POLITECNICO DI TORINO

Department of Mathematical Sciences, DISMA

Climbing Galois Mountain

A visual interpretation of Galois Theory

Supervisor
Prof. Antonio J. Di Scala

Student
Gessica Alecci

Academic Year 2018-2019

To Salvatore

Summary

Since ancient time mathematicians have been concerned with the process of solving polynomial equations. As early as 2000 B.C., the Babylonians could solve pairs of simultaneous equations of the form: *find two numbers given their sum and their product* [St]. The way to solve it was transmitted orally in this way:

1. Take half of their sum;
2. Square the result;
3. From this subtract their product;
4. Take the square root of the result;
5. Add this to half of their sum; this is one of the two numbers and the other one is their product minus the first one.

In terms of equations this is equivalent to:

$$\begin{cases} x + y = p \\ xy = q \end{cases} \tag{1}$$

that is the quadratic equation $x^2 + q = px$. The solution has been reduced to a formula by the Indian mathematician Brahmagupta [St] and nowadays is known as

$$x, y = \frac{p \pm \sqrt{p^2 - 4q}}{2}$$

The (1) shows that the solution of quadratic equation can be obtained in terms of the coefficients of the equation and using the operations of addition, subtraction, multiplication, division and extraction of roots: this technique is called by *radicals*. The resolution of cubic and quartic equations was a relevant problem until the 17th century; since that moment mathematician had tried to solve by radical equation of major degree. Around 1830, Evariste Galois gave a necessary and sufficient condition for the resolution by radical of a given equation: with his concept of *normal subgroup* he provided an aerial view of this maze.

The modern approach to the theory, through automorphisms, moves away from the original formulation of Galois and implies a certain level of knowledge by the reader regarding some algebraic structures. The original approach of Galois, on the other hand, is more suitable for a reader with a more basic background. The thesis wants to expose Galois theory as it was conceived by the mathematician: the study was carried out starting from his original article "Mémoir on the Conditions for Solvability of Equations by Radicals" accompanying it with concrete examples, adding a visual interpretation through the analogy with a mountain to climb.
The first part provides an overview of the mathematical tools needed to better understand Galois theory, including the concepts of group, field and cyclotomic equations. The second part presents the point from which Galois started to elaborate the theory, in particular the work of Lagrange. In the central part of the thesis the fundamental points of the theory are exposed, explained through the analogy with a mountain to climb and accompanied by a visual interpretation of the problem. The idea is to start from a base field that represents the field of the coefficients of the polynomial of degree n with unknown roots and to reach the top. The peak is reached when an extension of the base camp, in which the n roots are all distinct, has been found. The fundamental aspects of Galois theory are the relationship between the algebraic equation $f(x) = 0$ and the group associated with it, and how this group changes after the extension of the base field. The resolution of polynomial equations is therefore exposed as different paths to reach the top of a mountain. The elaboration is accompanied by images, examples, practical applications and some elaborations with the software Mathematica.
Nowadays Galois theory has assumed an important role: it has been used to show that classic problems, such as trisecting the angle and doubling the cube, cannot be solved or which polygons are constructible with compass and straightedge. One of the biggest project in modern mathematical research is *Langlands Program*: this project is born in the late $60's$ with the goal of relating Galois representations and automorphic forms [La]. This project has a relevant role in Theoretical Physics: in recent studies the connection between the geometric Langlands correspondence and dualities in quantum field theories have been investigated. Another remarkable application of Galois theory was made by Andrew Wiles in the study of Fermat's Last Theorem. A significant Galois' application is the Advanced Encryption Standard (AES), a subset of the Rijndael block cipher, that described a symmetric-key algorithm adopted by the U.S. government.

Acknowledgements

A special thanks to my supervisor, Professor Antonio J. Di Scala, any word would not be enough to thank him not only for the time he had dedicated to me, but above all, for his desire to pass on his acquired knowledge. I know I am very lucky to have met him: few people are able to involve others regarding the wonder and the amazement experienced with mathematics. Thank you also for the advice regarding the daily life of a mathematician.
My highest gratitude to my parents: I would not have been able to devote myself to the study of mathematics without their constant support. Thanks to my little star Clarissa, with her sweetness she was able to support me despite the physical distance.
I would like to express my thankfulness to everybody who made my stay in Turin a warm experience: thanks to Roberto, who has never been tired of listening my doubts and who has understood my relationship with mathematics; thank you to my flatmates which made the house more comfortable; a heartfelt thanks to all the guys of Casa Chiripas, my personal refuge during the difficult moments: none of them knows how much helped me. Thank you to Emilio, who has decided to deal with me all the white and the black of this last year, he was able to paint into shades of gray.

Contents

List of Figures

Two roads diverged in a yellow wood,
And sorry I could not travel both
And be one traveler, long I stood
And looked down one as far as I could
To where it bent in the undergrowth;
Then took the other, as just as fair,
And having perhaps the better claim,
Because it was grassy and wanted wear;
Though as for that the passing there
Had worn them really about the same,
And both that morning equally lay
In leaves no step had trodden black.
Oh, I kept the first for another day!
Yet knowing how way leads on to way,
I doubted if I should ever come back.
I shall be telling this with a sigh
Somewhere ages and ages hence:
Two roads diverged in a wood, and I—
I took the one less traveled by,
And that has made all the difference.

Robert Frost, *The Road not Taken*,
Mountain Interval.

Chapter 1

Tools to understand Galois Theory

> We are like dwarfs sitting on the shoulders of giants. We see more, and things that are more distant, than they did, not because our sight is superior or because we are taller than they, but because they raise us up, and by their great stature add to ours.
>
> John of Salisbury

1.1 Group, Ring and Field

A *group* is a set G with an operation $\cdot$ such that $(G, \cdot)$ satisfies the following four axioms:

1. *Closure* $\forall a, b \in G \Rightarrow a \cdot b \in G$
2. *Associativity* $\forall a, b, c \in G \Rightarrow (a \cdot b) \cdot c = a \cdot (b \cdot c) \in G$
3. *Identity element* $\exists! e \in G$ such that $\forall a \in G \Rightarrow a \cdot e = e \cdot a = a$
4. *Inverse element* $\forall a \in G \ \exists! b \in G$ such that $a \cdot b = b \cdot a = e$ where e is the identity element.

The result of an operation may depend on the order of the operands if $a \cdot b = b \cdot a$ the group is called *abelian group*. Example:

1. $(\mathbb{Z}, +)$ the integers with addiction is a group;
2. $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ and $(\mathbb{C}, +)$ are a group;

3. $(\mathbb{Z}, \cdot)$ the integers with multiplication is not a group since inverses do not exist: $x = 3$ is an integer but the only solution to the equation $xy = 1$ is $b = 1/3$ but $1/3 \notin \mathbb{Z}$;

4. $(\mathbb{Q}, \cdot)$ the rationals with multiplication form a group;

Let $(G, \cdot)$ be a group and X be a set, a *(left) group action* τ of G on X is a function:

$$\phi : G \times X \to X$$

that satisfies the following axioms:

1. $\forall x \in X \Rightarrow \phi(e, x) = e$;

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

Let $M = \{a, b, c, d, \cdots\}$ be a set; a group $(G, \cdot)$ *acts transitively* on M in the sense that $\forall x, y \in M$ then $\exists g \in G$ such that $g(x) = y$. In other words, the orbit of a generic element $e \in M$, that is the set of elements in M to which e can be moved by the elements of G, is equal to M.
A *finite group* is a group with a finite number of elements; for example the symmetric group S_n on a finite set of n symbols is the group whose elements are all the permutations of the n symbols so it is finite and its order is $n!$. Every finite group of order prime is a cyclic group.
A *cyclic group* is a group that is generated by a single element. This element is called a generator of the group and it is such that all the other elements are its powers. For example, $(\mathbb{Z}_3, +)$ is cyclic and 1 is a generator since $1 = 1$, $1+1 = 2$ and $1+1+1 = 3 = 0$.
A *Ring* is a set R with two binary operations $+$ and $\cdot$, called addition and multiplication respectively, satisfying the following axioms:

1. *R is an abelian group under addiction*

2. *R is a monoid under addiction* $(\forall a, b, c, \in R \Rightarrow (a \cdot b) \cdot c = a \cdot (b \cdot c)$ and $\exists\ 1 \in R$ such that $a \cdot 1 = 1 \cdot a = a)$.

3. *Multiplication is distributive with respect to addition* $(\forall a, b, c \in R \Rightarrow a \cdot (b + c) = a \cdot b + a \cdot c)$ and $(b + c) \cdot a = b \cdot a + c \cdot a)$.

Although ring addition is commutative, ring multiplication is not required to be commutative: rings that satisfy commutativity for multiplication are called *commutative rings*. For example, the set of the integers $\mathbb{Z}$ is a ring.
A *Field* is a set F together with two operations on F called addition and multiplication that satisfy the following axioms:

1. *Associativity* of addition $a+(b+c) = (a+b)+c$ and multiplication $a \cdot (b \cdot c) = (a \cdot b) \cdot c$;

2. *Commutativity* of addition $a + b = b + c$ and multiplication $a \cdot b = b \cdot a$;

3. *Additive and multiplicative identity*: $\exists\ 0 \in F$ and $\exists\ 1 \in F$ such that $a + 0 = a$ and $a \cdot 1 = a$;

4. *Additive inverses*: $\forall a \in F \; \exists(-a) \in F$ such that $a + (-a) = 0$;
5. *Multiplicative inverses*: $\forall a \neq 0 \in F \; \exists(a^{-1}) \in F$ such that $a \cdot a^{-1} = 1$;
6. *Distributivity of multiplication over addition*: $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$;

For example, the set of rational numbers $\mathbb{Q}$ and the one of real numbers $\mathbb{R}$ are fields.

1.1.1 Subgroups and Quotient groups

A subgroup H is a group contained into a bigger one G; H is such that it contains the identity element of G and $\forall h_1, h_2 \in H \Rightarrow h_1 \cdot h_2 \in H$. Given any subset S of a group G, the subgroup generated by S consists of all the elements of S, their inverse and the identity element. A subgroup defines left and right cosets which can be thought of as translations of H by arbitrary group elements $g \in G$.
For example, the right coset of H containing g is:

$$Hg = \{h \cdot g : h \in H\}$$

The left coset of H containing g is:

$$gH = \{g \cdot h : h \in H\}$$

If $Hg = gH$ than H is said to be a normal subgroup and it is indicated as $H \trianglelefteq G$.

Given any normal subgroup N of G, it is possible to construct a *quotient* (or *factor*) group of N in G that contains similar element of G using an equivalence relation (that is a reflexive, symmetric and transitive binary relation). This group is indicated as G/N and it is $G/N = \{aN : a \in G\}$.

1.1.2 Vector Space over a Field

Let V be a finite dimensional space over a field K; its dimension over K, $dim_K V$, is the cardinality of a basis of V over its base field. If $K(a)$ is an extension of K and the degree of the minimal polynomial of a, $deg(m_a)$, is equal to n then the degree of $K(a)$ as vector space over K is $[K(a) : K] = n$. Let E, F, K be fields such that $E \subset F \subset K$, then $[K : E] = [K : F][F : E]$.

Proof: Let $P \in E[x]$ be an irreducible polynomial of degree n and $\alpha, \beta, \cdots, \nu$ its roots. Suppose that $F = E(\alpha)$ and $K = E(\alpha, \beta)$ figure 1.1.

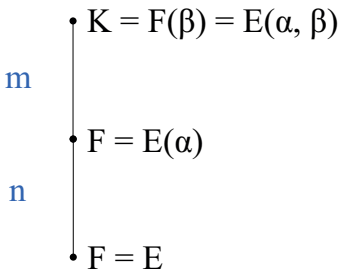

Figure 1.1. Dimension of Vector Space over a Field

This implies that α satisfies an equation of degree n and its minimal polynomial over K has degree n. In other words, each element $s \in F$ can be expressed as linear combination of vectors $< 1, \alpha, \alpha^2, \cdots, \alpha^{n-1} >$ with coefficients in E. So F is a vector space over E with dimension n. Following the same reasoning, let us suppose β satisfies an equation of degree m over F, therefore each $v \in K$ can be written as a linear combination of $< 1, \beta, \beta^2, \cdots, \beta^{m-1} >$, that is $v = c_0 1 + c_1\beta + \cdots + c_{m-1}\beta^{m-1}$. Since the coefficients $c_i \in F$, they are of types:

$$c_0 = c_{00}1 + c_{01}\alpha + \cdots + c_{0n-1}\alpha^{n-1}$$
$$c_i = c_{i0}1 + c_{i1}\alpha + \cdots + c_{in-1}\alpha^{n-1}$$

In other words,

$$v = \sum_{ji} c_{ij}\alpha^i\beta^j$$

Therefore the dimension of K is $m \cdot n$. □

The previous reasoning can be generalized as in the figure 1.2.

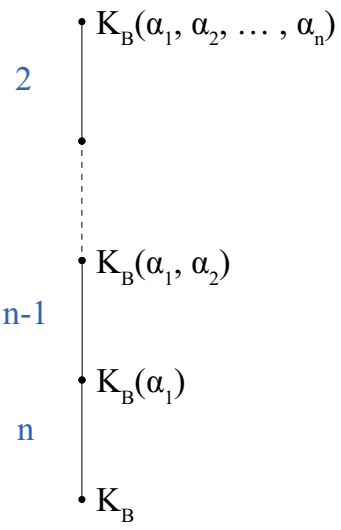

Figure 1.2. Degree of a Field Extension

The maximum $dim K_B(\alpha_1, \alpha_2, \cdots, \alpha_n)$ over K_B is $n!$.

1.2 Symmetric Polynomials

A symmetric polynomial is a particular polynomial in n variables such that

$$P(x_{\sigma_1}, x_{\sigma_2}, \cdots, x_{\sigma_n}) = P(x_1, x_2, \cdots, x_n)$$

for any permutation $\sigma \in S_n$. In other words, this means that if any of the unknowns are interchanged the polynomial doesn't change. For example,

$x_1^3 x_2 + (x_1 + x_2)^2 + x_1 x_2^3$

$x_1 x_2 + x_1 x_3 + x_2 x_3 + 5 x_1 x_2 x_3$

are symmetric polynomials, conversely

$3x_1^3 x_2 + (x_1 + x_2)^2 + 7 x_1 x_2^3$

$x_1 x_2 + x_1 x_3 - x_2 x_3$

are not symmetric since if one exchanges x_1 and x_2 one obtains a different expression. The elementary symmetric polynomials in $x_1, x_2, \cdots, x_n$ indicated as $e_k(x_1, x_2, \cdots, x_n)$ for $k = 0, 1, \cdots, n$ are defined as:

$$e_0(x_1, x_2, \cdots, x_n) = 1$$
$$e_1(x_1, x_2, \cdots, x_n) = \sum_{1\leq j\leq n} x_j$$
$$e_2(x_1, x_2, \cdots, x_n) = \sum_{1\leq j<k\leq n} x_j x_k$$
$$e_3(x_1, x_2, \cdots, x_n) = \sum_{1\leq j<k<l\leq n} x_j x_k x_l$$

For example, for $n = 2$ the elementary symmetric polynomials are:

$$e_0(x_1, x_2) = 1$$
$$e_1(x_1, x_2) = x_1 + x_2$$
$$e_2(x_1, x_2) = x_1 x_2$$

1.2.1 Fundamental Theorem on Symmetric Polynomials

This theorem is fundamental to the development of Galois Theory.
Let $P(x)$ be a polynomial over $K[x_1, x_2, \cdots, x_n]$, such that

$$P(x_1, x_2, \cdots, x_n) = P(x_{\sigma_1}, x_{\sigma_2}, \cdots, x_{\sigma_n})$$

for every σ permutation of $x_1, x_2, \cdots, x_n$.
Then $A(u_1, u_2, \cdots, u_n) \in K[u_1, u_2, \cdots, u_n]$ exists such that
$A(u_1, u_2, \cdots, u_n) = A(\sigma_1(x_1, \cdots, x_n), \sigma_2(x_1, \cdots, x_n), \cdots, \sigma_n(x_1, \cdots, x_n))$

$$P(x_1, x_2, \cdots, x_n) = A(\sigma_1(x_1, \cdots, x_n), \sigma_2(x_1, \cdots, x_n), \cdots, \sigma_n(x_1, \cdots, x_n))$$

Namely, *this means that any symmetric polynomial in the roots of an equation can be expressed in terms of the coefficients of that equation.*

Let us consider a concrete example. Let $P(x) = (x_1 - x_2)^2$ be symmetric with x_1 and x_2 solutions of a generic quadratic equation. The theorem says that any symmetric polynomial in the variables x_1 and x_2 can be written as a polynomial in the elementary symmetric functions $e_1 = x_1 + x_2$ and $e_2 = x_1 x_2$. This can be obtained as follow.

$$P(x_1, x_2) = (x_1 - x_2)^2 = x_1^2 + x_2^2 - 2x_1 x_2$$

Using σ_2, it becomes

$$P(x_1, x_2) = (x_1 - x_2)^2 = x_1^2 + x_2^2 - 2e_2$$

Since x_1 and x_2 are solutions of the quadratic equation,

$$(x + x_1)(x + x_2) = x^2 + e_1 x + e_2$$

then

$$x_1^2 + e_1 x_1 + e_2 = 0$$
$$x_2^2 + e_1 x_2 + e_2 = 0$$

These imply that

$$x_1^2 + x_2^2 = e_1(x_1 + x_2) - 2e_2 = e_1^2 - 2e_2$$

The expression in the symmetric polynomials is

$$A(e_2, e_1) = e_1^2 - 4e_2 = P(x_1, x_2).$$

1.3 Cyclotomic Equations

The cyclotomic equations are particular equations of the form $x^n - 1 = 0$ for any positive integer n. The contribution of Gauss for the solution of cyclotomic equations was remarkable. In the seventh section of his *Disquisitiones arithmeticae* (1801), Gauss investigated the ruler-and-compass constructability of regular polygons and how to solve algebraically the binomial equations of the form $x^n - 1 = 0$ [Ga].

The roots of cyclotomic equations are known as roots of unity and, in the complex plane, these roots divide the arc of the unit circle into n equal parts each of them with an angle $\theta = 2\pi/n$; $\omega = e^{i\theta}$ is a solution of $x^n - 1 = 0$ and all the other roots can be obtained multiplying this root for itself ($\omega^2, \omega^3, \cdots, \omega^n = 1$ are other solutions). So ω generates all the other roots and for such reason is called *primitive root of unity* or *generator*.

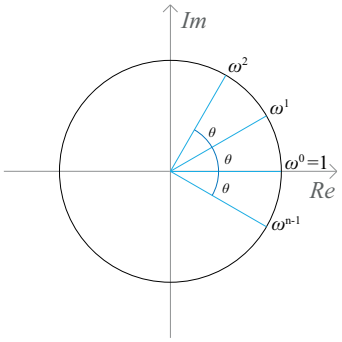

Figure 1.3. The nth roots of unity

The cyclic group Z_n is isomorphic to the set of the roots in the sense that:

$$\forall a \in Z_n \Rightarrow \omega^a - 1 = 0$$

In addition to ω defined as above, there will be other primitive roots of unity of the form ω^a with a such that a is *coprime* with n. So, if n is a prime number, all *nth* roots of unity, except 1, are generators.
In the case of $n = 4$, $\omega^2 = -1$ is not a generator as the roots $\omega = -i$ and $\omega = i$ can't be obtained by multiplication of ω^2 for itself, as figure 1.4 shows.

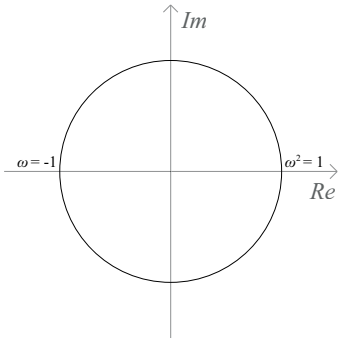

Figure 1.4. A 4th root of unity

1.4 Eisenstein's Criterion

This criterion gives a sufficient condition for a polynomial with integer coefficients to be irreducible over the rational numbers.
Let $P(x)$ be a polynomial with integer coefficients:

$$P(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

If there exists a prime number p such that the following three conditions all apply:

1. p divides each a_i for $0 \leq a_i < n$;
2. p does not divide a_n;
3. p^2 does not divide a_0;

then $P(x)$ is irreducible over the rational numbers.

Proof: Assume by contradiction that $P(x)$ is not irreducible in $\mathbb{Q}(x)$. Then Gauss showed that there is a factorization in $\mathbb{Z}[x]$. Namely,

$$P(x) = A(x) \cdot B(x)$$

with $A(x) = m_s x^s + \cdots + m_0$ $B(x) = r_d x^d + \cdots + r_0 \in \mathbb{Z}(x)$, $s, d > 0$.

Then reducing $(\mathrm{mod}\, p)$ we have

$$a_n x^n \equiv A(x) \cdot B(x) \pmod{p}. \tag{1.1}$$

hence

$$A(x) \equiv m_s x^s \pmod{p},$$
$$B(x) \equiv r_d x^d \pmod{p}.$$

Since $s, d > 0$ we get $m_0 \equiv 0 \pmod{p}$ and $r_0 \equiv 0 \pmod{p}$ hence

$$p^2 | a_0 = m_0 \cdot r_0$$

a contradiction coming from assuming $P(x)$ reducible over $\mathbb{Q}$. □

Chapter 2

Starting Points of Galois Theory

Tyger! Tyger! Burning bright
In the forests of the night:
What immortal hand or eye
Dare frame thy fearful symmetry?

The Tyger, William Blake

2.1 Lagrange Resolvents

In his *Réflexions sur la Résolution Algébrique des Equations*, Lagrange investigates the solution of equations of degree 2, 3 and 4, looking for a general approach to the problem. The basic idea of Lagrange[1] is to consider a quantity t, also known as the *Lagrange resolvent*, that is expression of the roots of a given nth-degree polynomial and a nth root of unity. This quantity has $n!$ values, depending on the order in which the roots are taken but sometimes two or more values can be the same. Once this quantity t has been found by radicals, the n roots of the given equation can be also found.
Let us see in details what happens in the case of $n = 2, 3, 4$.

1. Let $P(x) = x^2 + c_1x + c_0$ be a quadratic polynomial with $(c_0, c_1) \in K$ and let α and β be its roots (suppose that they exist in some field). So $P(x) = x^2 + c_1x + c_0 = (x - \alpha)(x - \beta)$. The auxiliary equation is

$$(x - t)(x + t) = 0 \Rightarrow x^2 - t^2 = 0$$

[1] A similar strategy was developed by Vandermonde a few months earlier, but it seems that Lagrange didn't know it.

where the resolvent t is $t = (\alpha - \beta)^2$ and, since it is symmetric in the roots of the given equation, it can be expressed in terms of the coefficients of the given equation thus $t \in K$. Therefore x can be found by radicals from $x^2 - t^2 = 0$. Using the expressions

$$\begin{cases} \alpha - \beta = \sqrt{t^2} \\ \alpha + \beta = c_1 \end{cases}$$

2. Let $P(x) = x^3 + c_2x^2 + c_1x + c_0$ be a cubic polynomial where $(c_0, c_1, c_2) \in K$ and α, β and γ are its roots, $P(x) = (x - \alpha)(x - \beta)(x - \gamma)$. Let ω be a cube root of unity, so $\omega \neq 1$ and $\omega^3 = 1$. Consider the quantities

$$\begin{cases} t_1 = (\alpha + \omega\beta + \omega^2\gamma)^3 \\ t_2 = (\gamma + \omega\alpha + \omega^2\beta)^3 \\ t_3 = (\beta + \omega\gamma + \omega^2\alpha)^3 \\ t_4 = (\alpha + \omega\gamma + \omega^2\beta)^3 \\ t_5 = (\beta + \omega\alpha + \omega^2\gamma)^3 \\ t_6 = (\gamma + \omega\beta + \omega^2\alpha)^3 \end{cases}$$

the auxiliary polynomial is

$$(x - t_1)(x - t_2)(x - t_3)(x - t_4)(x - t_5)(x - t_6) = A(x) \tag{2.1}$$

and it is symmetric in t_i and in the roots of the given cubic equation. Newton's Theorem implies that the coefficients of $A(x)$ belong to K. Observing that the values of t can be rewritten as

$$\begin{cases} t_1 = (\alpha + \omega\beta + \omega^2\gamma)^3 \\ t_2 = \omega t_1 \\ t_3 = \omega^2 t_1 \\ t_4 = (\alpha + \omega\gamma + \omega^2\beta)^3 \\ t_5 = \omega t_4 \\ t_6 = \omega^2 t_4 \end{cases}$$

The equation (2.1) becomes

$$A(x) = (x^3 - t_1^3)(x^3 - t_4^3) \tag{2.2}$$

Set $x^3 = u$, the equation (2.2) takes the form

$$B(u) = (u - t_1^3)(u - t_4^3) \tag{2.3}$$

that is an equation of degree 2 whose resolution is known. The resolution of the polynomial $A(x)$ is equivalent to the resolution of the polynomial with degree 2 and than the cubic one ($x^3 = u$). Similarly to the quadratic equation, the given cubic equation has been solved by radicals.

3. Lagrange's method can also be applied to the solution of quartic equations. Let $P(x) = x^4 + c_3x^3 + c_2x^2 + c_1x + c_0$ be a quartic polynomial with $(c_0, c_1, c_2, c_3) \in K$ and α, β, γ and θ as roots. Proceeding as before, it is possible to write the resolvent t as an expression of the roots α, β, γ, θ and a quartic root of unity (primitive or not). For example, if $t = \alpha + i\beta - \gamma - i\theta$, where $i = \sqrt{-1}$ is a primitive 4th root of unity, t will have $4! = 24$ different values depending on the order in which the roots have been chosen. So the auxiliary equation is of degree 24. If $t = \alpha - \beta + \gamma - \theta$, there are only 6 different values of t and not 24 like before. Each of the values occurs four times, so the auxiliary equation

$$A(x) = (x - t_1)(x - t_2)\cdots(x - t_{23})(x - t_{24}) \tag{2.4}$$

can be rewritten as

$$A(x) = (x - t_1)^4(x + t_1)^4(x - t_2)^4(x + t_2)^4(x - t_3)^4(x + t_3)^4 = g(x)^4 = 0 \tag{2.5}$$

where $g(x) = (x^2 - t_1^2)(x^2 - t_2^2)(x^2 - t_3^2)$. The resolution of the polynomial A(x) with degree 24 has been simplified in the resolution of a cubic equation in x^2. In other words, the quartic equation has been solved by radicals.

4. The natural way to extend Lagrange's method to the quintic equation is to take t as expression of the roots of the given equation and ω, a quintic square root of unity. Let $t = \alpha + \omega\beta + \omega^2\gamma + \omega^3\theta + \omega^4\nu$, than t has $5! = 120$ different values and it satisfies the auxiliary equation of degree 120. As before, if t_1 is one of the 120 values, then ωt_1, $\omega^2 t_1$, $\omega^3 t_1$, $\omega^4 t_1$ are as well. This implies that the auxiliary equation of degree 120 assumes the form

$$A(x) = (x^5 - t_1^5)(x^5 - t_2^5)(x^5 - t_3^5)(x^5 - t_4^5) \tag{2.6}$$

and cannot be rewritten as a quadratic or a cubic function. The problem is that every 5th root of unity other than 1 is primitive.

2.2 Galois and his predecessors

2.2.1 Lagrange and Galois

The starting point of Galois' study was the idea of Lagrange to use a resolvent t to solve polynomial equation. For Lagrange, the resolvent has three main features:

1. It is rationally expressible in terms of the roots of the equation and the coefficients of the given equation;

2. Each of the roots of the equation can be expressed rationally in terms of it;

3. It is the solution of a solvable equation.

Lagrange wondered about the possibility to find the resolvent for the general quintic equation and he stated an important theorem that can be seen as the basis of Galois' study [Ed]: *If t and y are any two functions in the roots $x', x'', x''', \dots$ of $x^\mu + mx^{\mu-1} + nx^{\mu-2} + \cdots = 0$ and if these functions are such that every permutation of the roots $x', x'', x''', \dots$ which changes y also changes t, one can, generally speaking, express y rationally in terms of t and $m, n, \dots$, so that when one knows a value of t one will also know immediately the corresponding value of y; we say generally speaking because if the known value of t is a double or triple or higher root of the equation for t then the corresponding value of y will depend on an equation of degree 2 or 3 or higher with coefficients that are rational in t and $m, n, \dots$.* The key point is that Lagrange thought about whether a function y of the roots can be expressed rationally in terms of the resolvent t rather then all single roots can be expressed rationally in terms of t and known quantities. In Lemma III of the original Galois' article, that will be explained later, he states *When the function t has been chosen such that it has $n!$ different values when the roots are permuted, it has the property that all the roots of the equation can be expressed rationally in terms of it.* The great step beyond Lagrange's work made by Galois was to come up with a way of analyzing the structure of the field $k(t)$ of rational functions of the roots which enables one to determine whether the roots can be expressed in terms of known quantities from k, the field of the polynomial's coefficients, and the operations of addition, subtraction, multiplication, division and extraction of roots.

2.2.2 Ruffini, Abel and Galois

In 1799, Paolo Ruffini published a book, *General theory of equations in which it is shown that the algebraic solution of the general equation of degree greater than four is impossible*, on the theory of equations where he wanted to demonstrate that the general quintic equation could not be solved by radicals; in his work, Ruffini was the first one to introduce the notion of the order of an element, conjugacy and the cycle decomposition of elements of permutation groups. In his work there was a gap since Ruffini assumed that all the radicals he was dealing with could be expressed from the roots of the polynomial using field operations alone; in 1824 Niels Abel was able to complete it.

It seems that Ruffini assumed, in case the equation is solvable by radicals, that the peak of the mountain can be reached by radicals from inside. This is not the case that is showed by the equation $P(x) = x^3 - 3x - 1$. The equation is of course solvable by radicals, it is irreducible over $\mathbb{Q}$ and has three real roots $a, b = a^2 - a - 2, c = -a^2 + 2$. So $Gal(P/\mathbb{Q})$ is cyclic with three elements generated by $\sigma = (abc)$. The mountain's peak is $\mathbb{Q}(a) = \mathbb{Q}(a, b, c)$ which is a subset of real numbers. If the peak could be reached from the inside by radicals then there is $e = e(a, b, c) \in \mathbb{Q}(a)$, $r \in \mathbb{Q}$ and $m \in \mathbb{N}$ such that $\mathbb{Q}(e) = \mathbb{Q}(a)$ and $e^m = r$. Observe that the roots of $x^m - r$ are $e\omega^j$, $j = 1, \cdots, m-1$, where ω is a primitive root of the unit. Thus $\sigma(e) = e(b, c, a) = e\omega^j$ is a real number hence $\omega^j = -1$. Then the polynomial $(x - e)(x - \sigma(e)) = x^2 + Ax + B$ has coefficients in $\mathbb{Q}$. This contradicts that $\mathbb{Q}(e) = \mathbb{Q}(a)$ since $Q(e)$ has degree two over $\mathbb{Q}$ and $Q(a)$ has degree three. Thus the peak can not be reached from inside by using radicals.
To reach the peak from inside it is necessary to change the base field of the equation, namely the mountain is going to be a bigger mountain. In case of $P(x) = x^3 - 3x - 1$

we consider as the base field $\mathbb{Q}(\omega)$ where ω is a primitive root of the unit of degree 3 i.e. $\Phi_3(\omega) = \omega^2 + \omega + 1 = 0$. Notice that the new mountain is $Q(\omega)(a)$.

Now by Galois' Proposition II (see Chapter 3) $Gal(P/\mathbb{Q}) = Gal(P/\mathbb{Q}(\omega))$. Then to reach the peak of $Q(\omega)(a)$ we use a Lagrange resolvent $L := a + \omega b + \omega^2 c$. Observe that $L^3 \in \mathbb{Q}(\omega)$. So $Gal(P/\mathbb{Q}(\omega)(L)) = \{Id\}$ i.e. the roots a, b, c are all in $\mathbb{Q}(\omega)(L)$ which means that we reach the peak.

Nowadays the famous Abel-Ruffini theorem is the result of their contribution: it states that there is no formula similar to the one for equation of degree second, third and fourth, for general equations of fifth degree or higher. However this theorem does not provide necessary and sufficient conditions for saying which quintic or higher equations are unsolvable by radicals. For this reason, Galois contribution is remarkable: the young Évariste was able to provide a concrete polynomial of degree 5 whose roots cannot be expressed in terms of radicals from its coefficients.

2.3 The parallelism between Galois Theory and mountain climbing

In this thesis, the main idea is to give a visual interpretation of Galois Theory using the concept of mountain climbing.
A given polynomial $P \in K[x]$ of degree n is strictly related to a base camp K that represents the field generated by its coefficients. If the polynomial is irreducible over K, this means that its n roots do not belong to K so it is necessary to climb the mountain until a new base camp (the one where the polynomial can be reduced into n factors) is reached (figure 2.1). The polynomial is associated with a Galois group that can change when one climbs the mountain; if it changes then it becomes smaller and when this group contains only an element the n roots are found.

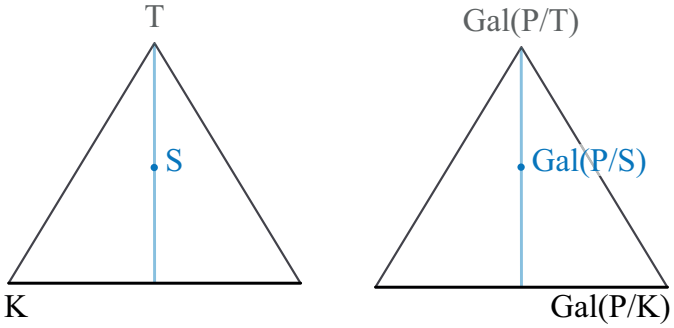

Figure 2.1. Galois Mountain

2.4 Foundation stone of Galois Theory

A key concept of Galois' ideas is the possibility to distinguish two elements from the point of view of a given field.
Let K be a field, a and b are said to be *conjugate* in K if $\forall E \in K[x]$ such that

$$E(a) = 0 \Rightarrow E(b) = 0$$

In other words, two elements are conjugate for K if any expression with coefficients in K satisfied by a is also satisfied by b. From the point of view of the mountain it is explained in figure 2.2.

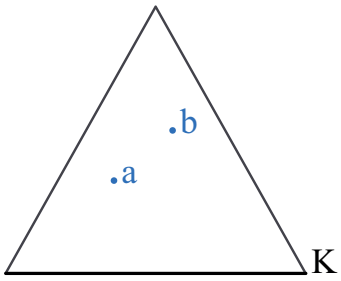

Figure 2.2. Conjugate Elements for K

Proposition

If a has not conjugate in a field K, then $a \in K$ as in figure 2.3

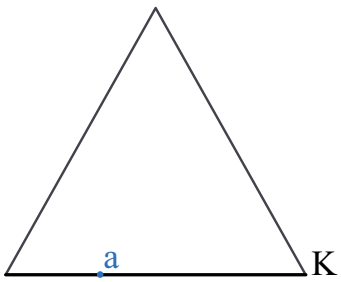

Figure 2.3. Example of $a \in K$

Proof: Let $m_a(x)$ be the minimal polynomial of a in K; then there might be two cases:

1. $deg(m_a) = 1$ so $m_a(x) = x - a$ that means $a \in K$;

2. $deg(m_a) \geq 2$ then there will be at least another root b of $m_a(x)$ such that $m_a(b) = 0$ but this contradicts the hypothesis. $\square$

Lemma I

Let $f(x)$ and $P(x)$ be polynomials over $K[x]$ with $f(x)$ irreducible.
If $f(x)$ and $P(x)$ have a common root, then $f(x)|P(x)$.

Proof: Let $d(x)$ be the maximum common divisor between $f(x)$ and $P(x)$,

$$MCD(f(x), P(x)) = d(x) = A(x)f(x) + B(x)P(x)$$

with $A(x)$ and $B(x)$ polynomials over $K(x)$.
Then, as $f(x)$ is irreducible there are only two possibilities:

1. $$d(x) = f(x)$$

   this implies that $f(x)|P(x)$.

2. $$d(x) = 1$$

   in that case
   $$A(\alpha)f(\alpha) + B(\alpha)P(\alpha) = 1$$
   $$0 + 0 = 1$$

   that is absurd. $\square$

From Lemma I it follows that if a and b are conjugated in K_B then their minimal polynomials are the same: $m_a(x) = m_b(x)$. Let $m_a(x)$ be the minimal polynomial of a that is irreducible for definition and let $P \in K_B[x]$ with a one of its roots; since $m_a(x)$ and $P(x)$ have a as common root and $m_a(x)$ is irreducible for definition, $m_a(x)|P(x)$ so b is another root of $P(x)$.

Lemma II

Let $a, b, c, \cdots$ be the n distinct roots of the equation

$$P(x) = 0$$

over $K[x]$. Then there is a function V of the roots such that *for $\forall\sigma : [1, n] \to \{a, b, c, \cdots\}$ the values

*From now on, $[1, n] = \{1, 2, \cdots, n\}$ is the set of the first n integers and σ are the injective functions of the type $\forall\sigma : [1, n] \to \{a, b, c, \cdots\}$.

$$V(\sigma(1), \sigma(2), \ldots, \sigma(n))$$

are all different.

Proof: Since the roots are n, $V \in K[x_1, x_2, \cdots, x_n]$ have to take $n!$ different values. V is of the form $V_i = \alpha_1\sigma_i(1) + \alpha_2\sigma_i(2) + \cdots + \alpha_n\sigma_i(n)$; so the $n!$ values of V are:

$$\begin{aligned} V_1 &= \alpha_1\sigma_1(1) + \alpha_2\sigma_1(2) + \cdots + \alpha_n\sigma_1(n) \\ V_2 &= \alpha_1\sigma_2(1) + \alpha_2\sigma_2(2) + \cdots + \alpha_n\sigma_2(n) \\ &\vdots \\ V_n &= \alpha_1\sigma_n(1) + \alpha_2\sigma_n(2) + \cdots + \alpha_n\sigma_n(n) \end{aligned}$$

and it has to be $V_1 \neq V_2 \neq \cdots \neq V_n$. Find such a V means to find the coefficients α_i that satisfy the condition above. Basically, it is possible to find the coefficients α_i such that the n equalities $V_i = V_j$ are verified and then to exclude them. □

Lemma III

Let $V \in Q[a, b, c, \ldots]$ be defined as above, with $a, b, c, \cdots$ distinct roots of a given polynomial $P \in K[x]$ and let $V_1 = V(a, b, c, \cdots)$. Then all the roots of $P(x) = 0$ can be expressed as rational functions of V_1.

Proof: Let a be the generic root of $P(x) = 0$, $R_P = \{a, b, c, \cdots\}$ and

$$F(Y, a) := \prod_{\sigma \in [2,n] \to R_P \setminus \{a\}} (Y - V(a, \sigma(2), \cdots, \sigma(n))) \tag{2.7}$$

that is of the form

$$F(Y, a) = \sum_j c_j(a, \sigma(2), \cdots, \sigma(n)) Y^j = \sum_j c_j(a) Y^j \tag{2.8}$$

Due to the fact that after any change of $b, c, \cdots$ the polynomial (2.7) doesn't change, therefore also the polynomial (2.8) doesn't.
In other words, the coefficients $c_j(a, \sigma(2), \cdots, \sigma(n))$ are symmetric functions of $b, c, \cdots$ in $K(a)$. For example, in the case of a cubic equation:

$$(x - a)(x - b)(x - c) = x^3 - S_1x^2 + S_2x + S_0$$

with S_1, S_2, S_3 in $K[x]$, there will be
$a + b + c = S_1 \Rightarrow b + c = S_1 - a$
$abc = S_0 \Rightarrow bc = S_0/a \Rightarrow bc = -a^2 + S_1a - S_2$
Set

$$F(V_1, x) := \sum_j c_j(x) V_1^j \tag{2.9}$$

then the polynomials $P(x)$ and $F(V_1, x)$ have just one common root: a. From the calculation of the maximum common divisor, it follows that

$$x - a = A(x)P(x) + B(x)F(V_1, x)$$

with $P(x)$ in K, $F(V_1, x)$ in $K(V_1)$ so $A(x)$ and $B(x)$ are in $K(V_1)$. For $x = 0$, it follows that $-a = A(0)P(0)+B(0)F(V_1,0) = f_1(V_1)$ that means $a \in Q(V_1)$ and a is an expression of V_1. To explain why $P(x)$ and $F(V_1, x)$ have only a common factor, a, note that the same procedure can be conducted for the other roots. Let us consider another polynomial, $H(Y, b)$ such that:

$$H(Y, b) = \sum_j c_j(b)Y^j \tag{2.10}$$

Since $b \neq a$ and $V_1 = V(a, b, c, \cdots)$, every product $V_1 - V(b, \sigma(2), \ldots, \sigma(n)) \neq 0$ with $\sigma \in [2, n] \to R_P \setminus \{b\}$, so $H(V_1, b) \neq 0$. In figure 2.4 it is shown from the point of view of the mountain.

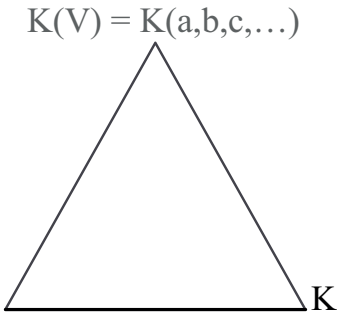

Figure 2.4. $K(V) = K(a, b, c, \cdots)$

□

Lemma IV

Suppose one has formed the equation for V,

$$R(x) := \prod_{\sigma \in [1,n] \to R_P} (x - V(\sigma(1), \sigma(2), \cdots, \sigma(n)))$$

with $R \in k[x]$ and that one has taken one of its irreducible factors $Q(x)$, so that V is the root of an irreducible equation. Let $V, V', V'', \ldots, V^s$ be all the roots of this irreducible equation. If the generic root a of $P(x) = 0$ is such that $a = f(V)$ then $f(V')$ will also be another root of the given equation.

Proof: First of all it is shown why $R \in K[x]$ such that $R(V) = 0$ exists.
Let us consider infinite vectors of powers of V $\{\ldots, V^4, V^3, V^2, V^1, V^0\}$; since V is an expression of the n roots $a, b, c, \ldots$, the infinite vectors above belong to the finite n-dimensional space $K[a, b, c, \ldots]$ so they are not all linearly independent. Let us suppose that the first k are linearly dependent, so

$$c_k V^k + c_{k-1} V^{k-1} + \cdots + c_0 = 0$$

This is a polynomial with coefficients $\in K$ such that V is a root, so it will exist a polynomial $R(x)$ of minimal degree of V.

Since $P(f(x)) \in K[x]$ and it has a common root with the irreducible polynomial $Q(x)$, from Lemma I it follows that $Q|P$: in other words all the roots of $Q(x)$ are also roots of $P(f(x))$. $\square$

Chapter 3

Interpretation of Galois' Memoir

I think it's in my basement... let me go upstairs and check.

M. C. Escher

3.1 Propositions

3.1.1 Proposition I

Let $P(x)$ be an equation with $P \in K[x]$ and let $R = \{a, b, c, \cdots\}$ be the set of its n distinct roots $a \neq b \neq c \cdots$. Let $Per(P)$ contain all the $n!$ permutations of $a, b, c, \cdots$. There will always be a group of permutations $Gal(P/K) \subset Per(P)$ of the roots with the following properties:

1. If $W \in K[X_1, X_2, \cdots X_n]$ and for each $\sigma \in Gal(P/K)$

$$W(\sigma(1), \sigma(2), \sigma(3), \cdots, \sigma(n)) = W(a, b, c, \dots)$$

   then $W(a, b, c, \cdots) \in K$.

2. If $W \in K[X_1, X_2, \cdots X_n]$ and $W(a, b, c, \cdots) \in K$, then for each $\sigma \in Gal(P/K)$

$$W(\sigma(1), \sigma(2), \sigma(3), \cdots, \sigma(n)) = W(a, b, c, \dots) \in K$$

Proof: Lemma III implies that the distinct roots $a, b, c, \cdots$ can be written as $a = f_1(V_1), b = f_2(V_1), \cdots, n = f_n(V_1)$ with $V_1 = V(a, b, c, \cdots)$. Let $V', V'', \cdots, V^s$ be

the other roots of the irreducible polynomial $Q(x)$ of V_1 (Lemma IV); there will be $degQ$ permutations of the roots $a, b, c, \cdots$:

$$\begin{array}{c|cccc} V_1 & f_1(V_1) & f_2(V_1) & \cdots & f_n(V_1) \\ V' & f_1(V') & f_2(V') & \cdots & f_n(V') \\ V'' & f_1(V'') & f_2(V'') & \cdots & f_n(V'') \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ V^s & f_1(V^s) & f_2(V^s) & \cdots & f_n(V^s) \\ \vdots & \vdots & \vdots & \vdots & \vdots \end{array} \tag{3.1}$$

It's important to note that $f_i(V^r) \neq f_j(V^r)$: if $f_i(V^r) = f_j(V^r)$ then $Q(x)$ divides $f_i(X) - f_j(X) \Rightarrow f_i(V_1) - f_j(V_1) = 0$ but it is not possible since the n roots are distinct. The $degQ$ permutations form a subset

$$Gal(P/K) := \{1, \sigma_1, \sigma_2, \cdots, \sigma_s, \cdots\}$$

$$\begin{array}{cccc} f_1(V_1) & f_2(V_1) & \cdots & f_n(V_1) \\ f_1(V') & f_2(V') & \cdots & f_n(V') \\ f_1(V'') & f_2(V'') & \cdots & f_n(V'') \\ \vdots & \vdots & \vdots & \vdots \\ f_1(V^s) & f_2(V^s) & \cdots & f_n(V^s) \\ \vdots & \vdots & \vdots & \vdots \end{array} = \begin{array}{cccc} a & b & c & \cdots \\ \sigma_1(1) & \sigma_1(2) & \cdots & \sigma_1(n) \\ \sigma_2(1) & \sigma_2(2) & \cdots & \sigma_2(n) \\ \vdots & \vdots & \vdots & \vdots \\ \sigma_s(1) & \sigma_s(2) & \cdots & \sigma_s(n) \\ \vdots & \vdots & \vdots & \vdots \end{array}$$

Let $v = W(a, b, c, \cdots)$ therefore $v = \psi(V_1)$ with $\psi \in K[x]$ such that

$$\psi(X) := W(f_1(X), f_2(X), \cdots, f_n(X))$$

1. Let

$$\mu := \psi(V_1) + \psi(V') + \psi(V'') + \cdots + \psi(V^s)$$

This sum is symmetric in the roots $V_1, V', V'', \cdots, V^s$ of $Q(x)$ and can be expressed in terms of the coefficient of $Q(x)$ by applying the fundamental theorem on symmetric polynomials. Since this coefficients are in K, it follows that $\mu \in K$. Moreover $\mu = deg(Q)W(a, b, c, \cdots)$ and $W(a, b, c, \cdots) = \mu/deg(Q) \in K$, as shown in figure 3.1.

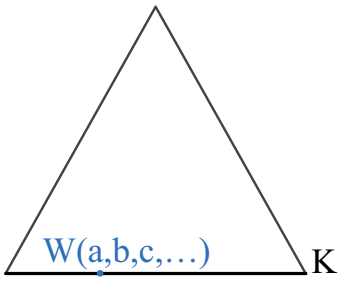

Figure 3.1. $W(a, b, c, \cdots \in K)$

2. The polynomials $v-\psi(x)$ and $Q(x)$ have a common root V_1, since $Q(x)$ is irreducible then $v = \psi(V^r)$ for each V^r root of $Q(x)$. In other words,

$$W(\sigma(1), \cdots, \sigma(n)) = v \in K$$

for each $\sigma \in Gal(P/K)$. □

3.1.2 Proposition II

If one adjoins to $Gal(P/K)$ the root r of an auxiliary irreducible equation of degree p, then:

1. one of these two will occur: either the group of the equation $Gal(P/K)$ will not change; or it will be partitioned into p groups, each belonging to the given equation respectively when one adjoins each of the roots of the auxiliary equation;

2. this group will have the remarkable property that one will pass from one to the other by applying the same substitution of letters to all permutations of the first.

Proof:

1. Let $H_1(x)$ be the minimal polynomial of V_1 in $k(r)[x]$ and $Q(x)$ the ones in $k[x]$. If $H_1(x) = Q(x)$ then $Gal(P/K)$ will not change because $H_1(x)$ has the same roots as $Q(x)$. From the point of view of the mountain this means that $r \in K$, as in figure 3.2.

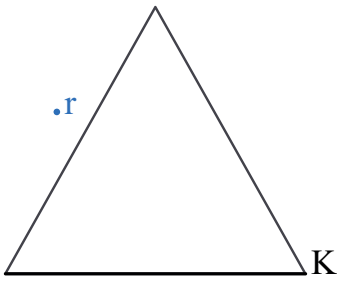

Figure 3.2. Example of an element out of the mountain

If $H_1(x) \neq Q(x)$ and $Q(x) = H_1(x)H_2(x)\cdots H_p(x)$ with H_i irreducible factors over $K(r)$. Let $V_2, \cdots, V_p$ be the roots of $H_2, \cdots, H_p$. The application of $Gal(P/K)$ properties, it follows that:

$$H_j(x) = \prod_{\sigma \in Gal(P/k(r))} (x - \sigma(V_j))$$

The elements of $Gal(P/k)$ will be grouped into p groups each one corresponding to the ones of the irreducible factors H_j.
The new group $Gal(P/k(r))$ is:

$$\begin{matrix} f_1(V_1) & f_2(V_1) & \cdots & f_n(V_1) \\ f_1(\sigma_1(V_1)) & f_2(\sigma_1(V_1)) & \cdots & f_n(\sigma_1(V_1)) \\ \vdots & \vdots & \vdots & \vdots \\ f_1(\sigma_{d-1}(V_1)) & f_2(\sigma_{d-1}(V_1)) & \cdots & f_n(\sigma_{d-1}(V_1)) \end{matrix} \tag{3.2}$$

with $Gal(P/k(r)) = \{1, \sigma_1, \cdots, \sigma_n\}$, as in figure 3.3

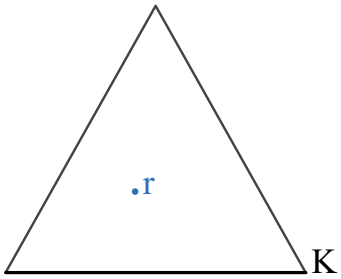

Figure 3.3. Example of an element in the mountain

2. The new subset associated to the factor H_j is:

$$\begin{matrix} f_1(V_j) & f_2(V_j) & \cdots & f_n(V_j) \\ f_1(\sigma_1(V_j)) & f_2(\sigma_1(V_j)) & \cdots & f_n(\sigma_1(V_j)) \\ \vdots & \vdots & \vdots & \vdots \\ f_1(\sigma_{d-1}(V_j)) & f_2(\sigma_{d-1}(V_j)) & \cdots & f_n(\sigma_{d-1}(V_j)) \end{matrix} \tag{3.3}$$

All these elements correspond to the d distinct roots of H_j. Let τ_j be the permutation associated to V_j, that is $\tau_j(V_i) = V_j$, then (3.3) can be rewritten as:

$$\begin{matrix} f_1(\tau_j(V_1)) & f_2(\tau_j(V_1)) & \cdots & f_n(\tau_j(V_1)) \\ f_1(\sigma_1(\tau_j(V_1))) & f_2(\sigma_1(\tau_j(V_1))) & \cdots & f_n(\sigma_1(\tau_j(V_1))) \\ \vdots & \vdots & \vdots & \vdots \\ f_1(\sigma_{d-1}(\tau_j(V_1))) & f_2(\sigma_{d-1}(\tau_j(V_1))) & \cdots & f_n(\sigma_{d-1}(\tau_j(V_1))) \end{matrix} \tag{3.4}$$

This means that it is possible to go from (3.2) to (3.3) just by applying τ_j as defined above; in other words all the rows of (3.3) can be obtained from (3.2) by applying τ_j and then respectively $\sigma_i \in \{I, \sigma_1, \cdots, \sigma_{d-1}\}$.□

3.1.3 Proposition III

If one adjoins to $Gal(P/K)$ all the roots of an auxiliary equations $r, r', r'', \cdots$, then each subgroup of Preposition II will have the same substitutions.

Proof: Let s be an expression of all the roots $r, r', r'', \cdots$ of an irreducible equation such that s satisfies Lemma II and Lemma III; this means that

$$k(r, r', r'', \cdots) = k(s)$$

Let us suppose that the new Galois group is $H = Gal(P/k(s)) = \{I, k_1, k_2, \cdots\}$. Let s' be a conjugate of s in k, so $k(s) = k(s')$ (as in Lemma IV) and let $\tau \in Gal(P/k)$ such that $s' = \tau(s)$. Let τ^{-1} be the inverse of τ, so $\tau^{-1}s' = s$. Let $k_i \in Gal(P/k(s))$, from the definition of $Gal(P/k(s))$, it follows that:

$$k_i\tau^{-1}s' = k_i s = s$$

Applying τ,

$$\tau k_i \tau^{-1} s' = \tau s = s'$$

In brief, $\forall \tau \in G = Gal(P/k)$ it follows that:

$$H = \tau H \tau^{-1}$$

This shows that all the rows of the second group can be obtained from the rows of the first one by applying τ. This is equivalent to:

$$\tau^{-1} Gal(P/k(s))\tau = Gal(P/k(s))$$

that is the definition of normal subgroup. □

Observation

Let us suppose that the first group (the one regarding s) is of the form:

$$\begin{array}{c|cccc} Id & Id_1 & Id_2 & \cdots & Id_n \\ s & s_1 & s_2 & \cdots & s_n \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots & \vdots \end{array}$$

The second line of the above table can be obtained by using the *position*: if Id_j in the first line goes to position k in the second line, then

$$p_s(j) = k$$

So $s_j = Id_{p_s^{-1}(j)}$ and the first group looks like:

$$(H) \quad \begin{array}{c|cccc} Id & Id_1 & Id_2 & \cdots & Id_n \\ s & Id_{p_s^{-1}(1)} & Id_{p_s^{-1}(2)} & \cdots & Id_{p_s^{-1}(n)} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots & \vdots \end{array}$$

Let us suppose that τ is the first line of the second group, then it can be observed that the second line is as follows:

$$(\tau \circ H) \quad \begin{array}{c|cccc} \tau & \tau_1 & \tau_2 & \cdots & \tau_n \\ \tau \circ s & \tau_{p_s^{-1}(1)} & \tau_{p_s^{-1}(2)} & \cdots & \tau_{p_s^{-1}(n)} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots & \vdots \end{array}$$

It must be proof that:

$$\tau(s(Id_j)) = \tau_{p_s^{-1}(j)}$$

From one hand:

$$s(Id_j) = Id_{p_s^{-1}(j)}$$

applying τ to both members:

$$\tau(s(Id_j)) = \tau(Id_{p_s^{-1}(j)})$$

From the other:

$$\tau(Id_{p_s^{-1}(j)}) = \tau_{p_s^{-1}(j)}$$

so:

$$\tau(s(Id_j)) = \tau_{p_s^{-1}(j)}$$

□

It is possible to repeat the above reasoning in order to obtain $H \circ \tau$ and the comparison of the two representations tells if the subgroup is normal. Let us consider two example:

1. $$(H_3) \quad \begin{array}{c|ccc} Id & a & b & c \\ s & b & c & a \\ t & c & a & b \end{array}$$

   Let us apply the technique above:

   (a) $$(\tau \circ H_3) \quad \begin{array}{c|ccc} \tau & b & a & c \\ \tau \circ s & a & c & b \\ \tau \circ t & c & b & a \end{array}$$

   (a) $$(H_3 \circ \tau) \quad \begin{array}{c|ccc} \tau & b & a & c \\ s \circ \tau & a & c & b \\ t \circ \tau & c & b & a \end{array}$$

   Immediately, it is possible to see that, unless a rearrangement of the rows' order, $\tau \circ H_3 = H_3 \circ \tau$ so H is a normal subgroup.

2. On the other hand, let us consider:

$$(H_4)\quad \begin{array}{c|cccc} Id & a & b & c & d \\ s & b & c & d & a \\ t & c & d & a & b \\ f & d & a & b & c \end{array}$$

Let us apply the technique above:

(a)

$$(\tau \circ H_4)\quad \begin{array}{c|cccc} \tau & b & a & c & d \\ \tau \circ s & a & c & d & b \\ \tau \circ t & c & d & b & a \\ \tau \circ f & d & b & a & c \end{array}$$

(a)

$$(H_4 \circ \tau)\quad \begin{array}{c|cccc} \tau & b & a & c & d \\ s \circ \tau & c & b & d & a \\ t \circ \tau & d & c & a & b \\ f \circ \tau & a & d & b & c \end{array}$$

Immediately, it is possible to see that $\tau \circ H_4 \neq H_4 \circ \tau$ so H is not a normal subgroup.

3.1.4 Proposition IV

If one adjoins to an equation the numerical value $r = R(a, b, c, \cdots)$ with $R \in k[x_1, x_2, \cdots, x_n]$, then $Gal(P/k)$ will be reduced as $Gal(P/k(r))$. In other words, the new group will contain only the permutations which leave r invariant.

Proof: Let us suppose to construct $Gal(P/k(r))$ as in Proposition I considering $k(r)$ as the new base camp. Let us consider the minimal polynomial $Q(x)$ of V_1 over $k(r)$, there will be $degQ$ permutations which constitute $Gal(P/k(r))$. By the way $Gal(P/k(r))$ has been constructed, its permutations, which are also in $Gal(P/k)$, are the ones that leave r invariant. □

Let us note that Proposition IV can be deduced from Proposition III because r can be seen as a root of an auxiliary equation since r belongs to a finite vector space.

3.1.5 Proposition V

In which case is an equation solvable by simple radicals?
First of all, an equation is solved when its group is reduced in such a way that it contains only one permutation. From now on, it will be explained how an equation can be solved by radicals.
Let us suppose to adjoin to the base camp K a radical (that is an extraction of roots of an element $\in K$); from Proposition II, it follows that: either the group of permutations of the equation remains the same or the group diminishes. Obviously, after a certain finite

number of extractions of a root the group will be diminished otherwise the equation would not be solvable. If there are several ways to diminish the group by the simple extraction of a root, then it is necessary to consider only a radical of the least possible degree among all the simple radicals that could diminish the group of the equation. Therefore let p be the prime number which represents this minimum degree such that the extraction of a root of degree p diminishes the group of the equation.
From now on, it is assumed that a pth root of unity α is included among the quantities of the base camp K. Let us suppose to be in the case on which the group of the equation should decompose into p groups (Proposition II) such that one passes from one to another by a single substitution and the groups contain the same substitutions. Conversely, if the group of the equation can be divided into p groups with the above properties, it is possible to reduce the group of the equation to one of these partial groups by a simple extraction of a pth root and by the adjunction of this pth root.
Let $s(a, b, c, \dots)$ be a function of the roots such that it is invariant under all substitutions of one of the partial groups $H \in Gal(P/K)$ and it is variant for any other substitution. It is shown why such $s(a, b, c, \dots)$ exists. Let $V = V(a, b, c, \dots)$ be a function as in Lemma II, by applying all the permutations $\in H$ to this V it is possible to construct a polynomial of degree $\#H = h$:

$$\prod_{\tau \in H} (x - \tau(V)) = a_0 + a_1 x + \cdots + a_{h-1} x^{h-1} + x^h \tag{3.5}$$

Since the polynomial $\prod_{\tau \in H}(x - \tau(V))$ is invariant for $\forall g \in H$, it follows that the h expressions $a_0, a_1, \dots, a_{h-1}$ are invariant under any substitution of H. So, not only an expression of $s(a, b, c, \dots)$ is invariant under all the substitutions of H, but h expressions have been found with this property. On the other hand, let us suppose to take a generic permutation $\sigma \in Gal(P/K)$ such that $\sigma(a_i) = a_i$ with $0 \leq i \leq (h-1)$ then $\sigma \in H$. Since the a_i's do not change under this σ, from (3.5) follows that $\prod_{\tau \in H}(x - \tau(V))$ does not. This means that:

$$\prod_{\tau \in H} (x - \tau(V)) = \prod_{\tau \in H} (x - \sigma \cdot \tau(V))$$

This implies that the permutations of the form $\sigma \cdot \tau$ are the same that the ones $\in H$, in particular from the combination of σ with the identity permutation ($I \in H$ since H is a subgroup) follows that $\sigma \cdot I = \sigma$ then $\sigma \in H$.
In brief, it has been shown that $\forall \tau \in H \subset Gal(P/K)$ an element $s(a, b, c, \dots)$ exists such that $\tau(s) = s$ and that if a generic permutation $\sigma \in Gal(P/K)$ is such that $\sigma(s) = s$ then $\sigma \in H$.
Let us apply to s one of the substitution $\theta \in (Gal(P/K) \setminus H)$: $\theta(s) = s_1$, let us apply again θ to s_1 , $\theta(s_1) = s_2$ and so forth. Since p is a prime number, this sequence will end with s_{p-1}. It is evident that the function

$$(s + \alpha s_1 + \alpha^2 s_2 + \cdots + \alpha^{p-1} s_{p-1})^p$$

will be invariant under all the permutations of $Gal(P/K)$ so it belongs to K (Proposition I). If one adjoins the pth root of this quantity to K, then the new Galois group will be H by Proposition IV. Now it is possible to see H as the preceding Galois group was seen

and decompose it as described above until the new group contains only one permutation. Let us apply the theory to the calculation of Galois group for a general polynomial equation of fourth degree; as was shown in Lagrange Resolvents, the general quartic equation can be reconducted to the resolution of a cubic, which itself requires the extraction of a square root. Let us suppose that the field of coefficients is K and let us adjoin to K a square root; since the first group contains twenty-four elements, it is decomposed into two groups of twelve elements. If the roots are designed by $\{a, b, c, d\}$ one of these groups is:

$$\begin{array}{ccc} abcd & acdb & adbc \\ badc & cabd & dacb \\ cdab & dbac & bcad \\ dcba & bdca & cbda \end{array}$$

Adjoin a cubic root to the first extension field, the new group is:

$$\begin{array}{c} abcd \\ badc \\ cdab \\ dcba \end{array}$$

that splits again into two groups:

$$\begin{array}{cc} abcd & cdab \\ badc & dcba \end{array}$$

After a simple extraction of a square root, the group will have:

$$\begin{array}{c} abcd \\ badc \end{array}$$

which will be resolved by a simple extraction of a square root.

3.1.6 Proposition VI

An irreducible equation of prime degree cannot become reducible by the adjunction of a radical unless it is factored into linear factors[1].

Proof: Let $K(\omega)$ be a field with ω a pth root of unity with $\omega \neq 1$, let $P \in K(\omega)$ be a polynomial of degree p prime and let r a radical. Let us consider the extension $K(\omega, r)$ of the above field. Let $P = F_1 F_2 \dots F_l$ be a factorization in $K(\omega, r)$; this means that the generic polynomial F_i has coefficients in $K(\omega, r)$: the aim is to show that, under the hypothesis above, every F_i is a polynomial of degree 1.
Let $r', r'', \dots$ be conjugates of r and let $\tau \in Gal(P/K)$ such that $\tau(r) = r'$; let us suppose without losing generality that r is a roof of F_1 and r' the one of the generic F_j with $j \neq 1$. Let us apply τ to r:

$$\tau P = \tau(F_1, F_2, \dots F_l) = \tau F_1 \tau F_2 \dots \tau F_l$$

[1] It is supposed that the field before the extension contains the roots of unity so that the adjunction of this radical implies the adjunction of all its conjugates.

From one hand, $\tau P = P$ since P has coefficients in K; on the other hand, since $K(\omega, r)$ contains all the conjugates of r, it follows that $\tau F_i = F_j$ for $i \neq j$. Since polynomial's factorization is unique in a field, except for the order of the factors, it follows that:

$$F_1, F_2, \dots F_l = \tau F_1 \tau F_2 \dots \tau F_l$$

This implies that the F_j have all the same degree and since p is prime they must have degree 1. This means that $Gal(P/K)$ leaves $K(\omega, r)$ invariant. □

3.1.7 Proposition VII

What is the group of an irreducible equation of prime degree p if it is solvable by radicals? If an irreducible equation of prime degree is solvable by radicals then the group of this equation can contain no substitutions other than those of the form:

$$x_k \quad x_{ak+b}$$

with a and b constants.

Proof: From Proposition VI, it follows that the smallest group possible before the one which contains only a single permutation will contains p permutations.
A group of permutations of p letters contains exactly p permutations if and only if each of them derives from any other by a cyclic substitution of order p. Let's $G \subset S_p$ where S_p is the symmetric group of p elements; first of all it is shown why G is cyclic and then, taken a generic element a, how to choose τ. Let us suppose that τ of order θ does not generate G, that means there is $\alpha \in G$ such that $\alpha \neq \tau^i$ for each $0 \leq i \leq (\theta - 1)$. The following sets of permutations $A = \{1, \tau, \tau^2, \cdots, \tau^{\theta-1}\}$ and $B = \{\alpha, \alpha\tau, \alpha\tau^2, \cdots, \alpha\tau^{\theta-1}\}$ are in G and such that they are all different ($\alpha\tau = \alpha\tau^2 \Rightarrow \tau = \tau^2$ but $\tau \neq \tau^2$ by the hypothesis) and $\alpha\tau^i \neq \tau^j$. Since A and B contain the same number of elements and since p is prime, it is not possible to divide p by 2 so τ is a generator of G. Let us take a generic permutation $\{a, \tau(a), \tau^2(a), \cdots, \tau^{p-1}(a)\}$ then this can be chosen as τ.
The next to the last group will be of the form:

$$(C) \quad \begin{array}{cccccccc} x_0 & x_1 & x_2 & x_3 & \cdots & \cdots & \cdots & x_{n-1} \\ x_1 & x_2 & x_3 & x_4 & \cdots & \cdots & x_{n-1} & x_0 \\ x_2 & x_3 & \cdots & \cdots & \cdots & x_{n-1} & x_0 & x_1 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ x_{n-1} & x_0 & x_1 & \cdots & \cdots & \cdots & \cdots & x_{n-2} \end{array}$$

with $a_0, x_1, x_2, \cdots, x_n$ being the roots. This cyclic group of permutations C is normal in the preceding one, so if τ is in the preceding group also the following is in it:

$$(\tau) \quad \begin{array}{cccccccc} x_{\tau(0)} & x_{\tau(1)} & x_{\tau(2)} & x_{\tau(3)} & \cdots & \cdots & \cdots & x_{\tau(n-1)} \\ x_{\tau(1)} & x_{\tau(2)} & x_{\tau(3)} & x_{\tau(4)} & \cdots & \cdots & x_{\tau(n-1)} & x_{\tau(0)} \\ x_{\tau(2)} & x_{\tau(3)} & \cdots & \cdots & \cdots & x_{\tau(n-1)} & x_{\tau(0)} & x_{\tau(1)} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ x_{\tau(n-1)} & x_{\tau(0)} & x_{\tau(1)} & \cdots & \cdots & \cdots & \cdots & x_{\tau(n-2)} \end{array}$$

Since the group C is cyclic, it follows that permutations obtained from τ are the same of the ones from C. The generic substitution of $x_i's \in \tau$ subindexes have to satisfy the following rule:

$$f(k+c) = f(k) + C$$

with C being independent of k. Therefore:

$$\begin{gathered} f(k+2c) = f(k) + 2C \\ \cdots\cdots\cdots\cdots \\ f(k+mc) = f(k) + mC \end{gathered}$$

If $c = 1$ and $k = 0$, one finds

$$f(m) = am + b$$

that in terms of k, it is:

$$f(k) = ak + b$$

with a and b being constants. For this reason, the group before G, let us call it $Gal(P/K)$, can contain only substitutions of the form x_k, x_{ak+b} and can contain no cyclic substitutions other than those of the group G. Since the splitting field can be reached by only one step, $Gal(P/K)$ is the actual group of the equation. On the other hand, if this condition is verified then the equation is solvable by radicals. Let us consider the functions:

$$\begin{gathered} (x_0 + \alpha x_1 + \alpha^2 x_2 + \cdots + \alpha^{n-1} x_{n-1})^n = X_1 \\ (x_0 + \alpha x_a + \alpha^2 x_{2a} + \cdots + \alpha^{n-1} x_{(n-1)a})^n = X_a \\ (x_0 + \alpha x_a^2 + \alpha^2 x_{2a^2} + \cdots + \alpha^{n-1} x_{(n-1)a^2})^n = X_{a^2} \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \end{gathered}$$

with α being an nth root of unity and a a primitive root of n. It is possible to find $X_1, X_a, X_{a^2}, \cdots$ since each of them is invariant by cyclic substitutions; so it is necessary and sufficient that every function invariant under the substitutions x_k, x_{ak+b} is rationally known. This means that the function $(X_1 - X)(X_a - X)(X_{a^2} - X)\cdots$ must be known; so the equation which gives this function of the roots must admit a rational value. Let us suppose that the given equation has rational coefficients, then the auxiliary equation of degree $1 \cdot 2 \cdot 3 \ldots (n-2)$ will also have rational coefficients and it will suffice to determine if it does or does not have a rational root. □

3.1.8 Proposition VIII

In order for an irreducible equation of prime degree p to be solvable by radicals it is necessary and sufficient that once any two of the roots are known the others can be deduced from them rationally.

Proof: The necessary condition can be demonstrated as follow.
Let us suppose to adjoin to the field K two roots a, b of the equation; this can be seen as the adjunction of $r = R(a, b)$ and from Proposition IV the new Galois group will contain only the permutations which leave r invariant. From the construction of Galois group,

it follows that the two substitutions x_k, x_{ak+b} never leave two letters in the same place. This implies that the new Galois group contains only one substitution.
On the other hand, this condition is also sufficient: from the hypothesis and from the fact that $Gal(P/K)$ acts transitively over the roots of P, it follows that $p|Gal(P/K)$ and $Gal(P/K) \geq p(p-1)$. From Cauchy's Theorem, it follows that $\mathbb{Z}_p$ is a subgroup of $Gal(P/K)$ and that is normal. □

Observation: the preceding Proposition can be interpreted as follows. Let $f \in Q[x]$ be an irreducible polynomial of prime degree p with all but two roots known; then $Gal(f/Q)$ is isomorphic to S_p. In the case of $p = 5$, the group will be:

$$
\begin{array}{c}
abcde \\
bcdea \\
cdeab \\
deabc \\
eabcd
\end{array}
\qquad
\begin{array}{c}
acebd \\
cebda \\
ebdac \\
bdace \\
daceb
\end{array}
\qquad
\begin{array}{c}
aedcb \\
edcba \\
dcbae \\
cbaed \\
baedc
\end{array}
\qquad
\begin{array}{c}
adbec \\
dbeca \\
becad \\
ecadb \\
cadbe
\end{array}
$$

3.2 Applications

The goal of Galois Theory is to find the roots of polynomial equations in a given field by calculating its group in such field. In practice, the main question arises at the beginning since Galois group is strictly related to these roots. In fact, a group isomorphic to Galois group is calculated and starting from this group it is possible to tell which are the properties of Galois group. In general, Galois group is isomorphic to a subgroup of a symmetric group.

Proposition
Let $P \in K[x]$ a polynomial of degree n with distinct roots; then its Galois group over K has order divisible by n.

Proof: Let r be a root of $P(x)$, $[K(r) : K] = n$ is a factor of the degree of the splitting field over K, which is the size of Galois group over K. □

Theorem
Let $P \in K[x]$ with distinct roots; then $P(x)$ is irreducible over K if and only if the Galois group $Gal(P/K)$ acts transitively on the roots.

Proof: Let P be irreducible over K and let $R = \{a, b, c, \cdots\}$ be the set of its roots; let us consider $P_a(x) = \prod_{\tau \in Gal(P/K)}(x - \tau(a))$. Since P and P_a share the root a, it follows that $P(x)|P_a(x)$ so any root of $P_a(x) \in R$ is of the form $\tau(a)$. This means that the group $Gal(P/K)$ acts transitively on R.
Let us suppose that $Gal(P/K)$ acts transitively on R and let us suppose that P is reducible over K, for example $P(x) = A(x)B(x)$ with $A, B \in K[x]$ such that $A(x) = (x-a)(x-b) = a_0 + a_1x + x^2$. Let us apply a generic $\tau \in Gal(P/K)$ to $A(x)$.

$$(\tau A)(x) = \tau(a_0 + a_1x + x^2) = \tau(a_0) + \tau(a_1)x + x^2$$

Since $A \in K[x]$ and $\tau \in Gal(P/K) \Rightarrow (\tau A)(x) = A(x) = x^2 - (a + b)x + ab$; this implies $\tau(a_1) = -(a + b)$ and $\tau(a_0) = ab$. This is a contradiction since $\exists\gamma \in Gal(P/K)$ such that $\gamma(a) = c$. So $P \in K[x]$ is irreducible. □

3.2.1 Example 1

Let us consider the polynomial $P(x) = x^4 - 4x^2 + 2$ that is irreducible over $\mathbb{Q}$ by the Eisenstein criterion.

$$x^4 - 4x^2 + 2 = (x^2 - 2)^2 - 4 + 2 = (x^2 - 2)^2 - 2 \tag{3.6}$$

Let us suppose to adjoin $\sqrt{2}$ to $\mathbb{Q}$; in the new field $\mathbb{Q}(\sqrt{2})$ the (3.6) becomes

$$(x^2 - 2)^2 - 2 = (x^2 - 2 - \sqrt{2})(x^2 - 2 + \sqrt{2}) = (x^2 - (2 + \sqrt{2}))(x^2 - (2 - \sqrt{2})) \tag{3.7}$$

Now let us adjoin $\sqrt{2 + \sqrt{2}}$ to $\mathbb{Q}(\sqrt{2})$, then (3.7) becomes:

$$(x^2 - 2)^2 - 2 = (x - \sqrt{2 + \sqrt{2}})(x + \sqrt{2 + \sqrt{2}})(x - \sqrt{2 - \sqrt{2}})(x + \sqrt{2 - \sqrt{2}})$$

Let us compute $Gal(P/\mathbb{Q})$. Since both $\sqrt{2}$ and $\sqrt{2+\sqrt{2}}$ satisfy an equation of degree 2, then $Gal(P/Q)$ contains four elements. Let us call with a, b, c, d the roots of $P(x)$ and let us suppose without losing of generality that $a = \sqrt{2+\sqrt{2}}, b = -\sqrt{2+\sqrt{2}}, c = \sqrt{2-\sqrt{2}}, d = -\sqrt{2-\sqrt{2}}$; then one of the four permutations will be $I = \{a\,b\,c\,d\}$. The other one, let us call it σ_1, will be $\{b\,a\,d\,c\}$ since the product $a \cdot c = \sqrt{2}$ then also $\sigma_1(a) \cdot \sigma_1(c) = \sqrt{2}$. Let us now complete the following representation of Galois group:

$$\begin{array}{c|cccc} I & a & b & c & c \\ \sigma_1 & b & a & d & c \\ \sigma_2 & - & - & - & - \\ \sigma_3 & - & - & - & - \end{array} \tag{3.8}$$

Since $P(x)$ is irreducible in $\mathbb{Q}$ then Galois group acts transitively on the roots and the order of the lines is irrelevant, (3.8) becomes:

$$\begin{array}{c|cccc} I & a & b & c & c \\ \sigma_1 & b & a & d & c \\ \sigma_2 & c & d & - & - \\ \sigma_3 & d & c & - & - \end{array} \tag{3.9}$$

In order to complete the representation, it must be consider that σ_2 and σ_3 have to be permutations such that since $a \cdot c = -\sqrt{2}$ then $\sigma_i(a) \cdot \sigma_i(c) = -\sqrt{2}$; the (3.9) becomes:

$$\begin{array}{c|cccc} I & a & b & c & c \\ \sigma_1 & b & a & d & c \\ \sigma_2 & c & d & b & a \\ \sigma_3 & d & c & a & b \end{array} \tag{3.10}$$

So $Gal(P/Q)$ is isomorphic to $\mathbb{Z}_4$. Figure 3.4 and figure 3.5 show the extension fields and the corresponding Galois groups.

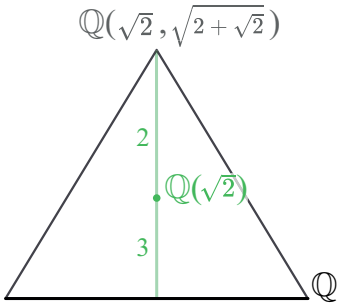

Figure 3.4. Field extensions for $x^4 - 4x^2 + 2$

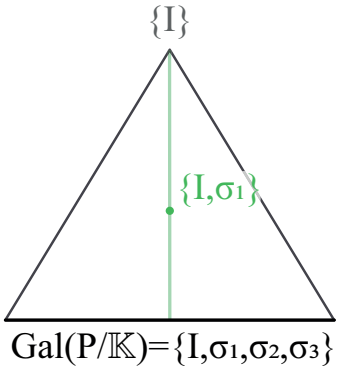

Figure 3.5. Galois groups for $x^4 - 4x^2 + 2$

3.2.2 Example 2

Let us consider the polynomial $P(x) = x^4 + px^2 + q$ that is irreducible over $\mathbb{Q}$ where p and q are transcendental numbers. Let us call $a\,b\,c\,d$ the four distinct roots end let us suppose to adjoin $\omega = \sqrt{p^2 - 4q}$ to $\mathbb{Q}$; after that let's adjoin $\mu = \sqrt{\frac{-p-\omega}{2}}$ and then $\eta = \sqrt{\frac{-p+\omega}{2}}$ as shown figure 3.6.

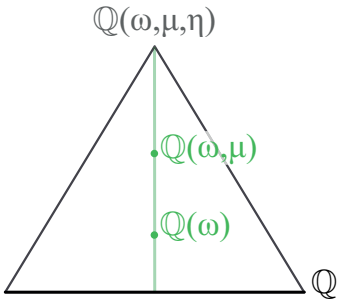

Figure 3.6. Field extensions for $x^4 + px^2 + q$

The corresponding Galois groups in each of the above fields are respectively: $D_4 = \{I, (ab), (cd), (ab)(cd), (ac)(bd), (ad)(bc), (acbd), (adbc)\}$, $K = \{I, (ab), (cd), (ab)(cd)\}$, $\mathbb{Z}_2 = \{I, (ab)\}$ and $E = \{I\}$. They are shown in figure 3.7.

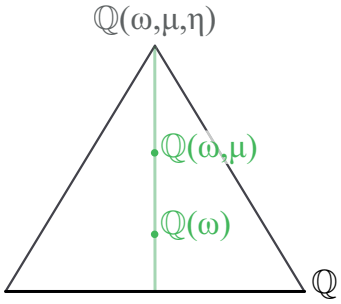

Figure 3.7. Galois groups for $x^4 + px^2 + q$

So $Gal(P/Q)$ is isomorphic to D_4.

3.2.3 Example 3

Given $P(x) = (x^2 - 2)(x^2 - 3)$ let us compute $Gal(P/\mathbb{Q})$.
Figure 3.8 shows the possible ways to go from $\mathbb{Q}$ to $\mathbb{Q}(\sqrt{2}, \sqrt{3})$:

1. adjoin $\sqrt{3}$ and then $\sqrt{2}$;
2. adjoin $\sqrt{6}$ and then $\sqrt{2}$;
3. adjoin $\sqrt{2}$ and then $\sqrt{3}$;

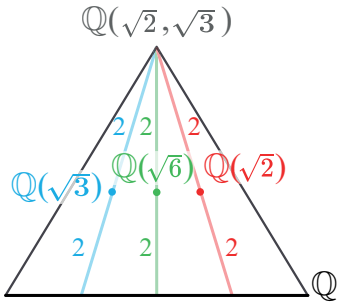

Figure 3.8. Field extensions for $(x^2 - 2)(x^2 - 3)$

From the above decomposition, it follows that $Gal(P/\mathbb{Q})$ contains four elements and if $\{a = \sqrt{3}, b = -\sqrt{3}, c = \sqrt{2}, d = -\sqrt{2}\}$, then these four permutations are:

I	$abcd$
σ_1	$bacd$
σ_2	$abdc$
σ_3	$badc$

In terms of groups, the corresponding Galois groups are (figure 3.9):

1. $\{1, \sigma_1\}$
2. $\{1, \sigma_3\}$
3. $\{1, \sigma_2\}$

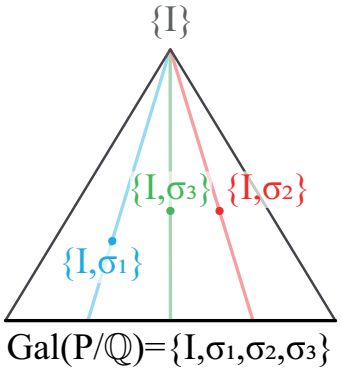

Figure 3.9. Galois groups for $(x^2-2)(x^2-3)$

3.2.4 Example 4

In this example, it is compute Galois group of $x^n - 1$ in $\mathbb{Q}$.

As Galois said in the first page of his Mémoire, Gauss was aware of the factorization of the equation $x^n - 1$. From Galois point of view, Gauss proved, somewhere in *Disquisitiones Arithmeticae*, that the Galois group $Gal(P/\mathbb{Q})$ of $P(x) = x^n - 1$ is isomorphic to $(\mathbb{Z}_n^*, \cdot)$ where

$$\mathbb{Z}_n^* = \{d < n : d \text{ is coprime with } n\} .$$

and $\cdot$ is the multiplication modulo n.

Here is a proof of Gauss' result by using Galois Theory.

Let $\omega := e^{i\frac{2\pi}{n}}$ be a primitive root. As explained in section 1.3 (Cyclotomic Equations) $P(x)$ is completely factorized in $\mathbb{Q}(\omega)$:

$$x^n - 1 = \prod_{j=1}^{n} (x - \omega^j) .$$

Observe that ω^d is also a primitive root if d is coprime with n. So the set of primitive roots is in 1-1 correspondence with $\mathbb{Z}_n^*$.

Gauss proved that the so called cyclotomic polynomial:

$$\Phi_n(x) := \prod_{d \in \mathbb{Z}_n^*} (x - \omega^d)$$

belongs to $\mathbb{Z}[x]$ and it is irreducible over $\mathbb{Q}(x)$. It turns out that this is equivalent to show that the Galois group of $P(x) = x^n - 1$ is isomorphic to $\mathbb{Z}_n^*$.

Let us start by observing that if $\tau \in Gal(P/\mathbb{Q})$ then

$$\tau(\omega) = \omega^d$$

where $d \in \mathbb{Z}_n^*$. This is so because the row associated to τ in the Galois group is going to be

$$\tau \,|\, \omega^d \; \omega^{2d} \; \omega^{3d} \cdots \; \omega^{nd}$$

and the powers of ω^{jd}, $j = 1, \cdots, n$ are distinct from each other if and only if $d \in \mathbb{Z}_n^*$. Thus $\tau(\Phi_n(x)) = \Phi_n(x)$ for each $\tau \in Gal(P/\mathbb{Q})$. This shows that the coefficients of $\Phi_n(x)$ are rational numbers i.e. $\Phi_n(x) \in \mathbb{Q}(x)$.

To show that $\Phi_n(x)$ is irreducible over $\mathbb{Q}$ we start by observing that $\Phi_n(x)$ has coefficients in $\mathbb{Z}$ i.e. $\Phi_n(x) \in \mathbb{Z}[x]$. This is so because $\Phi_n(x)$ divides $P(x) = x^n - 1$ and it has leading coefficient 1. Let $f(x)$ be the minimal polynomial of ω over $\mathbb{Q}$. Then $f(x) \in \mathbb{Z}[x]$ and there is $h(x) \in \mathbb{Z}[x]$ such that

$$\Phi_n(x) = f(x) \cdot h(x) \tag{3.11}$$

Let p be a prime number which does not divide n. Observe that

$$\Phi_n(\omega^p) = 0\,.$$

Claim: ω^p is also a root of $f(x)$.

Proof of the Claim: By contradiction, if not we should have $h(\omega^p) = 0$ by the equation (3.11). This implies that $f(x)$ divides $h(x^p)$. Now we reduce modulo p as in Eisenstein's criterion:

$$h(x^p) \equiv h(x)^p \equiv f(x) \cdot g(x) \pmod{p}$$

Then f and h as polynomials in $\mathbb{Z}_p[x]$ have a common factor hence a common root in some extension. But then $\Phi_n(x)$ has a multiple root regarded as polynomial in $\mathbb{Z}_p[x]$. Thus also $x^n - 1$ would have a multiple root in some extension of $\mathbb{Z}_p$. This is a contradiction since the multiple roots of $x^n - 1$ are also roots of the derivative $n \cdot x^{n-1}$. **This proves the claim.**

Now notice that ω^p is also a primitive root of n. Let q be another prime number which not divides n. Then the same argument shows that $(\omega^p)^q$ is a root of $f(x)$. Thus for $d \in \mathbb{Z}_n^*$ we got that ω^d is a root of $f(x)$. Then $f(x) = \Phi_n(x)$ showing that $\Phi_n(x)$ is irreducible over $\mathbb{Q}$.

The irreducibility of $\Phi_n(x)$ implies that $Gal(P/\mathbb{Q})$ acts transitively on the roots of $\Phi_n(x)$. So for each $d \in \mathbb{Z}_n^*$ there is a row of $Gal(P/\mathbb{Q})$ of the form

$$\tau \,|\, \omega^d \; \omega^{2d} \; \omega^{3d} \cdots \; \omega^{nd}$$

Thus $Gal(P/\mathbb{Q})$ is in 1-1 correspondence with $\mathbb{Z}_n^*$ and for each $\tau \in Gal(P/\mathbb{Q})$ there is $d \in \mathbb{Z}_n^*$:

$$\tau \leftrightarrow d$$

and if $\sigma \in Gal(P/\mathbb{Q})$ and $\sigma \leftrightarrow e$ then the composition $\tau \circ \sigma$ corresponds to the multiplication $e \cdot d \in \mathbb{Z}_n^*$:

$$\tau \circ \sigma \leftrightarrow e \cdot d$$

Notice that $Gal(P/\mathbb{Q}) = Gal(\Phi_n(x)/\mathbb{Q})$.

3.2.5 Example 5

Given $P(x) = x^3 - 2$ let us compute $Gal(P/\mathbb{Q})$.
As shown in figure 3.10 it is possible to go from the base camp $\mathbb{Q}$ to the top of the mountain $\mathbb{Q}(\omega, \alpha)$ into different ways.

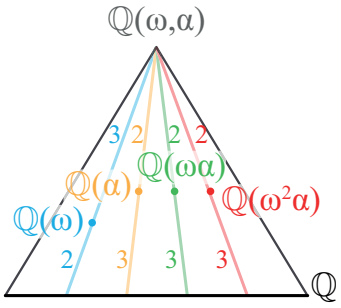

Figure 3.10. Field extensions for $x^3 - 2$

1. adjoin a cube root of unity ω to $\mathbb{Q}$ and then α (the real root of $P(x)$);
2. adjoin α and then ω;
3. adjoin $\omega\alpha$ and then ω;
4. adjoin $\omega^2\alpha$ and then ω;

From the above decomposition, it follows that $Gal(P/\mathbb{Q})$ contains six elements and if $\{a = \sqrt[3]{2}, b = \sqrt[3]{2}\omega, c = \sqrt[3]{2}\omega^2\}$ then these six permutations are:

I	abc
σ_1	acb
σ_2	bac
σ_3	bca
σ_4	cab
σ_5	cba

In terms of groups, the corresponding Galois groups are shown in figure 3.11 and they are:

1. $\{1, \sigma_3, \sigma_4\}$

2. $\{1, \sigma_1\}$
3. $\{1, \sigma_5\}$
4. $\{1, \sigma_2\}$

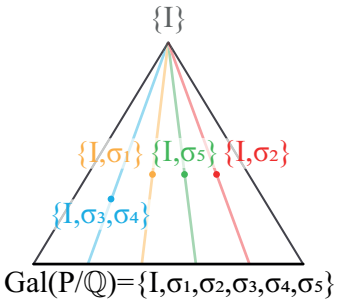

Figure 3.11. Galois groups for $x^3 - 2$

3.3 Other Interpretations of Galois Theory

According to modern algebra, Galois theory can be seen in terms of automorphisms and in particular permutation group of the roots are seen as the automorphism group of a field extension. This interpretation has been developed by Richard Dedekind, Leopold Kronecker and Emil Artin. In this formulation, a group is not associated with a given equation $P(x) = 0$ with coefficient in a field K, $(Gal(P/K)$, but with a normal extension field $L \supset K$, $Gal(L/K)$. In this case the group $Gal(L/K)$ is all made of automorphisms of L which leaves element of K fixed. In Galois' formulation it is evident that extending the field reduces or leaves unchanged the Galois group; on the other hand, Dedekindian's approach underlines that Galois group depends only on the splitting fields [Ed].
Using the software *Mathematica* and the code *galois.m* [Pa], it is possible to obtain the roots of a given polynomial in terms of automorphisms.
For example, let's consider the polynomial $P(x) = x^5 - 5x + 12$ over $\mathbb{Q}$; the steps to follow are:

```
Define[a^5, 5a-12]
Factor[X^5 - 5X + 12, a]
```

and it is obtained:

$$(-a+X)\left(2-\frac{5a}{4}-\frac{a^2}{4}-\frac{a^3}{4}-\frac{a^4}{4}+X+\frac{3aX}{4}-\frac{a^2X}{4}-\frac{a^3X}{4}-\frac{a^4X}{4}+X^2\right)$$
$$\left(-1-\frac{a}{2}-\frac{a^3}{2}-X+\frac{aX}{4}+\frac{a^2X}{4}+\frac{a^3X}{4}+\frac{a^4X}{4}+X^2\right)$$

After that,

```
Define[b^2, 1 + a / 2 + a^3 / 2 + b - a b / 4 - a^2 b / 4 - a^3 b / 4 - a^4 b / 4D]
Factor[X^5 - 5 X + 12, a, b]
```

obtaining:

$$(-a+X)(-b+X)\left(-1+\frac{a}{4}+\frac{a^2}{4}+\frac{a^3}{4}+\frac{a^4}{4}+b+X\right)$$
$$\left(\frac{3}{2}+\frac{a}{4}-\frac{a^2}{4}-\frac{a^3}{4}-\frac{a^4}{4}-\frac{b}{2}-\frac{ab}{2}+X\right)\left(-\frac{1}{2}+\frac{a}{2}+\frac{b}{2}+\frac{ab}{2}+X\right)$$

Looking at the result, it follows immediately that:

```
c = 1 - a / 4 - a^2 / 4 - a^3 / 4 - a^4 / 4 - b;
d = -3 / 2 - a / 4 + a^2 / 4 + a^3 / 4 + a^4 / 4 + b / 2 + a b / 2;
e = 1 / 2 - a / 2 - b / 2 - a b / 2;
```

Thanks to the command *Homomorph* of the package [Pa], it is possible to define a homomorphism.

```
Homomorph[F]
F[a] := b
F[b] := a

CheckHomo[F, a, b]

True

Homomorph[F]
F[a] := b
F[b] := c
CheckHomo[F, a, b]

f[b] * f[b] is not equal to f[b*b]
False

Homomorph[F]
F[a] := a
F[b] := c
CheckHomo[F, a, b]

True
```

In terms of permutations, the results above can be described as:

$$\begin{pmatrix}1&2&3&4&5\\2&1&4&3&5\end{pmatrix} \textit{ and } \begin{pmatrix}1&2&3&4&5\\1&3&2&5&4\end{pmatrix}$$

In *Mathematica* it is possible to use the command *P* and then *Group* in order to obtain the subgroup of S_5 generated by these two permutations:

```
P[2, 1, 4, 3, 5]

P[2, 1, 4, 3]

P[1, 3, 2, 5, 4]

P[1, 3, 2, 5, 4]

P[2, 1, 4, 3] · P[1, 3, 2, 5, 4]

P[2, 4, 1, 5, 3]

Group[{P[2, 1, 4, 3], P[1, 3, 2, 5, 4]}]

{P[], P[2, 1, 4, 3], P[1, 3, 2, 5, 4], P[3, 1, 5, 2, 4], P[2, 4, 1, 5, 3],
P[4, 2, 5, 1, 3], P[3, 5, 1, 4, 2], P[5, 3, 4, 1, 2],
P[4, 5, 2, 3, 1], P[5, 4, 3, 2, 1]}.
```

3.4 Further application

A remarkable application of Galois Theory is in criptography: the *Advanced Encryption Standard* is a subset of Rijndael block cipher used by the National Institute of Standards and Technology; the Rijndael S-Box is a substitution box that is a basic component of symmetric key algorithms. A S-Box takes some number of input bits m and transforms them into some number of output bits n, where n may be not equal to m.
The Rijndael S-Box is a bijective map $S : \mathbb{Z}_2^8 \to \mathbb{Z}_2^8$ obtained by composition of the inverse transformation and an affine transformation. This means:

$$S(\mathbf{a}) = \mathbf{A} \cdot \mathbf{v}$$

where

$$\mathbf{A} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix} \qquad \mathbf{a}^{-1} = \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \end{bmatrix}$$

Due to the inversion the map is non linear and this implies that the *confusion* is satisfied: in other words the relationship between the ciphertext and the symmetric key is as complex as possible.

Note Through Galois Theory bytes $\mathbf{a} = [a_7\, a_6 \cdots a_0]$ in $\mathbb{Z}_2^8$ are regarded as elements $a_7\alpha^7 + a_6\alpha^6 + \cdots + a_0$ of the Galois extension $\mathbb{Z}_2(\alpha)$ where α is a root of the irreducible polynomial $P(X) = X^8 + X^4 + X^3 + X + 1 \in \mathbb{Z}_2[X]$. So if $\mathbf{a} = [a_7\, a_6 \cdots a_0]$ and $\mathbf{b} = [b_7\, b_6 \cdots b_0]$ the product $\mathbf{a} \cdot \mathbf{b} = \mathbf{c} = [c_7\, c_6 \cdots c_0]$ is defined as the byte obtained from the remainder $c_7X^7 + c_6X^6 + \cdots + c_0$ of the product
$(a_7X^7 + a_6X^6 + \cdots + a_0) \cdots (b_7X^7 + b_6X^6 + \cdots + b_0)\ mod P(X)$.

Chapter 4

Mémoire

Sur les conditions de résolubilité des équations par radicaux. [Li]

PRINCIPES Je commencerai par établir quelques définitions et une suite de lemmes qui sont tous connus.

Définitions. Une équation est dite réductible quand elle admet des diviseurs rationnels; irréductible dans le cas contraire.

Il faut ici expliquer ce qu'on doit entendre par le mot *rationnel*, car il se représentera souvent.

Quand l'équation a *tous* ses coefficients numériques et rationnels, cela veut dire simplement que l'équation peut se décomposer en facteurs qui aient leurs coefficients numériques et rationnels.

Mais quand les coefficients d'une équation ne seront pas *tous* numériques et rationnels, alors il faudra entendre par diviseur rationnel un diviseur dont les coefficients s'exprimeraient en fonction rationnelle des coefficients de la proposée, en général par quantité rationnelle, une quantité qui s'exprime en fonction rationnelle des coefficients de la proposée.

Il y a plus: on pourra convenir de regarder comme rationnelle toute fonction rationnelle d'un certain nombre de quantités déterminées, supposées connues à priori. Par exemple, on pourra choisir une certaine racine d'un nombre entier, et regarder comme rationnelle toute fonction rationnelle de ce radical.

Lorsque nous conviendrons de regarder ainsi comme connues de certaines quantités, nous dirons que nous les *adjoignons* à l'équation qu'il s'agit de résoudre. Nous dirons que ces quantités sont *adjointes* à l'équation.

Cela posé, nous appellerons *rationnelle* toute quantité qui s'exprimera en fonction rationnelle des coefficients de l'équation et d'un certain nombre de quantités *adjointes* à l'équation et convenues arbitrairement.

Quand nous nous servirons d'équations auxiliaires, elles seront rationnelles, si leurs coefficients sont rationnels en notre sens.

On voit, au surplus, que les propriétés et les difficultés d'une équation peuvent être tout à fait différentes suivant les quantités qui lui sont adjointes. Par exemple, l'adjonction d'une quantité peut rendre réductible une équation irréductible.

Ainsi, quand on adjoint à l'équation $\frac{x^n-1}{x-1} = 0$, où n est premier, une racine d'une des

équations auxiliaires de M. Gauss, cette équation se décompose en facteurs, et devient par conséquent réductible.

Les substitutions sont le passage d'une permutation à l'autre. La permutation d'où l'on part pour indiquer les substitutions est toute arbitraire, quand il s'agit de fonctions; car il n'y a aucune raison pour que, dans une fonction de plusieurs lettres, une lettre occupe un rang plutôt qu'un autre. Cependant, comme on ne peut guère se former l'idée d'une substitution sans se former celle d'une permutation, nous ferons dans le langage un emploi fréquent des permutations, et nous ne considérerons les substitutions que comme le passage d'une permutation à une autre.

Quand nous voudrons grouper des substitutions, nous les ferons toutes provenir d'une même permutation. Comme il s'agit toujours de questions où la disposition primitive des lettres n'influe en rien dans les groupes que nous considérerons, on devra avoir les mêmes substitutions, quelle que soit la permutation d'où l'on sera parti. Donc, si dans un pareil groupe on a les substitutions S et T, on est sûr d' avoir la substitution ST. Telles sont les définitions que nous avons cru devoir rappeler.

Lemme I. «Une équation irréductible ne peut avoir aucune racine commune avec une équation rationnelle, sans la diviser.»

Car le plus grand commun diviseur entre l'équation irréductible et l'autre équation, sera encore rationnel; donc, etc.

Lemme II. «Étant donnée une équation quelconque, qui n'a pas de racines égales, dont les racines sont $a, b, c, \cdots$, on peut toujours former une fonction V des racines, telle qu'aucune des valeurs que l'on obtient en permutant dans cette fonction les racines de toutes manières, ne soient égales.»

Par exemple, on peut prendre

$$V = Aa + Bb + Cc + \cdots$$

$A, B, C, \cdots$ étant des nombres convenablement choisis.

Lemme III. «La fonction V étant choisie comme il est indiqué dans l'article précédent, elle jouira de cette propriété, que toutes les racines de l'équation proposée s'exprimeront rationnellement en fonction de V.»

En effet, soit

$$V = \phi(a, b, c, d, \cdots)$$

ou bien

$$V - \phi(a, b, c, d, \cdots) = 0$$

Multiplions entre elles toutes les équations semblables, que l'on obtient en permutant dans celles-ci toutes les lettres, la première seulement restant fixe ; il viendra une expression suivante:

$$(V - \phi(a, b, c, d, \cdots))(V - \phi(a, c, b, d, \cdots))(V - \phi(a, b, d, f, c, \cdots)) \cdots$$

symétrique en $b, c, d, \cdots$ laquelle pourra par conséquent s'écrire en fonction de a. Nous aurons donc une équation de la forme

$$F(V, a) = 0$$

Or je dis que de là on peut tirer la valeur de a. Il suffit pour cela de chercher la solution commune à cette équation et à la proposée. Cette solution est la seule commune, car on ne peut avoir, par exemple,

$$F(V, b) = 0$$

cette équation ayant un facteur commun avec l'équation semblable, sans quoi l'une des fonctions $\phi(a, \cdots)$ serait égale à l'une des fonctions $\phi(b, \cdots)$; ce qui est contre l'hypothèse.

Il suit de là que a s'exprime en fonction rationnelle de V, et il en est de même des autres racines.

Cette proposition est citée sans démonstration par Abel, dans le Mémoire posthume sur les fonctions elliptiques.

Lemme IV. « Supposons que l'on ait formé i'équation en V, et que l'on ait pris l'un de ses facteurs irréductibles, en sorte que V soit racine d'une équation irréductible. Soient $V, V', V'', \cdots$ les racines de cette équation irréductible. Si $a = f(V)$ est une des racines de la proposée, $f(V')$ de même sera une racine de la proposée. »

En effet, en multipliant entre eux tous les facteurs de la forme $V_\phi(a, b, c, \cdots, d)$, où l'on aura opéré sur les lettres toutes les permutations possibles, on aura une équation rationnelle en V , laquelle se trouvera nécessairement divisible par l'équation en question; donc V' doit s'obtenir par l'échange des lettres dans la fonction V. Soit $F(V, a) = 0$ l'équation qu'on obtient en permutant dans V toutes les lettres, hors la première. On aura donc $F(V', b) = 0$, b pouvant être égal à a, mais étant certainement l'une des racines de l'équation proposée ; par conséquent, de même que de la proposée et de $F(V, a) = 0$ est résulté $a = F(V)$, de même il résultera de la proposée et de F $F(V', b) = 0$ combinées, la suivante $b = F(V')$.

PROPOSITION I. Théorème. «Soit une équation donnée, dont $a, b, c, \cdots$ sont les m racines. Il y aura toujours un groupe de permutations des lettres $a, b, c, \cdots$. Qui jouira de la propriété suivante:

1^o. Que toute fonction des racines, invariable par les substitutions de ce groupe, soit rationnellement connue;

2^o. Réciproquement, que toute fonction des racines, déterminable rationnellement, soit invariable par les substitutions.»

(Dans le cas des équations algébriques, ce groupe n'est autre chose que l'ensemble des $1, 2, 3, \cdots, m$ permutations possibles sur les m lettres, puisque, dans ce cas, les fonctions symétriques sont seules déterminables rationnellement.)

Dans le cas de l'équation $\frac{x^n-1}{x-1} = 0$, si l'on suppose $a = r, b = r^g, c = b = r^{g^2}, \cdots$ g étant une racine primitive, le groupe de permutations sera simplement celui-ci:

$$\begin{array}{l} abcd\ldots k \\ bcd\ldots ka \\ cd\ldots kab \\ \ldots\ldots\ldots \\ kabc\ldots i; \end{array}$$

dans ce cas particulier, le nombre des permutations est égal au degré de l'équation, et la même chose aurait lieu dans les équations dont toutes les racines seraient des fonctions rationnelles les unes des autres.)

Démonstration. Quelle que soit l'équation donnée, on pourra trouver une fonction rationnelle V des racines, telle que toutes les racines soient fonctions rationnelles de V. Cela posé, considérons l'équation irréductible dont V est racine (lemmes III et IV). Soient $V, V', V'', \ldots, V^{n-1}$ les racines de cette équation.

Soient $\phi V, \phi_1 V, \phi_2 V, \ldots, \phi_{m-1} V$ les racines de la proposée.

Écrivons les n permutations suivantes des racines

$$\begin{array}{c|ccccc} (V) & \phi V & \phi_1 V & \phi_2 V & \cdots & \phi_{m-1}(V) \\ (V') & \phi V' & \phi_1 V' & \phi_2 V' & \cdots & \phi_{m-1}(V') \\ (V'') & \phi V'' & \phi_1 V'' & \phi_2 V'' & \cdots & \phi_{m-1}(V'') \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ (V^{n-1}) & \phi V^{n-1} & \phi_1 V^{n-1} & \phi_2 V^{n-1} & \cdots & \phi_{m-1}(V^{n-1}) \end{array}$$

je dis que ce groupe de permutations jouit de la propriété énoncée.

En effet, 1^o toute fonction F des racines, invariable par les substitutions de ce groupe, pourra être écrite ainsi: $F = \psi V$, et l'on aura

$$\psi V = \psi V' = \psi V'' = \cdots = \psi V n - 1$$

La valeur de F pourra donc se déterminer rationnellement.

2^o. *Réciproquement.* Si une fonction F est déterminable rationnellement, et que l'on pose $F = \psi V$ on devra avoir

$$\psi V = \psi V' = \psi V'' = \cdots = \psi V n - 1$$

puisque l'équation en V n'a pas de diviseur commensurable et que V satisfait à l'équation $F = \psi V$, F étant une quantité rationnelle. Donc la fonction F sera nécessairement invariable par les substitutions du groupe écrit ci-dessus.

Ainsi, ce groupe jouit de la double propriété dont il s'agit dans le théorème proposé. Le théorème est donc démontré.

Nous appellerons groupe de l'équation le groupe en question.

Scolie 1. Il est évident que dans le groupe de permutations dont il s'agit ici, la disposition des lettres n'est point à considérer, mais seulement les substitutions de lettres par lesquelles on passe d'une permutation à l'autre.

Ainsi l'on peut se donner arbitrairement une première permutation, pourvu que les autres permutations s'en déduisent toujours par les mêmes substitutions de lettres. Le nouveau groupe ainsi formé jouira évidemment des mêmes propriétés que le premier,

puisque dans le théorème précédent, il ne s'agit que des substitutions que l'on peut faire dans les fonctions.

Scolie 2. Les substitutions sont indépendantes même du nombre des racines.

PROPOSITION II.

Théorème. «Si l'on adjoint à une équation donnée la racine r d'une équation auxiliaire irréductible, 1^o il arrivera de deux choses l'une : ou bien le groupe de l'équation ne sera pas changé, ou bien il se partagera en p groupes appartenant chacun à l'équation proposée respectivement quand on lui adjoint chacune des racines de l'équation auxiliaire; 2^o ces groupes jouiront de la propriété remarquable, que l'on passera de l'un à l'autre en opérant dans toutes les permutations du premier une même substitution de lettres.»

1^o. Si, après l'adjonction de r, l'équation en V, dont il est question plus haut, reste irréductible, il est clair que le groupe de l'équation ne sera pas changé. Si, au contraire, elle se réduit, alors l'équation en V se décomposera en p facteurs, tous de même degré et de la forme

$$f(V,r) \times f(V,r') \times f(V,r'') \times \dots$$

$r, r', r'', \dots$ étant d'autres valeurs de r. Ainsi le groupe de l'équation proposée se décomposera aussi en groupes chacun d'un même nombre de permutations, puisqu'à chaque valeur de V correspond une permutation. Ces groupes seront respectivement ceux de l'équation proposée, quand on lui adjoindra successivement $r, r', r'', \dots$

2^o. Nous avons vu plus haut que toutes les valeurs de V étaient des fonctions rationnelles les unes des autres. D'après cela, supposons que V étant une racine de $f(V,r) = 0$, $F(V)$ en soit une autre; il est clair que de même si V' est une racine de $f(V,r') = 0$, $F(V')$ en sera une autre; car l'on aura

$f[F(V),r]$ = une fonction divisible par $f(Y,r)$.

Donc (*lemme I*)

$f[F(V'),r']$ = une fonction divisible par $f(V',r')$.

Cela posé, je dis que l'on obtient le groupe relatif à r' en opérant partout dans le groupe relatif à r une même substitution de lettres.

En effet, si l'on a, par exemple,

$$\phi_\mu F(V) = \phi_\nu(V)$$

on aura encore (lemme I)

$$\phi_\mu F(V') = \phi_\nu(V')$$

Donc, pour passer de la permutation $[F(V)]$ à la permutation $[F(V')]$, il faut faire la même substitution que pour passer de la permutation (V) à la permutation (V')

Le théorème est donc démontré.

PROPOSITION III.

Théorème. «Si l'on adjoint a une équation toutes les racines d'une équation auxiliaire, les groupes dont il est question dans le théorème II jouiront de plus de cette propriété, que les substitutions sont les mêmes dans chaque groupe.»

PROPOSITION IV.

Théorème. «Si l'on adjoint à une équation la valeur *numérique* d'une certaine fonction de ses racines, le groupe de l'équation s'abaissera de manière à n'avoir plus d'autres permutations que celles par lesquelles cette fonction est invariable.»

En effet, D'après la proposition I, toute fonction connue doit être invariable paries permutations du groupe de l'équation.

PROPOSITION V.

Problème. «Dans quels cas une équation est-elle soluble par de simples radicaux?»

J'observerai d'abord que, pour résoudre une équation, il faut successivement abaisser son groupe jusqu'à ne contenir plus qu'une seule permutation. Car, quand une équation est résolue, une fonction quelconque de ses racines est connue, même quand elle n'est invariable par aucune permutation.

Cela pose, cherchons à quelle condition doit satisfaire le groupe d'une équation, pour qu'il puisse s' abaisser ainsi par l'adjonction de quantités radicales.

Suivons la marche des opérations possibles dans cette solution, en considérant comme opérations distinctes l'extraction de chaque racine de degré premier.

Adjoignons à l'équation le premier radical extrait dans la solution. Il pourra arriver deux cas : ou bien, par l'adjonction de ce radical, le groupe des permutations de l'équation sera diminué; ou bien, cette extraction de racine n'étant qu'une simple préparation, le groupe restera le même.

Toujours sera-t-il qu'après un certain nombre *fini* d'extractions de racines, le groupe devra se trouver diminué, sans quoi l'équation ne serait pas soluble.

Si, arrivé à ce point, il y avait plusieurs manières de diminuer le groupe de l'équation proposée par une simple extraction de racine, il faudrait, pour ce que nous allons dire, considérer seulement un radical du degré le moins haut possible parmi tous les simples radicaux, qui sont tels que la connaissance de chacun d'eux diminue le groupe de l'équation.

Soit donc p le nombre premier qui représente ce degré minimum, en sorte que par une extraction de racine de degré p, on diminue le groupe de l'équation.

Nous pouvons toujours supposer, du moins pour ce qui est relatif au groupe de l'équation, que parmi les quantités adjointes précédemment à l'équation se trouve une racine $p^{ième}$ de l'unité, α. Car, comme cette expression s'obtient par des extractions de racines de degré inférieur à p, sa connaissance n'altérera en rien le groupe de l'équation.

Par conséquent, d'après les théorèmes II et III, le groupe de l'équation devra se décomposer en p groupes jouissant les uns par rapport aux autres de cette double propriété : 1^o Que l'on passe de l'un à l'autre par une seule et même substitution ; 2^o que tous contiennent les mêmes substitutions.

Je dis réciproquement, que si le groupe de l'équation peut se partager en p groupes qui jouissent de cette double propriété, on pourra, par une simple extraction de racine $p^{ième}$, et par l'adjonction de cette racine $p^{ième}$, réduire le groupe de l'équation à l'un de ces groupes partiels.

Prenons, en effet, une fonction des racines qui soit invariable pour toutes les substitutions de l'un des groupes partiels, et varie pour toute autre substitution. (Il suffit, pour

cela, de choisir une fonction symétrique des diverses valeurs que prend, par toutes les permutations de l'un des groupes partiels, une fonction qui n'est invariable pour aucune substitution). Soit θ cette fonction des racines.

Opérons sur la fonction θ une des substitutions du groupe total qui ne lui sont pas communes avec les groupes partiels. Soit θ_1 le résultat. Opérons sur la fonction θ_1 t la même substitution, et soit θ_2 le résultat, et ainsi de suite. Comme p est un nombre premier, cette suite ne pourra s'arrêter qu'au terme θ_{p-1}, ensuite l'on aura $\theta_p = \theta_1, \theta_{p+1} = \theta_1$, et ainsi de suite.

Cela posé, il est clair que la fonction

$$(\theta + \alpha\theta_1 + \alpha^2\theta_2 + \cdots + \alpha^{p-1}\theta_{p-1})^p$$

sera invariable par toutes les permutations du groupe total, et, par conséquent, sera actuellement connue.

Si l'on extrait la racine $p^{ième}$ de cette fonction, et qu'on l'adjoigne a l'équation, alors, par la proposition IV, le groupe de l'équation ne contiendra plus d' autres substitutions que celles des groupes partiels.

Ainsi, pour que le groupe d'une équation puisse s'abaisser par une simple extraction de racine, la condition ci-dessus est nécessaire et suffisante.

Adjoignons à l'équation le radical, en question; nous pourrons raisonner maintenant sur le nouveau groupe comme sur le précédent, et il faudra qu'il se décompose lui-même de la manière indiquée, et ainsi de suite, jusqu'à un certain groupe qui ne contiendra plus qu'une seule permutation.

Scolie. Il est aisé d'observer cette marche dans la résolution connue des équations générales du quatrième degré. En effet, ces équations se résolvent au moyen d'une équation du troisième degré, qui exige elle-même l'extraction d'une racine carrée. Dans la suite naturelle des idées, c'est donc par cette racine carrée qu'il faut commencer. Or, en adjoignant à l'équation du quatrième degré cette racine carrée, le groupe de l'équation, qui contenait en tout vingt-quatre substitutions, se décompose en deux qui n'en contiennent que douze. En désignant par a, b, c, d les racines, voici l'un de ces groupes:

$$\begin{array}{lll} abcd, & acdb, & adbc, \\ badc, & cabd, & dacb, \\ cdab, & dbac, & bcad, \\ dcba, & bdca, & cbda. \end{array}$$

Maintenant ce groupe se partage lui-même en trois groupes, comme il est indiqué aux théorèmes II et III. Ainsi, par l'extraction d'un seul radical du troisième degré, il reste simplement le groupe

$$\begin{array}{l} abcd, \\ badc, \\ cdab, \\ dcba. \end{array}$$

ce groupe se partage de nouveau en deux groupes:

$$\begin{array}{l} abcd, cdab, \\ badc, dcba. \end{array}$$

Ainsi, après une simple extraction de racine carrée, il restera

$$abcd,$$
$$badc.$$

ce qui se résoudra enfin par une simple extraction de racine carrée.

On obtient ainsi, soit la solution de Descartes, soit celle d'Euler; car, bien qu'après la résolution de l'équation auxiliaire du troisième degré, ce dernier extraye trois racines carrées, on sait qu'il suffit de deux, puisque la troisième s'en déduit rationnellement.

Nous allons maintenant appliquer cette condition aux équations irréductibles dont le degré est premier.

Application aux équations irréductibles de degré premier.

PROPOSITION VI.

Lemme. «Une équation irréductible de degré premier ne peut de venir réductible par l'adjonction d'un radical dont l'indice serait autre que le degré même de l'équation. »

Car si $r, r', r'', \ldots$ sont les diverses valeurs du radical, et $Fx = 0$ l'équation proposée, il faudrait que Fx se partageât en facteurs

$$f(x,r) \times f(x,r') \times f(x,r'') \times \ldots$$

tous de même degré, ce qui ne se peut, a moins que $f(x,r)$ ne soit du premier degré en x.

Ainsi une équation irréductible de degré premier ne peut devenir réductible, a moins que son groupe ne se réduise a une seule permutation.

PROPOSITION VII.

Problème. «Quel est le groupe d'une équation irréductible d'un degré premier n, soluble par radicaux?»

D'après la proposition précédente, le plus petit groupe possible avant celui qui n'a qu'une seule permutation, contiendra n permutations. Or un groupe de permutations d'un nombre premier n de lettres ne peut se réduire k n permutations, à moins que l'une de ces permutations ne se déduise de l'autre par une substitution circulaire de l'ordre n. (Voir le Mémoire de M. Cauchy, Journal de l'École Polytechnique, $xvii^e$ cahier.) Ainsi l'avant-dernier groupe sera

$$\begin{array}{cccccccc}
x_0, & x_1, & x_2, & x_3, & \cdots & \cdots & \cdots & x_{n-1}; \\
x_1, & x_2, & x_3, & x_4, & \cdots & \cdots & x_{n-1}, & x_0; \\
x_2, & x_3, & \cdots & \cdots & \cdots & x_{n-1}, & x_0, & x_1; \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
x_{n-1}, & x_0, & x_1, & \cdots & \cdots & \cdots & \cdots & x_{n-2};
\end{array}$$

$x_0, x_1, x_2, \ldots, x_{n-1}$ étant les racines. Maintenant, le groupe qui précédera immédiatement celui-ci dans l'ordre des décompositions devra se composer d'un certain nombre de groupes ayant tous les mêmes substitutions que celui-ci. Or j'observe que ces substitutions peuvent s' exprimer ainsi: (Faisons en général $x_n = x_0, xn - 1 = x_1, \ldots$ il est clair

que chacune des substitutions du groupe (G) s'obtient en mettant partout à la place de x_k, x_{k+c}, c étant une constante.)

Considérons l'un quelconque des groupes semblables au groupe (G). D'après le théorème II, il devra s'obtenir en opérant partout dans ce groupe une même substitution ; par exemple, en mettant partout dans le groupe (G), a la place de $x_k, x_{f(k)}$, f étant une certaine fonction.

Les substitutions de ces nouveaux groupes devant être les mêmes que celles du groupe (G), on devra avoir

$$f(k+c) = f(k) + C$$

C étant indépendant de K. Donc

$$\begin{gathered} f(k+2c) = f(k) + 2C \\ \cdots\cdots\cdots\cdots\cdots \\ f(k+mc) = f(k) + mC \end{gathered}$$

Si $c = 1$, $k = 0$, on trouvera

$$f(m) = am + b$$

ou bien

$$f(k) = ak + b$$

a et b étant des constantes.

Donc le groupe qui précède immédiatement le groupe (G) ne devra contenir que des substitutions telles que

$$x_k, x_{ak+b}$$

et ne contiendra pas, par conséquent, d'autre substitution circulaire que celle du groupe (G).

On raisonnera sur ce groupe comme sur le précédent, et il s'ensuivra que le premier groupe dans i'ordre des décompositions, c'est-à-dire le groupe *actuel* de l'équation, ne peut contenir que des substitutions de la forme

$$x_k, x_{ak+b}$$

Donc, « si une équation irréductible de degré premier est soluble par radicaux, le groupe de cette équation ne saurait contenir que des substitutions de la forme

$$x_k, x_{ak+b}$$

a et b étant des constantes.»

Réciproquement, si cette condition a lieu, je dis que l'équation sera soluble par radicaux. Considérons, en effet, les fonctions

$$\begin{gathered} (x_0 + \alpha x_1 + \alpha^2 x_2 + \cdots + \alpha^{n-1} x_{n-1})^n = X_1 \\ (x_0 + \alpha x_a + \alpha^2 x_2 a + \cdots + \alpha n - 1 x_{(n-1)a})^n = X_a \\ (x_0 + \alpha x_a^2 + \alpha^2 x_2 a^2 + \cdots + \alpha n - 1 x_{(n-1)a^2})^n = X_{a^2} \\ \cdots\cdots\cdots \end{gathered}$$

α étant une racine $n^{ième}$ de l'unité, a une racine primitive de n.

Il est clair que toute fonction invariable par les substitutions circulaires des quantités X, X_a, X_{a^2} sera, dans ce cas, immédiatement connue. Donc on pourra trouver $X, X_a, X_{a^2}, \ldots$, par la méthode de M. Gauss pour les équations binômes. Donc, etc.

Ainsi, pour qu'une équation irréductible de degré premier soit soluble par radicaux, il *faut* et il *suffit* que toute fonction invariable par les substitutions

$$x_k, x_{ak+b}$$

soit rationnellement connue. Ainsi la fonction

$$(X_1 - X)(X_a - X)(X_{a^2} - X)\ldots$$

devra, quel que soit X, être connue.

Il *faut* donc et il *suffit* que l'équation qui donne cette fonction des racines admette, quel que soit X, une valeur rationnelle.

Si l'équation proposée a tous ses coefficients rationnels ; l'équation auxiliaire qui donne cette fonction les aura tous aussi, et il suffira de reconnaître si cette équation auxiliaire du degré $1, 2, 3, \ldots (n-2)$ a ou non une racine rationnelle, ce que l'on sait faire.

C'est là le moyen qu'il faudrait employer dans la pratique. Mais nous allons présenter le théorème sous une autre forme.

PROPOSITION VIII. Théorème. « Pour qu'une équation irréductible de degré premier soit soluble par radicaux, *faut* et il *suffit* que deux quelconques des racines étant connues, les autres s'en déduisent rationnellement. »

Premièrement, il le faut, car la substitution

$$x_k, x_{ak+b}$$

ne laissant jamais deux lettres à la même place, il est clair qu'en adjoignant deux racines à l'équation, par la proposition IV, son groupe devra se réduire ù une seule permutation.

Eu second lieu, cela suffit; car, dans ce cas, aucune substitution du groupe ne laissera deux lettres aux mêmes places. Par conséquent, le groupe contiendra tout au plus $n(n-1)$ permutations. Donc il ne contiendra qu'une seule substitution circulaire (sans quoi il y aurait au moins n^2 permutations). Donc toute substitution du groupe, x_k, x_{fk} devra satisfaire à la condition

$$f(x + c) = fx + C$$

Donc, etc. Le théorème est donc démontré.

Exemple du théorème VII.

Soit $n = 5$; le groupe sera le suivant:

abcde
bcdea
cdeab
deabc
eabcd

acebd
cebda
ebdac
bdace
daceb

aedcb
edcba
dcbae
cbaed
baedc

adbec
dbeca
becad
ecadb
cadbe

Bibliography

[Ed] Edwards, H.M.: *Galois Theory,* GTM 101, Springer-Verlag, Second Edition 1993.

[Ga] Gauss, C.F.: *Disquisitiones Arithmeticae,* Springer-Verlag New York Berlin Heidelberg Tokyo, 1966.

[Pr] Procesi, C.: *Elementi di Teoria di Galois,* Decibel editrice, Second Edition 1991.

[St] Stillwell, J.: *Mathematics and Its History,* Springer, 1989.

[Pa] William Paulsen: *Computing Galois Groups in Mathematica* http://www2.cms.hu-berlin.de/newlogic/webMathematica/Logic/GalComp.pdf http://library.wolfram.com/infocenter/Articles/2872/, 1999.

[La] Langlands, R.P.: *Representation Theory Its Rise and Its Role in Number Theory* https://pdfs.semanticscholar.org/36bd/1d06de00cbe08592e21c466bf166963f5dde.pdf

[Li] Liouville, J.: *Les Oeuvres Mathématiques d'Évariste Galois,* Journal de Liouville, 1846.