type (2), we have

$$\begin{aligned} f &= (\phi_1 + \pi u)^k + \pi(\phi_1 + \pi u)^{k_1} w \\ &= \phi_1^k + \pi k u \phi_1^{k-1} + \pi \phi_1^{k_1} w \\ &= \phi_1^{k_1}(\phi_1^{k-k_1} + \pi w_1) \pmod{\pi^2} \end{aligned}$$

where $w_1 = ku\phi_1^{k-k_1-1} + w$. Since $w_1 \neq 0 \pmod{\pi}$ and $\phi_1 \nmid w_1 \pmod{\pi}$ the last factor is irreducible and this gives a new factorization. □

As a corollary, we can say exactly how many factorizations having this property there are:

Corollary 3.23. *Let q be the cardinality of the residue field of K. If f has a factorization of type (2) or f has a factorization of type (1) and $p \mid k$, there are $q^{\deg \phi}$ different factorizations of f satisfying the properties of the proposition above.*

Starting from one factorization, we can easily find all the factorizations with the maximum number of factors and having the minimum number of distinct irreducible factors. Indeed, it is enough to change the polynomial ϕ as in the last proposition. Surprisingly, we can even find something more:

Corollary 3.24.

- *Assume that f admits a factorization of type* (1)*, so that $f \equiv \phi^k \pmod{\pi^2}$. Let $w_1, \ldots, w_k \in \mathcal{O}_K/(\pi^2)[x]$ be polynomials of degree $< \deg \phi$ such that $\sum w_i = 0$. Then*
$$f = \prod_{i=1}^{k} (\phi + \pi w_i)$$
is a factorization into irreducible factors of f.

- *Assume that f admits a factorization of type* (2)*, so that $f = \phi^{k_1}(\phi^{k-k_1} + \pi w)$. Given $w_1, \ldots, w_{k_1}$ such that $\deg w_i < \deg \phi$ for $i = 1, \ldots, k_1$, define*
$$w_{k_1+1} = w - \phi^{k-k_1-1} \sum_{i=1}^{k_1} w_i$$
Then
$$f = (\phi^{k-k_1} + \pi w_{k_1+1}) \prod_{i=1}^{k_1} (\phi + \pi w_i)$$
is a factorization of f into the maximum number of irreducible factors.

Furthermore, these procedures give all the possible factorizations of f into the maximum number of irreducible factors.

The corollary follows immediately from the propositions proved above.

Now, we give the outline of the algorithm to find a factorization of f mod π^2 into the maximum number of factors and the minimum number of distinct irreducible factors.

Factoring polynomials mod π^2
Input: Monic polynomials $f, \phi \in \mathcal{O}_K/(\pi^2)[x]$ such that $f \equiv \phi^k \pmod{\pi}$ and ϕ is irreducible mod π
Output: A factorization of f of type (1) or (2) or "f is irreducible"

1: **if** $k = 1$ **then**
2: **return** f is irreducible
3: **end if**
4: Determine h such that $\pi h \equiv f - \phi^k \pmod{\pi^2}$
5: **if** $h \equiv 0 \pmod{\pi}$ **then**
6: **return** $f \equiv \phi^k \pmod{\pi^2}$
7: **end if**
8: Determine the maximum k_1 such that $\phi^{k_1} \mid h \pmod{\pi}$
9: Determine w such that $h \equiv \phi^{k_1} w \pmod{\pi}$
10: **if** $k_1 = 0$ **then**
11: **return** f is irreducible

12: **end if**
13: **if** $p \mid k$ or $k_1 \leq k-2$ **then**
14: **return** $f \equiv \phi^{k_1}(\phi^{k-k_1} + \pi w)$
15: **end if**
16: Determine u such that $u \equiv k^{-1}w \pmod{\pi}$
17: **return** $f \equiv (\phi + \pi u)^m$

Then, given the output of the algorithm, we can easily find all the factorizations with the maximum number of factors, as we show in the following example:

Example 3.25. *We consider the polynomial* $f = (x^2+1)^7 + 3(x^2+1)^4$ *over* $\mathbb{Z}/(9)$. f *is not irreducible and we can easily factor it. Indeed,* x^2+1 *is irreducible mod* 3 *and therefore we get a factorization*

$$f = (x^2+1)^4((x^2+1)^3+3)$$

Therefore f *admits a factorization of type* (2)*. All the other factorizations into the maximum number of factors can be obtained by corollary 3.24:*

$$f = ((x^2+1)^3+3+3w_5)(x^2+1+3w_1)(x^2+1+3w_2)(x^2+1+3w_3)(x^2+1+3w_4)$$

where $w_1, w_2, w_3, w_4 \in \mathbb{Z}/(9)[x]$ *have degree* < 2 *and* $w_5 = 1-(x^2+1)^2\sum_{i=1}^{4} w_i$.

The algorithm developed by Sălăgean is not fully satisfactory, because it provides only factorizations into the maximum number of factors, not all of them; as we have said before, the latter is a difficult problem to solve.

We now summarize what we have done in this chapter:

- We have presented the algorithm described in [10] and [6] to factor a polynomial f in $\mathbb{Z}/(p^l)$ with $l > v(\mathrm{disc}(f))$. The algorithm uses the p-adic factorization of f, projects it on $\mathcal{O}_K/(\pi^{l_1})$ for a suitable l_1 and then lifts this factorization to $\mathcal{O}_K/(\pi^l)$ obtaining all the factorizations of f.
- We have analyzed with the problem of finding a factorization mod π^2 regardless of its discriminant, as described in [21]. The key tools of the algorithm are Hensel's lemma and theorem 3.18, which provides a necessary and sufficient condition for irreducibility over $\mathcal{O}_K/(\pi^2)$. This criterion is easily verifiable and therefore gives rise immediately to an algorithm to find all the factorizations of f into the maximum number of factors.
- We presented a sufficient and necessary criterion of Von Zur Gathen and Hartlieb to lift a factorization from $\mathcal{O}_K/(\pi^i)$ to $\mathcal{O}_K/(\pi^{i+1})$ which leads to an algorithm for finding all the factorizations mod π^l for arbitrary l.

CHAPTER 4

Irreducibility Criteria

In this chapter, we give our contributions to the problem of finding a factorization into irreducible factors of a monic polynomial mod π^l. Our approach will be different from the one given by the other authors and we will mainly aim at finding an irreducibility criterion for monic polynomials over $\mathcal{O}_K/(\pi^l)$. We will analyze some of the main properties of polynomials that are irreducible mod π^l and try to understand what lies behind the difficulty of this problem.
In the first section, we are going to extend the properties of Newton polygons in the case of polynomials over $\mathcal{O}_K/(\pi^l)$. Then, we will discuss the connections between the index of the order generated by a root of a polynomial and its irreducibility over $\mathcal{O}_K/(\pi^l)$: the main ingredient of this part will be Dedekind's criterion. In the third section, we give a formula to bound the minimum $l \in \mathbb{N}$ such that a polynomial irreducible over $\mathcal{O}_K$ is irreducible over $\mathcal{O}_K/(\pi^l)$, using Krasner's Lemma. Finally, we show how these tools can be used to prove the irreducibility of polynomials over $\mathcal{O}_K/(\pi^3)$.

4.1 Newton polygons of polynomials over $\mathcal{O}_K/(\pi^l)$

We have seen in chapter 2 that Newton polygons provide an easy method to understand whether or not a polynomial over a p-adic field is irreducible. We are going to study whether it is possible to extend all the irreducibility results and obtain an irreducibility criterion similar to the one given by Sălăgean in theorem 3.18.

As usual, we denote by K a p-adic field, by $\mathcal{O}_K$ its ring of integers and we consider a uniformizing parameter π of $\mathcal{O}_K$. Let $f \in \mathcal{O}_K[x]/(\pi^l)$ be a monic polynomial. First of all, we want to develop a notion of Newton polygon of f. It would seem that the polygon could be defined in the same way as in the case of a p-adic field. However, $\mathcal{O}_K/(\pi^l)$ is not canonically endowed with a discrete valuation and considering a lift to $\mathcal{O}_K$ seems to be a solution to this problem. Unfortunately, this is far from being a complete solution, as the following example shows:

Example 4.1. *Consider the polynomials $f = x^3+2x^2$ and $g = x^3+2x^2+4$ over $\mathbb{Z}_2$. They have the same projection to $\mathbb{Z}/(4)[x]$ but their Newton polygons are*

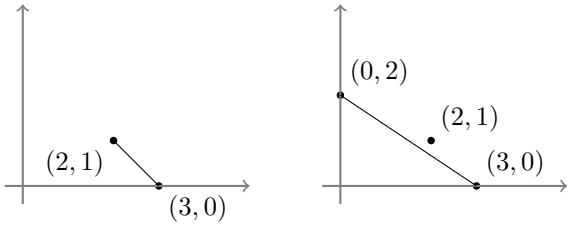


Figure 4.1: Newton polygons of f and g in Example 4.1

different. This means that the Newton polygon of f over $\mathbb{Z}/(4)$ can not be defined simply using lifts, because different lifts provide different Newton polygons.

This phenomenon can not happen when f has a non-zero constant term mod π^l, as we are going to show:

Lemma 4.2. *Let $f \in \mathcal{O}_K[x]/(\pi^l)$ be a monic polynomial such that its constant term is non-zero. Then every monic lift of f to $\mathcal{O}_K[x]$ has the same Newton polygon.*

Proof. Let $g, h \in \mathcal{O}_K[x]$ be two different monic lifts of f. Their difference is a polynomial divisible by π^l, hence $g(x) \equiv h(x) \pmod{\pi^l}$. We denote by a_i, b_i the coefficients of g, h respectively, so that

$$g = x^n + \sum_{i=1}^{n-1} a_i x^i \qquad\qquad h = x^n + \sum_{i=1}^{n-1} b_i x^i$$

By hypothesis, $a_0 \not\equiv 0 \pmod{\pi^l}$. Then $v(a_0) = v(b_0) < v(\pi^l)$. By the convexity of the Newton polygon, the point $(0, v(a_0)) = (0, v(b_0))$ is the vertex having the greatest y-coordinate of the Newton polygon of both g, h. Therefore, in order to prove that g and h share the same Newton polygon, it is enough to show that for all $i < n$, if $v(a_i) < v(\pi^l)$ then $v(a_i) = v(b_i)$ and this is clear since their projections to $\mathcal{O}_K[x]/(\pi^l)$ are the same. □

The same proof leads to the following lemma:

Lemma 4.3. *Let $f \in \mathcal{O}_K[x]/(\pi^l)$ be a monic polynomial such that $f \equiv \phi^k \pmod{\pi}$, where $\phi \in \mathcal{O}_K[x]$ is a monic polynomial which is irreducible mod π. If $\phi \nmid f$ over $\mathcal{O}_K/(\pi^l)$, every monic lift of f to $\mathcal{O}_k[x]$ has the same ϕ-polygon.*

Therefore, under the assumptions of the lemmas, we can easily extend the notion of Newton polygon

Definition 4.4. *Let $f \in \mathcal{O}_K[x]/(\pi^l)$ be a monic polynomial such that its constant term is non-zero. We define the Newton Polygon of f as the Newton Polygon of any of the monic lift of f to $\mathcal{O}_K[x]$.*

and in the same way, the generalized one:

Definition 4.5. *Let $f \in \mathcal{O}_K[x]/(\pi^l)$ be a monic polynomial such that $f \equiv \phi^k \pmod{\pi}$, where $\phi \in \mathcal{O}_K[x]$ is a monic polynomial irreducible mod π. Assume that $\phi \nmid f$. We define the ϕ-polygon of f as the ϕ-polygon of a monic lift of f to $\mathcal{O}_K[x]$.*

Giving directly the definition of the Newton Polygon in these rings would have required some additional work in order to give a notion of the valuation of a coefficient; this definition avoids the problem.
Now, we want to extend the irreducibility criterions given in chapter 2 to this setting. To achieve this result, we are going to relate the irreducibility of f to the irreducibility of its lifts by means of the following lemma:

Lemma 4.6. *Let $l \in \mathbb{N}$ be a positive integer and $\varphi\colon \mathcal{O}_K[x] \to \mathcal{O}_K[x]/(\pi^l)$ be the projection map. Given a monic polynomial $f \in \mathcal{O}_K[x]/(\pi^l)$, f is irreducible in $\mathcal{O}_K[x]/(\pi^l)$ if and only if, for every monic polynomial $g \in \mathcal{O}_K[x]$ such that $\varphi(g) = f$, g is irreducible in $\mathcal{O}_K[x]$.*

Proof. If f is irreducible, every monic polynomial $g \in \varphi^{-1}(f)$ is irreducible, since every factorization of g would give a factorization of f. Conversely, assume that f is reducible in $\mathcal{O}_K[x]/(\pi^l)$, so there exist $f_1, f_2 \in \mathcal{O}_K[x]/(\pi^l)$ monic polynomials such that $f = f_1 f_2$. We can lift f_1, f_2 to $\mathcal{O}_K[x]$, getting two monic polynomials g_1, g_2 and their product $g_1 g_2$ is a monic polynomial in $\varphi^{-1}(f)$. □

The previous lemma is the key to extend the theory we have presented in the first section of chapter 2. For instance, the following result corresponds to theorem 2.4:

Proposition 4.7. *Let $f \in \mathcal{O}_K[x]/(\pi^l)$ be a monic polynomial of degree n. Then:*

- *If f is irreducible over $\mathcal{O}_K/(\pi^l)$, the Newton Polygon of f is defined and one-sided.*
- *If the Newton polygon of f is defined, one-sided and its side has degree one, then f is irreducible over $\mathcal{O}_K/(\pi^l)$.*

Proof. If f is irreducible, its constant term is different from zero and therefore the Newton polygon of f is defined. Every every polynomial in its fiber is irreducible. In $\mathcal{O}_K[x]$, the Newton Polygon of an irreducible polynomial must have only one side and the first statement follows easily. The second is trivial, since the given condition assures that every polynomial in the fiber of f is irreducible and so we can apply lemma 4.6. □

When the generalized Newton polygon is well defined, the theorem of the product holds and therefore we can prove the following result, similar to the theorem of the polygon 2.22:

Theorem 4.8. *Let $f \in \mathcal{O}_K[x]/(\pi^l)$ be a monic polynomial such that $f \equiv \phi^k \pmod{\pi}$ and $\phi \in \mathcal{O}_K[x]$ is monic and irreducible over the residue field. Assume that $\phi \nmid f$ and that $N_\phi(f)$ is the sum of j sides $S_1, \dots, S_j$ of different slopes. Then there exists a factorization*

$$f(x) = F_1(x) \dots F_j(x) \pmod{\pi^l}$$

such that $N_\phi(F_i)$ is one-sided with the same slope as S_i. Furthermore, the maximum number of irreducible factors of F_i is $d(N_\phi(F_i))$, where d is the degree of a side. In particular, if $d(N_\phi(F_i)) = 1$, F_i is irreducible.

Proof. By hypothesis, all the monic lifts of f to $\mathcal{O}_K[x]$ share the same ϕ-polygon. We know that the theorem holds over $\mathcal{O}_K$ (2.22); choosing a monic lift $\widetilde{f}$ of f, we get a factorization $\widetilde{f} = \widetilde{F}_1 \dots \widetilde{F}_j$. Projecting the factors over $\mathcal{O}_K/(\pi^l)$ we get the first part of the theorem.
Since by lemma 4.6 every factorization of f is obtained as the projection of the factorization of a monic lift of f, it is enough to bound the number of the factors of the lifts. By corollary 2.23, the number of factors of $\widetilde{F}_i$ is bounded by the degree of $N_\phi(\widetilde{F}_i) = N_\phi(F_i)$, as desired. □

This easy extension of the properties of Newton polygons to our setting allows us to recover the irreducibility criterion for polynomials mod π^2 given by Sălăgean (3.18):

Theorem 4.9. *Let $f, \phi \in \mathcal{O}_K[x]$ be monic polynomials such that $f \equiv \phi^k \pmod{\pi}$ with $k \geq 2$ and ϕ is irreducible mod π. Let $h \in \mathcal{O}_K[x]$ be a polynomial such that $f = \phi^k + \pi h$ over $\mathcal{O}_K$. Then f is irreducible mod π^2 if and only if $h \not\equiv 0 \pmod{\pi}$ and $\phi \nmid h \pmod{\pi}$.*

Proof. If the conditions on h hold, the ϕ-polygon associated to f has a unique side of degree one, therefore f is irreducible. Assume now that f is irreducible mod π^2. We can consider its reduced ϕ-development:

$$f(x) = \sum_{i=0}^{k} a_i(x)\phi(x)^i = \phi^k + \pi h$$

The hypotheses imply that the ϕ-polygon of f is one-sided with endpoints $(0,1)$, $(k,0)$ and therefore $\pi^2 \nmid h(x)$. The second condition on h is obvious, since if $\phi \mid h \pmod{\pi}$, ϕ would divide f. □

An algorithm for irreducibility Now, we give an algorithm that determines whether or not a polynomial is irreducible, exploiting the theory we have developed so far. Let $f \in \mathcal{O}_K[x]/(\pi^l)$ be a monic polynomial. If f has two distinct irreducible factors mod π, then f is reducible by Hensel's lemma, and we can factor f. Therefore we can suppose that f has a unique irreducible factor ϕ mod π.
If $f \equiv \phi \mod \pi$, then f is irreducible and we are done. Otherwise, $f \equiv \phi^k \pmod{\pi}$ with $k \geq 2$. We can choose lifts $\widetilde{f}, \widetilde{\phi}$ of f, ϕ to $\mathcal{O}_K[x]$ and compute the reduced $\widetilde{\phi}$-development of $\widetilde{f}$

$$\widetilde{f}(x) = \sum a_i(x)\widetilde{\phi}(x)^i$$

If $a_0(x) = 0$, then f is clearly reducible because $\widetilde{\phi} \mid f \pmod{\pi^l}$. Hence we can assume that $a_0(x) \neq 0$ and we can construct the ϕ-polygon of f. By the theorem of the product, if the ϕ-polygon has more than one side, f splits and therefore it can not be irreducible. If it is one-sided, we have to distinguish two cases:

1. if the side has degree 1, f is irreducible by 4.8.
2. if the side has degree > 1, then we can only try to lift all the possible factorizations of f from the residue field to $\mathcal{O}_K/(\pi^l)$ following the algorithm by Von Zur Gathen and Hartlieb described in the previous chapter.

This must be done carefully: we do not need to search for all the possible factorizations, but we can select the lifts using the ϕ-polygon. Indeed, we know by 4.8 the maximum number of factors of f and their possible degree (the factors corresponds to a part of the side, so we know all the possible length and slopes) and this fact speeds up the calculations.

This algorithm can be used to find a factorization of f into irreducible factors. Indeed, if f is reducible the algorithm returns a proper factorization of f and therefore we can use the algorithm to determine if the factors are irreducible and so on. We will see an improvement that can be made to this algorithm in the last section of this chapter.

Slope factorization The irreducibility criterion we have discussed so far can be used to factor a polynomial mod π^l into irreducible factors. However, the factorization provided by Newton polygons (which is the main tool used in the irreducibility criterion) depends on the chosen lift to $\mathcal{O}_K[x]$. Indeed, as the following example shows, different lifts to $\mathcal{O}_K[x]$ can produce different factors of f:

Example 4.10. *Let $f \in \mathbb{Q}_2[x]$ the polynomial*

$$f(x) = (x+2)^2(x-4)$$

We want to factor f over $\mathbb{Z}/(32)$. Since $a_0 = -16$, we can consider the Newton polygon of f, which is well defined.

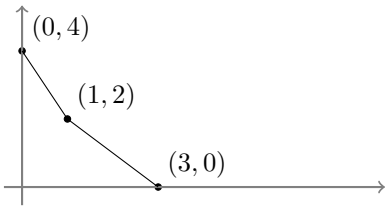


Figure 4.2: Newton polygon of f

Notice that

$$(x+2)^2(x-4) = (x+10)(x-6)(x-4) \pmod{32}$$

are two different factorizations that give rise to two different lifts, f and $g = (x-6)(x+10)(x-4)$. The slope factorization applied to f gives the factors $(x+2)^2$ and $(x-4)$, while the slope factorization applied to g gives $(x+10)(x-6)$ and $(x-4)$.

Even if the example shows that their use is difficult, in some situations Newton polygons can help in the search for all the factorizations. As usual, by the uniqueness theorem 1.65, we can consider a monic polynomial $f \in \mathcal{O}_K[x]/(\pi^l)$ and a monic polynomial $\phi \in \mathcal{O}_K[x]$ of degree d such that $f \equiv \phi^k \pmod{\pi}$ and ϕ is irreducible mod π. Assume first that the generalized ϕ-polygon is well defined, so that all the lifts of f share the same ϕ-polygon. Then, we know all the possible degrees of a factor of f, since they must be equal to the length of

a side contained in the ϕ-polygon. In particular, the number of factors of f is bounded by the sum of the degrees of the sides of the ϕ-polygon. If $l_1, \dots l_n$ are the lengths of the sides of the ϕ-polygon of f and $d_1, \dots, d_n$ are their degrees, the irreducible factors of f can only have degree

$$s \cdot d \cdot \frac{l_i}{d_i}$$

where s is a positive integer such that $s \mid d_i$. Furthermore, by the theorem of the product, the ϕ-polygon of every factor obtained in this way coincides, up to a translation, with a part of a side of $N_\phi(f)$ and therefore we know in advance the valuations of the terms of the reduced ϕ-development of every factor.

We still have to understand what we can say when the ϕ-polygon of f is not defined. Even if we can not repeat the argument presented above, sometimes it happens that all the lifts of f share a common part of their polygons.

Example 4.11. *We consider the polynomial $f = x^3 + 2x$ over $\mathbb{Z}/(16)$. Then it can be easily noticed that every lift of f to $\mathbb{Z}_2[x]$ has the side of ends $(1,1)$, $(3,0)$, while we can not say anything about the other one. Therefore in every factorization of f must appear a factor of degree 2.*

The argument presented before is still valid for the common part of the polygons of the lifts and therefore can be used to speed up the algorithm.

4.2 Dedekind's Criterion

In a certain sense, the criterion for irreducibility developed by Sălăgean hides the theoretical reasons necessary to understand it. Indeed, the proof of the criterion 3.18 is quite easy and uses simple techniques but it is not clear why such a criterion can not be generalized and holds only in this context. However, it turns out that this irreducibility criterion is similar to another famous criterion for normality, Dedekind's criterion, which relies on the following lemma:

Lemma 4.12. *Let R be a noetherian domain and assume that the integral closure $\overline{R}$ of R in its quotient field K is a finite R-module. Let $J \subseteq R$ be a non-trivial ideal of R. Then*

$$R \subseteq (J :_K J) \subseteq \overline{R}$$

Proof. The proof is an immediate consequence of Cayley-Hamilton theorem. Indeed, $(J :_K J)$ is a R-algebra since it is closed under multiplication. We need to check that every $\beta \in (J :_K J)$ is integral over R. Let $\varphi_\beta \colon J \to J$ be the multiplication by β map. J is finitely generated by noetherianity and then, by Cayley-Hamilton theorem, there exist $a_1, \dots, a_{n-1} \in R$ such that $\varphi_\beta^n + \sum a_i \varphi_\beta^i = 0$. Applying this relation to the element 1, we get $\beta^n + \sum a_i \beta^i = 0$ which means that β is integral over R. □

This lemma is the key for all the normalization algorithms such as the Round Two of Pohst-Zassenhauss (see [7]). These algorithms are usually expensive and Dedekind's Criterion is so important because it provides an easy tool to verify whether or not an order is integrally closed. We are going to prove it in the context of a p-adic field. In this case, their rings of integers are local rings of dimension one and the following lemma will be useful:

Lemma 4.13. *Let R be a regular local ring with maximal ideal $\mathcal{M}$. Given $f \in \mathcal{M}$, $R/(f)$ is regular if and only if $f \notin \mathcal{M}^2$*

Proof. Let $d = \dim R$. We will denote by dim the Krull dimension of a ring and with $\dim_{R/\mathcal{M}}$ the dimension as a $R/\mathcal{M}$-vector space.
By the definition of regular local ring, we know that $\dim_{R/\mathcal{M}} \mathcal{M}/\mathcal{M}^2 = d$. Since R is regular, R is an integral domain and $\dim R/(f) = \dim A - 1$ because f is not a zero-divisor. Therefore, if we call $\mathcal{N}$ the maximal ideal of $R/(f)$, it is enough to show that $\dim_{R/\mathcal{M}} \mathcal{N}/\mathcal{N}^2 = d-1$. If $f \notin \mathcal{M}^2$, then f can be completed to a basis of $\mathcal{M}/\mathcal{M}^2$ as a $R/\mathcal{M}$-vector space, $(\bar{f}, \bar{g}_1, \ldots, \bar{g}_{d-1})$. Therefore $\mathcal{N}/\mathcal{N}^2$ has a basis given by $(\bar{g}_1, \ldots, \bar{g}_{d-1})$ and $R/(f)$ is regular, proving one implication. Vice versa, assume that $f \in \mathcal{M}^2$. The natural map

$$\mathcal{M}\!\diagup_{\mathcal{M}^2} \longrightarrow \mathcal{N}\!\diagup_{\mathcal{N}^2}$$

is injective (as a $R/\mathcal{M}$-linear map) so $\dim_{R/\mathcal{M}} \mathcal{N}/\mathcal{N}^2 = \dim_{R/\mathcal{M}} \mathcal{M}/\mathcal{M}^2 = d$. Therefore $R/(f)$ is not regular. □

Theorem 4.14 (Local Dedekind's Criterion)**.** *Let K be a p-adic field with uniformizing element π and let $f \in \mathcal{O}_K[x]$ be a monic and irreducible polynomial. Consider the order $M = \mathcal{O}_K[x]/(f)$ and its quotient field L. Let I_p be the radical of (p) in M and*

$$(I_p : I_p) = \{\beta \in L \mid \beta I_p \subseteq I_p\}$$

Let $\phi \in \mathcal{O}_K[x]$ be a monic polynomial of degree d such that $f \equiv \phi^k \pmod{\pi}$, ϕ is irreducible over the residue field and

$$h = \frac{f - \phi^k}{\pi} \in \mathcal{O}_K[x]$$

Then

1. *M is integrally closed if and only if $(\phi, h) = 1 \pmod{\pi}$ or $k = 1$.*
2. *if M is not integrally closed,*

$$(I_p : I_p) = M + \frac{\phi(x)^{k-1}}{\pi} M$$

and $[(I_p : I_p) : M] = q^d$, where q is the cardinality of the residue field of K.

Proof. First of all, we show that I_p is generated by π and $\phi(x)$. Clearly, $\pi \in I_p$ and $\phi(x) \in I_p$ (by hypothesis, $\phi(x)^k \equiv 0 \pmod{\pi}$), so we only need to check the other containment, which follows directly from the fact that $(\pi, \phi(x))$ is a maximal ideal of $\mathcal{O}_K[x]$ (p can not be invertible and therefore its radical must be a proper ideal).

Then, we prove that M is integrally closed if and only if $(\phi, h) = 1 \pmod{\pi}$ or $k = 1$. Assume that M is integrally closed. If $k = 1$, we are done. Assume then that $k \geq 2$. We know that $\mathcal{O}_K[x]_{(\pi,\phi)}$ is a regular local ring and M is its quotient by f. For one-dimensional rings, being integrally closed is equivalent to being regular (see [2]), so M is a regular local ring and, by the previous lemma, $f \notin (\pi, \phi)^2 = (\phi^2, \pi\phi, \pi^2)$. We notice that

$$f \equiv \phi^k + \pi h \equiv \pi h \pmod{(\pi, \phi)^2}$$

If $h \equiv 0 \pmod{\pi}$, then $f \in (\pi, \phi)^2$ and M is not regular, giving a contradiction. Therefore $h \not\equiv 0 \pmod{\pi}$. Furthermore, it must hold $(\phi, h) \equiv 1 \pmod{\pi}$. Indeed, if $\phi \mid h \pmod{\pi}$, then there exists $\eta \in \mathcal{O}_K[x]$ such that $h \equiv \phi\eta \pmod{\pi}$ and $f \equiv \pi\phi\eta \equiv 0 \pmod{(\pi, \phi)^2}$. This contradicts the regularity assumption, therefore it must hold $(\phi, h) = 1 \pmod{\pi}$.

Vice versa, assume that $(\phi, h) \equiv 1 \pmod{\pi}$. We distinguish two cases:

- if $k = 1$, M is integrally closed because $\operatorname{disc}(f) = \operatorname{disc}(\phi)$ and the last is a unit. By the formula
$$\operatorname{disc}(f) = \operatorname{disc} M = \operatorname{ind}(M)^2 \operatorname{disc}(\mathcal{O}_L)$$
we get $\operatorname{ind}(M) = 1$, as desired.
- if $k \geq 2$, then $f \notin (\pi, \phi)^2$ and, by the lemma, M is a regular local ring and so integrally closed.

It remains to prove the statement in the case $(\phi, h) \neq 1 \pmod{\pi}$. Let α be a root of f in a fixed algebraic closure of $\mathbb{Q}_p$. Every element β of $(I_p : I_p)$ can be represented as $t(\alpha)/\pi$, where t is a polynomial in $\mathcal{O}_K[x]$, because $\beta \cdot \pi \in M = \mathcal{O}_K[\alpha]$. We want to give some conditions on t in order to have
$$\frac{t(\alpha)}{\pi}\phi(\alpha) \in I_p = (\pi, \phi(\alpha))$$
Equivalently, there exist $a_1, a_2 \in \mathcal{O}_K[x]$ such that
$$\frac{t(\alpha)}{\pi}\phi(\alpha) = \pi a_1(\alpha) + \phi(\alpha)a_2(\alpha)$$
We can lift this relation to the polynomial ring $\mathcal{O}_K[x]$; indeed, f is the minimal polynomial of α and therefore there exists $a_3 \in \mathcal{O}_K[x]$ such that
$$t(x)\phi(x) = \pi^2 a_1(x) + \pi\phi(x)a_2(x) + a_3(x)f(x)$$
Reducing this equation mod π, we get
$$t(x)\phi(x) = a_3(x)f(x) \pmod{\pi} \implies t(x) = a_3(x)\phi(x)^{k-1} \pmod{\pi}$$
This means that $t(x) = a_3(x)\phi(x)^{k-1} + \pi a_4(x)$, so $t(\alpha)/\pi$ is the sum of an element in $\phi(\alpha)^{k-1}/\pi\mathcal{O}_K[\alpha]$ and an element of $\mathcal{O}_K[\alpha]$. Since also $t(\alpha)/\pi = t(\alpha) \in I_p$,
$$(I_p : I_p) \subseteq M + \frac{\phi(x)^{k-1}}{\pi}M$$
To show the converse, it is enough to prove that $\phi^{k-1}(\alpha)/\pi \in (I_p : I_p)$. By definition,
$$\frac{\phi^{k-1}(\alpha)}{\pi} \cdot \pi = \phi^{k-1}(\alpha) \in I_p = (\pi, \phi(\alpha))$$
and
$$\frac{\phi^{k-1}(\alpha)}{\pi} \cdot \phi(\alpha) = \frac{\phi^k(\alpha)}{\pi} \in I_p$$
Indeed, we know that $\phi(\alpha) \mid h(\alpha)$ and $\phi^k + \pi h \equiv 0 \pmod{(\pi^2, f)}$, so there exists $h_2(x) \in \mathcal{O}_K[x]$ such that
$$\phi^k(\alpha) = -\pi h(\alpha) + \pi^2 h_2(\alpha)$$

in $\mathcal{O}_K[\alpha]$. Dividing by π the relation, we get

$$\frac{\phi(\alpha)^{k-1}}{\pi} = h(\alpha) + \pi h_2(\alpha) \in I_p$$

Since $\phi(\alpha) \mid h(\alpha)$, the right hand side lies in $(\pi, \phi(\alpha))$, as desired.
Consequently, a basis for $(I_p : I_p)$ is given by

$$1, \alpha, \dots, \alpha^{d(k-1)-1}, \frac{\phi(\alpha)^{k-1}}{\pi}, \dots, \frac{\alpha^{d-1}\phi(\alpha)^{k-1}}{\pi}$$

Consider the matrix given by the coordinates of these elements with respect to $1, \alpha, \dots, \alpha^{n-1}$. It is upper triangular, with diagonal elements $d_1, \dots, d_n$ equal to

$$d_i = \begin{cases} 1 & \text{if } i \leq d(k-1)-1 \\ \frac{1}{\pi} & \text{if } i \geq d(k-1) \end{cases}$$

and therefore the quotient $(I_p : I_p)/\mathcal{O}_K[\alpha]$ has cardinality q^d, where q is the cardinality of the residue field of K.

□

As we said before, the conditions required by Dedekind's Criterion are really similar to the hypotheses of the irreducibility criterion given by Sălăgean in theorem 3.18. We can easily state the following corollary:

Corollary 4.15. *Let $f \in \mathcal{O}_K[x]$ be a monic irreducible polynomial and let $M = \mathcal{O}_K[x]/(f)$. f is irreducible mod π^2 if and only if M is integrally closed.*

Proof. If f is irreducible mod π, we are in the hypotheses of Dedekind's Criterion and so M is integrally closed. If f is reducible mod π and irreducible mod π^2, then we can write

$$f \equiv \phi^k + \pi h \pmod{\pi^2}$$

with $k \geq 2$, $h \not\equiv 0 \pmod{\pi}$ and $(h, \phi) \equiv 1 \pmod{\pi}$. By Dedekind's Criterion, M is integrally closed, as desired.

Assume now that M is integrally closed and write $f \equiv \phi^k + \pi h \pmod{\pi^2}$ with $(\phi, h) \equiv 1 \pmod{\pi}$. We have to distinguish two cases:

- if $k = 1$, f is irreducible mod π and so it is mod π^2
- if $k \geq 2$, assume by contradiction that f is reducible

  $$\phi^k + \pi h \equiv (\phi^{k_1} + \pi h_1)(\phi^{k_2} + \pi h_2) \pmod{\pi^2}$$

  Then, computing the product, it must hold

  $$\phi^{k_1} h_2 + \phi^{k_2} h_1 \equiv h \pmod{\pi}$$

  By Dedekind's Criterion, we have $(h, \phi) \equiv 1 \pmod{\pi}$. However, the left-hand side is divisible by ϕ, giving a contradiction.

□

The result obtained by Sălăgean easily follows, with a more conceptual proof:

Corollary 4.16. *Let $f \in \mathcal{O}_K[x]$ be a monic polynomial such that $f \equiv \phi^k \pmod{\pi}$, where $\phi \in \mathcal{O}_K[x]$ is a monic polynomial, irreducible mod π. Assume that $k \geq 2$ and let $h \in \mathcal{O}_K[x]$ such that $f = \phi^k + \pi h$. Then f is irreducible mod π^2 if and only if $h \neq 0 \pmod{\pi}$ and $\phi \nmid h \pmod{\pi}$.*

This approach suggests a way for obtaining a stronger result and a generalization. Indeed, there seems to exists a connection between the index and the smallest $l \in \mathbb{N}$ such that an irreducible polynomial $f \in \mathcal{O}_K[x]$ is irreducible mod π^l; we will investigate this later in this chapter.

We end this section with a bound for the index of the order generated by a root of an irreducible polynomial over $\mathcal{O}_K$ in its integral closure $\mathcal{O}_L$:

Proposition 4.17. *Let $f \in \mathcal{O}_K[x]$ be a monic irreducible polynomial and assume $f \equiv \phi^k + \pi h \pmod{\pi^2}$, where ϕ is irreducible mod π of degree d. Let L be the field generated by a root α of f over K and let $M = \mathcal{O}_K[x]/(f)$. If $\phi \mid h \pmod{\pi}$ and $h \not\equiv 0 \pmod{\pi}$, then $q^{\lfloor k/2 \rfloor d} \mid [\mathcal{O}_L : M]$, where q is the cardinality of the residue field of K.*

Proof. We can assume without loss of generality that $k \geq 4$; indeed, if $k < 4$, the thesis follows directly from Dedekind's Criterion. We denote by s the integer $\lfloor k/2 \rfloor$.
In these hypotheses, $\phi^s \mid h$ over the residue field of K. This follows from the theory on Newton Polygons: if $\phi^s \nmid h$, the ϕ-polygon $N_\phi(f)$ of f would have two lines of different slopes and this can not happen since f is irreducible over $\mathcal{O}_K$ (2.22).
Now, we want to show that ϕ^{k-s}/π is integral over M. In order to achieve this result, we consider the ideal $J = (\pi, \phi^s) \subseteq M$ and we show that $\phi^{k-s}/\pi \cdot J \subseteq J$. We know that the following equality holds

$$\phi(\alpha)^k + \pi\phi(\alpha)^t h \equiv 0 \pmod{\pi^2}$$

where $t \geq s$. As a consequence, we can write $\phi^k(\alpha) = -\pi\phi^t(\alpha)h + \pi^2 h_1(\alpha)$, obtaining

$$\frac{\phi^{k-s}(\alpha)}{\pi} \cdot \pi = \phi(\alpha)^{k-s} \qquad \frac{\phi(\alpha)^{k-s}}{\pi} \cdot \phi(\alpha)^s = -\phi(\alpha)^t h + \pi h_1(\alpha)$$

Notice that $\phi(\alpha)^{k-s} \in J$ since $k \geq 2s$, so both the elements lie in J proving that $\phi(\alpha)^{k-s}/\pi$ is integral over M.

We are ready to prove the result about the index. The order $(J : J)$ obtained after the addition to M of the element $\phi^{k-s}(\alpha)/\pi$ is generated as a $\mathcal{O}_K$-module by

$$1, \alpha, \ldots, \alpha^{d(k-s)-1}, \frac{\phi(\alpha)^{k-s}}{\pi}, \frac{\alpha\phi(\alpha)^{k-s}}{\pi}, \ldots, \frac{\alpha^{d-1}\phi(\alpha)^{k-1}}{\pi}$$

Consider the matrix given by the coordinates of these elements with respect to $1, \alpha, \ldots, \alpha^{n-1}$. It is upper triangular with diagonal element $d_1, \ldots, d_n$ such that

$$d_i = \begin{cases} 1 & \text{if } i \leq d(k-s) - 1 \\ \frac{1}{\pi} & \text{otherwise} \end{cases}$$

Therefore $q^{ds} \mid [(J :_K J) : M]$ and this implies $p^{ds} \mid [\mathcal{O}_L : M]$, as desired. □

We will exploit this result later. Notice that it can be used to speed up the normalization algorithms over p-adic fields, since it determines a priori an order extending $\mathcal{O}_K[\alpha]$ that contains strictly the one given by Dedekind's criterion. There is also a global statement of this corollary, that generalizes the global statement of Dedekind's Criterion over $\mathbb{Z}$ (see [7] and [8]):

Proposition 4.18. *Let $f \in \mathbb{Z}[x]$ be a monic irreducible polynomial and $p \in \mathbb{N}$ be a prime. Let α be one of the roots of f, $K = \mathbb{Q}(\alpha)$, let $M = \mathbb{Z}[x]/(f)$ and let $\mathcal{O}_K$ be its normalization. If*

$$f \equiv \prod_{i=1}^{k} \phi_i^{e_i} + ph \pmod{p^2}$$

with ϕ_i irreducible for all i and $\prod_{i\in I} \phi_i^{s_i} \mid h$, where I is a subset of indexes $I \subseteq \{1, \ldots, k\}$ and $4 \leq 2s_i \leq e_i$ for $i \in I$, then the element

$$\frac{\prod_{i\in I} \phi_i^{e_i - s_i} \prod_{i\notin I} \phi_i^{e_i}}{p}$$

is integral over M. In particular, $p^{\sum_{i\in I} d_i s_i} \mid [\mathcal{O}_K : M]$, where $d_i = \deg \phi_i$.

Proof. As in the proof of the local case, we consider the ideal

$$J = \Big(p, \prod_{i\in I} \phi_i^{s_i} \prod_{i\notin I} \phi_i\Big)$$

and we show that

$$\frac{\prod_{i\in I} \phi_i^{e_i - s_i} \prod_{i\notin I} \phi_i^{e_i}}{p} \cdot p \in J$$

$$\frac{\prod_{i\in I} \phi_i^{e_i - s_i} \prod_{i\notin I} \phi_i^{e_i}}{p} \cdot \prod_{i\in I} \phi_i^{s_i} \prod_{i\notin I} \phi_i \in J$$

The first relation is obvious, since $\prod_{i\in I} \phi_i^{s_i} \prod_{i\notin I} \phi_i \mid \prod_{i\in I} \phi_i^{e_i - s_i} \prod_{i\notin I} \phi_i^{e_i}$ by the hypothesis $e_i \geq 2s_i$.
For the second relation, we use the equation

$$\prod_{i=1}^{k} \phi_i^{e_i} + ph \equiv 0 \pmod{p^2, f}$$

Multiplying by $\prod_{i\notin I} \phi_i$, we get

$$\prod_{i=1}^{k} \phi_i^{e_i} \prod_{i\notin I} \phi_i + ph \prod_{i\notin I} \phi_i \equiv 0 \pmod{p^2, f}$$

Notice that

$$\prod_{i\in I} \phi_i^{s_i} \prod_{i\notin I} \phi_i \mid h \prod_{i\notin I} \phi_i \tag{4.1}$$

by the definition of the s_i. As a consequence,

$$\prod_{i=1}^{k} \phi_i^{e_i} \prod_{i\notin I} \phi_i = -ph \prod_{i\notin I} \phi_i + p^2 h_2 \pmod{f}$$

and

$$\frac{\prod_{i\in I}\phi_i^{e_i-s_i}\prod_{i\notin I}\phi_i^{e_i}}{p}\cdot\prod_{i\in I}\phi_i^{s_i}\prod_{i\notin I}\phi_i=-h\prod_{i\notin I}\phi_i+ph_2 \pmod f$$

and the right-hand side lies in J. Indeed, $h\prod_{i\notin I}\phi_i\in J$ by (4.1) and $ph_2\in J$ because $p\mid ph_2$.
Let α be a root of f. The result about the index follows as usual by considering the matrix given by the coordinates of the basis obtained by the addition of

$$\frac{\prod_{i\in I}\phi_i^{e_i-s_i}\prod_{i\notin I}\phi_i^{e_i}}{p}$$

to $\mathbb{Z}[\alpha]$ with respect to $1,\alpha,\ldots,\alpha^{n-1}$. □

As far as we know, these results are new and they could provide an improvement for some of the existing normalization algorithm, as Round Two of Pohst and Zassenhauss. Indeed, whenever the hypotheses are satisfied, we can extend $\mathbb{Z}[\alpha]$ (where α is a root of f) by adding these integral elements and the order obtained in this way strictly contains the order provided by Dedekind's Criterion. This reduces the number of iterations needed to terminate the algorithm.

4.3 A formula for irreducibility

When dealing with the problem of factoring polynomials over a p-adic field, we have encountered some uses of Krasner's lemma (1.43), which gives a sufficient condition for two elements in $\overline{\mathbb{Q}}_p$ to generate the same field over $\mathbb{Q}_p$. There is an important and well-known consequence of this fact. Indeed, we can use Krasner's lemma to understand when every polynomial in the fiber of a monic irreducible polyomial $f\in\mathcal{O}_K[x]$ under the projection $\varphi\colon\mathcal{O}_K[x]\longrightarrow\mathcal{O}_K[x]/(\pi^l)$, where π is a uniformizer of $\mathcal{O}_K$, is irreducible. This condition would assure the irreducibility of f mod π^l by lemma 4.6. In this section, we will always assume that the valuation is normalized, so that $v(\pi)=1$.

Let $f\in\mathcal{O}_K[x]$ be a monic irreducible polynomial of degree n and $g\in\mathcal{O}_K[x]$ be another polynomial of degree n. Given α, β two roots of f and g respectively, then

$$[K(\alpha):K]=n \qquad\qquad [K(\beta):K]\leq n$$

In order to prove the irreducibility of g, it is enough to show that $K(\beta)\supseteq K(\alpha)$ and we are going to achieve this result by means of Krasner's Lemma. Let a_i and b_i be the coefficient of f and g respectively, $\alpha=\alpha_1,\alpha_2,\ldots,\alpha_n$ the roots of f and $\beta_1,\ldots,\beta_n$ the roots of g. We define

$$C=\max_{i\neq j}v(\alpha_i-\alpha_j)$$

Evaluating g at α, we get

$$v(g(\alpha))=\sum_{i=1}^{n}v(\alpha-\beta_i)$$

On the other hand, $g(\alpha) = g(\alpha) - f(\alpha)$, so

$$\begin{aligned} v(g(\alpha)) &= v(g(\alpha) - f(\alpha)) \\ &= v\Big(\sum_{i=0}^{n-1}(a_i - b_i)\alpha^i\Big) \\ &\geq \min_i v((a_i - b_i)\alpha^i) \\ &\geq \min_i v(a_i - b_i) \end{aligned}$$

Notice that in the last passage we have used the fact that an algebraic integer has valuation ≥ 0 and α is an integral element since it is a root of a monic polynomial. Therefore, if $v(a_i - b_i) > nC$, we get

$$\sum_{i=1}^{n} v(\alpha - \beta_i) > nC$$

In particular, there exists an index $\bar{\imath}$ such that $v(\alpha - \beta_{\bar{\imath}}) > C$, so $\beta_{\bar{\imath}}$ satisfies the hypotheses of Krasner's Lemma. We summarize this argument in the following proposition:

Proposition 4.19. *Let K be a p-adic field and $\mathcal{O}_K$ be its ring of integers. Let $f \in \mathcal{O}_K[x]$ be a monic irreducible polynomial of degree n and $g \in \mathcal{O}_K[x]$ be another monic polynomial of degree n. If $v(f - g) > nC$, then g is irreducible over $\mathcal{O}_K$.*

This fact is quite interesting; however, this formulation does not allow a practical use of it, because it is difficult to know the exact value of C. In order to use this proposition to detect the irreducibility of a polynomial, we need to estimate nC with an invariant that we can easily compute, such as the discriminant of f. We notice that

$$v(\mathrm{disc}(f)) = \sum_{i>j} 2 \cdot v(\alpha_i - \alpha_j)$$

Without loss of generality, we can assume that $v(\alpha_1 - \alpha_2) = C$. We want to lower bound the number of pairs (i, j) such that $v(\alpha_1 - \alpha_2) = v(\alpha_i - \alpha_j)$ and $i > j$. Let L be the splitting field of f; since f is irreducible, the Galois group of L/K acts transitively on the roots of f and for every index i there exists an element σ_i of $\mathrm{Gal}(L/K)$ such that $\sigma_i(\alpha_1) = \alpha_i$. We notice that by the unique extension property of valuations $v(\alpha_1 - \alpha_2) = v(\sigma(\alpha_1 - \alpha_2))$. This means that every σ_i acts on the set of pairs (i, j) such that $v(\alpha_i - \alpha_j) = C$. Let τ_i be the permutation induced by σ_i, so that $\tau_i(1) = i$ for all i. In the set

$$\tau_1(1,2) \qquad \tau_2(1,2) \qquad \dots \qquad \tau_n(1,2)$$

every pair can occur at most twice (we need to consider the ordered pairs, whose first component is greater than the second). This argument shows that

$$\#\{(i,j) \mid v(\alpha_i - \alpha_j) = C\} \geq \frac{n}{2}$$

Let S be a subset of these pairs of indices of cardinality $n/2$. We can divide the summands in the above relation into two groups: the pairs in S and the pairs in its complementary. Thus,

$$\begin{aligned} v(\mathrm{disc}(f)) &= 2C \cdot (\#S) + \sum_{(i,j)\notin S} 2v(\alpha_i - \alpha_j) \\ &= nC + \sum_{(i,j)\notin S} 2v(\alpha_i - \alpha_j) \end{aligned}$$

Notice that the cardinality of the complementary of S is

$$\frac{n(n-1)}{2} - \frac{n}{2} = \frac{n(n-2)}{2}$$

To bound the second sum, we use the triangular inequality, so that $v(\alpha_i - \alpha_j) \geq \min\{v(\alpha_i), v(\alpha_j)\} = v(\alpha_i)$, where the last equality comes again from the uniqueness of the extension of a valuation. Then

$$v(\mathrm{disc}(f)) \geq nC + \sum_{(i,j)\notin S} 2v(\alpha_i) \geq nC + 2v(\alpha_1) \cdot \frac{n(n-2)}{2}$$

Since the coefficients of a polynomial are symmetric functions of the roots, the constant term a_0 of f is the product of all the roots α_i. Therefore, $v(a_0) = nv(\alpha_i)$ and we get the inequality

$$v(\mathrm{disc}(f)) \geq nC + (n-2)v(a_0)$$

In this way, what we have is a bound of nC that allows to state the following proposition:

Proposition 4.20. *Let $f = \sum a_i x^i$ be a monic irreducible polynomial in $\mathcal{O}_K[x]$. If*

$$l > v(\mathrm{disc}(f)) - (n-2)v(a_0)$$

then f is irreducible in $\mathcal{O}_K[x]/(\pi^l)$.

Observation 4.21. *To improve the inequality, it is necessary to find a better bound for the cardinality of the set*

$$\{(i,j) \mid v(\alpha_i - \alpha_j) = C\}$$

For instance, if the Galois Group of the splitting field of f contains a n-cycle and n is odd, the orbit of the pair $(1,2)$ has cardinality $\geq n$ and the inequality becomes

$$l > \frac{v(\mathrm{disc}(f))}{2} - \frac{(n-3)v(a_0)}{2}$$

Indeed,

$$v(\mathrm{disc}(f)) \geq 2nC + \frac{2}{n}v(\alpha_1)\Big(\frac{n(n-1)}{2} - n\Big) = 2nC + (n-3)v(a_0)$$

If the Galois group is a doubly transitive subgroup of the symmetric group, then the orbit of the pair $(1,2)$ has cardinality $n(n-1)/2$ and the inequality changes because

$$v(\mathrm{disc}(f)) \geq n(n-1)C$$

and therefore

$$l \geq \frac{v(\mathrm{disc}(f))}{n-1}$$

This formula can be used to enhance the irreducibility criterion we developed in the first section of this chapter. Indeed, before starting to compute the lifts of the factorization mod π, it is convenient to choose a lift $\tilde{f}$ of f to the p-adic and factor it. If $\tilde{f}$ splits, then the same holds for f. If $\tilde{f}$ is irreducible, we can use the formula to understand if f is irreducible.

Example 4.22.

- *Let f be an Eisenstein polynomial of degree n over a p-adic field K. If $(n,p)=1$, then $v(\mathrm{disc}(f)) = n-1$. Using the formula, we get*

  $$k > n-1-(n-2) = 1$$

  and this is equivalent to say that f is irreducible mod π^2. We already knew this result by Dedekind's Criterion (even without the assumption of tameness), but the proposition provides a new proof.

- *Let f be a monic lift of an irreducible polynomial over the residue field of a p-adic field K. In this case, $v(\mathrm{disc}(f)) = 0$, $v(a_0) = 0$ and therefore $k > 0$, so that f is irreducible mod π.*

Observation 4.23. *Given a monic polynomial $f \in \mathcal{O}_K[x]/(\pi^l)$, it is false in general that the discriminant of each lift is the same and this can change the usefulness of the formula. For example, consider the polynomials $f = x^4 + 2$ and $g = x^4 + 4x + 2$ over $\mathbb{Z}_p$. They projects to the same polynomial mod 4, where they are irreducible (by theorem 4.15). However, the valuations of their discriminants are different:*

$$v(\mathrm{disc}(f)) = 11 \qquad\qquad v(\mathrm{disc}(g)) = 8$$

Therefore, the chosen lift can influence the effectiveness of the formula. For instance, in one case we get

$$l > 11 - 2 = 9$$

and in the other one

$$l > 8 - 2 = 6$$

In both cases the formula gives a result far from optimal ones, but in one case is better than the other.

Observation 4.24. *Even if the formula depends on the chosen lift, for some polynomials there is no hope to find a lift for which the formula gives the minimum l. This follows directly from Krasner's lemma, which, given two polynomials f, g, provides a condition for their roots to generate the same fields. Consider now $f = x^2 - 2$ and $x^2 - 6$ in $\mathbb{Z}_2[x]$. They both project to $x^2 - 2 \pmod 4$ and they are irreducible there. However, their roots generate different fields, because $\mathbb{Q}_2(\sqrt{2}) \neq \mathbb{Q}_2(\sqrt{6})$.*

Unfortunately, the formula is influenced by the valuation of a_0, which can be a unit. More precisely, let ϕ be a lift of the unique irreducible factor of f mod π. If $\deg \phi = 1$ and $\phi \neq x$, we can make a change of variables (a translation) in order to have $\phi = x$ and therefore the formula can still be useful.
However, we can not use this method when $\deg \phi \geq 2$. In this case, the second term of the inequality of the proposition 4.20 vanishes because $v(a_0) = 0$ and therefore the lower bound for k becomes $v(\mathrm{disc}(f))$, which is the bound we already knew given by Hensel's lemma 1.54.
Fortunately, by virtue of proposition 1.69, we can extend the scalar and reduce ourselves to work on a factor of f in the unramified extension. Let U be the splitting field of ϕ and let $F_1, \ldots, F_d \in \mathcal{O}_U[x]$ be the factors of f over $\mathcal{O}_U$ given by Hensel's lemma (notice that $d = \deg \phi$). Then the irreducible factor of every F_i over the residue field of U is linear and therefore we can make a change of variables and use the formula on each F_i. To use this method, we need to understand what happens to the index during this process:

Proposition 4.25. *Let K be a p-adic field and $f \in K[x]$ be a monic irreducible polynomial such that $f = \phi^k \pmod{\pi}$, where ϕ is a monic polynomial irreducible mod π. Let U be the unramified extension of K corresponding to the splitting field of ϕ and F be the field generated by one of the roots α of f. Denote by $\mathcal{O}_K$, $\mathcal{O}_U$ and $\mathcal{O}_F$ the rings of integers of K, U and F respectively. Then*

$$v(\mathrm{ind}(\mathcal{O}_K[\alpha])) = \deg(\phi) \cdot v(\mathrm{ind}(\mathcal{O}_U[\alpha]))$$

Observation 4.26. *Let R, S be principal ideal domains such that S is free of rank s over R and F be a free B-module of rank t. We consider basis $b_1, \ldots, b_s$ of S as an R-module and $m_1, \ldots, m_t$ of F as a S-module. Then $\{b_i m_j\}_{i,j}$ is a basis of F as an R-module. We will use this fact in the proof.*

Proof. Firstly, we show that $\mathcal{O}_K[\alpha] = \mathcal{O}_U[\alpha]$. Clearly, it holds $\mathcal{O}_K[\alpha] \subseteq \mathcal{O}_U[\alpha]$ and so it is enough to show that $\mathcal{O}_U \subseteq \mathcal{O}_K[\alpha]$. Notice that

$$\mathcal{O}_K[\alpha] \simeq {\mathcal{O}_K[x]}\big/{(f)}$$

and the maximal ideal of this ring (which is local) is generated by $(\pi, \phi(\alpha))$. Therefore the polynomial ϕ splits completely over the residue field; by Hensel's Lemma, the same must happen in $\mathcal{O}_K[x]/(f)$ and so $\mathcal{O}_K[\alpha]$ contains all the roots of ϕ. Since ϕ is irreducible mod π, the order generated by any of its roots is maximal and therefore coincides with $\mathcal{O}_U$. This means exactly that $\mathcal{O}_K[\alpha] \supseteq \mathcal{O}_U$, as desired. Therefore $\mathcal{O}_K[\alpha]$ is both a $\mathcal{O}_K$ and $\mathcal{O}_U$-module. We want now to use the preliminary observation. Let

- $u_1, \ldots, u_d$ be a $\mathcal{O}_K$-basis for $\mathcal{O}_U$
- $a_1, \ldots, a_l$ be a $\mathcal{O}_U$-basis for $\mathcal{O}_F$
- $b_1, \ldots, b_l$ be a $\mathcal{O}_U$-basis for $\mathcal{O}_K[x]/(f)$

Let B be the matrix representing the change of basis from $a_1, \ldots, a_l$ to $b_1, \ldots, b_l$ and let A be the matrix representing the change of basis from $(a_i u_j)$ and $(b_i u_j)$.

Then A is composed of d blocks, each one equal to B,

$$A = \begin{pmatrix} B & & & \\ & B & & \\ & & \ddots & \\ & & & B \end{pmatrix}$$

so that $\det A = \det B^d$, where $d = \deg \phi$ and this gives the thesis. □

By this proposition, we can reduce our problem to the case of a p-adic field K, an irreducible monic polynomial $f \in \mathcal{O}_K[x]$ such that $f \equiv x^k \pmod{\pi}$. In this case, we can obtain information from our formula 4.20.
As usual, let $f \in \mathcal{O}_K[x]$ be a monic irreducible polynomial and $\phi \in \mathcal{O}_K[x]$ be the monic polynomial such that ϕ is irreducible mod π and $f \equiv \phi^k \pmod{\pi}$. If $\deg \phi = 1$, we can use the formula 4.20, as explained above. If not, we can consider the unramified extension U generated by ϕ over K. By Hensel's lemma, we know that $f = F_1 \dots F_d$ over $\mathcal{O}_U$ and, using theorem 1.69, we can apply the formula to each F_i to get a bound for the minimum l such that f is irreducible mod π^l. Therefore we get the following:

Theorem 4.27. *Let $f \in \mathcal{O}_K[x]$ be an irreducible monic polynomial such that $f \equiv \phi^k \pmod{\pi}$, where $\phi \in \mathcal{O}_K[x]$ is a monic polynomial of degree d irreducible mod ϕ. Let U be the splitting field of ϕ over $\mathcal{O}_K$ and let $F_1, \dots, F_d$ be the factors of f over $\mathcal{O}_U$ obtained by Hensel's lemma. Let $\nu_i \in \mathcal{O}_K[x]$ be a monic lift of the irreducible factor of F_i mod π and let*

$$F_i = \sum b_{j,i} \nu_i(x)^j$$

be the reduced ν_i-development of F_i. If

$$l > v(\mathrm{disc}(F_i)) - (n-2)v(b_{i,0}) \quad i = 1, \dots, d$$

then f is irreducible mod π^l.

Unfortunately, this formula is not practical because it requires to know the discriminants of the F_i and their reduced ν_i-developments. Therefore, we want to give an estimation to the right hand side with quantities easily computable. By corollary 2.27, we know that, with the same notations as the theorem above, $N_{\nu_i}(F_i) = N_\phi(f)$ (both of them are principal polygons) and therefore, if

$$f(x) = \sum a_i(x)\phi(x)^i \qquad\qquad F_i(x) = \sum b_{j,i}\nu_i(x)^j$$

are the reduced ϕ-development of f and the reduced ν_i-developments of F_i, we get $v(a_j(x)) = v(b_{j,i})$ for all $i = 1, \dots, d$.

Theorem 4.28. *Let $f \in \mathcal{O}_K[x]$ be a monic irreducible polynomial of degree n such that $f \equiv \phi^k \pmod{\pi}$, where $\phi \in \mathcal{O}_K[x]$ is a monic polynomial of degree d, irreducible mod π. Consider the reduced ϕ-development of f:*

$$f(x) = \sum a_i(x)\phi(x)^i$$

If $l \in \mathbb{N}$ is such that

$$l > \frac{v(\mathrm{disc}(f))}{d} - (k-2)v(a_0(x))$$

then f is irreducible over $\mathcal{O}_K/(\pi^l)$.

Proof. By the preliminarily discussion and the theorem above, it is enough to prove that $v(\text{disc}(f)) = d \cdot v(\text{disc}(F_i))$ for all i, where F_i is one of the factors of f over $\mathcal{O}_U$ obtained using Hensel's lemma. We denote by L_i the field generated by a root α_i of F_i over $\mathcal{O}_U$.
By formula 1.1 and proposition 4.25, we know that

$$v(\text{disc}(f)) = d \cdot v(\text{ind}(\mathcal{O}_U[\alpha_i])) + v(\text{disc}(\mathcal{O}_{L_i}/\mathcal{O}_K))$$
$$v(\text{disc}(F_i)) = v(\text{ind}(\mathcal{O}_U[\alpha_i])) + v(\text{disc}(\mathcal{O}_{L_i}/\mathcal{O}_U))$$

By the proposition 1.41, we can compute the discriminant of these extensions by their different and we have to compare $N_{L/K}(\mathcal{D}_{L_i/K})$ and $N_{L_i/U}(\mathcal{D}_{L/U})$. The different is multiplicative, so $\mathcal{D}_{L/K} = \mathcal{D}_{L/U}\mathcal{D}_{U/K}$ and the latter is trivial since by hypothesis the extension is unramified. Therefore

$$v(\text{disc}(\mathcal{O}_{L_i}/\mathcal{O}_K)) = v(N_{L_i/K}(\mathcal{D}_{L_i/K})) = v(N_{L_i/K}(\mathcal{D}_{L_i/U}))$$

Assume that $\mathcal{D}_{L_i/U} = (\pi_{L_i}^s)$. Then

$$v(N_{L_i/K}(\mathcal{D}_{L_i/U})) = v(N_{L_i/K}(\pi_{L_i}^s)) = s \cdot v(N_{L_i/K}(\pi_L)) = sn \cdot v(\pi_{L_i}) = \frac{sn}{e}$$

where $e = e(L_i/U)$ is the ramification index and $n = \deg(f)$. On the other hand,

$$v(N_{L_i/U}(\mathcal{D}_{L_i/U})) = s \cdot v(N_{L_i/U}(\pi_{L_i})) = \frac{sk}{e}$$

Therefore, $v(\text{disc}(\mathcal{O}_L/\mathcal{O}_K)) = d \cdot v(\text{disc}(\mathcal{O}_L/\mathcal{O}_U))$, as desired. □

4.4 Irreducibility mod π^3

In the previous sections, we presented some tools that can be useful for detecting irreducibility. Now we focus on the particular case of a polynomial mod π^3. This part can be considered as an example of how the notion we have developed so far can be used to solve the problem of deciding whether or not a polynomial is irreducible.
We already know when a polynomial is irreducible mod π or mod π^2, so we consider a polynomial f such that f is reducible mod π^2. In this case, we can prove the following theorems by using the theory about Newton polygons:

Theorem 4.29. *Let $f \in \mathcal{O}_K[x]/(\pi^3)$ be a monic polynomial which is reducible mod π^2. If f is irreducible, there exist $\phi \in \mathcal{O}_K[x]$ and $h_1, h_2 \in \mathcal{O}_K[x]/(\pi^3)$ such that*

$$f \equiv \phi^{k_1} + \pi\phi^{k_2}h_1 + \pi^2 h_2 \pmod{\pi^3}$$

where

- *ϕ is monic and irreducible mod π*
- *$k_2 \geq \lfloor k_1/2 \rfloor$*
- *$(h_2, \phi) \equiv 1 \pmod{\pi}$*

Proof. First of all, by Hensel's lemma, we know that f has a unique irreducible factor $\widetilde{\phi}$ mod π and we can lift it to $\phi \in \mathcal{O}_K[x]$. Furthermore, the ϕ-polygon of f is defined and must be one-sided. This means that f can be written as follows:

$$f \equiv \phi^{k_1} + \pi\phi^{k_2}h_1 + \pi^2 h_2 \pmod{\pi^3}$$

where $h_2 \not\equiv 0 \pmod{\pi}$ and $\phi \nmid h_2 \pmod{\pi}$. Since the ϕ-polygon must be one-sided, we get $k_2 \geq \lfloor k_1/2 \rfloor$, as desired. □

As usual, whenever the ϕ-polygon of f is (well-defined and)one-sided with degree 1, the converse holds. Even if we have already stated this in the general case (see 4.8), we remark it again:

Theorem 4.30. *Let $f \in \mathcal{O}_K[x]/(\pi^3)$ be a monic polynomial which is reducible mod π^2 and let $\phi \in \mathcal{O}_K[x]$ be a monic polynomial such that $f \equiv \phi^k \pmod{\pi}$ and ϕ is irreducible mod π. Assume that f can be expressed as*

$$f = \phi^{k_1} + \pi\phi^{k_2}h_1 + \pi^2 h_2 \pmod{\pi^3}$$

with $k_2 \geq \lfloor k_1/2 \rfloor$ and $(h_2, \phi) = 1 \pmod{\pi}$. If k_1 is odd, f is irreducible mod π^3.

With the same hypotheses of the previous theorem, assume that k_1 is even and f is reducible. The degree of the Newton polygon is 2, so we only need to consider irreducible factors of the form

$$\phi^{k_1/2} + \pi\widetilde{h}_1 + \pi^2\widetilde{h}_2 \pmod{\pi^3}$$

This follows from the theorem of the polygon: since the ϕ-polygon is one-sided of degree 2, f can have at most 2 factors and their degrees are determined by the length of their polygons. Since the degree of $N_\phi(f)$ is 2, their length is half the length of $N_\phi(f)$. Furthermore, these factors are irreducible, and therefore we can apply the criterion given above (4.29). In particular, $\phi^{\lfloor k_1/4 \rfloor} \mid \widetilde{h}_1 \pmod{\pi}$ and $\phi \nmid \widetilde{h}_2 \pmod{\pi}$.

It remains the problem of understanding when, in the case k_1 is even, f is irreducible. To study this problem more deeply, we assume additional hypotheses concerning the index of the order generated by one of the roots of f over $\mathcal{O}_K$: as we have seen when presenting Dedekind's Criterion, the index is a numerical invariant involved in the problem of factorization over $\mathcal{O}_K/(\pi^l)$.

In our setting, we can use the bound given by 4.17 to estimate the index of the order generated by a polynomial which is reducible mod π^2:

Proposition 4.31. *Let $f \in \mathcal{O}_K[x]$ be a monic irreducible polynomial and assume $f \equiv \phi^{k_1} \pmod{\pi}$, where $\phi \in \mathcal{O}_K[x]$ is an irreducible polynomial mod π of degree d. Let $M = \mathcal{O}_K[x]/(f)$, let $\mathcal{O}_L$ be its normalization and $s = \lfloor k_1/2 \rfloor$. If f is reducible over $\mathcal{O}_K/(\pi^2)$, then $q^{sd} \mid [\mathcal{O}_L : M]$, where q is the cardinality of the residue field of K.*

Proof. M can not be integrally closed by corollary 4.15 and therefore Dedekind's Criterion implies that we are in one of the following cases:

$$f \equiv \phi^{k_1} + \pi\phi^{k_2}h_1 \pmod{\pi^2} \qquad f \equiv \phi^{k_1} \pmod{\pi^2}$$

In particular, we are in the hypotheses of the corollary 4.17, so we get $q^{sd} \mid [\mathcal{O}_L : M]$, as desired. □

The additional hypothesis we want to consider in our investigation is exactly the equality of the index in the bound above. In this case, f is forced to have a particular form:

Proposition 4.32. *Let $f \in \mathcal{O}_K[x]$ be a monic irreducible polynomial and let M be the order generated by one of its roots. Assume that $f \equiv \phi^k \pmod{\pi}$, with $\phi \in \mathcal{O}_K[x]$ monic, irreducible mod π of degree d. Let $\mathcal{O}_L$ be the normalization of M and denote by q the cardinality of its residue field. If $[\mathcal{O}_L : M] = q^{\lfloor k/2 \rfloor d+1}$, then the Newton polygon of f is one-sided with ending points $(0,2)$ and $(k,0)$.*

Proof. There are only two possible forms for $f \pmod{\pi^3}$ satisfying these hypotheses:

1. $f \equiv \phi^{k_1} + \pi^2 h_2 \pmod{\pi^3}$
2. $f \equiv \phi^{k_1} + \pi\phi^{k_2} h_1 + \pi^2 h_2 \pmod{\pi^3}$, with $k_2 \geq \lfloor k_1/2 \rfloor$

We want to show that the hypotheses on the index give extra information about the term divisible by π^2; in particular, ϕ can not divide it. If this happens, ϕ^{k_1-1}/π^2 is integral over M in both cases and it contradicts the assumptions.

1. First, assume that $f = \phi^{k_1} + \pi^2\phi^{k_3} h_2 \pmod{\pi^3}$ and $(h_2, \phi) \equiv 1 \pmod{\pi}$. Consider the ideal $J = (\pi, \phi, \phi^{k_1-1}/\pi) \subseteq \mathcal{O}$, where $\mathcal{O}$ is the order obtained by adding $\phi^{k_1-1}(\alpha)/\pi$ to $\mathcal{O}_K[\alpha]$, as in Dedekind's Criterion. We shall prove that $\phi^{k_1-1}/\pi^2 \cdot J \subseteq J$. We have to test the following relations:
   - $\dfrac{\phi^{k_1-1}}{\pi^2} \cdot \pi = \dfrac{\phi^{k_1-1}}{\pi} \in J$
   - $\dfrac{\phi^{k_1-1}}{\pi^2} \cdot \phi = \dfrac{\phi^{k_1}}{\pi^2} \in J$
   - $\dfrac{\phi^{k_1-1}}{\pi^2} \cdot \dfrac{\phi^{k_1-1}}{\pi} = \dfrac{\phi^{2k_1-2}}{\pi^3} \in J$

   The first is self-evident, we have to prove the second and the third relations. As usual, we know that
   $$\phi^{k_1} + \pi^2\phi^{k_3} h_2 \equiv 0 \pmod{\pi^3, f} \tag{4.2}$$
   and so there exists $a \in \mathcal{O}$ such that $\phi^{k_1} = -\pi^2\phi^{k_3} h_2 + \pi^3 a$ in $\mathcal{O}$. As a consequence,
   $$\frac{\phi^{k_1}}{\pi^2} = -\phi^{k_3} h_2 + \pi a$$
   and the right-hand side lies in J.
   For the third relation, multiplying the equation (4.2) by ϕ^{k_1-2}, we get
   $$\phi^{2k_1-2} + \pi^2\phi^{k_3+k_1-2} h_2 + \pi^3\phi^{k_1-2} h_3 \equiv 0 \pmod{\pi^4, f}$$
   As a consequence, there exists $h_4 \in \mathcal{O}$ such that
   $$\phi^{2k_1-2} = -\pi^2\phi^{k_3+k_1-2} h_2 - \pi^3\phi^{k_1-2} h_3 + \pi^4 h_4$$
   and
   $$\frac{\phi^{2k_1-2}}{\pi^3} = -\frac{\phi^{k_3+k_1-2}}{\pi} - \phi^{k_1-2} h_3 + \pi h_4$$
   lies in J.

2. Suppose now that $f = \phi^{k_1} + \pi\phi^{k_2}h_1 + \pi^2\phi^{k_3}h_2 \pmod{\pi^3}$, where $(h_2, \phi) = 1 \pmod{\pi}$. We consider the ring $\mathcal{O}$ obtained by the addition of the element ϕ^{k_1-t}/π to M, where $t = \lfloor k_1/2 \rfloor$ (which is integral by 4.17). This time, we consider the ideal
$$J = \left(\pi, \phi, \frac{\phi^{k_1-t}}{\pi}\right)$$
and we shall show that $\phi^{k_1-1}/\pi^2 \cdot J \subseteq J$. We only check this for $\frac{\phi^{k_1-t}}{\pi}$ and ϕ, since for π is trivial. We know that
$$\phi^{k_1} + \pi\phi^{k_2}h_1 + \pi^2\phi^{k_3}h_2 \equiv 0 \pmod{\pi^3, f} \tag{4.3}$$
First, we consider the element ϕ^{k_1}/π^2; by equation (4.3), there exists $h_3 \in \mathcal{O}$ such that $\phi^{k_1} = -\pi\phi^{k_2}h_1 - \pi^2\phi^{k_3}h_2 + \pi^3 h_3$ and so
$$\frac{\phi^{k_1}}{\pi^2} = -\frac{\phi^{k_2}}{\pi}h_1 - \phi^{k_3}h_2 + \pi h_3$$
and the right-hand side lies in J since $k_2 \geq k_1 - t$.
Now, we want to show that ϕ^{2k_1-t-1}/π^3 lies in J. Multiplying the equation (4.3) by ϕ^{k_1-t-1} we get
$$\phi^{2k_1-t-1} + \pi\phi^{k_2+k_1-t-1}h_1 + \pi^2\phi^{k_3+k_1-t-1}h_2 + \pi^3\widetilde{h}_3 \equiv 0 \pmod{(\pi^4, f)}$$
where $\phi \mid \widetilde{h}_3$. This means that there exists $h_4 \in \mathcal{O}$ such that
$$\phi^{2k_1-t-1} = -\pi\phi^{k_2+k_1-t-1}h_1 - \pi^2\phi^{k_3+k_1-t-1}h_2 - \pi^3\widetilde{h}_3 + \pi^4 h_4$$
As a consequence,
$$\frac{\phi^{2k_1-t-1}}{\pi^3} = -\frac{\phi^{k_2+k_1-t-1}}{\pi^2}h_1 - \frac{\phi^{k_3+k_1-t-1}}{\pi}h_2 - \widetilde{h}_3 + \pi h_4$$
We notice that $-\frac{\phi^{k_3+k_1-t-1}}{\pi}h_2 - \widetilde{h}_3 + \pi h_4 \in J$ since $k_3 + k_1 - t - 1 \geq k_1 - t$. We only have to prove that $\phi^{k_2+k_1-t-1}/\pi^2 \in J$. By the properties of Newton Polygons, k_2 must be strictly greater than $\lfloor k_1/2 \rfloor$; if it is not the case, f splits over $\mathcal{O}_K$ since the ϕ-polygon has two sides of different slopes, contradicting the hypothesis of irreducibility. Therefore $k_2 + k_1 - t - 1 \geq k_1$ and by (4.3), there exists $b \in \mathcal{O}$ such that
$$\frac{\phi^{k_2+k_1-t-1}}{\pi^2} = -\frac{\phi^{2k_2-t-1}}{\pi}h_1 - \phi^{k_2-t-1+k_3}h_2 + \pi b$$
as desired.

□

Applying the results given so far in this section, we discover an interesting criterion:

Theorem 4.33. *Let $f \in \mathcal{O}_K[x]$ be a monic irreducible polynomial such that $f = \phi^k \pmod{\pi}$ where $\phi \in \mathcal{O}_K[x]$ is a monic polynomial irreducible mod π of degree d. Let $\alpha \in \overline{\mathbb{Q}}_p$ be a root of f and let $\mathcal{O}_L$ be the integral closure of $\mathcal{O}_K[\alpha]$. Let q be the cardinality of the residue field of $\mathcal{O}_L$. If k is odd and*
$$[\mathcal{O}_L : \mathcal{O}_K[\alpha]] = q^{\lfloor k/2 \rfloor d}$$
then f is irreducible mod π^3.

Proof. The hypotheses imply that the Newton polygon of f over $\mathcal{O}_K/(\pi^3)$ is one-sided and its side has degree 1, hence f is irreducible. □

The interesting aspect of this theorem is the fact that we do not assume anything about the shape of the reduced ϕ-development of f (except the requirement for k).

Unfortunately, the techniques used above have been ineffective in the case when k is even. The last tool we can use is the formula developed in the third section.

Let K be a p-adic field and let q be the cardinality of its residue field. Assume that $f \in \mathcal{O}_K[x]$ is an irreducible monic polynomial of degree n such that

$$f(x) = \phi(x)^{k_1} + \pi\phi(x)^{k_2}h_1(x) + \pi^2 h_2(x) \pmod{\pi^3}$$

with $(h_2, \phi) \equiv 1 \pmod{\pi}$, k_1 is even and $k_2 \geq k_1/2$. Furthermore, suppose that $[\mathcal{O}_L : M] = q^{n/2}$, where M is the order generated by a root of f and $\mathcal{O}_L$ is its integral closure.

We apply the formula using the invariants of the field extension generated by a root of f.

If $\deg \phi = 1$, we can assume up to a translation that $\phi = x$ and we can apply the formula 4.20: then f is irreducible over $\mathcal{O}_K/(\pi^l)$ for all $l \in \mathbb{N}$ such that

$$\begin{aligned} l &> v(\mathrm{disc}(f)) - 2(n-2) \\ &= n + v(\mathrm{disc}(\mathcal{O}_L/\mathcal{O}_K)) - 2(n-2) \\ &= 4 - n + v(\mathrm{disc}(\mathcal{O}_L/\mathcal{O}_K)) \end{aligned}$$

In order to understand the valuation of the discriminant, we use proposition 1.33. Assume first that L is tamely ramified over K. Then, if $\mathcal{D}_{L/K} = (\pi^s)$,

$$v(\mathrm{disc}(\mathcal{O}_L/\mathcal{O}_K)) = \frac{sn}{e} = \frac{(e-1)n}{e}$$

where $e = e(L \mid K)$. By the theory about the Newton polygons (2.24), we know that e can have only two possible values: n or $n/2$. If $e = n$, then $\mathrm{disc}(\mathcal{O}_L/\mathcal{O}_K) = n - 1$ and the inequality becomes $l > 3$, proving in particular the irreducibility of such a polynomial over $\mathcal{O}_K/(\pi^4)$.

If $e \neq n$, necessarily $e = n/2$ and $\mathrm{disc}(\mathcal{O}_L/\mathcal{O}_K) = n - 2$, so that f is irreducible over $\mathcal{O}_K/(\pi^3)$.

If L is wildly ramified, the bound gets worse and we can not really say anything about it, since it depends too much on the valuation of n.

Now, we apply the same method when $\deg(\phi) = d \geq 2$, applying the formula given by 4.28. Since

$$v(\mathrm{disc}(f)) = n + \frac{(e-1)n}{e}$$

we get

$$\begin{aligned} l &> \frac{v(\mathrm{disc}(f))}{d} - 2(k_1 - 2) \\ &= k_1 + \frac{(e-1)k_1}{e} - 2(k_1 - 2) \\ &= 4 - k_1 + \frac{(e-1)k_1}{e} \end{aligned}$$

By the theory on Newton Polygon, we know that the ramification index of the extension can be k_1 or $k_1/2$ (corollary 2.24). Therefore, if $e = k_1/2$, $l > 2$, while if $e = k_1$ we obtain $l > 3$, as in the previous case. Summarizing,

Theorem 4.34. *Let $f \in \mathcal{O}_K[x]$ be a monic irreducible polynomial of degree n such that $f = \phi^k \pmod{\pi}$, where $\phi \in \mathcal{O}_K[x]$ is monic of degree d and irreducible mod π. Let $\alpha \in \overline{\mathbb{Q}}_p$ be a root of f and let $\mathcal{O}_L$ be the integral closure of $\mathcal{O}_K[\alpha]$. Assume that k is even and*

$$q^{\frac{n}{2}} = [\mathcal{O}_L : \mathcal{O}_K[\alpha]]$$

where q is the cardinality of the residue field of K. If the extension L/K is tamely ramified, then

- *if $e(L|K) = k$, f is irreducible mod π^4.*
- *if $e(L|K) = \frac{k}{2}$, f is irreducible mod π^3.*

4.5 Conclusions

Summarizing the results of this chapter, we have seen that it is possible to extend the theory of Newton polygons to our setting. Unfortunately, they are not as effective as in the case of a ring of integers of a p-adic field but they can provide an algorithm to test whether a polynomial is reducible or not over $\mathcal{O}_K/(\pi^l)$. In particular, Newton polygons give a more theoretical approach to the proof of the irreducibility criterion mod π^2. Another proof of the same criterion is an immediate corollary of Dedekind's criterion and this proof suggests a relation between normality and irreducibility. With the same techniques, we have obtained an estimation of the index of the order generated by the root of an irreducible polynomial in its integral closure and we have established some results that link the index with irreducibility. This work has produced a formula that upper bounds the maximum $l \in \mathbb{N}$ such that a polynomial f is irreducible mod π^l.

We have given some improvements over existing techniques, even though the problem of finding all the factorizations of a polynomial mod π^l is far from being solved effectively and the same is true for a complete irreducibility test. Further work can be done in this direction: indeed, the formula given in section 4.3 can certainly be improved. In particular, it would be interesting to find a more precise formula because this would yield a deeper understanding of p-adic factorization. From a theoretical point of view, the relation between the index and irreducibility mod π^l can be strengthened, We have only focused on the factorization mod π^3 but this approach can give a deeper comprehension of these phenomena. The search for all the possible factorizations is a harder problem. Indeed, as we have seen in some examples, p-adic factorization can be insufficient for this purpose and this means that the only possible approach is trying to lift the factorizations mod π to all the factorizations mod π^l. Future work should be directed toward understanding which factorizations lift and which do not.

Bibliography

[1] A. M. Andrew. Another Efficient Algorithm for Convex Hulls in Two Dimensions. *Info. Proc. Letters 9*, pages 216–219, 1979.

[2] M.F. Atiyah and I.G. MacDonald. *Introduction to commutative algebra.* 1969.

[3] Z.I. Borevich and I.R. Shafarevich. *Number Theory.* Academic Press, 1966.

[4] S. Bosch. *Algebra.* Springer, 2003.

[5] D. G. Cantor and D. M. Gordon. Factoring Polynomials over p-adic fields. *Proceedings of ANTS IV*, pages 185–208, 2000.

[6] H. Cheng and G. Labahn. Computing all factorizations in $\mathbb{Z}_N[x]$. *Proceedings of the 2001 International Symposium on Symbolic and Algebraic Computation*, pages 64–71, 2001.

[7] H. Cohen. *A Course in Computational Number Theory.* Springer-Verlag, 1993.

[8] H. Cohen. *Advanced Topics in Computational Number Theory.* Springer-Verlag, 1999.

[9] D. Ford, S. Pauli, and X. Roblot. A fast algorithm for polynomial factorization over $\mathbb{Q}_p$. *Journal de Théorie des Nombres de Bordeaux*, 14:151–169, 2002.

[10] J. Von Zur Gathen and S. Hartlieb. Factoring Modular Polynomials. *Proceedings of the 1996 International Symposium on Symbolic and Algebraic Computation*, 1996.

[11] J. Von Zur Gathen and S. Hartlieb. Factorization of polynomials modulo small prime powers. 1996.

[12] J. Guardia, J. Montes, and E. Nart. Newton polygons of higher order in algebraic number theory. *Transaction of the American Mathematical Society*, 364(1):361–416, 2012.

[13] S. Lang. *Algebra.* Springer, 2005.

[14] D.A. Marcus. *Number Fields.* Springer, 1995.

[15] B. R. McDonald. *Finite Rings with Identity.* Marcel Dekker Incorporated, 1974.

[16] J. Montes and E. Nart. On a Theorem of Øre. *Journal of Algebra*, 146:318–334, 1992.

[17] J. Neukirch. *Algebraic Number Theory*. Springer-Verlag, 1992.

[18] Ö. Ore. Newtonsche polygone in der theorie der algebraischen körper. *Mathematische Annalen*, 99:84–117, 1928.

[19] S. Pauli. Factoring Polynomials Over Local Fields. *Journal of Symbolic Computation*, 32:533–547, 2001.

[20] S. Pauli. Factoring Polynomials Over Local Fields II. *Algorithmic Number Theory*, pages 301–315, 2010.

[21] A. Salagean. Factoring polynomials over $\mathbb{Z}_4$ and over Certain Galois Rings. *Finite Fields and Their Application*, 11:56–70, 2005.

[22] A. Shamir. On the generation of polynomials which are hard to factor. *Proceedings of the 25th Annual ACM Symposium on the Theory of Computing*, pages 796–804, 1993.

[23] S.Lang. *Algebraic Number Theory*. Springer-Verlag, 2000.