J. Austral. Math. Soc. (*Series A*) **49** (1990), 434–448

COMPUTING SUBFIELDS IN ALGEBRAIC NUMBER FIELDS

JOHN D. DIXON

(Received 23 May 1989; revised 26 April 1990)

Communicated by R. Lidl

Dedicated to G. E. (Tim) Wall, in recognition of his distinguished contribution to mathematics in Australia, on the occasion of his retirement

Abstract

Let $K := \mathbb{Q}(\alpha)$ be an algebraic number field which is given by specifying the minimal polynomial $f(X)$ for α over $\mathbb{Q}$. We describe a procedure for finding the subfields L of K by constructing pairs $(w(X), g(X))$ of polynomials over $\mathbb{Q}$ such that $L = \mathbb{Q}(w(\alpha))$ and $g(X)$ is the minimal polynomial for $w(\alpha)$. The construction uses local information obtained from the Frobenius-Chebotarev theorem about the Galois group $\mathrm{Gal}(f)$, and computations over p-adic extensions of $\mathbb{Q}$.

1980 *Mathematics subject classification* (*Amer. Math. Soc.*) (1985 *Revision*): 12-04.

1. Introduction

Let $f(X) \in \mathbb{Z}[X]$ be an irreducible polynomial of degree n with a root α, and consider the algebraic number field $K := \mathbb{Q}(\alpha)$. Without any real loss in generality, we shall simplify the discussion by assuming that $f(X)$ is monic, so α is an algebraic integer. From Galois theory we know that K has only a finite number of subfields, and we want to describe a procedure to construct these subfields. Our objective is to specify each subfield L of K by a pair $(w(X), g(X))$ of polynomials in $\mathbb{Q}[X]$ such that $L = \mathbb{Q}(w(\alpha))$ and $g(X)$ is the minimal polynomial of $w(\alpha)$ over $\mathbb{Q}$.

© 1990 Australian Mathematical Society 0263-6115/90 $A2.00 + 0.00

https://doi.org/10.1017/S1446788700032432 Published online by Cambridge University Press

REMARK 1. It can be seen that the problem of describing a subfield L of degree m over $\mathbb{Q}$ in this way is formally equivalent to finding a pair of polynomials $w(X), g(X) \in \mathbb{Q}[X]$ with $g(X)$ irreducible of degree m such that

$$g(w(X)) \equiv 0 \pmod{f(X)}.$$

Since the relation will remain true if we replace $w(X)$ by its remainder modulo $f(X)$ there is no loss in generality in assuming that $\deg w(X) < n = \deg f(X)$. Clearly, if we are given a pair $w(X)$, $g(X)$ of polynomials it is easy to check whether they specify a subfield of K in this sense.

REMARK 2. If we are only given $w(X)$ then there is a well-known algorithm for computing $g(X)$ using linear algebra. Indeed $g(X)$ is the minimal polynomial of the linear transformation $\xi \mapsto \xi w(\alpha)$ of $\mathbb{Q}(\alpha)$ into itself, and a matrix for the latter over the basis $1, \alpha, \ldots, \alpha^{n-1}$ is easily constructed. The converse problem of finding $w(X)$ when $g(X)$ is given seems to be much harder, although the following lemma suggests one approach.

LEMMA. *Let K be an arbitrary field, and let $f(X)$ and $g(X)$ be separable irreducible polynomials over K of degrees n and m respectively, with $m \leq n$. Let α be a root of $f(X)$ in a suitable extension field. Define $h(X) \in K[X]$ to be the monic polynomial of degree mn whose roots are the products of roots of $g(X)$ by roots of $f(X)$, and assume all of these products are distinct (see Appendix* A*). Then*

(a) *each irreducible factor of $h(X)$ over K has degree divisible by n;*

(b) *$g(X)$ has a root in $K(\alpha)$ if and only if $h(X)$ has an irreducible factor $k(X)$ of degree n;*

and

(c) *if $h(X)$ has an irreducible factor $k(X)$ of degree n, then the greatest common divisor* $\mathrm{GCD}(k(X\alpha), g(X))$ *(calculated over $K(\alpha)[X]$) has the form $X - w(\alpha)$ where $w(X) \in K[X]$ and $w(\alpha)$ is a root of $g(X)$.*

PROOF. Let E be a splitting field for $f(X)g(X)$ over K, and let $G := \mathrm{Gal}(E/K)$. Let $\Omega, \Gamma \subseteq E$ be the sets of roots of $f(X)$ and $g(X)$, respectively. Then G acts in a natural way on $\Omega \times \Gamma$, and this action is permutation equivalent to the action of G on the set of roots of $h(X)$ because we are assuming that the latter roots are distinct. Moreover, elementary Galois theory shows that the orbits of G on $\Omega \times \Gamma$ correspond bijectively to the irreducible factors of $h(X)$ over K, such that the length of the orbit is equal to the degree of the corresponding factor. Since G acts transitively on Ω, the orbits of G on $\Omega \times \Gamma$ have lengths which are multiples of n, and so (a) follows.

https://doi.org/10.1017/S1446788700032432 Published online by Cambridge University Press

Moreover, if $g(X)$ has a root β in $K(\alpha)$, then $\alpha\beta$ has degree at most n over K, and so $h(X)$ has an irreducible factor of degree exactly n. This proves part of (b). Finally, if $k(X)$ is an irreducible factor of degree n of $h(X)$, then it has exactly one root of the form $\alpha\beta$ (for some root β of $g(X)$) because G is transitive on Ω. Hence $g(X)$ and $k(X\alpha)$ have exactly one root in common, namely β. Thus

$$\mathrm{GCD}(k(X\alpha), g(X)) = X - w(\alpha)$$

for some $w(\alpha) \in K[\alpha]$, and $\beta = w(\alpha)$. This proves (c) and completes the proof of (b). □

REMARK 3. The lemma is useful for computations over both algebraic number fields and finite fields, but the range of its application is limited by the degree of the polynomial $h(X)$ which has to be factored, so we have avoided using this approach below. (For factorization algorithms see [1] and [13].) We also note that, under the same hypotheses as the lemma, if β is a root of $g(X)$, then $K(\alpha) \cong K(\beta)$ if and only if $m = n$ and $g(X)$ has a root in $K(\alpha)$. Thus the lemma can be used as a basis for deciding isomorphism of extensions. Further results of this type appear in [23]. In particular, [23, Lemma 3.1] gives a generalization of part (c) of the lemma above.

Let $\Omega := \{\alpha = \alpha_1, \alpha_2, \ldots, \alpha_n\}$ be the set of roots of $f(X)$ in some splitting field F of $f(X)$ over $\mathbb{Q}$. (For later convenience we shall assume that Ω is contained in some "universal" field U which contains a copy $\mathbb{Q}_p$ of the p-adic closure of $\mathbb{Q}$ for each prime p.) The problem of finding subfields of K is related to the problem of calculating the action of the Galois group $\mathrm{Gal}(f)$ of F over $\mathbb{Q}$ on Ω. The latter problem appears to be quite difficult, even for moderate sized degrees ([6], [15], [20], [21] and [22]). The cases where $n \leq 4$ are classical and were solved in the last century using criteria based on the discriminant and the cubic resolvent (see [9] or [25]). In the past ten years or so, John McKay and his co-workers have developed techniques to handle polynomials of degrees up to 11. Some of these techniques have been incorporated in a procedure in the symbolic computation language MAPLE to compute the Galois group of any polynomial of degree $n \leq 7$. However, as it presently stands, McKay's technique requires an exhaustive catalogue of all transitive groups of the degree in question, and enough information about invariants to discriminate between these groups. Since there are over 300 transitive groups of degree 12 (see [18]), a straightforward application of these techniques would be very unwieldly for $n = 12$. One motivation to consider the problem of the present paper is that construction of subfields could help in simplifying such Galois computations.

https://doi.org/10.1017/S1446788700032432 Published online by Cambridge University Press

2. Two key ideas for computing Galois groups

Since the ideas are pertinent to our own problem, we shall briefly outline the two main ideas which lie behind McKay's programs ([15], [22]). It should first be noted that the action of $\mathrm{Gal}(f)$ on Ω is only to be determined up to permutation isomorphism since no labelling of the roots is prescribed.

(A) Use of the Frobenius-Chebotarev Theorem. Let p be a prime which does not divide the discriminant $\mathrm{disc}(f)$ of $f(X)$, and consider the factorization

$$f(X) \equiv f_1(X) \cdots f_r(X) \pmod{p} \tag{1}$$

where the $f_i(X) \in \mathbb{Z}[X]$ are monic of degree n_i, say, and irreducible modulo p. Then Frobenius showed that $\mathrm{Gal}(f)$ contains a permutation of Ω whose disjoint cycles have lengths $n_1, \ldots, n_r$, respectively (see [25, Section 61] for a simple proof). For later purposes we note that we have in fact more precise information about this permutation. The condition that $p \nmid \mathrm{disc}(f)$ is equivalent to the condition that the factors $f_i(X)$ are distinct modulo p. It therefore follows from (1) that the factorization of $f(X)$ over the p-adic field $\mathbb{Q}_p$ has the form

$$f(X) = \tilde{f}_1(X) \cdots \tilde{f}_r(X) \tag{2}$$

where $\tilde{f}_i(X)$ is a monic irreducible polynomial in $\mathbb{Z}_p[X]$ which is congruent $(\mathrm{mod}\, p)$ to $f_i(X)$ for $i = 1, \ldots, r$ [2, page 275]. Moreover, if $F_p = \mathbb{Q}_p(\Omega) \subseteq U$ is the splitting field of $f(X)$ over $\mathbb{Q}_p$, then $\mathrm{Gal}(F_p/\mathbb{Q}_p)$ is cyclic, and this group has a generator π which for each i permutes the roots of $\tilde{f}_i(X)$ in a cycle, say $(\gamma_{i0}, \ldots, \gamma_{is_i})$ where $s_i = n_i - 1$, such that

$$\gamma_{it} \equiv \gamma_{i0}^{p^t} \pmod{p} \quad \text{for } t = 0, \ldots, s_i$$

(see [17, pages 208–209]). Of course, as a permutation group on Ω, the cyclic group $\langle \pi \rangle$ is a subgroup of $\mathrm{Gal}(f)$; this is the essence of the Frobenius theorem quoted above.

In the case where (1) holds we shall use the notation $\mathrm{cycle}(p) = (n_1, \ldots, n_r)$, where we may assume that $n_1 \leq \cdots \leq n_r$. Chebotarev [24] showed that the density (in the sense of Dirichlet) of the primes p for which $\mathrm{cycle}(p)$ takes a specified value is equal to the proportion of permutations in $\mathrm{Gal}(f)$ with this cycle type. For example, asymptotically, $1/|\mathrm{Gal}(f)|$ of the primes have $\mathrm{cycle}(p) = (1, 1, \ldots, 1) = 1^n$ (the cycle type of the identity); these are the primes for which $f(X)$ factors into distinct linear factors modulo p. Recently, effective estimates have been obtained for the number of primes $p \leq x$ which have a specified value for $\mathrm{cycle}(p)$ (see [10] and [19]), but the

https://doi.org/10.1017/S1446788700032432 Published online by Cambridge University Press

bounds are so large that they do not enable us to use the Chebotarev theorem as more than a heuristic aid in computing Galois groups.

The first main step in McKay's program is to use fast methods of factorisation over finite fields (see, for example, [13]) to compute cycle(p) for enough values of p to give definite lower bounds on $\mathrm{Gal}(f)$. From the distribution of cycle types we can often guess what the action of $\mathrm{Gal}(f)$ on Ω probably is. Indeed, when $\mathrm{Gal}(f)$ acts as the symmetric or alternating group on Ω, the information obtained from a small number of cycle types is almost always enough to give a rigorous determination of $\mathrm{Gal}(f)$. (The two cases are distinguished by computing $\mathrm{disc}(f)$; the latter is a square exactly when $\mathrm{Gal}(f) \leq \mathrm{Alt}(\Omega)$.) We should add that a classical theorem of van der Waerden shows that for "almost all" polynomials $\mathrm{Gal}(f)$ will act as the symmetric group on Ω, so that polynomials with more interesting Galois groups have to be constructed rather carefully.

(B) Action of $\mathrm{Gal}(f)$ on k-sets and k-tuples. Let $k \geq 2$ and let $\Omega^{(k)}$ denote the set of subsets of size k of Ω. For each of these k-subsets we form the product of its elements, and consider the monic polynomial $h(X)$ of degree $\binom{n}{k}$ whose roots are these products. Assuming that the roots of $h(X)$ are distinct (see Appendix A), the action of $\mathrm{Gal}(f)$ on $\Omega^{(k)}$ is permutationally equivalent to its action on the set of roots of $h(X)$. In particular, each orbit of $\mathrm{Gal}(f)$ on $\Omega^{(k)}$ corresponds to an irreducible factor of $h(X)$ over $\mathbb{Q}$ whose degree is equal to the length of the orbit. Similarly, using for example the monic polynomial $g(X)$ of degree $n!/(n-k)!$ whose roots have the form

$$(\alpha_{i_1} + 1)(\alpha_{i_2} + 2) \cdots (\alpha_{i_k} + k)$$

with $i_1, i_2, \ldots, i_k$ distinct,the lengths of the orbits of G on the set of all k-tuples of distinct elements from Ω can be determined. Difficulties involved in factoring polynomials of high degree limit such calculations to the case where $k = 2$ or 3, but even this much information (together with the cyle information above) is sufficient to distinguish between the possible Galois groups in many cases (see [3] and [16]). Here as elsewhere we are describing the techniques in terms of products of the roots, but one can equally well work with sums or other suitable functions.

3. Subfields and bases

Put $G := \mathrm{Gal}(f)$ and note that G is transitive on Ω because $f(X)$ is irreducible. Let $F := \mathbb{Q}(\alpha_1, \ldots, \alpha_n)$ be the splitting field of $f(X)$ over $\mathbb{Q}$, and for each subgroup H of G let $\mathrm{Fix}(H)$ denote the subfield of F which is

https://doi.org/10.1017/S1446788700032432 Published online by Cambridge University Press

fixed under H in the Galois connection. In particular, $K = \mathbb{Q}(\alpha) = \mathrm{Fix}(G_\alpha)$ where G_α is the stabilizer of α in G.

Now suppose that L is a subfield of K, so $\mathbb{Q} \subseteq L \subseteq K$. Then for some subgroup H with $G_\alpha \leq H \leq G$ we have $L = \mathrm{Fix}(H)$. Let Δ be the orbit of α under H, and put $d := |\Delta|$. Then it is easily verified that Δ is a block of imprimitivity for G, H is the setwise stabilizer $G_{\{\Delta\}}$ of Δ in G, and $|\Delta| = |H : G_\alpha| = [K : L] = d$. Conversely, for each block Δ for G with $\alpha \in \Delta$, $L := \mathrm{Fix}(G_{\{\Delta\}})$ is a field with $\mathbb{Q} \subseteq L \subseteq K$. This gives a bijective correspondence between the blocks Δ of size d containing α and the intermediate fields L with $[L : \mathbb{Q}] = n/d$.

Next let $\Delta = \Delta_1, \Delta_2, \ldots, \Delta_m$ be the complete system of blocks which are images of Δ under G (so $m = n/d$). Assume that the products

$$\delta_t := \prod\{\alpha_j \mid \alpha_j \in \Delta_t\} \quad \text{for } t = 1, 2, \ldots, m$$

are distinct (see Appendix A). Then the action of G on the set of blocks is permutationally equivalent to its action on the set $\{\delta_1, \delta_2, \ldots, \delta_m\}$. In particular, $H := G_{\{\Delta\}}$ is the stabilizer of $\delta := \delta_1$, and so $L := \mathrm{Fix}(H)$ equals $\mathbb{Q}(\delta)$.

Thus the problem of finding the subfields of K reduces to two subproblems:

(i) find the blocks Δ for G which contain α;

(ii) express the product δ of the roots in Δ in the form $\delta = w(\alpha)$ where $w(X) \in \mathbb{Q}[X]$, and calculate the minimal polynomial of δ over $\mathbb{Q}$.

REMARK. Although δ is an algebraic integer, $w(X)$ need not lie in $\mathbb{Z}[X]$ because $1, \alpha, \ldots, \alpha^{n-1}$ need not be a basis for the algebraic integers in $\mathbb{Q}(\alpha)$ (but see Appendix C). However, the (monic) minimal polynomial $g(X)$ for δ does lie in $\mathbb{Z}[X]$ and its roots are the products δ_t defined above.

4. Finding blocks

If G has a block of size d then, of course, d must divide n. For each prime $p \nmid \mathrm{disc}(f)$, the Frobenius-Chebotarev Theorem gives local information about G which may restrict the sizes of possible blocks. In some cases this may be enough to show that are not blocks for certain values of d.

Suppose that Δ is a block of size d for G and suppose that we know that G contains an element π of cycle type $(n_1, \ldots, n_r)$. Since Δ is a block we known that $\Delta^\tau \cap \Delta = \Delta$ or $\emptyset$ for each $\tau \in G$. Therefore for some integer $k \geq 1$ we have

$$\Delta^{\pi^j} \cap \Delta = \emptyset \quad \text{for } 1 \leq j < k \text{ and } \Delta^{\pi^k} = \Delta.$$

https://doi.org/10.1017/S1446788700032432 Published online by Cambridge University Press

In this case, if some cycle of length n_i in π contains a point from Δ, then k divides n_i and the cycle contains exactly n_i/k poiints of Δ. Since this applies to each block in the system of imprimitivity containing Δ, there must be a partition $\{I_1, \dots, I_s\}$ of $\{1, 2, \dots, r\}$ and integers $k_t \geq 1$ such that for $t = 1, \dots, s$:

$$dk_t = \sum\{n_i \mid i \in I_t\} \text{ and } k_t \mid n_i \text{ for all } i \in I_t. \tag{3}$$

Often computing cycle(p) for a small set of primes will quickly eliminate certain values of d, but the following example shows that in general not all spurious values will be eliminated.

EXAMPLE. Let $G \leq \mathrm{Sym}(15)$ be permutation isomorphic to Alt(6) in its action on unordered pairs ($\binom{6}{2} = 15$). Then G is primitive (and so only has blocks of size 1 and 15). However, its cycle types are

$$1^{15}, 3^5, 5^3, 1^3 2^6, 1^1 2^1 4^3, 1^3 3^4,$$

which do not rule out 3 or 5 as possible block sizes.

Now suppose that d appears to be a possible block size. Then for any prime $p \nmid \mathrm{disc}(f)$ the factorization (2) of $f(X)$ over $\mathbb{Z}_p[X]$ and the corresponding information about the element π from the Galois group usually severely restricts the ways into which the roots in Ω can fall into blocks of size d. With some care in the choice of p we can always ensure that the roots in at least one block will consist of complete cycles of π. For example, recall that in any transitive permutation group the number of fixed points of an element averaged over the group is exactly 1. Thus, according to the Chebotarev theorem, it should not be difficult to find a prime p such that $n_1 = 1$ in cycle(p), and then any block Δ which contains a root in a 1-cycle of π must consist of roots from a union of complete cycles of π (compare with (3)). In such a case the product δ of the roots in Δ will be the product of all roots of a certain set of the $\tilde{f}_i(X)$, and hence $\delta \in \mathbb{Z}_p$. Note that because of the transitivity of G, there is no loss in generality in choosing Δ first and then specifying α arbitrarily as one of the roots in Δ.

In actual computation, of course, we cannot be sure a priori that a particular set Δ of roots which we choose is actually a block, nor can we compute the roots (or δ) exactly, so this step in finding a block is a tentative one. In the next section we shall see how to decide whether the chosen set Δ of roots really is a block. The point at this stage is to use the Frobenius theorem to restrict the number of sets Δ which we have to examine.

5. From blocks to fields

We now look at the second of the subproblems listed above. Suppose that Δ is a block of size d for G (with $m = n/d$), and let δ denote the product

https://doi.org/10.1017/S1446788700032432 Published online by Cambridge University Press

of the elements in Δ. We suppose further that we have chosen Δ so that for some prime $p \nmid \mathrm{disc}(f)$ the elements in Δ form the complete set of roots of certain $\tilde{f}_i(X)$ in (2) (see Section 4). We shall first describe the main algorithms which we shall need, and then explain how they can be used in practice.

Computation of δ to arbitrarily high precision in $\mathbb{Z}_p$ (in other words computing δ as an integer modulo p^k for an arbitrarily high value of k) is achieved by the use of Hensel lifting from the factorization (1). Specifically, for any integer $k \geq 1$, Hensel lifting enables us to go from the mod-p factorization

$$f(X) \equiv f_1(X) \cdots f_r(X) \pmod{p}$$

to a mod-p^k factorization

$$f(X) \equiv f_1^*(X) \cdots f_r^*(X) \pmod{p^k}$$

with $f_i^*(X) \equiv f_i(X) \pmod{p}$ for each i ([2], [27]). Since $f_i^*(X)$ is a mod-p^k approximation to $\tilde{f}_i(X)$, we can easily derive a mod-p^k approximation to δ.

The second step is to compute the minimal polynomial $g(X)$ of δ. This is done by using the algorithm of Lenstra, Lenstra and Lovasz [12]. The basic idea of the LLL-algorithm is to find "short vectors" in lattices over $\mathbb{Z}$, but as [12] shows the algorithm can be applied as follows. Let $u_0(X) \in \mathbb{Z}_p[X]$ be a given monic polynomial of degree l_0, and suppose that there exists an (unknown) monic polynomial $u(X) \in \mathbb{Z}[X]$ which is irreducible over $\mathbb{Z}$ such that $u_0(X)$ divides $u(X)$. If the degree l of $u(X)$ and a bound B on the size of its coefficients are specified, and the coefficients of $u_0(X)$ are given to within modulo p^k (where k can be computed from l and B) then the LLL-algorithm will either find $u(X)$ or show that no such polynomial satisfies the specified bounds. It is shown in [12] that the time to carry out this computation is $O(l^{12} + l^9(\log B)^3)$. Various modifications have been proposed (see, for example, [7] and [8]), but in practice the running times of programs which implement the LLL-algorithm remain highly dependent on the degree: $l = 10$ is certainly feasible, but $l = 20$ might not be.

Suppose now that the minimal polynomial $g(X)$ (of degree $m = n/d$) for δ has been computed. It remains to compute $w(X) \in \mathbb{Q}[X]$ such that $\delta = w(\alpha)$ for some $\alpha \in \Delta$. One approach to this is an application of the lemma at the beginning of the paper. This might be the easiest approach for small degrees, but the factorization of the polynomial $h(X)$ described there is a serious bottle-neck for even moderate values of n and m. A modification of this approach is to compute the polynomial $k(X)$ of degree

https://doi.org/10.1017/S1446788700032432 Published online by Cambridge University Press

n described in the lemma directly as the minimal polynomial of $\alpha\delta$ using the LLL-algorithm and a p-adic approximation to $\alpha\delta$; but again the efficiency is severely limited by the degree n. The following approach appears to be better except when the degrees are quite small.

Suppose $w(X) \in \mathbb{Q}[X]$ has degree $< n$ such that $\delta = w(\alpha)$ where δ is the product of elements in some block Δ for G, and $\alpha \in \Delta$. Then transitivity of the Galois group G shows that for each root $\alpha' \in \Omega$, we have $w(\alpha') = \delta'$ where δ' is the product of the elements in the block Δ' conjugate to Δ with $\alpha' \in \Delta'$; so w is the interpolating polynomial for the pairs (α', δ') $(\alpha' \in \Omega)$. Fix a prime $p \nmid \operatorname{disc}(f)$ and $p \nmid \operatorname{disc}(g)$ (this need not be the same prime as was used in computing $g(X)$), and compute the roots of $f(X) \bmod p$ and $g(X) \bmod p$ in some finite splitting field over the field $\mathbb{F}_p$ of p elements. Determine a partition of the set of roots of $f(X) \bmod p$ into subsets $\Gamma_1, \ldots, \Gamma_m$ of size d such that the product of the roots in each Γ_i gives a root γ_i of $g(X) \bmod p$ (we may have to consider several possible partitions of this form). Now construct an interpolating polynomial $w_0(X) \in \mathbb{Z}[X]$ of degree $< n$ such that $w_0(\beta) = \gamma_i$ for all $\beta \in \Gamma_i$. Then $g(w_0(X)) \equiv 0 \mod (f(X), p)$ and a natural modification of Newton's method in the ring $\mathbb{Z}_p[X]/(f(X))$ (see Appendix B) allows us to compute (to arbitrarily high accuracy in $\mathbb{Z}_p$) the polynomial $w(X) \in \mathbb{Z}_p[X]$ such that

$$g(w(X)) \equiv 0 \pmod{f(X)} \quad \text{and} \quad w(X) \equiv w_0(X) \pmod{p}.$$

Finally, the technique described, for example, in [5] shows how to recover from a mod-p^k approximation of the coefficients of $w(X)$ the rational values of these coefficients.

We now summarize the overall strategy of the steps involved in going from a (putative) block Δ and a p-adic approximation for the product δ of its elements to the computation of $g(X)$ and $w(X)$. (In step (a) we are assuming that $g(X)$ is separable; see Appendix A.)

(a) Use the LLL-algorithm to compute the minimal polynomial $g(X)$ of δ. The degree of $g(X)$ is m and its coefficients are easily bounded in terms of $f(X)$ because the roots of $g(X)$ are products of d roots of $f(X)$. If the LLL-algorithm fails to construct $g(X)$, then Δ is not a block.

(b) Assuming $g(X)$ has been constructed in (a), choose a prime $p \nmid \operatorname{disc}(f)\operatorname{disc}(g)$, and compute the roots of $f(X) \bmod p$ and $g(X) \bmod p$ in a finite extension of $\mathbb{F}_p$. Then partition the set of roots of the former into subsets of size d whose products give the roots of the latter. If such a partition does not exist, then Δ is not a block. If there is more than one partition of this form then the remaining steps must be carried out for each of these different partitions.

https://doi.org/10.1017/S1446788700032432 Published online by Cambridge University Press

(c) Find $w_0(X) \in \mathbb{Z}[X]$ of degree at most $n-1$ as the interpolating polynomial from the set of roots of $f(X) \bmod p$ to the set of roots of $g(X) \bmod p$ according to the partition obtained in (b).

(d) Apply Newton's method to compute $w^*(X) \in \mathbb{Z}[X]$ such that $g(w^*(X)) \equiv 0 \pmod{f(X), p^k}$ and $w^*(X) \equiv w_0(X) \pmod{p}$ for sufficiently large k, and then use the continued fraction technique described in [5] to compute $w(X) \in \mathbb{Q}[X]$ such that $w(X) \equiv w^*(X) \pmod{p^k}$. An upper bound of the sizes of the numerators and denominators of the coefficients of $w(X)$ is given in Appendix C, and this can be used to determine an upper bound on the order k to which the computations must be taken. However, in general we may expect much smaller values of k to be satisfactory.

(e) Finally, check that $g(w(X)) \equiv 0 \pmod{f(X)}$. This check succeeds if and only if Δ is a block. In the latter case, if we put $\delta = w(\alpha)$, then $\mathbb{Q}(\delta)$ is a subfield of $\mathbb{Q}(\alpha)$ of degree m over $\mathbb{Q}$ and $g(X)$ the minimal polynomial of δ over $\mathbb{Q}$.

6. An example

The method described above sounds more complicated than it is in practice. The following example should clarify some of the steps involved. All calculations were carried out with simple APL programs on a microcomputer. Polynomials are represented below by listing their coefficients in decreasing order of degree.

The polynomial

$$f = (1\ 0\ 0\ 6\ 4\ 0\ 8\ \ -4\ \ -12\ 8\ 0\ \ -8\ 8)$$

is irreducible over $\mathbb{Z}$ and has a root $\lambda\mu$ where λ and μ are roots of $q_1 = (1\ 0\ 0\ 2\ 2)$ and $q_2 = (1\ 0\ \ -1\ \ -1)$, respectively. Let α denote a root of $f(X)$. We shall compute a generator for a subfield of $\mathbb{Q}(\alpha)$ of degree 4 over $\mathbb{Q}$.

Using standard algorithms [13] to compute the factors of $f \bmod p$ for various primes p, we obtain

p	3	5	7	11	13	⋯
cycle(p)	12^1	$1^1 2^1 3^1 6^1$	$1^2 2^5$	$1^2 2^5$	3^4	⋯

Similar factorizations also show that 2, 23 and 37 divide $\mathrm{disc}(f)$ because in these cases $f \bmod p$ is not separable. Actually $\mathrm{disc}(f) = 2^{36} 23^4 37^2 101^3$, but we shall not use this.

We now look for a block of size $3\ (= 12/4)$. Taking $p = 5$, we can see that if there are blocks of size 3, then one must consist of the roots of the linear

https://doi.org/10.1017/S1446788700032432 Published online by Cambridge University Press

and quadratic factors of $f(X)$ over $\mathbb{Z}_5$. In particular, this shows that there is at most one block of size 3 which contains the root of the linear factor, and so there is at most one subfield of $\mathbb{Q}(\alpha)$ which has degree 4 over $\mathbb{Q}$. The two polynomials (1 3) and (1 2 3) are irreducible factors of $f(X) \pmod 5$. When we apply Hensel lifting to the product of these two factors we find that

$$f \equiv (1\ 3)(1\ 2\ 3)\cdots \pmod 5$$

lifts to

$$f \equiv (1\ 0\ 3156734\ 5497064)\cdots \pmod{5^{10}}.$$

The product of the roots of the linear and quadratic factors of $f(X)$ in $\mathbb{Z}_5[X]$ is therefore

$$\delta \equiv -5497064 \pmod{5^{10}}.$$

Using this approximation over $\mathbb{Z}_5$ in the LLL-algorithm gives (tentatively) the minimal polynomial for δ as

$$g = (1\ 6\ 12\ 8\ 8).$$

The process is tentative at this stage because it is based on the so-far unproved assumption that there is a block of size 3. It is easily verified that $g(X)$ is irreducible over $\mathbb{Q}$, so it remains to find a polynomial $w(X) \in \mathbb{Q}[X]$ of degree at most 11 such that $g(w(X)) \equiv 0 \pmod{f(X)}$.

For convenience, we change to the ring $\mathbb{Z}_7$ to carry out the remaining calculations. Factoring into irreducibles, we have

$$f \equiv (1\ 1)(1\ 3)(1\ 0\ 1)(1\ 3\ 6)(1\ 4\ 1)(1\ 4\ 5)(1\ 6\ 6) \pmod 7$$

and

$$g \equiv (1\ 1)(1\ 6)(1\ 6\ 6) \pmod 7.$$

Note that $7 \nmid \operatorname{disc}(f)\operatorname{disc}(g)$ because $f(X) \bmod 7$ and $g(X) \bmod 7$ clearly have distinct roots.

Let i be an element in an extension field of $\mathbb{F}_7$ with $i^2 = -1$. Then working modulo 7 we find that the roots of f can be grouped in sets of 3 in exactly one way so that the corresponding products give the roots of $g \pmod 7$, namely

$$6 \equiv 4(-2+i)(-2-i), \quad 1 \equiv 6(-3+2i)(-3-2i)$$

and

$$-3 \pm 2i \equiv \mp i(2 \pm 3i)(-2 \mp 2i).$$

We now interpolate to get a polynomial $w_0(X) \in \mathbb{Z}[X]$ such that $w_0(\alpha_i) \equiv \delta_j \pmod 7$ whenever α_i is a root of $f(X)$ and δ_j is the root of $g(X)$ in which α_i appears as a factor $\pmod 7$. This gives

$$w_0 \equiv (5\ 2\ 4\ 2\ 5\ 5\ 2\ 6\ 1\ 0\ 0\ 3) \pmod 7.$$

https://doi.org/10.1017/S1446788700032432 Published online by Cambridge University Press

Since $g(w_0(X)) \equiv 0 \pmod{f(X), 7}$, Newton's method (see Appendix B) can be applied to obtain a better approximation

$$w^* = (4362552 \cdots 934832) \pmod{7^8}$$

such that $w^* \equiv w_0 \pmod 7$ and $g(w^*(X)) \equiv 0 \pmod{f(X), 7^8}$.

Finally, using the technique described in [5], we obtain a rational approximation $w \equiv w^* \pmod{7^8}$, namely,

$$w = \frac{1}{74}(-8\ 15\ -5\ -34\ 41\ 48\ -6\ 108\ 60\ -84\ 28\ -44).$$

Since a direct check shows that $g(w(X)) \equiv 0 \pmod{f(X)}$, therefore $\delta = w(\alpha)$ is an element of degree 4 in $\mathbb{Q}(\alpha)$ with minimal polynomial $g(X)$, and the computation is complete. As we observed above, $\mathbb{Q}(\delta)$ is the only subfield of $\mathbb{Q}(\alpha)$ of degree 4 over $\mathbb{Q}$.

Appendix A. Products of k-subsets of roots

In Section 3 we assumed that the products δ_t $(t = 1, \ldots, m)$ of elements in a set of conjugate blocks for G were distinct. Occasionally this assumption may not hold, and then $\mathbb{Q}(\delta)$ is not equal to $\mathrm{Fix}(G_{\{\Delta\}})$. We shall detect this anomalous situation when we discover that the minimal polynomial $g(X)$ of δ has degree $< m$. The problem can be corrected by replacing $f(X)$ by $f(X - r)$ (or equivalently the roots α_i by $\alpha_i + r$) for suitable (almost any) integer r. To see why this is so, define

$$\varphi_t(X) := \prod\{X + \alpha_i \mid \alpha_i \in \Delta\} \quad \text{for } t = 1, \ldots, m.$$

These polynomials are all different since they have different roots. Thus there are at most $\binom{m}{2}d < \frac{1}{2}mn$ values of r such that for some s and t with $s \neq t$ we have $\varphi_s(r) = \varphi_t(r)$. Any other value of $r \in \mathbb{Z}$ has the required property.

Similar arguments apply in other computations where we need to have distinct products of roots of various polynomials. See also [23].

Appendix B. Newton's method

In Section 5 we refer to the use of Newton's method in $\mathbb{Z}_p[X]/(f(X))$. This requires a little bit of explanation because Newton's method is usually used over a field (compare with [11, pages 308–311]). The process in the present situation is as follows. Assume that $p > 2$ and that as an initial approximation we have $w_0(X) \in \mathbb{Z}[X]$ of degree at most $n - 1$ such that

$$g(w_0(X)) \equiv 0 \pmod{f(X), p}.$$

https://doi.org/10.1017/S1446788700032432 Published online by Cambridge University Press

We are also assuming that $p \nmid \mathrm{disc}(g)$ and so $g(X) \bmod p$ is separable; therefore $g'(w_0(X))$ is relatively prime to $f(X)$ modulo p. Thus we can use the Euclidean algorithm to compute $h_0(X) \in \mathbb{Z}[X]$ of degree at most $n-1$ such that

$$h_0(X)g'(w_0(X)) \equiv 1 \pmod{f(X), p}.$$

The general step is to go from

$$g(w_k(X)) \equiv 0 \pmod{f(X), p^{2^k}} \tag{4}$$

and

$$h_k(X)g'(w_k(X)) \equiv 1 \pmod{f(X), p^{2^k}} \tag{5}$$

(where $w_k(X)$ and $h_k(X)$ are integer polynomials of degree at most $n-1$) to the corresponding relations with $k+1$ in place of k ($k = 0, 1, \ldots$). The only tricky point is that it is not quite straightforward to compute $h_k(X)$ ($k \geq 1$) using the Euclidean algorithm because for $k > 0$ we are working over a ring $\mathbb{Z}/(p^{2^k})$ with divisors of 0. This problem is avoided by the double iteration given by

$$w_{k+1}(X) \equiv w_k(X) - h_k(X)g(w_k(X)) \pmod{f(X), p^{2^{k+1}}}$$

and

$$h_{k+1}(X) \equiv h_k(X)\{2 - h_k(X)g'(w_{k+1}(X))\} \pmod{f(X), p^{2^{k+1}}}.$$

A straightforward calculation shows that

$$w_{k+1}(X) \equiv w_k(X) \quad \text{and} \quad h_{k+1}(X) \equiv h_k(X) \pmod{p^{2^k}}$$

and that (4) and (5) remain invariant under the substitution of $k+1$ for k (it is here that we need $p > 2$).

Finally, the sequence $\{w_k(X)\}$ is a Cauchy sequence in the p-adic metric and so has a p-adic limit $w(X) \in \mathbb{Z}_p[X]$ such that $g(w(X)) \equiv 0 \pmod{f(X)}$ and $w(X) \equiv w_0(X) \pmod{p}$. Because $f(X) \bmod p$ and $g(X) \bmod p$ are separable, there last two conditions determine $w(X)$ uniquely. Indeed, if we also have $v(x) \in \mathbb{Z}_p[X]$ with degree at most $n-1$ such that $g(v(X)) \equiv 0 \pmod{f(X)}$ and $v(X) \equiv w_0(X) \pmod{p}$, then for each root $\alpha_i \in \Omega$, $v(\alpha_i)$ and $w(\alpha_i)$ are roots of $g(X)$ with $v(\alpha_i) \equiv w(\alpha_i) \pmod{p}$. Thus $v(\alpha_i) = w(\alpha_i)$ for each i because $g(X) \bmod p$ is separable, and so $v(X) = w(X)$ because $f(X)$ is separable. In particular, if there is a set of conjugate blocks $\Delta_1, \ldots, \Delta_m$ for G acting on Ω which map onto the given set of subsets $\Gamma_1, \ldots, \Gamma_m$ (see Section 5) under the $\bmod p$ mapping from $\mathbb{Z}_p[\Omega]$ onto the splitting field of $f(X) \bmod p$, then $w(X) \in \mathbb{Q}[X]$.

https://doi.org/10.1017/S1446788700032432 Published online by Cambridge University Press

For further examples of applications of Newton's method to algebraic problems see [14] and [26].

Appendix C. Bounds on the coefficients of $w(X)$

Suppose that the discriminant $\mathrm{disc}(f) = D_1^2 D_2$ where D_1 and D_2 are integers and D_2 is squarefree. Then every algebraic integer in $\mathbb{Q}(\alpha)$ lies in $D_1^{-1}\mathbb{Z}[\alpha]$ [17, page 58]. Thus, if $w(X) \in \mathbb{Q}[X]$ satisfies $g(w(\alpha)) = 0$, then $D_1 w(X)$ has the form $u_0 + u_1 X + \cdots u_{n-1} X^{n-1} \in \mathbb{Z}[X]$. This gives

$$u_0 + u_1\alpha_i + \cdots + u_{n-1}\alpha_i^{n-1} = D_1\delta_{t(i)} \qquad (i = 1, \ldots, n)$$

where $\alpha_i \in \Delta_{t(i)}$. If we define A to be the $n \times n$ matrix $[\alpha_j^{i-1}]$, and use the fact that $(\det A)^2 = D_1^2 D_2$, we can solve these equations to obtain

$$(u_0, u_1, \ldots, u_{n-1}) = D_1(\delta_{t(1)}, \delta_{t(2)}, \ldots, \delta_{t(n)})A^{-1}.$$

However $D_1 A^{-1} = \varepsilon |D_2|^{-1/2} \mathrm{Adj}(A)$ where $|\varepsilon| = 1$. Thus, if $|\alpha_i| \le c_0$ for all i, then Hadamard's determinant inequality gives the bound

$$|u_i| \le |D_2|^{-1/2} n^{(n-1)/2} c_0^{n(n-1)/2+d}.$$

It seems likely that these bounds will usually grossly overestimate the size of the numerators and denominators of the coefficients of $w(X)$. For further results on this problem see [1] and [3].

References

[1] J. A. Abbott, K. J. Bradford and J. H. Davenport, 'Factorization of polynomials', *Trends in Computer Algebra*, Lecture Notes Comput. Sci. 296, (Springer, New York, 1988).

[2] Z. I. Borevich and I. R. Shafarevich, *Number Theory*, (Academic Press, New York, 1966).

[3] R. J. Bradford, *On the Computation of Integral Bases and Defects of Integrity*, (Ph.D. thesis), Bath Univ., Bath, 1988.

[4] G. Butler and J. McKay, 'The transitive groups of degree up to 11', *Comm. Algebra* **11** (1983), 863–911.

[5] J. D. Dixon, 'Exact solutions of linear equations using p-adic expansions', *Numer. Math.* **40** (1982), 137–141.

[6] D. W. Erbach, J. Fischer and J. McKay, 'Polynomials with PSL(2, 7) as Galois group', *J. Number Theory* **11** (1979), 69–75.

[7] U. Fincke and M. Pohst, 'Improved methods for calculating vectors of short length in a lattice, including a complexity analysis', *Math. Comp.* **44** (1985), 463–471.

https://doi.org/10.1017/S1446788700032432 Published online by Cambridge University Press

[8] E. Kaltofen, 'On the complexity of finding short vectors in integer lattices', *Computer Algebra*, Lecture Notes Comput. Sci. 162, (Springer, New York, 1983).
[9] I. Kaplansky, *Fields and Rings*, (Univ. Chicago Press, Chicago, 1969).
[10] J. C. Lagarias, H. L. Montgomery and A. M. Odlyzko, 'A bound for the least prime ideal in the Chebotarev Density Theorem', *Invent. Math.* **54** (1979), 271–296.
[11] S. Lang, *Algebra*, (Addision-Wesley, Reading, Mass., 1965).
[12] A. K. Lenstra, H. W. Lenstra Jr. and L. Lovasz, 'Factoring polynomials with rational coefficients', *Math. Ann.* **261** (1982), 513–534.
[13] R. Lidl and H. Niederreiter, *Introduction to Finite Fields and Their Applications*, (Cambridge Univ. Press, 1986).
[14] J. Lipson, 'Newton's method: a great algebraic algorithm', *Proc.* 1976 *ACM Symposium on Symbolic and Algebraic Computing* (R. D. Jenks, ed.), A.C.M., 1976.
[15] J. McKay, 'Some remarks on computing Galois groups', *SIAM J. Comput.* **8** (1979), 344–347.
[16] J. McKay and E. Regener, 'Actions of permutation groups on r-sets', *Comm. Algebra* **13** (1985), 619–630.
[17] W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers*, (Polish Sci. Publ., Warsaw, 1974).
[18] G. F. Royle, 'The transitive groups of degree twelve', *J. Symbol. Comput.* **4** (1987), 255–268.
[19] J.-P. Serre, 'Quelques applications du théorème de densité de Chebotarev', Publ. Math. I.H.E.S., Bures-sur-Yvette, 1981.
[20] R. P. Stauduhar, 'The determination of Galois groups', *Math. Comp.* **27** (1973), 981–996.
[21] L. Soicher, *The Computation of Galois Groups*, (Master's thesis), Concordia Univ., Montreal, 1981.
[22] L. Soicher and J. McKay, 'Computing Galois groups over the rationals', *J. Number Theory* **20** (1985), 273–281.
[23] B. Trager, 'Algebraic factoring and rational function integration', *Proc.* 1976 *ACM Symposium on Symbolic and Algebraic Computing* (R. D. Jenks, ed.), A.C.M., 1976.
[24] N. Tschebotareff, 'Die Bestimmung der Dichtigkeit einer Menge von Primzahlen, welche zu einer gegebenen Substitutionsklasse gehören', *Math. Ann.* **95** (1926), 191–228.
[25] B. L. van der Waerden, *Modern Algebra*, (Ungar, New York, 1948).
[26] D. Y. Y. Yun, 'Algebraic algorithms using p-adic constructions', *Proc.* 1976 *ACM Symposium on Symbolic and Algebraic Computing* (R. D. Jenks, ed.), A.C.M., 1976.
[27] H. Zassenhaus, 'On Hensel factorization, I', *J. Number Theory* **1** (1969), 291–311.

Department of Mathematics and Statistics
Carleton University
Ottawa K1S 5B6
Canada

https://doi.org/10.1017/S1446788700032432 Published online by Cambridge University Press