Distribution of Galois groups

Da Cruz Rebelo Tania
Da Silva Carregueira Sara
Capesius Nicolas

supervised by
Belmans Pieter

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

Abstract

Consider the set
$\{p(x) = x^n + a_{n-1}x^{n-1} + ... + a_1x + a_0 \in \mathbb{Z}[x] |\ p \text{ irred.}, \forall i = 0, ..., n-1, |a_i| < M\}$
of monic irreducible polynomials of bounded height M. We will study the distribution of the Galois groups of splitting fields in this set, and how low values of M predict the asymptotic behaviour for M large.

Contents

1 Theory

Introduction

Consider the set of monic irreducible polynomials in the ring $\mathbb{Q}[X]$. We are interested in studying the distribution of their Galois groups by using experimental methods. Therefore we have to restrict ourselves to finite subsets of this infinite set. This can be achieved by considering, for fixed $n \in \mathbb{N}$, the set of monic irreducible polynomials $p(x) = x^n + a_{n-1}x^{n-1} + ... + a_1x + a_0 \in \mathbb{Q}[X]$ such that:

- $\forall i \in \{0, 1, ..., n-1\}: a_i \in \mathbb{Z}$
- $\forall i \in \{0, 1, ..., n-1\}: |a_i| < M$, for some constant $0 < M \in \mathbb{N}$
- increasing M to see which groups will appear most often as M gets large

Since these sets are finite the Galois groups $\mathrm{Gal}(p(x))$ can be computed in a finite amount of time. We will use SageMath for our calculations.

1.1 Groups

We begin by recalling the symmetric group, and its subgroups, in order to better understand the results we will get from our computations.

Definition (**Symmetric group**). Let X be a finite set of size $n \in \mathbb{N}$. The set

$$S_X = \{f: X \to X \mid f \text{ is a bijection } \}$$

equipped with the operation of function composition $\circ$ and the identity map id forms a group $(S_X, \circ, id)$. We will denote it S_n and call it the the **symmetric group**.

Suppose $X = \{x_1, ..., x_n\}$, then there are n ways to choose $f(x_1)$. After that, there are $(n-1)$ ways to choose $f(x_2)$ because f is injective. Repeating this argument for every element in X we arrive at the result that there are $n \times (n-1) \times ... \times 1 = n!$ possible bijections. Thus the **order of the symmetric group** is $n!$. Since $f \in S_n$ maps every element in X to a unique element in X, it rearranges the elements of the set.

Another family of groups are cyclic groups. These are the groups that can be generated by a single element.

Definition (**Cyclic group**). We say that a group $(G, \cdot, 1)$ is **cyclic** if there exists an element $g \in G$ such that:

$$G = \{g^k: k \in \mathbb{Z}\}$$

Example. Two important examples are $(\mathbb{Z}, +, 0)$ which can be generated by -1 and 1 as well as the integers modulo n $(\mathbb{Z}/n\mathbb{Z}, +, 0)$ which can be generated by 1, because any *infinite* cyclic group is isomorphic to $\mathbb{Z}$ and any *finite* cyclic group is isomorphic to $\mathbb{Z}/n\mathbb{Z}$.

Example. Consider the polynomial $z^n - 1 \in \mathbb{C}[z], n \in \mathbb{N}$ its roots $z = e^{2k\pi i/n}, k \in \{1, ..., n\}$ form a group that is generated by $\zeta_n = e^{2\pi i/n}$

Definition (**Dihedral group**). The **dihedral group** is noted D_n and has order $2n$. It is the group of symmetries, like rotations and reflections, of a regular polygon.

Definition (**Alternating group**). The **alternating group** is the group of even permutations. On a set of n elements, it is called the alternating group of degree n. It is denoted by A_n or $Alt(n)$.

Definition (**Frobenius group**). A **Frobenius group**, denoted F_{p^n}, where p is a prime number, is a transitive permutation group on a finite set such that no non-trivial element fixes more than one point and some non-trivial element fixes a point.

Definition (**Group action**). Let G be a group and X be a set. A **group action** on the set X is a map $G \times X \to X,\ (g, x) \to gx$ such that :

1. $\forall x \in X : 1x = x$
2. $\forall g, h \in G, \forall x \in X : g(hx) = (gh)x$

For each $x \in X$ the set $O(x) = \{gx : g \in G\} \subseteq X$ is called the **orbit** of x under the group action of G. Furthermore it is called **transitive** if there is only one orbit, that is,

$$\forall x, y \in X\ \exists g \in G \colon gx = y$$

For each $x \in X$ the **stabilizer** is the set of elements that keep x fixed:

$$Stab(x) = \{g \in G \colon gx = x\}$$

Definition (**Solvable group**). Let G be a group. We say that G is **solvable** if there exists a series of subgroups of $\{1\} = G_0 \leq G_1 \leq ... \leq G_n = G$ such that for every $i \in \{1, ..., n\}$:

1. $G_{i-1} \trianglelefteq G_i$
2. G_i/G_{i-1} is abelian

Useful in this context are simple groups, that is, groups G who only have $\{1\}$ and G as normal subgroups. Since every abelian group is normal the subgroups of abelian groups are also all normal. Thus an abelian group is simple if and only if it has no subgroups other than $\{1\}$ and itself.
It can be shown that $\forall n \geq 5 :\ A_n$ is simple. Using this, we see that $\forall n \geq 5 :\ S_n$ is not solvable. Because suppose by contradiction that S_n were solvable. Then all its subgroups would also be solvable. But, knowing that A_n is simple, we have that it is not solvable, namely $\{1\} \trianglelefteq A_n$ and $A_n/\{1\} = A_n$ is not abelian. Thus we get a contradiction.

Theorem 1 (**Orbit-Stabiliser theorem**). Let G be a group which acts on a finite set X. Let $x \in X$. Let $O(x)$ denote the orbit of x. Let $Stab(x)$ denote the stabilizer of x by G. Let $[G : Stab(x)]$ denote the index of $Stab(x)$ in G. Then :

$$|O(x)| = [G : Stab(x)] = \frac{|G|}{|Stab(x)|}$$

1.2 Polynomials and Fields

In group theory we usually are interested in studying subgroups of groups. In field theory we do the opposite. Given a monic irreducible polynomial $p(x) = x^n + a_{n-1}x^{n-1} + ... + a_1x + a_0 \in \mathbb{Q}[X]$ we want to extend our base field $\mathbb{Q}$ to a larger field over which the polynomial splits. If F is a field such that $\mathbb{Q} \subseteq F$, then we will call F a **field extension** of $\mathbb{Q}$ and denote it $F/\mathbb{Q}$. We want to find the smallest extension field of $\mathbb{Q}$ over which the polynomial splits into linear factors.
Thus we call F a **splitting field** of $p(x)$ if :

- $p(x) = (x - a_1)(x - a_2)...(x - a_n) \in F[X]$
- if $\mathbb{Q} \subseteq E \subseteq F$ is an intermediate field over which $p(x)$ splits, then $E = F$

Consider the polynomial $p(x) = x^2 - 2 \in \mathbb{Q}[X]$ it does not split over $\mathbb{Q}$ because it has a root $\sqrt{2} \notin \mathbb{Q}$. Thus $p(x)$ splits of $\mathbb{R}$, but that is not the smallest field. We can create the splitting field $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \colon a, b \in \mathbb{Q}\}$ by adjoining the root to $\mathbb{Q}$. It can be shown, with simple arithmetic, that this set satisfies the field axioms. Furthermore, it is the smallest extension field of $\mathbb{Q}$ that contains $\sqrt{2}$. If we interpret $a, b \in \mathbb{Q}$ as 'scalars' and the elements in $\mathbb{Q}(\sqrt{2})$ as 'vectors', then we see that $\mathbb{Q}(\sqrt{2})$ is a vector space and that $\{1, \sqrt{2}\}$ forms a basis of this vector space.
Thus we arrive at the notion of **the degree of a field extension**. If $F/\mathbb{Q}$ is a field extension, then we call the degree of the extension, denoted $[F : \mathbb{Q}]$, the dimension of the associated vector space.

Let F be a field, then the following set :

- $\phi \colon F \to F$ such that ϕ is a bijection
- $\forall x, y \in F \colon \phi(x + y) = \phi(x) + \phi(y)$ and $\phi(x \cdot y) = \phi(x) \cdot \phi(y)$

equipped with function composition and the identity map id forms a group called **the automorphism group** of F denoted $Aut(F)$. For a field extension $E \subseteq F$, the automorphisms ϕ such that $\forall x \in E \colon \phi(x) = x$, form a subgroup of $Aut(F)$, denoted $Aut(F/E)$, and are called E- automorphisms of F. For our case $Aut(F/\mathbb{Q})$ we have :

If $\mathbb{Q} \subseteq F$, $\phi \in Aut(F/\mathbb{Q})$, $q \in \mathbb{Q}$, then $1 \in F$ and there exist $m, n \in \mathbb{Z}, n \neq 0$ such that $q = \frac{m}{n}$. Since ϕ is an automorphism we have that

$$\phi(n) = \phi(1 + \cdots + 1) = n\phi(1) = n$$

Thus

$$\phi(q) = \phi(\frac{m}{n}) = \phi(m)\phi(\frac{1}{n}) = \phi(1 + \cdots + 1)\frac{1}{\phi(n)} = \frac{m}{n} = q$$

So that the elements $q \in \mathbb{Q}$ are kept fixed by the automorphisms in F. Therefore, $Aut(F) = Aut(F/\mathbb{Q})$ for every field F such that $\mathbb{Q} \subseteq F$.

Note that this is true for every prime field.

Definition (**Galois group**). Let $p(x) \in \mathbb{Q}[X]$ be a monic irreducible polynomial and F be its splitting field, then the **Galois group** of the polynomial is

$$Gal(p(x)) = Aut(F)$$

Suppose $\phi \in \text{Gal}(p(x))$ and $\alpha \in F$ is a root of $p(x) = x^n + a_{n-1}x^{n-1} + ... + a_1x + a_0$, then

$$\alpha^n + a_{n-1}\alpha^{n-1} + ... + a_1\alpha + a_0 = 0$$

$$\Rightarrow \phi(\alpha^n + a_{n-1}\alpha^{n-1} + ... + a_1\alpha + a_0) = \phi(0) = 0$$

Thus, since ϕ is an automorphism, we have that

$$\phi(\alpha)^n + \phi(a_{n-1})\phi(\alpha)^{n-1} + ... + \phi(a_1)\phi(\alpha) + \phi(a_0) = 0$$

$$\Rightarrow \phi(\alpha)^n + a_{n-1}\phi(\alpha)^{n-1} + ... + a_1\phi(\alpha) + a_0 = 0$$

This shows that $\phi(\alpha)$ is also a root of the polynomial $p(x)$. Let $R = \{\alpha_1, ..., \alpha_n\}$ be the set of roots of the polynomial. Then, since $\text{Gal}(F/\mathbb{Q})$ is a set of bijections, the Galois group permutes the set X. This explains why $\text{Gal}(p(x)) \leq S_n$. Let $F = \mathbb{Q}(x_1, ..., x_n)$ be the splitting field generated by adjoining to $\mathbb{Q}$ the set of roots. Since the $\mathbb{Q}$-automorphisms keep $\mathbb{Q}$ fixed we can determine the elements of the Galois group by how they act on the set of roots. In our case, where the polynomial $p(x)$ is irreducible, we also have that the $\text{Gal}(p(x))$ defines a transitive group action on the set R. In our experimentations we will test if these are indeed the groups that will appear.

Example 1.1. For the polynomial $p(x) = x^2 - 2$ we have the following:

(a) The splitting field of $p(x)$ is $\mathbb{Q}(\sqrt{2})$.

(b) The $\mathbb{Q}$-automorphisms of $p(x)$ are:

$$id : \sqrt{2} \longmapsto \sqrt{2}$$
$$\sigma : \sqrt{2} \longmapsto -\sqrt{2}$$

(c) $\text{Gal}(p) = \{id, \sigma\} \cong C_2$

We have that $\sigma \cdot \sigma = id$, because $(\sigma \cdot \sigma)(\sqrt{2}) = \sigma(\sigma(\sqrt{2})) = \sigma(-\sqrt{2}) = \sqrt{2} = id(\sqrt{2})$. So, the group G is the same as C_2, the cyclic group of order 2, or S_2, the symmetric group of order 2, because we have a single element σ with $\sigma^2 = \sigma \cdot \sigma = 1$ the identity on the group.

Example 1.2. For the polynomial $p(x) = x^4 - 5x^2 + 6$ we have the following:

(a) The splitting field of $p(x)$ is $\mathbb{Q}(\sqrt{2}, \sqrt{3})$.

(b) The $\mathbb{Q}$-automorphisms of $p(x)$ are:

$$id : \sqrt{2} \longmapsto \sqrt{2} \qquad \sigma_1 : \sqrt{2} \longmapsto -\sqrt{2}$$
$$\sqrt{3} \longmapsto \sqrt{3} \qquad \sqrt{3} \longmapsto \sqrt{3}$$

$$\sigma_2 : \sqrt{2} \longmapsto \sqrt{2} \qquad \sigma_3 : \sqrt{2} \longmapsto -\sqrt{2}$$
$$\sqrt{3} \longmapsto -\sqrt{3} \qquad \sqrt{3} \longmapsto -\sqrt{3}$$

(c) $\mathrm{Gal}(\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}) = \mathrm{Gal}(p) = \{id, \sigma_1, \sigma_2, \sigma_3\} \cong V_4$

Notice that

- $\sigma_i \cdot \sigma_i = id$ for $i = 1, 2, 3$
- $\sigma_1 \cdot \sigma_2 = \sigma_3$

So there are three elements of order 2, and $\mathrm{Gal}(\mathbb{Q}(\sqrt{2},\sqrt{3}) = \langle \sigma_1, \sigma_2 \rangle$. To see the connection with the symmetric group we label the roots of $p(x)$: $\sqrt{2} \to 1$, $-\sqrt{2} \to 2$, $\sqrt{3} \to 3$ and $-\sqrt{3} \to 4$. Then we see that $\sigma_1 = (12)$, $\sigma_2 = (34)$ and $\sigma_3 = (12)(34)$. So that

$$\mathrm{Gal}(p(x)) = \{(), (12), (34), (12)(34)\} = \langle (12), (34) \rangle \cong V_4 \leq S_4$$

Where V_4 is the Klein four group. It has three non trivial, cyclic subgroups of order 2 : $\langle (12) \rangle$, $\langle (34) \rangle$ and $\langle (12)(34) \rangle$

Example 1.3. For the polynomial $p(x) = x^3 - 2$ we have the following:

(a) The splitting field of $p(x)$ is $\mathbb{Q}(\sqrt[3]{2}, \zeta)$.

(b) The $\mathbb{Q}$-automorphisms of $p(x)$ are:

$$\begin{array}{lll} id : \zeta \longmapsto \zeta & \sigma_1 : \zeta \longmapsto \zeta^2 & \sigma_2 : \zeta \longmapsto \zeta \\ \quad \sqrt[3]{2} \longmapsto \sqrt[3]{2} & \quad \sqrt[3]{2} \longmapsto \sqrt[3]{2} & \quad \sqrt[3]{2} \longmapsto \zeta\sqrt[3]{2} \end{array}$$

$$\begin{array}{lll} \sigma_3 : \zeta \longmapsto \zeta & \sigma_4 : \zeta \longmapsto \zeta^2 & \sigma_5 : \zeta \longmapsto \zeta^2 \\ \quad \sqrt[3]{2} \longmapsto \zeta^2\sqrt[3]{2} & \quad \sqrt[3]{2} \longmapsto \zeta\sqrt[3]{2} & \quad \sqrt[3]{2} \longmapsto \zeta^2\sqrt[3]{2} \end{array}$$

(c) $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2}, \zeta)/\mathbb{Q}) \cong S_3$

We have $\mathrm{Gal}(p) = \{id, \sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5\}$. Notice that

$$\sigma_2^2(\zeta) = \zeta$$

$$\sigma_2^2(\sqrt[3]{2}) = \sigma_2(\zeta\sqrt[3]{2}) = \sigma_2(\zeta)\sigma_2(\sqrt[3]{2}) = \zeta^2\sqrt[3]{2}$$

Hence

$$\sigma_2^2 = \sigma_3$$

Furthermore

$$\sigma_1(\sigma_2(\zeta)) = \zeta^2$$

$$\sigma_1(\sigma_2(\sqrt[3]{2}) = \sigma_1(\zeta\sqrt[3]{2}) = \sigma_1(\zeta)\sigma_1(\sqrt[3]{2}) = \zeta^2\sqrt[3]{2}$$

Thus

$$\sigma_1 \cdot \sigma_2 = \sigma_5$$

Similar calculations show that $\sigma_1\sigma_2^2 = \sigma_4$, $\sigma_1^2 = \sigma_2^3 = id$ and $\sigma_2\sigma_1 = \sigma_1\sigma_2^2$. Hence, Gal($p$) = $\langle\sigma_1, \sigma_2\rangle$
Now we label the roots of p : $\sqrt[3]{2} \to 1$, $\zeta\sqrt[3]{2} \to 2$ and $\zeta^2\sqrt[3]{2} \to 3$. Then, since $\sigma_1(\sqrt[3]{2}) = \sqrt[3]{2}$, $\sigma_1(\zeta\sqrt[3]{2}) = \zeta^2\sqrt[3]{2}$ and $\sigma_1(\zeta^2\sqrt[3]{2}) = \zeta\sqrt[3]{2}$, we see that $\sigma_1 = (23)$. And, similarly, we see that $\sigma_2 = (123)$. The symmetric group S_3 is generated by $\langle(23), (123)\rangle$. Furthermore (23) and (123) satisfy the same relations as σ_1 and σ_2 above. For example :

$$(123)(123)(123) = (123)(132) = id$$

$$(23)(23) = id$$

$$\sigma_1\sigma_2 = (23)(123) = (13) = \sigma_5$$

$$\sigma_1\sigma_2^2 = (23)(123)(123) = (23)(132) = (12) = \sigma_4$$

From this we can then conclude that $Gal(p)$ is isomorphic to S_3.
Alternatively, we arrive at same result, in the following way: Each $\sigma \in \text{Gal}(\mathbb{Q}(\sqrt[3]{2}, \zeta)/\mathbb{Q})$ is determined by its effect on the 3 roots of the polynomial $x^3 - 2$, which we have seen in 1.3, are $\sqrt[3]{2}, \zeta\sqrt[3]{2}, \zeta^2\sqrt[3]{2}$. There are at most 6 permutations of these 3 roots, and since we know there are 6 automorphisms, every permutation of the roots comes from an automorphism of the field extension. Therefore $\text{Gal}(\mathbb{Q}(\sqrt[3]{2}, \zeta)/\mathbb{Q}) \cong S_3$ or $\text{Gal}(\mathbb{Q}(\sqrt[3]{2}, \zeta)/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. To show that $\text{Gal}(\mathbb{Q}(\sqrt[3]{2}, \zeta)/\mathbb{Q}) \cong S_3$ we need to show that the Galois group is not abelian. In fact we have that $\sigma_1 \circ \sigma_4 \neq \sigma_4 \circ \sigma_1$. Thus, $\text{Gal}(\mathbb{Q}(\sqrt[3]{2}, \zeta)/\mathbb{Q}) \cong S_3$.

Note that we can also write $\mathbb{Q}(\sqrt[3]{2}, \zeta) = \mathbb{Q}(a)$, where a is a primitive element. For instance we can choose $a = \sqrt[3]{2} + \zeta$. Then we have that $mipo_a \in \mathbb{Q}[x]$ such that $\mathbb{Q}(a)$ is the splitting field. Then $\text{Gal}(mipo_a) = S_3$ but $deg(mipo_a) = [\mathbb{Q}(a) : \mathbb{Q}] = 6$. **Hence $S_3 \leq S_6$ is a transitive subgroup**.

1.2.1 The fundamental theorem of Galois Theory

The fundamental theorem of Galois Theory establishes a one-to-one correspondence between subgroups of the Galois group of a field extension E/F and the intermediate fields between E and F. This result gives us the ability to use methods of group theory to solve problems in field theory. For example, the question whether a polynomial is solvable by radicals will be converted to the question whether the Galois group of the polynomial is solvable.

Corollary 2. Let G be a finite group of automorphisms of a field E; then

$$G = Aut(E/E^G)$$

Proof. As $G \subset Aut(E/E^G)$, we have inequalities

$$\left[E : E^G\right] \leq (G : 1) \leq (Aut(E/E^G) : 1) \leq \left[E : E^G\right]$$

□

Corollary 3. Let $E \supset M \supset F$; if E is Galois over F, then it is Galois aver M.

Proof. We know E is the splitting field of some separable $f \in F[X]$; it is also the splitting field of f regarded as an element of $M[X]$. □

Let E be an extension of F. A subextension of E/F is an extension M/F with $M \subset E$, i.e., a field M with $F \subset M \subset E$. When E is Galois over F, the subextensions of E/F are in one-to-one correspondence with the subgroups of Gal(E/F). More precisely, there is the following statement.

Theorem 4 (**Fundamental Theorem of Galois Theory**). Let E be a Galois extension of F with Galois group G. The map $H \mapsto E^H$ is a bijection from the set of subgroups of G to the set of subextensions of E/F ,

$$\{\text{subgroups } H \text{ of } G\} \overset{1:1}{\longleftrightarrow} \{\text{subextensions F} \subset M \subset E\ \},$$

with inverse $M \mapsto Gal(E/M)$. Moreover,

(a) the correspondence is inclusion-reversing: $H_1 \supset H_2 \iff E^{H_1} \subset E^{H_2}$;

(b) indices equal degrees: $(H_1 : H_2) = [E^{H_2} : E^{H_1}]$;

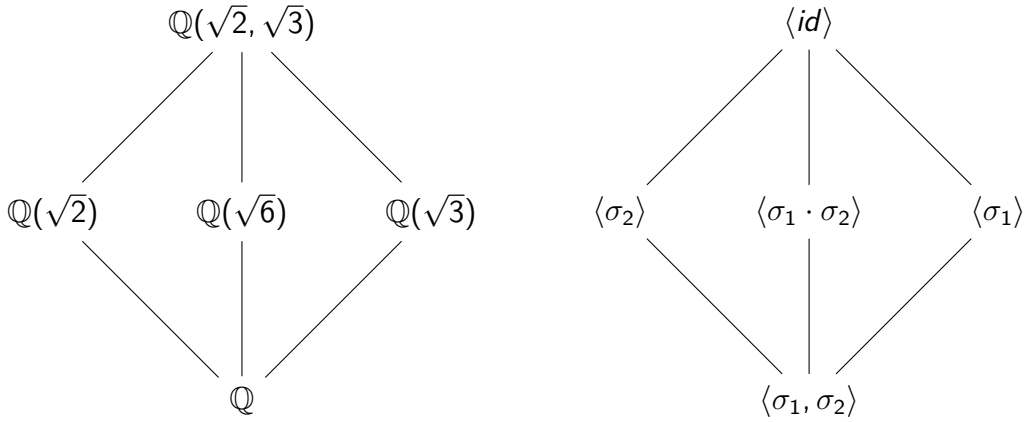
(c) $\sigma H \sigma^{-1} \iff \sigma M$, i.e., $E^{\sigma H \sigma^{-1}} = \sigma(E^H)$, $Gal(E/\sigma M) = \sigma Gal(E/M)\sigma^{-1}$;

(d) H is normal in $G \implies E^H$ is normal (hence Galois) over F, in which case

$$Gal(E^H/F) \simeq G/H$$

Example. Taking the polynomial $p(x) = x^4 - 5x^2 + 6$ we have $\text{Gal}(p) = \langle \sigma_1, \sigma_2 \rangle$ as we have seen in example 1.2. Notice that :

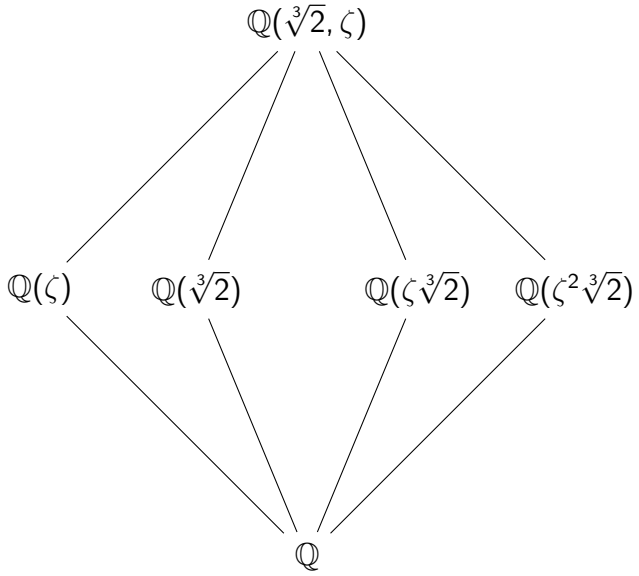
- the fixed field of $\langle id \rangle$ is $\mathbb{Q}(\sqrt{2}, \sqrt{3})$
- the fixed field of $\langle \sigma_1 \rangle = \langle (12) \rangle$ is $\mathbb{Q}(\sqrt{3})$
- the fixed field of $\langle \sigma_2 \rangle = \langle (34) \rangle$ is $\mathbb{Q}(\sqrt{2})$
- the fixed field of $\langle \sigma_1 \cdot \sigma_2 \rangle = \langle (12), (34) \rangle$ is $\mathbb{Q}(\sqrt{6})$

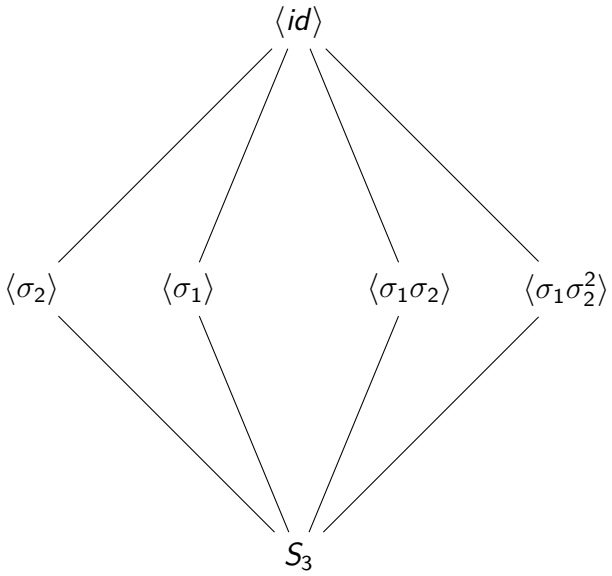


Example. Taking the polynomial $p(x) = x^3 - 2$, we have $\text{Gal}(p) = \langle \sigma_1, \sigma_2 \rangle$ as we have seen in example 1.3. Notice that :

- the fixed field of $\langle id \rangle$ is $\mathbb{Q}(\sqrt[3]{2}, \zeta)$

- the fixed field of $\langle \sigma_2 \rangle = \langle (123) \rangle$ is $\mathbb{Q}(\zeta)$
- the fixed field of $\langle \sigma_1 \rangle = \langle (23) \rangle$ is $\mathbb{Q}(\sqrt[3]{2})$
- the fixed field of $\langle \sigma_1 \sigma_2 = \sigma_5 \rangle = \langle (13) \rangle$ is $\mathbb{Q}(\zeta \sqrt[3]{2})$
- the fixed field of $\langle \sigma_1 \sigma_2^2 = \sigma_4 \rangle = \langle (12) \rangle$ is $\mathbb{Q}(\zeta^2 \sqrt[3]{2})$





1.2.2 The inverse Galois problem

Out of curiosity, one can ask whether given a field F and a finite group G there exists a polynomial with coefficients in the field F whose Galois group over F is isomorphic to the given group G?

This question has been solved for some fields and one can look it up. Among the fields where the problem has a solution, $\mathbb{C}(t)$ is the most distinguishable.

One can also ask whether every finite group appears as the Galois group of some polynomial $p \in \mathbb{Q}[x]$. In other words, we ask when given a finite group G and the field $\mathbb{Q}$, is there a Galois extension $K/\mathbb{Q}$ such that $\mathrm{Gal}(K/\mathbb{Q}) \cong G$?

This problem dates back to Hilbert, who realized S_n and A_n over $\mathbb{Q}$. Since 1892 many more groups have been realized over $\mathbb{Q}$. Shafarevich completed in 1958 the work begun by Scholz in 1936 and Reichardt in 1937, and realized all solvable groups over $\mathbb{Q}$.

2 Experimentation

2.1 Which groups can appear?

The Galois group G of an irreducible polynomial f of degree n over F permutes all the n different roots of f and therefore it has to be a transitive subgroup of S_n.

We used the following document to list the different transitive subgroups: `https://people.maths.bris.ac.uk/~matyd/GroupNames/T31.html`

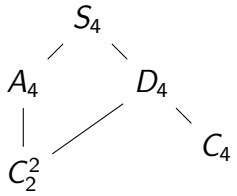
Let's look at the transitive subgroups of the symmetric group:

For a polynomial of degree 3, there are 2 transitive subgroups of S_3:

order	name
3	$A_3 = C_3$
6	S_3

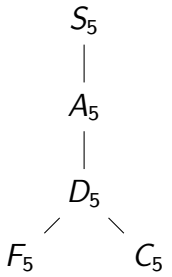
For a polynomial of degree 4 there are 5 transitive subgroups of S_4:

order	name
4	C_4
4	$C_2 x C_2 = V_4$
8	D_4
12	A_4
24	S_4



For a polynomial of degree 5 there are 5 transitive subgroups of S_5:

order	name
5	C_5
10	D_5
20	F_5
60	A_5
120	S_5



For a polynomial of degree 6 there are 15 transitive subgroups of S_6:

order	name
6	C_6
6	S_3
12	D_6
12	A_4
18	$C_3 \times S_3$
24	$C_2 \times A_4$
24	S_4
36	S_3^2
36	$C_3^2 \rtimes C_4$
48	$C_2 \times S_4$
60	A_5
72	$S_3 \wr C_2$
120	S_5
360	A_6
720	S_6

Here $\rtimes$ denotes the semi-direct product and $\wr$ denotes the wreath product. We are not going to define these notations here.

2.2 Program

Let's look at the program in SageMath that computed the Galois groups for us. In this program we define a function called Galois Groups that takes two inputs. The first is M, the bound on the coefficients of the polynomials and the second is N, the degree of the polynomials we are considering.

```
def Galois_Groups(M,N):
    R.<x> = QQ[]
    for i in range(1,M):
        C = cartesian_product([range(-i,i+1)]*N)
        d = {}
        m = C.cardinality()
        for k in range(0,m) :
            f = R(list(C[k])+[1])
            if f.is_irreducible():
                G = f.galois_group()
                S = G.structure_description()
                if S in d:
                    d.update( { S:d[S]+1 } )
                else:
                    d.update({S:1})
        print(i)
        print(d)
```

- we define an empty dictionary d to collect and count the Galois groups
- we determine if the polynomial f is irreducible and calculate its Galois group
- if the Galois Groups is already in the dictionary as a key we increase the associated value by 1
- if not we store the Galois group as a key and give it the value 1

To count the number of irreducible polynomials we defined the function irreducible which takes the same inputs.

```
def irreducible(M,N):
    R.<x> = QQ[]
    for i in range(1,M):
        C = cartesian_product([range(-i,i+1)]*N)
        ir = 0
        r = 0
        m = C.cardinality()
        for k in range(0,m) :
            f = R(list(C[k])+[1])
            if f.is_irreducible():
                ir = ir + 1
            else :
                r = r + 1
    print(ir)
    print(r)
```

2.2.1 Polynomials of degree 3

For polynomials of degree 3, we find 2 different groups: cyclic and symmetric groups. Furthermore, for height 9, we find that 83.9% of polynomials are irreducible.

height	1	2	3	4	5	6	7	8	9
S_3	12	68	216	496	976	1668	2670	3972	5654
$A_3 = C_3$	0	4	10	18	26	36	48	64	102

The full symmetric group S_n appears most often. For height 9, we see that 98.2% of irreducible polynomials have Galois group S_3.

2.2.2 Polynomials of degree 4

For the polynomials of degree 4 we find more groups. The higher the degree, the more groups we find. For polynomials of degree 4 we find 4 different groups. We have cyclic, symmetric, dihedral and alternating groups. Furthermore, for height 9, we find that 85.8% of polynomials are irreducible.

height	1	2	3	4	5	6	7	8	9
S_4	20	274	1382	4204	10382	21318	39660	67198	107652
D_4	10	70	188	444	774	1258	1834	2790	3808
C_4	2	2	4	8	10	52	60	76	92
$C_2 \times C_2$	2	6	9	32	46	73	94	129	174
A_4	0	2	8	12	16	28	62	86	130

Now let's take a look at the polynomials of degree 4. Here, we have more groups that appear. We have: S_4, D_4, C_4, $C_2 \times C_2$, and A_4. We notice that the dominant group is S_4. For height 9 we have that 96.2% of irreducible polynomials have Galois group S_4.

2.2.3 Polynomials of degree 5

height	1	2	3	4	5	6
S_5	104	1790	11324	43464	126396	302258
A_5	0	8	32	56	126	230
F_5	0	4	14	44	94	130
D_5	0	10	78	116	198	282
C_5	0	0	0	4	8	8

For the polynomials of degree 5, we see again that S_5 is the dominating group. For height 6, we see that 99.7% of irreducible polynomials have S_n as Galois group. And that 81.5% of polynomials are irreducible.

2.2.4 Polynomials of degree 6

height	1	2	3
S_6	240	8672	79596
S_4	20	59	155
$C_2 \times S_4$	18	167	819
D_6	2	46	108
$S_3 \wr C_2$	8	278	1056
C_6	4	4	4
A_5	0	4	22
$S_3 \times S_3$	0	8	36
$C_2 \times A_4$	0	8	48
A_6	0	4	46
A_4	0	2	6
$C_3 \times S_3$	0	12	28
S_5	0	0	6
S_3	0	0	10
$C_3^2 \rtimes C_4$	0	0	0

For polynomials of degree 6, we confirm again that the dominating group is S_6. Here we see that not all Galois groups appear yet because we only go to height 3. Furthermore, for height 3, we find that 69.6% of polynomials are irreducible.

2.3 Conclusion

For every degree, as the bound M on the coefficients gets large, we notice that :

- most polynomials are irreducible
- most irreducible polynomials have S_n as Galois group

For example, for polynomials of degree 3 and height 9, we have that 83.9% of polynomials are irreducible, and 98.2% of irreducible polynomials have Galois group S_3. From these results we arrive at the following questions:
For very large M

- are most monic polynomials of degree n irreducible and have Galois group S_n ?
- what is the probability that a random monic irreducible polynomial has the full symmetric group as Galois group ?

To answer quantitative questions like these one can use big O notation. For functions $f, g\colon \mathbb{N} \to \mathbb{N}$ we say that f is big O of g as n goes to infinity and write $f(n) = O(g(n))$ if there exist constants $K, N > 0$ such that :

$$\forall n \geq N\colon f(n) \leq Kg(n)$$

Next we define the following sets :
The set

$$A_n(M) = \{p \in \mathbb{Z}[X]\colon deg(p) = n, \text{p is monic}, \max_{1\leq i\leq n-i}\{|a_i|\} \leq M\}$$

of polynomials of degree n with integer coefficients bounded by M. Notice that there are $(2M+1)^n$ elements in this set. Since this is how many order pairs $(a_0, \dots, a_n - 1)$ one can form with coefficients drawn from $\{-M, \dots, -1, 0, 1, \dots, +M\}$. This means that

$$A_n(M) = O(M^n)$$

The subset :

$$B_n(M) = \{p \in A_n(M)\colon p \text{ is irreducible}\}$$

It is known that

$$\#B_n(M) = O(M^n)$$

To quantify how many polynomials have the full symmetric group as Galois group we define the following sets :
The set of polynomials in $A_n(M)$ with Galois group S_n :

$$C_n(M) = \{p \in A_n(M)\colon \text{Gal}(p) = S_n\}$$

And the complement :

$$D_n(M) = \{p \in A_n(M)\colon \text{Gal}(p) \neq S_n\}$$

Note that, then we have the following disjoint union :

$$B_n(M) = C_n(M) \bigsqcup D_n(M)$$

B.L. van der Waerden [3] [4] showed that

$$\frac{\#C_n(M)}{\#A_n(M)} \to 1$$

as M goes to infinity. And that for a random polynomial in $A_n(M)$

$$Prob(\text{Gal}(p) = S_n) \geq 1 - O(M^{-1/6})$$

Thus :

$$Prob(\text{Gal}(p) = S_n) = 1 \text{ as } M \to \infty$$

$O(M^{-1/6})$ is an error term that tells us how fast the $Prob(\text{Gal}(p) = S_n)$ tends to one.

References

[1] Gabor Wiese Algèbre

[2] Gabor Wiese Structures Mathématiques

[3] Hanson Hao, Eli Navarro, Henri Stern Irreducibility and Galois Groups of Random Polynomials

[4] B.L. van der Waerden Die Seltenheit der reduziblen Gleichungen und der Gleichungen mit Affekt.