Construction of non-solvable polynomials over $\mathbb{Q}$

Johan Bosman

Joint work with Bas Edixhoven

DIAMANT/EIDMA Symposium

November/December 2006, Vught

NWO

Netherlands Organisation for Scientific Research

What is a (non-)solvable polynomial?

Motivating examples

The quadratic polynomial

$$ax^2 + bx + c$$

has zeroes

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

and (Cardano, 1545) the cubic polynomial

$$ax^3 + bx^2 + cx + d$$

has zeroes

$$x = \sqrt[3]{C + \sqrt{D}} + \sqrt[3]{C - \sqrt{D}} - \frac{b}{3a}$$

where

$$C = \frac{-b^3}{27a^3} + \frac{bc}{6a^2} - \frac{d}{2a}$$

and

$$D = C^2 + \left(\frac{c}{3a} - \frac{b^2}{9a^2}\right)^3 .$$

What is a (non-)solvable polynomial?

We see that the expressions

$$\frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

and

$$\sqrt[3]{C + \sqrt{D}} + \sqrt[3]{C - \sqrt{D}} - \frac{b}{3a}$$

are built up from the operations $+$, $-$, $\cdot$, $/$ and $\sqrt[n]{\cdot}$.

Question.
Can the zeroes of every polynomial be expressed in terms of $+$, $-$, $\cdot$, $/$ and $\sqrt[n]{\cdot}$?

Answer.
For quartic polynomials this is still possible (Ferrari, 1540) but from degree 5 there are polynomials for which this is not the case (Abel, 1826).

Definition.
A polynomial is called *solvable* if the zeroes can be expressed in terms of $+$, $-$, $\cdot$, $/$ and $\sqrt[n]{\cdot}$ and *non-solvable* if this cannot be done.

Galois theory

From polynomials to groups

In 1832, Galois found a better proof of the nonsolvability. He attached a group to each polynomial P, obtaining more refined information about P than simply answering the solvability question with ”yes” or ”no”.

How does it work?

Consider

$$P(x) = a_n x^n + \cdots + a_0 = a_n(x - x_1)\cdots(x - x_n),$$

where $x_1, \ldots, x_n$ are the zeroes of P, supposed to be *distinct*. There can be many relations between the zeroes, e.g.

$$x_1 + \cdots + x_n = \frac{-a_{n-1}}{a_n}, \quad x_1 \cdots x_n = \frac{(-1)^n a_0}{a_n},$$

Definition.
The group of all permutations of the zeroes of P that preserve all relations between these zeroes is called the *Galois group* of P and denoted by $\mathsf{Gal}(P)$.

Galois theory

From polynomials to groups

Definition.
The group of all permutations of the zeroes of P that preserve all relations between these zeroes is called the *Galois group* of P and denoted by $\mathsf{Gal}(P)$.

'Most' P's have only relations deduceable from symmetric ones, so in that case $\mathsf{Gal}(P) \cong S_n$ consists of all permutations of the roots, but there are exceptions.

Example.
$P(x) = x^4 + x^3 + x^2 + x + 1 = (x - x_1) \cdots (x - x_4)$
where $x_k = \zeta_5^k$. There are relations

$$x_k = x_1^k.$$

So for each $\sigma \in \mathsf{Gal}(P)$ we have

$$\sigma(x_k) = \sigma(x_1)^k.$$

So σ is determined by what it does on x_1 and we see that $\mathsf{Gal}(P)$ consists of just 4 elements instead of $4! = 24$, the number of all permutations.

Galois theory

Solvability translated to groups

Whether P is solvable can be translated to properties of $G = \mathsf{Gal}(P)$.

Make a sequence $G_1 \supset G_2 \supset \cdots$ of groups as follows.

$$G_1 := G, \quad G_{n+1} := [G_n, G_n]$$

where

$$[G_n, G_n] = \left\langle xyx^{-1}y^{-1} : x, y \in G_n \right\rangle.$$

Then P is solvable iff there is an n with $G_n = \{e\}$.

Definition.
A finite group is called *solvable* if in the above sequence $(G_n)_n$ attached to it there is an n with $G_n = \{e\}$ and *non-solvable* otherwise.

All permutation groups acting on at most 4 elements are solvable. For $n \geq 5$ the group S_n of all permutations of n elements is non-solvable and usually many subgroups of S_n are non-solvable as well.

Inverse Galois theory

From groups to polynomials

Question.
Given a group G, does there exist a polynomial $P \in \mathbb{Q}[x]$ with $\mathsf{Gal}(P) \cong G$?

Usually one restricts attention to *irreducible* polynomials. This is equivalent to G being *transitive*.

Question.
Given a transitive permutation group G, does there exist a polynomial $P \in \mathbb{Q}[x]$ with $\mathsf{Gal}(P) \cong G$?

One can often use higher arguments to show the *existence* of such a polynomial but then it is still not clear how to *compute* it.

Question.
Given a transitive permutation group G, can one explicitly compute a polynomial $P \in \mathbb{Q}[x]$ with $\mathsf{Gal}(P)$ isomorphic to G?

Inverse Galois theory

From groups to polynomials

Question.
Given a transitive permutation group G, does there exist a polynomial $P \in \mathbb{Q}[x]$ with $\mathsf{Gal}(P) \cong G$?

Highly unsolved problem. At the moment, people conjecture it is possible for every G.

Partial answer 1 (Shafarevich, 1954).
For each solvable group there exists a polynomial!

So we concentrate on the non-solvable groups.

Partial answer 2.
Families of polynomials exist for certain types of non-solvable groups. For example S_n, A_n, many projective special linear groups, all but one of the sporadic simple groups and more.

Inverse Galois theory

Explicit constructions

Question.
Given a transitive permutation group G, can one explicitly compute a polynomial $P \in \mathbb{Q}[x]$ with $\mathsf{Gal}(P)$ isomorphic to G?

Partial answer (Klüners & Malle, 2000).
For many types of groups families of polynomials can be computed. All transitive groups of degree $\leq$ 15 occur among these types. Later they did all degree 16 groups as well.

Question (Klüners).
Can you compute a polynomial P of degree 17 with $\mathsf{Gal}(P) \cong \mathsf{SL}_2(\mathbb{F}_{16})$?

Note that indeed, $\mathsf{SL}_2(\mathbb{F}_{16})$ is a permutation group of degree 17 by letting it act on $\mathbb{P}^1(\mathbb{F}_{16}) = \mathbb{F}_{16} \cup \{\infty\}$:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}(x) = \frac{ax+b}{cx+d}.$$

Inverse Galois theory

Explicit constructions

Question (Klüners).
Can you compute a polynomial P of degree 17 with $\mathrm{Gal}(P) \cong \mathrm{SL}_2(\mathbb{F}_{16})$?

Answer (B.).
Yes, here is one:

$$\begin{aligned} &x^{17} - 5x^{16} + 12x^{15} - 28x^{14} + 72x^{13} \\ &- 132x^{12} + 116x^{11} - 74x^{9} + 90x^{8} - 28x^{7} \\ &- 12x^{6} + 24x^{5} - 12x^{4} - 4x^{3} - 3x - 1. \end{aligned}$$

The construction uses *modular forms* and their *Galois representations*.

Galois representations

There is a big group called $\mathsf{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ that encodes all Galois groups of polynomials in $\mathbb{Q}[x]$. It has a natural topology. A finite group is $\mathsf{Gal}(P)$ for some P if it occurs as a homomorphic image of $\mathsf{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

Using modular forms, one can make continuous homomorphisms

$$\rho : \mathsf{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathsf{GL}_2(\mathbb{F}_q),$$

for finite fields $\mathbb{F}_q$.

To show existence of a polynomial P with $\mathsf{Gal}(P) \cong \mathsf{SL}_2(\mathbb{F}_{16})$, we have to find a modular form giving rise to

$$\rho : \mathsf{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathsf{GL}_2(\mathbb{F}_{16})$$

with image equal to $\mathsf{SL}_2(\mathbb{F}_{16}) \subset \mathsf{GL}_2(\mathbb{F}_{16})$. With a computer search one can find such modular forms indeed.

Galois representations

Explicit calculations

Edixhoven, Couveignes and de Jong showed the existence of a polynomial time algorithm for calculating these modular Galois representations.

- It involves symbolic computations as well as numerical calculations.

- The computations are related to point counting on modular curves. Interesting in cryptography and coding theory.

Galois representations

Limitations of the algorithm

- The algorithm, though polynomial time, is in practise very slow.

- Many implementation tricks are needed to make it work practically.

- Already in simple cases, numerical calculations in hundreds of decimals are required.

- The output is huge. One needs to do reductions afterwards, using for instance LLL.

- The output needs to be verified afterwards.