Distribution of Galois groups

Yannick Verbeelen
Maxime Rubio

supervised by
Prof. Pieter Belmans

Experimental Mathematics 4
University of Luxembourg
Faculty of Science, Technology and Medicine
Academic Year 2021-2022 (Winter Semester)

Contents

1 Introduction

The influence and precocity of the work of Evariste Galois (1811-1832) lead some to recognize the mathematician as the Rimbaud of mathematics. Especially since Galois died very early, at the age of 20, from the tragic consequences of a duel. His work laid the foundation of Galois Theory which can be used to transform problems of field theory into problems of group theory which is often a simpler way of solving them.

In this project, we will start by giving a short introduction to Galois theory followed by its relation to the solvability by radicals of polynomials. After a short discussion on the inverse Galois problem, we will study the distribution of Galois groups on finite sets of polynomials. This study joins recent developments on van der Waerden's conjecture, since it was demonstrated by Manjul Bhargava in an article [1] published on November 15, 2021.

2 Theoretical Part

2.1 Galois Theory

The goal in this section is to remind the important results of Galois theory. However, some basic notions, such as the definition of an *algebraic field extension*, are supposed to be known by the reader. No proof will be given but every results are well known and can be found in the literature.
This section is inspired by the lecture notes of Gabor Wiese [4].

First of all we define a Galois extension as an algebraic field extension that is normal and separable.
Let us remind that an algebraic field extension L/K is:

- normal if every irreducible polynomial with a root in L splits into linear factors over L.
- separable if for every a in L its minimal polynomial in K is separable, that is every root of the polynomial is of multiplicity 1.

The final notion we need for the definition of a Galois group is the one of K-automorphism which is essentially an automorphism f of a field extension L/K but with the additional condition that $f(x) = x$ for every x in K.

We now possess all the needed notions to give a formal definition of the Galois group of a Galois extension:

Definition 2.1. The *Galois group* of a Galois extension L/K is the group of K-automorphism of L and is denoted $Gal(L/K)$.

Here a straightforward example:

- $\mathbb{C}/\mathbb{R}$ is a Galois extension with $Gal(\mathbb{C}/\mathbb{R}) = Aut_{\mathbb{R}}(\mathbb{C}) = \{id_{\mathbb{C}}; c\}$ with c being the complex conjugate.

Additionally we define the Galois group of a polynomial to be the Galois group of its splitting field, which is the notion that we will work with in this project.
Essentially what the elements of the Galois group do is leave all the elements of the original field unchanged and swap the roots in the field extension.
Let us for example take the rational polynomial $f(X) = X^2 - 2 \in \mathbb{Q}[X]$. Clearly its splitting field is $\mathbb{Q}(\sqrt{2})$. We have $Gal(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) = \{id, \sigma\}$ where σ is uniquely determined by $\sigma(\sqrt{2}) = -\sqrt{2}$.

An interesting property for Galois groups of finite Galois extensions L/K is that $\#Gal(L/K) = [L : K]$ which is the degree of the field extension.
Our two first examples were field extensions of degree 2 so probably not the

most interesting ones. For this reason let us consider the rational polynomial $f(X) = X^3 - 2 \in \mathbb{Q}[X]$ which has splitting field $\mathbb{Q}(\sqrt[3]{2}; \zeta_3)$ where $\zeta_3 = e^{\frac{2\pi i}{3}}$. This is a Galois extension of degree 6. So there are 6 elements in the Galois group of f. Let us start by looking at the $\mathbb{Q}$-automorphism in $\mathbb{Q}(\zeta_3)$. The minimal polynomial of ζ_3 is $X^2 + X + 1 \in \mathbb{Q}$ and has roots ζ_3 and ζ_3^2. This gives us 2 automorphism σ_i given by $\sigma_1(\zeta_3) = \zeta_3$ and $\sigma_2(\zeta_3) = \zeta_3^2$. Now our polynomial f is still irreducible on $\mathbb{Q}(\zeta_3)$, so for each $i \in 1, 2$ we can find 3 $\mathbb{Q}$-automorphism in $\mathbb{Q}(\sqrt[3]{2}; \zeta_3)$ defined by:

- $\sigma_{i,1}(\sqrt[3]{2}) = \sqrt[3]{2}$
- $\sigma_{i,2}(\sqrt[3]{2}) = \zeta_3 \sqrt[3]{2}$
- $\sigma_{i,3}(\sqrt[3]{2}) = \zeta_3^2 \sqrt[3]{2}$

Thus giving us the 6 elements of the Galois group.

The following notion is very important for our upcoming observations. Take a separable polynomial in $K[X]$ for K a field. Then its splitting field L is a Galois extension of K. Let $a_1, ..., a_n \in L$ be the roots of the polynomial then the following application is injective:

$$\phi : Gal(L/K) \to S_n; \sigma \to \phi(\sigma) \text{ where } \sigma(a_i) = a_{\phi(\sigma)(i)}$$

This is interesting as it allows us to identify the Galois groups of polynomials of degree n with subgroups of the symmetric group S_n.
This actually makes sense since as we already mentioned the elements of the Galois groups are swapping the n roots of the polynomials and S_n is the group of permutations of n objects. So from here on we will always use the symmetric group equivalent when observing the Galois group of polynomials. Furthermore as we will work with irreducible polynomials we will only encounter transitive subgroups of S_n.

As an example let us try to identify the Galois group of the previous example with such a subgroup. We summarise the elements of the group in the following table:

	σ_1	σ_2	σ_3	σ_4	σ_5	σ_6
$\sqrt[3]{2}$	$\sqrt[3]{2}$	$\sqrt[3]{2}$	$\zeta_3\sqrt[3]{2}$	$\zeta_3\sqrt[3]{2}$	$\zeta_3^2\sqrt[3]{2}$	$\zeta_3^2\sqrt[3]{2}$
ζ_3	ζ_3	ζ_3^2	ζ_3	ζ_3^2	ζ_3	ζ_3^2

To determine the structure of this group we can recognise that it has three elements of order 2: σ_2, σ_4, σ_6 and two elements of order 3: σ_3, σ_5. Thus it is isomorphic to S_3 as the other group structure of six elements is $(\frac{\mathbb{Z}}{6\mathbb{Z}}, +)$ which has only one element of order 2.

We will not show this result for every element as it is pretty simple to see, but as an example here is the argument for the order of σ_4:

- $\sigma_4(\sigma_4(\sqrt[3]{2})) = \sigma_4(\zeta_3\sqrt[3]{2}) = \zeta_3^2 * \zeta_3\sqrt[3]{2} = \sqrt[3]{2}$
- $\sigma_4(\sigma_4(\zeta_3)) = \sigma_4(\zeta_3^2) = (\zeta_3^2)^2 = \zeta_3$

So if you relate each root of X^3-2 with the numbers 1 to 3 (for example: $\sqrt[3]{2} = 1$, $\zeta_3\sqrt[3]{2} = 2$ and $\zeta_3^2\sqrt[3]{2} = 3$) you can construct the isomorphism from the Galois group to S_3:

σ_1	σ_2	σ_3	σ_4	σ_5	σ_6
id	(2 3)	(1 2 3)	(1 2)	(1 3 2)	(1 3)

Now to show an interesting fact let us recall that by the theorem on the primitive element the expansion $\mathbb{Q}(\sqrt[3]{2}; \zeta_3)/\mathbb{Q}$ of degree 6 can be written as a simple extension $\mathbb{Q}(\zeta_3 + \sqrt[3]{2})$.
This element has minimal polynomial of degree 6 but we have seen that the Galois group of this polynomial is S_3.
By this fact we can deduce that S_3 is a transitive subgroup of S_6. Finding the transitive subgroups of S_n is not a straightforward task, especially as n gets bigger, showing the helpfulness of this kind of observations using Galois Theory.

This brings us to the experimental observations we will be trying to make in this project. We will take a finite set of irreducible polynomials of degree n and calculate their Galois groups to observe which subgroups of S_n are appearing and how often. Through this we will among other things be able to determine the transitive subgroups of S_n.

2.2 Solvability by radicals

Another interesting application of Galois Theory is to observe if a polynomial is solvable by radicals. To understand this notion, one could informally say that a polynomial is solvable by radicals if its roots can be expressed by using just the operations of addition, substraction, multiplication, division and the extraction of roots.
The more rigorous definition is based on radical extensions. Let us remind that a field L is a radical extension of a field K if there exist non-zero elements a_i and positive integers n_i for $i \in \{1, ..., r\}$ s.t.: $L = K(a_1, a_2, ..., a_r)$ and

$$\begin{aligned} a_1^{n_1} &\in K, \\ a_2^{n_2} &\in K(a_1), \\ a_3^{n_3} &\in K(a_1, a_2), \\ &\dots \\ a_r^{n_r} &\in K(a_1, a_2, ..., a_{r-1}). \end{aligned}$$

For example $L = \mathbb{Q}(\sqrt{3}, \sqrt[5]{4 - \sqrt{3}})$ is a radical extension of $\mathbb{Q}$. We just need to take $a_1 = \sqrt{3}$ and $a_2 = \sqrt[5]{4 - \sqrt{3}}$ to see:

- $L = \mathbb{Q}(a_1, a_2)$,
- $a_1^2 = 3 \in \mathbb{Q}$,
- $a_2^5 = 4 - \sqrt{3} = 4 - a_1 \in \mathbb{Q}(a_1)$.

This brings us to our formal definition:

Definition 2.2. A polynomial $P \in K[X]$ is *solvable by radicals on* K if there exists a radical extension L of K containing the splitting field of P.

Of course we know that every polynomial of degree 2 is solvable by radicals in $\mathbb{Q}[X]$ giving us the well-known general solutions for their roots.
The same is true for polynomials of degrees 3 and 4 even if their general solutions might not be as simple.

Let us illustrate this with an example of degree 4:
$f(X) = X^4 + 6X^2 - 4 \in \mathbb{Q}$ is solvable by radicals since its roots are $\pm\sqrt{-3 \pm \sqrt{17}}$. So its splitting field:

$$\begin{aligned} L &= \mathbb{Q}\left[\sqrt{-3 + \sqrt{17}}, \sqrt{-3 - \sqrt{17}}\right] \\ &= \mathbb{Q}\left[\sqrt{17}, \sqrt{-3 + \sqrt{17}}, \sqrt{-3 - \sqrt{17}}\right] \end{aligned}$$

is a radical extension of $\mathbb{Q}$.

Now to show the relation of all this with Galois Theory we need one more notion which is the solvability of a group. A group G is solvable if there is a sequence of subgroups s.t.:

- $H_0 = G \supset H_1 \supset \ldots \supset H_n = \{e\}$;
- $\forall i : H_{i-1} \trianglerighteq H_i$;
- $\forall i : \frac{H_i}{H_{i-1}}$ is abelian.

A straightforward example of a solvable group is the one of an abelian group G, as $\{e\} \trianglelefteq G$ and $\frac{G}{\{e\}} \cong G$ which clearly is abelian.
Also S_3 is an example of a solvable group as we have:

- $\{(1)\} \trianglerighteq A_3 \trianglerighteq S_3$,
- $\frac{A_3}{\{(1)\}} \cong A3$ which has order 3 thus is abelian,
- $\left|\frac{S_3}{A_3}\right| = \frac{|S3|}{|A3|} = \frac{6}{3} = 2$ and a group of order 2 is again abelian.

We will find a whole set of solvable groups using this useful theorem involving Galois Theory:

Theorem 1. *Let K be a field contained in $\mathbb{C}$ and $P \in K[X]$ with splitting field N. If P is solvable by radicals then $Gal(N|K)$ is solvable.*

So essentially if we know that a polynomial is solvable by radicals we also know that its Galois group is solvable. As we have already mentioned before every polynomial of degree 2, 3 or 4 is solvable by radicals thus through this theorem we can deduce that every subgroup of S_2, S_3 and S_4 that appear as Galois groups of such polynomials are solvable.
To deduce that every subgroup of S_2, S_3 and S_4 is solvable using this theorem we would have to prove that for each of those groups there exists a polynomial having them as a Galois group. This is an open problem for general S_n, called the Inverse Galois Problem, and we will be addressing it further in the next section.
However for $n \leq 4$ this has already been proven showing that $\forall n \leq 4$ every subgroup of S_n is solvable.

The other interesting way of using this theorem is that if a polynomial has a non-solvable Galois group then it can not be solvable by radicals.
For example S_5 is not solvable so every polynomial possessing it as a Galois group is not solvable by radicals.

For instance the polynomial $P(X) = X^5 - 10X + 5$ is not solvable by radicals as its Galois group is S_5.
This also explains why there is only a general solution for the roots of polynomials of degree less than 4, as for degrees 5 or more, not every polynomial is solvable by radicals.

2.3 Inverse Galois Problem

The *Inverse Galois Problem* is an unsolved problem that concerns whether every finite group is a Galois group of some Galois extension of $\mathbb{Q}$. This problem has first been brought up in the early 19th century. As seen above the study of the Galois groups of polynomials of degree 2, 3 or 4 shows that any subgroup of S_2, S_3 or S_4 is a Galois group of an extension of $\mathbb{Q}$.
As mentioned their has been no prove, neither for a positive nor a negative answer of this question, however for a few family of groups it has been showed that they can be achieved as Galois groups:

- Abelian groups;
- The symmetric groups S_n and the alternating groups A_n (shown by Hilbert in 1892);
- The solvable groups (Shafarevitch 1954)

Those are of course not all the results that have been found to this day but mentioning them here would go further than our capacities. However this results can of course be found in the literature.

As a conclusion even tough a lot of work has been done on this problem we are yet to answer this question. No matter what the answer is, having a proof for this problem would help making advancement on the classification of finite groups.

3 Experimental Part

3.1 Computations

In this section, we will experiment with finite sets of polynomials that are defined as follows: For $n, N \in \mathbb{N}$, let

$$\mathcal{F}_{n,N} = \{f = \sum_{i=0}^{n} a_i X^i \in \mathbb{Z}[X] | a_n = 1, |a_i| \leq N, f \text{ is irreducible}\}$$

We created [1] these sets for different values of n and N. Then, for each set, we computed the Galois group of every polynomial and determined the frequency with which each group appears. We gathered all data in the following tables.

Table for $n = 3$

	N=3	N=4	N=5	N=6	N=7
S3	216	496	976	1668	2670
C3	10	18	26	36	48

Table for $n = 4$

	N=3	N=4	N=5	N=6	N=7
S4	1382	4204	10382	21318	39660
D4	188	444	774	1258	1834
C2 x C2	9	32	46	73	94
A4	8	12	16	28	62
C4	4	20	28	52	60

Table for $n = 5$

	N=3	N=4	N=5	N=6	N=7
S5	11324	43464	126396	302258	638004
D5	78	116	198	282	430
A5	32	56	126	230	338
C5 : C4	14	44	94	130	174
C5	0	4	8	8	8

[1] We made the experiments in Sage. We limited our computations to these values of n and N because of runtime duration. The code can be found in the appendix.

Table for $n = 6$

	N=3	N=4	N=5	N=6
S6	79596	395428	1406600	3982144
(S3 x S3) : C2	1056	3900	7616	15024
C2 x S4	819	2070	4367	7833
S4	155	360	623	999
D6	108	236	402	627
C2 x A4	48	96	192	336
A6	46	126	264	684
S3 x S3	36	112	170	278
C3 x S3	28	90	124	162
A5	22	120	264	462
S3	10	21	25	34
A4	6	12	18	30
S5	6	82	160	294
C6	4	8	12	20
(C3 x C3) : C4	0	4	18	36

3.2 Observations

The first observation we can make is that for $n \in \mathbb{N}$ at least 86% of polynomials in $\mathcal{F}_{N,n}$ have S_n as Galois group. To reinforce this fact, we can ask ourselves how the proportion of S_n evolves as n and N increase.
For some positive integer N, let $P_N(S_n)$ denote the proportion of polynomials in $\mathcal{F}_{N,n}$ that have S_n as Galois group. To observe the evolution of $P_N(S_n)$, we made the following table[2] of values for $P_N(S_n)$.
For example, $P_7(S_4) = 0.950851$.

	n=3	n=4	n=5	n=6
N=3	0.955752	0.868636	0.989168	0.971394
N=4	0.964981	0.892190	0.994964	0.982027
N=5	0.974052	0.923173	0.996641	0.989967
N=6	0.978873	0.937921	0.997854	0.993310
N=7	0.982340	0.950851	0.998513	NaN

We see in the table that for any n the proportion of S_n increases with N and when n grows, that proportion gets closer to 1. The biggest proportion we have is $P_7(S_5) = 0.998513$.
We may expect that for any positive integer N, $P_N(S_n)$ converges against 1 as $n \to \infty$. These observations are confirmed by van der Waerden's conjecture

[2]The NaN value denotes a missing value because we don't have data for $n = 6$ and $N = 7$.

that has been proved recently by Manjul Bhargava [1]. Let $E_n(N) = \#\{f \in \mathcal{F}_{N,n} |$ the Galois group of f is not $S_n\}$.
Then, the van der Waerden's conjecture which is now Bhargava's theorem states as follows:

Theorem 2 (Manjul Bhargava)**.** $E_n(N) = O(N^{n-1})$

Indeed by the theorem, for any $N \in \mathbb{N}$

$$P_N(S_n) = \frac{\#\mathcal{F}_{N,n} - E_n(N)}{\#\mathcal{F}_{N,n}} = 1 - \frac{E_n(N)}{(2N+1)^n} = 1 - \frac{O(N^{n-1})}{(2N+1)^n} \longrightarrow 1$$

when $n \to \infty$.

Remark 1. Let us remind that the *big O notation* is used to describe the asymptotic behaviour of functions, telling us how fast it grows or declines.
For example take the function $f(X) = 7X^3 - 2X^2 + 75$, if we ignore the constants and the slower growing terms, we could say that f grows at the order X^3 and thus $f(X) = O(X^3)$.
Formally for some real or complex valued function f and a real valued function g which is strictly positive for large enough values we say: $f(X) = O(g(X))$ if $\exists C \in \mathbb{R}_{\geq 0}$ and $X_0 \in \mathbb{R}$ s.t.:

$$|f(X)| \leq Cg(X) \quad \forall X \geq X_0.$$

Essentially this means that f does not grow faster than g.

Another thing we can observe is that by looking at the tables we see the different transitive subgroups of S_n, for instance S_3 is a transitive subgroup of S_6. Such facts illustrate the power of Galois' theory because it's more difficult to prove such things without using these notions.

Speaking of the table for $n = 6$, we can see that it contains 15 groups whereas the other tables are smaller by a factor at least 3. Moreover, the groups in the table for $n = 6$ are less familiar and maybe more surprising than in the other tables. For example, the group $S_3^2 \rtimes C_2$ $(= (S_3 \times S_3) : C_2)$ is a subgroup of order 72 that is solvable. It's the Galois group of $x^6 - 2x^5 + x^4 + 1$.

One last thing we can ask ourselves is that for a given value of n, is there a positive integer N and a Galois group of a polynomial in $\mathcal{F}_{N,n}$ such that this Galois group is not yet in our table? If we take bigger values of N will we have more Galois groups in our tables?
Our tables indicate that for $N \geq 4$, every Galois group that we encountered

is already in the tables. One way to answer this question is to check that for $n \in \{3, 4, 5, 6\}$, every transitive subgroup of S_n is in the table, as a Galois group is necessarily a transitive subgroup of S_n.
We can do that by using the following function in Sage:

```
def trans_subgroups(n):
    """Returns a list of every transitive subgroups of Sn"""
    G = SymmetricGroup(n)
    H = [group.structure_description()
         for group in G.subgroups() if group.is_transitive()]
    return list(set(H))
```

With this function, we checked that $\forall n \in \{3, 4, 5, 6\}$ every transitive subgroup of S_n is already in our tables.
However, this question also rises another interesting one. If we had found a transitive subgroup of S_n that is not in our table, would there be a polynomial of degree n that has this subgroup as Galois group? This problem is related to the Inverse Galois Problem introduced before.

4 Conclusion

After reminding the important notions of Galois Theory we dived into some interesting theoretical applications of it, such as observing the transitive subgroups of the symmetrical group or the solvability by radicals of polynomials. We shortly introduced the open Inverse Galois Problem before moving on to the experimental part where we computed the Galois groups of finite sets of irreducible polynomials. We observed the resulting groups and their frequencies to make some interesting findings. For example we noticed that the proportion of polynomials in our set that have S_n as a Galois group converges to 1 when n grows, which has been proven a few months ago by Manjul Bhargava. Additionally we observed that for $n = 3, 4, 5, 6$ every transitive subgroup of S_n can be achieved as a Galois group which answers the Inverse Galois Problem for those specific values of n.

Even though we did acquire a lot of new knowledge on Galois Theory and its application through this project, we also realised that there is an abundance of findings that we could still make on this subject. This is especially well shown by the Inverse Galois Problem that has still not been solved. As a conclusion we really enjoyed working on this project and think that, we could still have kept it going by digging deeper into some of the topics or even introducing other applications of the Galois theory.

References

[1] Manjul Bhargava. Galois groups of random integer polynomials and van der waerden's conjecture. 2021.

[2] Jean-Pierre Escofier. *Théorie de Galois : cours et exercices corrigés*. Sciences Sup. Dunod, Malakoff, 2e éd.. edition, 2020.

[3] Jean-Pierre Azra, Robert Bourgne. Galois Évariste - (1811-1832). `http://www.universalis-edu.com/encyclopedie/evariste-galois/`. Accessed: 2021-12-26.

[4] Gabor Wiese. Algèbre, september 2020.

Appendices

Here is the functions we used to create the sets $\mathcal{F}_{N,n}$ and make the tables in section 3.1.

```
R.<x>=PolynomialRing(QQ)
gen_set_F = lambda N, n: [R(list(coef)+[1]) for coef in
    cartesian_product([range(-N,N+1)]*n)]
gen_F_irred = lambda F: [pol for pol in F if pol.is_irreducible
    ()]

def procedure(N,n):
    """Generates the set F_{N,n}, compute the Galois group for
    every irreducible polynomial in this group
    Return a dictionnary with every Galois group and their
    occurences."""
    F = gen_set_F(N,n)
    F_irred = gen_F_irred(F)
    groups = {}
    for pol in F_irred:
        G = pol.galois_group().structure_description()
        groups[G] = groups.get(G,0)+1
    return groups
```