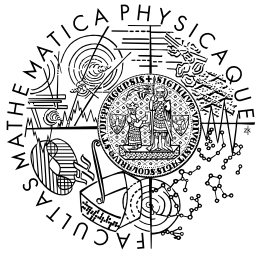

FACULTY
OF MATHEMATICS
AND PHYSICS
Charles University

MASTER THESIS

David Kubát

Algorithms for the computation of Galois groups

Department of Algebra

Supervisor of the master thesis: doc. Mgr. et Mgr. Jan Žemlička, Ph.D.
Study programme: Mathematics
Study branch: Mathematical Methods of Information Security

Prague 2018

I declare that I carried out this master thesis independently, and only with the cited sources, literature and other professional sources.

I understand that my work relates to the rights and obligations under the Act No. 121/2000 Sb., the Copyright Act, as amended, in particular the fact that the Charles University has the right to conclude a license agreement on the use of this work as a school work pursuant to Section 60 subsection 1 of the Copyright Act.

In ..... date ..... signature of the author

Title: Algorithms for the computation of Galois groups

Author: David Kubát

Department: Department of Algebra

Supervisor: doc. Mgr. et Mgr. Jan Žemlička, Ph.D., Department of Algebra

Abstract: This thesis covers the topic of the computation of Galois groups over the rationals. Beginning with the classic algorithm by R. Stauduhar, we then review the theory necessary to explain the modular algorithm by K. Yokoyama. More precisely, we discuss the notion of the universal splitting ring of a polynomial. For a separable polynomial, we then study idempotents in the universal splitting ring. The modular algorithm involves computations in the ring of p-adic integers. Examples are given for polynomials of degree 3 and 4.

Keywords: Algorithm, Galois group, Resolvent polynomial, Idempotent

I'd like to thank my supervisor, Jan Žemlička, for his guidance, patience, and help. I'd like to thank my parents, Jolana and Pavel, for their lifelong unconditional support.

Contents

Introduction

Galois theory emerged in the 19th century as a means to study algebraic equations and it remains an important part of modern algebra. The central object of Galois theory is the Galois group. Given a polynomial $f(x) \in \mathbb{Z}[x]$, the Galois group of f is defined to be the group of automorphisms of the splitting field of f. In this thesis, we study algorithms to determine the structure of the Galois group over $\mathbb{Q}$, given the polynomial f. There are methods to determine the Galois group over a number field or function field too (see [9]).

Van der Waerden [25, p. 189] showed that the problem of finding the Galois group can be reduced to the problem of multivariate polynomial factorization. This result is presented in the second chapter of this thesis as Theorem 2.14. Still, it's importance is rather theoretical than practical. Other more efficient algorithms are presented next. There are, in essence, two sorts of such algorithms: numerical and symbolic. The most notable example of the first is the Stauduhar's algorithm. [23]. It involves numerical computations with the roots of f. We present this method at the end of the second chapter. An example of a symbolic algorithm for the computation of the Galois group is the modular method by K. Yokoyama. [26]. It's largely based on the Stauduhar's algorithm but it doesn't involve numerical computations. Instead, p-adic approximations to the roots of f are used. The careful explanation of this algorithm constitutes the bulk of this thesis.

Applications of these algorithms include a modular method for computing the splitting field of an integral polynomial, which builds on Yokoyama's modular algorithm. [21]. The age-old question of whether a given polynomial is solvable by radicals is addressed in [27]. Another example is given later (see Note 2.22). For implementations, the reader can refer to the computer algebra system GAP, which solves the problem of finding the Galois group for polynomials of degree up to 15. It uses algorithms from [22]. The modular algorithm by Yokoyama is implemented in the computer algebra system ASIR (for polynomials of degree up to 8). [18]. It's also used in other, more advanced, algorithms such as [10].

This thesis is a compilation of known results. The author's merit consists of solving exercises and giving proofs that were omitted in the original articles. Such occurrences are recorded throughout the text (for example, see Note 2.39, Note 3.25, Note 3.50).

Chapter 1

Preliminaries

1.1 The field of p-adic numbers

Let $p \in \mathbb{N}$ stand for a prime number.

Theorem 1.1 ([13], Theorem 1.30)**.** Let $\mathbb{Q}_p$ consist of formal sums

$$\sum_{i=z}^{\infty} a_i p^i,$$

where $z \in \mathbb{Z}$, $a_i \in \{0, \ldots, p-1\}$ for $i \geq z$, and $a_z \neq 0$. In $\mathbb{Q}_p$, operations of addition, multiplication, and division are defined by Algorithm $1, 2, 3$, respectively. These give a field structure on $\mathbb{Q}_p$. The additive identity is $0 = 0p^0$ and the multiplicative identity is $1 = 1p^0$. We call $\mathbb{Q}_p$ the field of p-adic numbers.

Before describing the algorithms, let's introduce some notation. For

$$\sum_{i=z}^{\infty} a_i p^i \in \mathbb{Q}_p,\ n \in \mathbb{Z},\ z < n,$$

we define

$$a \bmod p^n := \sum_{i=z}^{\infty} a'_i p^i,$$

where

$$a'_i = \begin{cases} a_i & \text{if } z \leq i < n, \\ 0 & \text{otherwise.} \end{cases}$$

It will be a helpful convention to set $a_i := 0$ for all $i < z$. Firstly, addition in $\mathbb{Q}_p$ is done in practically the same way as how natural numbers in base p are added. This is formalised in Algorithm 1. Algorithm 2 specifies the operation of multiplication.

Algorithm 1 Addition in $\mathbb{Q}_p$

Input: $a = \sum_{i=z}^{\infty} a_i p^i,\ b = \sum_{i=z'}^{\infty} b_i p^i \in \mathbb{Q}_p$, $n \in \mathbb{Z}$ such that $z \leq z' < n$

Output: $(a + b) \bmod p^n$

$k := 0$
for $i = z, \ldots, n-1$ **do**
  $c_i := a_i + b_i + k$
  if $c_i \geq p$ **then**
    $c_i := c_i - p$
    $k := 1$
  else
    $k := 0$
  end if
end for
return $\sum_{i=z}^{n-1} c_i p^i$

Algorithm 2 Multiplication in $\mathbb{Q}_p$

Input: $a = \sum_{i=z}^{\infty} a_i p^i,\ b = \sum_{i=z'}^{\infty} b_i p^i \in \mathbb{Q}_p$, $n \in \mathbb{Z}$ such that $z + z' < n$

Output: $a \cdot b \bmod p^n$

$k := 0$
for $i = z + z', \ldots, n-1$ **do**
  $s := \left(\sum_{j+j'=i} a_j \cdot b_{j'}\right) + k$
  $c_i := s \bmod p$
  $k := (s - c_i) \operatorname{div} p$
end for
return $\sum_{i=z+z'}^{n-1} c_i p^i$

It's easy to verify that the additive inverse of 1 is

$$-1 = (p-1)p^0 + (p-1)p^1 + (p-1)p^2 + \cdots .$$

Hence it's possible to find the additive inverse of any element $a \in \mathbb{Q}_p$ by executing Algorithm 2 to compute

$$-a = (-1) \cdot a.$$

Finally, here's the division algorithm.

Algorithm 3 Division in $\mathbb{Q}_p$

Input: $a = \sum_{i=z}^{\infty} a_i p^i,\ b = \sum_{i=z'}^{\infty} b_i p^i \in \mathbb{Q}_p$, $n \in \mathbb{N}$ such that $b_{z'} \neq 0$ and $z - z' < n$

Output: $a/b \bmod p^n$

1: Find $\beta \in \{1, \ldots, p-1\}$ such that $b_{z'} \cdot \beta \equiv 1 \pmod{p}$

2: $d = \sum_{i=z}^{n+z'} d_i p^i := a \bmod p^{n+z'+1}$

3: **for** $j = z - z', \ldots, n-1$ **do**

4: $\quad c_j = \beta \cdot d_{j+z'} \bmod p$

5: $\quad d = \sum_{l=j+z'+1}^{n+z'} d_l p^l := (d + (-1) \cdot (c_j p^j) \cdot b) \bmod p^{n+z'+1}$

6: **end for**

7: **return** $\sum_{i=z-z'}^{n-1} c_i p^i$

Before we close this section, note that

$$\mathbb{Z}_p = \left\{ \sum_{i=z}^{\infty} a_i p^i \in \mathbb{Q}_p \mid z \geq 0 \right\}$$

is a subring of $\mathbb{Q}_p$; it's called the ring of p-adic integers. The ring of rational integers $\mathbb{Z}$ is contained in $\mathbb{Z}_p$ via the embedding

$$z \mapsto \sum_{i=0}^{n} d_i p^i,$$

where $\sum_{i=0}^{n} d_i p^i$ is the p-adic expansion of $z \in \mathbb{Z}$. The field $\mathbb{Q}$ of rational numbers is therefore contained in $\mathbb{Q}_p$, as $\mathbb{Q}$ is the quotient field of $\mathbb{Z}$.

1.2 On idempotents

Definition 1.2. Let R be a commutative ring. An element $0 \neq e \in R$ is called an idempotent if $e = e^2$. Two idempotents $e, f \in R$ are orthogonal if $ef = 0$. An idempotent is said to be primitive if it is not the sum of non-zero orthogonal idempotents.

Lemma 1.3 ([19], p. 42)**.** Let R be a commutative ring and $e, f \in R$ distinct primitive idempotents. Then $ef = 0$.

Proof. If we express

$$e = ef + (e - ef),\ f = ef + (f - ef),$$

it's clear that, since e and f are primitive, $ef \neq 0$ would imply

$$e - ef = f - ef = 0,$$

hence $e = f$, a contradiction. □

Lemma 1.4. If R is a field then 1 is the only (hence primitive) idempotent in R.

Proof. Let $0 \neq r \in R$ be an idempotent. Then $r = r \cdot 1 = r(rr^{-1}) = (rr)r^{-1} = rr^{-1} = 1$ □

Proposition 1.5. Let $F_1, \ldots, F_k$, $k \in \mathbb{N}$, be fields. Then the ring

$$R = F_1 \times \cdots \times F_k$$

has exactly k primitive idempotents $e_1, \ldots, e_k$. Moreover,

$$\sum_{i=1}^{k} e_i = 1. \tag{1.1}$$

Proof. By Lemma 1.4, $e_1 := (1, 0, \ldots, 0), e_2 := (0, 1, \ldots, 0), \ldots, e_k := (0, 0, \ldots, 1) \in R$ are all primitive idempotents and (1.1) clearly holds. Now consider a primitive idempotent $e \in R$. Suppose that $e \neq e_i$ for every $i = 1, \ldots, k$. We derive a contradiction. By Lemma 1.3, $ee_i = 0$ for every i. Hence

$$e = e \cdot 1 = e(e_1 + \cdots + e_k) = 0,$$

a contradiction. □

1.3 The Chinese Remainder Theorem

Theorem 1.6 (Chinese Remainder Theorem)**.** Let R be a commutative ring, $M_1, \ldots, M_k \subseteq R$ ideals such that $M_i + M_j = R$ whenever $i \neq j$ and let

$$M = \bigcap_{i=1}^{k} M_i$$

Then

$$r + M \mapsto (r + M_1, \ldots, r + M_k)$$

is an isomorphism between

$$R/M \cong R/M_1 \times \cdots \times R/M_k.$$

1.4 Group actions

Definition 1.7. Let G be a group, Ω a set, and $\mathcal{S}(\Omega)$ the symmetric group on Ω. A group action of G on Ω is a homomorphism $\phi : G \to \mathcal{S}(\Omega)$. For $g \in G$, $\omega \in \Omega$ we shall denote $g(\omega) := \phi(g)(\omega)$. The action ϕ is called faithful if $\mathrm{Ker}(\phi) = 1_G$.

Lemma 1.8 ([8], Lemma 7.2, p. 43)**.** Let $\phi : G \to \mathcal{S}(\Omega)$ be a group action. Let $\omega_1, \omega_2 \in \Omega$. There's an equivalence relation $\sim$ on Ω defined by $\omega_1 \sim \omega_2$ iff there's $g \in G$ s.t. $g(\omega_1) = \omega_2$. The set $G_{\omega_1} = \{g \in G \mid g(\omega_1) = \omega_1\}$ is a subgroup of G.

Definition 1.9. The equivalence classes of $\sim$ are called orbits of ϕ. Say that the action ϕ is transitive if there's only one orbit of ϕ. The group G_ω called the stabilizer of ω, $\omega \in \Omega$. A subgroup of $\mathcal{S}_n$ is transitive if its action on $\{1, \ldots, n\}$ is transitive.

Lemma 1.10. Let $\phi : G \to \mathcal{S}(\Omega)$ be a group action of G on Ω. For every $\omega \in \Omega$ denote by $[\omega]$ the orbit of ω. Then $|[\omega]| = [G : G_\omega]$ and $|G| = |G_\omega||[\omega]|$.

Proof. The first assertion is proved in [8] (Lemma 7.4). The rest follows from Langrange's theorem. □

Let R be a commutative ring. An example of a group action we'll encounter later on is the action of the symmetric group $\mathcal{S}_n$ on $R[x_1, \ldots, x_n]$, $n \in \mathbb{N}$, defined by

$$\tau \mapsto (f(x_1, \ldots, x_n) \mapsto f(x_{\tau(1)}, \ldots, x_{\tau(n)})). \tag{1.2}$$

In other words, given $\tau \in \mathcal{S}_n$, the indeterminates of polynomials in $R[x_1, \ldots, x_n]$ are permuted according to τ. To denote this action, we use the symbol $*$;

$$\tau * f(x_1, \ldots, x_n) = f(x_{\tau(1)}, \ldots, x_{\tau(n)}), \text{ where } f \in R[x_1, \ldots, x_n],\ \tau \in \mathcal{S}_n.$$

Proposition 1.11. Let R be a commutative ring. For every $\sigma, \tau \in \mathcal{S}_n$ and $f \in R[x_1, \ldots, x_n]$,

$$\sigma * (\tau * f) = (\sigma\tau) * f.$$

The map $f \mapsto \tau * f$ is an automorphism of $R[x_1, \ldots, x_n]$.

Proof. The first part follows from $\sigma*(\tau*f) = \sigma*f(y_{\tau(1)}, \ldots, y_{\tau(n)}) = f(y_{\sigma(\tau(1))}, \ldots, y_{\sigma(\tau(n))}) = (\sigma\tau) * f$ and the rest is a matter of direct verification. □

1.5 Symmetric polynomials

In this section, R denotes a commutative ring.

Definition 1.12. Using the notation from the previous section, polynomial $f \in R[x_1, \ldots, x_n]$ is symmetric if $\tau * f = f$ for every $\tau \in \mathcal{S}_n$.

Definition 1.13. Let $s_1, \ldots, s_n \in R[x_1, \ldots, x_n]$ be polynomials defined as

$$\begin{aligned}
s_1(x_1, \ldots, x_n) &= x_1 + x_2 + \cdots + x_n \\
s_2(x_1, \ldots, x_n) &= x_1x_2 + x_1x_3 + \cdots x_1x_n + x_2x_3 + \cdots + x_{n-1}x_n \\
s_3(x_1, \ldots, x_n) &= x_1x_2x_3 + x_1x_2x_4 + \cdots + x_{n-2}x_{n-1}x_n \\
&\vdots \\
s_n(x_1, \ldots, x_n) &= x_1x_2 \cdots x_n
\end{aligned}$$

Then s_i is called the i-th elementary symmetric polynomial.

The following is called the fundamental theorem of symmetric polynomials. Its proof can be found in [20, Věta 3.11]

Theorem 1.14. Let $f \in R[x_1, \ldots, x_n]$ be symmetric. There exists a polynomial $g \in R[x_1, \ldots, x_n]$ such that $f(x_1, \ldots, x_n) = g(s_1(x_1, \ldots, x_n), \ldots, s_n(x_1, \ldots, x_n))$.

Lemma 1.15 (Universal property of polynomial rings)**.** Let R, S be rings, $\phi : R \to S$ a homomorphism, and $s_1, \ldots, s_n \in S$. Then there's a unique homomorphism

$$\psi : R[x_1, \ldots, x_n] \to S$$

such that $\psi\restriction_R = \phi$ and $\psi(x_1) = s_1, \ldots, \psi(x_n) = s_n$.

1.6 Field extensions and homomorphisms

Let L/K be a field extension, $\alpha \in L$. Then $K(\alpha)$ denotes the smallest subfield of L that contains K and α. If α is algebraic over F (i.e. α is a root of a nonzero polynomial in $K[x]$) then $K(\alpha) = \{f(\alpha) \mid f \in K[x]\}$.

Lemma 1.16. Let L/K be a field extension. If $\alpha, \beta \in L$ are both roots of an irreducible polynomial $f \in K[x]$ then there exists a K-isomorphism $\phi : K(\alpha) \to K(\beta)$ such that $\phi(\alpha) = \beta$.

Proof. It can be verified in a straightforward way that $\phi : g(\alpha) \mapsto g(\beta)$ is a well defined field homomorphism and it's clear that $\phi(\alpha) = \beta$. □

Lemma 1.17. Let $K \subseteq L_1, L_2$ be fields and $\phi : L_1 \to L_2$ a field homomorphism such that $\phi\restriction_K = id_K$. If $f \in K[x]$ and $\alpha \in L_1$ then $f(\alpha) = 0$ iff $f(\phi(\alpha)) = 0$.

Proof. If $f(\alpha) = 0$ then $0 = \phi(f(\alpha)) = f(\phi(\alpha))$ because ϕ is a homomorphisim fixing K. The other direction is true because ϕ is injective. □

The proof of the following proposition relies on the Zorn's lemma and is commonly presented in courses on commutative rings.

Proposition 1.18. Let K, L be fields. Suppose $\overline{K}$ is an algebraic closure of both K and L. If $\phi : K \to L$ is a field homomorphism, $\phi \neq 0$, then there exists $\psi \in \mathrm{Aut}(\overline{K})$ such that $\psi\restriction_K = \phi$.

1.7 Separable and normal field extensions

Throughout the rest of this chapter, let $\overline{K}$ denote an algebraic closure of a field K.

Definition 1.19. Let $K \subseteq L \subseteq \overline{K}$ be fields. We say that $f \in K[x]$ is a separable polynomial if f has no multiple roots in $\overline{K}$. An element $\alpha \in \overline{K}$ is separable over K if $m_{\alpha,K}$, the minimal polynomial of α over K, is a separable polynomial. The extension L/K is separable if every element of L is separable. A homomorphism $\phi : L \to \overline{K}$ is called a K-homomorphism if its restriction to K is the identity map on K.

Lemma 1.20. Let $f(x) \in K[x]$, $\mathrm{char}(K) = 0$. Then f is separable iff $\gcd(f, f') = 1$.

Lemma 1.21. Let L/K be an algebraic field extension with $\mathrm{char}(K) = 0$. Then L/K is separable.

Proof. For every $\alpha \in L$, $m_{\alpha,K}$ is irreducible and the formal derivative $m'_{\alpha,F}$ is a nonzero polynomial. The polynomials $m_{\alpha,F}, m'_{\alpha,F}$ are therefore coprime and the minimal polynomial of α has no multiple roots. □

Denote by $\mathrm{Hom}_K(L,\overline{K})$ the set $\{\phi : L \to \overline{K} \mid \phi \text{ is a } K\text{-homomorphism}\}$. Separable field extensions are characterized as follows.

Proposition 1.22. Let L/K be a finite field extension. Then $|\mathrm{Hom}_K(L,\overline{K})| \leq [L : K]$. Furthermore, the following statements are equivalent

(i) L/K is separable

(ii) $L = K(a_1, \ldots, a_l)$ where $a_1, \ldots, a_l \in L$ are separable over K

(iii) $|\mathrm{Hom}_K(L,\overline{K})| = [L : K]$

Proof. See [7], Lemma II.2.3 and Proposition II.2.4. □

The proof of the following can also be found in [7, p. 32], stated as Theorem II.3.1.

Theorem 1.23 (Primitive element theorem)**.** Let L/K be finite and separable. Then there exists $\theta \in L$ such that $L = K(\theta)$.

Definition 1.24. Let $K \subseteq L \subseteq \overline{K}$ be fields. We say that L is normal over K if, for every $\sigma \in \mathrm{Hom}_K(L,\overline{K})$, the equality $\sigma(L) = L$ holds. The set

$$\mathrm{Gal}(L/K) = \{\phi \in \mathrm{Aut}(L) \mid \phi\restriction_K = id_K\}$$

is called the Galois group of the extension L/K. It's clearly a subgroup of the symmetric group on L.

Remark 1.25. We have $\mathrm{Gal}(L/K) \subseteq \mathrm{Hom}_K(L,\overline{K})$ and $\mathrm{Gal}(L/K) = \mathrm{Hom}_K(L,\overline{K})$ iff L is normal over K. Hence $|\mathrm{Gal}(L/K)| \leq |\mathrm{Hom}_K(L,\overline{K})|$ and the equality holds iff L is normal over K.

Let I be a set of indices and $\{f_i\}_{i\in I}$ a family of polynomials in $K[x]$, $\deg(f_i) \geq 1$ for all $i \in I$. By a splitting field for this family we shall mean a field L, $K \subseteq L \subseteq \overline{K}$, such that every f_i splits into linear factors in $L[x]$ and L is generated by the roots of all the polynomials f_i, $i \in I$. All such splitting fields are K-isomorphic

Proposition 1.26 ([7], Proposition II.3.5, p. 33)**.** Let $K \subseteq L \subseteq \overline{K}$ be fields. The following statements are equivalent:

(i) L is normal over K

(ii) L is a splitting field for a family of polynomials in $K[x]$

1.8 Galois field extensions

Definition 1.27. A finite field extension L/K is called Galois if L is normal and separable over K.

Proposition 1.28. Let L be the splitting field of a separable polynomial $f \in K[x]$, $\deg(f) \geq 1$. Then L is Galois over K.

Proof. If $a \in \overline{K}$ is a root of f then $m_{a,K}$ is separable since it divides f. The rest follows combining Proposition 1.22 and Proposition 1.26. □

Remark 1.29. Given a field L and a group $G \subseteq \mathrm{Aut}(L)$, the set

$$\mathrm{Fix}(L, G) = \{x \in L \mid (\forall \sigma \in G)(\sigma(x) = x)\}$$

is a subfield of L. The proof of the following theorem can be found in [16, Theorem 1.8, p. 264].

Theorem 1.30 (Artin)**.** Let L be a field and $G \subseteq \mathrm{Aut}(L)$ a finite subgroup. Set $K = \mathrm{Fix}(L, G)$. Then L/K is a Galois field extension, $[L : K] = |G|$, and $\mathrm{Gal}(L/K) = G$.

Corollary 1.31. Let L/K be a finite field extension and $G = \mathrm{Gal}(L/K)$. The following are equivalent:

(i) L/K is Galois

(ii) $[L : K] = |G|$

(iii) $K = \mathrm{Fix}(L, G)$

Proof. The statements (i) and (ii) are equivalent by Proposition 1.22 and Remark 1.25. Furthermore, by definition, $K \subseteq \mathrm{Fix}(L, G) \subseteq L$ and, by Theorem 1.30,

$$[L : K] = [L : \mathrm{Fix}(L, G)][\mathrm{Fix}(L, G) : K] = |G|[\mathrm{Fix}(L, G) : K].$$

Hence (ii) and (iii) are equivalent. □

Proposition 1.32. Let K be a field, $f \in K[x]$ a separable polynomial, $\deg(f) \geq 1$, and let L be the splitting field of f. There's a group action of $\mathrm{Gal}(L/K)$ on Ω, where Ω is the set of the roots of f in $\overline{K}$, defined by $\sigma \mapsto \sigma\restriction_\Omega$. This action is faithful and the orbits correspond exactly to the irreducible factors of f. More precisely, if $\Lambda \subseteq \Omega$ then Λ constitutes an orbit iff $\prod_{\lambda \in \Lambda}(x - \lambda)$ is an irreducible polynomial in $K[x]$. In particular, if f is irreducible then the action is transitive.

Proof. Let $\sigma \in \mathrm{Gal}(L/K)$. We show that $\sigma\restriction_\Omega$ is a permutation of Ω. If $\omega \in \Omega$ then $\sigma(\omega) \in \Omega$ by Lemma 1.17 and $\sigma\restriction_\Omega$ is a permutation of Ω because σ is injective. It's clear now that $\sigma \mapsto \sigma\restriction_\Omega$ is an action of $\mathrm{Gal}(L/K)$ on Ω.

Let $\Lambda \subseteq \Omega$ be an orbit and we show that $g(x) = \prod_{\lambda \in \Lambda}(x - \lambda)$ is an irreducible polynomial in $K[x]$. For every $\sigma \in \mathrm{Gal}(L/K)$, $\sigma(g(x)) = \prod_{\lambda \in \Lambda}(x - \sigma(\lambda)) = \prod_{\lambda \in \Lambda}(x - \lambda) = g(x)$ because σ permutes the elements of Λ, and the coefficients of g are therefore fixed by elements of the Galois group $\mathrm{Gal}(L/K)$. Because f is separable, L/K is Galois by Proposition 1.28. Thus $g \in K[x]$ by Corollary 1.31.

To see that g is irreducible, let $h \in K[x]$ divide g. We can assume that h is monic and the aim is to show that $g = h$. Let $\Lambda' \subseteq \Lambda$ be the set of the roots of h and fix an element $\lambda' \in \Lambda'$. By Lemma 1.17, $\sigma(\lambda') \in \Lambda'$ for every $\sigma \in \mathrm{Gal}(L/K)$. Let $\lambda \in \Lambda$. Since Λ is an orbit, there's $\sigma \in \mathrm{Gal}(L/K)$ such that $\sigma(\lambda') = \lambda$, which means that $\lambda \in \Lambda'$. Thus $\Lambda' = \Lambda$, $g = h$, and g is irreducible.

On the other hand, if $g(x) = \prod_{\lambda\in\Lambda}(x-\lambda) \in K[x]$ is irreducible then $\sigma(\Lambda) \subseteq \Lambda$ for every $\sigma \in \mathrm{Gal}(L/K)$ by Lemma 1.17. It remains to show that for every $\lambda_1, \lambda_2 \in \Lambda$, there's $\sigma \in \mathrm{Gal}(L/K)$ such that $\sigma(\lambda_1) = \lambda_2$. By Lemma 1.16, there's a K-homomorphism $\phi : K(\lambda_1) \to K(\lambda_2)$ such that $\phi(\lambda_1) = \lambda_2$. By Proposition 1.18, ϕ can be lifted to an automorphism $\bar{\phi}$ of $\overline{K}$. Finally, as L is normal by Proposition 1.28, the restriction of $\bar{\phi}$ to L is a K-automorphism of L that maps λ_1 to λ_2.

To show that the action of $\mathrm{Gal}(L/K)$ on Ω is faithful, note that $L = K(\Omega)$ and if $\sigma(\omega) = \omega$ for every $\omega \in \Omega$, σ must be the identity map on L. □

Definition 1.33. Let $f \in K[x]$ be separable, $\deg(f) = n$. Let L be its splitting field and $\Omega \subseteq L$ the set of its roots. Let $\phi : \mathrm{Gal}(L/K) \to \mathcal{S}(\Omega)$ be the action of $\mathrm{Gal}(L/K)$ on Ω from Proposition 1.32. Since this action is faithful, we can identify $\mathrm{Gal}(L/K)$ with its image $\mathrm{Im}(\phi) \subseteq \mathcal{S}(\Omega)$ under ϕ. Furthermore, once the roots $\alpha_1, \ldots, \alpha_n \in \Omega$ are ordered, $\mathrm{Gal}(L/K)$ can be identified with a subgroup of $\mathcal{S}_n$. We shall denote this subgroup by $\mathrm{Gal}(f)$ and call it the Galois group of f. Whenever we use this symbol, we do so with respect to a given order of the roots. Note that if f is irreducible, $\mathrm{Gal}(f)$ is transitive by Proposition 1.32. Recall that groups $G, G' \leq \mathcal{S}_n$ are conjugate in $\mathcal{S}_n$ if there exists a permutation $\pi \in \mathcal{S}_n$ such that $G = \pi G' \pi^{-1}$.

Lemma 1.34. Let $f \in K[x]$ be separable, $\deg(f) = n$. Let $\alpha_1, \ldots, \alpha_n \in \overline{K}$ be the roots of f and $\mathrm{Gal}(f)$ the Galois group of f. Rearranging the order of the roots changes $\mathrm{Gal}(f)$ into a conjugate group.

Proof. Let $\pi \in \mathcal{S}_n$ and let $H \subseteq \mathcal{S}_n$ be the Galois group of f with respect to the roots ordered as $(\alpha_{\pi(1)}, \ldots, \alpha_{\pi(n)})$. It's easy to verify that $\tau \in H$ iff there's $\sigma \in \mathrm{Gal}(f)$ such that $\tau = \pi^{-1}\sigma\pi$. □

Definition 1.35. Let L/K be a finite and separable field extension. Define the Galois closure of L in $\overline{K}$ to be the intersection of all subfields of $\overline{K}$ which are Galois over K and contain L.

Remark 1.36. Let the notation from the above definition hold. The Galois closure of L in $\overline{K}$ is the smallest (with respect to inclusion) field F such that $L \subseteq F$ and F/K is Galois. For $L_1, L_2 \subseteq \overline{K}$ fields, let the product L_1L_2 denote the smallest subfield of $\overline{K}$ containing both L_1, L_2.

Proposition 1.37. Let L/K be finite and separable, $L = K(\theta)$, $\theta \in L$, and let F be the Galois closure of L in $\overline{K}$. Then F is the splitting field of $m_{\theta,K}$, the minimal polynomial of θ over K.

Proof. Let $S \subseteq \overline{K}$ be the splitting field of $m_{\theta,K}$ and $\Omega = \{\theta_1, \ldots, \theta_n\} \subseteq \overline{K}$ the set of the roots of $m_{\theta,K}$. Then $S = K(\theta_1, \ldots, \theta_n) = \prod_{i=1}^{n} K(\theta_i)$. By Proposition 1.32, $\mathrm{Gal}(S/K)$ acts transitively on Ω and therefore $S = \prod_{\sigma\in\mathrm{Gal}(S/K)} K(\sigma(\theta))$.

For every $\sigma \in \mathrm{Gal}(S/K)$, there's $\bar{\sigma} \in \mathrm{Aut}(\overline{K})$ such that $\bar{\sigma}_{\restriction S} = \sigma$ by Proposition 1.18. We have $\bar{\sigma}(F) = F$ because F/K is normal. Hence

$$K(\sigma(\theta)) = \sigma(K(\theta)) = \sigma(L) \subseteq \bar{\sigma}(F) = F$$

and it follows that $S = \prod_{\sigma \in \mathrm{Gal}(S/K)} K(\sigma(\theta)) \subseteq F$. On the other hand, S/K is Galois by Proposition 1.28 and $F \subseteq S$ by Remark 1.36. □

1.9 Galois groups in number fields

Let $\overline{\mathbb{Q}}$ denote the field of algebraic numbers: $\overline{\mathbb{Q}} = \{z \in \mathbb{C} \mid z \text{ is algebraic over } \mathbb{Q}\}$.

Definition 1.38. A field K is called a number field if $\mathbb{Q} \subseteq K$ and $[K : \mathbb{Q}]$ is finite. The number $[K : \mathbb{Q}]$ is called the degree of the number field K.

By Theorem 1.23, every number field is a simple extension of $\mathbb{Q}$. Let $K = \mathbb{Q}(\alpha)$ be a number field, $\alpha \in \overline{\mathbb{Q}}$, and let f be the minimal polynomial of α over $\mathbb{Q}$. By Proposition 1.37, the Galois closure L of K in $\overline{\mathbb{Q}}$ coincides with the splitting field of f. The algorithms studied in this thesis take a separable polynomial $f \in \mathbb{Q}[x]$ as an input and the aim is to learn the structure of the group $\mathrm{Gal}(L/\mathbb{Q})$. Every automorphism in $\mathrm{Gal}(L/\mathbb{Q})$ is fully determined by its action on the roots of f and it is therefore sufficient to restrict our attention to finding the permutation group $\mathrm{Gal}(f)$ (with respect to some order of the roots of f).

The polynomial f can be assumed to be monic with integer coefficients because there's an integer k such that $g(x) := kf(x) \in \mathbb{Z}[x]$ and clearly L is the splitting field of g as well. Let $c \in \mathbb{Z}$ be the leading coefficient of g and consider the polynomial

$$c^{n-1} g\left(\frac{x}{c}\right).$$

It's monic with integer coefficients and, again, L is its splitting field. Thus to assume for the initial polynomial to be monic with integer coefficients causes no loss of generality. The roots f are then algebraic integers in the sense of the following definition.

Definition 1.39. Let $\alpha \in \mathbb{C}$. The α is called an algebraic integer if there's a monic polynomial in $\mathbb{Z}[x]$ that has a root α. We denote by $\mathbb{Z}_{\overline{\mathbb{Q}}}$ the set of algebraic integers.

The following is proved in [7], Corollary III.2.6.

Proposition 1.40. The set $\mathbb{Z}_{\overline{\mathbb{Q}}}$ of algebraic integers is a ring.

As a next step, we prove that the ring $\mathbb{Z}$ is an integrally closed domain. That is to say, if $\alpha \in \mathbb{Q}$ is an algebraic integer then $\alpha \in \mathbb{Z}$.

Lemma 1.41. Let $f = \sum_{i=0}^{n} a_i x^i \in \mathbb{Z}[x]$ and let $\dfrac{p}{q} \in \mathbb{Q}$ be its root, $\gcd(p, q) = 1$. Then $p \mid a_0$ and $q \mid a_n$.

Proof. See [20, Kapitola V., Cvičení 36 (i), p. 336]. □

Corollary 1.42. The ring $\mathbb{Z}$ is an integrally closed domain.

Proof. If $\alpha = p/q \in \mathbb{Q}$ is a root of a monic polynomial from $\mathbb{Z}[x]$ then $q \in \{1, -1\}$ by Lemma 1.41 and $\alpha \in \mathbb{Z}$. □

There's a simple relationship between the Galois group of a polynomial f and its discriminant $\operatorname{disc}(f)$.

Definition 1.43. Let R be an integral domain, $f \in R[x]$, $\deg(f) = n \geq 1$. Let K be the quotient field of R and $\alpha_1, \ldots, \alpha_n \in \overline{K}$ the roots of f. The number

$$\operatorname{disc}(f) = \operatorname{lc}(f)^{2n-2} \prod_{i<j} (\alpha_i - \alpha_j)^2$$

is called the discriminant of f.

Remark 1.44. By definition, f is separable over K iff $\operatorname{disc}(f) \neq 0$.

The following is a consequence of Proposition 2.4, which will be presented in the next chapter.

Lemma 1.45. With the above notation, $\operatorname{disc}(f) \in R$.

Recall that for a permutation $\tau \in \mathcal{S}_n$, $\operatorname{sgn}(\tau)$ is equal to 1 if the number of tuples (i, j) such that $i < j$ and $\tau(i) > \tau(j)$ is even and -1 otherwise. We say that τ is even if $\operatorname{sgn}(\tau) = 1$ and odd if $\operatorname{sgn}(\tau) = -1$. The set $\mathcal{A}_n \subseteq \mathcal{S}_n$ consisting of even permutations is a normal subgroup of $\mathcal{S}_n$.

Proposition 1.46. Let $f \in \mathbb{Z}[x]$ be monic and separable and let $\alpha_1, \ldots, \alpha_n \in \overline{\mathbb{Q}}$ be the roots of f. Then $\operatorname{Gal}(f) \subseteq \mathcal{A}_n$ iff $\operatorname{disc}(f)$ is a square.

Proof. Let L be the splitting field of f and let $\sigma \in \operatorname{Gal}(L/\mathbb{Q})$. There's a unique permutation $\sigma' \in \operatorname{Gal}(f)$ such that $\sigma(\alpha_i) = \alpha_{\sigma'(i)}$ for every i. Denote by d the product $d = \prod_{i<j}(\alpha_i - \alpha_j)$. Then

$$\begin{aligned}\sigma(d) = \prod_{i<j}(\sigma(\alpha_i) - \sigma(\alpha_j) = \prod_{i<j}(\alpha_{\sigma'(i)} - \alpha_{\sigma'(j)}) = \\ = \prod_{\substack{i<j \\ \sigma'(i)<\sigma'(j)}} (\alpha_{\sigma'(i)} - \alpha_{\sigma'(j)}) \prod_{\substack{i<j \\ \sigma'(i)>\sigma'(j)}} (\alpha_{\sigma'(i)} - \alpha_{\sigma'(j)}).\end{aligned}$$

If the number of the tuples (i, j) such that $i < j$ and $\sigma'(i) > \sigma'(j)$ is even then $\sigma(d) = d$. Otherwise, $\sigma(d) = -d$. We see that $\sigma(d) = \operatorname{sgn}(\sigma')d$ for every $\sigma \in \operatorname{Gal}(L/\mathbb{Q})$. Therefore $\operatorname{Gal}(f) \subseteq \mathcal{A}_n$ iff $\sigma(d) = d$ for every $\sigma \in \operatorname{Gal}(L/\mathbb{Q})$. By Corollary 1.31, the latter condition is equivalent to $d \in \mathbb{Q}$ because L is Galois over $\mathbb{Q}$. The roots of f are algebraic integers and, by Proposition 1.40, d is also an algebraic integer. Finally, Corollary 1.42 implies that $d \in \mathbb{Q}$ iff $d \in \mathbb{Z}$. □

Corollary 1.47. Let $f \in \mathbb{Z}$ be monic and irreducible of degree 3. If $\operatorname{disc}(f)$ is a square in $\mathbb{Z}$ then

$$\operatorname{Gal}(f) = \mathcal{A}_3.$$

Otherwise,

$$\operatorname{Gal}(f) = \mathcal{S}_3.$$

Proof. The group $\mathrm{Gal}(f)$ is a transitive subgroup of $\mathcal{S}_3$ by Proposition 1.32. $\mathcal{S}_3$ and $\mathcal{A}_3$ are the only transitive subroups of $\mathcal{S}_3$ and the rest follows from Proposition 1.46. Note that the particular order of the roots of f is irrelevant since $\mathcal{A}_3$ is normal in $\mathcal{S}_3$. □

Example 1.48. We have $\mathrm{disc}(x^3 - 2) = -108 \in \mathbb{Z} \setminus \mathbb{Z}^2$ and $\mathrm{Gal}(x^3 - 2) = \mathcal{S}_3$ (with respect to any order of the roots of $x^3 - 2$.
On the other hand, $\mathrm{disc}(x^3+x^2-2x-1) = 49 \in \mathbb{Z}^2$ and $\mathrm{Gal}(x^3+x^2-2x-1) = \mathcal{A}_3$.

1.10 Galois groups in finite fields

Let $p \in \mathbb{N}$ be a prime, $\mathbb{F}_{p^n}$ be a finite field and $\mathbb{F}_p$ its prime field. The extension

$$\mathbb{F}_p \leq \mathbb{F}_{p^n}$$

is Galois because $\mathbb{F}_{p^n}$ is the splitting field of the separable polynomial $x^{p^n} - x$ over $\mathbb{F}_p$. We now show that the Galois group $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ is generated by the Frobenius automorphism

$$\phi_p : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n},$$

defined by

$$\phi_p(\alpha) = \alpha^p.$$

Lemma 1.49. With the notation from the above paragraph we have $\phi_p \in \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$.

Proof. It is easily verified that ϕ_p is an endomorphism of $\mathbb{F}_{p^n}$. If $\alpha^p = \beta^p$, $\alpha, \beta \in \mathbb{F}_{p^n}$, then $\alpha^p - \beta^p = (\alpha - \beta)^p = 0$ and $\alpha = \beta$ and ϕ_p is injective. So ϕ_p is an automorphism. For every $\alpha \in \mathbb{F}_p$, $\alpha^p = \alpha$ holds because $|(\mathbb{F}_p)^\times| = p - 1$. Hence ϕ_p fixes $\mathbb{F}_p$. □

Theorem 1.50. Let $\mathbb{F}_{p^n}$ be a finite field, $n \in \mathbb{N}$, and let $\mathbb{F}_p$ be its prime field. The group $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ is cyclic of order n and the Frobenius automorphism is its generator.

Proof. As we know that the extension $\mathbb{F}_p \leq \mathbb{F}_{p^n}$ is Galois, it follows from Corollary 1.31 that $|\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)| = [\mathbb{F}_{p^n} : \mathbb{F}_p] = n$. The multiplicative group $\mathbb{F}_{p^n}^\times$ is cyclic and there's an element $\alpha \in \mathbb{F}_{p^n}^\times$ that generates it. The n values $\phi_p(\alpha) = \alpha^p$, $\phi_p^2(\alpha) = \alpha^{p^2}, \ldots, \phi_p^n(\alpha) = \alpha$ are distinct and ϕ_p therefore generates the whole group $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$. □

Chapter 2

The Galois Group

2.1 Tschirnhausen transformation

The Stauduhar's method of finding the Galois group relies partly on the so called Tschirnhausen transformation. This is an algorithm that, given a number field K, outputs an irreducible polynomial $g \in \mathbb{Z}[x]$ such that $K = \mathbb{Q}(\theta)$, where $\theta \in \overline{\mathbb{Q}}$ is a root of g. It also uses the notion of resultant, defined as follows.

Definition 2.1. Let R be an integral domain, K its quotient field, and let $\overline{K}$ be an algebraic closure of K. If $f, g \in R[x]$, where $\deg(f) = m$, $\deg(g) = n$, and

$$f(x) = a(x - \alpha_1) \cdots (x - \alpha_m)$$

$$g(x) = b(x - \beta_1) \cdots (x - \beta_n)$$

with $\alpha_i, \beta_j \in \overline{K}$, the resultant $\operatorname{res}(f, g)$ of f and g is defined as

$$\operatorname{res}(f, g) = a^n b^m \prod_{\substack{1 \le i \le m \\ 1 \le j \le n}} (\alpha_i - \beta_j)$$

Remark 2.2. It's clear that

$$\operatorname{res}(f, g) = a^n \prod_{1 \le i \le m} g(\alpha_i).$$

The polynomials f, g from the above definition are usually elements of $\mathbb{Z}[x]$ (i.e. $R = \mathbb{Z}$). It also makes sense to consider the the case $R = \mathbb{Z}[x]$, as we shall see later.

Proposition 2.3 ([6], Lemma 3.3.4, p. 119)**.** Let R be an integral domain. If $f(x) = \sum_{i=0}^{m} a_i x^i \in R[x]$ and $g(x) = \sum_{i=0}^{n} b_i x^i \in R[x]$, then the resultant $\operatorname{res}(f, g)$

is equal to the determinant of the following $(n+m)\times(n+m)$ matrix

$$\begin{pmatrix}
a_m & a_{m-1} & a_{m-2} & \dots & a_1 & a_0 & 0 & 0 & \dots & 0 \\
0 & a_m & a_{m-1} & a_{m-2} & \dots & a_1 & a_0 & 0 & \dots & 0 \\
0 & 0 & a_m & a_{m-1} & a_{m-2} & \dots & a_1 & a_0 & \dots & 0 \\
\vdots & \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\
0 & 0 & \dots & 0 & a_m & a_{m-1} & a_{m-2} & \dots & a_1 & a_0 \\
b_n & b_{n-1} & \dots & b_2 & b_1 & b_0 & 0 & 0 & \dots & 0 \\
0 & b_n & b_{n-1} & \dots & b_2 & b_1 & b_0 & 0 & \dots & 0 \\
0 & 0 & b_n & b_{n-1} & \dots & b_2 & b_1 & b_0 & \dots & 0 \\
\vdots & \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\
0 & 0 & \dots & 0 & b_n & b_{n-1} & \dots & b_2 & b_1 & b_0
\end{pmatrix}$$

where the coefficients of f are repeated on n rows, and the coefficients of g are repeated on m rows.

We see now that the resultant is always an element of R. For example, if $f, g \in \mathbb{Z}[x]$, then $\operatorname{res}(f,g) \in \mathbb{Z}$. Proposition 2.3 also gives us a practical method of computing the resultant $\operatorname{res}(f,g)$ (based only on the knowledge of the coefficients $a_i, b_i \in R$). This way (by computing the determinant of the matrix from Proposition 2.3), the resultant $\operatorname{res}(f,g)$ can be obtained using $O((m+n)^3)$ operations in R (where $\deg(f)=m$, $\deg(g)=n$).

The discriminant $\operatorname{disc}(f)$ of a polynomial f (Definition 1.43) can be expressed in terms of the resultant of f and f' as follows.

Proposition 2.4. Let R be an integral domain, $f \in R[x]$, $\deg(f) = n \geq 1$. Let K be the quotient field of R The discriminant of f is equal to

$$\operatorname{disc}(f) = (-1)^{n(n-1)/2} \cdot \operatorname{res}(f, f')/\operatorname{lc}(f),$$

where f' is the formal derivative of f.

Proof. Let $\alpha_1, \dots, \alpha_n \in \overline{K}$ be the roots of f. Since

$$f(x) = \operatorname{lc}(f)(x-\alpha_1)\cdots(x-\alpha_n),$$

the formal derivative of f is

$$f'(x) = \operatorname{lc}(f)(x-\alpha_2)\cdots(x-\alpha_n) + \operatorname{lc}(f)(x-\alpha_1)(x-\alpha_3)\cdots(x-\alpha_n) + \cdots$$

By Remark 2.2, we can express $\operatorname{res}(f,f')$ as

$$\operatorname{res}(f,f') = \operatorname{lc}(f)^{n-1} \prod_{1\leq i\leq n} f'(\alpha_i) = \operatorname{lc}(f)^{2n-1}(-1)^{n(n-1)/2} \prod_{1\leq i<j\leq n} (\alpha_i-\alpha_j)^2 =$$
$$= \operatorname{lc}(f)(-1)^{n(n-1)/2} \cdot \operatorname{disc}(f)$$

and the rest follows. □

A simple consequence is that the discriminant is an element of R. In the matrix from Proposition 2.3, the only nonzero elements of the first column are a_m and b_n and $\operatorname{res}(f,g)$ is therefore divisible by their greatest common divisor $\gcd(a_m, b_n)$. In particular, $\operatorname{res}(f,f')$ is divisible by $\operatorname{lc}(f)$ and

$$\operatorname{disc}(f) = (-1)^{n(n-1)/2} \cdot \operatorname{res}(f,f')/\operatorname{lc}(f) \in R.$$

Example 2.5. In Example 1.48, we used the fact that $\operatorname{disc}(x^3-2) = -108$. Let $f(x) = x^3 - 2 \in \mathbb{Z}[x]$ and $g(x) = f'(x) = 3x^2 \in \mathbb{Z}[x]$. By Proposition 2.3,

$$\operatorname{res}(f,g) = \det \begin{pmatrix} 1 & 0 & 0 & -2 & 0 \\ 0 & 1 & 0 & 0 & -2 \\ 3 & 0 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 & 0 \\ 0 & 0 & 3 & 0 & 0 \end{pmatrix} = 108$$

By Proposition 2.4, $\operatorname{disc}(f) = -\operatorname{res}(f, f') = -108$.

A more effective way to compute resultants is to use the sub-resultant algorithm, introduced below. It uses "pseudo-division" as a subroutine, which we now recall (as described in [4]). Given polynomials $f, g \in R[x]$, where R is a UFD, $g \neq 0$, it might not always be the case that the quotient and remainder $q, r \in R[x]$ exist, such that

$$f = qg + r, \ \deg(r) < \deg(g). \tag{2.1}$$

There are, for example, no polynomials $q, r \in \mathbb{Z}[x]$, such that $x^2 - 1 = q(x)(2x - 2) + r(x)$. Let $\deg(f) = m$, $\deg(g) = n$, $n \leq n$. There is, however, a solution to (2.1) if

$$\operatorname{lc}(g)^{m-n+1} f$$

is considered instead of f. In other words, there always exist polynomials $q, r \in R[x]$, such that

$$\operatorname{lc}(g)^{m-n+1} f(x) = q(x)g(x) + r(x), \ \deg(r) < \deg(g). \tag{2.2}$$

The following algorithm can be used to find these polynomials.

Algorithm 4 Pseudo-division

Input: Polynomials f and g with coefficients in a UFD R, $g \neq 0$, $\deg(f) = m$, $\deg(g) = n$, $n \leq m$.

Output: Polynomials $q, r \in R[x]$ that satisfy (2.2).

1: Set $r \leftarrow \operatorname{lc}(g)^{m-n+1} f$
2: **for** $i = m - n, \ldots, 0$ **do**
3: $\quad q_i \leftarrow a/\operatorname{lc}(g)$, where a is the coefficient of x^{m+i} in r
4: $\quad r \leftarrow r - q_i x^i g$
5: **end for**
6: **return** $q \leftarrow \sum_{i=0}^{m-n} q_i x^i$, r

The algorithm works correctly because, for every $i \in \{0, \ldots, m-n\}$,

$$f(x) = (q_{m-n}x^{m-n} + \cdots + q_i x^i)g(x) + r(x), \ \deg(r) < n + i,$$

and every coefficient of r is divisible by $\operatorname{lc}(g)$ because at most $m - n + 1$ divisions take place throughout the execution of the algorithm. Concerning the time complexity of Algorithm 4, the initial computation $r \leftarrow \operatorname{lc}(g)^{m-n+1} f$ can be done using

$$O(\deg(f) \cdot (m - n + 1)) = O(m(m - n + 1))$$

operations in R. Furthermore, the cycle runs $m-n+1$ times and its body takes $O(n)$ operations in R to execute. In total, the algorithm takes $O((m+n)(m-n+1))$ operations in R.

The following algorithm computes the resultant of two polynomials f, g with coefficients in a UFD R. Using Proposition 2.4, it can be used to compute the discriminant of a polynomial by substituting $R = \mathbb{Z}$. Later we show how to use it to compute the characteristic polynomial of an algebraic number by substituting $R = \mathbb{Z}[x]$. The proof of its correctness can be found in [6, p. 122].

Algorithm 5 Sub-Resultant

Input: Two polynomials f and g with coefficients in a UFD R.
Output: $\operatorname{res}(f, g)$.

1: If $f = 0$ or $g = 0$, output 0 and terminate the algorithm. Otherwise, set $a \leftarrow \operatorname{cont}(f)$, $b \leftarrow \operatorname{cont}(g)$, $f \leftarrow f/a$, $g \leftarrow g/b$, $u \leftarrow 1$, $v \leftarrow 1$, $s \leftarrow 1$ and $t \leftarrow a^{\deg(g)} b^{\deg(f)}$. Finally, if $\deg(f) < \deg(g)$ exchange f and g and if in addition $\deg(f)$ and $\deg(g)$ are odd set $s \leftarrow -1$.

2: Set $\delta \leftarrow \deg(f) - \deg(g)$. If $\deg(f)$ and $\deg(g)$ are odd, set $s \leftarrow -s$. Finally, compute r, q such that $\operatorname{lc}(g)^{\delta+1} f = gq + r$ (using Algorithm 1).

3: Set $f \leftarrow g$ and $g \leftarrow r/(uv^{\delta})$.

4: Set $u \leftarrow \operatorname{lc}(f)$, $v \leftarrow v^{1-\delta} u^{\delta}$. If $\deg(g) > 0$ go to step 2, otherwise set $v \leftarrow v^{1-\deg(f)} \operatorname{lc}(g)^{\deg(f)}$, output $s \cdot t \cdot v$ and terminate the algorithm.

The second step of Algorithm 2.1 is repeated at most $\deg(g)$ times. With the pseudo-division requiring $O((m+n)(m-n+1))$ operations in R, the total time complexity of Algorithm 2 is $O(n(m+n)(m-n+1))$ operations in R, where $\deg(f) = m$, $\deg(g) = n$. More details about it can also be found in [15].

Example 2.6. In Example 1.48, we used the fact that $\operatorname{disc}(x^3+x^2-2x-1) = 49$. We show this using Algorithm 5 with $R = \mathbb{Z}$, $f(x) = x^3 + x^2 - 2x - 1$, $g(x) = f'(x) = 3x^2 + 2x - 2$. Since the variables a, b, s, t are equal to 1 for the whole duration of the algorithm, we omit them in our computations.

- (1: Initializations)
  $u \leftarrow 1$, $v \leftarrow 1$
- (2: Pseudo division)
  $\delta \leftarrow 1 = \deg(f) - \deg(g)$
  The algorithm for pseudo division yields $q \leftarrow 3x + 1$, $r \leftarrow -14x - 7$
  (so that $3^{\delta+1} f(x) = g(x)q(x) + r(x)$).
- (3: Reduce remainder)
  $f \leftarrow 3x^2 + 2x - 2$, $g \leftarrow -14x - 7$.
- (4: Finished?)
  $u \leftarrow 3$, $v \leftarrow 3$. Since $\deg(g) > 0$, we go to Step 2 (Pseudo division).
- (2: Pseudo division)
  $\delta \leftarrow 1 = \deg(f) - \deg(g)$
  Again, the algorithm for pseudo division yields $q \leftarrow -42x - 7$, $r \leftarrow -441$

- (3: Reduce remainder)
  $f \leftarrow -14x - 7$, $g \leftarrow -49$
- (4: Finished?)
  As $\deg(g) = 0$, the output of the algorithm is $v \leftarrow -49$

We conclude that $\operatorname{res}(f, f') = -49$. By Proposition 2.4, we see that

$$\operatorname{disc}(f) = -\operatorname{res}(f, f') = 49.$$

Before giving the definition of the characteristic polynomial of an algebraic number, let us summarize what we know about number fields.

Proposition 2.7. Let $K = \mathbb{Q}(\alpha)$ be a number field of degree n. Then $|\operatorname{Hom}_{\mathbb{Q}}(K, \overline{\mathbb{Q}})| = n$ and $\{\sigma(\alpha) \mid \sigma \in \operatorname{Hom}_{\mathbb{Q}}(K, \overline{\mathbb{Q}})\}$ is the set of all the roots of $m_{\alpha,\mathbb{Q}}$ in $\overline{\mathbb{Q}}$. In particular, $m_{\alpha,\mathbb{Q}}(x) = \prod_{\sigma \in \operatorname{Hom}_{\mathbb{Q}}(K,\overline{\mathbb{Q}})}(x - \sigma(\alpha))$.

Proof. As shown in Lemma 1.21, $K/\mathbb{Q}$ is separable and the first assertion is true by Proposition 1.22. Lemma 1.17 implies that $\Omega := \{\sigma(\alpha) \mid \sigma \in \operatorname{Hom}_{\mathbb{Q}}(K, \overline{\mathbb{Q}})\}$ only contains roots of $m_{\alpha,\mathbb{Q}}$. Furthermore, α generates K and if two embeddings coincide on α then they must be equal. Thus, $|\Omega| = |\operatorname{Hom}_{\mathbb{Q}}(K, \overline{\mathbb{Q}})| = n = \deg(m_{\alpha,\mathbb{Q}})$ and every root of $m_{\alpha,\mathbb{Q}}$ is contained in Ω.

□

Definition 2.8. Let K be a number field of degree n, $\operatorname{Hom}_{\mathbb{Q}}(K, \overline{\mathbb{Q}}) = \{\sigma_1, \ldots, \sigma_n\}$, $\theta \in K$. The characteristic polynomial $C_{K,\theta}$ of θ in K is

$$C_{K,\theta}(x) = \prod_{i=1}^{n}(x - \sigma_i(\theta))$$

Remark 2.9. Let K be a number field and $\theta \in K$. Since every embedding of $\mathbb{Q}(\theta)$ lifts to exactly $d = [K : \mathbb{Q}(\theta)]$ embeddings of K, the characteristic polynomial of θ is equal to

$$C_{K,\theta}(x) = \prod_{\sigma \in \operatorname{Hom}_{\mathbb{Q}}(K,\overline{\mathbb{Q}})}(x - \sigma(\theta)) = \prod_{\sigma \in \operatorname{Hom}_{\mathbb{Q}}(\mathbb{Q}(\theta),\overline{\mathbb{Q}})}(x - \sigma(\theta))^d = (m_{\theta,K})^d,$$

where $m_{\theta,K}$ is the minimal polynomial of θ over K. Thus the question of finding the minimal polynomial of θ can be reduced to finding the characteristic polynomial.

If $K = \mathbb{Q}(\alpha)$, $[K : \mathbb{Q}] = n$, then $\{1, \alpha, \ldots, \alpha^{n-1}\}$ is a $\mathbb{Q}$-basis of K and every $\theta \in K$ can be represented as

$$\theta = \frac{1}{m}\left(\sum_{0 \le i \le n-1} a_i \alpha^i\right),$$

where $m \in \mathbb{N}$, $a_j \in \mathbb{Z}$ and $\gcd(a_0, a_1, \ldots, a_{n-1}, m) = 1$. Using resultants, the characteristic polynomial can be computed using the following proposition.

Proposition 2.10. Let $K = \mathbb{Q}(\alpha)$ be a number field, where α is a root of a monic, irreducible polynomial $f(x) \in \mathbb{Z}[x]$ of degree n. Furthermore, let $\theta \in K$, where

$$\theta = \frac{1}{m}\left(\sum_{0 \leq i \leq n-1} a_i \alpha^i\right),$$

$m \in \mathbb{N}$, $a_j \in \mathbb{Z}$. Set $p(y) = \sum_{0 \leq i \leq n-1} a_i y^i \in \mathbb{Z}[y]$. Then the characteristic polynomial $C_{K,\theta}$ of θ in K is given by the formula

$$C_{K,\theta}(x) = m^{-n} R_y(f(y), mx - p(y)),$$

where R_y denotes the resultant taken with respect to the variable y (in other words, the coefficient ring is $\mathbb{Z}[x]$ and $f(y), mx - p(y)$ are treated as polynomials from $(\mathbb{Z}[x])[y]$).

Proof. Let $\mathrm{Hom}_{\mathbb{Q}}(K, \overline{\mathbb{Q}}) = \{\sigma_1, \ldots, \sigma_n\}$. Clearly, $\sigma_i(\theta) = \frac{1}{m} p(\sigma_i(\alpha))$ for every i. By the definition,

$$C_{K,\theta}(x) = \prod_{i=1}^{n}(x - \sigma_i(\theta)) = \prod_{i=1}^{n}(x - p(\sigma_i(\alpha))/m) = m^{-n}\prod_{i=1}^{n}(mx - p(\sigma_i(\alpha))).$$

By Proposition 2.7, $\sigma_i(\alpha)$, $i = 1, \ldots, n$ are the roots of $f(y)$ in $\overline{\mathbb{Q}}$. The latter expression is therefore equal to to $m^{-n} R_y(f(y), mx - p(y))$ by Remark 2.2. □

Example 2.11. Let $K = \mathbb{Q}(\sqrt{2})$. Using Proposition 2.10, we compute the characteristic polynomial of $\theta = 1 + \sqrt{2}$ in K. The minimal polynomial of $\sqrt{2}$ over $\mathbb{Q}$ is $f(y) = y^2 - 2$. Setting $p(y) = 1 + y$, the characteristic polynomial $C_{K,\theta}(x)$ of θ in K is equal to

$$R_y(f(y), x - p(y)) = R_y(y^2 - 2, x - (y + 1)) \in \mathbb{Z}[x].$$

Algorithm 2 with $R = \mathbb{Z}[x]$, $f(y) = y^2 - 2 \in R[y]$, $g(y) = -y + x - 1 \in R[y]$ runs as follows:

- (1: Initializations)
  $f \leftarrow y^2 - 2$, $g \leftarrow -y + x - 1$,
  $u \leftarrow 1$, $v \leftarrow 1$
- (2: Pseudo division)
  $\delta \leftarrow 1 = \deg_y(f) - \deg_y(g)$
  The algorithm for pseudo division yields $q \leftarrow -y + (1 - x)$, $r \leftarrow x^2 - 2x - 1$ (so that $(-1)^{\delta+1} f = gq + r$).
- (3: Reduce remainder)
  $f \leftarrow -y + x - 1$, $g \leftarrow x^2 - 2x - 1$.
- (4: Finished?)
  $u \leftarrow -1$, $v \leftarrow -1$.
  Since $\deg(g) = 0$, the output of the algorithm is $x^2 - 2x - 1$.

In conclusion, we see that the characteristic polynomial of $\theta = 1 + \sqrt{2}$ in $K = \mathbb{Q}(\sqrt{2})$ is $C_{K,\theta}(x) = x^2 - 2x - 1$. Since $\theta \notin \mathbb{Q}$, the degree of its minimal polynomial over $\mathbb{Q}$ must be greater 1 but also less than or equal to $2 = [K : \mathbb{Q}]$. The polynomial $x^2 - 2x - 1$ is therefore the minimal polynomial of θ.

Finally, we proceed to the Tschirnhausen transformation algorithm. Its input is an irreducible polynomial f of degree n with integer coefficients. We need not know explicitly what its roots are, but fix one, say, $\theta \in \overline{\mathbb{Q}}$. Consider the number field $K = \mathbb{Q}(\theta)$. The aim of the algorithm is to find an irreducible polynomial $g \in \mathbb{Z}[x]$ such that $K = \mathbb{Q}(\theta')$, where θ' is a root of g. It follows from Proposition 1.37 that the polynomials f and g have the same splitting field. From the perspective of finding the Galois group, the polynomial f may be replaced by g.

The algorithm is randomized: in the first step we choose n integer coefficients at random and then consider the resulting polynomial of degree at most $n-1$, which we denote by h. Next (Step 2), we compute the characteristic polynomial of $\theta' = h(\theta)$, using Proposition 2.10. If $C_{K,\theta'}$ isn't square-free, start with a new h. Since $\mathbb{Q}(\theta') \subseteq K$, it remains to be shown that $\mathbb{Q}(\theta') = K$ if and only if the characteristic polynomial $C_{K,\theta'}$ is square-free. By Remark 2.9, $C_{K,\theta'}$ is square-free iff $C_{K,\theta'} = m_{\theta',K}$ iff $[K : \mathbb{Q}(\theta')] = 1$.

Algorithm 6 Tschirnhausen Transformation

Input: Irreducible, monic polynomial $f \in \mathbb{Z}[x]$ defining a number field $K = \mathbb{Q}(\theta)$.

Output: Polynomial g defining the same number field.

1: Let $n \leftarrow \deg(f)$. Choose at random a polynomial $h \in \mathbb{Z}[y]$ of degree less than or equal to $n-1$

2: Using the sub-resultant algorithm, set $g \leftarrow R_y(f(y), x - h(y))$.

3: Compute $d \leftarrow \gcd(g, g')$. If d is constant, then output g and terminate the algorithm, otherwise go to Step 1.

2.2 A general theorem

A straightforward approach toward identifying the Galois group is described in [25, p. 189]. Though the resulting algorithm is impractical, it has an interesting

corollary.
Let $f \in \mathbb{Z}$ be monic and separable, $\deg(f) = n$, and $\alpha_1, \ldots, \alpha_n \in \overline{K}$ be the roots of f. Let L be the splitting field of f. Recall that there's a group action $*$ of $\mathcal{S}_n$ on $L[y_1, \ldots, y_n]$ defined as $\tau * g(y_1, \ldots, y_n) = g(y_{\tau(1)}, \ldots, y_{\tau(n)})$, where $g \in L[y_1, \ldots, y_n]$, $\tau \in \mathcal{S}_n$ (c.f. Proposition 1.11). We start by forming the expression

$$\theta(y_1, \ldots, y_n) = \alpha_1 y_1 + \cdots + \alpha_n y_n,$$

where $y_1, \ldots, y_n$ are variables - in other words, $\theta \in L[y_1, \ldots, y_n]$. Define the polynomial $F(y_1, \ldots, y_n, x)$ as follows:

$$F(y_1, \ldots, y_n, x) = \prod_{\tau \in \mathcal{S}_n} (x - \tau * \theta(y_1, \ldots, y_n)). \tag{2.3}$$

It follows that $F(y_1, \ldots, y_n, x) \in \mathbb{Z}[y_1, \ldots, y_n, x]$. To prove this fact, we need an auxiliary lemma.

Lemma 2.12. With the above notation, let $\sigma \in \mathrm{Gal}(L/K)$ and $\sigma' \in \mathrm{Gal}(f)$ be the corresponding element of $\mathcal{S}_n$ (i.e. $\sigma(\alpha_i) = \alpha_{\sigma'(i)}$ for every i). Then we have

$$\sigma' * (\sigma(\theta(y_1, \ldots, y_n))) = \theta(y_1, \ldots, y_n)$$

and consequently

$$\sigma(\theta(y_1, \ldots, y_n)) = (\sigma')^{-1} * \theta(y_1, \ldots, y_n).$$

Proof. By definition,

$$\sigma' * (\sigma(\theta(y_1, \ldots, y_n))) = \sigma' * (\alpha_{\sigma'(1)} y_1 + \cdots + \alpha_{\sigma'(n)} y_n) = \alpha_{\sigma'(1)} y_{\sigma'(1)} + \cdots + \alpha_{\sigma'(n)} y_{\sigma'(n)} = \\ = \theta(y_1, \ldots, y_n)$$

and the rest follows from Proposition 1.11. □

Lemma 2.13. Let $f \in \mathbb{Z}[x]$ be monic and separable, $\deg(f) = n$,

$$f(x) = x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0.$$

Let L be the splitting field of f, and $\alpha_1, \ldots, \alpha_n \in L$ the roots of f. Every coefficient of $F(y_1, \ldots, y_n, x)$, the polynomial defined by (2.3), is equal to $p(a_0, \ldots, a_{n-1})$ for some $p(x_1, \ldots, x_n) \in \mathbb{Z}[x_1, \ldots, x_n]$. In particular, $F(y_1, \ldots, y_n, x) \in \mathbb{Z}[y_1, \ldots, y_n, x]$.

Proof. If we view the roots $\alpha_1, \ldots, \alpha_n$ as formal indeterminates, it follows from (2.3) that F is symmetric as a polynomial in $(\mathbb{Z}[y_1, \ldots, y_n, x])[\alpha_1, \ldots, \alpha_n]$. By Theorem 1.14, there exists a polynomial G such that $F(\alpha_1, \ldots, \alpha_n) = G(s_1(\alpha_1, \ldots, \alpha_n), \ldots, s_n(\alpha$

where $s_1, \ldots, s_n$ are the elementary symmetric polynomials. In the field L, the following equalities hold:

$$\begin{aligned} a_{n-1} &= -s_1(\alpha_1, \ldots, \alpha_n), \\ a_{n-2} &= s_2(\alpha_1, \ldots, \alpha_n), \\ &\vdots \\ a_0 &= (-1)^n s_n(\alpha_1, \ldots, \alpha_n). \end{aligned} \tag{2.4}$$

Now it's clear that every coefficient of $F(y_1, \ldots, y_n, x) \in L[y_1, \ldots, y_n, x]$ is a polynomial expression in the a_i's. □

Theorem 2.14. Let $f \in \mathbb{Z}[x]$ be monic and separable, $\deg(f) = n$. Let L be the splitting field of f and $\alpha_1, \ldots, \alpha_n \in L$ the roots of f. Let

$$\theta(y_1, \ldots, y_n) = \alpha_1 y_1 + \cdots + \alpha_n y_n \in L[y_1, \ldots, y_n]$$

and

$$F(y_1, \ldots, y_n, x) = F_1(y_1, \ldots, y_n, x) F_2(y_1, \ldots, y_n, x) \cdots F_k(y_1, \ldots, y_n, x)$$

be the factorization in $\mathbb{Z}[y_1, \ldots, y_n, x]$ of $F(y_1, \ldots, y_n, x)$, where F is defined by (2.3). Let the factors of F be labeled in such a way that $F_1(y_1, \ldots, y_n, x)$ is divided by $x - \theta(y_1, \ldots, y_n)$ in $L[y_1, \ldots, y_n, x]$. Define

$$G = \{\tau \in \mathcal{S}_n \mid F_1(y_1, \ldots, y_n, x) = F_1(y_{\tau(1)}, \ldots, y_{\tau(n)}, x)\}.$$

Then $G = \mathrm{Gal}(f)$, where $\mathrm{Gal}(f)$ is the Galois group of f with respect to the given order $\alpha_1, \ldots, \alpha_n$ of the roots of f.

Remark 2.15. The set G is clearly a subgroup of $\mathcal{S}_n$. To prove the theorem, we need two lemmata.

Note 2.16. In [25], the statement of Lemma 2.18 is given without a proof.

Lemma 2.17. Under the assumptions of Theorem 2.14, the group G consists precisely of those permutations $\tau \in \mathcal{S}_n$ such that $x - \tau * \theta(y_1, \ldots, y_n)$ is again a factor of F_1 in $L[y_1, \ldots, y_n, x]$.

Proof. Let $F_1(y_1, \ldots, y_n, x) = \prod_{i=1}^{l}(x - \theta_i(y_1, \ldots, y_n)$, where $\theta_1 = \theta, \ldots, \theta_l \in L[y_1, \ldots, y_n]$ is a suitably chosen sequence of polynomials (i.e. $\theta_i = \pi_i * \theta$ for some $\pi_i \in \mathcal{S}_n$). If $\tau \in G$ then $F_1(y_1, \ldots, y_n, x) = F_1(y_{\tau(1)}, \ldots, y_{\tau(n)}, x) = \prod_{i=1}^{k}(x - \tau * \theta_i(y_1, \ldots, y_n))$ and τ clearly maps $x - \theta(y_1, \ldots, y_n)$ onto another factor of F_1. Conversely, let $\tau \in \mathcal{S}_n$ transform $x - \theta(y_1, \ldots, y_n)$ into another factor of F_1. Note that τ induces an automorphism of $L[y_1, \ldots, y_n, x]$ that maps a polynomial $H(y_1, \ldots, y_n, x)$ to $H(y_{\tau(1)}, \ldots, y_{\tau(n)}, x)$. The polynomial F is fixed by τ:

$$\begin{aligned} F(y_{\tau(1)}, \ldots, y_{\tau(n)}, x) &= \prod_{\sigma \in \mathcal{S}_n} (x - \tau * (\sigma * \theta(y_1, \ldots, y_n))) = \\ &= \prod_{\sigma \in \mathcal{S}_n} (x - (\tau\sigma) * \theta(y_1, \ldots, y_n))) = F(y_1, \ldots, y_n, x). \end{aligned}$$

Furthermore, $F_1(y_{\tau(1)}, \ldots, y_{\tau(n)}, x) \in \mathbb{Z}[y_1, \ldots, y_n, x]$ is irreducible and divides

$$F(y_1, \ldots, y_n, x).$$

Therefore, $F_1(y_{\tau(1)}, \ldots, y_{\tau(n)}, x)$ is equal to $F_i(y_1, \ldots, y_n, x)$ for some $i \in \{1, \ldots, k\}$. Since it has a factor in common with F_1 in $L[y_1, \ldots, y_n, x]$, $F_1(y_{\tau(1)}, \ldots, y_{\tau(n)}, x) = F_1(y_1, \ldots, y_n, x)$ and $\tau \in G$. □

Lemma 2.18. Let $\tau \in \mathcal{S}_n$. Under the hypotheses of Theorem 2.14, $\tau \in \mathrm{Gal}(f)$ iff $x - \tau^{-1} * \theta(y_1, \ldots, y_n)$ is a factor of F_1 in $L[y_1, \ldots, y_n, x]$.

Remark 2.19. The expression $\tau^{-1} * \theta(y_1, \ldots, y_n)$ equals to $\theta(y_1, \ldots, y_n)$ with the coefficients interchanged according to the permutation τ:

$$\tau^{-1} * (\alpha_1 y_1 + \cdots + \alpha_n y_n) = \alpha_{\tau(1)} y_1 + \cdots + \alpha_{\tau(n)} y_n.$$

Proof. Again, let

$$F_1(y_1, \ldots, y_n, x) = \prod_{i=1}^{l} (x - \theta_i(y_1, \ldots, y_n)),$$

where $\theta_1 = \theta, \ldots, \theta_l \in L[y_1, \ldots, y_n]$ is a suitably chosen sequence of polynomials. Let $\tau \in \mathcal{S}_n$ be such that $\tau^{-1} * \theta = \theta_i$, $i \in \{1, \ldots, l\}$. We want to show that $\tau \in \mathrm{Gal}(f)$. The polynomial $F_1 \in \mathbb{Z}[y_1, \ldots, y_n, x] = (\mathbb{Z}[y_1, \ldots, y_n])[x]$ is irreducible and, with respect to the variable x, monic. It is therefore primitive and, by Gauss's lemma, F_1 is irreducible as a polynomial in $T[x]$, where $T = \mathbb{Q}(y_1, \ldots, y_n)$ is the quotient field of the UFD $\mathbb{Z}[y_1, \ldots, y_n]$. Denote $T' = L(y_1, \ldots, y_n)$ and note that $\theta, \theta_i \in T'$ are algebraic over T (they are both roots of $F_1 \in T[x]$). By Lemma 1.16, there's a field homomorphism (a T-homomorphism in fact)

$$\phi : T(\theta) \to T(\theta_i)$$

such that $\phi(\theta) = \theta_i$. Let $\overline{T}$ be an algebraic closure of T. By Proposition 1.18, ϕ can be lifted to an automorphism $\bar{\phi}$ of $\overline{T}$. The extension T'/T is clearly algebraic and we can assume $T' \subseteq \overline{T}$. In particular, $L \subseteq \overline{T}$. As the fields $\overline{\mathbb{Q}}, \bar{\phi}(\overline{\mathbb{Q}}) \subseteq \overline{T}$ are algebraic over $\mathbb{Q}$, $\bar{\phi}(\overline{\mathbb{Q}}) = \overline{\mathbb{Q}}$ and since $L/\mathbb{Q}$ is normal, the restriction of $\bar{\phi}$ to L is an element of $\mathrm{Gal}(L/K)$. The corresponding element of $\mathcal{S}_n$ is then equal to τ, in other words, $\tau \in \mathrm{Gal}(f)$.

To prove the converse - that $x - \tau^{-1} * \theta(y_1, \ldots, y_n)$ is a factor of F_1, provided that $\tau \in \mathrm{Gal}(f)$, let $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ be the automorphism corresponding to τ (i.e. $\sigma(\alpha_i) = \alpha_{\tau(i)}$ for every i). Since $F_1 \in \mathbb{Z}[y_1, \ldots, y_n, x]$ has integral coefficients, it remains fixed under σ:

$$F_1(y_1, \ldots, y_n, x) = \sigma(F_1(y_1, \ldots, y_n, x)) = \prod_{i=1}^{l} (x - \sigma(\theta_i(y_1, \ldots, y_n)).$$

By Lemma 2.12, the product is equal to $\prod_{i=1}^{l} (x - \tau^{-1} * \theta_i(y_1, \ldots, y_n))$. It is clear now that $x - \tau^{-1} * \theta(y_1, \ldots, y_n)$ is a factor of F_1. □

Proof of Theorem 2.14. By Lemma 2.18, $\tau \in \mathrm{Gal}(f)$ iff $x - \tau^{-1} * \theta(y_1, \ldots, y_n)$ is a factor of F_1 in $L[y_1, \ldots, y_n, x]$. By Lemma 2.17, the latter is true iff $\tau^{-1} \in G$. Since G is a subgroup of $\mathcal{S}_n$, we see that $\tau \in \mathrm{Gal}(f) \iff \tau \in G$. □

Theorem 2.14 holds also for finite fields (with analogous proof).

Theorem 2.20. Let $p \in \mathbb{N}$ be a prime, $f \in \mathbb{F}_p[x]$ be monic and separable, $\deg(f) = n$. Let L be the splitting field of f and $\alpha_1, \ldots, \alpha_n \in L$ the roots of f. Let

$$\theta(y_1, \ldots, y_n) = \alpha_1 y_1 + \cdots + \alpha_n y_n \in L[y_1, \ldots, y_n]$$

and define

$$F(y_1, \ldots, y_n, x) = \prod_{\pi \in \mathcal{S}_n} (x - \pi * \theta(y_1, \ldots, y_n)).$$

Then $F \in \mathbb{F}_p[y_1, \ldots, y_n, x]$. Let

$$F(y_1, \ldots, y_n, x) = F_1(y_1, \ldots, y_n, x)F_2(y_1, \ldots, y_n, x) \cdots F_k(y_1, \ldots, y_n, x)$$

be the factorization of F in $\mathbb{F}_p[y_1, \ldots, y_n, x]$ and let the factors of F be labeled in such a way that $x - \theta(y_1, \ldots, y_n)$ divides F_1 in $L[x_1, \ldots, x_n]$. Now, define

$$G = \{\tau \in \mathcal{S}_n : F_1(y_1, \ldots, y_n, x) = F_1(y_{\tau(1)}, \ldots, y_{\tau(n)}, x)\}.$$

Then $G = \mathrm{Gal}(f)$, where $\mathrm{Gal}(f)$ is the Galois group of f with respect to the given order $\alpha_1, \ldots, \alpha_n$ of the roots of f.

Corollary 2.21. Let $f \in \mathbb{Z}[x]$ be monic and separable, $\alpha_1, \ldots, \alpha_n \in \overline{\mathbb{Q}}$ the roots of f and let $\mathrm{Gal}(f)$ be the Galois group of f with respect to this order of the roots. Let $p \in \mathbb{Z}$ be a prime such that $p \nmid \mathrm{disc}(f)$ and $\bar{f} \in \mathbb{F}_p[x]$ be the polynomial derived from f by reducing its coefficients modulo p. Then the Galois group $\mathrm{Gal}(\bar{f})$ (as a permutation group with respect to a suitable order of the roots of $\bar{f}$) is a subgroup of $\mathrm{Gal}(f)$.

Proof. Although the polynomial $\bar{f} \in \mathbb{F}_p[x]$ may be reducible, the condition $p \nmid \mathrm{disc}(f)$ ensures that $\bar{f}$ is separable. Let $F(y_1, \ldots, y_n, x) \in \mathbb{Z}[y_1, \ldots, y_n, x]$ be the polynomial from Theorem 2.14 defined by (2.3) and let $\overline{F}(y_1, \ldots, y_n, x) \in \mathbb{F}_p[y_1, \ldots, y_n, x]$ be the corresponding polynomial with respect to $\bar{f}$. Denote by π the homomorphism $\mathbb{Z} \to \mathbb{F}_p$,

$$\pi(z) = z \bmod p.$$

Clearly, $\pi(f) = \bar{f}$. We show that $\pi(F) = \overline{F}$. Let $a_0, \ldots, a_{n-1} \in \mathbb{Z}$ be the coefficients of f and $b_0, \ldots, b_{n-1} \in \mathbb{F}_p$ the coefficients of $\bar{f}$ (i.e. $b_i = a_i \bmod p$ for every i). By Lemma 2.13, for every coefficient of F, there is $p(x_1, \ldots, x_n) \in \mathbb{Z}[x_1, \ldots, x_n]$ such that the coefficient is equal to $p(a_0, \ldots, a_{n-1})$. The corresponding coefficient of $\overline{F}$ is then equal to $p(b_1, \ldots, b_{n-1}) \bmod p$. In other words, $\pi(F) = \overline{F}$ Now, let

$$F(y_1, \ldots, y_n, x) = F_1(y_1, \ldots, y_n, x)F_2(y_1, \ldots, y_n, x) \cdots F_k(y_1, \ldots, y_n, x)$$

be the factorization of F in $\mathbb{Z}[y_1, \ldots, y_n, x]$. Then

$$\overline{F}(y_1, \ldots, y_n, x) = \overline{F_1}(y_1, \ldots, y_n, x)\overline{F_2}(y_1, \ldots, y_n, x) \cdots \overline{F_k}(y_1, \ldots, y_n, x),$$

where $\overline{F_i} = \pi(F_i)$ (and these polynomials may be reducible). If $\tau \notin \mathrm{Gal}(f)$ then τ maps F_1 onto another factor of F, i.e. $F_1(y_{\tau(1)}, \ldots, y_{\tau(n)}, x) \neq F_1(y_1, \ldots, y_n, x)$. In particular, any irreducible divisor of $\overline{F_1}$ is mapped this way onto another irreducible factor of $\overline{F}$ and $\tau \notin \mathrm{Gal}(\bar{f})$ by Theorem 2.20. □

Note 2.22. Let $\mathbb{Q}(\alpha)$ be a number field, $\alpha \in \overline{\mathbb{Q}}$, and let f be the minimal polynomial of α over $\mathbb{Q}$. Let $\mathrm{Gal}(f)$ be the Galois group of f with respect to some order of the roots of f. By [14], there's an algorithm to compute all subfields $\mathbb{Q}(\beta) \subseteq \mathbb{Q}(\alpha)$ of a given degree. The algorithm works with cyclic subgroups of $\mathrm{Gal}(f)$ and Corollary 2.21 provides a theoretical foundation of it.

Proposition 2.23. Let $f \in \mathbb{Z}[x]$ be monic and irreducible and let $p \in \mathbb{Z}$ be a prime such that $p \nmid \operatorname{disc}(f)$. Let $\bar{f} \in \mathbb{F}_p[x]$ be the polynomial derived from f by reducing its coefficients modulo p. If $\bar{f} = \bar{f}_1 \cdots \bar{f}_k$ is the factorization of $\bar{f}$ in $\mathbb{F}_p[x]$ and $d_i = \deg(\bar{f}_i)$, $i = 1, \ldots, k$, then $\operatorname{Gal}(f)$, the Galois group of f with respect to a fixed order of the roots, contains a permutation of the cycle type $(d_1, \ldots, d_k)$.

Proof. By Corollary 2.21, we can arrange the order of the roots $\alpha_1, \ldots, \alpha_n$ of $\bar{f}$ in such a way that $\operatorname{Gal}(\bar{f}) \subseteq \operatorname{Gal}(f)$. Hence it suffices to show that $\operatorname{Gal}(\bar{f})$ contains a permutation of the cycle type $(d_1, \ldots, d_k)$. By Theorem 1.50, $\operatorname{Gal}(\bar{f})$ is cyclic. Let τ be the generating permutation and let $\tau = (i_1 \ldots i_j)(i_{j+1} \ldots) \ldots$ be its representation as a product of disjoint cycles, $i_1, i_2, \ldots \in \{1, \ldots, n\}$. It follows that each cycle of τ corresponds to an orbit of transitivity of the action of $\operatorname{Gal}(\bar{f})$ on the roots of $\bar{f}$. For example, the roots $\alpha_{i_1}, \ldots, \alpha_{i_j}$ form an orbit corresponding to the cycle $(i_1, \ldots, i_j)$. We also know, by Proposition 1.32, that each orbit of transitivity corresponds to an irreducible factor of $\bar{f}$. This means, that the cycle type of τ is the same as the list of degrees of the irreducible factors of $\bar{f}$. □

Example 2.24 ([25], Exercise 1, p. 192)**.** We show that the Galois group of the polynomial

$$f(x) = x^4 + 2x^2 + x + 3 \in \mathbb{Q}[x]$$

is isomorphic to $\mathcal{S}_4$. The polynomial f is irreducible (as shown below) and $\operatorname{Gal}(f)$ is a transitive subgroup of S_4 by Proposition 1.32. The factorization of f mod 3 in $\mathbb{F}_3[x]$ is $x(x^3 + 2x + 1)$ and so $\operatorname{Gal}(f)$ contains a 3-cycle by Proposition 2.23. Let the 3-cycle be (123) (this can be always achieved by possibly rearranging the roots of f). The factorization of f mod 5 in $\mathbb{F}_5$ is $(x + 1)(x + 2)(x^2 + 2x + 4)$ and so $\operatorname{Gal}(f)$ contains a transposition (kl). Since $\operatorname{Gal}(f)$ is transitive, there's a permutation $\sigma \in \operatorname{Gal}(f)$ such that $\sigma(l) = 4$ and $\operatorname{Gal}(f)$ contains also the permutation

$$\sigma \circ (kl) \circ \sigma^{-1} = (\sigma(k)\ \sigma(l)) = (\sigma(k)\ 4).$$

Using the transposition $(\sigma(k)\ 4)$ and the cycle (123), one can obtain the three transpositions (14), (24) and (34). But these transpositions already generate $\mathcal{S}_4$ - any transposition $(ij) \in \mathcal{S}_4$ may be written as the product $(j4)(i4)(j4)$, $i, j \in \{1, 2, 3\}$, and $\mathcal{S}_4$ is generated by the set of the transpositions in $\mathcal{S}_4$.

Let's show that f is irreducible in $\mathbb{Q}[x]$. Using Proposition 1.41, it's easily verified that f has no rational root. To be reducible, it would have to be a factor of two degree 2 polynomials. Since f is primitive, it is irreducible in $\mathbb{Q}[x]$ iff it's irreducible in $\mathbb{Z}[x]$. Assume, for the sake of contradiction, that

$$f(x) = x^4 + 2x^2 + x + 3 = (x^2 + ax + b)(x^2 + cx + d),$$

where $a, b, c, d \in \mathbb{Z}$. Since $bd = 3$, either $b = 1$ or $b = 3$. If $b = 3$ then $d = 1$ and we can expand $f(x) = (x^2 + ax + 3)(x^2 + cx + 1) = x^4 + (a + c)x^3 + (4 + ac)x^2 + (3c + a)x + 3$, whence $a + c = 0$, $ac = -2$ and $3c + a = 1$. This set of equations has no solution in $\mathbb{Z}$.

If $b = 1$ and $d = 3$, we similarly derive $a + c = 0$, $ac = -2$ and $3a + c = 1$ and this set of equations also has no solution in $\mathbb{Z}$. We have arrived at a contradiction and $f \in \mathbb{Q}[x]$ is irreducible.

2.3 The resolvent polynomial

The aim of this section is to present the theory used in [23]. As we have seen, the symmetric group acts on $\mathbb{Q}[x_1, \ldots, x_n]$ by reordering the indeterminates:

$$\tau * f(x_1, \ldots, x_n) = f(x_{\tau(1)}, \ldots, x_{\tau(n)}),$$

where $f \in \mathbb{Q}[x_1, \ldots, x_n]$, $\tau \in \mathcal{S}_n$.

Lemma 2.25. Let L be the splitting field of $f \in \mathbb{Z}[x]$, where f is monic and separable. If $\alpha_1, \ldots, \alpha_n$ are the roots of f in L, $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ and $P \in \mathbb{Z}[x_1, \ldots, x_n]$ then

$$\sigma(P(\alpha_1, \ldots, \alpha_n)) = (\sigma' * P)(\alpha_1, \ldots, \alpha_n),$$

where $\sigma' \in \mathcal{S}_n$ is the permutation such that $\sigma(\alpha_i) = \alpha_{\sigma'(i)}$ for every i.

Proof. As σ fixes $\mathbb{Q}$, we have

$$\sigma(P(\alpha_1, \ldots, \alpha_n)) = P(\sigma(\alpha_1), \ldots, \sigma(\alpha_n)) = P(\alpha_{\sigma'(1)}, \ldots, \alpha_{\sigma'(n)}) = (\sigma' * P)(\alpha_1, \ldots, \alpha_n).$$

□

Definition 2.26. Let $P \in \mathbb{Z}[x_1, \ldots, x_n]$ and $H \subseteq G \subseteq \mathcal{S}_n$. We call P a G-relative H-invariant if

$$\tau * P = P \text{ for every } \tau \in H$$

and

$$\tau * P \neq P \text{ if } \tau \in G \setminus H.$$

Another way to express this is to say that $\mathrm{Stab}_G(P) = H$. If $G = \mathcal{S}_n$, we simply call P a H-invariant.

Proposition 2.27. For every pair $H \subseteq G$ of subgroups of $\mathcal{S}_n$, there exists a G-relative H-invariant $P \in \mathbb{Z}[x_1, \ldots, x_n]$.

Proof. Define $\tilde{P}(x_1, \ldots, x_n) = x_1^1 x_2^2 \cdots x_n^n$ and $P(x_1, \ldots, x_n) = \sum_{\tau \in H} \tau * \tilde{P}(x_1, \ldots, x_n)$. If $\tau \in H$ then $\tau * F = F$ because τ merely changes the order of the terms of P. Furthermore, every term of P is equal to $x_1^{\tau^{-1}(1)} \cdots x_n^{\tau^{-1}(n)}$ for some $\tau \in H$ and if $\tau \notin H$ then $\tau * P \neq P$. □

The task of finding a G-relative H-invariant P for a given pair $H \subseteq G$ of permutation groups is central to the Stauduhar's algorithm, which will be presented in the next section. It's also advantageous for $\deg(P)$ to be as low as possible. From this point of view, Proposition 2.27, where $\deg(P) = 1 + \cdots + n = n(n+1)/2$, isn't very useful. There are, however, algorithms that deal specifically with the problem of finding a G-relative H-invariant polynomial of a low degree. That is, given the groups $H \subseteq G$, the goal is to find a G-relative H-invariant P with $\deg(P) < n(n+1)/2$. For this, see [10, p. 5].

Lemma 2.28. Let $P \in \mathbb{Z}[x_1, \ldots, x_n]$ be a G-relative H-invariant, $H \subseteq G \subseteq \mathcal{S}_n$. Then the length of the orbit of P under the action of G is equal to $[G : H]$.

Proof. This is a direct consequence of Lemma 1.10. □

Proposition 2.29. Let $P \in \mathbb{Z}[x_1, \ldots, x_n]$ be a G-relative H-invariant, $H \subseteq G \subseteq \mathcal{S}_n$. If $\tau \in G$ then $\tau * P$ is a G-relative H'-invariant, where $H' = G \cap \tau H \tau^{-1}$.

Proof. The polynomial $\tau * P$ is a G-relative H'-invariant, where

$$H' = \{\tau' \in G : \tau' * (\tau * P) = \tau * P\}.$$

By Proposition 1.11, $H' = \{\tau' \in G : (\tau^{-1}\tau'\tau) * P = P\}$ and the latter set is clearly equal to $G \cap \tau H \tau^{-1}$. □

Definition 2.30 (Resolvent polynomial)**.** Let $f \in \mathbb{Z}[x]$ be monic and irreducible of degree n and $\alpha_1, \ldots, \alpha_n \in \overline{\mathbb{Q}}$ the roots of f. Let G be a transitive subroup of $\mathcal{S}_n$ such that $\mathrm{Gal}(f) \subseteq G$. Let $H \subseteq G$ and let $P[x_1, \ldots, x_n] \in \mathbb{Z}[x_1, \ldots, x_n]$ be a G-relative H-invariant. If $G * P = \{P_1, \ldots, P_k\}$ is the orbit of P under the action of G on $\mathbb{Q}[x_1, \ldots, x_n]$, define the resolvent polynomial associated with P, f, and G as:

$$R^G_{(P,f)}(x) = \prod_{i=1}^{k} (x - P_i(\alpha_1, \ldots, \alpha_n)). \tag{2.5}$$

By Lemma 2.28, the length of the orbit $G * P = \{P_1, \ldots, P_k\}$ is $k = [G : H]$. It can also be looked at as $\{\tau_1 * P, \ldots, \tau_k * P\}$, where $\tau_i \in G$ and $\tau_1 H, \ldots, \tau_k H$ are the k distinct cosets of G modulo H. For any $\pi \in G$, $\pi\tau_1 H, \ldots, \pi\tau_k H$ is again a partition of G into k distinct cosets. Hence $G * P = \{\pi * P_1, \ldots, \pi * P_k\}$. We use this fact in the following lemma.

Lemma 2.31. The resolvent polynomial $R^G_{(P,f)}$ defined above has integral coefficients.

Proof. Let $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$, where L is the splitting field of f, and let $\sigma' \in \mathrm{Gal}(f)$ such that $\sigma(\alpha_i) = \alpha_{\sigma'(i)}$ for every $i = 1, \ldots, n$. By Lemma 2.25, we have

$$\sigma(R^G_{(P,f)}) = \prod_{i=1}^{k} (x - \sigma(P_i(\alpha_1, \ldots, \alpha_n))) = \prod_{i=1}^{k} (x - (\sigma' * P_i)(\alpha_1, \ldots, \alpha_n)) = R^G_{(F,f)}$$

because $\mathrm{Gal}(f) \subseteq G$ and $\{\sigma' * P_1, \ldots, \sigma' * P_k\} = \{P_1, \ldots, P_k\}$. By Corollary 1.31, it follows that the coefficients of $R^G_{(P,f)}$ are in $\mathbb{Q}$. By Proposition 1.40, $P_i(\alpha_1, \ldots, \alpha_n)$ is an algebraic integer for every i and the coefficients of $R^G_{(P,f)}$ are therefore algebraic integers. Hence $R^G_{(P,f)}(x) \in \mathbb{Z}[x]$ by Corollary 1.42. □

Although the polynomials $P_1, \ldots, P_k$ are formally distinct, the values $P_i(\alpha_1, \ldots, \alpha_n)$ (i.e. the roots of $R^G_{(P,f)}$) may not be distinct.

Example 2.32. The polynomial $f(x) = x^4 + 1 \in \mathbb{Z}[x]$ is irreducible and its roots are

$$\alpha_1 = \frac{\sqrt{2}}{2}(-1 + i),\ \alpha_2 = \frac{\sqrt{2}}{2}(1 + i),\ \alpha_3 = \frac{\sqrt{2}}{2}(1 - i),\ \alpha_4 = \frac{\sqrt{2}}{2}(-1 - i).$$

Let

$$P_1(x_1, x_2, x_3, x_4) = x_1x_2^2 + x_2x_3^2 + x_3x_4^2 + x_4x_1^2,$$

and

$$P_2(x_1, x_2, x_3, x_4) = (14)(23) * P_1(x_1, x_2, x_3, x_4) = x_2x_1^2 + x_3x_2^2 + x_4x_3^2 + x_1x_4^2.$$

Then $P_1(\alpha_1, \alpha_2, \alpha_3, \alpha_4) = P_2(\alpha_1, \alpha_2, \alpha_3, \alpha_4) = 0$.

One of the roots of the polynomial $R^G_{(P,f)}$ defined above is $P(\alpha_1, \ldots, \alpha_n)$ because $P \in G * P$. The following proposition can be used when the root $P(\alpha_1, \ldots, \alpha_n)$ is simple.

Proposition 2.33. Let $f \in \mathbb{Z}[x]$ be monic and irreducible of degree n and $\alpha_1, \ldots, \alpha_n \in \overline{\mathbb{Q}}$ the roots of f. Let G be a transitive subroup of $\mathcal{S}_n$ such that $\mathrm{Gal}(f) \subseteq G$. Let $H \subseteq G$ and $P[x_1, \ldots, x_n] \in \mathbb{Z}[x_1, \ldots, x_n]$ be a G-relative H-invariant. If $R^G_{(P,f)}$ is the resolvent polynomial associated with P, f and G and its root $P(\alpha_1, \ldots, \alpha_n)$ is simple then the equivalence

$$\mathrm{Gal}(f) \subseteq H \iff P(\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}$$

holds. The implication $\implies$ holds even if $P(\alpha_1, \ldots, \alpha_n)$ is a multiple root.

Proof. Let L be the splitting field of f. For $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$, we denote by σ' the corresponding permutation in $\mathrm{Gal}(f)$ (i.e. $\sigma(\alpha_i) = \alpha_{\sigma'(i)}$ for every i). If $\mathrm{Gal}(f) \subseteq H$, $\sigma(P(\alpha_1, \ldots, \alpha_n)) = (\sigma' * P)(\alpha_1, \ldots, \alpha_n) = P(\alpha_1, \ldots, \alpha_n)$ for every $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$, where the first equality follows from Lemma 2.25. By Corollary 1.31, $P(\alpha_1, \ldots, \alpha_n) \in \mathbb{Q}$. As noted before, $P(\alpha_1, \ldots, \alpha_n)$ is an algebraic integer, which means that $P(\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}$ by Lemma 1.42.

Let $\tau \in G$. Since $P(\alpha_1, \ldots, \alpha_n)$ is a non-repeated root of $R^G_{(P,f)}$, the following equivalence holds:

$$(\tau * P)(\alpha_1, \ldots, \alpha_n) = P(\alpha_1, \ldots, \alpha_n) \iff \tau \in H$$

Thus if $P(\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}$, we have

$$(\sigma' * P)(\alpha_1, \ldots, \alpha_n) = \sigma(P(\alpha_1, \ldots, \alpha_n)) = P(\alpha_1, \ldots, \alpha_n)$$

for every $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ and therefore $\mathrm{Gal}(f) \subseteq H$. □

Corollary 2.34. Under the assumptions of Proposition 2.33, let $P_i = \tau * P$, $\tau \in G$, and let $P_i(\alpha_1, \ldots, \alpha_n)$ be a non repeated root of $R^G_{(P,f)}$. Then

$$\mathrm{Gal}(f) \subseteq \tau H \tau^{-1} \iff P_i(\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}.$$

The implication $\implies$ holds even if $P_i(\alpha_1, \ldots, \alpha_n)$ is a multiple root.

Proof. First note that $R^G_{(P_i,f)} = R^G_{(P,f)}$. By Proposition 2.29, $P_i = \tau * P$ is a G-relative H'-invariant, where $H' := G \cap \tau H \tau^{-1}$. As Proposition 2.33 applies here, $(\tau * P)(\alpha_1, \ldots, \alpha_n)$ is a simple root iff $\mathrm{Gal}(f) \subseteq G \cap \tau H \tau^{-1} \subseteq \tau H \tau^{-1}$. □

Remark 2.35. As noted previously, the Galois group $\mathrm{Gal}(f) \subseteq \mathcal{S}_n$ depends on how the roots of f are arranged: if $\mathrm{Gal}(f)$ corresponds to $\alpha_1, \ldots, \alpha_n$ in this order and $\tau \in \mathcal{S}_n$, then $\tau^{-1}\mathrm{Gal}(f)\tau$ is the Galois group with respect to $\alpha'_1, \ldots, \alpha'_n$, where $\alpha'_i = \alpha_{\tau(i)}$.

Corollary 2.36. Let the assumptions of Proposition 2.33 hold. Suppose $P_i(\alpha_1, \ldots, \alpha_n)$ is a simple root of $R^G_{(P,f)}$ and that $P_i(\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}$. By Corollary 2.34, $\mathrm{Gal}(f) \subseteq \tau H \tau^{-1}$, where $P_i = \tau * P$, $\tau \in G$. If the roots of f are reordered according to the rule $\alpha'_i = \alpha_{\tau(i)}$ then $\mathrm{Gal}(f) \subseteq H$ (where $\mathrm{Gal}(f)$ is understood with respect to $(\alpha'_1, \ldots, \alpha'_n)$).

2.4 Stauduhar's method of finding the Galois group

This method was introduced by Richard Stauduhar in [23]. The input is a monic and irreducible polynomial f and high-precision approximations $\alpha_1, \ldots, \alpha_n$ to the roots of f. By Proposition 1.32, the Galois group of f is a transitive subgroup of $\mathcal{S}_n$. Throughout the course of the algorithm a table with all transitive subgroups of $\mathcal{S}_n$ is used, where $n = \deg(f)$. Such a table exists for every $n \leq 31$ [12].
Let $H \subsetneq \mathcal{S}_n$ be a (proper) transitive subgroup, maximal among the transitive subgroups of $\mathcal{S}_n$ (i.e. if $H \subsetneq H'$ and H' is transitive then $H' = \mathcal{S}_n$). By Proposition 2.27, there's a H-invariant polynomial $P \in \mathbb{Z}[x_1, \ldots, x_n]$. To start with, we know that $\mathrm{Gal}(f) \subseteq G = \mathcal{S}_n$ and we can use Corollary 2.34 to determine whether $\mathrm{Gal}(f)$ or some its conjugates is a subset of H. If $R^G_{(P,f)}$ is square-free and doesn't have an integral root, we know that no matter how we order the roots, $\mathrm{Gal}(f) \not\subseteq H$, and we can choose H to be another proper transitive subgroup of G, maximal among the transitive subgroups of $\mathcal{S}_n$. If $\mathrm{Gal}(f)$ isn't contained in any proper transitive subgroup of G then $\mathrm{Gal}(f) = G$. Suppose, on the other hand, that $(\tau * P)(\alpha_1, \ldots, \alpha_n)$ is a simple and integral root of $R^G_{(P,f)}$. Then, by Corollary 2.34, $\mathrm{Gal}(f) \subseteq \tau H \tau^{-1}$ and after renaming the roots according to τ (c.f. Corollary 2.36) we get that $\mathrm{Gal}(f) \subseteq H$. Then we set $G := H$ an repeat the procedure. If there's no proper transitive subgroup H of G then $\mathrm{Gal}(f) = G$.

2.5 Example: Degree 4

If $\deg(f) = 4$, $\mathrm{Gal}(f)$ is a transitive subgroup of $\mathcal{S}_4$ isomorphic to either

$$\begin{aligned}
\mathcal{C}_4 &= \langle (1234) \rangle, \text{ the cyclic group of order four,} \\
\mathcal{C}_2^2 &= \{id, (12)(34), (14)(23), (13)(24)\}, \text{ the normal Klein 4-group,} \\
\mathcal{D}_8 &= \langle (1234), (13) \rangle, \text{ the dihedral group of order 8,} \\
\mathcal{A}_4 &= \langle (123), (12)(34) \rangle, \text{ the group of even permutations,} \\
\mathcal{S}_4 &= \langle (1234), (12) \rangle, \text{ the whole group.}
\end{aligned}$$

Figure 2.1 shows the simplified inclusion diagram (simplified because there are three groups conjugate to $\mathcal{D}_8$ and three groups conjugate to $\mathcal{C}_4$ - the diagram doesn't show all of them). Before we give a formal description of the algorithm, here's a brief overview and examples. To start with, one computes $\mathrm{disc}(f)$ to decide whether $\mathrm{Gal}(f)$ is a subgroup of $\mathcal{A}_4$ (as in Proposition 1.46). Then we use the $\mathcal{D}_8$-invariant polynomial

$$P(x_1, x_2, x_3, x_4) = x_1 x_3 + x_2 x_4$$

to compute the resolvent polynomial $R^{\mathcal{S}_4}_{(P,f)}$. Using Corollary 2.36, we then decide whether $\mathrm{Gal}(f)$ is a subgroup of $\mathcal{D}_8$ or not. That leaves us with four possible options:

- If $\mathrm{Gal}(f) \subseteq \mathcal{A}_4 \cap \mathcal{D}_8$, conclude $\mathrm{Gal}(f) = \mathcal{C}_2^2$.
- If $\mathrm{Gal}(f) \subseteq \mathcal{A}_4$ and if $\mathrm{Gal}(f) \not\subseteq \mathcal{D}_8$, conclude $\mathrm{Gal}(f) = \mathcal{A}_4$.

- If $\mathrm{Gal}(f) \not\subseteq \mathcal{A}_4$ and $\mathrm{Gal}(f) \not\subseteq \mathcal{D}_8$, conclude $\mathrm{Gal}(f) = \mathcal{S}_4$.

The last option is that $\mathrm{Gal}(f) \subseteq \mathcal{D}_8$ (possibly after reordering the roots of f). In this case, we set $G = \mathcal{D}_8$, $H = \mathcal{C}_4$ and use the G-relative H-invariant polynomial

$$P(x_1, x_2, x_3, x_4) = x_1x_2^2 + x_2x_3^2 + x_3x_4^2 + x_4x_1^2$$

to compute the resolvent polynomial $R^G_{(P,f)}$. Again, using Corollary 2.36, we then decide whether $\mathrm{Gal}(f)$ (or some of its conjugates) is equal to H.

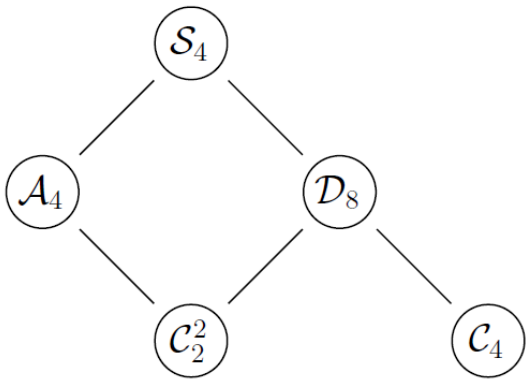

Figure 2.1: Transitive subgroups of $\mathcal{S}_4$

One aspect of the algorithm we have so far neglected is that the resolvent polynomial $R^G_{(P,f)}$ might not be square-free. There's a proof in [11, Theorem 3, (2)] that applying a Tschirnhausen transformation on f eventually leads to square-free $R^G_{(P,f)}$. Before giving examples, let's prove that the above assertions about P were correct.

Lemma 2.37. The polynomial

$$P(x_1, x_2, x_3, x_4) = x_1x_3 + x_2x_4$$

is a $\mathcal{D}_8$-invariant.

Proof. We denote by

$$\mathrm{Stab}(P) = \{\tau \in \mathcal{S}_4 \mid \tau * P = P\}.$$

Since $\mathcal{D}_8 = \langle (1234), (13) \rangle$, the inclusion $\mathcal{D}_8 \subseteq \mathrm{Stab}(P)$ follows. Next, note that the length of the orbit of P under the action of $\mathcal{S}_4$ is (at least) equal to 3. This is clear because

$$\begin{aligned} P(x_1, x_2, x_3, x_4) &= x_1x_3 + x_2x_4, \\ (12) * P(x_1, x_2, x_3, x_4) &= x_2x_3 + x_1x_4, \\ (14) * P(x_1, x_2, x_3, x_4) &= x_1x_2 + x_3x_4, \end{aligned}$$

are all distinct polynomials. Hence $[\mathcal{S}_4 : \mathrm{Stab}(P)] \geq 3$ by Lemma 1.10. Since

$$3 = [\mathcal{S}_4 : \mathcal{D}_8] = [\mathcal{S}_4 : \mathrm{Stab}(P)][\mathrm{Stab}(P) : \mathcal{D}_8],$$

$[\mathrm{Stab}(P) : \mathcal{D}_8] = 1$ and $\mathrm{Stab}(P) = \mathcal{D}_8$. □

Lemma 2.38. The polynomial

$$P(x_1, x_2, x_3, x_4) = x_1x_2^2 + x_2x_3^2 + x_3x_4^2 + x_4x_1^2$$

is a $\mathcal{C}_4$ invariant. In particular, P is a $\mathcal{D}_8$-relative $\mathcal{C}_4$-invariant.

Proof. Again, denote

$$\mathrm{Stab}(P) = \{\tau \in \mathcal{S}_4 \mid \tau * P = P\}.$$

The inclusion $\mathcal{C}_4 = \langle(1234)\rangle \subseteq \mathrm{Stab}(P)$ is clear. Similarly to the previous lemma, it's easy to check that the polynomials

$$\begin{aligned}
P(x_1, x_2, x_3, x_4) &= x_1x_2^2 + x_2x_3^2 + x_3x_4^2 + x_4x_1^2,\\
(12) * P(x_1, x_2, x_3, x_4) &= x_2x_1^2 + x_1x_3^2 + x_3x_4^2 + x_4x_2^2,\\
(13) * P(x_1, x_2, x_3, x_4) &= x_3x_2^2 + x_2x_1^2 + x_1x_4^2 + x_4x_3^2,\\
(14) * P(x_1, x_2, x_3, x_4) &= x_4x_2^2 + x_2x_3^2 + x_3x_1^2 + x_1x_4^2,\\
(23) * P(x_1, x_2, x_3, x_4) &= x_1x_3^2 + x_3x_2^2 + x_2x_4^2 + x_4x_1^2,\\
(34) * P(x_1, x_2, x_3, x_4) &= x_1x_2^2 + x_2x_4^2 + x_4x_3^2 + x_3x_1^2,
\end{aligned}$$

are distinct and, by Lemma 1.10, $[\mathcal{S}_4 : \mathrm{Stab}(P)] \geq 6$. Combined with the equality

$$6 = [\mathcal{S}_4 : \mathcal{C}_4] = [\mathcal{S}_4 : \mathrm{Stab}(P)][\mathrm{Stab}(P) : \mathcal{C}_4],$$

it follows that $\mathrm{Stab}(P) = \mathcal{C}_4$. □

Note 2.39. The following three examples have been solved as part of Exercise 14 in [6, p. 364].

Example 2.40. Let $f(x) = x^4 + x^3 + x^2 + x + 1$. Its roots are

$$\alpha_1 = e^{2\pi i/5},\ \alpha_2 = e^{4\pi i/5},\ \alpha_3 = e^{6\pi i/5},\ \alpha_4 = e^{8\pi i/5}.$$

The discriminant of f is equal to

$$\mathrm{disc}(f) = 125 \in \mathbb{Z} \setminus \mathbb{Z}^2.$$

By Proposition 1.46, $\mathrm{Gal}(f)$ contains an odd permutation. To investigate whether $\mathrm{Gal}(f)$ is contained in $\mathcal{D}_8$, let

$$P(x_1, x_2, x_3, x_4) := x_1x_3 + x_2x_4$$

be the $\mathcal{D}_8$-invariant polynomial from Lemma 2.37. For $G := \mathcal{S}_4$, the resolvent polynomial $R^G_{(P,f)}$ is equal to

$$R^G_{(P,f)}(x) = \Pi_{i=1}^3(x - P_i(\alpha_1, \alpha_2, \alpha_3, \alpha_4)) = x^3 - x^2 - 3x + 2 = (x-2)(x^2 + x - 1),$$

where

$$\begin{aligned}
P_1(x_1, x_2, x_3, x_4) &:= P(x_1, x_2, x_3, x_4),\\
P_2(x_1, x_2, x_3, x_4) &:= (12) * P(x_1, x_2, x_3, x_4),\\
P_3(x_1, x_2, x_3, x_4) &:= (14) * P(x_1, x_2, x_3, x_4).
\end{aligned}$$

The root 2 of $R^G_{(P,f)}$ is equal to $((12) * P)(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$. After we reorder the roots of f according to the permutation (12), we get $\mathrm{Gal}(f) \subseteq \mathcal{D}_8$.

So with the roots ordered as

$$\alpha_1 = e^{4\pi i/5},\ \alpha_2 = e^{2\pi i/5}, \alpha_3 = e^{6\pi i/5},\ \alpha_4 = e^{8\pi i/5},$$

let's decide whether or not $\mathrm{Gal}(f)$ is equal to $\mathcal{C}_4$. For $G := \mathcal{D}_8$, $H := \mathcal{C}_4$,

$$P(x_1, x_2, x_3, x_4) := x_1x_2^2 + x_2x_3^2 + x_3x_4^2 + x_4x_1^2$$

is the G-relative H-invariant from Lemma 2.38. The resolvent polynomial $R^G_{(P,f)}$ is equal to

$$R^G_{(P,f)}(x) = (x - P(\alpha_1, \alpha_2, \alpha_3, \alpha_4))(x - ((13) * P)(\alpha_1, \alpha_2, \alpha_3, \alpha_4)) = x^2 - 3x - 4 = (x+1)(x-4)$$

and so, by Proposition 2.33, $\mathrm{Gal}(f) = \mathcal{C}_4$.

The need to reorder the roots during the course of the algorithm may seem bothersome but it ensures that when the algorithm terminates, we know exactly how $\mathrm{Gal}(f)$ acts on the roots of f.

Example 2.41. Let $f(x) = x^4 + 1$. Its roots are

$$\alpha_1 = \frac{\sqrt{2}}{2}(-1 + i),\ \alpha_2 = \frac{\sqrt{2}}{2}(1 + i),\ \alpha_3 = \frac{\sqrt{2}}{2}(1 - i),\ \alpha_4 = \frac{\sqrt{2}}{2}(-1 - i).$$

The discriminant

$$\mathrm{disc}(f) = 256 = 16^2$$

is a square and $\mathrm{Gal}(f) \subseteq \mathcal{A}_4$ by Proposition 1.46. Now, for $G := \mathcal{S}_4$ and

$$P(x_1, x_2, x_3, x_4) = x_1x_3 + x_2x_4,$$

the resolvent polynomial $R^G_{(P,f)}$ is equal to

$$R^G_{(P,f)}(x) = \prod_{i=1}^{3}(x - P_i(\alpha_1, \alpha_2, \alpha_3, \alpha_4)) = x^3 - 4x = x(x-2)(x+2),$$

where

$$\begin{aligned} P_1(x_1, x_2, x_3, x_4) &:= P(x_1, x_2, x_3, x_4), \\ P_2(x_1, x_2, x_3, x_4) &:= (12) * P(x_1, x_2, x_3, x_4), \\ P_3(x_1, x_2, x_3, x_4) &:= (14) * P(x_1, x_2, x_3, x_4). \end{aligned}$$

By Proposition 2.33, $\mathrm{Gal}(f) \subseteq \mathrm{Stab}(P) = \mathcal{D}_8$. It follows that $\mathrm{Gal}(f) \subseteq \mathcal{A}_4 \cap \mathcal{D}_8$ and $\mathrm{Gal}(f) = \mathcal{C}_2^2$, the normal Klein 4-group.

Remark 2.42. It's not always the case that the roots of f are explicitly known as in the above two examples. Often, only approximations to the roots are available. The way to compute the resolvent polynomial is then to expand the product on the right-hand side of (2.5) and round coefficients of the resulting polynomial to the nearest integer. This is illustrated by the next example.

Example 2.43. Let

$$f(x) = x^4 + 8x + 12.$$

The roots of f are approximately equal to

$$\begin{aligned} \alpha_1 &= 1.3709 - 1.8271i, \quad \alpha_2 = 1.3709 + 1.8271i, \\ \alpha_3 &= -1.3709 - 0.6485i, \ \alpha_4 = -1.3709 + 0.6485i \end{aligned}$$

Let $P(x_1, x_2, x_3, x_4) = x_1x_3 + x_2x_4$ be the $\mathcal{D}_8$-invariant polynomial from Lemma 2.37. The product

$$(x - P(\alpha_1, \alpha_2, \alpha_3, \alpha_4))(x - ((12) * P)(\alpha_1, \alpha_2, \alpha_3, \alpha_4))(x - ((14) * P)(\alpha_1, \alpha_2, \alpha_3, \alpha_4))$$

is equal to the polynomial

$$x^3 - 0.0001x^2 - 48.0008x - 63.9924.$$

Hence the resolvent polynomial $R^{\mathcal{S}_4}_{(P,f)}$ is equal to

$$R^{\mathcal{S}_4}_{(P,f)} = x^3 - 48x - 64.$$

That's a polynomial irreducible over $\mathbb{Q}$, so $\mathrm{Gal}(f) \nsubseteq \mathcal{D}_8$ by Corollary 2.34. Finally, the discriminant $\mathrm{disc}(f)$ is equal to

$$\mathrm{disc}(f) = 576^2,$$

and we conclude that $\mathrm{Gal}(f) = \mathcal{A}_4$ by Proposition 1.46.

Using approximations to the roots of f to compute the resolvent polynomial can become unwieldy. A modular method, which is the subject of the fourth chapter, has been devised by K. Yokoyama ([26]) to work around this problem. To conclude this section, here's a formal description of the algorithm.

Algorithm 7 Galois group - degree 4

Input: Irreducible, monic polynomial $f \in \mathbb{Z}[x]$ of degree 4

Output: $\mathrm{Gal}(f)$ (with respect to some order $\alpha_1, \alpha_2, \alpha_3, \alpha_4 \in \overline{\mathbb{Q}}$ of the roots of f)

1: $P(x_1, x_2, x_3, x_4) := x_1x_3 + x_2x_4$, $r(x) := R^{\mathcal{S}_4}_{(P,f)}(x)$.
2: Using Algorithm 2.1, compute the resultant $\mathrm{res}(r, r')$ *r(x) *is square-free iff* *res(r, r') ≠ 0*
3: **if** $\mathrm{res}(r, r') = 0$ **then**
4: Apply a Tschirnhausen transformation (Algorithm 3) on f and go to Step 1
5: **end if**
6: Using Algorithm 2.1, compute $d := \mathrm{res}(f, f')$ *d = *disc(f) by Proposition 2.4*
7: Factor $r(x)$ over $\mathbb{Z}[x]$
8: **if** $\sqrt{d} \in \mathbb{Z}$ **and** $r(x)$ has no integral roots **then**
9: **return** $\mathcal{A}_4$
10: **end if**
11: **if** $\sqrt{d} \in \mathbb{Z}$ **and** $r(x)$ has an integral root **then**
12: **return** $\mathcal{C}_2^2$
13: **end if**
14: **if** $\sqrt{d} \notin \mathbb{Z}$ **and** $r(x)$ has no integral roots **then**
15: **return** $\mathcal{S}_4$
16: **end if**
17: **if** $\sqrt{d} \notin \mathbb{Z}$ **and** $R(x)$ has an integral root **then**
18: Rearrange the roots $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ of f so that $\alpha_1\alpha_3 + \alpha_2\alpha_4 \in \mathbb{Z}$
19: $P(x_1, x_2, x_3, x_4) := x_1x_2^2 + x_2x_3^2 + x_3x_4^2 + x_4x_1^2$, $r(x) := R^{\mathcal{D}_8}_{(P,f)}(x)$
20: **if** $\mathrm{res}(r, r') = 0$ **then**
21: Apply a Tschirnhausen transformation on f and go to Step 18.
22: **end if**
23: Factor $r(x)$ over $\mathbb{Z}[x]$
24: **if** $r(x)$ has an integral root **then**
25: **return** $\mathcal{C}_4$
26: **else**
27: **return** $\mathcal{D}_8$
28: **end if**
29: **end if**

Chapter 3

The Universal Splitting Ring

3.1 The universal splitting ideal

The aim of this section is to prove Theorem 3.20. Throughout sections 3.1, 3.2, and 3.3, R denotes a commutative ring and K denotes a perfect field.

Definition 3.1. Let $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \in R[x]$. We denote by I_f the ideal of $R[x_1, \ldots, x_n]$ generated by the polynomials

$$\begin{array}{c} s_1(x_1, \ldots, x_n) + a_{n-1}, \\ s_2(x_1, \ldots, x_n) - a_{n-2}, \\ \vdots \\ s_n(x_1, \ldots, x_n) + (-1)^{n-1}a_0, \end{array} \tag{3.1}$$

where $s_1, \ldots, s_n \in R[x_1, \ldots, x_n]$ are the elementary symmetric polynomials, and call it the universal splitting ideal of f. The ring $S_f = R[x_1, \ldots, x_n]/I_f$ is called the universal splitting ring of f (over R).

Note 3.2. The above definition uses terminology from [26]. In [17], for example, I_f is called the ideal of symmetric relations. For a more thorough threatment of the properties of the universal splitting ring, the reader can refer to [3].

Remark 3.3. The ring R can be embedded into S_f and we may assume that $R \subseteq S_f$. Furthermore, the equality

$$f(x) = \prod_{i=1}^{n}(x - [x_i])$$

holds over S_f because the product on the right-hand side is equal to

$$x^n - s_1([x_1], \ldots, [x_n])x^{n-1} + \cdots + (-1)^n s_n([x_1], \ldots, [x_n]),$$

which is a polynomial equal to $f(x)$, since clearly

$$[a_{n-1}] = [-s_1(x_1, \ldots, x_n)], \ldots, [a_0] = [(-1)^n s_n(x_1, \ldots, x_n)]$$

holds in S_f.

Lemma 3.4 (Universal Property of the Splitting Ring)**.** Let $S_f = R[x_1, \ldots, x_n]/I_f$ be the universal splitting ring of f over R, $f \in R[x]$ monic, $\deg(f) = n$. If $R \subseteq S$ is a ring and $\rho_1, \ldots, \rho_n \in S$ exist such that

$$f(x) = \prod_{i=1}^{n}(x - \rho_i) \tag{3.2}$$

holds in $S[x]$, then

$$[x_i] \mapsto \rho_i,\ i = 1, \ldots, n \tag{3.3}$$

induces a homomorphism

$$S_f \to S.$$

Proof. By Lemma 1.15, there's a homomorphism

$$\psi : R[x_1, \ldots, x_n] \to S$$

such that $\psi(x_i) = \rho_i$, $i = 1, \ldots, n$. Let

$$f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_0.$$

Then (3.2) implies that

$$\begin{aligned} s_1(\rho_1, \ldots, \rho_n) + a_{n-1} &= 0, \\ s_2(\rho_1, \ldots, \rho_n) - a_{n-2} &= 0, \\ &\vdots \\ s_n(\rho_1, \ldots, \rho_n) + (-1)^{n-1}a_0 &= 0 \end{aligned}$$

in S. Hence $I_f \subseteq \mathrm{Ker}(\psi)$ and ψ factors as $\psi = \overline{\psi} \circ \pi$, where

$$\pi : R[x_1, \ldots, x_n] \to S_f$$

is the natural projection and

$$\overline{\psi} : S_f \to S$$

is defined by (3.3). □

Let $f(x) \in K[x]$ a monic and separable polynomial. Let $\alpha_1, \ldots, \alpha_n \in \overline{K}$ be the roots of f and $L = K(\alpha_1, \ldots, \alpha_n)$ the splitting field of f. There's a surjective homomorphism

$$\phi : K[x_1, \ldots, x_n] \to L,$$

defined by

$$\phi(g(x_1, \ldots, x_n)) = g(\alpha_1, \ldots, \alpha_n)$$

for every $g \in K[x_1, \ldots, x_n]$. We denote by M its kernel:

$$M = \mathrm{Ker}(\phi) = \{g(x_1, \ldots, x_n) \in K[x_1, \ldots, x_n] \mid g(\alpha_1, \ldots, \alpha_n) = 0\}. \tag{3.4}$$

By the First isomorphism theorem, we have

$$K[x_1, \ldots, x_n]/M \cong L. \tag{3.5}$$

We see that $K[x_1, \ldots, x_n]/M$ is a field, hence M is a maximal ideal.

Definition 3.5. We call the ideal M defined by (3.4) the splitting ideal of f with respect to the order $(\alpha_1, \ldots, \alpha_n)$ of the roots of f.

Note 3.6. Let S_f be the universal splitting ring of f over K, $f \in K[x]$ monic and separable. Furhermore, let $\mathrm{Gal}(f) \subseteq \mathcal{S}_n$ and M be the Galois group and the splitting ideal of f with respect to the order of the roots given above, respectively. Let

$$[\mathcal{S}_n : \mathrm{Gal}(f)] = k \text{ and } \{\sigma_1, \ldots, \sigma_k\} \subseteq \mathcal{S}_n$$

be a left transversal for $\mathrm{Gal}(f)$ in $\mathcal{S}_n$. We further denote by M^{σ_i} the ideal

$$M^{\sigma_i} = \{\sigma_i * g(x_1, \ldots, x_n) \mid g(x_1, \ldots, x_n) \in M\}. \tag{3.6}$$

Our aim for the rest of this section is to prove

$$I_f = \bigcap_{i=1}^{k} M^{\sigma_i}, \tag{3.7}$$

thereby proving that S_f is a direct product of fields. A proof of this fact, one using methods of algebraic geometry, can be found in [2]. The proof presented here is slightly lengthy but only requires elementary commutative algebra.

Lemma 3.7. With the above notation, let $\tau \in \mathcal{S}_n$. Then

$$M^{\tau} = \{\tau * g(x_1, \ldots, x_n) \mid g(x_1, \ldots, x_n) \in M\}$$

equals M^{σ_i} for some $i \in \{1, \ldots, k\}$.

Proof. Since $\{\sigma_1, \ldots, \sigma_k\}$ is a left transversal for $\mathrm{Gal}(f)$, there exists $j \in \{1, \ldots, k\}$ such that $\tau\mathrm{Gal}(f) = \sigma_j\mathrm{Gal}(f)$. To show that $M^{\tau} = M^{\sigma_j}$, we first note that for any $\pi \in \mathcal{S}_n$,

$$M = M^{\pi} \iff \pi \in \mathrm{Gal}(f)$$

by (3.5). Therefore

$$M^{\tau} = M^{\sigma_j} \iff M = M^{\tau^{-1}\sigma_j} \iff \tau^{-1}\sigma_j \in \mathrm{Gal}(f) \iff \tau\mathrm{Gal}(f) = \sigma_j\mathrm{Gal}(f). \tag{3.8}$$

□

Lemma 3.8. With the above notation, let $i \in \{1, \ldots, k\}$. Then M^{σ_i} is a maximal ideal, $I_f \subseteq M^{\sigma_i}$, and the ideals $M^{\sigma_1}, \ldots, M^{\sigma_k}$ are pairwise comaximal.

Proof. For every i, M^{σ_i} is a maximal ideal because the map

$$\begin{aligned} \sigma : K[x_1, \ldots, x_n] &\to K[x_1, \ldots, x_n], \\ \sigma(g(x_1, \ldots, x_n)) &= g(x_{\sigma_i(1)}, \ldots, x_{\sigma_i(n)}) \end{aligned}$$

is an automorphism of $K[x_1, \ldots, x_n]$ and $M^{\sigma_i} = \sigma(M)$. The inclusion $I_f \subseteq M$ clearly holds and hence

$$I_f = \sigma(I_f) \subseteq \sigma(M) = M^{\sigma_i}.$$

By (3.8), the ideals $M^{\sigma_1}, \ldots, M^{\sigma_k}$ are pairwise distinct and hence comaximal. □

A direct implication of Lemma 3.8 is the inclusion $\subseteq$ in (3.7). Next we argue that the ideal I_f is a radical ideal.

Definition 3.9. Let R be a ring and $I \subseteq R$ an ideal. Then the set

$$\sqrt{I} = \{r \in R \mid r^l \in I \text{ for some } l \in \mathbb{N}\}$$

is called the radical of I. I is called a radical ideal if $I = \sqrt{I}$.

Remark 3.10. For every ideal I in R, the radical of I is an ideal such that $I \subseteq \sqrt{I}$. Every prime ideal is a radical ideal. In particular, every maximal ideal is a radical ideal.

Proposition 3.11 ([5], Lemma 8.13, p. 341)**.** Let J be an ideal of $K[x_1, \ldots, x_n]$ such that for each $i \in \{1, \ldots, n\}$, there's a separable polynomial $f_i(x_i) \in J \cap K[x_i]$. Then J is a radical ideal.

To prove Proposition 3.11, we need three auxiliary lemmata. The following is a consequence of Lemma 1.15.

Lemma 3.12. Let R, S be rings, $\phi : R \to S$ a homomorphism of rings. Then the map

$$R[x_1, \ldots, x_n] \to S[x_1, \ldots, x_n],$$
$$\sum a_j x_1^{j_1} \cdots x_n^{j_n} \mapsto \sum \phi(a_j) x_1^{j_1} \cdots x_n^{j_n}$$

is a homomorphism of rings. It is surjective iff ϕ is surjective.

Lemma 3.13 ([5], Lemma 1.62, p. 35)**.** Let R, S be rings, $\phi : R \to S$ a surjective homomorphism of rings. We denote by $\mathcal{I}_\phi(R)$ the set of the ideals I of R satisfying $\mathrm{Ker}(\phi) \subseteq I$ and by $\mathcal{I}(S)$ the set of ideals of S. Then $I \mapsto \phi(I)$ is a bijection between $\mathcal{I}_\phi(R)$ and $\mathcal{I}(S)$. The map $J \mapsto \phi^{-1}(J)$ is its inverse. If $J \in \mathcal{I}(S)$ is maximal in S then $\phi^{-1}(J)$ is maximal in R.

Proof. Let $I \in \mathcal{I}_\phi(R)$ and $r_1, r_2 \in I$. Then $r_1 + r_2 \in I$ and $\phi(r_1) + \phi(r_2) = \phi(r_1 + r_2) \in \phi(I)$. Now we show that $s\phi(r_1) \in \phi(I)$ for every $s \in S$. Since ϕ is surjective, there exists $t \in R$ such that $\phi(t) = s$. Then $s\phi(r_1) = \phi(t)\phi(r) = \phi(tr_1) \in \phi(I)$. We've shown that $\phi(I) \in \mathcal{I}(S)$ for every $I \in \mathcal{I}_\phi(R)$. Now, let $J \in \mathcal{I}(S)$ and let $r_1, r_2 \in \phi^{-1}(J)$. Then $r_1 + r_2 \in \phi^{-1}(J)$ because $\phi(r_1 + r_2) = \phi(r_1) + \phi(r_2) \in J$ and $\phi^{-1}(J)$ is closed under addition. For every $r \in R$, $\phi(rr_1) = \phi(r)\phi(r_1) \in J$ because $\phi(r_1) \in J$ and J is an ideal. If $r \in \mathrm{Ker}(\phi)$, then $\phi(r) = 0 \in J$ and $\mathrm{Ker}(\phi) \subseteq \phi^{-1}(J) \in \mathcal{I}_\phi(R)$.

To show that the map $I \mapsto \phi(I)$ is a bijection between $\mathcal{I}_\phi(R)$ and $\mathcal{I}(S)$, we show that $J \mapsto \phi^{-1}(J)$ is its inverse, i.e. $\phi(\phi^{-1}(J)) = J$ for every $J \in \mathcal{I}(S)$ and $\phi^{-1}(\phi(I)) = I$ for every $I \in \mathcal{I}_\phi(R)$.

Let $J \in \mathcal{I}(S)$. The inclusion $\phi(\phi^{-1}(J)) \subseteq J$ follows directly from the definition of image and preimage of a map. For the reverse inclusion, let $j \in J$. Since ϕ is surjective, there exists $r \in R$ such that $\phi(r) = j$. All we need to show for $J \subseteq \phi(\phi^{-1}(J))$ to hold is that $r \in \phi^{-1}(J)$, which is true by the choice of r.

Let $I \in \mathcal{I}_\phi(R)$ and $i \in I$. Then $\phi(i) \in \phi(I)$, proving $I \subseteq \phi^{-1}(\phi(I))$. Conversely, let $r \in R$ be an element such that $\phi(r) \in \phi(I)$. This means there exists

$r' \in I$ with $\phi(r) = \phi(r')$. Then $r - r' \in \mathrm{Ker}(\phi) \subseteq I$ and consequently $r \in I$. Thus $\phi^{-1}(\phi(I)) \subseteq I$.

Finally, we show that if $J \in \mathcal{I}(S)$ is a maximal ideal, then $\phi^{-1}(J)$ is a maximal ideal in R. Suppose $I = \phi^{-1}(J)$ is not maximal and let $I' \in \mathcal{I}_\phi(R)$ be such that $I \subsetneq I' \subsetneq R$. Then, due to the fact that $\mathrm{Ker}(\phi) \subseteq I$, $\phi(I) \subsetneq \phi(I') \subsetneq \phi(R)$ and $\phi(I) = J$ is not maximal. □

Lemma 3.14 ([5], Lemma 8.5, p. 337)**.** Let I be an ideal of $K[x_1, \ldots, x_n]$. Assume that $f, g_1, \ldots, g_r \in K[x_1]$ are such that

$$f = g_1 \cdots g_r$$

is a factorization of f in $K[x_1]$ into pairwise relatively prime factors. then

$$I + (f) = \bigcap_{i=1}^{r} (I + (g_i))$$

Proof. Clearly $I+(f) \subseteq I+(g_i)$ for every $i \in \{1, \ldots, r\}$ and the inclusion $I+(f) \subseteq \bigcap_{i=1}^{r} (I + (g_i))$ follows. To prove the reverse inclusion, consider $h \in K[x_1, \ldots, x_n]$ such that for every $i \in \{1, \ldots, r\}$, $h \in I + (g_i)$. This means that there exist polynomials $q_i \in K[x_1, \ldots, x_n]$ and $s_i \in I$, $i = 1, \ldots, r$, such that $h = q_i g_i + s_i$. Now we define for $i \in \{1, \ldots, r\}$,

$$f_i = \prod_{\substack{j=1 \\ j \neq i}}^{r} g_j.$$

Then clearly $hf_i \in I + (f)$ for $i = 1, \ldots, r$. From the fact that g_i and g_j are relatively prime for $i \neq j$, one concludes that the greatest common divisor of $f_1, \ldots, f_r$ in $K[x_1]$ is 1. Hence there exist $u_1, \ldots, u_r \in K[x_1]$ satisfying

$$1 = u_1 f_1 + \cdots + u_r f_r,$$

implying

$$h = u_1 h f_1 + \cdots + u_r h f_r \in I + (f).$$

□

Proof of Proposition 3.11. The idea of the proof is to show that J is an intersection of finitely many maximal ideals, which clearly implies that J is a radical ideal.

To show that J is a finite intersection of maximal ideals, we proceed by induction on n. If $n = 1$, then $J \subseteq K[x_1]$ is a principle ideal, i.e. $J = (g)$, $g \in K[x_1]$, and the generator g is square-free (because f_1, a multiple of g, is separable and therefore square-free). Let

$$g = g_1 \cdots g_r$$

with pairwise non-associated, irreducible polynomials $g_1, \ldots, g_r \in K[x_1]$. Then the g_i are pairwise relatively prime, and so

$$J = (g) = \bigcap_{i=1}^{r} (g_i)$$

by Lemma 3.14 (where the ideal I from the statement of Lemma 3.14 is the zero ideal). The ideals occuring in the intersection on the right-hand side are maximal because the g_i are irreducible.

Now let $n > 1$. We may write $f_1 = g_1 \cdot \cdots \cdot g_r$ with pairwise non-associated, irreducible polynomials $g_1, \ldots, g_r \in K[x_1]$ and, again by Lemma 3.14, we obtain

$$J = J + (f_1(x_1)) = \bigcap_{i=1}^{r} (J + (g_i(x_1))).$$

To finish the proof, we show that each of the ideals $J + (g_i(x_1))$, $i = 1, \ldots, r$, is an intersection of finitely many maximal ideals. To this end, fix $i \in \{1, \ldots, r\}$ and denote $J' = J + (g_i)$. Since g_i is irreducible, $K[x_1]/(g_i)$ is a field and we may consider the natural projection

$$\phi : K[x_1] \to K[x_1]/(g_i)$$

that maps a polynomial $h \in K[x_1]$ to the residue class $h + (g_i)$. We note that K may be considered a subfield of $K[x_1]/(g_i)$ and ϕ fixes K. By Lemma 3.12, there's an epimorphism ψ from $(K[x_1])[x_2, \ldots, x_n] = K[x_1, \ldots, x_n]$ to $(K[x_1]/(g_i))[x_2, \ldots, x_n]$ that extends ϕ. We claim that the kernel of ψ is the ideal generated by g_i (in $K[x_1, \ldots, x_n]$). It's clear that $(g_i) \subseteq \mathrm{Ker}(\psi)$. Now, let $h \in \mathrm{Ker}(g_i)$ and express h as

$$h(x_1, \ldots, x_n) = \sum_j h_j(x_1) x_2^{j_2} \cdots x_n^{j_n} \in (K[x_1])[x_2, \ldots, x_n].$$

Since $\psi(h)$ is the zero polynomial in $(K[x_1]/(g_i))[x_1, \ldots, x_n]$, $\phi(h_j) = 0 \in K[x_1]/(g_i)$ for every j (recall that ϕ denotes the natural projection from $K[x_1]$ to $K[x_1]/(g_i)$). In other words, $h_j \in (g_i)$ for every j and $h \in (g_i)$. We've established that $\mathrm{Ker}(\psi) = (g_i) \subseteq J'$.

As ψ is surjective, $\psi(J') \subseteq (K[x_1]/(g_i))[x_2, \ldots, x_n]$ is an ideal by Lemma 3.13. To verify that it satisfies the induction hypothesis, recall that the map ψ fixes K and $\psi(f_2) = f_2 \in \psi(J') \cap (K[x_1]/(g_i))[x_2], \ldots, \psi(f_n) = f_n \in \psi(J') \cap (K[x_1]/(g_i))[x_n]$ are indeed separable polynomials. By the induction hypothesis, there exist maximal ideals $M_1, \ldots, M_s$ such that $\psi(J') = \bigcap_{i=1}^{s} M_i$. By Lemma 3.13,

$$J' = \psi^{-1}\left(\bigcap_{i=1}^{s} M_i\right) = \bigcap_{i=1}^{s} \psi^{-1}(M_i)$$

is an intersection of maximal ideals. □

Corollary 3.15. Let I_f be the universal splitting ideal of f, where $f(x) \in K[x]$ is monic and separable. Then for each $i = 1, \ldots, n$, $f(x_i) \in I_f$, and I_f is a radical ideal.

Proof. We have seen in Remark 3.3 that

$$f(x) = \prod_{i=1}^{n} (x - [x_i])$$

holds in the universal splitting ring $S_f = K[x_1, \ldots, x_n]/I_f$. Hence for every i, $f([x_i]) = [f(x_i)] = [0]$ and $f(x_i) \in I_f$. Since f is separable by assumption, I_f is a radical ideal by Proposition 3.11. □

Next, we recall a well known description of radicals.

Proposition 3.16 ([7], Tvrzení I.3.12, p. 14)**.** Let R be a commutative ring, $J \subseteq R$ an ideal. Then $\sqrt{J}$ equals the intersection of all prime ideals of R containing J.

Proposition 3.17. Let J be a proper ideal of $K[x_1, \ldots, x_n]$. Then $K[x_1, \ldots, x_n]/J$ is finite-dimensional as a K-vector space iff there's a non-zero polynomial in $J \cap K[x_i]$ for every $i \in \{1, \ldots, n\}$.

Proof. For $g(x_1, \ldots, x_n) \in K[x_1, \ldots, x_n]$, we denote by $[g(x_1, \ldots, x_n)]$ the element $g + J$ of $K[x_1, \ldots, x_n]/J$. Suppose $\dim_K(K[x_1, \ldots, x_n]/J) = m \in \mathbb{N}$ and let $i \in \{1, \ldots, n\}$. Then the $m + 1$ elements $[1], [x_i], \ldots, [x_i^{m-1}], [x_i^m]$ are linearly dependent and there are coefficients $c_0, \ldots, c_m \in K$, $(c_0, \ldots, c_m) \neq (0, \ldots, 0)$, such that $[0] = \sum_{j=0}^m c_j [x_i^j] = [\sum_{j=0}^m c_j x_i^j]$. Hence $0 \neq \sum_{j=0}^m c_j x_i^j \in J$.

Conversely, let $f_i(x_i) \in J$, $n_i = \deg(f_i) \geq 1$, $i = 1, \ldots, n$. Let $G = \{[x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n}] \mid 0 \leq i_1 < n_1, \ldots, 0 \leq i_n < n_n\}$. We claim that G generates $K[x_1, \ldots, x_n]/J$. Let $i \in \{1, \ldots, n\}$. We prove by induction that $[x_i^k] \in \langle [1], [x_i], \ldots, [x_i^{n_i - 1}] \rangle$ for every $k \geq 0$. This is obvious for $0 \leq k \leq n_i - 1$. Let $k > n_i - 1$. By the induction hypothesis, $[x_i^{k-1}] = c_0 + c_1 [x_i] + \cdots + c_{n_i - 1} [x_i^{n_i - 1}]$ with $c_0, \ldots, c_{n_i - 1} \in K$. As $[x_i^{n_i}] = [x_i^{n_i} - f_i(x_i)] \in \langle [1], [x_i], \ldots, [x_i^{n_i - 1}] \rangle$, we see that

$$[x_i^k] = [x_i^{k-1}][x_i] = c_0 [x_i] + c_1 [x_i^2] + \cdots + c_{n_i - 2} [x_i^{n_i - 1}] + c_{n_i - 1} [x_i^{n_i}] \tag{3.9}$$

is also an element of $\langle [1], [x_i], \ldots, [x_i^{n_i - 1}] \rangle$. But now it's clear that $[x_1^{j_1} \cdots x_n^{j_n}] \in \langle G \rangle$ for every n-tuple $(j_1, \ldots, j_n)$, $j_i \geq 0$, $i = 1, \ldots, n$, and G generates $K[x_1, \ldots, x_n]/J$. □

Proposition 3.18 ([5], Exercise 7.43, p. 315)**.** Let $J \subsetneq K[x_1, \ldots, x_n]$ be a prime ideal such that there's a non-zero polynomial in $J \cap K[x_i]$ for every $i \in \{1, \ldots, n\}$. Then J is maximal.

Proof. Let's denote $D = K[x_1, \ldots, x_n]/J$. Since J is a prime ideal, D is a domain. To show that it's a field, fix a non-zero element $a \in D$ and consider the map $\psi : D \to D$ defined by $\psi(x) = ax$. It's easily verified that ψ is an injective K-endomorphism of D (as a K-vector space). Furthermore, D is finitely dimensional over K by the previous proposition, so ψ is surjective and there's $c \in D$ such that $ac = 1_D$. Thus D is a field and J is maximal. □

It has been shown in the proof of Corollary 3.15 that $f(x_i) \in I_f$ for every $i \in \{1, \ldots, n\}$. We therefore have

$$I_f = \sqrt{I_f} = \bigcap_{\substack{I_f \subseteq N \\ N \text{ maximal}}} N$$

because every prime ideal containing I_f is maximal by Proposition 3.18. The following proposition states that every maximal ideal containing I_f is equal to M^τ, $\tau \in \mathcal{S}_n$.

Proposition 3.19. Let $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in K[x]$ be separable and let I_f be the universal splitting ideal of f. Let $\alpha_1, \ldots, \alpha_n \in \overline{K}$ be the roots of f and $M \subseteq K[x_1, \ldots, x_n]$ the splitting ideal of f associated with the assignment of the roots x_1 to $\alpha_1, \ldots, x_n$ to α_n. Let $N \subseteq K[x_1, \ldots, x_n]$ be a maximal ideal such that $I_f \subseteq N$. There's a permutation $\tau \in \mathcal{S}_n$ such that $N = M^\tau$.

Proof. We work under the assumption that the fields $F_1 = K[x_1, \ldots, x_n]/M$ and $F_2 = K[x_1, \ldots, x_n]/N$ both contain K as a subfield. For $g(x_1, \ldots, x_n) \in K[x_1, \ldots, x_n]$, let's denote by $[g(x_1, \ldots, x_n)]_M$ the element $g(x_1, \ldots, x_n) + M$ in F_1 and $[g(x_1, \ldots, x_n)]_N$ the element $g(x_1, \ldots, x_n) + N$ in F_2. We've already seen that F_1 is a splitting field of f. By the same argument we used to show that f splits over the universal splitting ring, we get that $f(x) = \prod_{i=1}^n (x - [x_i]_N)$ holds in F_2. Since F_2 is clearly generated by $[x_1]_N, \ldots, [x_n]_N$, F_2 too is a splitting field of f and there's an K-isomorphism

$$\psi : F_1 \to F_2.$$

The isomorphism ψ sends a root of f in F_1 to a root of f in F_2. It follows that there's a permutation $\tau \in \mathcal{S}_n$ such that $\psi([x_i]_M) = [x_{\tau(i)}]_N$ for every i. As a consequence, $\psi([g(x_1, \ldots, x_n)]_M) = [g(x_{\tau(1)}, \ldots, x_{\tau(n)})]_N$ for every $g \in K[x_1, \ldots, x_n]$.

We show that $N = M^\tau$. Since both the ideals are maximal, it suffices to show $M^\tau \subseteq N$. Consider $g \in M$. This means $[0]_N = \psi([g(x_1, \ldots, x_n)]_M) = [g(x_{\tau(1)}, \ldots, x_{\tau(n)})]_N$ and $g(x_{\tau(1)}, \ldots, x_{\tau(n)}) \in N$.

□

Theorem 3.20. Let $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in K[x]$ be a separable polynomial, $\alpha_1, \ldots, \alpha_n \in \overline{K}$ its roots. Let $\mathrm{Gal}(f)$ and M be the Galois group and the splitting ideal of f with respect to this order of the roots, respectively. Let $\{\sigma_1, \ldots, \sigma_k\}$ be a left transversal for $\mathrm{Gal}(f)$ in $\mathcal{S}_n$ and

$$M^{\sigma_i} = \{g(x_{\sigma_i(1)}, \ldots, x_{\sigma_i(n)}) \mid g(x_1, \ldots, x_n) \in M\},\ i \in \{1, \ldots, k\}.$$

Then

$$\{M^{\sigma_i} \mid i = 1, \ldots, k\}$$

is the set of the maximal ideals in $K[x_1, \ldots, x_n]$ containing I_f,

$$I_f = \bigcap_{i=1}^{k} M^{\sigma_i},$$

where I_f is the universal splitting ideal of f, and there's an isomorphism

$$\psi : K[x_1, \ldots, x_n]/I_f \to K[x_1, \ldots, x_n]/M^{\sigma_1} \times \cdots \times K[x_1, \ldots, x_n]/M^{\sigma_k},$$

$$\psi([g(x_1, \ldots, x_n)]) = ([g(x_1, \ldots, x_n)], \ldots, [g(x_1, \ldots, x_n)]),$$

$g(x_1, \ldots, x_n) \in K[x_1, \ldots, x_n]$.

Proof. So far, we've shown that

$$I_f = \sqrt{I_f} = \bigcap_{\substack{I_f \subseteq N \\ N \text{ maximal}}} N.$$

Let $N \subseteq K[x_1, \ldots, x_n]$ be a maximal ideal containing I_f. By the previous proposition, there's $\tau \in \mathcal{S}_n$ such that $N = M^\tau$. By Lemma 3.7, there's $j \in \{1, \ldots, k\}$ such that $M^\tau = M^{\sigma_j}$. Hence

$$I_f = \bigcap_{i=1}^{k} M^{\sigma_i}.$$

By Lemma 3.8, the ideals M^{σ_i} are comaximal and the Chinese remainder theorem implies the existence of the isomorphism ψ. □

3.2 The standard generating set

Lemma 3.21 (Double Factorization Lemma)**.** Let R, S be rings and $\phi : R \to S$ a surjective homomorphism. Let $I \subseteq R$ and $J \subseteq S$ be ideals such that

$$\phi^{-1}(J) = I.$$

Then the map

$$[r] \mapsto [\phi(r)]$$

is an isomorphism

$$R/I \to S/J.$$

Proof. Let

$$\pi_I : R \to R/I,$$
$$\pi_J : S \to S/J$$

denote the natural projection homomorphisms. Then

$$\mathrm{Ker}(\pi_J \circ \phi) = \{r \in R \mid \phi(r) \in J\} = \phi^{-1}(J) = I.$$

By the Homomorphism Theorem, there exists a monomorphism

$$\psi : R/I \to R/J$$

such that $\psi \circ \pi_I = \pi_J \circ \phi$ and ψ is surjective because ϕ is surjective. □

Lemma 3.22. Let R be a ring. Let $f(x) \in R[x]$ be monic, $\deg(f) = n$. We denote

$$\begin{aligned}
g_1(x_1) &= f(x_1) \\
g_2(x_1, x_2) &= \frac{g_1(x_1) - g_1(x_2)}{x_1 - x_2} \\
&\vdots \\
g_{i+1}(x_1, \ldots, x_{i+1}) &= \frac{g_i(x_1, \ldots, x_{i-1}, x_i) - g_i(x_1, \ldots, x_{i-1}, x_{i+1})}{x_i - x_{i+1}} \\
&\vdots \\
g_n(x_1, \ldots, x_n) &= \frac{g_{n-1}(x_1, \ldots, x_{n-2}, x_{n-1}) - g_{n-1}(x_1, \ldots, x_{n-2}, x_n)}{x_{n-1} - x_n}.
\end{aligned}$$

Then $g_1(x_1), g_2(x_1, x_2), \ldots, g_n(x_1, \ldots, x_n) \in R[x_1, \ldots, x_n]$.

Proof. For every $1 \leq j < n$ and $k \in \mathbb{N}$,

$$x_j^k - x_{j+1}^k = (x_j - x_{j+1})(x_j^{k-1} + x_j^{k-2}x_{j+1} + \cdots + x_j x_{j+1}^{k-2} + x_{j+1}^k),$$

so every term of $g_j(x_1, \ldots, x_{j-1}, x_j) - g_j(x_1, \ldots, x_{j-1}, x_{j+1})$ is divisible by $x_j - x_{j+1}$ and $g_{j+1}(x_1, \ldots, x_{j+1}) \in R[x_1, \ldots, x_n]$. □

Example 3.23. For $n \in \{1, 2, 3, 4\}$ and $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$, we have:

$n = 2$

$$g_1(x_1) = x_1^2 + a_1 x_1 + a_0$$
$$g_2(x_1, x_2) = x_1 + x_2 + a_1$$

$n = 3$

$$g_1(x_1) = x_1^3 + a_2 x_1^2 + a_1 x_1 + a_0$$
$$g_2(x_1, x_2) = x_1^2 + x_1 x_2 + x_2^2 + a_2(x_1 + x_2) + a_1$$
$$g_3(x_1, x_2, x_3) = x_1 + x_2 + x_3 + a_2$$

$n = 4$

$$g_1(x_1) = x_1^4 + a_3 x_1^3 + a_2 x_1^2 + a_1 x_1 + a_0$$
$$g_2(x_1, x_2) = x_1^3 + x_1^2 x_2 + x_1 x_2^2 + x_2^3 + a_3(x_1^2 + x_1 x_2 + x_2^2) + a_2(x_1 + x_2) + a_1$$
$$g_3(x_1, x_2, x_3) = x_1^2 + x_2^2 + x_3^2 + x_1 x_2 + x_1 x_3 + x_2 x_3 + a_3(x_1 + x_2 + x_3) + a_2$$
$$g_4(x_1, x_2, x_3, x_4) = x_1 + x_2 + x_3 + x_4 + a_3$$

Definition 3.24. We call the polynomials $g_1(x_1), \ldots, g_n(x_1, \ldots, x_n)$ from Lemma 3.22 the standard generating set for f.

Note 3.25. We use the terminology of [26, Definition 3]. In [17, p. 90], $g_1, \ldots, g_n$ are called the Cauchy moduli of f. We show in this section that the ideal in $R[x_1, \ldots, x_n]$ generated by $g_1, \ldots, g_n$ is the universal splitting ideal I_f of f. This fact is stated in [26] but not proved. The author has found it difficult to provide a reference for the complete proof. In [24, Theorem 4.4], for example, only the inclusion $(g_1, \ldots, g_n) \subseteq I_f$ is proved.

The following notation is used in Lemma 3.29: for $j, m \in \mathbb{N}$, let

$$h_m^j(x_1, \ldots, x_m) \in R[x_1, \ldots, x_m]$$

denote the sum of all (monic) terms in $x_1, \ldots, x_m$ of degree j:

$$h_m^j(x_1, \ldots, x_n) = \sum_{\substack{i_1 + \cdots + i_m = j \\ i_1, \ldots, i_m \geq 0}} x_1^{i_1} \cdots x_m^{i_m}$$

Example 3.26. Let

$$f(x) = x^4 + a_3 x^3 + a_2 x^2 + a_1 x + a_0 \in R[x].$$

Then

$$\begin{aligned} g_1(x_1) &= f(x_1), \\ g_2(x_1, x_2) &= h_2^3(x_1, x_2) + a_3 h_2^2(x_1, x_2) + a_2 h_2^1(x_1, x_2) + a_1, \\ g_3(x_1, x_2, x_3) &= h_3^2(x_1, x_2, x_3) + a_3 h_3^1(x_1, x_2, x_3) + a_2, \\ g_4(x_1, x_2, x_3, x_4) &= h_4^1(x_1, x_2, x_3, x_4) + a_3, \end{aligned}$$

as one observes comparing with Example 3.23. This example is generalized in Lemma 3.29.

Lemma 3.27. With the above notation, let $m, j \in \mathbb{N}$. Then

$$h_m^j(x_1,\dots,x_{m-1},x_m) - h_m^j(x_1,\dots,x_{m-1},x_{m+1}) = (x_m - x_{m+1})h_{m+1}^{j-1}(x_1,\dots,x_m,x_{m+1})$$

Proof. Note that

$$h_m^j(x_1,\dots,x_m) = x_m^j + x_m^{j-1}h_{m-1}^1(x_1,\dots,x_{m-1}) + \cdots \\ \cdots + x_m h_{m-1}^{j-1}(x_1,\dots,x_{m-1}) + h_{m-1}^j(x_1,\dots,x_{m-1})$$

by the definition of h_m^j. Hence

$$h_m^j(x_1,\dots,x_{m-1},x_m) - h_m^j(x_1,\dots,x_{m-1},x_{m+1}) = \\ = x_m^j - x_{m+1}^j + (x_m^{j-1} - x_{m+1}^{j-1})h_{m-1}^1(x_1,\dots,x_{m-1}) + \cdots + (x_m^2 - x_{m+1}^2)h_{m-1}^{i-2}(x_1,\dots,x_{m-1}) + \\ +(x_m - x_{m+1})h_{m-1}^{i-1}(x_1,\dots,x_{m-1}) = (x_m - x_{m+1})h_{m+1}^{j-1}(x_1,\dots,x_m,x_{m+1})$$

□

Note 3.28. No reference in literature has been found for the proof of Lemma 3.29.

Lemma 3.29. Let $f(x) \in R[x]$ be monic, $\deg(f) = n \geq 2$,

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0.$$

Let $g_1,\dots,g_n$ be the standard generating set for f. Then

$$\begin{aligned} g_1(x_1) &= h_1^n(x_1) + a_{n-1}h_1^{n-1}(x_1) + \cdots + a_1 h_1^1(x_1) + a_0 = f(x_1), \\ g_2(x_1,x_2) &= h_2^{n-1}(x_1,x_2) + a_{n-1}h_2^{n-2}(x_1,x_2) + \cdots + a_2 h_2^1(x_1,x_2) + a_1, \\ g_3(x_1,x_2,x_3) &= h_3^{n-2}(x_1,x_2,x_3) + a_{n-1}h_3^{n-3}(x_1,x_2,x_3) + \cdots + a_3 h_3^1(x_1,x_2,x_3) + a_2, \\ &\vdots \\ g_n(x_1,\dots,x_n) &= h_n^1(x_1,\dots,x_n) + a_{n-1}. \end{aligned}$$

In particular, for every $i \geq 2$,

$$g_i(x_1,\dots,x_i) \in (R[x_1,\dots,x_{i-1}])[x_i]$$

is monic and $\deg_{x_i}(g_i) = n - i + 1$.

Proof. We prove by induction on i that

$$g_i(x_1,\dots,x_i) = h_i^{n-i+1}(x_1,\dots,x_i) + a_{n-1}h_i^{n-i}(x_1,\dots,x_i) + a_{n-2}h_i^{n-i-1}(x_1,\dots,x_i) + \cdots \\ \cdots + a_i h_i^1(x_1,\dots,x_i) + a_{i-1}$$

for $i \in \{1,\dots,n\}$. This is true for $i = 1$, since

$$g_1(x_1) = f(x_1) = h_1^n(x_1) + a_{n-1}h_1^{n-1}(x_1) + \cdots + a_1 h_1^1(x_1) + a_0.$$

Let $i > 1$. By definition,

$$g_i(x_1,\dots,x_i) = \frac{g_{i-1}(x_1,\dots,x_{i-2},x_{i-1}) - g_{i-1}(x_1,\dots,x_{i-2},x_i)}{x_{i-1} - x_i}$$

By the induction hypothesis,

$$g_{i-1}(x_1,\dots,x_{i-2},x_{i-1}) = h_{i-1}^{n-i+2}(x_1,\dots,x_{i-1}) + a_{n-1}h_{i-1}^{n-i+1}(x_1,\dots,x_i) + \cdots \\ \cdots + a_{i-1}h_{i-1}^{1}(x_1,\dots,x_{i-1}) + a_{i-2}$$

By Lemma 3.27,

$$g_{i-1}(x_1,\dots,x_{i-2},x_{i-1}) - g_{i-1}(x_1,\dots,x_{i-2},x_i) = \\ = (x_{i-1}-x_i)h_i^{n-i+1}(x_1,\dots,x_{i-1},x_i) + a_{n-1}(x_{i-1}-x_i)h_i^{n-i}(x_1,\dots,x_{i-1},x_i) + \cdots \\ \cdots + a_{i-1}(x_{i-1}-x_i),$$

hence

$$\frac{g_{i-1}(x_1,\dots,x_{i-2},x_{i-1}) - g_{i-1}(x_1,\dots,x_{i-2},x_i)}{x_{i-1}-x_i} = \\ = h_i^{n-i+1}(x_1,\dots,x_{i-1},x_i) + a_{n-1}h_i^{n-i}(x_1,\dots,x_{i-1},x_i) + \cdots + a_{i-1}$$

which is what we wanted to prove. □

Lemma 3.30. Let R be an integral domain, $S = R[x_1,\dots,x_n]$, $n \geq 2$. Let

$$F(X) = \prod_{i=1}^{n}(X - x_i) \in S[X] \tag{3.10}$$

and $G_1(X_1),\dots,G_n(X_1,\dots,X_n) \in S[X_1,\dots,X_n]$ be the standard generating set for F. Then

$$G_i(x_1,\dots,x_i) = 0 \text{ in } S$$

for every $i \in \{1,\dots,n\}$.

Proof. We prove the following: for every $1 \leq i \leq n$, $\tau \in \mathcal{S}_n$,

$$G_i(x_{\tau(1)},\dots,x_{\tau(i)}) = 0 \text{ in } S.$$

This is clear for $i = 1$, because

$$G_1(x_j) = F(x_j) = 0$$

for every $j \in \{1,\dots,n\}$. Let $i > 1$. Then

$$(X_{\tau(i-1)} - X_{\tau(i)})G_i(X_{\tau(1)},\dots,X_{\tau(i)}) = G_{i-1}(X_{\tau(1)},\dots,X_{\tau(i-1)}) - G_{i-1}(X_{\tau(1)},\dots,X_{\tau(i)})$$

by the definition of G_i. By the induction hypothesis,

$$G_{i-1}(x_{\tau(1)},\dots,x_{\tau(i-1)}) - G_{i-1}(x_{\tau(1)},\dots,x_{\tau(i)}) = 0,$$

hence

$$(x_{\tau(i-1)} - x_{\tau(i)})G_i(x_{\tau(1)},\dots,x_{\tau(i)}) = 0$$

and

$$G_i(x_{\tau(1)},\dots,x_{\tau(i)}) = 0$$

as S is an integral domain. □

Lemma 3.31. Let R be an integral domain, $f(x) \in R[x]$, $\deg(f) = n \geq 2$,

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0.$$

Let $g_1, \ldots, g_n \in R[x_1, \ldots, x_n]$ be the standard generating set for f. Then

$$(g_1, \ldots, g_n) \subseteq I_f.$$

Proof. By definition, $I_f = (p_1, \ldots, p_n)$, where

$$\begin{aligned} p_1(x_1, \ldots, x_n) &:= s_1(x_1, \ldots, x_n) + a_{n-1}, \\ p_2(x_1, \ldots, x_n) &:= s_2(x_1, \ldots, x_n) - a_{n-2}, \\ &\vdots \\ p_n(x_1, \ldots, x_n) &:= s_n(x_1, \ldots, x_n) + (-1)^{n-1}a_0, \end{aligned}$$

and $s_1, \ldots, s_n$ are the elementary symmetric functions. Now, let $S = R[x_1, \ldots, x_n]$ and $F(x) \in S[x]$ be the polynomial defined by (3.10). We note that

$$F(X) = X^n - s_1(x_1, \ldots, x_n)X^{n-1} + \cdots + (-1)^n s_n(x_1, \ldots, x_n).$$

Let $i \in \{1, \ldots, n\}$. By Lemma 3.29,

$$g_i(x_1, \ldots, x_i) = h_i^{n-i+1}(x_1, \ldots, x_i) + a_{n-1}h_i^{n-i}(x_1, \ldots, x_i) + \cdots + a_i h_i^1(x_1, \ldots, x_i) + a_{i-1}.$$

Let $G_1, \ldots, G_n \in S[X_1, \ldots, X_n]$ be the standard generating set for F. Again, by Lemma 3.29,

$$\begin{aligned} G_i(X_1, \ldots, X_i) = h_i^{n-i+1}(X_1, \ldots, X_i) - s_1(x_1, \ldots, x_n)h_i^{n-i}(X_1, \ldots, X_i) + \cdots \\ \cdots + (-1)^{n-i}s_{n-i}(x_1, \ldots, x_n)h_i^1(X_1, \ldots, X_i) + (-1)^{n-i+1}s_{n-i+1}(x_1, \ldots, x_n). \end{aligned}$$

Hence

$$\begin{aligned} &g_i(x_1, \ldots, x_i) - G_i(x_1, \ldots, x_i) = \\ &= p_1(x_1, \ldots, x_n)h_i^{n-i}(x_1, \ldots, x_i) + \cdots + (-1)^{n-i+1}p_{n-i}(x_1, \ldots, x_n)h_i^1(x_1, \ldots, x_i) + \\ &\qquad + (-1)^{n-i}p_{n-i+1}(x_1, \ldots, x_n) \in I_f. \end{aligned}$$

By Lemma 3.30, $G_i(x_1, \ldots, x_i) = 0$, so $g_i(x_1, \ldots, x_i) \in I_f$. □

Lemma 3.32. Let R be a commutative ring, $f(x) \in R[x]$, $\deg(f) = n \geq 2$, and let $g_1(x_1), \ldots, g_n(x_1, \ldots, x_n) \in R[x_1, \ldots, x_n]$ be the standard generating set for f. Then

$$f(x) = \prod_{i=1}^{n}(x - [x_i])$$

over

$$R[x_1, \ldots, x_n] \Big/ (g_1(x_1), \ldots, g_n(x_1, \ldots, x_n)).$$

Proof. We proceed by induction on n. Let $n = 2$ and denote $R_1 = R[x_1]/(g_1(x_1))$. There's an epimorphism

$$\phi : R[x_1, x_2] \to R_1[x_2]$$

such that $\phi(x_2) = x_2$ and $\phi_{\restriction R[x_1]}$ is the natural projection $R[x_1] \to R_1$. Since

$$(x_2 - x_1)g_2(x_1, x_2) = f(x_2) - f(x_1)$$

holds in $R[x_1, x_2]$,

$$(x_2 - [x_1])g_2([x_1], x_2) = f(x_2) - \underbrace{f([x_1])}_{=[0]} = f(x_2)$$

holds in $R_1[x_2]$. Furthermore, the degree of $\tilde{f}(x) := g_2([x_1], x) \in R_1[x]$ is 1. Hence

$$f(x) = (x - [x_1])\tilde{f}(x)$$

splits over R_1, let alone over $R_1 \hookrightarrow R_1[x_2]/(\tilde{f}(x_2))$. By Lemma 3.21, the assignment

$$[h(x_1, x_2)] \mapsto [\phi(h(x_1, x_2))]$$

induces an isomorphism

$$R[x_1, x_2]/(g_1(x_1), g_2(x_1, x_2)) \to R_1[x_2]/(\tilde{f}(x_2)).$$

So f splits over

$$R[x_1, x_2] \Big/ (g_1(x_1), g_2(x_1, x_2)).$$

Let $n > 2$. Similarly, f factors as

$$f(x) = (x - [x_1])\tilde{f}(x)$$

over R_1, where $\tilde{f}(x) = g_2([x_1], x) \in R_1[x]$ and $\deg(\tilde{f}) = n - 1$. Applying the induction hypothesis on $\tilde{f}$,

$$\tilde{f}(x) = \prod_{i=2}^{n}(x - [x_i])$$

holds over

$$R_1[x_2, \ldots, x_n] \Big/ (g_2([x_1], x_2), \ldots, g_n([x_1], x_2, \ldots, x_n)).$$

Thus f splits over

$$R[x_1, \ldots, x_n] \Big/ (g_1(x_1), \ldots, g_n(x_1, \ldots, x_n)) \cong$$
$$\cong R_1[x_2, \ldots, x_n] \Big/ (g_2([x_1], x_2), \ldots, g_n([x_1], x_2, \ldots, x_n))$$

because the two rings are isomorphic by Lemma 3.21. □

Theorem 3.33. Let R be an integral domain, $f(x) \in R[x]$, $\deg(f) = n \geq 2$,

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0,$$

and let $g_1(x_1), \ldots, g_n(x_1, \ldots, x_n) \in R[x_1, \ldots, x_n]$ be the standard generating set for f. Then

$$I_f = (g_1, \ldots, g_n),$$

where I_f is the universal splitting ideal of f.

Proof. By Lemma 3.31, $J := (g_1, \ldots, g_n) \subseteq I_f$. For the reverse inclusion, consider the n elementary symmetric functions $s_1, \ldots, s_n \in R[x_1, \ldots, x_n]$. Recall that $I_f \subseteq R[x_1, \ldots, x_n]$ is the ideal generated by

$$\begin{aligned} p_1(x_1, \ldots, x_n) &= s_1(x_1, \ldots, x_n) + a_{n-1}, \\ p_2(x_1, \ldots, x_n) &= s_2(x_1, \ldots, x_n) - a_{n-2}, \\ &\vdots \\ p_n(x_1, \ldots, x_n) &= s_n(x_1, \ldots, x_n) + (-1)^{n-1} a_0. \end{aligned}$$

By Lemma 3.32,

$$f(x) = \prod_{i=1}^{n} (x - [x_i]) = x^n - s_1([x_1], \ldots, [x_n]) x^{n-1} + \cdots + (-1)^n s_n([x_1], \ldots, [x_n])$$

holds over $R[x_1, \ldots, x_n]/J$. Hence the equalities

$$\begin{aligned} [a_{n-1}] &= [-s_1(x_1, \ldots, x_n)], \\ [a_{n-2}] &= [s_2(x_1, \ldots, x_n)], \\ &\vdots \\ [a_0] &= [(-1)^n s_n(x_1, \ldots, x_n)], \end{aligned}$$

and $p_1, \ldots, p_n \in J$ holds. □

Lemma 3.34. Let R be an integral domain, $f(x) \in R[x]$, $\deg(f) = n \geq 2$. Let

$$S_f = R[x_1, \ldots, x_n]/I_f$$

be the universal splitting ring of f over R. Then

$$B = \{[x_1^{e_1} \cdots x_{n-1}^{e_{n-1}}] \mid 0 \leq e_i \leq n - i,\ i = 1, \ldots, n-1\}$$

generates the R-module S_f.

Proof. Let $h \in R[x_1, \ldots, x_n]$. We show that for every $i \in \{1, \ldots, n\}$, there's a polynomial $r_i \in R[x_1, \ldots, x_n]$ such that

$$h - r_i \in I_f$$

and

$$\deg_{x_n}(r_i) < 1,\ \deg_{x_{n-1}}(r_i) < 2, \ldots, \deg_{x_{n-i+1}}(r_i) < i. \tag{3.11}$$

Let $g_1, \ldots, g_n$ be the standard generating set for f. By Theorem 3.33,

$$I_f = (g_1, \ldots, g_n).$$

By Lemma 3.29, $g_n(x_1, \ldots, x_n) \in (R[x_1, \ldots, x_{n-1}])[x_n]$ is monic and $\deg_{x_n}(g_n) = 1$. Dividing h by g_n with remainder in $(R[x_1, \ldots, x_{n-1}])[x_n]$, we obtain polynomials $q, r_1 \in R[x_1, \ldots, x_n]$ such that

$$h(x_1, \ldots, x_n) = q(x_1, \ldots, x_n) g_n(x_1, \ldots, x_n) + r_1(x_1, \ldots, x_n)$$

and $\deg_{x_n}(r_1) < 1 = \deg_{x_n}(g_n)$. Let $i > 1$. By the induction hypothesis, there's $r_{i-1} \in R[x_1, \ldots, x_n]$ such that

$$h - r_{i-1} \in I_f$$

and

$$\deg_{x_n} r_{i-1} < 1,\ \deg_{x_{n-1}}(r_{i-1}) < 2, \ldots, \deg_{x_{n-i+2}}(r_{i-1}) < i - 1.$$

By Lemma 3.29, g_{n-i+1} is monic with respect to the variable x_{n-i+1} and

$$\deg_{x_{n-i+1}}(g_{n-i+1}) = i.$$

So we can divide r_{i-1} with remainder by g_{n-i+1} in $(R[x_1, \ldots, \hat{x}_{n-i+1}, \ldots, x_n])[x_{n-i+1}]$:

$$r_{i-1}(x_1, \ldots, x_n) = q_i(x_1, \ldots, x_n) g_{n-i+1}(x_1, \ldots, x_{n-i+1}) + r_i(x_1, \ldots, x_n).$$

The polynomial r_i then satisfies (3.11) and the condition

$$h - r_i \in I_f$$

also holds. Finally, we note that r_n is a linear combination of elements from B and $[h] = [r_n]$ in S_f. □

Lemma 3.35. Let R be an integral domain, $f(x) \in R[x]$, $\deg(f) = n \geq 2$. Let

$$S_f = R[x_1, \ldots, x_n]/I_f$$

be the universal splitting ring of f over R. Then

$$B = \{[x_1^{e_1} \cdots x_{n-1}^{e_{n-1}}] \mid 0 \leq e_i \leq n - i,\ i = 1, \ldots, n-1\}$$

is R-linearly independent.

Proof. Let $g_1, \ldots, g_n$ be the standard generating set for f. Let

$$h(x_1, \ldots, x_n) \in R[x_1, \ldots, x_n]$$

be a polynomial with terms over

$$\{x_1^{e_1} \cdots x_{n-1}^{e_{n-1}} \mid 0 \leq e_i \leq n - i,\ i = 1, \ldots, n-1\} \tag{3.12}$$

such that

$$h(x_1, \ldots, x_n) \in I_f \text{ (i.e. } [h(x_1, \ldots, x_n)] = 0 \text{ in } S_f).$$

We want to show that h is the zero polynomial. By Theorem 3.33, there exist polynomials $c_1, \ldots, c_n \in R[x_1, \ldots, x_n]$:

$$h(x_1, \ldots, x_n) = \sum_{i=1}^{n} c_i(x_1, \ldots, x_n) g_i(x_1, \ldots, x_i).$$

We prove by induction that

$$c_{n-j+1} = 0$$

for every $j \in \{1, \ldots, n\}$. By Lemma 3.29, $\deg_{x_n}(g_n) = 1$ but $\deg_{x_n}(h) = 0$ because h has terms from (3.12). This implies $c_n = 0$. Let $j > 1$. By the induction hypothesis,

$$c_n = c_{n-1} = \cdots = c_{n-j+2} = 0,$$

hence

$$h(x_1, \ldots, x_n) = \sum_{i=1}^{n-j+1} c_i(x_1, \ldots, x_n) g_i(x_1, \ldots, x_i).$$

Moreover, By the choice of h, we have

$$\deg_{x_{n-j+1}}(h) \leq j - 1.$$

By Lemma 3.29,

$$\deg_{x_{n-j+1}}(g_{n-j+1}) = j.$$

This implies $c_{n-j+1} = 0$. So $c_i = 0$ for every i and h is the zero polynomial. □

By Lemma 3.34 and 3.35, we have the following theorem.

Theorem 3.36. Let R be an integral domain, $f(x) \in R[x]$, $\deg(f) \geq 2$. Let

$$S_f = R[x_1, \ldots, x_n]/I_f$$

be the universal splitting ring of f over R. Then

$$B = \{[x_1^{e_1} \cdots x_{n-1}^{e_{n-1}}] \mid 0 \leq e_i \leq n - i,\ i = 1, \ldots, n-1\}$$

is a free basis of the free R-module S_f. That is, B is R-linearly independent set which generates S_f.

In case R is a field, the standard generating set for f is a Gröbner basis of I_f.

Proposition 3.37 ([4], Tvrzení 22.5, p. 152)**.** Let K be a field and let $f_1, \ldots, f_n \in K[x_1, \ldots, x_n]$ be a triangular basis of an ideal $I \subseteq K[x_1, \ldots, x_n]$. In other words, $\{f_1, \ldots, f_n\}$ generates I and

$$f_1 \in I \cap K[x_1],\ f_2 \in I \cap K[x_1, x_2], \ldots, f_{n-1} \in I \cap K[x_1, \ldots, x_{n-1}].$$

Then $\{f_1, \ldots, f_n\}$ is a Gröbner basis of I with respect to the lexicographic order $<$ on terms such that $x_1 < \cdots < x_n$. In particular, the standard generating set $g_1, \ldots, g_n$ for $f \in K[x]$ is a Gröbner basis with respect to the lexicographic order $<$ on terms such that $x_1 < \cdots < x_n$.

3.3 The universal splitting ring of a separable polynomial

Recall that K denotes a perfect field. Throughout this part, we use the following notation:

$$\left.\begin{array}{c} f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in K[x] \text{ is a separable polynomial,} \\ \alpha_1, \ldots, \alpha_n \in \overline{K} \text{ are its roots, } I_f \text{ is the universal splitting ideal of } f, \\ M \text{ is the splitting ideal of } f \text{ with respect to the given order of the roots} \end{array}\right\} \tag{3.13}$$

Remark 3.38. With the above notation, let

$$S_f = K[x_1, \ldots, x_n]/I_f$$

be the universal splitting ring of f. By Theorem 3.36, every element of S_f has a unique representative from $K[x_1, \ldots, x_n]$ with terms from

$$\{x_1^{e_1} \cdots x_{n-1}^{e_{n-1}} \mid 0 \leq e_i \leq n - i,\ i = 1, \ldots, n-1\}. \tag{3.14}$$

So we can identify elements of S_f with their representatives from $K[x_1, \ldots, x_n]$ (such that their terms are from (3.14)).

Theorem 3.39. With the notation of (3.13), the universal splitting ring

$$S_f = K[x_1, \ldots, x_n]/I_f$$

of f has exactly $k = [\mathcal{S}_n : \mathrm{Gal}(f)]$ primitive idempotents $e_1, \ldots, e_k$, where $\mathrm{Gal}(f)$ is the Galois group of f with respect to the order of the roots of f given by (3.13). Moreover,

$$\sum_{i=1}^{k} e_i = 1 \tag{3.15}$$

and there is a unique element $e \in \{e_1, \ldots, e_k\}$ such that

$$M = \{g \in K[x_1, \ldots, x_n] \mid ge \in I_f\}. \tag{3.16}$$

We call the idempotent e the primitive idempotent corresponding to the ideal M.

Proof. By Theorem 3.20, S_f is the direct product of the k fields

$$K[x_1, \ldots, x_n]/M_i,\ i = 1, \ldots k,$$

where $k = [\mathcal{S}_n : \mathrm{Gal}(f)]$ and $I_f \subseteq M_1 (= M), \ldots, M_k$ are maximal ideals. Let

$$\psi : S_f \to K[x_1, \ldots, x_n]/M_1 \times \cdots \times K[x_1, \ldots, x_n]/M_k,$$

$$\psi([x_i]) = ([x_i], \ldots, [x_i]),\ i = 1, \ldots, k,$$

be the isomorphism from Theorem 3.20. By Proposition 1.5, S_f has k idempotents $e_1, \ldots, e_k$ and there's exactly one $e \in \{e_1, \ldots, e_k\}$ such that

$$\psi(e) = (1, 0, \ldots, 0).$$

As

$$e - 1 \in M_1,\ e \in M_i \text{ for } i = 2, \ldots, k, \tag{3.17}$$

we're ready to prove (3.16). If $g \in M_1$, then $ge \in \cap_{i=1}^{k} M_i = I_f$ by (3.17). On the other hand, let $ge \in I_f \subseteq M_1$. Since M_1 is maximal, it is prime and either $g \in M_1$ or $e \in M_1$. As we know $e \notin M_1$, it follows that $e \in M_1$. Finally, (3.15) is again a direct consequence of Proposition 1.5. □

Recall that for $\tau \in \mathcal{S}_n$ and $g(x_1, \ldots, x_n) \in K[x_1, \ldots, x_n]$, we denote by $\tau * g(x_1, \ldots, x_n)$, or simply $\tau * g$, the polynomial $g(x_{\tau(1)}, \ldots, x_{\tau(n)})$.

Lemma 3.40. With the notation of (3.13), let $g \in K[x_1, \ldots, x_n]$ and $\tau \in \mathcal{S}_n$. Then the map $[g] \mapsto [\tau * g]$ is an automorphism of $S_f = K[x_1, \ldots, x_n]/I_f$ and thus the symmetric group acts on S_f.

Proof. We first show that the map is defined correctly. Let $g_1, g_2 \in K[x_1, \ldots, x_n]$ such that $g_1 - g_2 \in I_f$. Then $\tau * (g_1 - g_2) \in I_f$ because I_f is generated by symmetric polynomials. It follows

$$[\tau * g_1] - [\tau * g_2] = [\tau * g_1 - \tau * g_2] = [\tau * (g_1 - g_2)] = [0],$$

hence $[\tau * g_1] = [\tau * g_2]$. From the fact that the map $g \mapsto \tau * g$ is an automorphism of $K[x_1, \ldots, x_n]$ it follows that the map $[g] \mapsto [\tau * g]$ is an endomorphism of S_f, which is clearly surjective. To show that it's injective, let $g_1, g_2 \in K[x_1, \ldots, x_n]$ be such that $[\tau * g_1] = [\tau * g_2]$, which is equivalent to $\tau * (g_1 - g_2) \in I_f$. Again, as I_f is generated by symmetric polynomials, $g_1 - g_2 = \tau^{-1} * (\tau * (g_1 - g_2)) \in I_f$, i.e. $[g_1] = [g_2]$. □

Proposition 3.41. With the notation of (3.13), let $e \in S_f = K[x_1, \ldots, x_n]/I_f$ be the primitive idempotent corresponding to M and $\tau \in \mathcal{S}_n$. Then

$$\mathrm{Stab}(\tau * e) = \tau \mathrm{Gal}(f) \tau^{-1},$$

where $\mathrm{Stab}(\tau * e) \subseteq \mathcal{S}_n$ is the stabilizer of $\tau * e$ under the action from Lemma 3.40 and $\mathrm{Gal}(f)$ is the Galois group of f with respect to the order of the roots of f given by (3.13). In particular,

$$\mathrm{Stab}(e) = \mathrm{Gal}(f).$$

Proof. By (3.5), the field

$$K[x_1, \ldots, x_n]/M$$

is isomorphic to $K(\alpha_1, \ldots, \alpha_n)$, the splitting field of f, via the assignment

$$[x_i] \mapsto \alpha_i,\ i = 1, \ldots, k.$$

The group $\mathrm{Aut}_K(K[x_1, \ldots, x_n]/M)$ can be therefore identified with a subgroup of $\mathcal{S}_n$ equal to $\mathrm{Gal}(f)$. Now, let

$$\psi : S_f \to K[x_1, \ldots, x_n]/M_1 \times \cdots \times K[x_1, \ldots, x_n]/M_k,$$

$$\psi([x_i]) = ([x_i], \ldots, [x_i]),\ i = 1, \ldots, k$$

be the isomorphism from Theorem 3.20, where $k = [\mathcal{S}_n : \mathrm{Gal}(f)]$ and

$$I_f \subseteq M_1(= M), \ldots, M_k$$

are maximal ideals. Since e is the primitive idempotent corresponding to $M_1 = M$,

$$\psi(e) = (1, 0, \ldots, 0),$$

and there's an isomorphism

$$eS_f \cong K[x_1, \ldots, x_n]/M,$$

$$e[x_i] \mapsto [x_i],\ i = 1, \ldots, k.$$

Thus $\mathrm{Gal}(f)$ is also the group of automorphisms of eS_f. Then for every $\tau \in \mathrm{Gal}(f)$, $\tau * (e[1]_{I_f}) = e[1]_{I_f}$ and $\mathrm{Gal}(f) \subseteq \mathrm{Stab}(e)$. Conversely, if $\tau \in \mathrm{Stab}(e)$, τ induces an automorphism of eS_f by Lemma 3.40. Hence $\tau \in \mathrm{Gal}(f)$ and $\mathrm{Gal}(f) = \mathrm{Stab}(e)$.

Finally, let $\tau \in \mathcal{S}_n$. Denote $M^\tau = \{\tau * g \mid g \in M\}$. By (3.16),

$$M^\tau = \{g \in K[x_1, \ldots, x_n] \mid g \cdot (\tau * e) \in I_f\}.$$

Hence $\tau * e$ is the primitive idempotent corresponding to M^τ. It's an easy observation that M^τ is the splitting ideal of f with respect to the order $\alpha_{\tau^{-1}(1)}, \ldots, \alpha_{\tau^{-1}(n)}$ of the roots of f. So by the above paragraph, $\mathrm{Stab}(\tau * e)$ is the Galois group of f with respect to the roots reodered according to τ^{-1}, i.e. $\mathrm{Stab}(\tau * e) = \tau \mathrm{Gal}(f) \tau^{-1}$ by Lemma 1.34. □

Proposition 3.42. With the notation of (3.13), let $\mathcal{E}$ be the set of primitive idempotents of the universal splitting ring S_f. Then $\mathcal{S}_n$ act transitively on $\mathcal{E}$.

Proof. Let $\tau \in \mathcal{S}_n$. By Lemma 3.40,

$$[g] \mapsto [\tau * g]$$

induces an automorphism of S_f for every $\tau \in \mathcal{S}_n$. Thus $\tau * e$ is a primitive idempotent for every $e \in \mathcal{E}$ and $\mathcal{S}_n$ acts on $\mathcal{E}$. Let e be the primitive idempotent corresponding to the ideal M. By Lemma 1.10, the length of the orbit of e is equal to $[\mathcal{S}_n : \mathrm{Stab}(e)]$. As $\mathrm{Stab}(e) = \mathrm{Gal}(f)$ by Proposition 3.41, the length of the orbit of e is equal to

$$[\mathcal{S}_n : \mathrm{Gal}(f)] = |\mathcal{E}|,$$

where the last equality follows from Theorem 3.39. □

Lemma 3.43. Let $e \in S_f$ be an idempotent. Then e is a sum of primitive idempotents (we call those its primitive components). A primitive idempotent $f \in S_f$ is a component of e iff $ef = f$.

Proof. The first assertion follows if we view S_f as a product of fields using the isomorphism ψ from Theorem 3.20. So let $e = e_1 + \cdots + e_l$, $l \in \mathbb{N}$, $e_1, \ldots, e_l \in S_f$ primitive idempotents. By Lemma 1.3, if $f = e_i$ for some i then $ef = f$. Otherwise, $ef = 0$. □

3.4 More about idempotents

Let $f \in \mathbb{Z}[x]$, $\deg(f) = n$. Throughout this section,

$$S_f = \mathbb{Q}[x_1, \ldots, x_n]/I_f$$

denotes the universal splitting ring of f over $\mathbb{Q}$.

Definition 3.44. Let $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$, $p \in \mathbb{N}$ a prime. We denote by $I_f^{(\infty)}$ the universal splitting ideal of f over $\mathbb{Q}_p$. In other words, $I_f^{(\infty)}$ is the ideal generated in $\mathbb{Q}_p[x_1, \ldots, x_n]$ by the polynomials

$$\begin{gathered} s_1(x_1, \ldots, x_n) + a_{n-1}, \\ s_2(x_1, \ldots, x_n) - a_{n-2}, \\ \vdots \\ s_n(x_1, \ldots, x_n) + (-1)^{n-1}a_0, \end{gathered}$$

where $s_1, \ldots, s_n$ are the elementary symmetric polynomials. Moreover, we denote by

$$S_f^{(\infty)} = \mathbb{Q}_p[x_1, \ldots, x_n]/I_f^{(\infty)}$$

the universal splitting ring of f over $\mathbb{Q}_p$.

Proposition 3.45. Let $f(x) \in \mathbb{Z}[x]$ be monic, $\deg(f) = n$, $p \in \mathbb{N}$ a prime. Let

$$S_f = \mathbb{Q}[x_1, \ldots, x_n]/I_f$$

be the universal splitting ring of f over $\mathbb{Q}$. Then S_f embeds into $S_f^{(\infty)}$.

Proof. As $\mathbb{Q} \subseteq S_f^{(\infty)} = \mathbb{Q}_p[x_1, \ldots, x_n]/I_f^{(\infty)}$, Lemma 3.4 implies that there's a homomorphism

$$\psi : S_f \to S_f^{(\infty)}$$

such that $\psi([x_i]) = [x_i]$, $i = 1, \ldots, n$. To show that ψ is injective, note that by Theorem 3.36,

$$B = \{[x_1^{e_1} \cdots x_{n-1}^{e_{n-1}}] \mid 0 \leq e_i \leq n - i,\ i = 1, \ldots, n-1\} \subseteq S_f^{(\infty)}$$

is a $\mathbb{Q}_p$-basis of $S_f^{(\infty)}$. In particular, elements of B are $\mathbb{Q}_p$-linearly independent. Let

$$0 \leq e_i \leq n - i,\ i = 1, \ldots, n-1.$$

As

$$\psi([x_1^{e_1} \cdots x_{n-1}^{e_{n-1}}]) = [x_1^{e_1} \cdots x_{n-1}^{e_{n-1}}],$$

it follows that ψ is injective because

$$\{[x_1^{e_1} \cdots x_{n-1}^{e_{n-1}}] \in S_f,\ 0 \leq e_i \leq n - i,\ i = 1, \ldots, n-1\}$$

is a $\mathbb{Q}$-basis of S_f by Theorem 3.36. □

Corollary 3.46 ([26], Proposition 17)**.** Let e be an idempotent in $S_f = \mathbb{Q}[x_1, \ldots, x_n]/I_f$. Then e is an idempotent in $S_f^{(\infty)}$.

Although every idempotent in S_f is an idempotent in $S_f^{(\infty)}$, it is not true that every primitive idempotent in S_f is a primitive idempotent in $S_f^{(\infty)}$, as we shall see later. Recall that $\mathbb{Z}_p \subseteq \mathbb{Q}_p$ denotes the ring of p-adic integers.

Definition 3.47. Let $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$, $p \in \mathbb{N}$ a prime. We denote by I_f^+ the universal splitting ideal of f over $\mathbb{Z}_p$. That is, I_f^+ is the ideal generated in $\mathbb{Z}_p[x_1, \ldots, x_n]$ by the polynomials

$$\begin{gathered} s_1(x_1, \ldots, x_n) + a_{n-1}, \\ s_2(x_1, \ldots, x_n) - a_{n-2}, \\ \vdots \\ s_n(x_1, \ldots, x_n) + (-1)^{n-1}a_0, \end{gathered}$$

where $s_1, \ldots, s_n$ are the elementary symmetric polynomials. Moreover, we denote by

$$S_f^+ = \mathbb{Z}_p[x_1, \ldots, x_n]/I_f^+$$

the universal splitting ring of f over $\mathbb{Z}_p$.

Proposition 3.48. Let $f \in \mathbb{Z}[x_1, \ldots, x_n]$ be monic, $\deg(f) = n$, $p \in \mathbb{N}$ a prime. Then S_f^+ embeds into $S_f^{(\infty)}$.

Proof. Recall that

$$S_f^{(\infty)} = \mathbb{Q}_p[x_1, \ldots, x_n]/I_f^{(\infty)}.$$

As $\mathbb{Z}_p \subseteq S_f^{(\infty)}$, there's a ring homomorphism

$$\psi : S_f^+ \to S_f^{(\infty)},$$

$\psi([x_i]) = [x_i]$, $i = 1, \ldots, n$, by Lemma 3.4. By Theorem 3.36,

$$B' = \{[x_1^{e_1} \cdots x_{n-1}^{e_{n-1}}] \mid 0 \leq e_i \leq n - i,\ i = 1, \ldots, n-1\} \subseteq S_f^+$$

generates S_f^+ as a $\mathbb{Z}_p$-module. Similarly, by Theorem 3.36,

$$B = \{[x_1^{e_1} \cdots x_{n-1}^{e_{n-1}}] \mid 0 \leq e_i \leq n - i,\ i = 1, \ldots, n-1\} \subseteq S_f^{(\infty)}$$

is a $\mathbb{Q}_p$-basis of $S_f^{(\infty)}$. Let $s = \sum_i z_i b_i \in S_f^+$ with $z_i \in \mathbb{Z}_p$, $b_i \in B'$. If

$$s = 0$$

then

$$\psi(s) = \sum_i z_i \psi(b_i) = 0$$

and $\psi(b_i)$ are distinct elements of B. Hence $z_i = 0$ for every i and ψ is injective. □

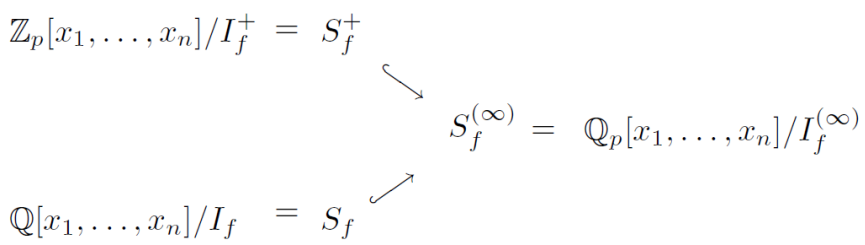

Figure 3.1: S_f and S_f^+ embed into $S_f^{(\infty)}$

We need three more auxiliary lemmata before addressing the main topic of this section.

Lemma 3.49. Let $f(x) \in \mathbb{Z}[x]$ be a monic polynomial separable over $\mathbb{Q}$, $p \in \mathbb{N}$ a prime. Then $\bar{f} := f \bmod p \in \mathbb{F}_p[x]$ is separable (over $\mathbb{F}_p$) iff $p \nmid \operatorname{disc}(f)$.

Proof. By Proposition 2.3,

$$R(\bar{f}, \bar{f}') = R(f, f') \bmod p.$$

Hence, by Proposition 2.4, the discriminant of $\bar{f}$ over $\mathbb{F}_p$ is equal to

$$\operatorname{disc}(\bar{f}) = (-1)^{n(n-1)/2} R(\bar{f}, \bar{f}') = \operatorname{disc}(f) \bmod p.$$

So $\bar{f}$ is separable over $\mathbb{F}_p$ iff $p \nmid \operatorname{disc}(f)$ by Remark 1.44. □

Note 3.50. The following lemma is stated in [26, Lemma 13] without a proof.

Lemma 3.51. Let $f(x) \in \mathbb{Z}[x]$ be a monic polynomial separable over $\mathbb{Q}$, $\deg(f) = n$, let $p \in \mathbb{N}$ be a prime such that $p \nmid \operatorname{disc}(f)$. Let I_f be the universal splitting ideal of f over $\mathbb{Q}$ and $\bar{I}_f := I_{\bar{f}}$ the universal splitting ideal of $\bar{f} = f \bmod p$ over $\mathbb{F}_p$. Then

$$\bar{I}_f = \pi(I_f \cap \mathbb{Z}[x_1,\ldots,x_n]),$$

where

$$\pi : \mathbb{Z} \to \mathbb{F}_p$$

is the canonical epimorphism (such that $\pi(z) = z \bmod p$ for every $z \in \mathbb{Z}$).

Proof. As π is surjective, $\pi(I_f \cap \mathbb{Z}[x_1,\ldots,x_n])$ is an ideal in $\mathbb{F}_p[x_1,\ldots,x_n]$ by Lemma 3.13. Let

$$g_1,\ldots,g_n \in \mathbb{Z}[x_1,\ldots,x_n]$$

be the standard generating set for f. By Lemma 3.29, $\pi(g_1),\ldots,\pi(g_n)$ is the standard generating set for $\bar{f} \in \mathbb{F}_p$. By Theorem 3.33,

$$\bar{I}_f = (\pi(g_1),\ldots,\pi(g_n)) \subseteq \pi(I_f \cap \mathbb{Z}[x_1,\ldots,x_n]).$$

For the reverse inclusion, we note that by Proposition 3.37, $g_1,\ldots,g_n$ is a Gröbner basis of I_f with respect to the lexicographic order $<$ on terms such that $x_1 < \cdots < x_n$. For each i, the leading monomial of g_i is monic. This means that every polynomial from $\mathbb{Z}[x_1,\ldots,x_n]$ can be reduced modulo $\{g_1,\ldots,g_n\}$ without

using fractions. More precisely, if $h \in I_f \cap \mathbb{Z}[x_1, \ldots, x_n]$, there exist polynomials $q_1, \ldots, q_n \in \mathbb{Z}[x_1, \ldots, x_n]$ such that

$$h = \sum_{i=1}^{n} q_i g_i.$$

Now, $\pi(h) \in \pi(I_f \cap \mathbb{Z}[x_1, \ldots, x_n])$ can be expressed as

$$\pi(h) = \sum_{i=1}^{n} \pi(q_i)\pi(g_i) \in \bar{I}_f.$$

□

Lemma 3.52. Let $f(x) \in \mathbb{Z}[x]$ be separable over $\mathbb{Q}$, $p \in \mathbb{N}$ a prime. Then f is separable over $\mathbb{Q}_p$.

Proof. As f is separable over $\mathbb{Q}$, the discriminant $d :=\text{disc}(f) \neq 0$ by Remark 1.44. Over $\mathbb{Q}_p$, the discriminant is also equal to d, so f is separable over $\mathbb{Q}_p$. □

Let $f(x) \in \mathbb{Z}[x]$ be monic and separable over $\mathbb{Q}$, $p \in \mathbb{N}$ a prime, $p \nmid \text{disc}(f)$. Then f is separable over $\mathbb{Q}_p$ by Lemma 3.52 and $\bar{f} := f \bmod p$ is separable over $\mathbb{F}_p$ by Lemma 3.49. We can therefore apply what we proved in Section 3.3 on the rings $S_f^{(\infty)}$ and

$$S_{\bar{f}} = \mathbb{F}_p[x_1, \ldots, x_n]/\bar{I}_f,$$

where $\bar{I}_f := I_{\bar{f}}$ is the universal splitting ideal of $\bar{f}$ over $\mathbb{F}_p$. In fact, there's a one-to-one correspondence between primitive idempotents in these two rings. This is what we aim to prove in the rest of this section.

Remark 3.53. Let $z = \sum_{i\geq 0}^{\infty} a_i p^i \in \mathbb{Z}_p$. Define

$$z \bmod p := a_0.$$

Then

$$z \mapsto z \bmod p$$

is a surjective homomorphism

$$\mathbb{Z}_p \to \mathbb{F}_p.$$

Lemma 3.54. Let $f(x) \in \mathbb{Z}[x]$ be monic and separable, $\deg(f) = n$. Let p be a prime such that $p \nmid \text{disc}(f)$. Let

$$S_f^+ = \mathbb{Z}_p[x_1, \ldots, x_n]/I_f^+$$

be the universal splitting ring of f over $\mathbb{Z}_p$ and $\bar{I}_f$ the universal splitting ideal of $f \bmod p$ over $\mathbb{F}_p$. There's a surjective ring homomorphism

$$\pi_p : S_f^+ \to \mathbb{F}_p[x_1, \ldots, x_n]/\bar{I}_f$$

such that $\pi_p(z) = z \bmod p$ for every $z \in \mathbb{Z}_p$.

Proof. The homomorphism

$$\mathbb{Z}_p \to \mathbb{F}_p$$
$$z \mapsto z \bmod p := a_0$$

can be extended to a surjective ring homomorphism

$$\mathbb{Z}_p[x_1, \ldots, x_n] \to \mathbb{F}_p[x_1, \ldots, x_n]/\bar{I}_f$$

by Lemma 3.12. Using Lemma 3.51, it's easy to verify that the kernel of this homomorphism contains I_f^+. Hence,

$$\mathbb{Z}_p[x_1, \ldots, x_n]/I_f^{(\infty)+} \to \mathbb{F}_p[x_1, \ldots, x_n]/\bar{I}_f,$$
$$\sum_{\underline{u}} z_{\underline{u}}[\mathbf{x}^{\underline{u}}] \mapsto \sum_{\underline{u}} \pi(z_{\underline{u}})[\mathbf{x}^{\underline{u}}]$$

is a well defined epimorphism that extends π_p. □

By Proposition 3.48, $S_f^+ = \mathbb{Z}_p[x_1, \ldots, x_n]/I_f^+$ may be considered a subring of $S_f^{(\infty)}$ and we use this fact in the following lemma. We also use the fact that every element of $S_f^{(\infty)}$ (resp. S_f^+) has a unique representative from $\mathbb{Q}_p[x_1, \ldots, x_n]$ (resp. $\mathbb{Z}_p[x_1, \ldots, x_n]$) with terms from

$$\{x_1^{e_1} \cdots x_{n-1}^{e_{n-1}}] \mid 0 \leq e_i \leq n - i, i = 1, \ldots, n-1\}$$

by Theorem 3.36. This way, we may identify elements of $S_f^{(\infty)}$ with their representatives from $\mathbb{Q}_p[x_1, \ldots, x_n]$.

Lemma 3.55 ([26], Lemma 15)**.** Let $f(x) \in \mathbb{Z}[x]$ be monic and separable, $\deg(f) = n$. Let p be a prime such that $p \nmid \operatorname{disc}(f)$. Let

$$e^{(\infty)} = \sum_{0 \leq e_1 \leq n-1} \cdots \sum_{0 \leq e_{n-1} \leq 1} q_{e_1, \ldots, e_{n-1}} x^{e_1} \cdots x^{e_{n-1}} \in \mathbb{Q}_p[x_1, \ldots, x_n]$$

be an idempotent in $S_f^{(\infty)}$. Then

$$e^{(\infty)} \in \mathbb{Z}_p[x_1, \ldots, x_n].$$

Now, let $\bar{I}_f \subseteq \mathbb{F}_p[x_1, \ldots, x_n]$ be the universal splitting ideal of $\bar{f} = f \bmod p$ over $\mathbb{F}_p$ and

$$\pi_p : S_f^+ \to \mathbb{F}_p[x_1, \ldots, x_n]/\bar{I}_f$$

the homomorphism from Lemma 3.54. Then

$$\bar{e} = \pi_p(e^{(\infty)}) \neq 0$$

is an idempotent in the universal splitting ring $S_{\bar{f}}$ of $\bar{f}$ over $\mathbb{F}_p$.

Proof. For a contradiction, assume that $q_{e_1, \ldots, e_{n-1}} \in \mathbb{Q}_p \setminus \mathbb{Z}_p$ for some $e_1, \ldots, e_{n-1}$. Then there exists a positive integer $k \in \mathbb{N}$ such that

$$p^k q_{e_1, \ldots, e_{n-1}} \in \mathbb{Z}_p$$

for every $0 \leq e_1 \leq n-1, \ldots, 0 \leq e_{n-1} \leq 1$. Let k be the smallest such integer. Then $\pi_p(p^k q_{e_1,\ldots,e_{n-1}}) \neq 0$ for some $(e_1, \ldots, e_{n-1})$. Now, define

$$u = \sum_{0 \leq e_1 \leq n-1} \cdots \sum_{0 \leq e_{n-1} \leq 1} (p^k q_{e_1,\ldots,e_{n-1}})[x^{e_1} \cdots x^{e_{n-1}}] \in S_f^+.$$

By the choice of k, $\pi_p(u) \neq 0$. Since

$$(e^{(\infty)})^2 = e^{(\infty)}$$

holds in $S_f^{(\infty)}$ and $u = p^k e^{(\infty)}$, it follows that

$$u^2 = p^k u$$

holds in S_f^+. Consequently, as k is positive,

$$0 = \pi_p(p^k u) = \pi_p(u^2) = (\pi_p(u))^2.$$

By Theorem 3.20, $\mathbb{F}_p[x_1, \ldots, x_n]/\bar{I}_f$ is a direct product of fields and $(\pi_p(u))^2 = 0$ implies $\pi_p(u) = 0$. That's a contradiction.

We've established that $e^{(\infty)} \in \mathbb{Z}_p[x_1, \ldots, x_n]$. Clearly,

$$(\pi_p(e^{(\infty)}))^2 = \pi_p(e^{(\infty)})$$

because π_p is a homomorphism. So we need to show that

$$\bar{e} := \pi_p(e^{(\infty)}) \neq 0.$$

Again, assume for a contradiction that $\bar{e} = 0$. There's a positive integer $l \in \mathbb{N}$ and $z^{(\infty)} \in \mathbb{Z}_p[x_1, \ldots, x_n]$, $\pi_p(z^{(\infty)}) \neq 0$, such that

$$e^{(\infty)} = p^l z^{(\infty)}.$$

In $S_f^{(\infty)}$,

$$p^l z^{(\infty)} = e^{(\infty)} = (e^{(\infty)})^2 = p^{2l}(z^{(\infty)})^2$$

holds. Hence

$$z^{(\infty)} = p^l (z^{(\infty)})^2 = e^{(\infty)} z^{(\infty)}$$

and

$$0 \neq \pi_p(z^{(\infty)}) = \underbrace{\pi_p(e^{(\infty)})}_{=0} \pi_p(z^{(\infty)}).$$

This is a contradiction. □

Definition 3.56. Let $p \in \mathbb{N}$ be a prime,

$$a = \sum_{i \geq 0}^{\infty} a_i p^i, \ b = \sum_{i \geq 0}^{\infty} b_i p^i \in \mathbb{Z}_p,$$

$n \in \mathbb{N}$. We write $a \equiv b \pmod{p^n}$ if $(a-b)/p^n \in \mathbb{Z}_p$, where $(a-b)/p^n$ is considered an element of $\mathbb{Q}_p$. This is equivalent to $a_i = b_i$ for every $i = 0, \ldots, n-1$.

For polynomials $a(x_1, \ldots, x_n), b(x_1, \ldots, x_n) \in \mathbb{Z}_p[x_1, \ldots, x_n]$,

$$a(x_1, \ldots, x_n) \equiv b(x_1, \ldots, x_n) \pmod{p^n}$$

if

$$(a(x_1,\ldots,x_n)-b(x_1,\ldots,x_n))/p^n \in \mathbb{Z}_p[x_1,\ldots,x_n].$$

By Theorem 3.36, every element of

$$S_f^+ = \mathbb{Z}_p[x_1,\ldots,x_n]/I_f^+$$

has a unique representative from $\mathbb{Z}_p[x_1,\ldots,x_n]$ with coefficients from

$$\{[x_1^{e_1}\cdots x_{n-1}^{e_{n-1}}] \mid 0 \le e_i \le n-i, i=1,\ldots,n-1\}.$$

The equivalence $\equiv$ thus translates to S_f^+ by emulating the representatives.

Theorem 3.57 ([26], Theorem 20)**.** Let $f(x) \in \mathbb{Z}[x]$ be monic and separable, $\deg(f)=n$. Let p be a prime such that $p \nmid \operatorname{disc}(f)$. The homomorphism

$$\pi_p : S_f^+ \to \mathbb{F}_p[x_1,\ldots,x_n]/\bar{I}_f$$

from Lemma 3.54 gives a one-to-one corresponcence between the set of idempotents of $S_f^{(\infty)}$ and the set of idempotents of $S_{\bar{f}} = \mathbb{F}_p[x_1,\ldots,x_n]/\bar{I}_f$, where $\bar{I}_f \subseteq \mathbb{F}_p[x_1,\ldots,x_n]$ is the universal splitting ideal of $\bar{f} = f \bmod p$ over $\mathbb{F}_p$.

Proof. By Lemma 3.55, every idempotent in $S_f^{(\infty)}$ belongs to S_f^+ and its image under π_p is an idempotent in $\mathbb{F}_p[x_1,\ldots,x_n]/\bar{I}_f$. Now we show that for every idempotent

$$\bar{e} \in \mathbb{F}_p[x_1,\ldots,x_n]/\bar{I}_f,$$

there's exactly one idempotent $e^{(\infty)} \in S_f^{(\infty)}$ such that $\pi_p(e^{(\infty)}) = \bar{e}$.

Let $n \in \mathbb{Z}$, $n \ge 0$. We show by induction on n that there's

$$e^{(n)} \in S_f^+ = \mathbb{Z}_p[x_1,\ldots,x_n]/I_f^{(\infty)+}$$

such that

$$\pi_p(e^{(n)}) = \bar{e} \tag{3.18}$$

and

$$\left(e^{(n)}\right)^2 \equiv e^{(n)} \pmod{p^{n+1}}. \tag{3.19}$$

By Lemma 3.54, π_p is surjective and we may define $e^{(0)}$ to be the inverse image of $\bar{e}$. Such a choice of $e^{(0)}$ satisfies both (3.18) and (3.19) by the definition of the map π_p and by the fact that $\bar{e} \in \mathbb{F}_p[x_1,\ldots,x_n]/\bar{I}_f$ is an idempotent.

Now let $n \ge 0$. By the induction hypothesis, we have

$$e^{(n)} \equiv \bar{e} \pmod{p}$$

and

$$\left(e^{(n)}\right)^2 \equiv e^{(n)} \pmod{p^{n+1}}.$$

The last congruence implies that

$$\Delta_n = ((e^{(n)})^2 - e^{(n)})/p^{n+1}$$

is an element of $\mathbb{Z}_p[x_1,\ldots,x_n]/I_f^{(\infty)+}$. If we define

$$\Gamma_{n+1} = (-2e^{(0)}+1)\Delta_n$$

and

$$e^{(n+1)} = e^{(n)} + p^{n+1}\Gamma_{n+1}, \tag{3.20}$$

then surely $\pi_p(e^{(n+1)}) = \bar{e}$. Furthermore,

$$(e^{(n+1)})^2 - e^{(n+1)} = (e^{(n)})^2 - e^{(n)} + p^{n+1}\Gamma_{n+1}(2e^{(n)} - 1) + p^{2n+2}\Gamma_{n+1}^2,$$

hence

$$\frac{(e^{(n+1)})^2 - e^{(n+1)}}{p^{n+1}} = \Delta_n + \Gamma_{n+1}(2e^{(n)} - 1) + p^{n+1}\Gamma_{n+1}^2.$$

Modulo p, the middle summand on the right-hand side is equal to

$$\Gamma_{n+1}(2e^{(n)}-1) = \Delta_n(-2e^{(0)}+1)(2e^{(n)}-1) \equiv \Delta_n(-2e^{(0)}+1)(2e^{(0)}-1) \equiv -\Delta_n \pmod{p}.$$

This implies that

$$\frac{(e^{(n+1)})^2 - e^{(n+1)}}{p^{n+1}} \equiv 0 \pmod{p}.$$

Hence

$$(e^{(n+1)})^2 \equiv e^{(n+1)} \pmod{p^{n+2}}.$$

Note that by (3.20), $e^{(n+1)} \equiv e^{(n)} \pmod{p^{n+1}}$ for every n. This means there's an element

$$e^{(\infty)} \in \mathbb{Z}_p[x_1, \ldots, x_n]/I_f^+, \ \forall n \geq 0 : e^{(\infty)} \equiv e^{(n)} \pmod{p^{n+1}}.$$

By (3.18) and (3.19), $e^{(\infty)}$ is an idempotent and $\pi_p(e^{(\infty)}) = \bar{e}$.

To show the uniqueness of $e^{(\infty)}$, suppose there's an idempotent $f^{(\infty)} \in \mathbb{Z}_p[x_1, \ldots, x_n]/I_f^+$ such that

$$\pi_p(f^{(\infty)}) = \bar{e}.$$

We show that $f^{(\infty)} \equiv e^{(n)} \pmod{p^{n+1}}$ for every $n \geq 0$. This is clear for $n = 0$. For $n > 0$, suppose

$$f^{(\infty)} \equiv e^{(n)} + ap^n \pmod{p^{n+1}},$$

where $a \in \mathbb{Z}_p[x_1, \ldots, x_n]/I_f^+$. The aim is to show $a \equiv 0 \pmod{p}$. As $f^{(\infty)}$ is an idempotent, we have

$$(e^{(n)} + ap^n)^2 \equiv e^n + ap^n \pmod{p^{n+1}}.$$

This is equivalent to

$$(e^{(n)})^2 - e^{(n)} \equiv ap^n(1 - 2e^{(n)}) \pmod{p^{n+1}},$$

which is in turn equivalent to

$$\frac{(e^{(n)})^2 - e^{(n)}}{p^n} \equiv a(1 - 2e^{(n)}) \pmod{p}.$$

By (3.19), the fraction on the left-hand side is a multiple of p, hence

$$a(1 - 2e^{(n)}) \equiv 0 \pmod{p}.$$

Finally, we observe that $(1 - 2e^{(n)})$ is invertible modulo p because $(1 - 2e^{(n)})^2 \equiv 1 \pmod{p}$. Therefore, a is congruent to 0 modulo p. □

Theorem 3.58 ([26], Theorem 16)**.** Let $f(x) \in \mathbb{Z}[x]$ be monic and separable, $\deg(f) = n$. Let p be a prime such that $p \nmid \operatorname{disc}(f)$. The homomorphism

$$\pi_p : S_f^+ \to \mathbb{F}_p[x_1, \ldots, x_n]/\bar{I}_f,$$

introduced in Lemma 3.54, gives a bijection between the set of primitive idempotents in $S_f^{(\infty)}$ and the set of primitive idempotents in

$$S_{\bar{f}} = \mathbb{F}_p[x_1, \ldots, x_n]/\bar{I}_f,$$

where $\bar{I}_f \subseteq \mathbb{F}_p[x_1, \ldots, x_n]$ is the universal splitting ideal of $\bar{f} = f \bmod p$ over $\mathbb{F}_p$.

Proof. First we show that for a primitive idempotent $\bar{e} \in S_{\bar{f}}$, its inverse image $e^{(\infty)}$ under π_p is a primitive idempotent in $S_f^{(\infty)}$. To this end, assume that $e^{(\infty)} = e_1^{(\infty)} + e_2^{(\infty)}$, where $e_1^{(\infty)}, e_2^{(\infty)} \neq 0$ are orthogonal idempotents. By Lemma 3.55, $\pi_p(e_i^{(\infty)})$, $i = 1, 2$, are (non-zero) orthogonal idempotents. That's a contradiction because $\bar{e}$ is primitive and at the same time equal to

$$\pi_p(e^{(\infty)}) = \pi_p(e_1^{(\infty)}) + \pi_p(e_2^{(\infty)}).$$

By a similar argument, it can be shown that the image of a primitive idempotent in $S_f^{(\infty)}$ is a primitive idempotent (in $S_{\bar{f}}$). □

Theorem 3.58 has the consequence that $\operatorname{Stab}(e^{(\infty)}) = \operatorname{Stab}(\bar{e})$ for each pair $(e^{(\infty)}, \bar{e})$ of corresponding primitive idempotents.

Corollary 3.59 ([26], Theorem 16)**.** Let $f(x) \in \mathbb{Z}[x]$ be monic and separable, $\deg(f) = n$. Let p be a prime such that $p \nmid \operatorname{disc}(f)$. For each pair $(e^{(\infty)}, \bar{e})$ such that $e^{(\infty)} \in S_f^{(\infty)}$ is a primitive idempotent and $\bar{e} = \pi_p(e^{(\infty)})$,

$$\operatorname{Stab}(e^{(\infty)}) = \operatorname{Stab}(\bar{e}),$$

where $\operatorname{Stab}(e^{(\infty)}) \subseteq \mathcal{S}_n$ is the stabilizer of $e^{(\infty)}$ under the action of $\mathcal{S}_n$ on $S_f^{(\infty)}$ and $\operatorname{Stab}(\bar{e}) \subseteq \mathcal{S}_n$ is the stabilizer of $\bar{e}$ under the action of $\mathcal{S}_n$ on $S_{\bar{f}}$ (see Lemma 3.40).

Proof. By Lemma 3.52, f is separable over $\mathbb{Q}_p$. By Lemma 3.40, $\mathcal{S}_n$ acts on the universal splitting ring $S_f^{(\infty)} = \mathbb{Q}_p[x_1, \ldots, x_n]/I_f^{(\infty)}$ of f over $\mathbb{Q}_p$. Let $(e^{(\infty)}, \bar{e})$ be a pair of primitive idempotents described above and let $\operatorname{Gal}(\bar{f})$ be the Galois group of $f \bmod p \in \mathbb{F}_p[x]$ with respect to some order of the roots of f in $\overline{\mathbb{F}}_p$. By Theorem 3.39, there are $[\mathcal{S}_n : \operatorname{Gal}(\bar{f})]$ primitive idempotents in $S_{\bar{f}}$. By Proposition 3.41, $\operatorname{Gal}(\bar{f}) = \tau \operatorname{Stab}(\bar{e}) \tau^{-1}$ for some $\tau \in \mathcal{S}_n$. Hence the number of primitive idempotents in $S_{\bar{f}}$ is equal to

$$[\mathcal{S}_n : \tau \operatorname{Stab}(\bar{e}) \tau^{-1}] = [\mathcal{S}_n : \operatorname{Stab}(\bar{e})].$$

Similarly, there are $[\mathcal{S}_n : \operatorname{Stab}(e^{(\infty)})]$ primitive idempotents in $S_f^{(\infty)}$. By Theorem 3.58,

$$[\mathcal{S}_n : \operatorname{Stab}(\bar{e})] = [\mathcal{S}_n : \operatorname{Stab}(e^{(\infty)})],$$

and $|\operatorname{Stab}(\bar{e})| = |\operatorname{Stab}(e^{(\infty)})|$. Now, to prove that $\operatorname{Stab}(\bar{e}) = \operatorname{Stab}(e^{(\infty)})$, it suffices to show that $\operatorname{Stab}(e^{(\infty)}) \subseteq \operatorname{Stab}(\bar{e})$. But this is clear since for every $\tau \in \operatorname{Stab}(e^{(\infty)})$,

$$\tau * \bar{e} = \tau * \pi_p(e^{(\infty)}) = \pi_p(\tau * e^{(\infty)}) = \pi_p(e^{(\infty)}) = \bar{e}$$

and $\tau \in \operatorname{Stab}(\bar{e})$. □

Chapter 4

A Modular Method

4.1 An outline of the method

As we've seen in section 2.4, a pivotal step of the Stauduhar's algorithm is deciding whether the resolvent polynomial $R^G_{(P,f)}$ has an integral root. In theory, this could be done simply by evaluating the expression $P(\alpha_1, \ldots, \alpha_n)$, where $\alpha_1, \ldots, \alpha_n$ are the roots of f. Unfortunately, the roots of f are usually known by their approximations, which makes it necessary to actually compute $R^G_{(P,f)}$ and then check for integral roots by, for example, factoring $R^G_{(P,f)}$ over $\mathbb{Z}[x]$. The following lemma provides an alternative approach.

Lemma 4.1 ([26], Remark 1)**.** Let $f \in \mathbb{Z}[x]$ be monic, separable, $\deg(f) = n$, and let $\alpha_1, \ldots, \alpha_n \in \overline{\mathbb{Q}}$ be the roots of f. Let $\mathcal{G}$ be a Gröbner basis of the ideal

$$M = \{g(x_1, \ldots, x_n) \in \mathbb{Q}[x_1, \ldots, x_n] \mid g(\alpha_1, \ldots, \alpha_n) = 0\}$$

with respect to some term order and let $P \in \mathbb{Z}[x_1, \ldots, x_n]$. Denote by $\mathrm{NF}_{\mathcal{G}}(P)$ the normal form of P with respect to $\mathcal{G}$. Then $P(\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}$ iff $P(\alpha_1, \ldots, \alpha_n) = \mathrm{NF}_{\mathcal{G}}(P)$ iff $\mathrm{NF}_{\mathcal{G}}(P)$ is a constant polynomial.

Proof. If $\mathrm{NF}_{\mathcal{G}}(P) \in \mathbb{Q}$ then $\mathrm{NF}_{\mathcal{G}}(P) = P(\alpha_1, \ldots, \alpha_n)$ because

$$P(x_1, \ldots, x_n) - \mathrm{NF}_{\mathcal{G}}(P) \in M.$$

Furhermore, since we assume $f \in \mathbb{Z}[x]$ to be monic, $P(\alpha_1, \ldots, \alpha_n)$ is an algebraic integer by Proposition 1.40. Hence

$$P(\alpha_1, \ldots, \alpha_n) \in \mathbb{Q} \iff P(\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}$$

by Corollary 1.42. □

So if we have a Gröbner basis $\mathcal{G}$ of the ideal M defined above, it's very easy to decide whether $R^G_{(P,f)}$ has an integral root simply by checking if $\mathrm{NF}_{\mathcal{G}}(P_i) \in \mathbb{Z}$ for some polynomial P_i conjugate to P.

Example 4.2. Let $f(x) = x^4 + x^3 + x^2 + x + 1$ be the polynomial from Example 2.40. Recall that the roots of f are

$$\alpha_1 = e^{2\pi i/5},\ \alpha_2 = e^{4\pi i/5},\ \alpha_3 = e^{6\pi i/5},\ \alpha_4 = e^{8\pi i/5}.$$

Let

$$M = \{g(x_1, x_2, x_3, x_4) \in \mathbb{Q}[x_1, x_2, x_3, x_4] \mid g(\alpha_1, \alpha_2, \alpha_3, \alpha_4) = 0\} \tag{4.1}$$

and

$$\begin{aligned} g_1(x_1) &= x_1^4 + x_1^3 + x_1^2 + x_1 + 1, \\ g_2(x_1, x_2) &= x_2 - x_1^2, \\ g_3(x_1, x_2, x_3) &= x_3 - x_1^3, \\ g_4(x_1, x_2, x_3, x_4) &= x_4 - x_1^4. \end{aligned}$$

Then $\mathcal{G} = \{g_1, g_2, g_3, g_4\}$ is a Gröbner basis of M with respect to the lexicographic order $<$ on terms such that $x_1 < x_2 < x_3 < x_4$. Now, let

$$P(x_1, x_2, x_3, x_4) = x_1x_3 + x_2x_4$$

be the $\mathcal{D}_8$-invariant polynomial from Lemma 2.37. Then

$$\begin{aligned} \mathrm{NF}_{\mathcal{G}}(P) &= -x_1^3 - x_1^2 - 1, \\ \mathrm{NF}_{\mathcal{G}}((12) * P) &= 2, \\ \mathrm{NF}_{\mathcal{G}}((14) * P) &= x_1^3 + x_1^2. \end{aligned}$$

Hence by Lemma 4.1, $((12) * P)(\alpha_1, \ldots, \alpha_n) = 2$ and $R^{\mathcal{S}_4}_{(P,f)}$ has a simple integral root. By Corollary 2.36, if we swap the values of α_1 and α_2 (i.e. reorder the roots of f according to (12)), $\mathrm{Gal}(f) \subseteq \mathcal{D}_8$. Now that the roots have been reordered, we have to find a new basis of M. Let

$$\begin{aligned} g_1(x_2) &:= x_2^4 + x_2^3 + x_2^2 + x_2 + 1, \\ g_2(x_2, x_1) &:= x_1 - x_2^2, \\ g_3(x_2, x_1, x_3) &:= x_3 - x_2^3, \\ g_4(x_2, x_1, x_3, x_4) &:= x_4 - x_2^4 \end{aligned}$$

and $\mathcal{G} := \{g_1, g_2, g_3, g_3\}$. Then $\mathcal{G}$ is a Gröbner basis of M with respect to the lexicographic order $<$ on terms such that $x_2 < x_1 < x_3 < x_4$. We're now ready to decide whether $\mathrm{Gal}(f) \subseteq \mathcal{C}_4$:
Let $P(x_1, x_2, x_3, x_4) := x_1x_2^2 + x_2x_3^2 + x_3x_4^2 + x_4x_1^2$ be the $\mathcal{D}_8$-relative $\mathcal{C}_4$-invariant from Lemma 2.38. Then

$$\begin{aligned} \mathrm{NF}_{\mathcal{G}}(P) &= -1, \\ \mathrm{NF}_{\mathcal{G}}((13) * P) &= 4. \end{aligned}$$

So, by Lemma 4.1, $P(\alpha_1, \alpha_2, \alpha_3, \alpha_4) = -1$, $P(\alpha_3, \alpha_2, \alpha_1, \alpha_4) = 4$, and the resolvent polynomial $R^{\mathcal{D}_8}_{(P,f)}$ does have an integral root. By Corollary 2.36,

$$\mathrm{Gal}(f) \subseteq \mathcal{C}_4.$$

Now, instead of actually computing a Gröbner basis of M, we reduce f modulo a prime p and then compute a Gröbner basis $\overline{\mathcal{G}}$ of the respective ideal over $\mathbb{F}_p$. It is possible to then lift $\overline{\mathcal{G}}$ over to its counterpart in $\mathbb{Q}_p[x_1, \ldots, x_n]$ (or, more precisely, to its approximation). Since the ideas presented above also work over

$\mathbb{Q}_p[x_1, \ldots, x_n]$, it's possible to compute the Galois group as suggested above - without resorting to computations with the roots of f.

In the rest of this chapter, we present three preparatory propositions. Then we'll discuss how to lift a Gröbner basis over $\mathbb{F}_p$ to a basis over $\mathbb{Z}/(p^k)$ for some $k \in \mathbb{N}$. This is done in Section 4.2. Finally, we present the algorithm itself.

Proposition 4.3 ([26], Proposition 17)**.** Let $f \in \mathbb{Z}[x]$ be monic and separable, $\deg(f) = n$. Let $p \in \mathbb{N}$ be a prime such that $p \nmid \operatorname{disc}(f)$. Let

$$e \in S_f = \mathbb{Q}[x_1, \ldots, x_n]/I_f$$

be a primitive idempotent and let

$$\pi_p : S_f^+ \to \mathbb{F}_p[x_1, \ldots, x_n]/\bar{I}_f$$

be the homomorphism from Lemma 3.54, where $\bar{I}_f$ is the universal splitting ideal of

$$\bar{f} := f \bmod p \in \mathbb{F}_p[x].$$

By Lemma 3.46, e is an idempotent in $S_f^{(\infty)}$. By Lemma 3.55, $e \in S_f^+$ and $\pi_p(e)$ is an idempotent in $S_{\bar{f}} = \mathbb{F}_p[x_1, \ldots, x_n]/\bar{I}_f$; we let $\bar{e}$ be its primitive component. Then $\mathrm{Stab}(\bar{e}) \subseteq \mathrm{Stab}(e)$. Moreover, if $\mathcal{T}$ is the set of left coset representatives of $\mathrm{Stab}(\bar{e})$ in $\mathrm{Stab}(e)$ then

$$\pi_p(e) = \sum_{\tau \in \mathcal{T}} \tau * \bar{e}.$$

By Corollary 3.58, $\bar{e}$ corresponds to a unique primitive idempotent $e^{(\infty)} \in S_f^{(\infty)}$. Then

$$e = \sum_{\tau \in \mathcal{T}} \tau * e^{(\infty)}. \tag{4.2}$$

Proof. We let $\mathcal{E}$ be the set of primitive idempotents in S_f and $\overline{\mathcal{E}}$ the set of primitive idempotents in $S_{\bar{f}}$ (the universal splitting ring of $\bar{f} = f \bmod p$ over $\mathbb{F}_p$). By Proposition 3.41, $\mathrm{Gal}(f) = \mathrm{Stab}(e)$. By Theorem 3.39,

$$m := |\mathcal{E}| = [\mathcal{S}_n : \mathrm{Gal}(f)] = [\mathcal{S}_n : \mathrm{Stab}(e)].$$

Similarly, $|\overline{\mathcal{E}}| = [\mathcal{S}_n : \mathrm{Stab}(\bar{e})]$. Next, we enumerate $\mathcal{E} = \{e_1, \ldots, e_m\}$ (wlog $e_1 = e$) and further denote by $\overline{\mathcal{E}_i} \subseteq \overline{\mathcal{E}}$ the primitive components of $\pi(e_i)$, $i = 1, \ldots, m$.

Using the fact that the elements of $\mathcal{E}$ are orthogonal to each other (by Lemma 1.3) and that, by Theorem 3.39, $\sum_{e \in \mathcal{E}} \pi_p(e) = 1$, one can prove that the sets $\overline{\mathcal{E}_i}$ are disjoint and $\overline{\mathcal{E}} = \cup_{i=1}^m \overline{\mathcal{E}_i}$.

Let us show that $|\overline{\mathcal{E}_i}| = |\overline{\mathcal{E}_1}|$ for every $i = 1, \ldots, m$. By Proposition 3.42, there's $\tau \in \mathcal{S}_n$ such that $e_i = \tau * e_1$. Thus

$$\sum_{\epsilon \in \overline{\mathcal{E}_i}} \epsilon = \pi_p(e_i) = \pi_p(\tau * e_1) = \tau * \pi_p(e_1) = \sum_{\epsilon \in \overline{\mathcal{E}_1}} \tau * \epsilon.$$

The decomposition of an idempotent into the sum of its primitive components is unique and $\epsilon \mapsto \tau * \epsilon$ is a bijection between $\overline{\mathcal{E}_1}$ and $\overline{\mathcal{E}_i}$. Hence

$$|\overline{\mathcal{E}_1}| = |\overline{\mathcal{E}}|/m = [\mathcal{S}_n : \mathrm{Stab}(\bar{e})]/[\mathcal{S}_n : \mathrm{Stab}(e)] = |\mathrm{Stab}(e)|/|\mathrm{Stab}(\bar{e})| \tag{4.3}$$

In this paragraph we show that $\mathrm{Stab}(e)$ acts on $\overline{\mathcal{E}_1}$. Let $\tau \in \mathrm{Stab}(e)$. By Lemma 3.43, $\bar{e} \cdot \pi_p(e) = \bar{e}$ because $\bar{e}$ is a component of $\pi_p(e)$. Hence

$$(\tau * \bar{e}) \cdot \pi_p(e) = (\tau * \bar{e}) \cdot \pi_p(\tau * e) = (\tau * \bar{e}) \cdot (\tau * \pi_p(e)) = \tau * (\bar{e} \cdot \pi_p(e)) = \tau * \bar{e}.$$

Again, by Lemma 3.43, $\tau * \bar{e}$ is a component of $\pi_p(e)$. This shows that $\mathrm{Stab}(e)$ acts on $\overline{\mathcal{E}_1}$ and consequently, $|\overline{\mathcal{E}_1}|$ is greater than or equal to the lenght of the orbit of $\bar{e}$, i.e.

$$|\overline{\mathcal{E}_1}| \geq [\mathrm{Stab}(e) : \mathrm{Stab}(e) \cap \mathrm{Stab}(\bar{e})] \geq |\mathrm{Stab}(e)|/|\mathrm{Stab}(\bar{e})| \overset{(4.3)}{=} |\overline{\mathcal{E}_1}|.$$

Hence,

$$[\mathrm{Stab}(e) : \mathrm{Stab}(e) \cap \mathrm{Stab}(\bar{e})] = |\mathrm{Stab}(e)|/|\mathrm{Stab}(\bar{e})|$$

and $\mathrm{Stab}(\bar{e}) \subseteq \mathrm{Stab}(e)$. This also shows that $\overline{\mathcal{E}_1}$ only consists of $\mathrm{Stab}(e)$ conjugates of $\bar{e}$ whence

$$\pi(e) = \sum_{\tau \in \mathcal{T}} \tau * \bar{e}. \tag{4.4}$$

Finally, we note that by Corollary 3.59,

$$\mathrm{Stab}(e^{(\infty)}) = \mathrm{Stab}(\bar{e}),$$

so $\mathcal{T}$ is also the set of left coset representatives of $\mathrm{Stab}(e^{(\infty)})$ in $\mathrm{Stab}(e)$. To show (4.2), it suffices to prove that $e^{(\infty)'}$ is a component of e iff $e^{(\infty)'}$ is $\mathrm{Stab}(e)$ conjugate to $e^{(\infty)}$. By Lemma 3.43, $e^{(\infty)'}$ is a component of e iff $e \cdot e^{(\infty)'} = e^{(\infty)'}$. So let $\tau \in \mathcal{T}$ and note that $\pi(e) \cdot (\tau * \bar{e}) = \tau * \bar{e}$ because $\tau * \bar{e}$ is a component of $\pi(e)$ by (4.4). Hence $e \cdot (\tau * e^{(\infty)}) = \tau * e^{(\infty)}$ because π gives a bijection between idempotents in $S_f^{(\infty)}$ and $S_{\bar{f}}$ by Theorem 3.57.

Conversely, let $e^{(\infty)'} \in S_f^{(\infty)}$ be a primitive idempotent such that $e \cdot e^{(\infty)'} = e^{(\infty)'}$. Then $\pi(e) \cdot \pi(e^{(\infty)'}) = \pi(e^{(\infty)'})$ and $\pi(e^{(\infty)'})$ is a component of $\pi(e)$. Again, by (4.4), $\pi(e^{(\infty)'})$ is $\mathrm{Stab}(e)$-conjugate to $\bar{e}$ and consequently, $e^{(\infty)'}$ is $\mathrm{Stab}(e)$-congugate to $\pi^{-1}(\bar{e}) = e^{(\infty)}$. □

Note 4.4. The following is stated as Lemma 12 in [26] without a proof.

Lemma 4.5. Let $f \in \mathbb{Z}[x]$ be monic and separable over $\mathbb{Q}$, $\deg(f) = n$. Let $\alpha_1, \ldots, \alpha_n \in \overline{\mathbb{Q}}$ be the roots of f and let $\mathrm{Gal}(f)$ and M be the Galois group and the splitting ideal of f with respect to this order of the roots, respectively. Let $S_f = \mathbb{Q}[x_1, \ldots, x_n]/I_f$ be the universal splitting ring of f over $\mathbb{Q}$ and let $e \in S_f$ be the primitive idempotent corresponding to M. If $g \in \mathbb{Q}[x_1, \ldots, x_n]$ is a polynomial such that $g(\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}$, then

$$[g(\alpha_1, \ldots, \alpha_n) - g]e = 0 \tag{4.5}$$

in S_f. Furthermore, suppose $H \subseteq G \subseteq \mathcal{S}_n$ are groups such that $\mathrm{Gal}(f) \subseteq G$ and $P \in \mathbb{Z}[x_1, \ldots, x_n]$ is a G-relative H-invariant. We let $R^G_{(P,f)} \in \mathbb{Z}[x_1, \ldots, x_n]$ be the G-relative H-invariant resolvent polynomial. Furthermore, we denote

$$R^G_P(y, x_1, \ldots, x_n) = \prod_{i=1}^{m} (y - P_i(x_1, \ldots, x_n)),$$

where $G * P = \{P_1 = P, \ldots, P_m\}$ is the orbit of P under the action of G on $\mathcal{S}_n$ (so $m = [G : H]$). Then

$$[R^G_{(P,f)}(y) - R^G_P(y, x_1, \ldots, x_n)] \cdot e = 0 \tag{4.6}$$

(in $S_f[y]$).

Proof. As $g(\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}$, $g - g(\alpha_1, \ldots, \alpha_n) \in M$ by the definition of the ideal M. Hence

$$(g - g(\alpha_1, \ldots, \alpha_n))e \in I_f$$

by (3.16). This shows (4.5). To prove (4.6), consider the polynomial

$$\sum_i c_i y^i := R^G_P(y, x_1, \ldots, x_n) - R^G_{(P,f)}(y) \in (\mathbb{Z}[x_1, \ldots, x_n])[y].$$

For $i \in \{0, \ldots, k\}$, the coefficient $c_i \in \mathbb{Z}[x_1, \ldots, x_n]$ of y^{n-i} is equal to

$$(-1)^i(s_i(P_1(x_1, \ldots, x_n), \ldots, P_k(x_1, \ldots, x_n)) - s_i(P_1(\alpha_1, \ldots, \alpha_n), \ldots, P_k(\alpha_1, \ldots, \alpha_n)))$$

which is clearly a polynomial from M. Hence, by Theorem 3.39, $c_i \cdot e \in I_f$, which implies (4.6). □

Lemma 4.6. Under the assumptions of Lemma 4.5, let $p \in \mathbb{N}$ be a prime such that $p \nmid \operatorname{disc}(f)$. Let

$$S_f^{(\infty)} = \mathbb{Q}_p[x_1, \ldots, x_n]/I_f^{(\infty)}$$

be the universal splitting ring of f over $\mathbb{Q}_p$ and $e^{(\infty)} \in S_f^{(\infty)}$ a primitive component of e. If $g \in \mathbb{Z}[x_1, \ldots, x_n]$ is a polynomial such that $g(\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}$, then

$$[g - g(\alpha_1, \ldots, \alpha_n)] \cdot e^{(\infty)} = 0$$

in $S_f^{(\infty)}$. Let π_p be the homomorphism from Lemma 3.54. Then

$$[\pi_p(g) - \pi_p(g(\alpha_1, \ldots, \alpha_n))] \cdot \bar{e} = 0 \tag{4.7}$$

for every primitive component $\bar{e}$ of $\pi_p(e)$ in $S_{\bar{f}}$.

Proof. By Lemma 3.43, $e^{(\infty)} = e \cdot e^{(\infty)}$ because $e^{(\infty)}$ is a component of e. Hence

$$[g - g(\alpha_1, \ldots, \alpha_n)] \cdot e^{(\infty)} = ([g(\alpha_1, \ldots, \alpha_n) - g] \cdot e) \cdot e^{(\infty)} = 0$$

by Lemma 4.5. By Theorem 3.58, there's a unique primitive idempotent $e^{(\infty)'} \in S_f^{(\infty)}$ such that $\pi_p(e^{(\infty)'}) = \bar{e}$. Then

$$\pi_p(\underbrace{[g - g(\alpha_1, \ldots, \alpha_n)] \cdot e^{(\infty)'}}_{=0}) = [\pi_p(g) - \pi_p(g(\alpha_1, \ldots, \alpha_n))] \cdot \bar{e} = 0$$

□

4.2 Lifting a basis

Let K be a perfect field, $f \in K[x]$, monic and irreducible, $\deg(f) = n$. Let $\alpha_1, \ldots, \alpha_n \in \overline{K}$ be the roots of f and let

$$M = \{g(x_1, \ldots, x_n) \in K[x_1, \ldots, x_n] \mid g(\alpha_1, \ldots, \alpha_n) = 0\} \tag{4.8}$$

be the universal splitting ideal of f with respect to the above order of the roots. We outline how to find a Gröbner basis of M. More details can be found in [1].

- Let $f_1(x_1) := f(x_1)$ and $K_1 := K[x_1]/(f_1(x_1))$.
- Let $f_2(x_1, x_2) \in K[x_1, x_2]$ be a polynomial such that $f_2([x_1], x)$ is a non-linear, irreducible factor of $f(x)$ over K_1. Set $K_2 := K_1[x_2]/(f_2([x_1], x_2))$.
  $\vdots$
- Similarly, let $f_m([x_1], \ldots, [x_{m-1}], x)$ be a non-linear, irreducible factor of $f(x)$ over K_{m-1}. Set $K_m := K_{m-1}[x_m]/(f_m([x_1], \ldots, [x_{m-1}], x_m))$. Suppose that $f(x)$ factors into linear factors over $K_m \cong K(\alpha_1, \ldots, \alpha_m)$. Then polynomials
  $$h_{m+1}(x_1, \ldots, x_m), \ldots, h_n(x_1, \ldots, x_m)$$
  exist such that
  $$\alpha_{m+1} = h_{m+1}(\alpha_1, \ldots, \alpha_m), \ldots, \alpha_n = h_n(\alpha_1, \ldots, \alpha_m).$$
- Set
  $$\begin{aligned} f_{m+1}(x_1, \ldots, x_m, x_{m+1}) &:= x_{m+1} - h_{m+1}(x_1, \ldots, x_m), \\ &\vdots \\ f_n(x_1, \ldots, x_n) &:= x_n - h_n(x_1, \ldots, x_m). \end{aligned}$$

Then $f_1, \ldots, f_n$ is a Gröbner basis of M with respect to the lexicographic order $<$ on terms such that $x_1 < \cdots < x_n$.

Example 4.7. Let $f(x) = x^4 + x^3 + x^2 + x + 1$ be the polynomial from example 4.2. Let $f_1(x_1) = f(x_1)$ and $K_1 = \mathbb{Q}[x_1]/(f_1(x_1))$. Then f factors as

$$f(x) = (x - [x_1])(x - [x_1^2])(x - [x_1^3])(x - [x_1^4])$$

over K_1. Let

$$\begin{aligned} h_2(x_1) &= x_1^2, \\ h_3(x_1) &= x_1^3, \\ h_4(x_1) &= x_1^4. \end{aligned}$$

Then

$$f(x) = (x - [x_1])(x - [h_2(x_1)])(x - [h_3(x_1)])(x - [h_4(x_1)]).$$

By the above paragraph,

$$\begin{aligned} f_1(x_1) &= x_1^4 + x_1^3 + x_1^2 + x_1 + 1, \\ f_2(x_1, x_2) &= x_2 - x_1^2, \\ f_3(x_1, x_2, x_3) &= x_3 - x_1^3, \\ f_4(x_1, x_2, x_3, x_4) &= x_4 - x_1^4 \end{aligned}$$

is a Gröbner basis of the ideal (4.1) with respect to the lexicographic order $<$ on terms such that $x_1 < x_2 < x_3 < x_4$.

Lemma 4.8 (Hensel's Lemma)**.** Let $f(x) \in \mathbb{Z}[x]$ be primitive, $p \in \mathbb{N}$ a prime,

$$\operatorname{lc}(f) \bmod p \neq 0.$$

Let $g_1, \ldots, g_m \in (\mathbb{Z}/(p))[x]$ be pairwise coprime polynomials such that

$$f \equiv g_1 \cdots g_m \pmod{p}$$

and $\operatorname{lc}(g_1) = \operatorname{lc}(f) \bmod p$, $\operatorname{lc}(g_2) = \cdots = \operatorname{lc}(g_m) = 1$. Then, for every $k \in \mathbb{N}$, there exist polynomials $g_1^{(k)}, \ldots, g_m^{(k)} \in (\mathbb{Z}/(p^k))[x]$ such that

$$f \equiv g_1^{(k)} \cdots g_m^{(k)} \pmod{p^k}, \tag{4.9}$$

$\operatorname{lc}(g_1^{(k)}) = \operatorname{lc}(f) \bmod p^k$, $\operatorname{lc}(g_2^{(k)}) = \cdots = \operatorname{lc}(g_m^{(k)}) = 1$ and

$$g_i^{(k)} \equiv g_i \pmod{p} \tag{4.10}$$

for every i.

Proof. See [4, Věta 17.3] □

By [4, Algoritmus 28], this is how to compute the polynomials $g_1^{(k)}, \ldots, g_m^{(k)}$:

Algorithm 8 Hensel lifting

Input: $f, g_1, \ldots, g_m$ from Lemma 4.8, $k \in \mathbb{N}$, $p \in \mathbb{N}$ a prime

Output: $g_1^{(k)}, \ldots g_m^{(k)}$ satisfying (4.9) and (4.10)

1: **for** $i = 1, \ldots, m$ **do**

2: $\quad \tilde{g}_i := \prod_{j \neq i} g_j \bmod p$

3: **end for**

4: **for** $i = 1, \ldots, k-1$ **do**

5: $\quad \mathrm{lc}(g_1) := \mathrm{lc}(f) \bmod p^{i+1}$

6: $\quad d := (f - g_1 \cdots g_m)/p^i \bmod p$

7: $\quad$ Find $u_1, \ldots, u_m \in (\mathbb{Z}/(p))[x]$ such that $d \equiv \sum_j u_j \tilde{g}_j \bmod p$ and $\deg(u_j) < \deg(g_j)$

8: $\quad g_j := (g_i + p^i u_j) \bmod p^{i+1}$, $j = 1, \ldots, m$

9: **end for**

10: **return** $g_1, \ldots, g_m$

For details on Step 7 of the above algorithm, see [4, Algoritmus 27].

Theorem 4.9 ([26], Theorem 21)**.** Let $f(x) \in \mathbb{Z}[x]$ be monic and separable. Let $p \in \mathbb{N}$ be a prime such that $p \nmid \mathrm{disc}(f)$, let

$$\bar{f} := f \bmod p \in \mathbb{F}_p[x],$$

and let $\bar{I}_f$ be the universal splitting ideal of $\bar{f}$ over $\mathbb{F}_p$. Let $\overline{M}$ be the splitting ideal of $\bar{f}$ with respect to some order of the roots of $\bar{f}$ in $\overline{\mathbb{F}}_p$ and let

$$\bar{f}_1, \ldots, \bar{f}_n$$

be a Gröbner basis of $\overline{M}$ with respect to the lexicographic order $<$ on terms such that $x_1 < \cdots < x_n$. By Theorem 3.39, there's a unique primitive idempotent

$$\bar{e} \in \mathbb{F}_p[x_1, \ldots, x_n]/\bar{I}_f$$

corresponding to $\overline{M}$. By Theorem 3.58, there's a unique primitive idempotent

$$e^{(\infty)} \in S_f^{(\infty)} = \mathbb{Q}_p[x_1, \ldots, x_n]/I_f^{(\infty)}$$

such that $\pi_p(e^{(\infty)}) = \bar{e}$, where

$$\pi_p : S_f^+ \to \mathbb{F}_p[x_1, \ldots, x_n]/\bar{I}_f$$

is the homomorphism from Lemma 3.54. Then $\bar{f}_1, \ldots, \bar{f}_n$ can be lifted to a basis

$$f_1^{(\infty)}, \ldots, f_n^{(\infty)}$$

of a maximal ideal $M^{(\infty)} \subseteq \mathbb{Q}_p[x_1, \ldots, x_n]$ such that $e^{(\infty)}$ is the primitive idempotent corresponding to $M^{(\infty)}$.

Proof. For a formal proof, see [26, Theorem 21]. We outline how to compute $f_i^{(\infty)} \bmod p^k$ for every $k \geq 1$, $i = 1, \ldots, n$. First, let $i = 1$. As $\bar{f}_1$ is a factor of $\bar{f}$, there's $\bar{h}_1(x) \in \mathbb{F}_p[x]$ be such that

$$\bar{f}(x) = \bar{f}_1(x) \cdot \bar{h}_1(x).$$

Since $\bar{f}$ is separable, $\bar{f}_1, \bar{h}_1$ are coprime and, by Lemma 4.8, there are polynomials $f_1^{(k)}, h_1^{(k)}$ such that $f \equiv f_1^{(k)} \cdot h_1^{(k)} \pmod{p^k}$ for every k. Moreover, Algorithm 8 can be used to compute these polynomials.

Let $i > 1$ and set

$$K_{i-1} := \mathbb{F}_p[x_1, \ldots, x_{i-1}]/(\bar{f}_1, \ldots, \bar{f}_{i-1}).$$

Again, there's a polynomial $\bar{h}_i \in K_{i-1}[x]$ such that

$$f(x_i) = \bar{f}_i(x_i) \cdot \bar{h}_i(x_i)$$

over K_{i-1}. Set

$$f_i^{(1)} := \bar{f}_i \text{ and } h_i^{(1)} = \bar{h}_i. \tag{4.11}$$

In (4.11), we consider $f_i^{(1)}, h_i^{(1)}$ to be polynomials from $\mathbb{Z}([x_1, \ldots, x_{i-1}])[x_i]$. For $k > 1$, Algorithm 9 computes $f_i^{(k)}, h_i^{(k)} \in \mathbb{Z}[x_1, \ldots, x_i]$ such that

$$f(x_i) \equiv f_i^{(k)}(x_1, \ldots, x_i) \cdot h_i^{(k)}(x_1, \ldots, x_i) \pmod{p^k, \langle \mathcal{G}_{i-1}^{(k+1)} \rangle}, \tag{4.12}$$

where

$$\mathcal{G}_{i-1}^{(k+1)} := \{f_1^{(k+1)}, \ldots, f_{i-1}^{(k+1)}\}.$$

□

Algorithm 9 Basis Lifting

Input: With the above notation, let $f_i^{(1)}, h_i^{(1)}$ satisfy (4.11), let $k > 1$.

Output: $f_i^{(k)}, h_i^{(k)}$ satisfying (4.12)

1: $\tilde{f}_i := h_i^{(1)}$, $\tilde{h}_i := f_i^{(1)}$
2: Find $u_0, v_0 \in K_{i-1}[x_i]$ such that $1 = u_0\tilde{f}_i + v_0\tilde{h}_i$
3: **for** $j = 1, \ldots, k-1$ **do**
4: $\quad \mathcal{G}_{i-1}^{(j+1)} := \{f_1^{(j+1)}, \ldots, f_{i-1}^{(j+1)}\}$
5: $\quad d(x_1, \ldots, x_i) := \mathrm{NF}_{\mathcal{G}_{i-1}^{(j+1)}}(f(x_i) - f_i^{(j)}(x_1, \ldots, x_i) \cdot g_i^{(j)}(x_1, \ldots, x_i))/p^j$
6: $\quad d := d \bmod p \in K_{i-1}[x_i]$
7: $\quad u := u_0 \bmod \tilde{h}_i$
8: $\quad v := v_0 d + \tilde{f}_i(u_0 \operatorname{div} \tilde{h}_i)$
9: $\quad f_i^{(j+1)} := f_i^{(j)} + p^j u \bmod p^{j+1}$
10: $\quad h_i^{(j+1)} := h_i^{(j)} + p^j v \bmod p^{j+1}$
11: **end for**
12: **return** $f_i^{(k)}$, $h_i^{(k)}$

Example 4.10. Let

$$f(x) = x^4 + x + 1 \in \mathbb{F}_5[x].$$

Then f factors as

$$f(x) = (x+2)(x^3 + 3x^2 + 4x + 3)$$

in $\mathbb{F}_5[x]$. Let

$$\begin{aligned} \bar{f}_1(x_1) &= x_1 + 2, \\ \bar{f}_2(x_2) &= x_2^3 + 3x_2^2 + 4x_2 + 3. \end{aligned}$$

The polynomial f factors as

$$f(x) = (x+2)(x + [4x_2])(x + [4x_2^2 + 3])(x + [x_2^2 + x_2])$$

over $\mathbb{F}_5[x_2]/(\bar{f}_2(x_2))$. Let $h_3(x_2) = 4x_2^2 + 3$, $h_4(x_2) = x_2^2 + x_2$ and

$$\begin{aligned} \bar{f}_3(x_2, x_3) &= x_3 + 4x_2^2 + 3 = x_3 + h_3(x_2), \\ \bar{f}_4(x_2, x_4) &= x_4 + x_2^2 + x_2 = x_4 + h_4(x_2). \end{aligned}$$

Then $\bar{f}_1, \bar{f}_2, \bar{f}_3, \bar{f}_4$ is a Gröbner basis of the splitting ideal $\overline{M}$ of f (with respect to some order of the roots of f in $\overline{\mathbb{F}}_p$). If we run Algorithm 8 on $\bar{f}_1, \bar{f}_2$ for

$k = 1, 2, 3, 4, 5, 6$, the results are as follows:

$$\begin{aligned}
f_1^{(1)}(x_1) &= x_1 + 2, & f_2^{(1)}(x_2) &= x_2^3 + 3x_2^2 + 4x_2 + 3,\\
f_1^{(2)}(x_1) &= x_1 + 12, & f_2^{(2)}(x_2) &= x_2^3 + 13x_2^2 + 19x_2 + 23,\\
f_1^{(3)}(x_1) &= x_1 + 37, & f_2^{(3)}(x_2) &= x_2^3 + 88x_2^2 + 119x_2 + 98,\\
f_1^{(4)}(x_1) &= x_1 + 287, & f_2^{(4)}(x_2) &= x_2^3 + 338x_2^2 + 494x_2 + 98,\\
f_1^{(5)}(x_1) &= x_1 + 1537, & f_2^{(5)}(x_2) &= x_2^3 + 1588x_2^2 + 2994x_2 + 1348,\\
f_1^{(6)}(x_1) &= x_1 + 7787, & f_2^{(6)}(x_2) &= x_2^3 + 7838x_2^2 + 12369x_2 + 10723.
\end{aligned}$$

Note that

$$f_1^{(k)}(x) \cdot f_2^{(k)}(x) \equiv x^4 + x + 1 \pmod{p^k}$$

for $k = 1, 2, 3, 4, 5, 6$.

Let $i = 3$ and

$$\bar{h}_3(x_2, x_3) := x_3^3 + (x_2^2 + 2)x_3^2 + (4x_2^2 + 4x_2 + 3)x_3 + 4x_2^2 + 3x_2 + 1.$$

Then

$$f(x) = \bar{f}_3([x_2], x_3) \cdot \bar{h}_3([x_2], x_3)$$

over $K_2 = \mathbb{F}_5[x_2]/(\bar{f}_2(x_2))$. If we run Algorithm 9 on $f_3^{(1)} := \bar{f}_3$, $h_3^{(1)} := \bar{h}_3$ for $k = 1, 2, 3, 4, 5$, the results are as follows:

$$\begin{aligned}
f_3^{(1)}(x_2, x_3) &= x_3 + 4x_2^2 + 3,\\
f_3^{(2)}(x_2, x_3) &= x_3 + 9x_2^2 + 15x_2 + 18,\\
f_3^{(3)}(x_2, x_3) &= x_3 + 34x_2^2 + 115x_2 + 43,\\
f_3^{(4)}(x_2, x_3) &= x_3 + 159x_2^2 + 115x_2 + 293,\\
f_3^{(5)}(x_2, x_3) &= x_3 + 1409x_2^2 + 2615x_2 + 293,
\end{aligned}$$

$$\begin{aligned}
h_3^{(1)}(x_2, x_3) &= x_3^3 + (x_2^2 + 2)x_3^2 + (4x_2^2 + 4x_2 + 3)x_3 + 4x_2^2 + 3x_2 + 1,\\
h_3^{(2)}(x_2, x_3) &= x_3^3 + (16x_2^2 + 10x_2 + 7)x_3^2 + (14x_2^2 + 4x_2 + 8)x_3 + 14x_2^2 + 8x_2 + 16,\\
h_3^{(3)}(x_2, x_3) &= x_3^3 + (91x_2^2 + 10x_2 + 82)x_3^2 + (114x_2^2 + 29x_2 + 83)x_3 + 14x_2^2 + 8x_2 + 91,\\
h_3^{(4)}(x_2, x_3) &= x_3^3 + (466x_2^2 + 510x_2 + 332)x_3^2 + (114x_2^2 + 279x_2 + 458)x_3 +\\
&\quad + 14x_2^2 + 8x_2 + 466,\\
h_3^{(5)}(x_2, x_3) &= x_3^3 + (1716x_2^2 + 510x_2 + 2832)x_3^2 + (2614x_2^2 + 1529x_2 + 458)x_3 +\\
&\quad + 1889x_2^2 + 1258x_2 + 1716.
\end{aligned}$$

Note that

$$f(x_i) \equiv f_3^{(k)}(x_2, x_3) \cdot h_3^{(k)}(x_2, x_3) \pmod{p^k, \langle \mathcal{G}_2^{(k+1)} \rangle},$$

for every k, where $\mathcal{G}_2^{(k+1)} = \{f_1^{(k+1)}, f_2^{(k+1)}\}$.

Finally, let $i = 4$. Then

$$\bar{h}_4(x_2, x_4) := x_4^3 + (4x_2^2 + 4x_2)x_4^2 + (x_2 + 3)x_4 + 4x_2^2 + x_2 + 4$$

is the cofactor of $\bar{f}_4$ and for $f_4^{(1)} = \bar{f}_4$, $h_4^{(1)} = \bar{h}_4$, the following are the results obtained by Algorithm 9:

$$\begin{aligned}
f_4^{(1)}(x_2, x_4) &= x_4 + x_2^2 + x_2, \\
f_4^{(2)}(x_2, x_4) &= x_4 + 16x_2^2 + 11x_2 + 20, \\
f_4^{(3)}(x_2, x_4) &= x_4 + 91x_2^2 + 11x_2 + 45, \\
f_4^{(4)}(x_2, x_4) &= x_4 + 466x_2^2 + 511x_2 + 45, \\
f_4^{(5)}(x_2, x_4) &= x_4 + 1716x_2^2 + 511x_2 + 1295,
\end{aligned}$$

$$\begin{aligned}
h_4^{(1)}(x_2, x_4) &= x_4^3 + (4x_2^2 + 4x_2)x_4^2 + (x_2 + 3)x_4 + 4x_2^2 + x_2 + 4, \\
h_4^{(2)}(x_2, x_4) &= x_3^3 + (9x_2^2 + 14x_2 + 5)x_3^2 + (10x_2^2 + 21x_2 + 23)x_3 + 24x_2^2 + 11x_2 + 9, \\
h_4^{(3)}(x_2, x_4) &= x_4^3 + (34x_2^2 + 114x_2 + 80)x_4^2 + (10x_2^2 + 96x_2 + 48)x_4 + 74x_2^2 + 111x_2 + 34, \\
h_4^{(4)}(x_2, x_4) &= x_4^3 + (159x_2^2 + 114x_2 + 580)x_4^2 + (510x_2^2 + 346x_2 + 298)x_4 + \\
&\quad + 324x_2^2 + 486x_2 + 159, \\
h_4^{(5)}(x_2, x_4) &= x_4^3 + (1409x_2^2 + 2614x_2 + 1830)x_4^2 + (510x_2^2 + 1596x_2 + 2798)x_4 + \\
&\quad + 2824x_2^2 + 1736x_2 + 1409
\end{aligned}$$

4.3 The p-adic decision step

Let $f(x) \in \mathbb{Z}[x]$ be a monic, irreducible polynomial of degree n. Let $p \in \mathbb{N}$ be a prime such that $p \nmid \operatorname{disc}(f)$ and

$$\bar{f} := f \bmod p \in \mathbb{F}_p.$$

Let $\overline{M}$ be the splitting ideal of $\bar{f}$ with respect to some order of the roots of f in $\overline{\mathbb{F}}_p$ and let

$$\mathcal{G} = \{\bar{f}_1, \ldots, \bar{f}_n\}$$

be a Gröbner basis of $\overline{M}$ with respect to the lexicographic order $<$ on terms such that $x_1 < \ldots < x_n$.

Let $S_{\bar{f}}$ be the universal splitting ring of $\bar{f}$ over $\mathbb{F}_p$ and let $\bar{e} \in S_{\bar{f}}$ be the primitive idempotent corresponding to the ideal $\overline{M}$. Let S_f be the universal splitting ring of f over $\mathbb{Q}$. Let π_p be the homomorphism from Lemma 3.54. It's clear from the proof of Proposition 4.3 that there's a primitive idempotent $e \in S_f$ such that $\bar{e}$ is a component of $\pi_p(e)$. Let $\alpha_1, \ldots, \alpha_n \in \overline{\mathbb{Q}}$ be the roots of f. Suppose the order of the roots corresponds to the primitive idempotent e (that is, $\operatorname{Stab}(e) = \operatorname{Gal}(f)$ with respect to this order of the roots).

Given groups $H \subseteq G \subseteq \mathcal{S}_n$, where G is transitive such that $\operatorname{Gal}(f) \subseteq G$, Algorithm 9 can be used to decide whether $\operatorname{Gal}(f) \subseteq \tau H \tau^{-1}$ for some $\tau \in \mathcal{S}_n$. Before we give the algorithm, note that for $P \in \mathbb{Z}[x_1, \ldots, x_n]$, $\pi_p(P) \equiv P \pmod p$ can be considered a polynomial from $\mathbb{F}_p[x_1, \ldots, x_n]$ and $\operatorname{NF}_{\mathcal{G}}(\, \pi_p(P)\,) \in \mathbb{F}_p[x_1, \ldots, x_n]$ denotes the normal form of $\pi_p(P)$ with respect to $\mathcal{G}$.

Remark 4.11. We shall represent elements of $\mathbb{Z}/(p^k)$ as integers from

$$\{-(p^k-1)/2, \ldots, (p^k-1)/2\}$$

if $2 < p$ and

$$\{-2^{k-1}, \ldots, 2^{k-1}-1\}$$

if $p = 2$. This will be an important thing to note at Step 22 of Algorithm 9.

Lemma 4.12 is technical.

Lemma 4.12 ([26], Lemma 24)**.** With the above notation, let

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$$

and

$$\|f\| := \sqrt{\sum_i a_i^2}.$$

For $P \in \mathbb{Z}[x_1, \ldots, x_n]$, let $T(P)$ be the set of terms of P. For $t \in T(P)$, we denote by $c_t \in \mathbb{Z}$ the coefficient of t, i.e.

$$P = \sum_{t \in T(P)} c_t t.$$

Moreover, for $t \in T(P)$, let $d(t) := \max\{\deg_{x_1}(t), \ldots, \deg_{x_n}(t)\}$. Then

$$|(\tau * P)(\alpha_1, \ldots, \alpha_n)| < \sum_{t \in T(P)} |c_t| \cdot \|f\|^{d(t)}$$

for every $\tau \in \mathcal{S}_n$. In particular,

$$B := \max\left\{ \sum_{t \in T(P)} |c_t| \cdot \|f\|^{d(t)}, [G : H] + 1 \right\}$$

satisfies the conditions from Step 4 of Algorithm 10.

Algorithm 10 The p-adic decision step

Input: With the above notation, let $H \subseteq G \subseteq \mathcal{S}_n$, where G is transitive such that $\mathrm{Gal}(f) \subseteq G$, $[G : H] = m$.

Output: $\tau \in \mathcal{S}_n$ such that $\mathrm{Gal}(f) \subseteq \tau H \tau^{-1}$; 0 if no such τ exists

1: $k := 1$, $\mathcal{G}^{(1)} := \{f_1^{(1)}, \ldots, f_n^{(1)}\}$, where $f_i^{(1)} = \bar{f}_i$, $i = 1, \ldots, n$

2: Compute a list $(\sigma_1, \ldots, \sigma_m)$ of left coset representatives of H in G.

3: Compute an H-relative G-invariant $P \in \mathbb{Z}[x_1, \ldots, x_n]$

4: Compute a bound $B \in \mathbb{N}$ such that $[G : H] < B$ and $|(\sigma_i * P)(\alpha_1, \ldots, \alpha_n)| < B$ for every $i = 1, \ldots, m$

5: $\mathcal{T} := \emptyset$

6: **for** $i = 1, \ldots, m$ **do**
7: **if** $\mathrm{NF}_{\mathcal{G}^{(1)}}(\ \pi(\sigma_i * P)\ ) \in \mathbb{F}_p$ **then**
8: $\mathcal{T} := \mathcal{T} \cup \{\sigma_i\}$
9: **end if**
10: **end for**

11: **if** $\mathcal{T} = \emptyset$ **then**
12: **return** 0
13: **end if**

14: **if** $p^k \leq (2B)^{[G:H]}$ **then**
15: Find k' such that $p^{k'} > (2B)^{[G:H]}$
16: Lift $f_1^{(k)}, \ldots, f_n^{(k)}$ to $f_1^{(k')}, \ldots, f_n^{(k')}$
17: $k := k'$
18: $\mathcal{G}^{(k)} := \{f_1^{(k)}, \ldots, f_n^{(k)}\}$
19: **end if**

20: $\Lambda := \emptyset$

21: **for** $i = 1, \ldots, m$ **do**

22: $A_i := \mathrm{NF}_{\mathcal{G}^{(k)}}(\ \sigma_i * P\ )$

23: **if** $A_i \in \mathbb{Z}$ and $|A_i| < B$ **then**
24: $\Lambda := \Lambda \cup \{i\}$
25: **end if**

26: **end for**

27: **if** $\Lambda = \emptyset$ **then**
28: **return** 0
29: **end if**

30: **if** $\exists i \in \Lambda : (\forall j \in \Lambda \setminus \{i\} : A_i \neq A_j)$ **then**
31: **return** σ_i
32: **else**
33: Go to Line 3
34: **end if**

First, let's show that the decision step from Line 10 of Algorithm 9 is correct.

Lemma 4.13. With the above notation, let $\tau \in \mathcal{S}_n$ be such that $\mathrm{Gal}(f) \subseteq \tau H \tau^{-1}$. Then

$$\mathrm{NF}_{\mathcal{G}^{(1)}}(\ \pi_p(\tau * P)\ ) \in \mathbb{F}_p. \tag{4.13}$$

Proof. If $\mathrm{Gal}(f) \subseteq \tau H \tau^{-1}$, then $A := (\tau * P)(\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}$ by Corollary 2.34. Hence

$$[\pi_p(\tau * P) - \pi_p(A)] \cdot \bar{e} = 0$$

in $S_{\bar{f}}$ by Lemma 4.6. By (3.16) (from Theorem 3.39), $\pi_p(\tau * P) - \pi_p(A) \in \overline{M}$. Hence

$$\mathrm{NF}_{\mathcal{G}^{(1)}}(\ \pi_p(\tau * P)\ ) = \pi_p(A),$$

which implies (4.13). □

Example 4.14. Let

$$f(x) = x^4 + x + 1.$$

Then $\mathrm{disc}(f) = 229 \in \mathbb{Z} \setminus \mathbb{Z}^2$. By Proposition 1.46, $\mathrm{Gal}(f) \nsubseteq \mathcal{A}_4$. We show that $\mathrm{Gal}(f) = \mathcal{S}_4$. It suffices to prove $\mathrm{Gal}(f) \nsubseteq \mathcal{D}_8$. Let $G := \mathcal{S}_4$, $H := \mathcal{D}_8$, and let

$$P(x_1, x_2, x_3, x_4) = x_1x_3 + x_2x_4$$

be the H-invariant polynomial from Lemma 2.37. Then

$$\{(), (12), (14)\}$$

are the left coset representatives of H in G and $\mathcal{G} = \{\bar{f}_1, \bar{f}_2, \bar{f}_3, \bar{f}_4\}$ is a Gröbner basis of the splitting ideal $\overline{M} \subseteq \mathbb{F}_5[x_1, x_2, x_3, x_4]$ of f, where

$$\begin{aligned}
\bar{f}_1(x_1) &= x_1 + 2, \\
\bar{f}_2(x_2) &= x_2^3 + 3x_2^2 + 4x_2 + 3, \\
\bar{f}_3(x_2, x_3) &= x_3 + 4x_2^2 + 3, \\
\bar{f}_4(x_2, x_4) &= x_4 + x_2^2 + x_2.
\end{aligned}$$

Then

$$\begin{aligned}
\mathrm{NF}_{\mathcal{G}}(P(x_1, x_2, x_3, x_4)) &= 4 + 4x_2, \\
\mathrm{NF}_{\mathcal{G}}((12) * P(x_1, x_2, x_3, x_4)) &= 2 + 4x_2^2, \\
\mathrm{NF}_{\mathcal{G}}((14) * P(x_1, x_2, x_3, x_4)) &= 4 + x_2 + x_2^2.
\end{aligned}$$

None of the above is a constant polynomial and $\mathrm{Gal}(f) \nsubseteq \mathcal{D}_8$ by Lemma 4.13. Hence $\mathrm{Gal}(f) = \mathcal{S}_4$.

Now we show that the decision step from Line 26 is correct.

Lemma 4.15. With the above notatin, let $\tau \in \mathcal{S}_n$ be such that $\mathrm{Gal}(f) \subseteq \tau H \tau^{-1}$ and let $k \in \mathbb{N}$. Then

$$A := \mathrm{NF}_{\mathcal{G}^{(k)}}(\ \tau * P\ )$$

is an integer such that $|A| < B$.

Proof. By Theorem 3.58, there's a unique primitive idempotent $e^{(\infty)} \in S_f^{(\infty)}$ such that $\pi_p(e^{(\infty)}) = \bar{e}$. Since $\bar{e}$ is a component of $\pi_p(e)$, $e^{(\infty)}$ is a component of e by Proposition 4.3. By Corollary 2.34, $A := (\tau * P)(\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}$ and $|A| < B$ by the definition of B. By Theorem 4.9, $\mathcal{G}$ can be lifted to $f_1^{(\infty)}, \ldots, f_n^{(\infty)} \in \mathbb{Z}_p[x_1, \ldots, x_n]$ such that $e^{(\infty)}$ is the primitive idempotent corresponding to the ideal $M^{(\infty)}$ generated by $f_1^{(\infty)}, \ldots, f_n^{(\infty)}$ in $\mathbb{Q}_p[x_1, \ldots, x_n]$. By Lemma 4.6,

$$[\tau * P - A] \cdot e^{(\infty)} = 0.$$

By (3.16) (from Theorem 3.39), $\tau * P - A \in M^{(\infty)}$. For every i,

$$f_i^{(k)} \equiv f_i^{(\infty)} \pmod{p^k},$$

hence $\tau * P \equiv A \pmod{p^k, \langle \mathcal{G}^{(k)} \rangle}$ and $A = \mathrm{NF}_{\mathcal{G}^{(k)}}(\ \tau * P\ )$. □

Lemma 4.16. With the above notation, suppose σ_i, $i \in \{1, \ldots, m\}$, is output by Algorithm 10. Then $\mathrm{Gal}(f) \subseteq \sigma_i H \sigma_i^{-1}$.

Proof. Let $\mathcal{G}^{(\infty)}$ be the basis lifted from $\mathcal{G}^{(1)}$. Let $A := \mathrm{NF}_{\mathcal{G}^{(\infty)}}(\sigma_i * P)$. Then

$$A_i \equiv A \pmod{p^k}$$

by the construction of A_i. Furthermore, by Theorem 3.39,

$$[\sigma_i * P - A] \cdot e^{(\infty)} = 0$$

in $S_f^{(\infty)}$, where $e^{(\infty)}$ is the primitive idempotent corresponding to the ideal $M^{(\infty)}$ generated by $\mathcal{G}^{(\infty)}$ in $\mathbb{Q}_p[x_1, \ldots, x_n]$. Hence

$$[\sigma_i * P - A_i] \cdot e^{(\infty)} \equiv 0 \pmod{p^k}. \tag{4.14}$$

Let

$$R_P^G(y, x_1, \ldots, x_n) = \prod_{j=1}^{m} (y - (\sigma_j * P)(x_1, \ldots, x_n)).$$

For every $Q(x_1, \ldots, x_n) \in M^{(\infty)}$,

$$[Q(x_1, \ldots, x_n)] \cdot e^{(\infty)} = 0$$

in $S_f^{(\infty)}$ by Theorem 3.39. Hence

$$[R_P^G(y, x_1, \ldots, x_n)] \cdot e^{(\infty)} = \prod_{i=j}^{m} [y - \mathrm{NF}_{\mathcal{G}^{(\infty)}}((\sigma_j * P)(x_1, \ldots, x_n))] \cdot e^{(\infty)}$$

in $S_f^{(\infty)}$. By (4.14),

$$[R_P^G(A_i, x_1, \ldots, x_n)] \cdot e^{(\infty)} \equiv 0 \pmod{p^k}.$$

Moreover, $R_P^G(A_i, x_{\tau(1)}, \ldots, x_{\tau(n)}) = R_P^G(A_i, x_1, \ldots, x_1)$ for every $\tau \in G$. By Proposition 4.3, $\mathrm{Stab}(\bar{e}) \subseteq \mathrm{Stab}(e)$ and

$$e = \sum_{\tau \in \mathcal{T}} \tau * e^{(\infty)},$$

where $\mathcal{T}$ is the set of left coset representatives of $\mathrm{Stab}(\bar{e})$ in $\mathrm{Stab}(e)$. By Lemma 4.5,

$$R^G_{(P,f)}(A_i) \cdot e = R^G_P(A_i, [x_1], \ldots, [x_n]) \cdot e = \sum_{\tau \in \mathcal{T}} R^G_P(A_i, [x_1], \ldots, [x_n]) \cdot (\tau * e^{(\infty)}) =$$
$$= \sum_{\tau \in \mathcal{T}} \tau * (R^G_P(A_i, [x_1], \ldots, [x_n]) \cdot e^{(\infty)}) \equiv 0 \pmod{p^k},$$

where $R^G_{(P,f)} \in \mathbb{Z}[x]$ is the resolvent polynomial associated with P, f, and G. Let $M \subseteq \mathbb{Q}[x_1, \ldots, x_n]$ be the maximal ideal such that e is the primitive idempotent corresponding to M. By Theorem 3.20,

$$\nu : S_f \to \mathbb{Q}[x_1, \ldots, x_n]/M$$
$$[g]_{I_f} \mapsto [g]_M.$$

is a surjective homomorphism. Since e is the primitive idempotent corresponding to M, $\nu(e) = [1]_M$. Hence

$$\nu(R^G_{(P,f)}(A_i) \cdot e) = [R^G_{(P,f)}(A_i)]_M.$$

As

$$R^G_{(P,f)} \cdot e \equiv 0 \pmod{p^k},$$

$R^G_{(P,f)}(A_i) \bmod p^k \in M$. But M is a maximal (hence proper) ideal, so

$$R^G_{(P,f)}(x) = (x - A_i)u(x) + p^{k+1}v(x)$$

for some $u, v \in \mathbb{Z}[x]$. Now, either A_i is a root of $R^G_{(P,f)}$ or $R^G_{(P,f)}(A_i) \geq p^k$.

By the definition of the resolvent polynomial,

$$R^G_{(P,f)}(A_i) = \prod_{i=1}^{m} (A_i - (\sigma_i * P)(\alpha_1, \ldots, \alpha_n)) < (2B)^m.$$

By the choice of k,

$$(2B)^m < p^k$$

and A_i is a root of $R^G_{(P,f)}$. By Corollary 2.34, if we show that A_i is a simple root of $R^G_{(P,f)}$ then $\mathrm{Gal}(f) \subseteq \sigma_i H \sigma_i^{-1}$. Suppose $j \in \{1, \ldots, m\}$ is such that $(\sigma_j * P)(\alpha_1, \ldots, \alpha_n) = A_i$. By Lemma 4.6, $[\sigma_j * P - A_i] \cdot e^{(\infty)} = 0$. Hence

$$\sigma_j * P \equiv A_i \pmod{p^k, \langle \mathcal{G}^{(k)} \rangle}$$

and thus $A_i = \mathrm{NF}_{\mathcal{G}^{(k)}}(\ \sigma_j * P\ )$. By the condition from Line 30 of Algorithm 10, $j = i$ and A_i is a simple root. $\square$

Lemma 4.17. If $P \in \mathbb{Z}[x_1, \ldots, x_n]$ is such that $R^G_{(P,f)}$ is separable then the condition of Line 30 of Algorithm 10 holds, i.e. the algorithm terminates.

Proof. Let $A \in \mathbb{Z}$, $|A| < B$, be an integer such that $R^G_{(P,f)}(A) \equiv 0 \pmod{p^k}$, where $(2B)^m < p^k$ and B is from Line 4 of Algorithm 10. Let

$$R^G_{(P,f)}(x) = x^m + r_{m-1}x^{m-1} + \cdots + r_1 x + r_0.$$

Let $s_1, \ldots, s_m$ be the elementary symmetric functions in m variables. For every $i \in \{0, \ldots, m-1\}$,

$$|r_i| = |s_{m-i}((\sigma_1 * P)(\alpha_1, \ldots, \alpha_n), \ldots, (\sigma_m * P)(\alpha_1, \ldots, \alpha_n))| \leq \binom{m}{m-i} B^{m-i}.$$

We denote by R' the formal derivative of $R^G_{(P,f)}$. As $|A| < B$,

$$\begin{aligned} |R'(A)| &\leq mB^{m-1} + (m-1)|r_{m-1}|B^{m-2} + \cdots + |r_1| < \\ &< mB^{m-1}\left(1 + \binom{m}{1} + \cdots + \binom{m}{m-1}\right) \end{aligned}$$

Since $m < B$,

$$|R'(A)| < (2B)^m. \tag{4.15}$$

Assume that A is a multiple root modulo p^k of $R^G_{(P,f)}$:

$$R^G_{(P,f)}(x) \equiv (x - A)^v h(x) \pmod{p^k},$$

where $v \geq 2$, $h \in \mathbb{Z}[x]$. Then

$$R'(A) \equiv 0 \pmod{p^k}$$

so either $R'(A) = 0$ or $R'(A) \geq p^k$. Recall that $(2B)^m < p^k$. Hence $R'(A) = 0$ by (4.15). This contradicts the separability of $R^G_{(P,f)}$. □

Conclusion

In the 2nd chapter, we've looked at some fundamental methods for the computation of Galois groups. The rest of this thesis was concerned with the p-adic method, both from the theoretical and algorithmic point of view. Examples were given for polynomials of degree 3 and 4. More examples of higher degree polynomials would be desirable too but that would probably exceed the usual scope of a master thesis.

List of Figures

Bibliography

[1] H. Anai, M. Noro, and K. Yokoyama. "Computation of the Splitting Fields and the Galois Groups of Polynomials". In: *Progress in Mathematics* 143 (1996), pp. 29–50.

[2] J.-M. Arnaudies and A. Valibouze. "Résolvantes de Lagrange". In: *Rapport LITP* (1993).

[3] A. D. Barnard. "Commutative Rings with Operators". In: *Proceedings of the London Mathematical Society* s3-28 (1974), pp. 274–290.

[4] L. Barto and D. Stanovský. *Počítačová Algebra*. Matfyzpress, 2011. ISBN: 978-80-7378-167-5.

[5] T. Becker, V. Weispfenning, and H. Kredel. *Gröbner Bases - A Computational Approach to Commutative Algebra*. Springer-Verlag, 1993. ISBN: 0-387-97971-9.

[6] H. Cohen. *A Course in Computational Algebraic Number Theory*. 3rd corrected edition. Springer-Verlag, 1996. ISBN: 3-540-55640-0.

[7] A. Drápal. *Skripta k předmětu Komutativní Okruhy*. Online: `http://www.karlin.mff.cuni.cz/~zemlicka/11-12/komalg.pdf`.

[8] A. Drápal. *Teorie Grup - Základní Aspekty*. Karolinum, 2009.

[9] K. Geissler. *Berechnung von Galoisgruppen über Zahl- und Funktionenkörpern*. Dissertation: Technical University of Berlin, 2003.

[10] K. Geissler and J. Klüners. "Galois Group Computation for Rational Polynomials". In: *Journal of Symbolic Computation* 30 (2000), pp. 653–674.

[11] K. Girstmair. "On the Computation of Resolvents and Galois Groups". In: *Manuscripta Mathematica* 43 (1983), pp. 289–307.

[12] A. Hulpke. *Konstruktion transitiver Permutationsgruppen*. Rheinisch-Westfälische Technische Hochschule, Aachen, Germany, 1996.

[13] S. Katok. *P-adic Analysis Compared with Real*. Student Mathematical Library, 2007. ISBN: 978-0-8218-4220-1.

[14] J. Klüners. "On Computing Subfields. A Detailed Description of the Algorithm". In: *Journal de Théorie des Nombres de Bordeaux* 10 (1998), pp. 243–271.

[15] D. E. Knuth. *The Art of Computer Programming, Volume 2*. 3rd ed. Addison-Wesley Publishing Company, 1981. ISBN: 0-201-89684-2.

[16] S. Lang. *Algebra*. 3rd ed. Springer-Verlag, 2002. ISBN: 978-0-387-95385-4.

[17] H. Lombardi and C. Quitté. *Commutative Algebra: Constructive Methods*. Springer, 2015. ISBN: 978-94-017-9943-0.

[18] M. Noro. "A Computer Algebra System: Risa/Asir". In: *Joswig M., Takayama N. (eds) Algebra, Geometry and Software Systems* (2003), pp. 147–162.

[19] M. Pohst and H. Zassenhaus. *Algorithmic Algebraic Number Theory*. Cambridge University Press, 1989. ISBN: 0-521-33060-2.

[20] L. Procházka. *Algebra*. Academia, 1990.

[21] G. Renault and K. Yokoyama. "A Modular Method for Computing the Splitting Field of a Polynomial". In: *ANTS 2006: Algorithmic Number Theory* (2006), pp. 124–140.

[22] L. Soicher and J. McKay. "Computing Galois groups over the rationals". In: *Journal of Number Theory* 20 (1985), pp. 273–281.

[23] R. Stauduhar. "The Determination of Galois Groups". In: *Mathematics of Computation* 27 (1973), pp. 981–996.

[24] A. Valibouze. *Theory of Equations, Lagrange and Galois Theory*. Lecture Notes: `https://hal.archives-ouvertes.fr/cel-00403452`.

[25] B. L. Waerden. *Modern Algebra*. Frederick Ungar Publishing, 1953.

[26] K. Yokoyama. "A Modular Method for Computing the Galois Groups of Polynomials". In: *Journal of Pure and Applied Algebra* 117 (1997), pp. 617–636.

[27] K. Yokoyama, M. Noro, and T. Takeshima. "On Determining the Solvability of Polynomials". In: *Proceedings of the International Symposium on Symbolic and Algebraic Computation*. ISSAC '90. Tokyo, Japan: ACM, 1990, pp. 127–134. ISBN: 0-201-54892-5. DOI: `10.1145/96877.96910`. URL: `http://doi.acm.org/10.1145/96877.96910`.