ON THE COMPUTATION OF EMBEDDINGS AND SPLITTING FIELDS OF NUMBER FIELDS.

B. ALLOMBERT

ABSTRACT. We describe an algorithm for computing the embeddings and the splitting field of a number field which makes use of factorization of polynomials over number fields in a novel way.

1. Embedding of number fields

1.1. **Introduction.** Let $S, T \in \mathbb{Z}[X]$ be monic irreducible polynomials and assume that $\deg S < \deg T$. The object of this note is the computation of the embeddings between $K = \mathbb{Q}[X]/(S)$ and $L = \mathbb{Q}[X]/(T)$, if any. Such homomorphism can be specified by the image of $X \pmod S$ in L.

The classical algorithm to solve this problem relies on computing the roots of S in L which requires to perform algebraic numbers reconstructions in L. The algorithm presented is this note relies on the factorization of T over K, which only requires to perform algebraic numbers reconstructions in the smaller field K.

In this section we compute the factorization of the étale algebra $A = K \otimes_{\mathbb{Q}} L \cong \mathbb{Q}[X,Y]/(T(X), S(Y))$ as a product of fields in two different ways.

First note that A is isomorphic both to $L[X]/(S(X))$ and $K[X]/(T(X))$.

Denote by $S(Y) = \prod_{i=1}^{n} S_i(Y)$ the factorization of S as a product on monic irreducible polynomials over L. Note that S being irreducible implies that the S_i are distinct. By the Chinese remainder theorem,

$$A \cong \prod_{i=1}^{n} L[Y]/(S_i(Y)) \cong \prod_{i=1}^{n} \mathbb{Q}[X,Y]/(T(X), S_i(X,Y))$$

where $S_i(X,Y))$ is the lift of $S_i(Y)$ in $(\mathbb{Q}[X]/(T(X)))[Y]$ to $\mathbb{Q}[X,Y]$. In the same way, if $T(Y) = \prod_{i=1}^{m} T_i(Y)$, then

$$A \cong \prod_{i=1}^{m} K[Y]/(T_i(Y)) \cong \prod_{i=1}^{m} \mathbb{Q}[X,Y]/(S(X), T_i(X,Y))$$

where $T_i(X,Y))$ is the lift of $T_i(Y)$ in $(\mathbb{Q}[X]/(S(X)))[Y]$ to $\mathbb{Q}[X,Y]$.

Since A is étale, the factorization as a product of fields is unique. In particular $n = m$. The codimension of the ideal $(T(X), S_i(X,Y))$ is equal to $\deg T(X) \deg S_i(Y)$ and the codimension of the ideal $(S(X), T_i(X,Y))$ is equal to $\deg S(X) \deg T_i(Y)$.

Date: on November 17, 2020.

1991 *Mathematics Subject Classification.* Primary 11Y40.

Key words and phrases. Number field, Algorithm.

In particular, the number of embeddings is equal to the number of S_i such that $\deg S_i = 1$,which is equal to the number of T_i such that $\deg T_i = \frac{\deg T}{\deg S}$.

1.2. **Elimination theory.** Let $(S(X), T_i(X, Y))$ an ideal of $\mathbb{Q}[X, Y]$ such that S is irreducible over $\mathbb{Q}$ and $T_i(X, Y) \pmod{S}$ is irreducible over $\mathbb{Q}(X)/(S(X))$. Then by elimination theory, it exists two polynomials $T(Y)$ and $S_i(X, Y)$ such that $(T(X), S_i(X, Y)) = (S(Y), T_i(X, Y))$. Then can be computed explicitly using resultants and the concept of Last non-constant polynomial in the Euclidean remainder sequence (LERS). Precisely:

$$T(Y) = \mathrm{Res}_X(S(X), T_i(X, Y)) \tag{1}$$

$$S_i(X, Y) = \mathrm{LERS}_X(S(X), T_i(X, Y)) \tag{2}$$

Both can be computed efficiently using multimodular quasi-linear algorithms. Note that when computed this way, S_i is not monic in general, which can be advantageous, see below.

1.3. **Computing the embeddings.** Starting from a factor T_i of degree $\frac{\deg T}{\deg S}$, the previous section leads to a polynomial S_i such that $\deg_X S_i = 1$, which can be written as $S_i(X, Y) = A(Y)X + B(Y)$ where A and B are polynomials in $\mathbb{Q}[Y]$ of degree strictly less than $\deg T$.

So the corresponding root of S in $\mathbb{Q}[X]/(T(X))$ is $-B(X)/A(X) \pmod{T}(X)$. Using multimodular division algorithms, it is possible to find $R(X) \in \mathbb{Q}[X]$ such that $R(X) \equiv -B(X)/A(X) \pmod{T(X)}$ which the embedding requested. However R is in general much larger that A and B so for a number of applications it can be preferable to return $-B(X)/A(X)$ as a rational function.

1.4. **The algorithm.** This leads to the following algorithm:

Algorithme 1. *Let S and T be monic irreducible polynomials over $\mathbb{Q}$, the following algorithm returns the embeddings from $\mathbb{Q}[X]/(S(X))$ to $\mathbb{Q}[X]/(T(X))$.*

(1) *Compute the factorization of T over $\mathbb{Q}[Y]/(S(Y))$ as $T(X) = \prod_{i=1}^{n} T_i(X)$.*
(2) *For all factors T_i of degree $\frac{\deg T}{\deg S}$, compute $S_i(X) = LERS_X(S(X), T_i(X, Y))$.*
(3) *For each S_i, return the quotient $-B(X)/A(X) \pmod{T(X)}$.*

2. Computing splitting fields

Let T be monic irreducible polynomial over $\mathbb{Q}$. The splitting field of $K = \mathbb{Q}[X]/(T(X))$ is the smallest field L such that $L \otimes K \cong L^{\deg T}$.

The following algorithm balances the costs of factorization with the cost of algebraic numbers reconstructions by doing all the factorizations over K.

Algorithme 2. *Set $K = \mathbb{Q}[Y]/(T(Y))$, $L_0 = T$ and for $j = 0, 1, 2, \ldots$ do*

(1) *factor $L_j(X)$ over K as $L_j(X) = \prod_{i=1}^{n} F_i(X, Y) \pmod{T(Y)}$.*
(2) *if $n = \deg T$, return L_j.*
(3) *otherwise let S be one of the T_i of maximal degree, find a small integer k such that $R(X) = Res_Y(S(X + kY, Y), T(Y))$ is squarefree.*
(4) *Set $L_{j+1} = R$.*

Bill Allombert, IMB, Université de Bordeaux, 351 cours de la Libération, 33 405 Talence, France.

Email address: `allomber@math.u-bordeaux.fr`