Extremely light introduction to Galois Theory

Armando Gonçalves[1,a]

[1]*MEFT, 100290*

Abstract. Brief discussion of some jargon related to Galois Theory, mentioning some applications to engineering. The discussion will largely follow the content of the YouTube channel Mathemaniac's video on Galois Theory, that can be found here.

Keywords: Galois Groups, Fields, Quintic Polynomials

1 Introduction

The applications of Galois Theory span across various domains, influencing cryptographic protocols based on finite fields, aiding design graphics, computer vision, and geometric modeling; the study of dynamical systems benefits from Galois Theory as well, particularly in the analysis of polynomial transformations, revealing connections to Julia sets and the Mandelbrot set. Its role extends to control engineering, where problems related to stability and optimal control are cast in terms of polynomial equations. Its relevance also extends to coding theory, information transmission, and mathematical modeling, making it a cornerstone in the toolkit of applied mathematics. Polynomial equations are prevalent in engineering and physics. Trajectories in robotic systems play a pivotal role in defining the motion of robotic arms or manipulators. These trajectories, often represented as a series of joint positions over time, determine how a robot moves from one point to another. The challenge lies in planning these trajectories effectively to ensure smooth and efficient movements, considering factors such as joint limits, singularities, and the overall task at hand. **Quintic polynomials** are commonly employed to generate trajectories that adhere to specific constraints[1][2], ensuring not only positional accuracy but also maintaining velocity and acceleration profiles. Fifth-degree polynomial equations can be encountered as well in certain fields like civil engineering, computer graphics, among others (see [3][4][5]).

It is therefore essential to know how to solve these polynomial equations. The current approach to solve quintic equations is through numerical methods, predominantly employing techniques like Newton's method. Despite its effectiveness, this computational method can be slower[1] and less reliable, sometimes requiring the selection of an appropriate initial value, and there are instances where it may not work consistently. However, as established by the works of Galois and Abel-Ruffini, **it is the only viable way to do so**, as quintic equations do not possess analytical solutions. In this way, the ensuing discussion aims to give a light-weighted introduction to some Galois Theory, referring some terminology and ideas.

[a]e-mail: armandogoncalves@tecnico.ulisboa.pt

[1]When compared to directly plugging in the analytical solutions, in the quartic equation case.

2 Field Extensions

As we have seen in our classes, the set of rational numbers $\mathbb{Q}$ forms a field, as it is a ring with commutative multiplication, and all elements in $\mathbb{Q} \setminus \{0\}$ have multiplicative inverses. We now need to introduce the concept of a field extension. For example, $\mathbb{Q}(\sqrt{2})$ is the set of rationals extended along with all combinations $a + b\sqrt{2}$, where $a, b \in \mathbb{Q}$. We can perform successive extensions (or radical extensions) such as $\mathbb{Q}(\sqrt[5]{23}) \to \mathbb{Q}(\sqrt[5]{23}, \sqrt[3]{1+\sqrt[5]{23}}) \to \ldots$ - and if the equation is solvable, we can find successive extensions that ultimately lead to an extension of rationals containing all the roots of the polynomial (the analytical solution, at last!...). The **splitting field** is the smallest field extension of $\mathbb{Q}$ that includes all the roots of the polynomial.

3 Galois Group

An **automorphism** is a surjective function that maps a field L to itself $\sigma : L \to L$, with the following properties:

(1) $\sigma(x \bigstar y) = \sigma(x) \bigstar \sigma(y)$ for $\bigstar = +, \cdot, \div$ and $x, y \in L$

(2) $\sigma(x) = x$ if $x \in K \subseteq L$[2]

An example of an automorphism is the conjugation operation for $L = \mathbb{C}$ and $K = \mathbb{R}$.

Now, let's consider the situation where K is the field where the coefficients of an arbitrary polynomial $p(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0$ "live," and L is the splitting field of $p(x)$. By this point forward, we always assume there are no repeated roots. If we consider an $\alpha \in \{\alpha : p(\alpha) = 0\}$ and plug it into $p(x)$, that is $p(\alpha)$, we get $0 = a_n(\alpha)^n + a_{n-1}(\alpha)^{n-1} + ... + a_1(\alpha) + a_0$. We can apply $\sigma(x)$ to both sides of the equation, and we would have $0 = a_n\sigma(\alpha)^n + a_{n-1}\sigma(\alpha)^{n-1} + ... + a_1(\alpha) + a_0$ (using properties **(1)** and **(2)** and the fact that $0 = a_n - a_n = \sigma(a_n) - \sigma(a_n) = 0$). So $\sigma(\alpha)$ is also a root of $p(x)$! That is σ permutes one root of $p(x)$ to another root (to itself is also valid). Thus, the extension from K to L, i.e., from the field with the coefficients of some$p(x)$ extended with the roots of some$p(x)$, gets a special name: **Galois Extension**. The set of the collection of automorphisms σ from the extension of L over K, or $\mathbf{Aut}(L/K)$, forms a group, called the **Galois Group**. We can check it forms a group checking the three properties:

[2]In this context, we can interpret extension from K to L.

(1) For $\sigma_1, \sigma_2, \sigma_3 \in$ Aut(L/K), we have that they are associative since either $\sigma_i(x) = x$ or it is a permutation - in both cases there is associativity (permutations do associate);

(2) The neutral element e is given by e(x) = x;

(2) We can always find an inverse automorphism: for $x \in K$, $f^{-1}(x) = x$, for x outside of K, you do the opposite permutation of f(x).

4 Tower Extensions

Let's consider $p(x) = x^5 - 1 = 0$ as an example. It has 5 roots, one of them being $1 \in \mathbb{Q}$. Imagining the unitary circle in the complex plane, we have the first root (1,0), the second root, let's call it ζ, the next one would be ζ^2, and then ζ^3 and ζ^4. If we consider $K = \mathbb{Q}$ and $L = \mathbb{Q}(\zeta)$, we have a Galois Extension since L has all the roots of our equation (indeed $\zeta^l = a + b\zeta$). As we're adjoining just the n-th roots of the unity this extension is said to be **Cyclotomic**. Also, if we consider an automorphism $\sigma_l(\zeta) = \zeta^l$, for this specific example, what we observe is that $\sigma_l\sigma_m(\zeta) = \sigma_m\sigma_l(\zeta) = \zeta^{lm}$, and the Galois Group is said to be **abelian**.

On the other hand, if we consider $p(x) = x^5 - \theta = 0$, we will still have 5 roots, but now they will be of the form $\{\alpha\zeta, \alpha\zeta^2, \alpha\zeta^3, \alpha\zeta^4\}$, where ζ^l are the unit solutions scaled by a certain α. Its Galois Group in this case is once again abelian, and once again, we can construct a Galois extension by considering $K = \mathbb{Q}$ and $L = \mathbb{Q}(\alpha, \zeta)$. But note that it would be perfectly legitimate and equally a Galois Extension to have chosen $K = \mathbb{Q}(\zeta)$ and $L = \mathbb{Q}(\alpha, \zeta)$. When you adjoint n-th root of some number while the already n-th roots of unity are already there you have a **Kummer extension**. Something we can do and will be important shortly is to stack Kummer and Cyclotomic extensions: $\mathbb{Q} \to \mathbb{Q}(\zeta) \to \mathbb{Q}(\zeta, \alpha)$. All the extensions that can be formed with this stacking are too Galois Extensions, as we defined previously.

5 Relation between Groups

Now let's consider the tower of Galois extensions $K \to L \to M$, with K containing the coefficients of a polynomial p(x), L being the splitting field of that polynomial, and M being an even larger extended field, along with their respective Galois groups for each extension: Aut(L/K), Aut(M/L), and Aut(M/K). If $\sigma \in$ Aut(M/L), then $\sigma \in$ Aut(M/K), or in other words, Aut$(M/L) \subseteq$ Aut(M/K). Since Aut(M/L) is a group, we conclude that Aut(M/L) is a subgroup of Aut(M/K). Furthermore, let $\sigma_g \in$ Aut(M/K) and $\sigma_h \in$ Aut(M/L), where l is an element belonging to L. $\sigma_g \cdot \sigma_h \cdot \sigma_g^{-1}(l)$ will still belong to L because (1) $g^{-1}(L) = L$ since if l is in K, $g^{-1}(l) = l$, and if l is a root, by definition σ(root) = root, meaning it's still in L (2) $\sigma_h(L) = L$ by the definition of an automorphism (3) g(L)=L, similar reasoning applies to g^{-1}. Thus, we can classify Aut(M/L) as a **normal subgroup** of Aut(M/K).

On the other hand, Aut(L/K) = Aut(M/K)/Aut(M/L). Intuitively, when we think about automorphisms of M/K, M is mapped to M, but L is also mapped to L as we've seen because the elements of K go to K, and the remaining elements of L, the roots, must also be mapped to L by the way the function σ was defined. So, if we "zoom in" on L, we can have the same automorphism L/K occurring, even though, looking through the "window", the other elements of M are being mapped differently — different automorphisms M/K that leave Aut(M/L) unchanged or fixed ($\equiv M/L$). In other words, we can construct equivalence classes or "boxes" based on whether the automorphisms L/K are the same or different for the different automorphisms M/K — basically it is the mentioned quotient group.[3]

6 Whiff of Solvability

Finally, the idea is to create successive extensions of the form $\mathbb{Q} \to \mathbb{Q}(\beta_1) \to \ldots \to \mathbb{Q}(\beta_1, \ldots, \beta_i)$ with $\beta_i = \sqrt[n]{\theta_i}$. All these extensions will either be Kummer or Cyclotomic, until we reach the largest extension, which will also be, without showing proof, a Galois Extension. Let's think about the intermediate extensions, for example, in G = Aut$(\mathbb{Q}(\beta_1, \beta_2, \ldots, \beta_r)/\mathbb{Q})$ and G_1 = Aut$(\mathbb{Q}(\beta_1, \beta_2, \ldots, \beta_r)/\mathbb{Q}(\beta_1))$. As we saw earlier, G_1 would be a normal subgroup of G, and Aut$(\mathbb{Q}(\beta_1)/\mathbb{Q})$ = G/G_1. If we now repeat the reasoning for G_2 = Aut$(\mathbb{Q}(\beta_1, \beta_2, \ldots, \beta_r)/\mathbb{Q}(\beta_1, \beta_2))$, we would conclude again that G_2 is a normal subgroup of G. We can repeat the reasoning until G_{r-1} = Aut$(\mathbb{Q}(\beta_1, \beta_2, \ldots, \beta_r)/\mathbb{Q}(\beta_1, \beta_2, \ldots, \beta_{r-1}))$ and create a chain of normal subgroups of G. Note that since all extensions are either Kummer or Cyclotomic, all subgroups will be abelian, and this type of relationship gets a name: **Solvable**. If we can find indeed these normal subgroups, then the biggest group G is called solvable. If we build an extension like $\mathbb{Q} \to L \to M$, where L is a splitting field and G = Aut$(M/\mathbb{Q})$ is the aforementioned biggest group, it turns out that if G is solvable, so is $G/$Aut(M/L). We reach then our final stop: if our polynomial is solvable by radicals (we can locate it in this splitting field), then it is solvable by the Galois group. Or, if the Galois cannot be solvable, then the polynomial isn't solvable by radicals. This will have huge implications and would show why does quintic polynomial equations doesn't have an analytical solution, but I'm afraid my journey ends here. At least for now :)

References

[1] *Trajectory planning columbia edu*, https://www.cs.columbia.edu/ allen /F15/NOTES/trajectory.pdf

[2] W. Zhang, *Ece5463: Introduction to robotics lecture note 9: Trajectory generation spring 2018*, https://www2.ece.ohio-state.edu/ zhang/ RoboticsClass/docs/LN9$_T$*rajectoryGeneration.pdf*

[3] I'm aware that this last explanation is a bit messy. Given that it's a brief explanation and this part isn't the focus of the discussion, I recommend watching the video for more clarity.

[3] X. Fan, W. Jiang, N. Mei, C.Q. Su, Journal of Physics: Conference Series **2174**, 012090–012090 (2022)

[4] B. Mama, O. Oguaghabmba, C. Ike, *QUINTIC POLYNOMIAL SHAPE FUNCTIONS FOR THE FINITE ELEMENT ANALYSIS OF ELASTIC BUCKLING LOADS OF EULER-BERNOULLI BEAM RESTING ON WINKLER FOUNDATION* (2020)

[5] A.M. Rababah, International Journal of Electrical and Computer Engineering (IJECE) **9**, 3779 (2019)