GALOIS THEORY AND SOME NUTRITIOUS APPLICATIONS

DAVID PAUKSZTELLO

1. Introduction

Galois theory is a showpiece of mathematical unification. The central application of Galois theory is the proof of the insolubility of the general quintic polynomial by radicals. Moreover, Galois theory gives precise criteria for the insolubility of a given polynomial by radicals. The brief history given here can be found at the beginning of Stewart [2].

1.1. **Applications.** Galois theory provides a means of proving the impossibility of duplicating the cube, squaring the circle and trisecting a general angle. It also gives a beautiful and almost completely algebraic proof of the fundamental theorem of algebra.

1.2. **Some history.** The ancient Greeks were known to have solved quadratic equations by geometrical constructions but there was no sign of an algebraic formulation of the solution of the general quadratic until at least AD 100. We had to wait until 1545 until a physician Girolamo Cardano published a general solution to the cubic due to Niccolo Fontana. This was in the era in Italy when mathematicians wished to keep their methods secret because of the public spectacle of "mathematical jousting". Shortly after Ludovico Ferrari solved the quartic by reducing to a cubic. The next question was the quintic.

Lagrange took an important step in 1770. Lagrange showed that the solutions to the quadratic, cubic and quartic depended on finding functions of the roots of the equation which were unchanged by certain permutations of the roots. This approach failed when he applied the technique to the quintic. There was now a general feeling that it was impossible to solve the quintic by radicals. In 1824 the Norwegian mathematician Abel finally settled the question, proving that the quintic could not be solved by radicals.

The problem was now thus: how does one decide whether or not a given polynomial equation can be solved by radicals? Abel was working on it at the time of his death in 1829. In 1832 a twenty year old Frenchman died in a duel.

1.3. **The duel.** At a Banquet on 9 May 1831 a young Frenchman, Évariste Galois proposed a toast to the King of France, Louis-Philippe (newly installed after an unsuccessful coup d'état by the previous king, Charles X), with an open knife. This was interpreted as a threat on the new king's life and the following day Galois was arrested. He admitted everything at the trial but claimed that his toast had actually been: "To Louis-Philippe, if he turns traitor," but that

Date: 13th October 2005.

the last phrase had been drowned out by the uproar at the banquet. Galois was aquitted by the jury.

On the 14 July 1831 Galois was a the head of a Republican demonstration wearing the uniform of the disbanded artillery of the Republican National Guard whilst carrying a knife and a gun. He was arrested for illegally wearing a uniform and sentence to six months' imprisonment. Upon freedom he experienced his first and only love affair to a Mlle Stéphanie-Felice Poterin du Motel. Galois's advances were spurned and he took rejection badly. Not long afterwards he was challenged to a duel because of the girl. The motivation behind the duel is shrowded in mystery, some claim political motives, but Galois's own testament that it was simply a matter of honour. Pistols at 25 paces, Galois was a better mathematician than a marksman and was shot in the stomach, dying a day later on 31 May 1832.

Eleven years later, Joseph Liouville addressed the Academy of Sciences in Paris, opening with the words: "I hope to interest the Academy in announcing that among the papers of Évariste Galois I have found a solution, as precise as it is profound, of this beautiful problem: whether or not it is soluble by radicals."

2. Sketch of Fontana's solution of the cubic

This sketch is taken from [1]. Every schoolchild knows that the solution to the general quadratic equation $x^2 + bx + c$ is

$$\frac{-b \pm (b^2 - 4c)^{1/2}}{2}$$

Here we sketch a derivation of the formula for the general cubic. Reduce the general cubic $x^3 + ax^2 + bx + c$ to $x^3 + 3px + 2q$ by the change of variable $x \mapsto x + \frac{1}{3}b$. In order to find the formula we start by searching for three roots α, β, γ with

$$\begin{aligned} \alpha + \beta + \gamma &= 0 \\ \alpha\beta + \alpha\gamma + \beta\gamma &= 3p \\ \alpha\beta\gamma &= -2q \end{aligned}$$

Now, here's the trick. We look for solutions of the form

$$\begin{aligned} \alpha &= y + z \\ \beta &= \omega y + \omega^2 z \\ \gamma &= \omega^2 y + \omega z \end{aligned}$$

where ω is a primitive cube root of unity. Subsituting the equations above into the ones above that we obtain:

$$\begin{aligned} yz &= -p \\ y^3 + z^3 &= -2q \end{aligned}$$

It follows that y^3 and z^3 are the two roots of the auxiliary quadratic equation $t^2 + 2qt - p^3 = 0$. The quadratic formula gives the solutions

$$y^3, z^3 = -q \pm (q^2 + p^3)^{1/2}.$$

We will see later that the trick employed above is no accident.

3. Some algebra!

Definition 1. A *field extension* is an inclusion $k \to K$ of k into a bigger field. We will denote a field extension by K/k and regard k as a subfield of K.

Suppose K/k and L/k are two extensions. A field homomorphism $\phi : K \to L$ is called a *k-homomorphism* if $\phi(a) = a$ for all $a \in k$.

Suppose k/K is a field extension and $S \subseteq K$ is a subset. We write $k[S]$ for the subring of K generated by k and S and $k(S)$ for the subfield of K generated by k and S. If $S = \{x_1, \ldots, x_n\}$ is a finite set then we write $k[x_1, \ldots, x_n]$ and $k(x_1, \ldots, x_n)$ for $k[S]$ and $k(S)$ respectively. Note that $k(S)$ is the field of fractions of $k[S]$.

Definition 2. The *degree* $[K : k]$ of the field extension K/k is defined as the dimension of K as a vector space over k

$$[K : k] = \dim_k K.$$

The field extension K/k is called *finite* if it has finite degree.

Theorem 3 (Tower Law)**.** *Suppose K/k and L/K are field extensions. Then*

$$[L : k] = [L : K][K : k].$$

4. Ruler and compass

The ancient Greeks had constructions involving the use of only ruler and compass for the following constructions (among many): the division of a line into arbitrarily many segments, the bisection of angles, the drawing of parallel lines and the construction of a square equal in area to any given polygon. However, the Greeks couldn't find constructions by ruler and compass of the following problems: the duplication of the cube, the trisection of the angle and the squaring of the circle. And with good reason: they are impossible.

Now let us formulate algebraically what we mean by a ruler and compass construction. Let $S \subseteq \mathbb{R}^2$ be a set of points in the Euclidean plane.

Ruler: Given two points $P, Q \in S$ join $P, Q \in S$ by a straight line.

Compass: Given points $P, Q_1, Q_2 \in S$ draw a circle with centre P and radius Q_1Q_2.

Definition 4. A point $R \in \mathbb{R}^2$ is *constructible in one step* (or 1-*constructible*) from S if R is a point of intersection of any two distinct curves obtained from S by either of the two constructions above.

A point $R \in \mathbb{R}^2$ is *constructible* from S if there exist points $R_1, \ldots, R_n$ with $R_n = R$ such that R_1 is constructible in one step from S and each R_i for $1 < i \leqslant n$ is constructible in one step from $S \cup \{R_1, \ldots, R_{i-1}\}$.

Definition 5. Let $S \subseteq \mathbb{R}^2$ be a set of points in the Euclidean plane. The *field* of S is defined to be the subfield of $\mathbb{R}$ generated by the x- and y-coordinates of the points of S:

$$\mathbb{Q}(S) = \mathbb{Q}(x, y : (x, y) \in S).$$

Proposition 6. *(i) If $R \in \mathbb{R}^2$ is constructible in one step from S then $[\mathbb{Q}(S \cup \{R\}) : \mathbb{Q}(S)] = 1$ or 2.*

(ii) If S' is constructible from S then $[\mathbb{Q}(S') : \mathbb{Q}(S)]$ is a power of 2.

Proof: (i) Suppose R is a point of intersection of two curves L_1, L_2 given by our two constructions, $R = L_1 \cap L_2$. L_1, L_2 have equations

$$\begin{aligned} L_1 : a_1(x^2 + y^2) + b_1 x + c_1 y + d_1 &= 0 \\ L_2 : a_2(x^2 + y^2) + b_2 x + c_2 y + d_2 &= 0 \end{aligned}$$

with coefficients $a_1, \ldots, d_2 \in \mathbb{Q}(S)$.

If $a_1 = 0 = a_2$ then L_1, L_2 are straight lines and the coordinates of R belong to $\mathbb{Q}(S)$. Hence $\mathbb{Q}(S \cup \{R\}) = \mathbb{Q}(S)$ and $[\mathbb{Q}(S \cup \{R\}) : \mathbb{Q}(S)] = 1$.

Now assume at least one of a_1 or a_2 is nonzero. Consider the line $M = a_2 L_1 - a_1 L_2$ given by the equation $b_3 x + c_3 y + d_3 = 0$, where $b_3 = a_2 b_1 - a_1 b_2$ etc. If $c_3 \neq 0$, say (one of b_3 or c_3 must be nonzero otherwise L_1 and L_2 are the same curve), then

$$y = \frac{-d_3 - b_3 x}{c_3}$$

and then the quadratic equation obtained by subsituting for y in L_1 is satisfied by the x-coordinate of R. That is, we have a quadratic equation $\lambda x^2 + \mu x + \nu = 0$ with $\lambda, \mu, \nu \in \mathbb{Q}(S)$. Thus

$$\mathbb{Q}(S \cup \{R\}) = \mathbb{Q}(S)(x, y) = \mathbb{Q}(S)(x).$$

Hence, since x satisfies a polynomial equation of degree 2 it follows that $[\mathbb{Q}(S \cup \{R\}) : \mathbb{Q}(S)] = 1$ or 2.

(ii) Now suppose S' is constructible from S, hence $S' = S \cup \{R_1, \ldots, R_n\}$ and

$$\mathbb{Q}(S) \subseteq \cdots \subseteq \mathbb{Q}(S \cup \{R_1, \ldots, R_i\}) \subseteq \mathbb{Q}(S \cup \{R_1, \ldots, R_{i+1}\}) \subseteq \cdots \subseteq \mathbb{Q}(S').$$

By (i) each step has degree 1 or 2. Hence (ii) follows from the Tower Law, Theorem 3. □

4.1. **Impossibility proofs.**

Theorem 7. *The cube cannot be doubled by ruler and compass, i.e. it is impossible to construct a cube with precisely doubled the volume of a given cube by ruler and compass.*

Proof: Suppose for a contraction that the cube can be doubled by ruler and compass. Suppose we are given a cube. Thus we are given a side of the cube. Without loss of generality we may assume that this side is the unit interval on the x-axis. We may assume that $S = \{(0,0),(1,0)\}$ so that $\mathbb{Q}(S) = \mathbb{Q}$. In order to double the cube we would need to be able to construct the point $(\alpha, 0)$ where $\alpha^3 = 2$. But α is a zero of the polynomial $x^3 - 2$ over $\mathbb{Q}$ which is irreducible over $\mathbb{Q}$ by Eisenstein's criterion. Thus $\mathbb{Q}(S)(\alpha, 0) = \mathbb{Q}(S)(\alpha) = \mathbb{Q}(\alpha)$. Hence $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$ since $x^3 - 2$ is the minimum polynomial of α over $\mathbb{Q}$. But this contradicts Proposition 6, proving that it is impossible to double the cube by ruler and compass. □

Theorem 8. *The angle of $\frac{\pi}{6}$ cannot be trisected by ruler and compass.*

Proof: To construct an angle trisecting $\frac{\pi}{6}$ is equivalent of constructing the point $R = (\sin\frac{\pi}{18}, \cos\frac{\pi}{18})$. The formula $\sin 3\theta = 3\sin\theta - 4\sin^3\theta$ gives the equation

$$4\sin^3\frac{\pi}{18} - 3\sin\frac{\pi}{18} = -\sin\frac{\pi}{6} = -\frac{1}{2}.$$

That is, $\alpha = 2\sin\frac{\pi}{18}$ is a root of the polynomial $f(x) = x^3 - 3x + 1$. f is irreducible over $\mathbb{Q}$ by Eisenstein's criterion and thus $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$. This contradicts Proposition 6, and hence R is not constructible and thus it is impossible to trisect the angle of $\frac{\pi}{6}$ using ruler and compass. □

If it were possible to trisect the general angle by ruler and compass then it certainly would be possible to trisect the angle of $\frac{\pi}{6}$ by ruler and compass. Hence it is impossible to trisect the general angle using ruler and compass.

The proof of the impossibility of squaring the circle follows in a similar vein.

4.2. **Which constructions are possible?** We have seen a couple of examples of constructions by ruler and compass which are impossible. Does Galois theory provide us with a means of proving which constructions are possible rather than just which are impossible. In short, yes. There is a famous theorem by Gauss which goes as follows:

Theorem 9 (Gauss)**.** *The regular n-gon is constructible by ruler and compass if and only if $n = 2^r p_1 \ldots p_s$ where r, s are non-negative integers and $p_1, \ldots, p_s$ are odd primes of the form $p_i = 2^{2^{r_i}} + 1$ for positive integers r_i.*

We omit the proof, but the interested reader is directed to Chapter 17 of Stewart [2]. Primes of the form above are known as *Fermat primes* after the French mathematician of Last Theorem fame. The only Fermat primes we know are those which were found by Fermat.

5. More algebra!

We've seen just how powerful a tool the degree of a field extension can be, but unfortunately it turns out that it's not quite powerful enough to answer the problem Galois set out to solve. The degree of a field extension gives us an idea of the size of the field extension but no ideas about it's shape. And the problem of Galois theory has a lot to do with symmetry. We need to delve deeper and we need some more algebra!

Definition 10. A field extension K/k is said to be *normal* if every irreducible polynomial $f \in k[x]$ that has a root in K splits into linear factors over K.

The notion of a normality of a field extension is a trade unionist definition, the slogan being: one out, all out!

Definition 11. Let $f \in k[x]$ be a polynomial. A field extension K/k is called a *splitting field* for f over k if:

(i) f splits into linear factors over K, that is

$$f = c\prod_{i=1}^{n}(x - \alpha_i)$$

with $a\alpha_i \in K$;

(ii) $K = k(\alpha_1, \cdots, \alpha_n)$.

The second condition ensures that K is the smallest field extension of k such that the first condition holds.

Example 12. Suppose k is a field which contains all p^{th} roots of unity for some p. Suppose $a \in k$ is not a p^{th} power of any element of k. Then $x^p - a$ is irreducible and the extension $k \subset k(\alpha)$ with $\alpha^p = a$ is a splitting field of $x^p - a$ over k.

Theorem 13 (Existence and uniqueness of splitting fields)**.** *(a) Given any $f \in k[x]$ there is a splitting field for f over k.*

(b) The splitting field is unique up to k-isomorphism.

6. Galois correspondence

From now on we will assume that the characteristic of k, $\text{char}k = 0$ because of a pathology occurs in the case $\text{char}k = p$.

Recall that a k-automorphism of K is a field automorphism $\phi : K \to K$ such that $\phi(a) = a$ for all $a \in K$. The *Galois group* is defined by:

$$\text{Gal}(K/k) = \{k - \text{automorphisms of } K\}.$$

Theorem 14. *Suppose K/k is a finite field extension. Then $\text{Gal}(K/k)$ has order $[K : k]$ if and only if K/k is normal.*

Let G be a subgroup of the group of automorphisms of K. Define $K^G = \{a \in K | g(a) = a \text{ for all } g \in G\}$. K^G is called the *fixed field* of G. A field extension K/k is called a *Galois extension* if there is a finite subgroup G of the automorphism group of K such that $k = K^G$.

Theorem 15. *K/k is Galois if and only if it is finite and normal. Moreover, the G such that $K^G = k$ is $\text{Gal}(K/k)$.*

It follows that $[K : k] = |G|$. Note that any field extension K/k sits inside a "minimal" normal field L in a unique way.

For a field extension K/k with Galois group $G = \text{Gal}(K/k)$ define

$$\mathcal{F} = \{\text{intermediate fields } F | k \subset F \subset K\}$$

and

$$\mathcal{G} = \{\text{subgroups } H \subset G\}.$$

For $F \in \mathcal{F}$ we write:

$$F^* = \{g \in G | g(x) = x \text{ for all } x \in F\},$$

and for $H \in \mathcal{G}$ we write:

$$H^\dagger = K^H.$$

Theorem 16 (Fundamental theorem of Galois theory)**.** *Let K/k be a finite Galois extension with Galois group G. Then $F = F^{*\dagger}$ and $H = H^{\dagger *}$.*

Example 17. Let $x^3 - 5 \in \mathbb{Q}[x]$. Write $\alpha^3 = 5$ with $\alpha \in \mathbb{R}$ and let ω be a primitive cube root of unity. The splitting field of $x^3 - 5$ over $\mathbb{Q}$ is

$$K = \mathbb{Q}(\alpha, \omega\alpha, \omega^2\alpha) = \mathbb{Q}(\omega, \alpha).$$

The minimal polynomial of α over $\mathbb{Q}$ is $x^3 - 5$, so $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$. The minimal polynomial of ω over $\mathbb{Q}(\alpha)$ is $x^2 + x + 1$, so $[\mathbb{Q}(\omega, \alpha) : \mathbb{Q}(\alpha)] = 2$. So by the Tower Law $[\mathbb{Q}(\omega, \alpha) : \mathbb{Q}] = 6$. Now K is normal as the splitting field for $x^3 - 5$ over $\mathbb{Q}$, therefore $|\mathrm{Gal}(K/\mathbb{Q})| = 6$ and $\mathrm{Gal}(K/\mathbb{Q}) = \mathbb{Z}/6\mathbb{Z}$ or S_3.

Let $\sigma : K \to K$ be given by $\sigma(x) = x$ for $x \in \mathbb{Q}$, $\sigma(\alpha) = \omega\alpha$ and $\sigma(\omega) = \omega$. Then clearly σ is a $\mathbb{Q}$-automorphism of K and $\sigma^3 = 1$. Let $\tau : K \to K$ be given by $\tau(x) = x$ for $x \in \mathbb{Q}$, $\tau(\alpha) = alpha$ and $\tau(\omega) = \omega^2$. Then τ is a $\mathbb{Q}$-automorphism of K and $\tau^2 = 1$. Now $\sigma\tau(\alpha) = \omega\alpha$ and $\tau\sigma(\alpha) = \omega^2\alpha$, hence $\sigma\tau \neq \tau\sigma$ and therefore $\mathrm{Gal}(K/\mathbb{Q})$ is not abelian. Hence $\mathrm{Gal}(K/\mathbb{Q}) = S_3$.

We now illustrate the Galois correspondence given by the fundamental theorem of Galois theory. The subgroups of S_3 are $H_1 = \{1\}$, $H_2 = \{1, \sigma, \sigma^2\}$, $H_3 = \{1, \tau\}$, $H_4 = \{1, \sigma\tau\}$, $H_5 = \{1, \sigma^2\tau\}$ and $H_6 = S_3$. By the fundamental theorem of Galois theory there are the following intermediate fields $\mathbb{Q} \subset F \subset K$: $H_1^\dagger = \mathbb{Q}(\alpha, \omega) = K$, $H_2^\dagger = \mathbb{Q}(\omega)$, $H_3^\dagger = \mathbb{Q}(\alpha)$, $H_4^\dagger = \mathbb{Q}(\omega^2\alpha)$, $H_5 = \mathbb{Q}(\omega\alpha)$ and $H_6^\dagger = \mathbb{Q}$.

7. Solving equations by radicals

7.1. **Soluble Groups.**

A finite group G is said to be *soluble* if there exists a chain

$$G = A_0 \supset A_1 \supset \cdots \supset A_r = \{1\}$$

of subgroups of G such that for $i = 0, \dots, r-1$ A_{i+1} is a normal subgroup of A_i and A_i/A_{i+1} is abelian.

If G is a soluble group and $H \subset G$ is a subgroup, then H is also soluble. It can be shown that the alternating group A_n is not soluble for $n \geq 5$, and therefore the symmetric group S_n is not soluble for $n \geq 5$.

7.2. **Radical extensions.**

A field extension K/k is called *radical* if there exists a chain

$$k = k_0 \subset k_1 \subset \cdots \subset k_r = K$$

such that for each i $k_{i+1} = k_i(\alpha_i)$ with $\alpha_i^{p_i} \in k_i$; that is each step consists of adjoining a p^{th} root. In particular, each step just consists of allowing you take a p^{th} root.

A field extension K/k is called *soluble* if there exists an extension $K \subset L$ such that $k \subset L$ is radical. If $f \in k[x]$ is an irreducible polynomial and $K = k(\alpha)$ is a field extension in which f has a root, then K/k is a soluble extension if and only if a root of f can be got by applying field operations and taking roots; that is, if and only if f can be solved by radicals.

Theorem 18. *Let K/k be a field extension. Then K/k is soluble if and only if its Galois closure L has a soluble Galois group.*

Example 19. Let $f = x^5 - 6x + 3 \in \mathbb{Q}[x]$. It can be shown that f is irreducible over $\mathbb{Q}$. Let $K = \mathbb{Q}(\alpha_1, \ldots, \alpha_5)$ be the splitting field of f over $\mathbb{Q}$. The Galois group $G = \mathrm{Gal}(K/\mathbb{Q})$ acts transitively on the set of roots, i.e. given a root α of f then $\alpha^G = \{\alpha_1, \ldots, \alpha_5)$. Sketching the graph of f we see that f has three real roots and thus has a complex conjugate pair of roots. Complex conjugation restricts to K to give a $\mathbb{Q}$-automorphism of K which transposes the complex conjugate pair of roots. It can be shown with some group theory that this means G is the whole of S_5. But we know that S_5 is not soluble, hence by the theorem above f is not soluble by radicals.

8. The inverse Galois problem

We have seen how every polynomal f has associated to it a Galois group, namely the Galois group of the field extension consisting of the splitting field of f. Now given a finite group G, does there exist an extension K/k with Galois group G? In particular, for $k = \mathbb{Q}$, does G occur as the Galois group of a polynomial f over $\mathbb{Q}$? This question is still open. However, it was shown by Shaferevich that all soluble groups occur as Galois groups of field extensions $K/\mathbb{Q}$ (1954).

References

[1] M. Reid, lecture notes from a course *MA3D5 Galois Theory* given at the University of Warwick in 2003.

[2] I. Stewart, "Galois Theory" second edition; Chapman and Hall/CRC, Boca Raton, Florida 1989.