Galois theory and the Abel-Ruffini theorem

Bas Edixhoven

November 4, 2013, Yogyakarta, UGM

A lecture of two times 45 minutes. Audience: bachelor, master and PhD students, plus maybe some lecturers.

This text was very quickly written on November 3. Apologies for typesetting, style, etc.

1 Goal of the lectures

The goal of these two lectures is to show that for each $n \geq 5$ there is a polynomial equation in one variable that cannot be solved by radicals, over some extension of $\mathbb{Q}$. This is called the Abel-Ruffini theorem. Ruffini seemed to have proved this first, in 1799, but his notation for permutations was not understandable, and maybe he even had no notation. Then Abel proved this more rigorously in 1823, and it was greatly clarified by Galois around 1830.

I encourage everyone here to read more about this in any book on algebra that you can get. It is probably better to get a book that treats all details, so, Jacobson's Basic Algebra 1 is easier than Lang's Algebra. Maybe Gallian's "Contemporary Abstract Algebra" is easier.

2 Linear and quadratic equations

This is what most people learn in highschool. The equation

$$ax + b = 0,$$

where $a \neq 0$ and b are real numbers, and x is the variable to be solved, has a unique solution:

$$x = -b/a.$$

It also turns out that we can do this with $\mathbb{R}$ replaced by any field: we only need the operations $+$, $-$, $\cdot$ and $/$. The quadratic equation already makes it natural for us to consider fields in which all square roots exist, for example the field $\mathbb{C}$. The equation

$$ax^2 + bx + c = 0,$$

with $a \neq 0$, b and c in a field F, has the solutions:

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

One says that already Babylonians were able to solve quadratic equations. This was around 2000 BC.

3 Equations of degree 3 and 4

In the Italian renaissance, the equations of degree 3 and 4 were solved. Tartaglia and del Ferro discovered how to solve degree 3 equations. This happened around 1500. They kept their solutions secret, but Cardano wrote them up in his book "Ars Magna". Ferrari found how to solve degree 4 equations. It seems that the reduction from degree 4 to degree 3 was known *before* degree 3 equations could be solved.

What is common in both cases (degree 3 and degree 4) is that the roots are obtained by applying the operations $+$, $-$, $\cdot$ and $/$, and 3rd roots for degree 3, and 3rd and 4th roots for degree 4.

People then tried to solve equations of degree 5 and higher, hoping for formulas of the same kind. They hoped that one could solve the degree n equation by radicals, meaning the field operations plus rth roots, for all positiveintegers r.

4 The Abel-Ruffini theorem

4.1 Theorem. (Abel-Ruffini) *Let $n \geq 5$. Then there exist $a_0, \ldots, a_{n-1}$ in $\mathbb{C}$ such that no root in $\mathbb{C}$ of the equation $x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ can be obtained from $\{0, 1, a_0, \ldots, a_{n-1}\}$, in a finite number of steps, using the operations $+$, $-$, $\cdot$ and $/$, and $()^{1/r}$ (with choice) for all $r \geq 1$ in $\mathbb{Z}$.*

Our goal is to prove this theorem. I hope that it is not too ambitious. We will first develop Galois theory for subfields of $\mathbb{C}$.

5 Galois theory for subfields of $\mathbb{C}$

5.1 Definition. A subfield of $\mathbb{C}$ is a subset $F \subset \mathbb{C}$ that contains 0 and 1 and is closed under $+$, $-$, $\cdot$ and $/$.

5.2 Proposition. *Let $F \subset \mathbb{C}$ be a subfield. Then $(F, 0, 1, +, -, \cdot, /)$ is a field.*

Let F and E be subfields of $\mathbb{C}$ with $F \subset E$; E is called an *extension* of F. Then E is an F-vector space, and $\dim_F(E)$ is called the *degree* of E over F. The extension is *finite* if $\dim_F(E)$ is finite.

5.3 Theorem. *Let $F_1 \subset F_2 \subset F_3 \subset \mathbb{C}$ be subfields. Let $(v_i)_{i \in I}$ be an F_1-basis of F_2, and let $(w_j)_{j \in J}$ be an F_2-basis of F_3. Then $(v_i w_j)_{(i,j) \in I \times J}$ is an F_1-basis of F_3.*

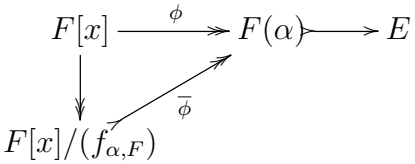
Proof. This is a very good exercise in applying definitions. I think that no idea is required. □

5.4 Remark. Just this theorem, plus the irreducibility of $x^3 - 3x + 1$ in $\mathbb{Q}[x]$ which has $\cos(2\pi/9)$ as root, plus simple considerations on coordinates of points constructible with ruler and compass, show that the angle $2\pi/3$ cannot be trisected with ruler and compass.

5.5 Definition. Let $F \subset \mathbb{C}$ be a subfield, and let $S \subset \mathbb{C}$ be a subset. Then the subfield of $\mathbb{C}$ generated over F by S is the smallest subfield $F(S)$ of $\mathbb{C}$ containing F and S. It is the intersection of all such subfields, and it consists of the fractions a/b with a and $b \neq 0$ of the form $\sum_{\text{finite}} f_i \prod_{\text{finite}} s_j$

5.6 Theorem. *Let $F \subset E$ be a finite extension of subfields of $\mathbb{C}$, and let $\alpha \in E$. Then there is a unique ring morphism $\phi\colon F[x] \to E$ such that $\phi|_F = \mathrm{id}_F$ and $\phi(x) = \alpha$. The image of ϕ is the subfield $F(\alpha)$. The kernel of ϕ is non-zero (because the $(\alpha^n)_n$ are not F-linearly independent, E is finite dimensional as F-vector space). Hence there is a unique $f_{\alpha,F}$ in $F[x]$, monic, such that $\ker(\phi) = (f_{\alpha,F})$. This $f_{\alpha,F}$ is called the* minimum polynomial *of α over F.*

The morphism ϕ factors as follows:



In particular, $F[x]/(f_{\alpha,F})$ is a field, hence $f_{\alpha,F}$ is irreducible.

The following theorem is very important.

5.7 Theorem. *Let $F \subset E$ be a finite extension of subfields of $\mathbb{C}$. Let $\sigma\colon F \to \mathbb{C}$ be a morphism of rings (that is, an embedding of fields). We define:*

$$\mathrm{Hom}_{F,\sigma}(E, \mathbb{C}) := \{\tau\colon E \to \mathbb{C} : \tau|_F = \sigma\}.$$

Then $\#\mathrm{Hom}_{F,\sigma}(E, \mathbb{C}) = \dim_F(E)$, and for all $\alpha \in E$, the set $\{\tau(\alpha) : \tau \in \mathrm{Hom}_{F,\sigma}(E, \mathbb{C})\}$ is the set of roots in $\mathbb{C}$ of $\sigma(f_{\alpha,F})$.

Proof. Induction on $\dim_F(E)$. It is true if $\dim_F(E) = 1$. Assume now that $\dim_F(E) > 1$. Take α in E such that $\alpha \notin F$. Then we have

$$F \subset F(\alpha) \subset E, \quad \dim_F(E) = \dim_F F(\alpha) \cdot \dim_{F(\alpha)} E > \dim_{F(\alpha)}(E).$$

Theorem 5.6 gives an isomorphism $\overline{\phi}\colon F[x]/(f_{\alpha,F}) \to F(\alpha)$. The universal properties of $F \to F[x]$ and $F[x] \to F[x]/(f_{\alpha,F})$ give a bijection between the set of $\tau\colon F(\alpha) \to \mathbb{C}$ extending σ and the set of roots of $\sigma(f_{\alpha,F})$ in $\mathbb{C}$, of which there are exactly $\deg(f_{\alpha,F}) = \dim_F F(\alpha)$. For each $\tau\colon F(\alpha) \to \mathbb{C}$ extending σ, there are, *by induction*, exactly $\dim_{F(\alpha)} E$ extensions of τ to an $\epsilon\colon E \to \mathbb{C}$. Hence

$$\#\mathrm{Hom}_{F,\sigma}(E, \mathbb{C}) = \dim_F F(\alpha) \cdot \dim_{F(\alpha)} E = \dim_F E.$$

The second statement follows from the fact that all τ's have an extension to an ϵ. □

5.8 Definition. For $F \subset E$ a finite extension of subfields of $\mathbb{C}$, we define

$$\mathrm{Aut}_F(E) := \{\sigma \in \mathrm{Aut}(E) : \sigma|_F = \mathrm{id}_F\}.$$

5.9 Corollary. *Situation as in Definition 5.8. Then $\#\mathrm{Aut}_F(E) \leq \dim_F(E)$.*

Proof. This is because $\mathrm{Aut}_F(E)$ is the subset of $\mathrm{Hom}_{F,\mathrm{incl}}(E, \mathbb{C})$ of the τ with $\tau(E) = E$. □

5.10 Definition. Let $F \subset E$ be a finite extension of subfields of $\mathbb{C}$. This extension is *Galois* if $\#\mathrm{Aut}_F(E) = \dim_F(E)$.

5.11 Proposition. *Let $F \subset E$ be a finite extension of subfields of $\mathbb{C}$.*

1. *The extension $F \subset E$ is Galois if and only if $\mathrm{Aut}_F(E) = \mathrm{Hom}_{F,\mathrm{incl}}(E, \mathbb{C})$.*

2. *If $F \subset E$ is Galois, then for all $\alpha \in E$,*

$$\mathrm{Roots}_{\mathbb{C}}(f_{\alpha,F}) = \{\sigma(\alpha) : \sigma \in \mathrm{Aut}_F(E)\} = \mathrm{Aut}_F(E)\cdot\alpha.$$

3. *If f is in $F[x]$, and $E = F(\mathrm{Roots}_{\mathbb{C}}(f))$, then $F \subset E$ is Galois.*

Proof. The first statement is the definition of Galois extension, plus the fact that $\mathrm{Aut}_F(E)$ is the subset of $\mathrm{Hom}_{F,\mathrm{incl}}(E,\mathbb{C})$ of the τ with $\tau(E) = E$. The second statement is the definition of Galois, plus the last statement of Theorem 5.7. The third statement holds because every $\tau\colon E \to \mathbb{C}$ such that $\tau|_F = \mathrm{inj}_F$ has $\tau(E) = E$. □

5.12 Definition. Let E be a field, and let G be a group acting on E by automorphisms. Then we define the invariant subfield $E^G := \{x \in E : \text{for all } g \text{ in } G,\ g\cdot x = x\}$.

5.13 Proposition. *Let $F \subset E$ be a finite Galois extension of subfields of $\mathbb{C}$, $G := \mathrm{Aut}_F(E)$. Then $E^G = F$.*

Proof. Suppose $\alpha \in E$ with $\alpha \notin F$. Then $F(\alpha)$ is bigger than F, hence $\deg(f_{\alpha,F}) > 1$, and there is a $\beta \in \mathrm{Roots}_{\mathbb{C}}(f_{\alpha,F})$ with $\beta \neq \alpha$. By Proposition 5.11 there is a σ in $\mathrm{Aut}_F(E)$ such that $\sigma(\alpha) = \beta$. □

5.14 Proposition. *Let $F \subset E$ be a finite extension of subfields of $\mathbb{C}$, and let G be a subgroup of $\mathrm{Aut}_F(E)$. Let $K := E^G$. Then $\dim_K E = \#G$.*

Proof. Corollary 5.9 says that $\dim_K E \geq \#G$. To prove that $\dim_K E = \#G$ it suffices to prove that $\dim_K E \leq \#G$. I think this part of the proof is due to Emil Artin. Let $n := \#G$. It suffices to show that all $n+1$-tuples $(x_0,\ldots,x_n)$ in E^n are K-linearly dependent. So, let $x_0,\ldots,x_n$ be in E. We want to show that there is a non-zero $(\lambda_0,\ldots,\lambda_n)$ in K^{n+1} such that $\lambda_0 x_0 + \cdots + \lambda_n x_n = 0$. Write $G = \{\sigma_1 = \mathrm{id}_E, \sigma_2, \ldots, \sigma_n\}$.

Consider the system of linear equations over E (the $\sigma_i(x_j)$ are the coefficients):

$$\begin{cases} \sigma_1(x_0)\lambda_0 + \cdots + \sigma_1(x_n)\lambda_n = 0 \\ \qquad\qquad\qquad\qquad\qquad\vdots \\ \sigma_n(x_0)\lambda_0 + \cdots + \sigma_n(x_n)\lambda_n = 0 \end{cases}$$

It has the property that if $(\lambda_0,\ldots,\lambda_n)$ is a solution, and $\sigma \in G$, then $(\sigma(\lambda_0),\ldots,\sigma(\lambda_n))$ is also a solution. Also, this system has more variables than equations, hence there are non-zero solutions in E^n. Let $(\lambda_0,\ldots,\lambda_n)$ be a non-zero solution with minimal number of non-zero coefficients. Renumbering the x_i, we may assume that $\lambda_0 \neq 0$, and dividing by λ_0, we may assume that $\lambda_0 = 1$. We claim that then $(\lambda_0,\ldots,\lambda_n)$ is in K^{n+1}. Suppose not. We may assume that $\lambda_1 \notin K$. Then there is a σ in G with $\sigma(\lambda_1) \neq \lambda_1$. Then $(\lambda_0 - \sigma(\lambda_0),\ldots,\lambda_n - \sigma(\lambda_n))$ is a non-trivial solution ($\lambda_n - \sigma(\lambda_n) \neq 0$) with fewer non-zero coefficients ($\lambda_0 - \sigma(\lambda_0) = 0$). □

5.15 Proposition. *Let $F \subset E$ be a Galois extension of subfields of $\mathbb{C}$. Let K be a subfield of $\mathbb{C}$ with $F \subset K \subset E$. Then the extension $K \subset E$ is Galois.*

Proof. As $F \subset E$ is Galois, every $\tau\colon E \to \mathbb{C}$ such that $\tau|_F = \mathrm{inj}_F$ has $\tau(E) = E$ (see Proposition 5.11). Hence certainly for every $\tau\colon E \to \mathbb{C}$ such that $\tau|_K = \mathrm{inj}_K$ we have $\tau(E) = E$. Hence the conclusion. □

5.16 Proposition. *Let $F \subset E$ be a finite extension of subfields of $\mathbb{C}$. The following conditions are equivalent:*

1. *$F \subset E$ is Galois,*

2. *for all $\alpha \in E$, $f_{\alpha,F}$ splits over E, that is,* $\mathrm{Roots}_{\mathbb{C}}(f_{\alpha,F}) \subset E$.

If $F \subset E$ is Galois, then for every α in E we have $\mathrm{Roots}_{\mathbb{C}}(f_{\alpha,F}) = \mathrm{Roots}_E(f_{\alpha,F}) = \mathrm{Aut}_F(E)\cdot\alpha$.

Proof. Let us prove that (1) implies (2). Write $G := \mathrm{Aut}_F(E)$. Let $\alpha \in E$. Proposition 5.11 says that $\mathrm{Roots}_{\mathbb{C}}(f_{\alpha,F}) \subset E$.

Let us prove that (2) implies (1). Induction on $\dim_F(E)$. It is true if $\dim_F(E) = 1$. Assume now that $\dim_F(E) > 1$. Let $\alpha \in E$ such that $\alpha \notin F$. Then $\#\mathrm{Hom}_{F,\mathrm{inj}}(F(\alpha), E) = \dim_F F(\alpha)$, using Theorem 5.6. By induction, $F(\alpha) \subset E$ is Galois (we use that for all $\beta \in E$, $f_{\beta,F(\alpha)}$ divides $f_{\alpha,F}$, hence splits in E). Hence for every τ in $\mathrm{Hom}_{F,\mathrm{inj}}(F(\alpha), E)$ we have $\#\mathrm{Hom}_{F(\alpha),\tau}(E, E) = \dim_{F(\alpha)} E$. We get $\#\mathrm{Aut}_F(E) = \dim_F E$. □

5.17 Theorem. (Galois correspondence) *Let $F \subset E$ be a Galois extension of subfields of $\mathbb{C}$. Let $G := \mathrm{Aut}_F(E)$. Then the following maps f and g*

$$\{K \subset \mathbb{C} \text{ subfield s.t. } F \subset K \subset E\} \underset{f}{\overset{g}{\rightleftarrows}} \{H \subset G \text{ subgroup}\}$$

are inverses of each other, and they reverse the orderings by inclusion on both sides. Moreover, for each K in the left set, $\#\mathrm{Aut}_K(E) = \dim_K E$, and for each H in the right set, $\dim_{E^H} E = \#H$.

Proof. Let K_1 and K_2 be in the left set, with $K_1 \subset K_2$. Then $\mathrm{Aut}_{K_2}E \subset \mathrm{Aut}_{K_1}E$. Hence g reverses inclusions.

Let H_1 and H_2 be in the right set, with $H_1 \subset H_2$. Then $E^{H_2} \subset E^{H_1}$, hence f reverses inclusions.

Let K be in the left set. Then we have $f(g(K)) = E^{\mathrm{Aut}_K(E)} \supset K$. We also have $\#g(K) = \dim_K(E)$ by Proposition 5.15. Then Proposition 5.14 gives us $\dim_{f(g(K))} E = \#g(K) = \dim_K(E)$. Together with the inclusion $K \subset f(g(K))$ this gives $f(g(K)) = K$.

Let H be in the right set. Then $g(f(H)) = \mathrm{Aut}_{E^H}(E) \supset H$. We also have $\dim_{f(H)} E = \#H$ by Proposition 5.14. Then Proposition 5.15 gives us $\#\mathrm{Aut}_{f(H)}(E) = \dim_{f(H)} E = \#H$. Together with the inclusion $H \subset g(f(H))$ this gives $g(f(H)) = H$. □

6 Sketch of the proof of the Abel-Ruffini theorem

Let $F \subset \mathbb{C}$ be a subfield, and let f be in $F[x]$. Then the extension $F \subset F(\mathrm{Roots}_{\mathbb{C}}(f))$ is Galois (Proposition 5.11), and is called the *splitting field* of f over F. The Galois group $\mathrm{Aut}_F F(\mathrm{Roots}_{\mathbb{C}}(f))$ is called the Galois group of f over F. It acts on $\mathrm{Roots}_{\mathbb{C}}(f)$. Nowadays, for $F = \mathbb{Q}$ and finite extensions of $\mathbb{Q}$, there exist good algorithms to compute these groups (for example in SAGE, pari/gp, Magma, and who knows).

6.1 Proposition. *Let $F \subset K \subset E$ be finite extensions of subfields of $\mathbb{C}$, with $F \subset E$ Galois and $F \subset K$ Galois. Then the morphism $f\colon \mathrm{Aut}_F(E) \to \mathrm{Aut}_F(K)$ that sends σ to $\sigma|_K$ is a surjective morphism of groups. In particular:* $\mathrm{Aut}_F(K)$ *is a quotient of* $\mathrm{Aut}_F(E)$, *and* $\mathrm{Aut}(K(E)$ *is a normal subgroup of* $\mathrm{Aut}_F(E)$.

Let $F \subset \mathbb{C}$ be a subfield, and $f \in F[x]$. Suppose that all roots of f in $\mathbb{C}$ can be obtained by radicals from F and the coefficients of f. Then these radicals, when taking all the choices of the roots that are taken, and also all the roots of the "conjugates" of the roots that are

taken (see "normal closure" in any textbook), generate a Galois extension $F \subset E$ such that $F(\mathrm{Roots}_{\mathbb{C}}(f)) \subset E$. Hence the Galois group of f over F is then a quotient of Aut)$F(E)$. We will show that $\mathrm{Aut}_F(E)$ is *solvable*.

6.2 Definition. A solvable finite group is a finite group G such that there exists an $n \geq 1$ and subgroups

$$G = G_0 \supset G_1 \supset \cdots \supset G_r = \{1\},$$

such that each G_{i+1} is normal in G_i and each G_i/G_{i+1} is abelian.

We will show two ingredients for the proof that solvability by radicals implies that the Galois group is solvable.

6.3 Theorem. *Let $F \subset \mathbb{C}$ be a subfield, $n \geq 1$, and $f := x^n - 1$ in $F[x]$. Then $\mathrm{Roots}_{\mathbb{C}}(f)$ is the cyclic subgroup of $\mathbb{C}^\times$ generated by $z := e^{2\pi i/n}$. Then $\mathrm{Aut}_F F(\mathrm{Roots}_{\mathbb{C}}(f))$ acts on $\mathrm{Roots}_{\mathbb{C}}(f)$ by automorphisms, hence by a morphism to $(\mathbb{Z}/n\mathbb{Z})^\times$. This morphism is injective.*

Proof. This is a good exercise. □

6.4 Theorem. *Let $F \subset \mathbb{C}$ be a subfield, $a \in F$, $n \geq 1$ and $f := x^n - a$ in $F[x]$. Let $b \in \mathbb{C}$ be one root of f, and $z = e^{2\pi i/n}$. Then $\mathrm{Roots}(f) = \{z^j b : j \in \mathbb{Z}/n\mathbb{Z}\}$. Let $E := F(\mathrm{Roots}_{\mathbb{C}}(f))$. Assume that F contains z. Then the map $\mathrm{Aut}_F(E) \to \mu_n(\mathbb{C})$ to the group of nth roots of unity in $\mathbb{C}$ given by $\sigma \mapsto \sigma(b)/b$ is an injective morphism of groups, independent of the choice of b.*

Proof. This is also a very good exercise. □

Let us now show that non-solvable groups occur as Galois groups of polynomials of all degrees $n \geq 5$. We take it as a fact that for $n \geq 5$ the group A_n is simple and non-abelian, hence S_n non-solvable.

6.5 Theorem. *Let $n \geq 5$. Let $r_1, \ldots, r_n$ be algebraically independent elements of $\mathbb{C}$, and let $E := \mathbb{Q}(r_1, \ldots, r_n)$. Let S_n act on E via its permutation action on the set of r_i. Let $F := E^{S_n}$. Then $\mathrm{Aut}_F(E) = S_n$, and $F = \mathbb{Q}(p_1, \ldots, p_n)$, where $p_i = \sum_{j_1 < \cdots < j_i} r_{j_1} \cdots r_{j_i}$ are the elementary symmetric polynomials in the r_i, and $E = F(\mathrm{Roots}_{\mathbb{C}}(f))$, where $f = (x - r_1) \cdots (x - r_n) = x^n - p_{n-1}x^{n-1} + \cdots + (-1)^n p_n$.*

6.6 Remark. Also over $\mathbb{Q}$ these Galois groups occur, and they are even the most occurring Galois groups. For example, the Galois group over $\mathbb{Q}$ of $x^5 - x + 1$ is S_5 (computation done by pari/gp).