ALGORITHMIC GALOIS THEORY

Hendrik W. Lenstra jr.

Mathematisch Instituut,
Universiteit Leiden

Department of Mathematics,
University of California, Berkeley

$K =$ field of characteristic zero,

$\Omega =$ algebraically closed
field containing K.

$$\sqrt{K^*} = \{\alpha \in \Omega^* : \exists n \in \mathbf{Z}_{>0} : \alpha^n \in K^*\}$$

$$K \subset K(\sqrt{K^*})$$

$K =$ (algebraic) number field
$=$ *finite* extension of $\mathbf{Q}$.

$$K = K_0 \subset K_1 \subset K_2 \subset \ldots$$
$$K_{i+1} = K_i(\sqrt{K_i^*})$$
$$K_\infty = \bigcup_{i \geq 0} K_i$$

K_∞ is the *solvable*
closure of K inside Ω.

Its elements can be written
as *nested radicals* over K.

The *nesting depth* $d_K(\alpha)$
of $\alpha \in K_\infty$ over K is the
smallest i with $\alpha \in K_i$.

Example:
$0 < d_{\mathbf{Q}}\big(\sqrt{1+\sqrt{2}}\big) \leq 2.$

Exercise:
compute $d_{\mathbf{Q}}(\sqrt{1+\sqrt{2}})$.

For any (possibly infinite) Galois extension $K \subset L$, the following three algorithmic questions are equivalent:

- decide whether a given finite extension $K \subset M$ satisfies $M \subset L$,
- for a given finite extension $K \subset M$, compute the subfield $L \cap M$ of M,
- factor a given polynomial in $K[X]$ into irreducible factors in $L[X]$.

Theorem (Carl Cotner, 1995)**.**
There is an algorithm that,
given algebraic number fields
$K \subset M$ *and* $\alpha \in M$*,*
decides whether $\alpha \in K_\infty$*,*
and if so computes $d_K(\alpha)$*.*

Equivalently:

Theorem. *There is an*
algorithm that, given algebraic
number fields $K \subset M$*, computes*
all subfields $K_0 \cap M$*,* $K_1 \cap M$*,*
$K_2 \cap M$*, ... of* M*.*

Can one do this
in polynomial time?

Polynomial time algorithms

An algorithm runs in *polynomial time* if there is a constant c, such that for every input, the run time of the algorithm is at most $(2 + \text{length of input})^c$.

Specifying number fields

A number field is numerically specified by a system (a_{ijk}) of n^3 rational numbers a_{ijk}.

The additive group of the field is $\mathbf{Q}^n$, and the multiplication is given by $(r_i)_{i=1}^n \cdot (s_j)_{j=1}^n = \\ = \left(\sum_{i,j} a_{ijk} r_i s_j\right)_{k=1}^n$.

Elements of a number field are specified as vectors of rational numbers.

Field homomorphisms (such as embeddings and automorphisms) are specified as matrices over $\mathbf{Q}$.

There are polynomial time algorithms for:

- deciding whether a given system $(a_{ijk}) \in \mathbf{Q}^{n^3}$ specifies an algebraic number field,
- finding all homomorphisms between two given number fields,
- finding a primitive element for a given extension $K \subset M$,
- determining the irreducible polynomial of a given element in a given extension $K \subset M$,
- intersecting subfields,
- factoring polynomials.

Fact. *There is no polynomial time algorithm for computing the Galois closure of a given field extension $K \subset M$.*

Proof. Take $K = \mathbf{Q}$ and $M = \mathbf{Q}(\alpha)$, where

$$\alpha^n - \alpha - 1 = 0.$$

Length of input: $O(n^c)$.

The degree of the Galois closure equals $n!$, so:

run time $\geq$ length of output

$$\geq n! \qquad \blacksquare$$

What about Galois *groups*?

Main techniques for determining Galois groups:

- reduction modulo primes

Not much can be proved about the run time or about the correctness of such methods.

- results on permutation groups.

Theorem. *There is an algorithm that for some c does the following: given an extension $K \subset M$ of number fields, and $b \in \mathbf{Z}_{>0}$, it decides in time at most* $(b + \text{length of input})^c$ *whether the Galois group G of the normal closure F of $K \subset M$ satisfies $\#G \leq b$, and if so computes F and G.*

Corollary. *For each n there is a polynomial time algorithm that computes the Galois group of the Galois closure of a given extension $K \subset M$ of degree n.*

Open problem. Given finite extensions $K \subset M$, $K \subset M'$, compute in polynomial time the intersection of M' with the Galois closure of M.

Theorem. *There is a polynomial time algorithm that, given an extension $K \subset M$ of number fields, decides whether the Galois group of its Galois closure equals the full symmetric group $S_{[M:K]}$. Same for the alternating group $A_{[M:K]}$.*

The proof uses that for $n \geq 8$, the only sixfold transitive permutation groups of degree n are S_n and A_n.

$K^{\mathrm{ab}} = $ maximal abelian extension
of K inside Ω,
$K_\infty = $ solvable closure
of K inside Ω.

Theorem. *There is a polynomial time algorithm for deciding whether a given extension $K \subset M$ of number fields satisfies $M \subset K^{\mathrm{ab}}$.*

Theorem (Susan Landau & Gary Miller, 1985)**.** *There is a polynomial time algorithm for deciding whether a given extension $K \subset M$ of number fields satisfies $M \subset K_\infty$.*

For any (possibly infinite) Galois extension $K \subset L$, the following three algorithmic questions are equivalent:

- decide whether a given finite extension $K \subset M$ satisfies $M \subset L$,
- for a given finite extension $K \subset M$, compute the subfield $L \cap M$ of M,
- factor a given polynomial in $K[X]$ into irreducible factors in $L[X]$.

The last two are equivalent under polynomial time reductions.

Open problem: is there a polynomial time reduction of the second to the first?

We can decide whether $M \subset K^{\mathrm{ab}}$ and whether $M \subset K_\infty$ in polynomial time.

Can we compute $K^{\mathrm{ab}} \cap M$ and $K_\infty \cap M$ in polynomial time?

Equivalently, can one factor in $K^{\mathrm{ab}}[X]$ and $K_\infty[X]$ in polynomial time?

$\mu = \{\zeta \in \Omega^* : \zeta^n = 1$
for some positive integer $n\}$,
$K(\mu) =$ maximal cyclotomic
extension of K inside Ω,
$K^{\mathrm{ab}} =$ maximal abelian extension
of K inside Ω,
$K_\infty =$ solvable closure
of K inside Ω.

Theorem. *There are polynomial time algorithms that for a given extension $K \subset M$ of number fields compute the subfields $K(\mu) \cap M$, $K^{\mathrm{ab}} \cap M$ and $K_\infty \cap M$ of M.*

Computing $K^{\mathrm{ab}} \cap M$.

Step 1: compute the largest Galois extension E of K inside M.

1a: write $M = K(\alpha)$ and factor the irreducible polynomial of α over K in $M[X]$.

1b: if there is an irreducible factor g of degree > 1, form $M(\beta) = M[X]/(g)$, replace $M = K(\alpha)$ by $K(\alpha) \cap K(\beta)$, and start again at **1a**.

1c: otherwise $E = M$.

Step 2: compute $G = \mathrm{Aut}_K E$ and $H = [G, G]$; now $K^{\mathrm{ab}} \cap M$ equals $\{\gamma \in E : \forall \sigma \in H : \sigma\gamma = \gamma\}$.

Computing $K(\mu) \cap M$:

Kronecker-Weber: $\mathbf{Q}^{\mathrm{ab}} = \mathbf{Q}(\mu)$,

$K(\mu) \cap M = K \cdot \big(\mathbf{Q}^{\mathrm{ab}} \cap M\big)$.

Computing $K_\infty \cap M$ is done
using fields $K(\alpha, \beta, \gamma, \delta)$,
where $M = K(\alpha)$ and β, γ, δ
are conjugates of α over K.
It uses the following result.

Theorem (Ákos Seress, 1996)**.**
For each primitive solvable
permutation group G of a finite
set X there is a subset $Y \subset X$
with $\#Y \leq 4$ such that each
$\sigma \in G$, $\sigma \neq 1$, moves at least
one element of Y.

Conclusion. For every number field K we can, in polynomial time, factor polynomials into irreducible factors in each of the rings $K(\mu)[X]$, $K^{\mathrm{ab}}[X]$, $K_\infty[X]$.

Problem. Do the same for the rings $K_i[X]$, $i \geq 0$, where $K_0 = K$, $K_{i+1} = K_i(\sqrt{K_i^*})$, so that *denesting of radicals* will become feasible.

First result in the right direction:

Theorem. *There is a polynomial time algorithm that, given an extension $K \subset M$ of number fields, computes a set of representatives for the torsion subgroup of M^*/K^*.*