SÉMINAIRE DE THÉORIE DES NOMBRES DE BORDEAUX

HENRI COHEN
FRANCISCO DIAZ Y DIAZ

A polynomial reduction algorithm

Séminaire de Théorie des Nombres de Bordeaux, tome 3, n° 2 (1991), p. 351-360

<http://www.numdam.org/item?id=JTNB_1991__3_2_351_0>

© Université Bordeaux 1, 1991, tous droits réservés.

L'accès aux archives de la revue « Séminaire de Théorie des Nombres de Bordeaux » (http://jtnb.cedram.org/) implique l'accord avec les conditions générales d'utilisation (http://www.numdam.org/conditions). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM
Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
http://www.numdam.org/

Séminaire de Théorie des Nombres,
Bordeaux **3** *(1991), 351-360*

A polynomial reduction algorithm.

PAR HENRI COHEN AND FRANCISCO DIAZ Y DIAZ

Résumé — *L'algorithme que nous décrivons dans ce papier est une approche pratique de la représentation d'un corps de nombre K par la racine d'un polynôme aussi canonique que possible. Nous utilisons l'algorithme LLL pour trouver une base de petits vecteurs pour le réseau de $\mathbb{R}^n$ image des entiers de K par le plongement canonique.*

Abstract — *The algorithm described in this paper is a practical approach to the problem of giving, for each number field K a polynomial, as canonical as possible, a root of which is a primitive element of the extension $K/\mathbb{Q}$. Our algorithm uses the LLL algorithm to find a basis of minimal vectors for the lattice of $\mathbb{R}^n$ determined by the integers of K under the canonical map.*

Very often, number fields arise as $K = \mathbb{Q}[\theta]$, where θ is an algebraic integer of degree n root of a minimal monic polynomial $P \in \mathbb{Z}[X]$. There of course exist an infinite number of such polynomials P, one for every algebraic integer of degree exactly equal to n belonging to K.

Given a number field K, it would be nice be able to find a unique P defining K if we add a few extra properties. For example, this would immediately solve the problem of deciding whether two number fields are isomorphic or not.

In this note, we give an algorithm which is a first approach to answering this problem, and which has proved to be very useful. After explaining the basic algorithm, we give four examples for which we thank our colleague M. Olivier, and we conclude by giving a variation on the basic algorithm which gives a polynomial which is as canonical as possible.

1. Description of the algorithm

A natural idea is to define a notion of "simplicity" of a polynomial. For example, we could say that a polynomial is simple if the largest absolute value of its coefficients is as small as possible (i.e. the L^∞ norm on the coefficients), or such that the sum of the squares of the coefficients is as small as possible (the L^2 norm). Unfortunately, we know of no really

Manuscrit reçu le 19 mai 1991.

efficient way of finding "simple" polynomials in this sense, even if we do not ask for *the* simplest, but a simple polynomial defining K.

What we will in fact consider is the following "norm" on polynomials.

DEFINITION. *Let $P \in \mathbb{C}[X]$, and let α_i be the complex roots of P repeated with multiplicity. We define the* size *of P by the formula*

$$size(P) = \sum_i |\alpha_i|^2 .$$

This is not a norm on $\mathbb{C}[X]$ in the usual mathematical sense, but it seems reasonable to say that if the size (in this sense) of a polynomial is not large, then the polynomial is simple, and its coefficients should not be too large.

More precisely, one can show that if $P = \sum_{k=0}^{n} a_k X^k$ is a monic polynomial and if $S = \text{size}(P)$, then

$$|a_{n-k}| \leq \binom{n}{k} \left(\frac{S}{n}\right)^{k/2},$$

hence the size of P is related to the size of

$$\max |a_{n-k}|^{2/k} .$$

The reason for which we take this definition instead of an L^p definition on the coefficients is that we can apply the LLL algorithm to find a polynomial of small size which defines the same number field K as the one defined by a given polynomial P, while we do not know how to achieve this for the norms on the coefficients.

The method is as follows. Let K be defined by a monic irreducible polynomial $P \in \mathbb{Z}[X]$. We first compute an integral basis $\omega_1, \ldots, \omega_n$ of the ring of integers of K, by using for example the Pohst-Zassenhaus round 2 or round 4 algorithms.

Denote by σ_j the n isomorphisms of K into $\mathbb{C}$. If we set

$$x = \sum_{i=1}^{n} x_i \omega_i$$

where the x_i are in $\mathbb{Z}$, then x is an arbitrary algebraic integer in K, hence its characteristic polynomial M_x will be of the form $P_d^{n/d}$, where P_d is

the minimal polynomial of x and d is the degree of x. Now P_d defines a subfield of K, and in particular when $n = d$, it defines an equation for K. Futhermore it is clear that all equations for K or its subfields are obtained in this way.

Now we have by definition

$$M_x(X) = \prod_{k=1}^{n} \left(X - \sum_{i=1}^{n} x_i \sigma_k(\omega_i) \right)$$

hence

$$\text{size}(M_x) = \sum_{k=1}^{n} \left| \sum_{i=1}^{n} x_i \sigma_k(\omega_i) \right|^2$$

This is clearly a positive definite quadratic form in the x_i's, and more precisely

$$\text{size}(M_x) = \sum_{i,j} \left(\sum_{1 \le k \le n} \sigma_k(\omega_i) \overline{\sigma_k}(\omega_j) \right) x_i x_j.$$

Note that in the case where K is totally real, that is when all the σ_k are real embeddings, then this simplifies to

$$\text{size}(M_x) = \sum_{i,j} \text{Tr}(\omega_i \omega_j) x_i x_j$$

which is now a quadratic form with integer coefficients which can easily be computed from the knowledge of the ω_i.

In any case, whether K is totally real or not, we can apply the LLL algorithm to the lattice $\mathbb{Z}^n$ and the quadratic form $\text{size}(M_x)$. The result will be a set of n vectors x corresponding to reasonably small values of the quadratic form (see [LLL] for quantitative statements), hence to polynomials M_x of small size, which is what we want. Note that we will often obtain in this way algebraic integers x of degree $d < n$, hence this will give us for free some subfields of K. In particular, $x = 1$ is always obtained as a short vector, and this defines the subfield $\mathbb{Q}$ of K. Practical experiments with this method show however that, at least for small values of n, there is always at least one element x of degree exactly n, hence defining K. On the other hand, it is definitely possible that no polynomial of degree n occurs, although it is a very rare occurence. That this is possible in principle has been shown by H. W. Lenstra (private communication), but in practice, on more than 10000 polynomials of various degree we have never encountered

a failure. In this unfavorable case, we can of course try to look for elements of small norm other than those given by LLL, but it will be much slower.

Although the minimal polynomials of the elements of degree n that we obtain have usually smaller coefficients than the polynomial P from which we started, it is also often the case that they have much greater coefficients than those of P, and this is because the "size" of P does not directly reflect the size of the coefficients (see above).

Note that it is absolutely not true that our algorithm will give *all* the subfields of K. In fact, the LLL algorithm gives us exactly n vectors, but a number field of degree n may have much more than n distinct subfields.

The algorithm, which we name POLRED for polynomial reduction, is as follows.

Algorithm. Let $K = \mathbb{Q}[\theta]$ be a number field defined by a monic irreducible polynomial $P \in \mathbb{Z}[X]$. This algorithm gives a list of polynomials defining certain subfields of K (including $\mathbb{Q}$), and which are often simpler than the polynomial P so can be used to define the field K if they are of degree equal to the degree of K.

1. [Compute the maximal order] Using for example the round 2 algorithm (see e.g. [Ford]), compute an integral basis $\omega_1, \ldots, \omega_n$ as polynomials in θ.

2. [Compute matrix] If the field K is totally real (which can be easily checked using Sturm's algorithm), set $m_{i,j} \leftarrow \mathrm{Tr}(\omega_i\omega_j)$ for $1 \leq i, j \leq n$, which will be an element of $\mathbb{Z}$.

Otherwise, compute a reasonably accurate approximation of θ and its conjugates $\sigma_j(\theta)$ as the roots of P in $\mathbb{C}$, then the numerical values of $\sigma_j(\omega_k)$, and finally compute

$$m_{i,j} \leftarrow \sum_{1 \leq k \leq n} \sigma_k(\omega_i)\overline{\sigma_k}(\omega_j)$$

(note that this will be a real number).

3. [Apply LLL] Using the LLL algorithm applied to the inner product defined by the matrix $M = (m_{i,j})$ and to the standard basis of the lattice $\mathbb{Z}^n$, compute an LLL-reduced basis $\mathbf{b}_1, \ldots, \mathbf{b}_n$.

4. [Compute characteristic polynomials] For $1 \leq i \leq n$, compute the characteristic polynomial C_i of the element of $\mathbb{Z}_K$ corresponding to $\mathbf{b}_i$ on the basis $1, \theta, \ldots, \theta^{n-1}$.

5. [Compute minimal polynomials] For $1 \leq i \leq n$, set

$$P_i \leftarrow C_i / \gcd(C_i, C_i')$$

where the gcd is always normalized so as to be monic, output the polynomials P_i and terminate the algorithm.

Since we will have $C_i = P_i^{n/d_i}$, it is clear that the computation of step 5 gives us P_i in terms of C_i.

2. Examples

We now give examples of the use of the POLRED algorithm.

In [Kwon-Mart], the smallest discriminant of a quintic number field with one real place and having the metacyclic group M_{20} as the Galois group of its Galois closure, is shown to be generated by a root of the polynomial

$$P(X) = X^5 - 2X^4 - 4X^3 - 96X^2 - 352X - 568$$

of discriminant $2^4 \cdot 13^3 \cdot (2^4 \cdot 10429)^2$. Using POLRED on this polynomial we find that our quintic number field can also be generated by a root of the simpler polynomial

$$Q(X) = X^5 - X^4 + 2X^3 - 4X^2 + X - 1$$

whose discriminant is $2^4 \cdot 13^3$ equal to the discriminant of the field.

The next example is taken from work of M. Olivier. Consider the polynomial

$$P(X) = X^6 + 2X^5 - 7X^4 - 12X^3 + 10X^2 + 17X + 4.$$

This polynomial is irreducible over $\mathbb{Q}$, hence defines a number field K of degree 6. Furthermore, one computes that the complex roots of P are approximately equal to

$$-2.7494482169, -1.7152399972, -0.8531562311, -0.3074682781,$$
$$1.5839340557, 2.0413786677.$$

Now one computes that

$$\mathrm{disc}(P) = 11699^2,$$

hence the Galois group G of the Galois closure of K, considered as a permutation group on the roots of P, is a subgroup of the alternating group A_6. Furthermore, direct computations on the roots show that K does not have any non-trivial subfields. The classification of transitive permutation groups of degree 6 then shows that G is isomorphic either to A_5 or to A_6.

To distinguish between the two, we use a resolvent function given by [Stau] and the resolvent polynomial thus obtained is

$$R(X) = X^6 + 3694X^5 + 1246830X^4 - 7355817976X^3 - 5140929655107X^2 + 3486026298845999X + 2593668315970494361.$$

A computation of the roots of this polynomial shows that it has an integer root $x = -673$, and this shows that G is isomorphic to A_5. In addition, $Q(X) = R(X)/(X + 673)$ is an irreducible fifth degree polynomial which defines a number field with the same discriminant as K. We have

$$Q(X) = X^5 + 3021X^4 - 786303X^3 - 6826636057X^2 - 546603588746X + 3853890514072057,$$

and the discriminant of Q (which must be a square) has 63 decimal digits. Now if we apply the POLRED algorithm, we obtain five polynomials, four of which defining the same field as Q, and the polynomial with smallest discriminant is

$$S(X) = X^5 + 2X^4 - 13X^3 - 37X^2 - 21X + 1,$$

a much more appealing polynomial than Q.

Note that we also have $\mathrm{disc}(S) = 11699^2$.

There was a small amount of cheating in the above example: since $\mathrm{disc}(Q)$ is a 63 digit number, the POLRED algorithm, which in particular computes an integral basis of K hence needs to factor $\mathrm{disc}(Q)$, may need quite a lot of time to factor this discriminant. However, we can in this case help the POLRED algorithm by telling it that $\mathrm{disc}(Q)$ is a square, which we know a priori, but which is not usually tested for in a factoring algorithm since it is quite rare an occurence. This is how the above example was computed in practice, and the whole computation, including typing the commands, took a few minutes on a workstation.

A similar example is obtained by starting with the polynomial

$$P(X) = X^6 + 2X^5 + X^4 + 4X^3 + 2X^2 - 4X + 1.$$

We also find that its Galois group is isomorphic to A_5, and the fifth degree polynomial $Q(X)$ obtained as above is

$$Q(X) = X^5 - 436X^4 - 50552X^3 - 2486048X^2 - 58353392X - 612934720.$$

The use of POLRED gives us as polynomial of the fifth degree with smallest discriminant the polynomial

$$S(X) = X^5 + 2X^3 - 4X^2 + 6X - 4.$$

Now as remarked in [Oliv], the polynomial P is interesting because it gives a primitive sextic number field with A_5 as Galois group of the Galois closure, and of discriminant $d = 287296 = (2^3 \cdot 67)^2$, and it is the one with smallest discriminant in absolute value. Curiously enough, this discriminant is also the smallest for primitive sextic number fields with A_6 as Galois group of the Galois closure (defined for example by $X^6 + 2X^5 - X^4 + 2X^2 - 1$).

Another interesting property of the polynomial P becomes again apparent with the use of POLRED. If we apply POLRED to the polynomial P itself (which is already simple enough, but no matter), we obtain five other sixth degree polynomials, one of which is

$$T(X) = X^6 + 2X^5 + X^4 - 2X^3 + 2X^2 - 4X + 1.$$

Now A. Brumer has noticed that the plus part $J^+(67)$ of the Jacobian of the modular curve $X_0(67)$ is isogenous to the Jacobian of the curve $y^2 = T(-x)$, and the minus part $J^-(67)$ is isogenous to the product of the Jacobian of $y^2 = P(-x)$ by the elliptic curve 67a of [Ant IV].

As a last example, we give examples of the use of POLRED in showing that different polynomials generate isomorphic fields. For this, we use totally real octic polynomials of discriminant 282300416 and 309593125 given in [PMD].

A totally real octic field K of discriminant $d = 282300416$ is generated by a root of the polynomial

$$P(X) = X^8 + 2X^7 - 7X^6 - 8X^5 + 15X^4 + 8X^3 - 9X^2 - 2X + 1$$

Applying POLRED to $P(X)$ we obtain

$$\begin{aligned}
&X-1\\
&X^8+2X^7-7X^6-8X^5+15X^4+8X^3-9X^2-2X+1\\
&X^8+2X^7-7X^6-8X^5+15X^4+8X^3-9X^2-2X+1\\
&X^8-2X^7-7X^6+12X^5+8X^4-14X^3+4X-1\\
&X^8-4X^7+14X^5-8X^4-12X^3+7X^2+2X-1\\
&X^2-2\\
&X^8+4X^7-14X^5-8X^4+12X^3+7X^2-2X-1\\
&X^8-2X^7-7X^6+8X^5+15X^4-8X^3-9X^2+2X+1
\end{aligned}$$

thus showing that the fields generated by the roots of the polynomials given in [PMD] are isomorphic, and also that $\mathbb{Q}(\sqrt{2})$ is a subfield. The fact that the same polynomial is obtained several times gives also some information on the Galois group of the Galois closure of the number field K, since it shows that the automorphism group of K is non-trivial.

For discriminant $d = 309593125$, applying POLRED to the polynomial

$$P(X) = X^8+3X^7-5X^6-21X^5-3X^4+35X^3+28X^2+4X-1$$

we obtain

$$\begin{aligned}
&X-1\\
&X^2-X-1\\
&X^4+X^3-3X^2-X+1\\
&X^4+2X^3-2X^2-3X+1\\
&X^8+3X^7-5X^6-14X^5+8X^4+16X^3-2X^2-5X-1\\
&X^8+X^7-10X^6-8X^5+22X^4+15X^3-13X^2-8X-1\\
&X^8+3X^7-5X^6-21X^5-3X^4+35X^3+28X^2+4X-1\\
&X^8-4X^7-X^6+17X^5-5X^4-23X^3+6X^2+9X-1,
\end{aligned}$$

where four of the polynomials given for this field in [PMD] occur, and in addition a polynomial for $\mathbb{Q}(\sqrt{5})$, and two quartic polynomials. Another application of POLRED shows that both generate the unique (up to isomorphism) quartic number field of discriminant 725.

If we apply POLRED to the other polynomials given in [PMD] for discriminant $d = 309593125$, i.e. for

$$Q(X) = X^8 + X^7 - 10X^6 - 17X^5 + 8X^4 + 22X^3 + 2X^2 - 5X - 1$$

$$R(X) = X^8 + X^7 - 10X^6 + 23X^4 - 5X^3 - 15X^2 + 3X + 1$$

and for

$$S(X) = X^8 + 2X^7 - 9X^6 - 9X^5 + 20X^4 + 14X^3 - 11X^2 - 8X - 1$$

we obtain the same polynomials (up to the trivial change X into $-X$), showing that the fields generated by all these polynomials are isomorphic.

3. A pseudo-canonical defining polynomial

As mentioned in the introduction, we can use the basic POLRED algorithm to obtain a polynomial defining a number field K which is as canonical as possible.

We first need a notation. If $Q(X) = \sum_{0 \le i \le n} a_i X^i$ is a polynomial of degree n, we set

$$v(Q) = (|\operatorname{disc}(Q)|, \operatorname{size}(Q), |a_n|, |a_{n-1}|, \ldots, |a_1|, |a_0|).$$

Algorithm. Given a number field K defined by a monic irreducible polynomial $P \in \mathbb{Z}[X]$ of degree n, this algorithm outputs another polynomial defining K which is as canonical as possible.

1. [Apply POLRED] Apply the POLRED algorithm to P, and let P_i (for $i = 1, \ldots, n$) be the n polynomials which are output by the POLRED algorithm. If none of the P_i are of degree n, output a message saying that the algorithm has failed, and terminate the algorithm. Otherwise let $\mathcal{L}$ be the set of i such that P_i is of degree n.

2. [Minimize $v(P_i)$] If $\mathcal{L}$ has a single element, let Q be this element. Otherwise for each $i \in \mathcal{L}$ compute $v_i \leftarrow v(P_i)$ and let v be the smallest v_i for the lexicographic ordering of the components. Let Q be any P_i such that $v(P_i) = v$.

3. [Possible sign change] Search for the non-zero monomial of largest degree d such that $d \not\equiv n \pmod 2$. If such a monomial exists, make if necessary the change $Q(X) \leftarrow (-1)^n Q(-X)$ so that the sign of this monomial is negative.

4. [Terminate] Output Q and terminate the algorithm.

Remarks.

(1) As already mentioned the POLRED algorithm may give only polynomials of degree less than n, hence the above algorithm will fail in that case. This is a very rare occurence.

(2) At the end of step 2 there may be several i such that $v_i = v$. In that case, it may be useful to output all the possibilities (after executing step 3 on each of them) instead of only one. In practice, this is also rare.

References

[Ford] D. J. Ford, *The construction of maximal orders over a Dedekind domain*, J. Symbolic Computation **4** (1987), 69–75.

[Kwon-Mart] S.-H. Kwon and J. Martinet, *Sur les corps résolubles de degré premier*, J. Reine Angew. Math. **375/376** (1987), 12–23.

[LLL] A. K. Lenstra, H. W. Lenstra, Jr. and L. Lovász, *Factoring polynomials with rational coefficients*, Math. Annalen **61** (1982), 515–534.

[Oliv] M. Olivier, *Corps sextiques primitifs*, Ann. Institut Fourier **40** (1990), 757–767.

[PMD] M. Pohst, J. Martinet and F. Diaz y Diaz, *The minimum discriminant of totally real octic fields*, J. Number Theory **36** (1990), 145–159.

[Stau] R. P. Stauduhar, *The determination of Galois groups*, Math. Comp. **27** (1973), 981–996.

Centre de Recherches en Mathématiques de Bordeaux
351 Cours de la Libération
33405 Talence Cedex
France.