Article Submitted to Journal of Symbolic Computation

Factoring Polynomials over Local Fields

Sebastian Pauli

Department of Mathematics, Concordia University, 1455 de Maisonneuve Blvd. W., Montréal, Québec H3G 1M8, Canada

Abstract

We describe an efficient new algorithm for factoring a polynomial $\Phi(x)$ over a field $\mathbf{k}$ that is complete with respect to a discrete prime divisor. For every irreducible factor $\varphi(x)$ of $\Phi(x)$ this algorithm returns an integral basis for $\mathbf{k}[x]/\varphi(x)\mathbf{k}[x]$ over $\mathbf{k}$.

1. Introduction

Much attention has been given lately to the factorization of polynomials over local fields. This problem is closely related to the computation of integral bases of local and global fields and can be applied to the factorization of ideals in global fields. Several polynomial factorization algorithms have been published:

- The Round Four algorithm of Zassenhaus (Ford, 1978, 1987; Ford and Letard, 1994) was originally conceived as an algorithm for the computation of integral bases of algebraic number fields and is fast in most cases. In some cases however a branch of the algorithm with exponential complexity is needed.
- Chistov (1990) proved the existence of a polynomial-time algorithm for factoring polynomials over local fields.
- The algorithm for factoring ideals of Buchmann and Lenstra described by Cohen (1993, section 6.2) can be used for factoring polynomials over a local field in polynomial time. Its main disadvantage is that it needs an integral basis as an input.
- The algorithm by Montes (1999) is formulated as an algorithm for the decomposition of ideals over number fields and is based on ideas of Ore (1928). He does not provide a complexity analysis.
- The improved Round Four algorithm by Ford, Pauli, and Roblot (2000) is considerably faster than the original Round Four algorithm. Formulated as

an algorithm for factoring a polynomial $\Phi(x)$ over $\mathbb{Q}_p$, it returns a local integral basis (in fact, a power basis) for $\mathbb{Q}_p[x]/\varphi(x)\mathbb{Q}_p[x]$ for each irreducible factor $\varphi(x)$ of $\Phi(x)$. The algorithm terminates in polynomial time.

- Cantor and Gordon (2000) have developed an algorithm for deriving an irreducible factor of a polynomial $\Phi(x) \in \mathbf{k}[x]$ of degree N over an extension $\mathbf{k}$ of degree k over $\mathbb{Q}_p$. In their talk at the fourth Algorithmic Number Theory Symposium in July 2000 they announced that they had reduced the expected number of bit operations to $O\big(N^{4+\varepsilon} v_\mathfrak{p}(\operatorname{disc}\Phi)^{2+\varepsilon} \log^{1+\varepsilon} p^k\big)$.

The algorithm presented here has its origins in the Round Four algorithm. It returns all irreducible factors $\varphi(x)$ of a polynomial $\Phi(x)$ over the valuation ring of a local field $\mathbf{k}$ together with an integral basis for $\mathbf{k}[x]/\varphi(x)\mathbf{k}[x]$. If $\mathbf{k}$ is a finite extension of $\mathbb{Q}_p$ of degree k, our algorithm derives a complete factorization of a polynomial $\Phi(x)$ of degree N with the expected number of bit operations being

$$O\big(N^{3+\varepsilon} v_\mathfrak{p}(\operatorname{disc}\Phi)^{1+\varepsilon} \log^{1+\varepsilon} p^k + N^{2+\varepsilon} v_\mathfrak{p}(\operatorname{disc}\Phi)^{2+\varepsilon} \log^{1+\varepsilon} p^k\big).$$

The following notations are used throughout this paper. Let $\mathbf{k}$ be a local field, that is, a field complete with respect to a discrete prime divisor $\mathfrak{p}$ (see Weiss (1963)). Let $\mathcal{O}_\mathbf{k}$ be the valuation ring of $\mathbf{k}$ and let π be a prime element of $\mathfrak{p}$. Denote the non-archimidean valuation on $\mathbf{k}$ by $|\cdot|$ and let $v_\mathfrak{p}$ denote the exponential valuation on $\mathbf{k}$ with $v_\mathfrak{p}(\pi) = 1$. Let $\underline{\mathbf{k}} := \mathcal{O}_\mathbf{k}/\mathfrak{p}$ be the residue class field of $\mathbf{k}$. For $\gamma \in \mathbf{k}$ denote by $\underline{\gamma}$ the class $\gamma + \mathfrak{p}$ in $\underline{\mathbf{k}}$. Let $\overline{\mathbf{k}}$ be an algebraic closure of $\mathbf{k}$. The unique extensions of $|\cdot|$ and $v_\mathfrak{p}$ to $\overline{\mathbf{k}}$ or any intermediate field $\widehat{\mathbf{k}}$ will also be denoted by $|\cdot|$ and $v_\mathfrak{p}$, respectively.

Let $\Phi(x)$ be a monic, separable, and squarefree polynomial of degree N in $\mathcal{O}_\mathbf{k}[x]$. In order to find a proper factorization of $\Phi(x)$ or to prove its irreducibility, we construct a polynomial $\varphi(x) \in \mathbf{k}[x]$ with $\deg\varphi$ less than or equal to the degree of every irreducible factor of $\Phi(x)$. The polynomial $\varphi(x)$ is iteratively modified such that $|\varphi(\xi)|$ decreases strictly for all roots $\xi \in \overline{\mathbf{k}}$ of $\Phi(x)$. In section 2 we describe how a proper factorization of $\Phi(x)$ can be derived if $|\varphi(\xi_i)| \neq |\varphi(\xi_j)|$ for some roots ξ_i and ξ_j of $\Phi(x)$. In section 3 we describe how an integral basis of $\mathbf{k}[x]/\Phi(x)\mathbf{k}[x]$ over $\mathbf{k}$ can be obtained from the data computed in the algorithm. In section 4 we show that $\Phi(x)$ is irreducible if $|\varphi(\xi)|^N < |\operatorname{disc}\Phi|^2$ for some root ξ of $\Phi(x)$. In section 5 we present an algorithm that returns a proper factorization of $\Phi(x)$ over $\mathcal{O}_\mathbf{k}$ if one exists or an integral basis of $\mathbf{k}[x]/\Phi(x)\mathbf{k}[x]$ over $\mathbf{k}$ otherwise. This algorithm is illustrated by two examples in section 6. In section 7 we analyse the complexity of the algorithm.

2. Reducibility

Definition 2.1: Let $\Phi(x) = \prod_{j=1}^N (x - \xi_j) \in \mathcal{O}_\mathbf{k}[x]$. For $\vartheta(x) \in \mathbf{k}[x]$ we define

$$\chi_\vartheta(t) := \prod_{i=1}^N (t - \vartheta(\xi_i)) = \operatorname{res}_x(\Phi(x), t - \vartheta(x)).$$

DEFINITION 2.2: Let $\vartheta(x) \in \mathbf{k}[x]$ with $\chi_\vartheta(t) = t^N + c_1 t^{N-1} + \cdots + c_N \in \mathcal{O}_\mathbf{k}[t]$. We say $\vartheta(x)$ passes the Hensel test if $\underline{\chi}_\vartheta(t) = \underline{\nu}_\vartheta(t)^s$ for some $s \geqslant 1$, where $\underline{\nu}_\vartheta(t)$ is monic and irreducible in $\underline{\mathbf{k}}[t]$.

Furthermore we define $v_\mathfrak{p}^*(\vartheta) := \min\limits_{1 \leqslant i \leqslant N} \dfrac{v_\mathfrak{p}(c_i)}{i}$.

We say the polynomial $\vartheta(x)$ passes the Newton test if $\dfrac{v_\mathfrak{p}(c_N)}{N} = v_\mathfrak{p}^*(\vartheta)$.

Note that we have $v_\mathfrak{p}(\vartheta(\xi_1)) = \cdots = v_\mathfrak{p}(\vartheta(\xi_N)) = v_\mathfrak{p}(c_N)/N$ if $\vartheta(x)$ passes the Newton test.

PROPOSITION 2.3: *Let $\gamma(x) \in \mathbf{k}[x]$ with $\chi_\gamma(t) \in \mathcal{O}_\mathbf{k}[t]$. If $\gamma(x)$ fails the Hensel test then $\Phi(x)$ is reducible in $\mathcal{O}_\mathbf{k}[x]$.*

Proof: As $\gamma(x)$ fails the Hensel test, $\underline{\chi}_\gamma(t)$ has at least two irreducible factors. Hensel's lemma gives relatively prime monic polynomials $\chi_1(t)$ and $\chi_2(t)$ in $\mathcal{O}_\mathbf{k}[t]$ with $\chi_1(t)\chi_2(t) = \chi_\gamma(t)$. Reordering the roots of $\Phi(x)$ if necessary, we may write

$$\chi_1(t) = (t - \gamma(\xi_1)) \cdots (t - \gamma(\xi_r)) \text{ and } \chi_2(t) = (t - \gamma(\xi_{r+1})) \cdots (t - \gamma(\xi_N)),$$

where $1 \leqslant r < N$. It follows that

$$\Phi(x) = \gcd(\Phi(x), \chi_1(\gamma(x))) \cdot \gcd(\Phi(x), \chi_2(\gamma(x)))$$

is a proper factorization of $\Phi(x)$. $\square$

COROLLARY 2.4: *Let $\vartheta(x) \in \mathbf{k}[x]$ with $\chi_\vartheta(t) = t^N + c_1 t^{N-1} + \cdots + c_N \in \mathcal{O}_\mathbf{k}[t]$. If $\vartheta(x)$ fails the Newton test then $\Phi(x)$ is reducible in $\mathcal{O}_\mathbf{k}[x]$.*

Proof: If $\vartheta(x)$ fails the Newton test we have $v_\mathfrak{p}^*(\vartheta) = r/s < v_\mathfrak{p}(c_N)/N$. Setting $\gamma := \vartheta^s/\pi^r$ we get

$$\min\{v_\mathfrak{p}(\gamma(\xi_1)), \ldots, v_\mathfrak{p}(\gamma(\xi_N))\} = 0 < \max\{v_\mathfrak{p}(\gamma(\xi_1)), \ldots, v_\mathfrak{p}(\gamma(\xi_N))\}.$$

Consequently $\gamma(x)$ fails the Hensel test and it follows from proposition 2.3 that $\Phi(x)$ is reducible. $\square$

In general it is not possible to compute exactly the greatest common divisor of two polynomials over a local field. The following result from Ford and Letard (1994) (also see Ford, Pauli, and Roblot (2000)) provides a method for approximating the greatest common divisor to a given precision.

For two polynomials $\Psi(x) = b_0 x^M + \cdots + b_M$ and $\Phi(x) = c_0 x^N + \cdots + c_N$ we call the $(M+N) \times (M+N)$-matrix

$$\begin{pmatrix} b_0 & \cdots & b_M & & 0 \\ & \ddots & & \ddots & \\ 0 & & b_0 & \cdots & b_M \\ c_0 & \cdots & c_N & & 0 \\ & \ddots & & \ddots & \\ 0 & & c_0 & \cdots & c_N \end{pmatrix}$$

the Sylvester matrix of $\Psi(x)$ and $\Phi(x)$.

Proposition 2.5 (Ford): *Let $\Phi(x) \in \mathcal{O}_{\mathbf{k}}[x]$ be monic. Let relatively prime polynomials $\Psi_1(x)$ and $\Psi_2(x)$ in $\mathcal{O}_{\mathbf{k}}[x]$ and $r_0 \in \mathbb{N}$ be given, such that*

$$\Phi(x) \mid \Psi_1(x)\Psi_2(x) \quad \textit{and} \quad \mathfrak{p}^{r_0} = \big(\Psi_1(x)\mathcal{O}_{\mathbf{k}}[x] + \Psi_2(x)\mathcal{O}_{\mathbf{k}}[x]\big) \cap \mathcal{O}_{\mathbf{k}}.$$

Choose $m \in \mathbb{N}$, $m > r_0$. For $j = 1, 2$ let S_{Φ,Ψ_j} be the Sylvester matrix of $\Phi(x)$ and $\Psi_j(x)$. Let $\pi^{r_j}\Phi_j(x)$ with $\Phi_j(x)$ monic, $r_j \in \mathbb{N}$ be the polynomial given by the last non-zero row of the matrix obtained by row reduction of S_{Φ,Ψ_j} modulo $\mathfrak{p}^m$. Then

$$\Phi_j(x) \equiv \gcd\big(\Phi(x), \Psi_j(x)\big) \bmod \mathfrak{p}^{m-r_0}.$$

Remark 2.6: In the construction of $\Phi_1(x)$ and $\Phi_2(x)$ it is sufficient to have approximations to $\Phi(x)$, $\Psi_1(x)$, and $\Psi_2(x)$ that are correct modulo $\mathfrak{p}^m$.

Remark 2.7: Let $\gamma(x) \in \mathbf{k}[x]$ such that $\chi_1(t)\chi_2(t) = \chi_\gamma(t) \in \mathcal{O}_{\mathbf{k}}[t]$ where $\gcd(\underline{\chi}_1(t), \underline{\chi}_2(t)) = 1$. There exist $\alpha_1(t), \alpha_2(t) \in \mathcal{O}_{\mathbf{k}}[t]$ with

$$\underline{\alpha}_1(t)\underline{\chi}_1(t) + \underline{\alpha}_2(t)\underline{\chi}_2(t) = 1.$$

Because the index of $\mathbf{k}[x]/\Phi(x)\mathbf{k}[x]$ in its maximal order is at most $\mathfrak{p}^d$, where $d = \lfloor v_{\mathfrak{p}}(\operatorname{disc}\Phi)/2 \rfloor$, and

$$\pi^d\alpha_1(\gamma(x))\pi^d\chi_1(\gamma(x)) + \pi^d\alpha_2(\gamma(x))\pi^d\chi_2(\gamma(x)) \equiv \pi^{2d} \bmod \mathfrak{p}^{2d+1},$$

it follows that $r_0 \leqslant 2d \leqslant v_{\mathfrak{p}}(\operatorname{disc}\Phi)$.

Both criteria for finding a proper factorization of $\Phi(x)$ need a factorization of the polynomial over the residue class field before Hensel lifting can be applied. If the residue class field $\underline{\mathbf{k}}$ is finite we can use the algorithms of Berlekamp (1970), Cantor and Zassenhaus (1970), or one of the many improvements of these algorithms, Kaltofen and Shoup (1998) for example. If $\mathbf{k}$ is the completion of a function field over a number field then polynomials over $\underline{\mathbf{k}}$ can be factored using the algorithms for factoring polynomials over number fields by Trager (1976), Pohst (1999), Roblot (2000), or Fieker and Friedrichs (2000).

We will see that it is convenient to factor the polynomial $\Phi(x)$ over an unramified extension $\widehat{\mathbf{k}}$ of $\mathbf{k}$. Then the norm of the factors of $\Phi(x)$ over $\widehat{\mathbf{k}}$ can be used to derive a factorization of $\Phi(x)$ over $\mathbf{k}$. For more on the norm of a polynomial see Pohst and Zassenhaus (1989, section 5.4).

Definition 2.8: Let $\widehat{\mathbf{k}}[x]$ be an algebraic extension of $\mathbf{k}$ of degree n. Let $\vartheta(x) \in \widehat{\mathbf{k}}[x]$ and $\vartheta^{(j)}(x) \in \widehat{\mathbf{k}}^{(j)}[x]$ $(1 \leqslant j \leqslant n)$ be the corresponding polynomials over the conjugate fields obtained by applying conjugation to the coefficients of $\vartheta(x)$ only. Then the norm of $\vartheta(x)$ is defined by $\mathrm{N}_{\widehat{\mathbf{k}}/\mathbf{k}}(\vartheta) := \prod_{j=1}^{n} \vartheta^{(j)}(x)$.

REMARK 2.9: Note that $\mathrm{N}_{\widehat{\mathbf{k}}/\mathbf{k}}(\vartheta(x)) \in \mathbf{k}[x]$ and that

$$\mathrm{N}_{\widehat{\mathbf{k}}/\mathbf{k}}(\vartheta_1(x)\vartheta_2(x)) = \mathrm{N}_{\widehat{\mathbf{k}}/\mathbf{k}}(\vartheta_1(x))\mathrm{N}_{\widehat{\mathbf{k}}/\mathbf{k}}(\vartheta_2(x))$$

for all $\vartheta_1(x)$, $\vartheta_2(x) \in \widehat{\mathbf{k}}[x]$.

REMARK 2.10: Let $\nu(t) \in \mathcal{O}_{\mathbf{k}}[t]$ be irreducible and let $\widehat{\mathbf{k}} := \mathcal{O}_{\mathbf{k}}[t]/\nu(t)\mathcal{O}_{\mathbf{k}}[t]$. Let $\varphi(x) = \sum_{i=0}^{n} c_i(t)x^n$ be a polynomial in $\mathbf{k}[x]$. Denote by C_i a lift of c_i from $\mathcal{O}_{\mathbf{k}}[t]/\nu(t)\mathcal{O}_{\mathbf{k}}[t]$ to $\mathcal{O}_{\mathbf{k}}[t]$. Then $\mathrm{N}_{\widehat{\mathbf{k}}/\mathbf{k}}(\varphi(x)) = \mathrm{res}_t\big(\nu(t), \sum_{i=0}^{n} C_i(t)x^n\big)$.

3. Two Element Certificates and Integral Bases

For a polynomial $\vartheta(x) \in \mathbf{k}[x]$ the values E_ϑ and F_ϑ defined below give a lower bound for the ramification indices and the inertia degrees of the extensions $\mathbf{k}(\xi)$ for all roots ξ of $\Phi(x)$.

DEFINITION 3.1: Let $\vartheta(x) \in \mathbf{k}[x]$, with $\chi_\vartheta(t) \in \mathcal{O}_{\mathbf{k}}[t]$, such that $\vartheta(x)$ passes the Hensel and Newton tests. We define $\nu_\vartheta(t)$ to be an arbitrary monic polynomial in $\mathcal{O}_{\mathbf{k}}[t]$, with $\underline{\nu}_\vartheta(t)$ irreducible in $\underline{\mathbf{k}}[t]$, such that $\underline{\chi}_\vartheta(t) = \underline{\nu}_\vartheta(t)^s$ for some $s \geqslant 1$. We set $F_\vartheta := \deg \underline{\nu}_\vartheta$. Furthermore we define G_ϑ and E_ϑ to be the unique relatively prime integers with $G_\vartheta/E_\vartheta = v_{\mathfrak{p}}^*(\vartheta)$.

DEFINITION 3.2: Let $\Phi(x)$ be a monic polynomial in $\mathcal{O}_{\mathbf{k}}[x]$. A two-element certificate for $\Phi(x)$ is a pair $(\Gamma(x), \Pi(x))$ with $\Gamma(x) \in \mathbf{k}[x]$ and $\Pi(x) \in \mathbf{k}[x]$ such that $\chi_\Gamma(t) \in \mathcal{O}_{\mathbf{k}}[t]$, $\chi_\Pi(t) \in \mathcal{O}_{\mathbf{k}}[t]$, and $F_\Gamma E_\Pi = \deg \Phi$.

REMARK 3.3: If a two-element certificate exists then $\Phi(x)$ is irreducible and an integral basis of the extension of $\mathbf{k}$ generated by a root ξ of $\Phi(x)$ is given by the elements $\Gamma(\xi)^i\Pi(\xi)^j$ with $0 \leqslant i \leqslant F_\Gamma - 1$ and $0 \leqslant j \leqslant E_\Pi - 1$.

Let $\Phi(x) \in \mathcal{O}_{\mathbf{k}}[x]$ be irreducible and let E be the ramification index and F the inertia degree of $\mathbf{k}[x]/\Phi(x)\mathbf{k}[x]$. Set $\widehat{\mathbf{k}}_0 := \mathbf{k}$. Assume we are given a tower of unramified extensions

$$\begin{array}{rcl}
\widehat{\mathbf{k}}_r & := & \widehat{\mathbf{k}}_{r-1}[t_r]/\nu_{\gamma_{r-1}}\widehat{\mathbf{k}}_{r-1}[t_r] \\
& \vdots & \\
\widehat{\mathbf{k}}_2 & := & \widehat{\mathbf{k}}_1[t_2]/\nu_{\gamma_1}(t_2)\widehat{\mathbf{k}}_1[t_2] \\
\widehat{\mathbf{k}}_1 & := & \widehat{\mathbf{k}}_0[t_1]/\nu_{\gamma_0}(t_1)\widehat{\mathbf{k}}_0[t_1] \\
\widehat{\mathbf{k}}_0 & := & \mathbf{k}
\end{array}$$

with $\gamma_i(x) \in \widehat{\mathbf{k}}_i[x]$, such that $\widehat{\mathbf{k}}_r$ is isomorphic to the inertia field of $\mathbf{k}[x]/\Phi(x)\mathbf{k}[x]$. Denote by $\widetilde{\gamma}_i(x)$ a lift of $\gamma_i(x)$ to $\mathbf{k}[t_1, \ldots, t_i][x]$ and by ξ a root of $\Phi(x)$. Define a sequence $\delta_i(x) \in \mathbf{k}[x]$ by $\delta_0(x) := \widetilde{\gamma}_0(x)$ and $\delta_i(x) := \widetilde{\gamma}\big(\delta_0(x), \ldots, \delta_{i-1}(x)\big)(x)$ for $1 \leqslant i \leqslant r$. Then the inertia field of $\mathbf{k}(\delta_0(\xi), \ldots, \delta_i(\xi))$ is isomorphic to $\widehat{\mathbf{k}}_i$.

Let $\Gamma(x) \in \mathbf{k}[x]$ be such that $\underline{\Gamma(\xi)}$ is a primitive element of $\widehat{\underline{\mathbf{k}}}_r$ over $\underline{\mathbf{k}}$. Then $F_\Gamma = F$. Assume that a polynomial $\psi(x) \in \widehat{\mathbf{k}}_r[x]$ with $\chi_\psi(t) \in \mathcal{O}_{\widehat{\mathbf{k}}_r}[t]$ and $v_{\mathfrak{p}}^*(\psi) = 1/E$ is known. Denote by $\widetilde{\psi}(x)$ a lift of $\psi(x)$ to $\mathbf{k}[t_1, \ldots, t_i][x]$ and set

$$\Pi(x) = \widetilde{\psi}\big(\delta_0(x), \ldots, \delta_r(x)\big)(x).$$

Then $(\Gamma(x), \Pi(x))$ is a two-element certificate for $\Phi(x)$.

If the residue class field $\underline{\mathbf{k}}$ of $\mathbf{k}$ is finite the following lemma can be used to find a primitive element of $\widehat{\underline{\mathbf{k}}}_r$.

Lemma 3.4: *Let $\mathbb{F}_q$ be the finite field with q elements. Let $\underline{\beta}$ and $\underline{\gamma}$ be elements of an algebraic closure of $\mathbb{F}_q$. Let $F_\beta := [\mathbb{F}_q(\underline{\beta}) : \mathbb{F}_q]$, $F_\gamma := [\mathbb{F}_q(\underline{\gamma}) : \mathbb{F}_q]$ and $F := \operatorname{lcm}(F_\beta, F_\gamma)$. Let $\underline{\delta} \in \mathbb{F}_q(\underline{\beta}, \underline{\gamma})$ be randomly chosen. Then the probability that $\mathbb{F}_q(\underline{\delta}) = \mathbb{F}_q(\underline{\beta}, \underline{\gamma})$ is at least $1/2$.*

Proof: The number of elements of $\mathbb{F}_{q^F}$ generating a proper subfield of $\mathbb{F}_{q^F}$ is at most

$$\sum_{\substack{l \text{ prime} \\ l<F,\, l|F}} q^{F/l} \leqslant (\log_2 F) q^{F/2}.$$

Therefore the probability that a randomly chosen element of $\mathbb{F}_{q^F}$ belongs to a proper subfield of $\mathbb{F}_{q^F}$ is at most

$$\frac{(\log_2 F)q^{F/2}}{q^F} = \frac{\log_2 F}{q^{F/2}} \leqslant \frac{\log_2 F}{2^{F/2}} \leqslant \frac{1}{2}. \qquad \square$$

For the case that $\mathbf{k}$ is the completion of a function field over a number field, the residue class field $\underline{\mathbf{k}}$ is a number field. Cohen (1999, section 2.1) presents an algorithm for computing a primitive element of the compositum of two number fields.

4. Irreducibility

The following proposition gives an upper bound for the number of steps needed in our algorithm either to derive a proper factorization of $\Phi(x)$ or to produce a two-element certificate that Φ is irreducible.

Proposition 4.1: *Let $\xi_1, \ldots, \xi_N$, $\alpha_1, \ldots, \alpha_n$ be elements of an algebraic closure of $\mathbf{k}$ and assume the following hypotheses hold.*

- $\Phi(x) = \prod_{j=1}^N (x - \xi_j)$ *is a squarefree polynomial in* $\mathcal{O}_{\mathbf{k}}[x]$.
- $\varphi(x) = \prod_{i=1}^n (x - \alpha_i) \in \mathbf{k}[x]$.
- $|\varphi(\xi_j)|^N < |\operatorname{disc} \Phi|^2$ *for* $1 \leqslant j \leqslant N$.
- *The degree of any irreducible factor of $\Phi(x)$ is greater than or equal to n.*

Then $N = n$ and $\Phi(x)$ is irreducible over $\mathbf{k}$.

For the proof of this proposition we need a few lemmas.

LEMMA 4.2: *Let* $\Phi(x)=\prod_{j=1}^{N}(x-\xi_j)\in\mathbf{k}[x]$. *Let* α *be an element of the algebraic closure of* $\mathbf{k}$ *and assume that* $\widetilde{\xi}$ *is chosen among the roots of* $\Phi(x)$ *such that* $|\alpha-\widetilde{\xi}|$ *is minimal. Then*

$$|\Phi(\alpha)|=\prod_{i=1}^{N}\max\{|\alpha-\widetilde{\xi}|,\,|\widetilde{\xi}-\xi_i|\}.$$

Proof: We have $|\Phi(\alpha)|=\prod_{i=1}^{N}|\alpha-\xi_i|$ and $|\alpha-\xi_i|=|\alpha-\widetilde{\xi}+\widetilde{\xi}-\xi_i|\leqslant\max\{|\alpha-\widetilde{\xi}|,\,|\widetilde{\xi}-\xi_i|\}$. If $|\alpha-\widetilde{\xi}|<|\widetilde{\xi}-\xi_i|$ then $|\alpha-\xi_i|=|\widetilde{\xi}-\xi_i|$, and if $|\alpha-\widetilde{\xi}|\geqslant|\widetilde{\xi}-\xi_i|$ then $|\alpha-\xi_i|=|\widetilde{\xi}-\alpha|$. □

LEMMA 4.3: *Assume the hypotheses of proposition 4.1 hold. Then* $\varphi(x)\in\mathcal{O}_{\mathbf{k}}[x]$ *and* $\varphi(x)$ *is irreducible over* $\mathbf{k}$. *Furthermore there exist a root* ξ *of* $\Phi(x)$ *and a root* α *of* $\varphi(x)$ *such that* $\mathbf{k}(\xi)=\mathbf{k}(\alpha)$, *so that the minimal polynomial of* ξ *over* $\mathbf{k}$ *is an irreducible factor of* $\Phi(x)$ *of degree* n.

Proof: Let $\Phi_i(x)=\prod_{j=1}^{N_i}(x-\xi_{i,j})$ $(i=1,\ldots,m)$ denote the m irreducible factors of $\Phi(x)$. Let $\mathcal{G}_i$ be the Galois group of the extension $\mathbf{k}[\xi_{i,1},\ldots,\xi_{i,N_i}]/\mathbf{k}$. Let $\Delta\Phi_i$ be the minimal distance between two distinct zeroes of $\Phi_i(x)$. Let $\widetilde{\xi}_{i,j}$ denote a root of $\Phi_i(x)$ such that $|\alpha_j-\widetilde{\xi}_{i,j}|$ is minimal. Assume that $|\alpha_j-\widetilde{\xi}_{i,j}|\geqslant\Delta\Phi_i$. Then for $1\leqslant i\leqslant m$ and $1\leqslant j\leqslant n$, and using lemma 4.2, we get

$$\begin{aligned}
|\Phi_i(\alpha_j)| &= \prod_{k=1}^{N_i}|\alpha_j-\xi_{i,k}| = \prod_{k=1}^{N_i}\max\{|\alpha_j-\widetilde{\xi}_{i,j}|,\,|\widetilde{\xi}_{i,j}-\xi_{i,k}|\}\\
&\geqslant \prod_{k=1}^{N_i}\max\{\Delta\Phi_i,\,|\widetilde{\xi}_{i,j}-\xi_{i,k}|\}\\
&= \Delta\Phi_i\prod_{\xi_{i,k}\neq\widetilde{\xi}_{i,j}}\max\{\Delta\Phi_i,\,|\widetilde{\xi}_{i,j}-\xi_{i,k}|\} \;=\; \Delta\Phi_i\prod_{\xi_{i,k}\neq\widetilde{\xi}_{i,j}}|\widetilde{\xi}_{i,j}-\xi_{i,k}|.
\end{aligned}$$

Assume w.l.o.g. that $\Delta\Phi_i=|\xi_{i,1}-\xi_{i,2}|$. Choose $\sigma_{i,1},\ldots,\sigma_{i,n}\in\mathcal{G}_i$ so that $\widetilde{\xi}_{i,1}^{\sigma_{i,1}},\ldots,\widetilde{\xi}_{i,1}^{\sigma_{i,n}}$ are distinct and choose $\tau_{i,1},\ldots,\tau_{i,n}\in\mathcal{G}_i$ so that $\widetilde{\xi}_{i,1}^{\tau_{i,1}},\ldots,\widetilde{\xi}_{i,n}^{\tau_{i,n}}$ are distinct. Then $\Delta\Phi_i=|\xi_{i,1}^{\sigma_{i,j}}-\xi_{i,2}^{\sigma_{i,j}}|$ for $1\leqslant j\leqslant n$ and $|\widetilde{\xi}_{i,j}-\xi_{i,k}|=|\widetilde{\xi}_{i,j}^{\tau_{i,j}}-\xi_{i,k}^{\tau_{i,j}}|$ for $1\leqslant j\leqslant n$ and $1\leqslant k\leqslant N_i$. Hence

$$\begin{aligned}
\prod_{j=1}^{n}|\Phi_i(\alpha_j)| &\geqslant \prod_{j=1}^{n}\Bigg(\Delta\Phi_i\prod_{\xi_{i,k}\neq\widetilde{\xi}_{i,j}}|\widetilde{\xi}_{i,j}-\xi_{i,k}|\Bigg)\\
&= \Bigg(\prod_{j=1}^{n}|\xi_{i,1}^{\sigma_{i,j}}-\xi_{i,2}^{\sigma_{i,j}}|\Bigg)\Bigg(\prod_{j=1}^{n}\prod_{\xi_{i,k}\neq\widetilde{\xi}_{i,j}}|\widetilde{\xi}_{i,j}^{\tau_{i,j}}-\xi_{i,k}^{\tau_{i,j}}|\Bigg) \;\geqslant\; |\mathrm{disc}\,\Phi_i|^2.
\end{aligned}$$

Now

$$\begin{aligned}\max_{1\leqslant k\leqslant N} |\varphi(\xi_k)|^N &\geqslant \prod_{k=1}^{N} |\varphi(\xi_k)| = \prod_{j=1}^{n} |\Phi(\alpha_j)| = \prod_{i=1}^{m}\prod_{j=1}^{n} |\Phi_i(\alpha_j)| \\ &\geqslant \prod_{i=1}^{m} |\operatorname{disc}\Phi_i|^2 \geqslant |\operatorname{disc}\Phi|^2.\end{aligned}$$

Thus if $\max_{k=1}^{N} |\varphi(\xi_k)|^N < |\operatorname{disc}\Phi|^2$ then there exist i, j with $1 \leqslant i \leqslant m$ and $1 \leqslant j \leqslant n$ such that $|\alpha_j - \widetilde{\xi}_{i,j}| < \Delta\Phi_i$. It follows from Krasner's lemma (lemma 4.4 below) that $\mathbf{k}(\widetilde{\xi}_{i,j}) \subseteq \mathbf{k}(\alpha_j)$. As $\deg\varphi = n \leqslant \deg\Phi_i = N_i$ we get $\mathbf{k}(\widetilde{\xi}_{i,j}) = \mathbf{k}(\alpha_j)$. Therefore $N_i = n$, and $\Phi_i(x)$, which is the minimal polynomial of $\widetilde{\xi}_{i,j}$ over $\mathbf{k}$, is an irreducible factor of $\Phi(x)$ of degree n. Because $\Phi(x) \in \mathcal{O}_{\mathbf{k}}[x]$ and $|\alpha_j - \widetilde{\xi}_{i,j}| < \Delta\Phi_i$ it follows that that $\varphi(x) \in \mathcal{O}_{\mathbf{k}}[x]$. □

Lemma 4.4 (Krasner): *Let ξ and α be two elements of an algebraic closure of $\mathbf{k}$. Assume that ξ is separable and that the distance between α and ξ is strictly smaller than the distance between ξ and any of its conjugates. Then $\mathbf{k}(\xi) \subseteq \mathbf{k}(\alpha)$.*

Lemma 4.5: *Assume the hypotheses of proposition 4.1 hold. Then $\mathbf{k}(\xi) \cong \mathbf{k}(\alpha)$ for every root ξ of $\Phi(x)$ and every root α of $\varphi(x)$.*

Proof: The result is an immediate consequence of lemma 4.3 if $n = N$, so we assume $n < N$. Let $\Phi_1(x) := \prod_{i=1}^{n}(x - \xi_{1,i})$ denote the irreducible factor of $\Phi(x)$ given by lemma 4.3 and write $\Phi_2(x) := \prod_{j=1}^{N-n}(x - \xi_{2,j}) = \Phi(x)/\Phi_1(x)$. Let $B = \max_{j=1}^{N} |\varphi(\xi_j)|$. By lemma 4.3 $\varphi(x)$ is an irreducible polynomial in $\mathcal{O}_{\mathbf{k}}[x]$; because $\prod_{i=1}^{n} |\Phi_1(\alpha_i)| = \prod_{j=1}^{n} |\varphi(\xi_{1,j})| \leqslant B^n$ and $\prod_{i=1}^{n} |\Phi_2(\alpha_i)| = \prod_{j=1}^{N-n} |\varphi(\xi_{2,j})| \leqslant B^{N-n}$ it follows that $|\Phi_1(\alpha)| \leqslant B$ and $|\Phi_2(\alpha)| \leqslant B^{(N-n)/n}$ for each root α of $\varphi(x)$. We have

$$|\operatorname{disc}\Phi_1|\,|\operatorname{res}(\Phi_1,\Phi_2)| = \prod_{i=1}^{n}\left(\prod_{j\neq i} |\xi_{1,i} - \xi_{1,j}| \prod_{j=1}^{N-n} |\xi_{1,i} - \xi_{2,j}|\right).$$

Let $\mathcal{G}$ be the Galois group of the extension $\mathbf{k}[\xi_{1,1},\ldots,\xi_{1,n}]/\mathbf{k} = \mathbf{k}[\alpha_1,\ldots,\alpha_n]/\mathbf{k}$. For $1 \leqslant i \leqslant n$ let $\widetilde{\alpha}_i$ be a root of $\varphi(x)$ that is closest to $\xi_{1,i}$, and for $1 \leqslant j \leqslant n$ let $\sigma_{j,i}$ be a member of $\mathcal{G}$ such that $\xi_{1,j}^{\sigma_{j,i}} = \xi_{1,i}$. Then

$$|\widetilde{\alpha}_i - \xi_{1,i}| \leqslant |\widetilde{\alpha}_i^{\sigma_{j,i}} - \xi_{1,i}| = |\widetilde{\alpha}_i^{\sigma_{j,i}} - \xi_{1,j}^{\sigma_{j,i}}| = |\widetilde{\alpha}_i - \xi_{1,j}|$$

for $1 \leqslant j \leqslant n$.

Thus

$$
\begin{aligned}
A_i &:= \left(\prod_{j\neq i} |\xi_{1,i}-\xi_{1,j}|\right)\left(\prod_{j=1}^{N-n} |\xi_{1,i}-\xi_{2,j}|\right)\\
&= \left(\prod_{j\neq i} |\xi_{1,i}-\widetilde{\alpha}_i+\widetilde{\alpha}_i-\xi_{1,j}|\right)\left(\prod_{j=1}^{N-n} |\xi_{1,i}-\widetilde{\alpha}_i+\widetilde{\alpha}_i-\xi_{2,j}|\right)\\
&\leqslant \left(\prod_{j\neq i} \max\{|\xi_{1,i}-\widetilde{\alpha}_i|,|\widetilde{\alpha}_i-\xi_{1,j}|\}\right)\left(\prod_{j=1}^{N-n} \max\{|\xi_{1,i}-\widetilde{\alpha}_i|,|\widetilde{\alpha}_i-\xi_{2,j}|\}\right)\\
&= \left(\prod_{j\neq i} |\widetilde{\alpha}_i-\xi_{1,j}|\right)\left(\prod_{j=1}^{N-n} \max\{|\xi_{1,i}-\widetilde{\alpha}_i|,|\widetilde{\alpha}_i-\xi_{2,j}|\}\right).
\end{aligned}
$$

If $|\xi_{1,i}-\widetilde{\alpha}_i| \geqslant |\widetilde{\alpha}_i-\xi_{2,j}|$ for some j then $A_i \leqslant |\Phi_1(\widetilde{\alpha}_i)| \leqslant B$, and if $|\xi_{1,i}-\widetilde{\alpha}_i| < |\widetilde{\alpha}_i-\xi_{2,j}|$ for all j then $A_i \leqslant \prod_{j=1}^{N-n} |\widetilde{\alpha}_i-\xi_{2,j}| = |\Phi_2(\widetilde{\alpha}_i)| \leqslant B^{(N-n)/n} \leqslant B$. Hence

$$
B^N < |\operatorname{disc}\Phi|^2 = |\operatorname{disc}\Phi_1|^2|\operatorname{res}(\Phi_1,\Phi_2)|^4|\operatorname{disc}\Phi_2|^2 \leqslant B^n|\operatorname{disc}\Phi_2|^2.
$$

It follows that $B^{N-n} < |\operatorname{disc}\Phi_2|^2$, and also that $N-n \geqslant n$ (otherwise $\Phi(x)$ would have an irreducible factor of degree less than n). Repeatedly applying lemma 4.3 in this manner we decompose $\Phi(x)$ as a product of irreducible polynomials each of degree n, and the result follows. □

Proof (of proposition 4.1): By lemma 4.5 N must be a multiple of n. If $n = N$ we are done. But if $n < N$ then $\Phi(x)$ is the product of N/n irreducible polynomials, say $\Phi_1(x),\ldots,\Phi_{N/n}(x)$, each of degree n. For $1 \leqslant r \leqslant N/n$ let $\Phi_r(x) = \prod_{i=1}^{n}(x-\xi_{r,i})$, and for $1 \leqslant i \leqslant n$ let $\widetilde{\alpha}_{r,i}$ denote a root of $\varphi(x)$ that is closest to $\xi_{r,i}$. Arguing as in the proof of lemma 4.5 we have

$$
\begin{aligned}
A_{r,i} &:= \left(\prod_{j\neq i} |\xi_{r,i}-\xi_{r,j}|\right)\left(\prod_{s\neq r}\prod_{j=1}^{n} |\xi_{r,i}-\xi_{s,j}|\right)\\
&\leqslant \left(\prod_{j\neq i} \max\{|\xi_{r,i}-\widetilde{\alpha}_{r,i}|,|\widetilde{\alpha}_{r,i}-\xi_{r,j}|\}\right)\left(\prod_{s\neq r}\prod_{j=1}^{n} |\xi_{r,i}-\xi_{s,j}|\right)\\
&\leqslant \left(\prod_{j\neq i} |\widetilde{\alpha}_{r,i}-\xi_{r,j}|\right)\left(\prod_{s\neq r}\prod_{j=1}^{n} \max\{|\xi_{r,i}-\widetilde{\alpha}_{r,i}|,|\widetilde{\alpha}_{r,i}-\xi_{s,j}|\}\right)\\
&\leqslant B,
\end{aligned}
$$

hence

$$
|\operatorname{disc}\Phi| = \prod_{r=1}^{N/n}\prod_{i=1}^{n} A_{r,i} \leqslant B^N < |\operatorname{disc}\Phi|^2,
$$

which is impossible. □

5. Polynomial Factorization Algorithm

The following algorithm constructs a polynomial $\varphi(x)$ as described in the introduction. To use proposition 4.1 to show that the algorithm terminates we need to ensure that $\deg\varphi$ is less than or equal to the degree of any irreducible factor of $\Phi(x)$.

As the algorithm progresses we accumulate polynomials $\varphi_i(x)$ with $E_{\varphi_i} > 1$ and use these for altering $\varphi(x)$ so that the valuation of $\varphi(x)$ evaluated at the roots of $\Phi(x)$ increases (see remarks 5.5 and 5.3). When we find an element γ with $F_\gamma > 1$ we ensure the condition on the degree of $\varphi(x)$ by determining an unramified extension $\widehat{\mathbf{k}}$ of $\mathbf{k}$ with $\widehat{\mathbf{k}} \subseteq \widehat{\mathbf{k}}(\xi)$ for every root ξ of $\Phi(x)$, finding a factor $\widehat{\Phi}(x)$ of $\Phi(x)$ with $\deg(\widehat{\Phi}) = \deg(\Phi)/F_\gamma$ over $\widehat{\mathbf{k}}$, then factoring $\widehat{\Phi}(x)$ itself over $\widehat{\mathbf{k}}$. As we collect more information about the fields generated by the roots of $\Phi(x)$, we enlarge the unramified extension $\widehat{\mathbf{k}}$.

Algorithm 5.1 (Polynomial Factorization):

Input: a monic, separable, squarefree polynomial $\Phi(x)$ over a local field $\mathbf{k}$

Output: a proper factorization of $\Phi(x)$ if one exists,
a two-element certificate for $\Phi(x)$ otherwise

- Initialize $\varphi(x) \leftarrow x$, $\widehat{\Phi}(x) \leftarrow \Phi(x)$, $\widehat{\mathbf{k}} \leftarrow \mathbf{k}$, $E \leftarrow 1$, $P \leftarrow \{\,\}$.
- Repeat:
  - **a**) If $\varphi(x)$ fails the Newton test then: [remark 5.2]
    - Return a proper factorization of $\Phi(x)$.
  - **b**) If $E_\varphi \nmid E$ then [**increase** E]: [remark 5.3]
    - $P \leftarrow P \cup \{\varphi\}$, $S \leftarrow \operatorname{lcm}(E, E_\varphi)/E$, $E \leftarrow SE$, $\varphi(x) \leftarrow \varphi(x)^S$.
    - If $E = \deg\widehat{\Phi}$ then: [remark 5.4]
      - Return a two-element certificate for $\Phi(x)$.
  - **c**) Find $\psi(x) = \pi^{c_0}\varphi_1(x)^{c_1}\varphi_2(x)^{c_2}\cdots\varphi_k(x)^{c_k}$ with: [remark 5.5]
    $v_{\mathfrak{p}}^*(\psi) = v_{\mathfrak{p}}^*(\varphi)$, $\varphi_i(x) \in P$, $c_0 \in \mathbb{Z}$, $c_i \in \mathbb{N}$ $(i > 0)$, $\deg\psi < E$.
  - **d**) Set $\gamma(x) \leftarrow \varphi(x)\psi^{-1}(x)$. [remark 5.6]
  - **e**) If $\gamma(x)$ fails the Hensel test then: [remark 5.2]
    - Return a proper factorization of $\Phi(x)$.
  - **f**) If $EF_\gamma = \deg\widehat{\Phi}$ then: [remark 5.4]
    - Return a two-element certificate for $\Phi(x)$.
  - **g**) If $F_\gamma > 1$ then [**extend the ground field**]: [remark 5.7]
    - Replace $\widehat{\mathbf{k}} \leftarrow \widehat{\mathbf{k}}[t]/\nu_\gamma(t)\widehat{\mathbf{k}}[t]$.
    - Derive a proper factorization $\widehat{\Phi}(x) = \widehat{\Phi}_1(x)\cdots\widehat{\Phi}_r(x)$ of $\widehat{\Phi}(x)$ over $\widehat{\mathbf{k}}$.
    - Replace $\widehat{\Phi}(x) \leftarrow \widehat{\Phi}_i(x)$, with $\deg\widehat{\Phi}_i = \big(\deg\widehat{\Phi}\big)/F_\gamma$.
  - **h**) Find $\delta \in \mathcal{O}_{\widehat{\mathbf{k}}}$ with $\delta \equiv \gamma(\xi) \bmod \pi\mathcal{O}_{\widehat{\mathbf{k}}}$ for all roots ξ of $\Phi(x)$.
  - **i**) Replace $\varphi(x) \leftarrow \varphi(x) - \delta\psi(x)$. [remark 5.3]

Remark 5.2: A proper factorization of $\widehat{\Phi}(x)$ over $\widehat{\mathbf{k}}$ can be derived by applying proposition 2.3 to $\widehat{\Phi}(x)$ and $\varphi(x)$ or corollary 2.4 to $\widehat{\Phi}(x)$ and $\gamma(x)$. From this factorization of $\widehat{\Phi}(x)$ over $\widehat{\mathbf{k}}$ a factorization of $\Phi(x)$ over $\mathbf{k}$ can be obtained using remark 2.9.

Remark 5.3: Replacing $\varphi(x)$ by $\varphi(x)^S$ ensures that $\deg\varphi = E$ when E is replaced by SE, and as $\deg\delta\psi < E$ the degree of $\varphi(x)$ remains equal to E when $\varphi(x)$ is replaced by $\varphi(x) - \delta\psi(x)$. As $\varphi(x) = x$ initially, $\varphi(x)$ remains monic.

Remark 5.4: If $E = \deg\widehat{\Phi}$ then every root ξ of $\Phi(x)$ generates an extension of degree $\deg\widehat{\Phi}$, and hence $\widehat{\Phi}(x)$ is irreducible. It follows from proposition 4.1 that $\deg\varphi = E = \deg\widehat{\Phi}$ if $\deg\widehat{\Phi}\cdot v_{\mathfrak{p}}^*(\varphi) > 2v_{\mathfrak{p}}(\operatorname{disc}\Phi)$. As $v_{\mathfrak{p}}^*(\varphi)$ increases strictly algorithm 5.1 terminates. There exist $c_0 \in \mathbb{Z}$ and $c_1, \dots, c_s \in N$ such that $\Pi(x) := \varphi_1(x)^{c_1}\cdots\varphi_s(x)^{c_s}$ with $\varphi_i(x) \in P$ and $v_{\mathfrak{p}}^*(\Pi) = 1/E$. By section 3 we find a two-element certificate of $\Phi(x)$.

Remark 5.5: Let the elements in P be numbered so that the increase of E by the factor S_j due to $\varphi_j(x)$ is followed by the increase of E by the factor S_{j+1} due to $\varphi_{j+1}(x)$. As $E_\varphi \mid E$ there is an element $\psi(x) = \pi^c\varphi_1(x)^{c_1}\cdots\varphi_k(x)^{c_k}$ with $v_{\mathfrak{p}}^*(\psi) = v_{\mathfrak{p}}^*(\varphi)$. By construction of the $\varphi_j(x)$ we have the relations

$$v_{\mathfrak{p}}^*(\varphi_j^{S_j}) = v_{\mathfrak{p}}^*(\pi^{b_j}\varphi_1^{b_{j,1}}\cdots\varphi_{j-1}^{b_{j,j-1}})$$

with $b_j \in \mathbb{Z}$ and $b_{j,i} \in \mathbb{N}$; hence we can reduce the exponents $c_1, \dots, c_k$ so that $0 \leqslant c_j < S_j$ for $1 \leqslant j \leqslant k$. We get

$$\begin{aligned} \deg\psi &\leqslant (S_1 - 1) + (S_2 - 1)S_1 + (S_3 - 1)S_1S_2 + \cdots + (S_k - 1)S_1\cdots S_{k-1} \\ &= (-1 + S_1\cdots S_k) \;=\; E - 1. \end{aligned}$$

Remark 5.6: In practice we find $\widehat{\psi}(x) \in \widehat{\mathbf{k}}[x]$ such that $\widehat{\psi}(x)\psi(x) \equiv 1 \bmod \widehat{\Phi}(x)$ and set $\gamma(x) \leftarrow \varphi(x)\widehat{\psi}(x)$. Note that $v_{\mathfrak{p}}^*(\gamma) = 0$. As only the values of the polynomials $\gamma(x)$ and $\widehat{\psi}(x)$ at the roots of $\widehat{\Phi}(x)$ are of concern, these polynomials can be reduced modulo $\widehat{\Phi}(x)$.

Remark 5.7: As $F_\gamma > 1$, and as $\widehat{\Phi}(x)$ and therefore $\nu_\gamma(t)$ are separable, $\nu_\gamma(t)$ must have at least two distinct factors over $\widehat{\mathbf{k}}[t]/\nu_\gamma(t)\widehat{\mathbf{k}}[t]$, at least one of which is linear. Proposition 2.3 gives a factorization of $\widehat{\Phi}(x)$ over $\widehat{\mathbf{k}}[t]/\nu_\gamma(t)\widehat{\mathbf{k}}[t]$.

6. Examples

In the first example we show the irreducibility of a polynomial $\Phi(x)$ whose roots generate totally ramified extensions of $\mathbb{Q}_2$. We need to increase the ramification index bound E twice to show the irreducibility of $\Phi(x)$. From the polynomials collected in the set P we compile a certificate for the irreducibility of $\Phi(x)$.

In the second example a polynomial $\Psi(x)$ is factored over $\mathbb{Q}_3$. In the first iteration of the algorithm we discover that all extensions of $\mathbb{Q}_3$ generated by roots of $\Psi(x)$ contain an unramified extension $\widehat{\mathbf{k}}/\mathbb{Q}_3$. We derive a factorization of $\Psi(x)$ over $\widehat{\mathbf{k}}$ from which we obtain a factorization of $\Psi(x)$ over $\mathbb{Q}_3$.

EXAMPLE 6.1: Let $\mathbf{k} = \mathbb{Q}_2$ and

$$\Phi(x) = x^6 + 3\cdot 2x^4 + 2^5x^3 + 3\cdot 2^2x^2 - 3\cdot 2^6x + 33\cdot 2^3.$$

Initially we set $P := \{\,\}$ and $\varphi(x) := x$, hence $\chi_\varphi(t) = \Phi(t)$. It follows that $\varphi(x)$ passes the Hensel and Newton tests. We get $v_2^*(\varphi) = 1/2$, thus $E_\varphi = 2$ and we set $E := 2$, $\varphi_1(x) := \varphi(x)$ and replace P by $\{\varphi_1(x)\}$.

We replace $\varphi(x)$ by x^2, thus $\psi(x) = 2$ and $\gamma(x) = \varphi(x)\psi^{-1}(x) = 2^{-1}x^2$ with $\underline{\chi}_\gamma(t) = t^6 - t^4 + t^2 - 1$. Hence $\nu_\gamma(t) = t + 1$.

We replace $\varphi(x)$ by $\varphi(x) - (-1)\psi(x) = x^2 + 2$. As

$$\chi_\varphi(t) = t^6 - 2^9t^3 + 9\cdot 2^{11}t^2 - 3\cdot 2^{15}t + 3\cdot 2^{16}$$

the polynomial $\varphi(x)$ passes the Hensel and Newton tests. We have $v_2^*(\varphi) = 8/3$ and $E_\varphi = 3$. We replace E by $\operatorname{lcm}(E, E_\varphi) = 6$, set $\varphi_2(x) := \varphi(x)$ and replace P by $\{\varphi_1(x),\, \varphi_2(x)\}$.

The ramification index of all extensions of $\mathbb{Q}_2$ generated by roots of $\Phi(x)$ must be at least $E = 6$. As the degree of $\Phi(x)$ is six, $\Phi(x)$ is irreducible. The irreducibility of $\Phi(x)$ is certified by the two-element certificate $(1, \Pi(x))$ with $\Pi(x) := 2^{-3}\varphi_1(x)\varphi_2(x) = 2^{-3}x^3 + 2^{-2}x$. Note that $v_2^*(\Pi) = 1/6$.

EXAMPLE 6.2: Let $\mathbf{k} = \mathbb{Q}_3$ and

$$\Psi(x) = x^8 + 4x^6 + 2\cdot 3x^4 + 7x^2 + 3^2x + 13.$$

We derive a factorization of $\Psi(x)$ over $\mathbb{Q}_3$ to a precision of twelve 3-adic digits.

Initially we set $\varphi(x) := x$. Then $\chi_\varphi(t) = \Psi(t)$ and $\nu_\varphi(t) = t^2 + 1$. Thus we continue our computation over the extended ground field $\widehat{\mathbf{k}} := \mathbf{k}[t]/\nu_\varphi(t)\mathbf{k}[t]$. Let α be a primitive element of $\widehat{\mathbf{k}}$. Hensel lifting gives the factors

$$\begin{aligned}\widehat{\Psi}(x) = x^4 \; &+ 435740\alpha x^3 + (-33734\cdot 3^2\alpha - 59774\cdot 3)x^2 \\ &+ (-89882\alpha + 8443\cdot 3^2)x + (-5132\cdot 3^2\alpha + 520585)\end{aligned}$$

and its conjugate

$$\begin{aligned}x^4 \; &- 435740\alpha x^3 + (33743\cdot 3^2\alpha - 59774\cdot 3)x^2 \\ &+ (89882\alpha + 8443\cdot 3^2)x + (5132\cdot 3^2\alpha + 520585)\end{aligned}$$

of Ψ over $\widehat{\mathbf{k}}$. We now factorize $\widehat{\Psi}(x)$ over $\widehat{\mathbf{k}}$.

Over $\widehat{\mathbf{k}}$ the polynomial $\varphi(x) = x$ has characteristic polynomial $\chi_\varphi(t) = \widehat{\Psi}(t)$. Hence $\varphi(x)$ passes the Hensel and Newton tests and $\nu_\varphi(t) = t + 2\alpha$.

Thus $\psi(x) = 1$, $\gamma(x) = \varphi_1(x)$, and $\delta = -2\alpha$. Replacing $\varphi(x)$ by $\varphi(x) - \delta\psi(x) = x + 2\alpha$. we get

$$\begin{aligned}\chi_\varphi(t) = t^4 &+ 145244\cdot 3\alpha t^3 + (-33734\cdot 3^2\alpha - 24679\cdot 3^2)t^2 \\ &+ (-116638\cdot 3\alpha + 50654\cdot 3^2)t + 53869\cdot 3^2\alpha - 33559\cdot 3^2;\end{aligned}$$

thus $\varphi(x)$ fails the Newton test. Note that the valuations of the roots of $\chi_\varphi(t)$ are $1/3$ and 1. The polynomial $\vartheta(x) := \varphi(x)^3/3$ with

$$\begin{aligned}\chi_\vartheta(t) = t^4 &+ (-155281\cdot 3\alpha + 16838\cdot 3^2)t^3 + (-3793\cdot 3^2\alpha + 60782\cdot 3)t^2 \\ &+ (277066\alpha + 9565\cdot 3^2)t + 8165\cdot 3^2\alpha - 8350\end{aligned}$$

fails the Hensel test. Hensel lifting gives the factors

$$\begin{aligned}\chi_{\vartheta,1}(t) &= t - 4151\cdot 3^2\alpha + 57679\cdot 3^2, \\ \chi_{\vartheta,2}(t) &= t^3 + (-142828\cdot 3\alpha + 5156\cdot 3^3)t^2 + (-30373\cdot 3^2\alpha + 150737\cdot 3)t \\ &\quad + (-520028\alpha - 17123\cdot 3^2)\end{aligned}$$

of $\chi_\vartheta(t)$. We obtain the factors

$$\begin{aligned}\widehat{\Psi}_1(x) &:= \gcd(\widehat{\Psi}, \chi_{\vartheta,1}(\vartheta(x))) = x + 391409\alpha - 26500\cdot 3, \\ \widehat{\Psi}_2(x) &:= \gcd(\widehat{\Psi}, \chi_{\vartheta,2}(\vartheta(x))) = x^3 + (14777\cdot 3\alpha - 150647\cdot 3)x^2 \\ &\qquad + (158332\cdot 3\alpha - 117802\cdot 3)x + 188791\alpha - 185620\end{aligned}$$

of $\widehat{\Psi}(x)$. As $\chi_\varphi(t)$ has a root of valuation $1/3$ at least one of the extensions given by roots of $\widehat{\Psi}(x)$ must have ramification index greater than or equal to three. Thus $\widehat{\Psi}_2(x)$ is irreducible. Computing the norm of $\widehat{\Psi}_1(x)$ and $\widehat{\Psi}_2(x)$ we get the irreducible factors of $\Psi(x)$ modulo 3^{12} over $\mathbf{k}$:

$$\begin{aligned}\Psi_1(x) &:= \mathrm{N}_{\widehat{\mathbf{k}}/\mathbf{k}}(\widehat{\Psi}_1) = x^2 - 53000\cdot 3x + 204634 \\ \Psi_2(x) &:= \mathrm{N}_{\widehat{\mathbf{k}}/\mathbf{k}}(\widehat{\Psi}_2) = x^6 - 124147\cdot 3x^5 - 128147\cdot 3x^4 + 120868\cdot 3x^3 \\ &\qquad + 28201\cdot 3x^2 + 107405\cdot 3x + 312880.\end{aligned}$$

$\Psi_1(x)$ is certified by the two-element certificate $(\Gamma_1(x), \Pi_1(x)) = (x, 3)$; $\Psi_2(x)$ is certified by the two-element certificate $(\Gamma_2(x), \Pi_2(x)) = (x, \mathrm{N}_{\widehat{\mathbf{k}}/\mathbf{k}}(x + 2\alpha)) = (x, x^2 + 4)$.

7. Complexity Analysis

As algorithm 5.1 is formulated over a general local field $\mathbf{k}$ its complexity is given in terms of arithmetic operations in $\mathbf{k}$. Fix the following notation.

- We write $\mathsf{P}(n, f)$ for the number of steps required to factorize a polynomial of degree n over an extension of the residue class field of $\mathbf{k}$ of degree f.

- Denote by $\mathsf{M}(n)$ the number of ring operations needed for multiplying two polynomials of degree at most n in $\mathbf{k}[x]$. Schönhage and Strassen (1971) have shown that $\mathsf{M}(n) = O(n \log n \log\log n)$.
- Let β, γ be in the algebraic closure $\overline{\mathbf{k}}$ of $\mathbf{k}$ with $[\underline{\mathbf{k}} : \underline{\mathbf{k}}(\underline{\beta})] \leqslant n$ and $[\underline{\mathbf{k}} : \underline{\mathbf{k}}(\underline{\gamma})] \leqslant n$ for some $n \in \mathbb{N}$. Denote by $\mathsf{C}(n)$ the number of arithmetic operations in $\mathbf{k}$ needed to compute an element $\delta \in \overline{\mathbf{k}}$ such that $\underline{\delta}$ is a primitive element of the compositum $\underline{\mathbf{k}}(\underline{\beta}, \underline{\gamma})$.
- Denote by $\mathsf{T}(m, n)$ the number of ring operations required for triangularizing a $m \times n$ matrix over the valuation ring $\mathcal{O}_{\mathbf{k}}$ of $\mathbf{k}$. Hafner and McCurley (1991) have shown that $\mathsf{T}(n, n) = O(n^2 \mathsf{T}(1, 2) + n^{2.376})$.
- Denote by $\mathsf{R}(m, n)$ the number of ring operations needed for computing the resultant in x of two polynomials in $\mathbf{k}[t][x]$ of degree in x at most n and of degree in t at most m. There exists an algorithm such that $\mathsf{R}(m, n) = O(n\mathsf{M}(nm)\log(nm))$.

The extended euclidian algorithm for two polynomials of degree at most n is of complexity $O(\mathsf{M}(n)\log n)$. See von zur Gathen and Gerhard (1999) and the references cited therein for the relevant algorithms.

Theorem 7.1: *Let $\mathbf{k}$ be a local field, let $\Phi(x) \in \mathcal{O}_{\mathbf{k}}[x]$ be monic, separable, and squarefree of degree N.*

There exists an algorithm that derives a factorization of $\Phi(x)$ into irreducible factors and returns an integral basis of $\mathbf{k}[x]/\varphi(x)\mathbf{k}[x]$ for every irreducible factor $\varphi(x)$ of $\Phi(x)$ with the number of arithmetic operations in $\mathbf{k}$ being

$$O\big(\log N(\mathsf{P}(N, N) + \mathsf{T}(N, N) + \mathsf{C}(N)) + v_{\mathfrak{p}}(\operatorname{disc}\Phi)(\mathsf{R}(1, N) + \mathsf{P}(N, N))\big).$$

Lemma 7.2: *Let $\mathbf{k}$ be a local field, let $\Phi(x) \in \mathbf{k}[x]$ be monic, separable, and squarefree of degree N. Let E_Φ be the minimum of the ramification indices and F_Φ be the minimum of the inertia degrees of all extensions of $\mathbf{k}$ generated by roots of $\Phi(x)$.*

Algorithm 5.1 derives a proper factorization of $\Phi(x)$ or a two-element certificate for $\Phi(x)$ with the number of arithmetic operations in $\mathbf{k}$ being

$$O\Big(\log F_\Phi\big(\mathsf{P}(N, F_\Phi) + \mathsf{C}(F_\Phi) + \mathsf{T}(N, N)\big) + E_\Phi \frac{v_{\mathfrak{p}}(\operatorname{disc}\Phi)}{N}\big(\mathsf{R}(1, N) + \mathsf{P}(N, F_\Phi)\big)\Big).$$

Proof: Let $\widehat{\mathbf{k}}$ be an unramified extension of $\mathbf{k}$ contained in $\mathbf{k}(\xi)$ for all roots ξ of $\Phi(x)$ and let $F = [\widehat{\mathbf{k}} : \mathbf{k}]$ then $v_{\mathfrak{p}}(\operatorname{disc}\Phi) \geqslant F v_{\mathfrak{p}}(\operatorname{disc}\widehat{\Phi})$, where $\widehat{\Phi}(x)$ is a factor of degree N/F of $\Phi(x)$ over $\widehat{\mathbf{k}}$. Therefore extending the ground field does not increase the number of repetitions of the main loop *i.e.*, steps **a**), **c**) to **f**) and **i**) are repeated at most $2E_\Phi/N v_{\mathfrak{p}}(\operatorname{disc}\Phi)$ times by proposition 4.1. Note that two polynomials of degree $(\deg\Phi)/F$ over an extension $\widehat{\mathbf{k}}$ of degree F of $\mathbf{k}$ can be multiplied in $\mathsf{M}(F \cdot N/F) = \mathsf{M}(N)$ operations in $\mathbf{k}$.

a) The resultant required for the Hensel test needs $\mathsf{R}(1,N)$ arithmetic operations in $\mathbf{k}$.

b) [**increase** E] An increase of E can occur at most $\log_2 E_\Phi$ times. Computing $\varphi(x)^S$ is of complexity $\mathsf{M}(N)\log E_\Phi$.

c) The extended euclidian algorithm needed for the computation of ψ^{-1} is of complexity $O(\mathsf{M}(N)\log N)$.

e) The resultant required for the Newton test needs $\mathsf{R}(1,N)$ arithmetic operations in $\mathbf{k}$.

g) [**extend the ground field**] The ground field can be extended at most $\log_2 F_\Phi$ times. Factoring $\chi_\gamma(t)$ over the residue class field is of complexity $\mathsf{P}(N/F,F)$. The computation of primitive element of a compositum of two residue class field is of complexity $\mathsf{C}(F_\Phi)$. Deriving a proper factorization requires approximating the greatest common divisor (see proposition 2.5) and computing the norm of $\widehat{\Phi}(x)$ over $\mathbf{k}$ (see remark 2.10). This can be achieved in $\mathsf{T}(N,N)$ respectively $\mathsf{R}(F,N/F)$ operations in $\mathbf{k}$.

h) This step requires factoring $\chi_\gamma(t)$ over the residue class field which is of complexity $\mathsf{P}(N/F,F)$.

Thus a proper factorization of $\Phi(x)$ or a two-element certificate for $\Phi(x)$ can be derived with the number of arithmetic operations in $\mathbf{k}$ being

$$\begin{aligned}&O\Big(\log F_\Phi\big(\mathsf{R}(1,N)+\mathsf{P}(N,F_\Phi)+\mathsf{C}(F_\Phi)+\mathsf{T}(N,N)\big)+\log E_\Phi\big(\mathsf{M}(N)\log(N)\big)\\&\qquad\qquad+E_\Phi\frac{v_{\mathfrak{p}}(\operatorname{disc}\Phi)}{N}\big(\mathsf{R}(1,N)+\mathsf{P}(N,F_\Phi)\big)\Big)\\&=O\Big(\log F_{\Phi_i}\big(\mathsf{P}(N,F_{\Phi_i})+\mathsf{C}(F_\Phi)+\mathsf{T}(N,N)\big)+E_{\Phi_i}\frac{v_{\mathfrak{p}}(\operatorname{disc}\Phi)}{N}\big(\mathsf{R}(1,N)+\mathsf{P}(N,F_{\Phi_i})\big)\Big).\end{aligned}$$

□

Proof (of theorem 7.1): Denote by $\Phi_1(x),\dots,\Phi_m(x)$ the irreducible factors of $\Phi(x)$. Let F_{Φ_i} be the inertia degree of the field given by $\Phi_i(x)$. Let E_{Φ_i} be the ramification index of the field given by $\Phi_i(x)$. It follows from 7.2 that the number of arithmetic operations required for deriving a factorization of $\Phi(x)$ into irreducible factors is

$$\begin{aligned}&\sum_{i=1}^m O\Big(\log F_{\Phi_i}\big(\mathsf{P}(N,F_{\Phi_i})+\mathsf{C}(F_\Phi)+\mathsf{T}(N,N)\big)+E_{\Phi_i}\frac{v_{\mathfrak{p}}(\operatorname{disc}\Phi)}{N}\big(\mathsf{R}(1,N)+\mathsf{P}(N,F_{\Phi_i})\big)\Big)\\&\quad= O\big(\log N(\mathsf{P}(N,N)+\mathsf{C}(N)+\mathsf{T}(N,N))+v_{\mathfrak{p}}(\operatorname{disc}\Phi)(\mathsf{R}(1,N)+\mathsf{P}(N,N))\big).\end{aligned}$$

□

Note that there are algorithms for factoring a polynomial of degree N over $\mathbb{F}_q$ with the expected number of bit operations being $O(N^2\log q)$ (see Kaltofen and Shoup (1998)).

If the residue class field of $\mathbf{k}$ is finite then lemma 3.4 implies that the expected number of resultants needed to find an element δ such that $\underline{\delta}$ is a primitive element of the compositum $\underline{\mathbf{k}}(\underline{\beta}, \underline{\gamma})$ is $O(1)$. Therefore $\mathsf{C}(N)$ is $O(N\mathsf{M}(N)\log(N))$ expected operations in $\mathbf{k}$ in this case.

It follows from proposition 4.1 and remark 2.7 that throughout the algorithm a precision of $2v_{\mathfrak{p}}(\operatorname{disc}\Phi)$ digits in the ground field is sufficient.

Corollary 7.3: *Let $\mathbf{k}$ be a finite extension of $\mathbb{Q}_p$ of degree k. There exists an algorithm that derives a factorization of a monic, separable, and squarefree polynomial $\Phi(x) \in \mathcal{O}_{\mathbf{k}}[x]$ and returns an integral basis for $\mathbf{k}[x]/\varphi(x)\mathbf{k}[x]$ for every irreducible factor $\varphi(x)$ of $\Phi(x)$ into irreducible factors with the expected number of bit operations being*

$$O\big(N^{3+\varepsilon}v_{\mathfrak{p}}(\operatorname{disc}\Phi)^{1+\varepsilon}\log^{1+\varepsilon}p^k + N^{2+\varepsilon}v_{\mathfrak{p}}(\operatorname{disc}\Phi)^{2+\varepsilon}\log^{1+\varepsilon}p^k\big).$$

8. Acknowledgements

The author would like to thank

- David Cantor and Dan Gordon for convincing him that working over unramified extensions is better,
- David Ford, Carsten Friedrichs, and Xavier Roblot for their careful reading of this paper and their useful suggestions,
- John Cannon and Claus Fieker for inviting him to Sydney to implement the polynomial factorization algorithm in Magma (Cannon et al. , 2000).

References

E. Berlekamp, *Factoring polynomials over large finite fields*, Math. Comp. **24** (1970).

J. Cannon et al., *The Magma Computational Algebra System*, University of Sydney, 2000, `http://www.maths.usyd.edu.au:8000/u/magma/index.html`.

D. G. Cantor and D. Gordon, *Factoring polynomials over p-adic fields*, In Proc. ANTS IV, volume 1838 of LNCS, Springer Verlag, 2000.

D. G. Cantor and H. Zassenhaus, *A new algorithm for factoring polynomials over finite fields*, Math. Comp. **36** (1981).

A. L. Chistov, *Efficient factoring polynomials over local fields and its applications*, In Proc. ICM 1990, Springer-Verlag, 1991.

H. Cohen, *Advanced topics in computational number theory*, Springer Verlag, 1999.

H. Cohen, *A Course in computational number theory*, Springer Verlag, 1993.

C. Fieker and C. Friedrichs, *On reconstruction of algebraic numbers*, In Proc. ANTS IV, volume 1838 of LNCS, Springer Verlag, 2000.

D. Ford, *On the Computation of the maximal order in a Dedekind domain*, PhD Dissertation, Ohio State University, 1978.

D. Ford, *The construction of maximal orders over a Dedekind domain*, J. Symb. Comp. **4** (1987) 69–75.

D. Ford and P. Letard, *Implementing the Round Four maximal order algorithm*, J. Théor. Nombres de Bordeaux **6** (1994) 39–80, `http://almira.math.u-bordeaux.fr:80/jtnb/1994-1/jtnb6-1.html`.

D. Ford, S. Pauli and X.-F. Roblot, *A guide to polynomial factorization over* $\mathbb{Q}_p$, CICMA Reports, Concordia Laval McGill, 2000-3, `http://www-cicma.concordia.ca/faculty/cicma/CP00.html`.

J. von zur Gathen and J. Gerhard, *Modern computer algebra*, Cambridge University Press, 1999.

J. Hafner and K. McCurley, *Asymptotically fast triangulization of matrices over rings*, SIAM Journal of Computing **20** (1991).

E. Kaltofen and V. Shoup, *Subquadratic-time factoring of polynomials over finite fields*, Math. Comp. **67** (1998).

J. Montes, *Polígonos de Newton de orden superior y aplicaciones aritméticas*, PhD Thesis, Universitat de Barcelona, 1999.

Ö. Ore, *Newtonsche Polygone in der Theorie der algebraischen Körper*, Math. Ann **99** (1928).

M. E. Pohst, *Factoring polynomials over global fields*, submitted to J. Symb. Comp. (1999).

M. E. Pohst and H. Zassenhaus, *Algorithmic algebraic number theory*, Cambridge University Press, 1989.

X.-F. Roblot, *Factorization algorithms over number fields*, submitted to J. Symb. Comp. (2000).

A. Schönhage and V. Strassen, *Schnelle Multiplikation großer Zahlen*, Computing **7** (1971).

B. M. Trager, *Algebraic factoring and rational function integration*, In Proc. Symposium on Symbolic and Algebraic Computation, ACM Press 1976.

E. Weiss, *Algebraic number theory*, McGraw-Hill, 1963.