About solvable groups and some applications

Hanecart Valentin, Abergel Antoine

2023

Table of contents

Introduction

Have you ever wondered why general polynomial equations of degree greater or equal than 5 can not be solved by radicals ? Or even, if it is possible to cut a pie for 7 guests using only the same methods as the ancient Greek geometricians ? Well, all these questions are related to the same mathematical notion that we are going to explore in this paper : solvable groups.

Finding a general expression to solve general polynomial equations has been the work of many mathematicians over time. For example, Lagrange found an expression to solve general quartic equation by radicals. Later, Abel proved that the general quintic equation can not be solved by radicals. Evariste Galois worked on this problem and his search led him to introduce the concept of groups, and more specifically of solvable groups. The first appearance of solvable groups was in a theorem about solvable extensions (that is to say a field extension whose Galois group is a solvable group). Here is an extract from his statement : "I first observe that to solve an equation, it is necessary to reduce its group until it contains only a single permutation... Given this, we will try to find the condition satisfied by the group of an equation for which it is possible to reduce the group by adjunction of radical quantities". His work on group theory led to other applications, like in geometric construction for example.

The objective of this paper will be to answer the following question :

What is a solvable group and how useful is it in mathematics ?

To answer this question, we will first of all introduce in a first chapter the concept of solvable group, give first properties and some complements to go further. After that, we will study the links between solvable groups and some other types of groups (and in particular simple groups) in a second chapter. Then in a third chapter, we will see an application of solvable groups in geometry with the construction of regular polygons using only the non-graduated ruler and the compass. Finally, in a last chapter, we will give an important application to Galois theory and solution of general polynomial equations.

For this paper, we assume that the reader is familiar with the basics of group theory, as well as Galois theory and finally the theory of representations and characters.

Finally, in all this paper, we will use the misuse of language which consists in designating an algebraic structure (more precisely a group and a field) only by their set and not by their set and the associated laws of composition.

Chapter 1

Concept of solvable group

This first chapter aims to introduce the concept of solvable groups, give first properties and some complements about these groups.

The first section of this chapter aims to define solvable groups and study some basic properties. These groups play an important role in the theory of resolution of general polynomial equation by radicals (as we will see later in chapter 4). The second section of this chapter aims to state and prove a first Burnside's theorem. Finally, we will give some complements about solvable groups.

For the whole chapter we consider a group $(G, *)$ (denoted G) and the identity element is denoted e_G for the law of internal composition "$*$".

I Solvable groups

Solvable groups were first defined and studied by Galois in his work on the resolution of equations by radicals. They have since proved to be extremely important in many branches of mathematics (particularly in group theory !).

I.1 Definitions and first examples

We begin by defining solvable groups and give first examples and properties.

Definition 1 : Solvable group :

We say that G is a **solvable group** (or **soluble group**), when there is a finite series of subgroups :

$$\{e_G\} := G_0 \subseteq G_1 \subseteq \cdots \subseteq G_n := G \quad (\star)$$

such that :

- For all i in $[\![0; n-1]\!]$, G_i is a normal subgroup of G_{i+1}. $(*)$

- For all i in $[\![0; n-1]\!]$, G_{i+1}/G_i is an abelian group.

Remark :
Note that condition $(*)$ does not imply that $G_i \lhd G$, since $G_i \lhd G_{i+1} \lhd G_{i+2}$ does not imply $G_i \lhd G_{i+2}$.
Moreover, the finite series $(\star)$ is called a **subnormal series** (or **normal series**).

Example 1 :

- Every abelian group G is solvable.
  Indeed, let us consider the finite series : $\{e_G\} \subseteq G$.
  Then :
  - $\{e_G\}$ is (always) a normal subgroup of group G.
  - $G/\{e_G\} \cong G$, so it is an abelian group (by hypothesis).

- Every cyclic group is solvable because it is abelian.

- The symmetric group $\mathfrak{S}_3$ of degree 3 is solvable, since it has a normal subgroup of order 3 generated by the 3-cycle (1 2 3) and whose quotient has order 2, so it is an abelian group.
  Indeed :
  $$\left\{\mathrm{Id}_{[\![1;3]\!]}\right\} \lhd \mathfrak{A}_3 \lhd \mathfrak{S}_3$$
  The quotient groups are :
  $$\mathfrak{A}_3/\left\{\mathrm{Id}_{[\![1;3]\!]}\right\} \cong \mathbb{Z}/3\mathbb{Z} \ \ \text{(abelian of order 3)}$$
  $$\mathfrak{S}_3/\mathfrak{A}_3 \cong \mathbb{Z}/2\mathbb{Z} \ \ \text{(abelian of order 2)}$$

- The dihedral group D_4 of order 8 is solvable.
  Indeed, it has a cyclic normal subgroup S of order 4 and whose quotient has order 2, so it is an abelian group.

- The symmetric group $\mathfrak{S}_4$ of degree 4 is solvable, having the series :
  $$\left\{\mathrm{Id}_{[\![1;4]\!]}\right\} \lhd V_4 \lhd \mathfrak{A}_4 \lhd \mathfrak{S}_4$$
  where $\mathfrak{A}_4$ is the alternating group of order 12, and V_4 consists of the permutations $\mathrm{Id}_{[\![1;4]\!]}$, (1 2)(3 4), (1 3)(2 4), (1 4)(2 3) and is a direct product of two groups of order 2 (and named **Klein four-group**).
  The quotient groups are :
  $$V_4/\{\mathrm{Id}_{[\![1;4]\!]}\} \cong V_4 \ \ \text{(abelian of order 4)}$$
  $$\mathfrak{A}_4/V_4 \cong \mathbb{Z}/3\mathbb{Z} \ \ \text{(abelian of order 3)}$$
  $$\mathfrak{S}_4/\mathfrak{A}_4 \cong \mathbb{Z}/2\mathbb{Z} \ \ \text{(abelian of order 2)}$$

- The symmetric group $\mathfrak{S}_5$ of degree 5 and $\mathfrak{A}_5$ are not solvable groups (we will show this result in the theorem 5 and corollary 6 in the next chapter).

- The quaternion group is a solvable group.
  Indeed, we have :
  $$\mathbb{H}_8 := \{1, -1, i, -i, j, -j, k, -k\} \text{ and } i^2 = j^2 = k^2 = i \times j \times k = -1$$
  So, $< k >:= \{1, k, -1, -k\}$ is a normal subgroup of $\mathbb{H}_8$ (because its index is 2) and $\mathbb{H}_8/ < k >$ is a group of order 2 (then abelian).

  Moreover, $< k >$ is an abelian subgroup and then, $< k > /\{1_{\mathbb{H}_8}\} \cong < k >$ is an abelian group.

Remark :
The examples of $\mathfrak{S}_5$ and $\mathfrak{A}_5$ are very important because they are central in resolution of polynomial equations by radicals theory.

Definition 2 : Solvability series of a group :

When the group G is solvable, we call **solvability series of** G, a finite series as in $(\star)$ defined in the previous definition.

Remark :
Moreover, if for all i in $[\![0; n-1]\!]$, $G_i \neq G_{i+1}$, then the solvability series of G is also called **resolubility series without repetitions**.

Definition 3 : Solvable number :

We call **solvable number**, a natural number n in $\mathbb{N}^*$ such that every group of order n is solvable.

I.2 First properties

We recall the following isomorphism theorems :

Theorem 1 : Second isomorphism theorem :

Let N and H be two subgroups of G.
If N is a normal subgroup of G, then $H \cap N$ is a normal subgroup of H and we have :

$$H/(H \cap N) \cong (HN)/N$$

Theorem 2 : Third isomorphism theorem :

Let N and M be two normal subgroups of G.
If $M \subseteq N$, then N/M is a normal subgroup of G/M and we have the following isomorphism :

$$(G/M)/(N/M) \cong G/N$$

A judicious use of these isomorphism theorems allows us to prove that solvable groups persist in being solvable even when subjected to quite drastic treatment :

Proposition 1 :

Let H be a subgroup of G.
If G is solvable, then H is solvable.

Proof :

Let us consider H a subgroup of G.
Let us assume that G is solvable.
Then, there exists a finite series of subgroups :

$$\{e_G\} := G_0 \subseteq G_1 \subseteq \cdots \subseteq G_n := G$$

such that :

- For all i in $[\![0; n-1]\!]$, G_i is a normal subgroup of G_{i+1}.
- For all i in $[\![0; n-1]\!]$, G_{i+1}/G_i is an abelian group.

For all i in $[\![0; n]\!]$, let $H_i := G_i \cap H$.

Then H has a finite series :

$$\{e_G\} := H_0 \lhd H_1 \lhd \cdots \lhd H_n := H$$

Indeed, for all i in $[\![0; n-1]\!]$, we have :

$$\forall g \in G_{i+1},\ gG_i = G_i g$$

So, in particular for all g in H_{i+1}, $gH_i = H_i g$.
Thus for all g in H_{i+1}, we have $gH_i = H_i g$, that is to say that H_i is a normal subgroup of H_{i+1}.

Let us show that the factors are abelian :
According to the second isomorphism theorem, we have :

$$\forall i \in [\![0; n-1]\!],\ \frac{H_{i+1}}{H_i} := \frac{G_{i+1} \cap H}{G_i \cap H} = \frac{G_{i+1} \cap H}{G_i \cap (G_{i+1} \cap H)} \cong \frac{G_i(G_{i+1} \cap H)}{G_i}$$

But this latter group is a subgroup of G_{i+1}/G_i which is abelian. Hence, H_{i+1}/H_i is an abelian group.

Finally, according to definition 1, H is a solvable group.

■

Proposition 2 :

Let N be a normal subgroup of G.
If G is solvable, then G/N is solvable.

Proof :

Let us consider N a normal subgroup of G.
Let us assume that G is solvable.
Then, there exists a finite series of subgroups :

$$\{e_G\} := G_0 \subseteq G_1 \subseteq \cdots \subseteq G_n := G$$

such that :

- For all i in $[\![0; n-1]\!]$, G_i is a normal subgroup of G_{i+1}.
- For all i in $[\![0; n-1]\!]$, G_{i+1}/G_i is an abelian group.

Then, G/N has a finite series :

$$N/N := (G_0N)/N \lhd (G_1N)/N \lhd \cdots \lhd (G_nN)/N := G/N$$

Indeed, for all i in $[\![0; n-1]\!]$, G_iN is a normal subgroup of $G_{i+1}N$ (because N is a normal subgroup of G (thus in each G_i) and G_i is also a normal subgroup of G_{i+1}) and finally, according to the correspondence theorem, $(G_iN)/N$ is a normal subgroup of $(G_{i+1}N)/N$.

Moreover, typical quotient is $(G_{i+1}N/N)/(G_iN/N)$, which by the third isomorphism theorem is isomorphic to $(G_{i+1}N)/(G_iN)$.

Moreover, by the second and third isomorphism theorem :

$$\forall i \in [\![0; n-1]\!],\ \frac{G_{i+1}N}{G_iN} = \frac{G_{i+1}(G_iN)}{G_iN} \cong \frac{G_{i+1}}{G_{i+1} \cap (G_iN)} \cong \frac{G_{i+1}/G_i}{(G_{i+1} \cap (G_iN))/G_i}$$

which is a quotient of the abelian group G_{i+1}/G_i, so is abelian.

Therefore, according to definition 1, G/N is a solvable group.

■

Remark :
By the first isomorphism theorem, the last proposition is equivalent to :
If there exists a group homomorphism from a solvable group P onto G, then G is solvable.

Proposition 3 :

Let N be a normal subgroup of G.
If N and G/N are solvable, then G is solvable.

Proof :

Let us consider N a normal subgroup of G.
Let us assume that N and G/N are solvable.
Then, there exists two finite series of subgroups :

$$\{e_G\} := N_0 \lhd N_1 \lhd \cdots \lhd N_r := N$$

$$N/N := G_0/N \lhd G_1/N \lhd \cdots \lhd G_s/N := G/N$$

with abelian quotients and for all i in $[\![0;s]\!]$, G_i is a subgroup of G containing N such that (and N is a normal subgroup of G_i).

According to the correspondence theorem about the subgroup of a quotient, we can consider the series of G given by :

$$\{e_G\} := N_0 \lhd N_1 \lhd \cdots \lhd N_r := N := G_0 \lhd G_1 \lhd \cdots \lhd G_s := G$$

The quotients are either N_{i+1}/N_i (which is abelian) or G_{i+1}/G_i, which is isomorphic to $(G_{i+1}/N)/(G_i/N)$, and thus abelian.

Therefore, according to definition 1, G is solvable.

■

Remark :
We can notice that the three previous propositions give us the following equivalence :

$$(N \text{ and } G/N \text{ are solvable}) \iff (G \text{ is solvable})$$

So, in particular, if G and N are solvable, the direct product $G \times N$ is solvable. And also, if we have an action φ and N and H are solvable, then the semidirect product $N \rtimes_\varphi H$ is solvable.

Corollary 1 :

If G is not simple and any group of order smaller than $\mathrm{Card}(G)$ is solvable, then G is solvable.

Proof :

Let us assume that G is not simple and any group of order smaller than $\mathrm{Card}(G)$ is solvable.
In particular, G has a strict normal subgroup H then, by hypothesis, H and G/H are solvable.

Then, according to proposition 3, G is solvable.

■

Remark :
Let us say that G is an **extension of a group** A **by a group** B, when G has a normal subgroup N isomorphic to A such that G/N is isomorphic to B. In others terms, a group extension is a way of describing a group in terms of two "smaller" groups. Specifically, an extension of a group A by a group B is a group G that fits into a short exact sequence :

$$\{e\} \longrightarrow B \longrightarrow G \longrightarrow A \longrightarrow \{e\}$$

So a solvable group is a group that can be constructed from abelian groups by a finite sequence of extensions. Then we may sum up the three last properties by saying that the class of solvable groups is closed under taking subgroups, quotients and extensions. In the same way, the class of abelian groups is closed under subgroups and quotients, but not extensions. It is largely for this reason that we are led to define solvable groups.

II Burnside's theorem

This second section aims to prove Burnside's theorem on solvable groups (theorem 3). Burnside's theorem states that a finite group whose order has no more than two distinct prime divisors is solvable.

We will assume here that all p-groups are solvable (see proposition 18 of section IV of chapter 2).

II.1 Preliminaries

In this first subsection, we will give some results about representation theory which will be used in the proof of Burnside's theorem.

In this whole subsection, we will assume that G is a finite group of order d, and we denote $\mathrm{Irr}(G)$ the set of character of irreducible representations of G on finite dimensional $\mathbb{C}$-vector space (and we just consider such representations) and finally $\mathbb{L} := \mathbb{Q}\left(e^{\frac{2i\pi}{d}}\right)$.

We recall that for all (g, g') in G^2, we have :

$$\sum_{\chi \in \mathrm{Irr}(G)} \overline{\chi(g)}\chi(g') = \frac{d}{\mathrm{Card}(\Omega_g)}\delta_{\Omega_g,\Omega_{g'}} \quad \text{(orthogonality relations)}$$

In particular, if $g' = e_G$ and $\Omega_g \neq \{e_G\}$, we have :

$$\sum_{\chi \in \mathrm{Irr}(G)} \deg(\chi)\chi(g) = 0$$

Proposition 4 :

If (V, ρ) is a complex representation of G of character χ, then for all g in G, $\chi(g)$ is in $\mathcal{O}_{\mathbb{L}}$.

Proof :

Let us assume that (V, ρ) is a complex representation of G of character χ.
Let g in G.
We have : $\rho(g)^d = \rho\left(g^d\right) = \rho(e_G) = \mathrm{Id}_V$.
Hence, the minimal polynomial of $\rho(g)$ divides $X^d - 1$. So, the minimal polynomial of $\rho(g)$ is split with simple zeros and thus, $\rho(g)$ is diagonalizable and its eigenvalues are d^{th} roots of unity of the form $e^{\frac{2ik\pi}{d}}$, with k in $[\![0; d-1]\!]$.

But, we know that for all k in $[\![0; d-1]\!]$, $e^{\frac{2ik\pi}{d}}$ is in the ring $\mathcal{O}_{\mathbb{L}}$ as roots of $X^d - 1$ (unitary and in $\mathbb{Z}[X]$), and since $\chi(g)$ is the sum of the eigenvalues of $\rho(g)$, we can deduce that $\chi(g)$ is in $\mathcal{O}_{\mathbb{L}}$.

■

Proposition 5 :

Let (V, ρ) be a complex irreducible representation of G of character χ.
If Ω_g is the conjugacy class of an element g in G, then we have :

$$\frac{\mathrm{Card}(\Omega_g)\chi(g)}{\deg(\chi)}\mathrm{Id}_V = \sum_{s \in \Omega_g} \rho(s)$$

Proof :

Let us consider (V,ρ) a complex irreducible representation of G of character χ.
Let us assume that Ω_g is the conjugacy class of an element g in G.
We denote $f := \sum\limits_{s\in\Omega_g} \rho(s)$.
Then, f is an endomorphism of V and for all h in G, we have :

$$\begin{aligned} f\circ\rho(h) &:= \left(\sum_{s\in\Omega_g}\rho(s)\right)\circ\rho(h) \\ &= \sum_{s\in\Omega_g}(\rho(s)\circ\rho(h)) \\ &= \sum_{s\in\Omega_g}\rho(sh) \\ &= \sum_{s\in\Omega_g}\rho(h)\circ\rho\left(h^{-1}sh\right) \\ &= \rho(h)\circ\left(\sum_{s\in\Omega_g}\rho\left(h^{-1}sh\right)\right) \end{aligned}$$

Moreover, the application :

$$\varphi : \left|\begin{array}{ccc} \Omega_g & \longrightarrow & \Omega_g \\ s & \longmapsto & h^{-1}sh \end{array}\right.$$

is well defined, bijective and of inverse the application :

$$\varphi^{-1} : \left|\begin{array}{ccc} \Omega_g & \longrightarrow & \Omega_g \\ r & \longmapsto & hrh^{-1} \end{array}\right.$$

Hence, we have :

$$f\circ\rho(h) = \rho(h)\circ\left(\sum_{s\in\Omega_g}\rho\left(h^{-1}sh\right)\right) = \rho(h)\circ\left(\sum_{r\in\Omega_g}\rho(r)\right) := \rho(h)\circ f$$

So, f is a representation homomorphism. As ρ is irreducible, Schur's lemma states that there exists λ in $\mathbb{C}$ such that $f = \lambda\mathrm{Id}_V$.

Hence :

$$\mathrm{Tr}(f) = \deg(\chi)\lambda \text{ and } \mathrm{Tr}(f) := \sum_{s\in\Omega_g}\chi(s) = \mathrm{Card}(\Omega_g)\chi(g)$$

So, $\lambda = \dfrac{\mathrm{Card}(\Omega_g)\chi(g)}{\deg(\chi)}$ and we finally have :

$$\frac{\mathrm{Card}(\Omega_g)\chi(g)}{\deg(\chi)}\mathrm{Id}_V = \sum_{s\in\Omega_g}\rho(s)$$

■

Proposition 6 :

Let (V, ρ) be a complex irreducible representation of G of character χ.
If Ω_g is the conjugacy class of an element g in G, then we have :

$$\frac{\mathrm{Card}(\Omega_g)\chi(g)}{\deg(\chi)} \in \mathcal{O}_{\mathbb{L}}$$

Proof :

Let us consider (V, ρ) a complex irreducible representation of G of character χ.
Let us assume that Ω_g is the conjugacy class of an element g in G.
Let $u_g := \dfrac{\mathrm{Card}(\Omega_g)\chi(g)}{\deg(\chi)}$.
According to proposition 4, we already know that u_g is an element of $\mathbb{L}$. To show that u_g is an element of $\mathcal{O}_{\mathbb{L}}$, we will create a finitely generated $\mathbb{Z}$-module $M \subseteq \mathbb{L}$ such that $u_g M \subseteq M$.
This module is the set of finite sums $\displaystyle\sum_{s\in G} m_s u_s$, where m_s belongs to $\mathbb{Z}$. By linearity, we just have to show that, for all h in G, $u_g u_h$ is an element of M :

According to proposition 5 :

$$u_g u_h \mathrm{Id}_V = (u_g \mathrm{Id}_V) \circ (u_h \mathrm{Id}_V) := \left(\sum_{s\in\Omega_g} \rho(s)\right) \circ \left(\sum_{s'\in\Omega_h} \rho(s')\right) = \sum_{(s,s')\in\Omega_g\times\Omega_h} \rho(ss')$$

We now have to understand the set $\Omega_g\Omega_h$ formed with the products ss' where (s, s') is in $\Omega_g \times \Omega_h$:
The set $\Omega_g\Omega_h$ is an union of conjugacy classes. Indeed, if $\Omega_\alpha \cap \Omega_g\Omega_h \neq \emptyset$, then $\Omega_\alpha \subseteq \Omega_g\Omega_h$ (because if $\alpha := ss'$, then for all γ in G, $\gamma\alpha\gamma^{-1} := (\gamma s\gamma^{-1})(\gamma s'\gamma^{-1})$ with $\gamma s\gamma^{1}$ in Ω_g and $\gamma s'\gamma^{-1}$ in Ω_h).

So, there exists $\alpha_1, ..., \alpha_n$ in G such that :

$$\Omega_g\Omega_h = \bigsqcup_{i=1}^{n} \Omega_{\alpha_i}$$

Moreover, if x and y are in Ω_{α_i}, then there exists a bijection between the sets $A_x := \{(s, s') \in \Omega_g \times \Omega_h \text{ st } ss' = x\}$ and $A_y := \{(s, s') \in \Omega_g \times \Omega_h \text{ st } ss' = y\}$. Indeed, if $y := uxu^{-1}$, then the bijection is $(s, s') \longmapsto (usu^{-1}, us'u^{-1})$.

For all i in $[\![1; n]\!]$, let m_{α_i} be the common cardinal of all A_x for x in Ω_{α_i}.
We have :

$$\mathrm{Card}((s, s') \in \Omega_g \times \Omega_h \text{ st } ss' \in \Omega_{\alpha_i}) = m_{\alpha_i}\mathrm{Card}(\Omega_{\alpha_i})$$

Hence :

$$u_g u_h \mathrm{Id}_V = \sum_{(s,s')\in\Omega_g\times\Omega_h} \rho(ss') = \sum_{i=1}^{n} m_{\alpha_i}\left(\sum_{x\in\Omega_{\alpha_i}} \rho(x)\right) = \sum_{i=1}^{n} m_{\alpha_i} u_{\alpha_i} \mathrm{Id}_V$$

So, we can conclude that :

$$u_g u_h = \sum_{i=1}^{n} m_{\alpha_i} u_{\alpha_i} \in M$$

Finally, we have $u_g M \subseteq M$, and thus, $u_g := \dfrac{\mathrm{Card}(\Omega_g)\chi(g)}{\deg(\chi)}$ is in $\mathcal{O}_{\mathbb{L}}$.

■

Corollary 2 :

Let (V,ρ) be a complex irreducible representation of G of character χ and Ω_g the conjugacy class of g in G. If $\mathrm{Card}(\Omega_g)$ and $\deg(\chi)$ are coprime integers, then $\chi(g)=0$ or $\rho(g)$ is an homothety.

In particular, if moreover $\chi(g)\neq 0$, then $\rho(g)$ is in $Z(\rho(G))$.

Proof :

Let us consider (V,ρ) a complex irreducible representation of G of character χ and Ω_g the conjugacy class of g in G.
Let us assume that $\mathrm{Card}(\Omega_g)$ and $\deg(\chi)$ are coprime integers.
According to Bézout's identity, there exists (u,v) in $\mathbb{Z}^2$ such that :

$$u\,\mathrm{Card}(\Omega_g)+v\deg(\chi)=1$$

So, we have :

$$\frac{\chi(g)}{\deg(\chi)}=u\frac{\mathrm{Card}(\Omega_g)\chi(g)}{\deg(\chi)}+v\chi(g)\in\mathcal{O}_{\mathbb{L}}$$

Moreover, by definition, $\chi(g)=\sum_{i=1}^{\deg(\chi)}\omega_i$, where ω_i are the eigenvalues of $\rho(g)$ (with multiplicities). But, ω_i are also d^{th} roots of unity, thus their modulus are equal to 1, hence : $\left|\frac{\chi(g)}{\deg(\chi)}\right|\leq 1$.

Let $x:=\frac{\chi(g)}{\deg(\chi)}$.

For all σ in $\mathrm{Gal}(\mathbb{L}/\mathbb{Q})$, $|\sigma(x)|\leq 1$, because $\sigma(x)=\sigma\left(\frac{\chi(g)}{\deg(\chi)}\right)=\frac{1}{\deg(\chi)}\sum_{i=1}^{\deg(\chi)}\sigma(\omega_i)$ and each $\sigma(\omega_i)$ is again a root of unity.

Hence, we can deduce that :

$$\left|\mathrm{N}_{\mathbb{L}/\mathbb{Q}}(x)\right|:=\left|\prod_{\sigma\in\mathrm{Gal}(\mathbb{L}/\mathbb{Q})}\sigma(x)\right|=\prod_{\sigma\in\mathrm{Gal}(\mathbb{L}/\mathbb{Q})}|\sigma(x)|\leq 1$$

As $\mathrm{N}_{\mathbb{L}/\mathbb{Q}}(x)$ belongs to $\mathbb{Z}$ (because x is an element of $\mathcal{O}_{\mathbb{L}}$), we can deduce that $\mathrm{N}_{\mathbb{L}/\mathbb{Q}}(x)$ belongs to the set $\{-1;0;1\}$. So, we have two cases :

- If $\mathrm{N}_{\mathbb{L}/\mathbb{Q}}(x)=0$, then $x=0$ and thus $\chi(g)=0$.

- If $\mathrm{N}_{\mathbb{L}/\mathbb{Q}}(x)$ is in $\{-1;1\}$, then $|\mathrm{N}_{\mathbb{L}/\mathbb{Q}}(x)|:=\prod_{\sigma\in\mathrm{Gal}(\mathbb{L}/\mathbb{Q})}|\sigma(x)|=1$ and thus we have in particular $|x|=1$ (because for all σ in $\mathrm{Gal}(\mathbb{L}/\mathbb{Q})$, $|\sigma(x)|\leq 1$ so here, as $\left|\mathrm{N}_{\mathbb{L}/\mathbb{Q}}(x)\right|=1$, we have $|\sigma(x)|=1$).

  Moreover, if there exists (i,j) in $[\![1;\deg(\chi)]\!]^2$ such that $\omega_i\neq\omega_j$, then $|x|<1$. Indeed, if we denote $\omega_i:=e^{\frac{2ik_1\pi}{d}}$ and $\omega_j:=e^{\frac{2ik_2\pi}{d}}$ (with k_1 and k_2 in $[\![0;d-1]\!]$), then :

  $$|\omega_i+\omega_j|=|\omega_i|\left|1+\frac{\omega_j}{\omega_i}\right|=\left|1+\frac{\omega_j}{\omega_i}\right|=\left|1+e^{\frac{2i(k_2-k_1)\pi}{d}}\right|=2\left|\cos\left(\frac{(k_2-k_1)\pi}{d}\right)\right|<2$$

  Consequently, $x=\omega_1=...=\omega_{\deg(\chi)}$ and thus, $\rho(g)$ is an homothety.

In particular, if moreover $\chi(g)\neq 0$, then $\rho(g)$ is an homothety and thus $\rho(g)$ is in $Z(\rho(G))$.

■

II.2 Proof of Burnside's theorem

This second subsection aims to prove Burnside's theorem.

This is a result demonstrated by William Burnside in 1904 and published in the newspaper *Proceeding of London Mathematical Society*. This result extends the work of Camille Jordan published in 1898, which itself come after results on the same subject due to Georg Frobenius. Burnside's demonstration uses representation theory and exploits the properties of the rings of integers of certain fields of numbers. Although some demonstrations avoid the theory of representations, we made the choice to follow more or less the original Burnside demonstration.

Lemma 1 :

Let G be a finite group of order p^aq^b with $p \neq q$ two prime numbers and a and b be two natural integers such that $ab \neq 0$.
If $Z(G) = \{e_G\}$, then there exists a conjugacy class different from a singleton of order a power of p or a power of q.

Proof :

Let us consider G a finite group of order p^aq^b with $p \neq q$ two prime numbers and a and b two natural integers such that $ab \neq 0$.
Let us assume that $Z(G) = \{e_G\}$.
We denote $\Omega_1, ..., \Omega_s$ the conjugacy class of G.
We know that all the conjugacy class are different from a singleton (because $Z(G) = \{e_G\} \neq G$) and the order of each conjugacy class divides the order of G.
Hence, for all i in $[\![1; s]\!]$, there exists (a_i, b_i) in $[\![0; a]\!] \times [\![0; b]\!]$ such that $\text{Card}(\Omega_i) = p^{a_i}q^{b_i}$.

We can not have for all i in $[\![1; s]\!]$, $a_i \neq 0$ and $b_i \neq 0$.
Indeed, if this is the case, according to the conjugacy class equation, we have :

$$\text{Card}(G) = \text{Card}(Z(G)) + \sum_{i=1}^{s} \text{Card}(\Omega_i)$$

That is to say :

$$p^aq^b = 1 + \sum_{i=1}^{s} p^{a_i}q^{b_i}$$

So, we have :

$$p^aq^b \equiv 1 + \sum_{i=1}^{s} p^{a_i}q^{b_i} \ [p]$$

That is to say :

$$0 \equiv 1 \ [p]$$

So, we have a contradiction.
Thus, there exists i in $[\![1; s]\!]$ such that $a_i = 0$ or $b_i = 0$. That is to say that there exists i in $[\![1; s]\!]$ such that $\text{Card}(\Omega_i)$ is a power of p or a power of q.

■

Proposition 7 :

Let G be a finite group.
If there exists a conjugacy class of order p^m (where p is a prime number and m in $\mathbb{N}^*$), then G contains a strict normal subgroup H (that is to say $H \lhd G$, $H \neq G$ and $H \neq \{e_G\}$).

Proof :

Let us consider G a finite group and g in G.
Let us assume that there exists a conjugacy class of order p^m (where p is a prime number and m in $\mathbb{N}^*$).
We denote $\Omega_g := \{xgx^{-1},\ x \in G\}$ the conjugacy class of g.
We know that :

$$\sum_{\chi \in \mathrm{Irr}(G)} \deg(\chi)\chi(g) = 0$$

We denote : $X := \{\chi \in \mathrm{Irr}(G) \text{ st } p \mid \deg(\chi)\}$ and $Y := \{\chi \in \mathrm{Irr}(G) \text{ st } p \nmid \deg(\chi)\}$.
So, we have :

$$\sum_{\chi \in Y} \deg(\chi)\chi(g) = -\sum_{\chi \in X} \deg(\chi)\chi(g)$$

Let d be the order of G and $\mathbb{L} := \mathbb{Q}\left(e^{\frac{2i\pi}{d}}\right)$.
We know that, for all χ in X, $\chi(g)$ is in $\mathcal{O}_{\mathbb{L}}$ (according to proposition 4). Moreover, for all χ in X, there exists n_χ in $\mathbb{N}^*$ such that $\deg(\chi) = pn_\chi$.

Hence, we have :

$$\sum_{\chi \in Y} \deg(\chi)\chi(g) = -p\sum_{\chi \in X} n_\chi\chi(g)$$

Finally, if we denote $Y_0 := \{\chi \in Y \text{ st } \chi(g) \neq 0\}$ and $\alpha := -\sum_{\chi \in X} n_\chi\chi(g) \in \mathcal{O}_{\mathbb{L}}$, we have :

$$\sum_{\chi \in Y_0} \deg(\chi)\chi(g) = p\alpha$$

We know that $\mathbb{1}_G$ is in Y_0, but $Y_0 \neq \{\mathbb{1}_G\}$. Indeed, if this is the case, we have $1 = p\alpha$ and thus $\alpha = \dfrac{1}{p}$ is not in $\mathcal{O}_{\mathbb{L}}$, which is a contradiction.

So, there exists ψ in Y_0 such that $\psi \neq \mathbb{1}_G$ and $\psi(g) \neq 0$.
Moreover, $\mathrm{Card}(\Omega_g) := p^m$ and $\deg(\psi)$ are coprime integers (because ψ is in $Y_0 \subseteq Y$), thus $\rho_\psi(g)$ is in $Z(\rho_\psi(G))$ (according to corollary 2).

If we denote $H := \mathrm{Ker}(\rho_\psi)$, then $H \lhd G$ and $H \neq \{e_G\}$ and $H \neq G$.
Indeed :

- $H \neq G$, because $\psi \neq \mathbb{1}_G$.

- And $H \neq \{e_G\}$. Indeed, if $H = \{e_G\}$, then since $\rho_\psi(g)$ in $Z(\rho_\psi(G))$, we have :

  $$\forall h \in \rho_\psi(G),\ h\rho_\psi(g) = \rho_\psi(g)h$$

  Which is equivalent to :

  $$\forall i \in G,\ \rho_\psi(i)\rho_\psi(g) = \rho_\psi(g)\rho_\psi(i)$$

  Hence :

  $$\forall i \in G,\ \rho_\psi(ig) = \rho_\psi(gi)$$

  And since ρ_ψ is an injective function (as $\mathrm{Ker}(\rho_\psi) = \{e_G\}$), we can conclude that for all i in G, $ig = gi$. And so, g is in $Z(G)$. So, in particular, $\Omega_g = \{g\}$ and thus, we have a contradiction with the hypothesis about the cardinal of Ω_g.

Finally, H is a strict normal subgroup of G.

■

We are now able to prove Burnside's theorem about solvable groups :

Theorem 3 : Burnside's theorem (1904) :

If G is a finite group of order $p^a q^b$ (where p and q are distinct prime numbers and a and b are two natural integers others than zero), then G is solvable.

Proof :

Let us assume that G is a finite group of order $p^a q^b$ (where p and q are distinct prime numbers and a and b are two natural integers others than zero).
Let us show the theorem by induction on the order of G :
For $\text{Card}(G) = 1$:
We already know that the trivial group is solvable.
So, the result is true for $\text{Card}(G) = 1$.

For $\text{Card}(G) = p^a q^b$:
Let us assume that the property is true for all groups of order smaller than $\text{Card}(G)$. What about $\text{Card}(G)$?
We have three cases to examine :

- If $Z(G) = \{e_G\}$ and $a = 0$ or $b = 0$, then G is a finite p-group and thus solvable (it is even the trivial group because $Z(G) = \{e_G\}$).

- If $Z(G) = \{e_G\}$ and $a \neq 0$ and $b \neq 0$, then according to lemma 1, there exists a conjugacy class different from a singleton and of order a power of p or q.
  Moreover, according to proposition 7, there exists a strict normal subgroup H of G.
  Hence, G/H and H are solvable (according to the induction hypothesis) and so, G is solvable (according to proposition 3).

- If $Z(G) \neq \{e_G\}$, then $\text{Card}(G/Z(G)) < \text{Card}(G)$, so according to the induction hypothesis, $G/Z(G)$ is solvable. Moreover, $Z(G)$ is abelian and thus solvable too.
  Finally, G is solvable (according to proposition 3).

So, the property is true for $\text{Card}(G) = p^a q^b$.

Finally, we have shown by induction Burnside's theorem.

■

Remark :
It is natural to wonder whether there is a proof of Burnside's theorem that does not use character theory. The answer to this question is positive, but it took more than 60 years to get such a demonstration !

Remark :
Burnside's theorem does not allow extension if the cardinal of G admits at least three prime factors. For example, $\mathfrak{A}_5$ (its cardinal is $\dfrac{5!}{2} = 60 = 2^2 \times 3 \times 5$) is not solvable (as we will see in the next chapter).

There is also another Burnside's theorem. This second result of Burnside that we are going to present (as a matter of curiosity) is probably less famous but it is as interesting as the first one !

Theorem 4 :

Let χ be an irreducible character of G of degree greater or equal than 2.
If G is a finite group, then there exists g in G such that $\chi(g) = 0$.

III To go further...

This last section is about Feit-Thompson theorem and some complements on the concept of solvable groups.

III.1 Feit-Thompson theorem

William Burnside conjectured that every non-abelian finite simple group has even order. Richard Brauer suggested using the centralizers of involutions of simple groups to classify finite simple groups, as the Brauer–Fowler theorem shows that there are only a finite number of finite simple groups with given centralizer of an involution. A group of odd order has no involutions, so to carry out Brauer's method it is first necessary to show that non-cyclic finite simple groups never have odd order. This is equivalent to show that odd order groups are solvable, which is what Feit and Thompson proved.

Theorem 5 : Feit-Thompson theorem :

Every finite group of odd order is solvable.

The theorem itself and many methods that Feit and Thompson introduced in their proofs played an essential role in the classification of finite simple groups. Besides, Feit and Thompson original proof, more than two hundred and fifty pages long, has been simplified in some details, but it has not been considerably shortened and its general structure has not been altered.

Remark :
From Feit-Thompson theorem we deduce that every odd number is a solvable number.

III.2 Supersolvable groups and polycyclic groups

In this last subsection, we briefly study the concepts of supersolvable and polycyclic groups.

Definition 4 : Supersolvable group :

We say that G is a **supersolvable group**, when there is a finite series of subgroups :

$$\{e_G\} := G_0 \subseteq G_1 \subseteq \cdots \subseteq G_n := G$$

such that :

- For all i in $[\![0;n]\!]$, G_i is a normal subgroup of G.
- For all i in $[\![0;n-1]\!]$, G_{i+1}/G_i is a cyclic group.

Remark :
An abelian group is supersolvable if, and only if, it is finitely generated.

Definition 5 : Polycyclic group :

We say that G is a **polycyclic group** , when there is a finite series of subgroups :

$$\{e_G\} := G_0 \subseteq G_1 \subseteq \cdots \subseteq G_n := G$$

such that :

- For all i in $[\![0; n-1]\!]$, G_i is a normal subgroup G_{i+1}.
- For all i in $[\![0; n-1]\!]$, G_{i+1}/G_i is a cyclic group.

Remark :
When each quotient G_{i+1}/G_i in the previous definition in infinite, we said that G is a **strongly polycyclic group**.

Remark :
The concepts of supersolvable and polycyclic groups are thus two refinements of the concept of solvable groups. Moreover, we have the following implications :

$$(G \text{ is supersolvable}) \implies (G \text{ is polycyclic}) \implies (G \text{ is solvable})$$

Moreover, when G is a finite group, it is possible to show that the concepts of polycyclic group and solvable group are equivalent (see theorem 9 of chapter 2).

Example 2 :

- For all integer n in $\mathbb{N}^*$, $\mathbb{Z}/n\mathbb{Z}$ is a supersolvable group.
  Indeed, we have the following finite series :

  $$\{\overline{0}\} \lhd \mathbb{Z}/n\mathbb{Z}$$

  and $(\mathbb{Z}/n\mathbb{Z})/\{\overline{0}\} \cong \mathbb{Z}/n\mathbb{Z}$, which is a cyclic group.

- For all integer $n \geq 2$, the dihedral group D_n of order $2n$ is supersolvable.
  Indeed, we have the following finite series :

  $$\{\mathrm{Id}\} \lhd \mathbb{Z}/n\mathbb{Z} \lhd D_n \quad \text{(unique up to an isomorphism)}$$

  and by definition :

  $$D_n = \mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$$

  So, $D_n/(\mathbb{Z}/n\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z}$ and $(\mathbb{Z}/n\mathbb{Z})/\{\mathrm{Id}\} \cong \mathbb{Z}/n\mathbb{Z}$ which are cyclic.

  Hence, D_n is a supersolvable group (and thus a polycyclic and solvable group).

- $\mathfrak{A}_4$ is not a supersolvable group, because it has the unique finite series :

  $$\left\{\mathrm{Id}_{[\![1;4]\!]}\right\} \lhd V_4 \lhd \mathfrak{A}_4$$

  But $V_4/\{\mathrm{Id}_{[\![1;4]\!]}\} \cong V_4$ is not a cyclic group.
  And so $\mathfrak{A}_4$ is not a polycyclic group either.

Proposition 8 :

Any subgroup of a supersolvable group is a supersolvable group.

Proof :

Let us consider H a subgroup of G.
Let us assume that G is supersolvable.
Then, there exists a finite series of subgroups :

$$\{e_G\} := G_0 \subseteq G_1 \subseteq \cdots \subseteq G_n := G$$

such that :

- For all i in $[\![0;n]\!]$, G_i is a normal subgroup G.

- For all i in $[\![0;n-1]\!]$, G_{i+1}/G_i is a cyclic group.

For all i in $[\![0;n]\!]$, let $H_i := G_i \cap H$.

Then H has a finite series :

$$\{e_G\} := H_0 \subseteq H_1 \subseteq \cdots \subseteq H_n := H$$

Indeed, for all i in $[\![0;n]\!]$, we have :

$$\forall g \in G_, \ gG_i = G_i g$$

So, in particular for all g in H, $gH_i = H_i g$.
Thus for all g in H, we have $gH_i = H_i g$, that is to say that H_i is a normal subgroup of H.

Let us show that the quotients are cyclic :
According to the second isomorphism theorem, we have :

$$\forall i \in [\![0;n-1]\!], \ \frac{H_{i+1}}{H_i} := \frac{G_{i+1} \cap H}{G_i \cap H} = \frac{G_{i+1} \cap H}{G_i \cap (G_{i+1} \cap H)} \cong \frac{G_i(G_{i+1} \cap H)}{G_i}$$

But this latter group is a subgroup of G_{i+1}/G_i which is cyclic. Hence, H_{i+1}/H_i is a cyclic group.

Finally, according to definition 4, H is a supersolvable group.

■

Proposition 9 :

Any quotient group of a supersolvable group is a supersolvable group.

Proof :

Let us consider N a normal subgroup of G.
Let us assume that G is supersolvable.
Then, there exists a finite series of subgroups :

$$\{e_G\} := G_0 \subseteq G_1 \subseteq \cdots \subseteq G_n := G$$

such that :

- For all i in $[\![0;n]\!]$, $G_i \lhd G$.
- For all i in $[\![0;n-1]\!]$, G_{i+1}/G_i is a cyclic group.

Then, G/N has a finite series :

$$\frac{N}{N} := \frac{G_0 N}{N} \subseteq \frac{G_1 N}{N} \subseteq \cdots \subseteq \frac{G_n N}{N} := \frac{G}{N}$$

Indeed, for all i in $[\![0;n]\!]$, G_iN is a normal subgroup of GN (because N is a normal subgroup of G (thus of each G_i) and G_i is also a normal subgroup of G) and finally, according to the correspondence theorem, $(G_iN)/N$ is a normal subgroup of $(GN)/N$.

Moreover, a typical quotient is $(G_{i+1}N/N)(G_iN/N)$, which by the third isomorphism theorem is isomorphic to $(G_{i+1}N)/(G_iN)$.

Moreover by the second and the third isomorphism theorem :

$$\forall i \in [\![0;n-1]\!],\ \frac{G_{i+1}N}{G_iN} = \frac{G_{i+1}(G_iN)}{G_iN} \cong \frac{G_{i+1}}{G_{i+1} \cap (G_iN)} \cong \frac{G_{i+1}/G_i}{(G_{i+1} \cap (G_iN))/G_i}$$

which is a quotient of the cyclic group G_{i+1}/G_i, so is cyclic.

Therefore, according to definition 4, G/N is a supersolvable group.

■

Proposition 10 :

Any subgroup of a polycyclic group is a polycyclic group.

Proof :

Let us consider H a subgroup of G.
Let us assume that G is polycyclic.
Then, there exists a finite series of subgroups :

$$\{e_G\} := G_0 \subseteq G_1 \subseteq \cdots \subseteq G_n := G$$

such that :

- For all i in $[\![0;n-1]\!]$, G_i is a normal subgroup of G_{i+1}.

- For all i in $[\![0;n-1]\!]$, G_{i+1}/G_i is a cyclic group.

For all i in $[\![0;n]\!]$, let $H_i := G_i \cap H$.

Then H has a finite series :

$$\{e_G\} := H_0 \lhd H_1 \lhd \cdots \lhd H_n := H$$

Indeed, for all i in $[\![0;n-1]\!]$, we have :

$$\forall g \in G_{i+1},\ gG_i = H_i g$$

So, in particular for all g in H_{i+1}, $gH_i = H_i g$.
Thus for all g in H_{i+1}, we have $gH_i = H_i g$, that is to say that H_i is a normal subgroup of H_{i+1}.

Let us show that the quotients are cyclic :
According to the second isomorphism theorem, we have :

$$\forall i \in [\![0;n-1]\!],\ \frac{H_{i+1}}{H_i} := \frac{G_{i+1} \cap H}{G_i \cap H} = \frac{G_{i+1} \cap H}{G_i \cap (G_{i+1} \cap H)} \cong \frac{G_i(G_{i+1} \cap H)}{G_i}$$

But this latter group is a subgroup of G_{i+1}/G_i which is cyclic. Hence, H_{i+1}/H_i is a cyclic group.

Finally, according to definition 5, H is a polycyclic group.

■

Proposition 11 :

Any quotient group of a polycyclic group is a polycyclic group.

Proof :

Let us consider N a normal subgroup of G.
Let us assume that G is polycyclic.
Then, there exists a finite series of subgroups :

$$\{e_G\} := G_0 \subseteq G_1 \subseteq \cdots \subseteq G_n := G$$

such that :

- For all i in $[\![0; n-1]\!]$, $G_i \lhd G_{i+1}$.
- For all i in $[\![0; n-1]\!]$, G_{i+1}/G_i is a cyclic group.

Then, G/N has a finite series :

$$\frac{N}{N} := \frac{G_0N}{N} \subseteq \frac{G_1N}{N} \subseteq \cdots \subseteq \frac{G_nN}{N} := \frac{G}{N}$$

Indeed, for all i in $[\![0; n-1]\!]$, G_iN is a normal subgroup of $G_{i+1}N$ (because N is a normal subgroup of G (thus each G_i) and G_i is also a normal subgroup of G_{i+1}) and finally, according to the correspondence theorem, $(G_iN)/N$ is a normal subgroup of $(G_{i+1}N)/N$.

Moreover, a typical quotient is $(G_{i+1}N/N)/(G_iN/N)$, which by the third isomorphism theorem is isomorphic to $(G_{i+1}N)/(G_iN)$.

Moreover by the second and the third isomorphism theorem :

$$\forall i \in [\![0; n-1]\!],\ \frac{G_{i+1}N}{G_iN} = \frac{G_{i+1}(G_iN)}{G_iN} \cong \frac{G_{i+1}}{G_{i+1} \cap (G_iN)} \cong \frac{G_{i+1}/G_i}{(G_{i+1} \cap (G_iN))/G_i}$$

which is a quotient of the cyclic group G_{i+1}/G_i, so is cyclic.

Therefore, according to definition 5, G/N is a supersolvable group.

■

Remark :

There exists also the concepts of **virtually solvable groups** (groups that have a solvable subgroup of finite index. And so, all solvable groups are virtually solvable, since one can just choose the group itself, which has index 1), **virtually polycyclic groups** (groups that have a polycyclic subgroup of finite index), and some others...

Chapter 2

Links with other types of groups

This chapter aims to study different links between the concept of solvable group and other types of groups.

We will start with some reminders about the notions of commutators and commutator subgroup, and then we will look at different types of groups and their relationship with solvable groups.

Although chapter's goal is to study several types of groups, the main objective is not to study these groups in detail (even if a few reminders will be made), but rather to examine the links between these groups and solvable groups.

For the whole chapter we consider a group $(G, *)$ (denoted G) and the identity element is denoted e_G for the law of internal composition "$*$".

I Reminders about commutators and commutator subgroup

The goal of this first section is to resume basic definitions and properties in order to apply these results to solvable groups.

I.1 Reminders

In this first subsection, we will give reminders about commutators and commutator subgroup.

Definition 1 : Commutator of two elements :

Let us consider g and h in G.
We call **commutator of** g **and** h, the element $g^{-1}h^{-1}gh$ in G.

Notations :

- We denote $[g, h]$ the commutator of g in G and h in G.
- When A and B are subgroups of G, we denote $[A, B]$ the subgroup of G generated by all the elements of the form $[a, b]$, with a in A and b in B.

Remark :

This definition is equivalent to $ghg^{-1}h^{-1}$ in G because $[g, h]^{-1} := \left(g^{-1}h^{-1}gh\right)^{-1} = h^{-1}g^{-1}hg := [h, g]$.

Proposition 1 : Properties of commutators :

- Two elements commute if, and only if, their commutator is the neutral element e_G.
- The inverse of a commutator is again a commutator.
- The conjugate of a commutator is again a commutator.
- For all x, y, z in G, we have :

$$\left[\left[x, y^{-1}\right], z\right]^{y}\left[\left[y, z^{-1}\right], x\right]^{z}\left[\left[z, x^{-1}\right], y\right]^{x} = e_G \quad \text{(Hall-Witt identity)}$$

Proposition 2 :

Let G_1 and G_2 be two groups and $f : G_1 \longrightarrow G_2$ a group homomorphism.
If A and B are two subgroups of G_1, then : $f([A, B]) = [f(A), f(B)]$.

Definition 2 : Commutator subgroup of a group :

We call **commutator subgroup of** G (or **derived subgroup of** G), the subgroup of G generated by all the commutators of elements of G.

Notation :
We denote G' (or again $D(G)$) the commutator subgroup of G :

$$G' = D(G) := [G, G] = \left\langle [g, h],\ (g, h) \in G^2 \right\rangle$$

Remark :
Be careful, the word "generated" of definition 2 is crucial ! Indeed, the set of all the commutators is not a subgroup of G in general. An element of the commutator subgroup of G is not necessary a commutator of G.
More precisely, let us consider $\mathcal{C} = \left\{[g, h],\ (g, h) \in G^2\right\}$ the set of commutators of G.

The commutator subset G is :

$$D(G) := \{\gamma_1^{\varepsilon_1} \cdots \gamma_r^{\varepsilon_r},\ r \in \mathbb{N},\ (\gamma_1, ..., \gamma_r) \in \mathcal{C}^r \text{ and } (\varepsilon_1, ..., \varepsilon_r) \in \{-1; 1\}^r\}$$

As the set $\mathcal{C}$ is stable by inverse, we can also write :

$$D(G) := \{\gamma_1 \cdots \gamma_r,\ r \in \mathbb{N} \text{ and } (\gamma_1, ..., \gamma_r) \in \mathcal{C}^r\}$$

Proposition 3 :

A group is abelian if, and only if, its commutator subgroup is trivial.

Proposition 4 :

- Let H be a subgroup of G.
  H contains $D(G)$ if, and only if, H is normal in G and the quotient G/H is abelian.
- The commutator subgroup $D(G)$ of G is the intersection of all the normal subgroups H of G whose quotient G/H is abelian :

$$D(G) = \bigcap_{\substack{G/H \text{ commutative} \\ H \trianglelefteq G}} H$$

Proposition 5 :

Let G_1 and G_2 be two groups.
If f is a group homomorphism from G_1 to G_2, then $f(D(G_1)) \subseteq D(G_2)$.

Moreover, if f is surjective, then $f(D(G_1)) = D(G_2)$.

Remark :
If $G_1 = G_2 = G$ in proposition 5, then $D(G)$ is stable by all automorphism of G. Thus, $D(G)$ is a characteristic subgroup (and then a normal subgroup) of G.

Definition 3 : Abelianization of a group :

We call **abelianization of** G (an denoted G^{ab}), the quotient group of G by its commutator subgroup.

Remark :
Abelianization of G is its "biggest abelian quotient".

Example 1 :

Let see commutator subgroups and abelianization of some classic groups :

- If G is an abelian group, then $D(G) = \{e_G\}$ and $G^{ab} = G$.

- For all integer $n \geq 2$, $D(\mathfrak{S}_n) = \mathfrak{A}_n$ and $\mathfrak{S}_n^{ab} \cong \mathbb{Z}/2\mathbb{Z}$.

- For all n in $\{1; 2; 3\}$, $D(\mathfrak{A}_n) = \{\mathrm{Id}\}$ ($\mathfrak{A}_2 = \{\mathrm{Id}\}$ and $\mathfrak{A}_3 \cong \mathbb{Z}/3\mathbb{Z}$ are abelian).

  Commutator subgroup of $\mathfrak{A}_4$ is $V = \{\mathrm{Id}; (1\ 2)(3\ 4); (1\ 3)(2\ 4); (1\ 4)(2\ 3)\}$, its unique proper normal subgroup. By cardinality, we have $\mathfrak{A}_4^{ab} \cong \mathbb{Z}/3\mathbb{Z}$.

  For all integer $n \geq 5$, $D(\mathfrak{A}_n) = \mathfrak{A}_n$ and $\mathfrak{A}_n^{ab} = \left\{\overline{\mathrm{Id}}\right\}$ (we will discuss it later).

- Let us consider $\mathbb{K}$ a field and n an integer non equal to 0.

  - If $n \neq 2$ or $\mathbb{K} \neq \mathbb{F}_2$, then we have : $D(\mathrm{GL}_n(\mathbb{K})) = \mathrm{SL}_n(\mathbb{K})$ and the determinant induce the following group isomorphism : $\mathrm{GL}_n(\mathbb{K})^{ab} \cong \mathbb{K}^*$.

  - If $n = 2$ and $\mathbb{K} = \mathbb{F}_2$, then we have : $D(\mathrm{GL}_2(\mathbb{F}_2)) = \mathrm{SL}_2(\mathbb{F}_2) \cong \mathfrak{S}_3$.

  - If $n \neq 2$ or $\mathbb{K}$ is different of $\mathbb{F}_2$ or $\mathbb{F}_3$, then we have : $D(\mathrm{SL}_n(\mathbb{K})) = \mathrm{SL}_n(\mathbb{K})$.

Proposition 6 :

Let H be a group, φ a group homomorphism from G to H and π^{ab} the natural surjection from G to its quotient G^{ab}.
φ gets factorise by π^{ab} if, and only if, $\mathrm{Im}(\varphi)$ is abelian.

I.2 Links with solvable group

This second subsection uses the reminders made above to give a characterization of resolvability that will be easier to manipulate than the definition (and in particularly to demonstrate the simplicity of group $\mathfrak{A}_5$).

Definition 4 : Derived series of a group :

We call **derived series of** G, the series $(D^n(G))_{n\in\mathbb{N}}$ defined by :

$$D^0(G) := G \text{ and for all } n \text{ in } \mathbb{N},\ D^{n+1}(G) := D(D^n(G))$$

Remark :
The series $(D^n(G))_{n\in\mathbb{N}}$ is a decreasing series (but not necessary stationary to $\{e_G\}$).

Proposition 7 :

Let $f : G_1 \longrightarrow G_2$ be a group homomorphism.
For all natural number n, we have : $f(D^n(G_1)) \subseteq D^n(G_2)$.

Moreover, if f is surjective, then : $f(D^n(G_1)) = D^n(G_2)$.

Proof :

Let us consider $f : G_1 \longrightarrow G_2$ a group homomorphism.
Let us show by induction that for all n in $\mathbb{N}$, $f(D^n(G_1)) \subseteq D^n(G_2)$ (and if f is surjective then we have the equality).
For $n = 0$:
By definition : $D^0(G_1) = G_1$ and $D^0(G_2) = G_2$.
Hence, by definition of f, we have $f(D^0(G_1)) \subseteq D^0(G_2)$ (and the equality is f is surjective).
So, the property is true for $n = 0$.

For n in $\mathbb{N}$:
Let us assume that the property is true for n. What about $n + 1$?
We know that if A and B are two subgroups of G_1, then $f([A, B]) = [f(A), f(B)]$.
So, with $A = B = D^n(G_1)$, we have :

$$f(D^{n+1}(G_1)) := f([D^n(G_1), D^n(G_1)]) = [f(D^n(G_1)), f(D^n(G_1))] := D(f(D^n(G))) \quad (*)$$

Moreover, by hypothesis, we have : $f(D^n(G_1)) \subseteq D^n(G_2)$ (and the equality is true if f is surjective). Thus, we have : $D(f(D^n(G_1))) \subseteq D^{n+1}(G_2)$ (and the equality is f is surjective).

So, according to $(*)$, we have : $f(D^{n+1}(G_1)) \subseteq D^{n+1}(G_2)$ (and the equality if f is surjective).
So, the property is true for the natural number $n + 1$.

Hence, we have shown by induction that for all natural number n, $f(D^n(G_1)) \subseteq D^n(G_2)$ (and if f is surjective, we have the equality).

■

Corollary 1 :

For all n in $\mathbb{N}$, $D^n(G)$ is a characteristic subgroup (and thus a normal subgroup) of G.

Proof :

Let us consider n a natural number.
According to proposition 7 with $G_1 := G_2 := G$, we have that, for all group automorphism, $f(D^n(G)) \subseteq D^n(G)$.

Hence, by definition, G is a characteristic subgroup of G (and thus a normal subgroup of G).

■

Theorem 1 :

If there exists a series such that :

- $G_0 := G$
- For all n in $\mathbb{N}$, G_{n+1} is a normal subgroup of G_n.
- For all n in $\mathbb{N}$, G_n/G_{n+1} is an abelian group.

then for all n in $\mathbb{N}$: $D^n(G) \subseteq G_n$.

Proof :

Let us assume that there is a series such that :

- $G_0 := G$
- For all n in $\mathbb{N}$, G_{n+1} is a normal subgroup of G_n.
- For all n in $\mathbb{N}$, G_n/G_{n+1} is an abelian group.

And let us show the by induction that for all n in $\mathbb{N}$, $D^n(G) \subseteq G_n$.
For $n = 0$:
By definition, we have : $D^0(G) := G$ and $G_0 := G$.
Hence, we immediately have : $D^0(G) \subseteq G$.
So, the property is true for $n = 0$.

For n in $\mathbb{N}$:
Let us assume that the property is true for n. What about $n + 1$?
By hypothesis, we know that G_n/G_{n+1} is an abelian group. Hence, $D(G_n) \subseteq G_{n+1}$ (according to proposition 4).

Moreover, $D^n(G) \subseteq G_n$, thus : $D^{n+1}(G) \subseteq D(G_n) \subseteq G_{n+1}$.
So, the property is true for the natural number $n + 1$.

Hence, we have shown by induction that for all natural number n, $D^n(G) \subseteq G_n$.

■

Corollary 2 :

If G is solvable, then for all k in $[\![0;n]\!]$, $D^k(G) \subseteq G_k$ (with notations of definition 1).

Proof :

Let us assume that G is a solvable group.
By definition, there exists a finite series such that :

- $G_0 := G$
- For all k in $[\![0;n]\!]$, G_{k+1} is a normal subgroup of G_k.
- For all k in $[\![0;n]\!]$, G_k/G_{k+1} is an abelian group.

Moreover, for all $k \geq n+1$, we denote $G_k := \{e_G\}$.

Then the series $(G_k)_{k\in\mathbb{N}}$ verifies the hypothesis of theorem 1. Hence, according to theorem 1, we can conclude that for all k in $\mathbb{N}$, $D^k(G) \subseteq G_k$.

So, we have in particular that for all k in $[\![0;n]\!]$, $D^k(G) \subseteq G_k$.

■

Remark :
In this proof we reverse the indexes of definition 1 of chapter 1, but the sequence is still the same.

Theorem 2 : Characterisation of a solvable group by its derived series :

G is a solvable group if, and only if, its derived series is stationary to $\{e_G\}$.

Proof :

- The assume that G is solvable.
  According to corollary 2, we have in particular : $D^n(G) \subseteq G_n := \{e_G\}$.
  Hence, $D^n(G) = \{e_G\}$. Moreover, $(D^n(G))_{n\in\mathbb{N}}$ is a decreasing series.
  So, the derived series of G is stationary to $\{e_G\}$.

- Let us assume that the derived series of G is stationary to $\{e_G\}$.
  Then, we have :
  - $G := D^0(G) \supseteq \cdots \supseteq D^n(G) := \{e_G\}$
  - Moreover, we know that for all i in $[\![0;n-1]\!]$:

$$D^{i+1}(G) := D\left(D^i(G)\right) = \bigcap_{\substack{D^i(G)/H \text{ commutative} \\ H \trianglelefteq D^i(G)}} H \quad \text{(according to proposition 4)}$$

  Thus, $D^{i+1}(G)$ is a normal subgroup of $D^i(G)$.

- $*$ By the same way, for all i in $[\![0;n-1]\!]$: $D^i(G)/D^{i+1}(G) := D^i(G)/D\left(D^i(G)\right) := D^i(G)^{ab}$ is abelian.

So, according to definition 1 of chapter 1, G is a solvable group.

Finally, we have shown the theorem by double implication.

■

Corollary 3 :

G is a solvable group if, and only if, $D(G)$ is a solvable group.

Proof :

- If G is a solvable group, then its derived series is stationary to $\{e_G\}$. Hence, if we denote $H := D(G)$, there exists n in $\mathbb{N}$ such that $D^n(H) = \{e_G\}$.
  So, $(D^n(H))_{n\in\mathbb{N}}$ is stationary to $\{e_G\}$ and thus, according to theorem 2, $D(G)$ is solvable.

- If $D(G)$ is a solvable group, then its derived series is stationary to $\{e_G\}$.
  Moreover, the derived series of G verifies :
  $$\forall n \in \mathbb{N}^*,\ D^n(G) = D^{n-1}(D(G))$$
  So, the derived series of G is also stationary to $\{e_G\}$.
  Hence, G is a solvable group (according to theorem 2).

Finally, we have shown the corollary by double implication.

■

Proposition 8 :

A non-trivial solvable group is different from its commutator group.

Proof :

Let us assume that G is a non trivial solvable group.
Let us assume, by contradiction, that $G = D(G)$.
Hence, for all n in $\mathbb{N}$, $D^n(G) = G$ and so, $(D^n(G))_{n\in\mathbb{N}}$ is stationary to $\{G\}$.

Moreover, G is a solvable group, so the series $(D^n(G))_{n\in\mathbb{N}}$ is stationary to $\{e_G\}$.

But we assumed that G is a non-trivial group, so we have a contradiction.

Finally, we can conclude that a non-trivial solvable group is different from its commutator group.

■

Definition 5 : Solvability class :

When G a solvable group, we call **solvability class**, the smallest natural number n such that $D^n(G) = \{e_G\}$.

Proposition 9 :

- A group is solvable for solvability class equal to 0 if, and only if, it is reduce to $\{e_G\}$.
- A group is solvable for solvability class equal to 1 if, and only if, it is a non-trivial abelian group.

Proof :

Let us show the first assertion :

- If $G = \{e_G\}$, then we have for all n in $\mathbb{N}$, $D^n(G) = \{e_G\}$.
  Then, $\{e_G\}$ is solvable for solvability class equal to 0.
- If G is a solvable group for solvability class equal to 0, then we have $D^0(G) = \{e_G\}$, that is to say $G = \{e_G\}$.

So, we have shown the first assertion.

Let us show the second assertion :

- If G is a non-trivial abelian group, then we have $D^1(G) := D(G) = \{e_G\}$ (according to proposition 3).
  Hence, G is solvable for solvability class equal to 1.
- If G is solvable for solvability class equal to 1, then $D^1(G) := D(G) = \{e_G\}$. So, G is an abelian group (according to proposition 3).
  Moreover, G is non-trivial because its solvability class is different from 0.

So, we have shown the second assertion.

We have finally shown the proposition.

■

Remark :
According to proposition 9, we can deduce that solvable groups for solvability class less or equal than 1 are exactly abelian groups.

Remark :
If the solvability class of G is equal to 2, then we say that G is a **metabelian group** (that is to say that the commutator subgroup of G is abelian).

Proposition 10 :

If $D(G)$ is a solvable group for solvability class equal to n in $\mathbb{N}$ and G is a non-trivial group, then G is a solvable group for solvability class equal to $n + 1$.

Proof :

Let us assume that $D(G)$ is a solvable group for solvability class equal to n in $\mathbb{N}$ and G is a non-trivial group.
according to corollary 3, G is also solvable.
As, G is a non-trivial solvable group, it is different from its commutator group (according to proposition 8).

Moreover, we have for all i in $\mathbb{N}^*$, $D^i(G) = D^{i-1}(D(G))$, so $D^{n+1}(G) = D^n(D(G)) = \{e_G\}$.

So, G has for solvability class $n+1$ (the minimality is due to the fact that is it is not the case, then there is a contradition with the hypothesis that $D(G)$ is solvable for solvability class equals to n).

■

Remarks :

- Let us consider $f : G_1 \longrightarrow G_2$ a group homomorphism and n a natural number.
  We know that, for all n in $\mathbb{N}$, $f(D^n(G_1)) = D^n(f(G_1))$ (according to an extension by induction of proposition 2). Hence, if G_1 is solvable for solvability class equal to n, then $f(G_1)$ is also solvable for solvability class less of equal than n.

  In particular, if H_1 is a normal subgroup of G, then :
  If G_1 is solvable for solvability class equal to n, then G_1/H_1 is solvable for solvability class less or equal than n.

- If f is a group isomorphism, according to the previous remark, we can conclude that :
  If G is solvable for solvability class equal to n in $\mathbb{N}$, then every group who is isomorphic to G is solvable for solvability class equal to n.

- We know that if H is a subgroup of G, then for all n in $\mathbb{N}$, $D^n(H) \subseteq D^n(G)$.
  So, if G is solvable for solvability class equal to n in $\mathbb{N}$, then H is solvable for solvability class less of equal than n.

These remarks allows us to consider the following theorem :

Theorem 3 :

Let H be a normal subgroup of G.
If G/H is solvable for solvability class equal to p and H is solvable for solvability class equal to q, then G is solvable for solvability class less or equal than $p+q$.

Proof :

Let us consider H a normal subgroup of G.
Let us assume that G/H is solvable for solvability class equal to p and H is solvable for solvability class equal to q,
Let π be the natural projection from G to G/H.
We have :

$$\pi(D^p(G)) = D^p(\pi(G)) = D^p(G/H) = \{e_G\}$$

Hence, $D^p(G) \subseteq H$. So :

$$D^{p+q}(G) := D^q(D^p(G)) \subseteq D^q(H) = \{e_G\}$$

So, $D^{p+q}(G) = \{e_G\}$ and we can conclude that G is solvable for solvability class less of equal than $p+q$ (according to theorem 2).

■

Remark :

It is possible that G is solvable for solvability class smaller than $p+q$. Indeed, if G is a direct product of a non-trivial abelian group H by another non-trivial abelian group K, then G, H and $G/H \cong K$ are all solvable for solvability class equal to 1.

Theorem 4 :

Let n be a natural number.
The following assertions are equivalents :

- G is solvable for solvability class less or equal to n.
- There exists a finite series $\{e_G\} := G_0 \subseteq \cdots \subseteq G_n := G$, whose quotients G_{i+1}/G_i are abelian and each G_i is a normal subgroup of G.
- There exists a finite series $\{e_G\} := G_0 \subseteq \cdots \subseteq G_n := G$, whose quotients G_{i+1}/G_i are abelian.

Proof :

Let us consider n a natural number.

- Let us assume that G is solvable for solvability class less or equal to n.
  If we denote, for all i in $\mathbb{N}$, $G_i := D^{n-i}(G)$, then we have immediately that : $\{e_G\} := G_0 \subseteq \cdots \subseteq G_n := G$, quotients G_{i+1}/G_i are abelian and $G_i := D^{n-i}(G)$ is a normal subgroup of G.
- Let us assume that there is a finite series $\{e_G\} := G_0 \subseteq \cdots \subseteq G_n := G$, whose quotients G_{i+1}/G_i are abelian and each G_i is a normal subgroup of G.
  We can immediately say that the same series verifies : $\{e_G\} := G_0 \subseteq \cdots \subseteq G_n := G$ and quotients G_{i+1}/G_i are abelian.
- Let us assume that there exists a finite series $\{e_G\} := G_0 \subseteq \cdots \subseteq G_n := G$, whose quotients G_{i+1}/G_i are abelian.
  We know that for all i in $\mathbb{N}$, $D^i(G) \subseteq G_{n-i}$ (according to theorem 1).
  In particular : $D^n(G) \subseteq G_0 := \{e_G\}$. Hence, $D^n(G) = \{e_G\}$ and G is solvable for solvability class less of equal than n.

Finally, we have shown the theorem by cyclic implications.

■

II Nilpotent groups

Nilpotent groups arise in Galois theory, as well as in the classification of groups. They also appear prominently in the classification of Lie groups.

This section aims to define nilpotent groups and give basic properties in order to give applications to solvable groups.

II.1 Definitions and properties

In this first subsection, we give the definition of a nilpotent group and first definitions.

Definition 6 : Lower central series :

We call **lower central series of** G (or again **descending central series of** G), the series :

$$G := C^1(G) \triangleright C^2(G) \triangleright \cdots \triangleright C^n(G) := \{e_G\}$$

where :

$$C^1(G) := G \text{ and for all } n \geq 2,\ C^n(G) := [C^{n-1}(G), G]$$

Definition 7 : Nilpotent group :

We say that G is a **nilpotent group**, when its lower central series is stationary to $\{e_G\}$.

Remark :
That is to say that there exists n in $\mathbb{N}$ such that $C^n(G) = \{e_G\}$ (and in particular, $C^2(G) := [G, G] := D(G)$).

Remark :
This definition of a nilpotent group is the definition with lower central series. But there exists also two others equivalent definitions :

- With the **central series** :
  That is, a series of normal subgroups $\{e_G\} := G_0 \triangleleft G_1 \triangleleft \cdots \triangleleft G_n := G$.
  Where, for all i in $[\![0; n-1]\!]$, $G_{i+1}/G_i \subseteq Z(G/G_i)$ (or equivalently $[G, G_{i+1}] \subseteq G_i$).

- With the **upper central series** :
  That is, a series of normal subgroups $\{e_G\} := Z_0 \triangleleft Z_1 \triangleleft \cdots \triangleleft Z_n := G$.
  Where, $Z_1 = Z(G)$ and for all i in $[\![0; n-1]\!]$, Z_{i+1} is the subgroup such that $Z_{i+1}/Z_i = Z(G/Z_i)$.

Definition 8 : Nilpotency class of a nilpotent group :

When G is a nilpotent group, we call **nilpotency class of** G, the smallest natural integer n in $\mathbb{N}$ such that $C^{n+1}(G) = \{e_G\}$.

Remark :
In this case, G is said to be **nilpotent of class** n.

Intuitively, a nilpotent group is a group that is "almost abelian". This idea is motivated by the fact that nilpotent groups are solvable, and for finite nilpotent groups, two elements having relatively prime orders must commute (it is also true that finite nilpotent groups are supersolvable). The concept is credited to work in the 1930s by Russian mathematician Sergei Chernikov.

Example 2 :

- Every abelian group G is nilpotent.
  Indeed, we know that $D(G) = \{e_G\}$, that is to say : $C^2(G) = C^{1+1}(G) = \{e_G\}$.
- The quaternion group $\mathbb{H}_8$ is nilpotent of class 2.
  Indeed, $C^2(\mathbb{H}_8) = D(\mathbb{H}_8) = \{-1; 1\}$ and $C^3(\mathbb{H}_8) := [\{-1; 1\}, \mathbb{H}_8] = \{1\}$.

Proposition 11 :

- A group is nilpotent of class 0 if, and only if, it is trivial.
- A group is nilpotent of class 1 if, and only if, it is abelian and non trivial.

Proof :

- Let us show the first assertion :
  - If G is the trivial group, then : $C^1(G) := G = \{e_G\}$.
    Hence, G is nilpotent of class 0.
  - If G is nilpotent of class 0, we have (by definition of nilpotency class) $C^1(G) := G = \{e_G\}$.
    So, G is the trivial group.

  So, we have shown the first assertion.
- Le us show the second assertion :
  - If G is a non trivial abelian group, according to example 2, we have that G is nilpotent of class 1.
  - If G is nilpotent of class 1, then $C^1(G) := G \neq \{e_G\}$ and $C^2(G) := D(G) = \{e_G\}$.
    Hence, G is abelian and non trivial.

  So, we have shown the second assertion.

Finally, we have shown the proposition.

■

Proposition 12 :

Let H be a subgroup of G.
If G is nilpotent, then H is nilpotent.

Proof :

Let us consider H a subgroup of G.
Let us assume that G is nilpotent.
Let us show by induction that for all i in $\mathbb{N}^*$, $C^i(H)$ is a subgroup of $C^i(G)$.
For $i = 1$:
By definition, we have : $C^1(H) := H$ is a subgroup of $C^1(G) := G$.
So, the property is true for $i = 1$.

For i in $\mathbb{N}^*$:
Let us assume that the property is true for i. What about $i + 1$?
We have :

$$C^{i+1}(H) := \left[C^i(H), H\right] \text{ a subgroup of } \left[C^i(G), G\right] := C^{i+1}(G)$$

Hence, we can conclude that the property is true for $i + 1$.

Finally, we have shown by induction that for all i in $\mathbb{N}^*$, $C^i(H)$ is a subgroup of $C^i(G)$.

As G is nilpotent, there exists n in $\mathbb{N}^*$ such that $C^n(G) = \{e_G\}$ and so, according to the previous induction, $C^n(H)$ is a subgroup of $\{e_G\}$, thus $C^n(H) = \{e_G\}$.

So, we can conclude that H is nilpotent.

■

Proposition 13 :

Let H be a normal subgroup of G.
If G is nilpotent, then G/H is nilpotent.

Proof :

Let us consider H a normal subgroup of G.
Let us assume that G is nilpotent.
Let $\left(C^i(G)\right)_{i\in\mathbb{N}^*}$ be a lower central series of G.
The image series by the natural projection from G to G/H is $\left(C^i(G)H/H\right)_{i\in\mathbb{N}^*}$.
And we have :

$$\left[C^i(H)/H, G/H\right] = \left[C^i(G), G\right] H/H$$

which is a subgroup of $C^{i-1}(G)H/H$ (because a commutator $[xH, yH]$ can be written $[x, y]H$).

The obtained series is a lower central series of G/H.

Finally, G/H is a nilpotent group.

■

II.2 Application to solvable groups

This subsection aims to show a link between nilpotent groups and solvable groups and also state and prove Schmidt's theorem.

II.2.1 General results

First, we give some links between nilpotent groups and solvable groups (and more precisely between their nilpotency class and solvability class).

Lemma 1 : Lemma of the three subgroups :

Let N be a normal subgroup of G and H, K and L three subgroups of G.
If two of the subgroups $[[H,K],L]$, $[[K,L],H]$ and $[[L,H],K]$ are include in N, then the last one is also include in N.

Proof :

Let us consider N a normal subgroup of G and H, K and L three subgroups of G.
Let us assume that two of the subgroups $[[H,K],L]$, $[[K,L],H]$ and $[[L,H],K]$ are include in N.
We just have to show that if $[[K,L],H]$ and $[[L,H],K]$ are include in N then $[[H,K],L]$ is also include in N (the other cases are deduced by a circular permutation of the variables).

Let us begin with the case where $N = \{e_G\}$.
In this case, we have $[[K,L],H] = [[L,H],K] = \{e_G\}$, and we have to prove that $[[H,K],L] = \{e_G\}$. So, we have just to show that all the elements of L commutes with all the elements of $[H,K]$. But $[H,K]$ is generated by the elements $[h,k]$ (with (h,k) in $H \times K$). So, we have to show that for all h, k, ℓ in $H \times K \times L$, we have $[[h,k],l] = e_G$:

Let h, k, ℓ in $H \times K \times L$.
According to Hall-Witt identity, we have :

$$[[h,k],\ell]^{k^{-1}} \left[\left[k^{-1},\ell^{-1}\right],h\right]^{\ell} \left[\left[\ell,h^{-1}\right],k^{-1}\right]^{h} = e_G$$

By hypothesis, we have $[[K,L],H] = [[L,H],K] = \{e_G\}$, then $\left[\left[k^{-1},\ell^{-1}\right],h\right] = \left[\left[\ell,h^{-1}\right],k^{-1}\right] = e_G$.

So, we have $\left[\left[k^{-1},\ell^{-1}\right],h\right]^{\ell} \left[\left[\ell,h^{-1}\right],k^{-1}\right]^{h} = e_G$ and then $[[h,k],\ell]^{k^{-1}} = e_G$.

Hence, we have $[[h,k],\ell] = e_G$.
So, we can conclude that we have $[[H,K],L] \subseteq N$ when $N = \{e_G\}$.

Let us consider the general case :
If we denote p the natural projection from G to G/N, then we have :

$$[[p(K),p(L)],p(H)] = p([[K,L],H]) \text{ and } [[p(L),p(H)],p(K)] = p([[L,H],K])$$

As $[[K,L],H]$ is supposed contained in N, we have $p([[K,L],H]) = \{N\}$. By the same way, $p([[L,H],K]) = \{N\}$.

According to the first part of the demonstration, $[[p(H),p(K)],p(L)] = \{N\}$, that is to say that $p([[H,K],L]) = \{N\}$, and thus $[[H,K],L] \subseteq N$.

Finally, we have shown the lemma of the three subgroups.

■

Corollary 4 :

If H, K and L are three normal subgroups of G, then :

$$[[H,K],L] \subseteq [[K,L],H][[L,H],K]$$

Proof :

Let us consider H, K and L three normal subgroups of G.
Because H, K and L are three normal subgroups of G, we can deduce that $[[K,L],H]$ and $[[L,H],K]$ are normal too (because conjugacy is a group homomorphism).

So, $[[K,L],H][[L,H],K]$ is a normal subgroup of G and it contains $[[K,L],H]$ and $[[L,H],K]$, then according to the lemma of the three subgroups, $[[H,K],L]$ is contained in $[[K,L],H][[L,H],K]$.

■

We can now use these results to demonstrate the following lemma :

Lemma 2 :

For all i, j in $\mathbb{N}^*$, we have : $\left[C^i(G), C^j(G)\right] \subseteq C^{i+j}(G)$.

Proof :

Let i be a natural number different form 0.
Let us show by induction that for all j in $\mathbb{N}^*$, $\left[C^i(G), C^j(G)\right] \subseteq C^{i+j}(G)$.
For $j = 1$:
We have :

$$\left[C^i(G), C^1(G)\right] := \left[C^i(G), G\right] := C^{i+1}(G)$$

So, the property is true for $j = 1$.

For j in $\mathbb{N}^*$:
Let us assume that the property is true for j in $\mathbb{N}^*$. What about $j+1$?
According to corollary 4 :

$$\begin{aligned}\left[C^{j+1}(G), C^i(G)\right] &:= \left[\left[C^j(G), G\right], C^i(G)\right] \\ &\subseteq \left[\left[G, C^i(G)\right], C^j(G)\right]\left[\left[C^i(G), C^j(G)\right], G\right] \\ &\subseteq \left[C^{i+1}(G), C^j(G)\right]\left[C^{i+j}(G), G\right]\end{aligned}$$

Moreover, $\left[C^{i+1}(G), C^j(G)\right] \subseteq C^{i+j+1}(G)$ (by hypothesis) and $\left[C^{i+j}(G), G\right] := C^{i+j+1}(G)$.
So, each to the factors to the second member are include in $C^{i+j+1}(G)$, thus : $\left[C^i(G), C^j(G)\right] \subseteq C^{i+j+1}(G)$.
So, the property is true for $j+1$.

Hence, we have shown by induction that for all j in $\mathbb{N}^*$, $\left[C^i(G), C^j(G)\right] \subseteq C^{i+j}(G)$.

Finally, we have shown the lemma.

■

Remark :
Sometimes, we have the equality but this is not true in generality (for example with dihedral groups).

Lemma 3 :

For all i, j in $\mathbb{N}^*$, we have : $C^i\left(C^j(G)\right) \subseteq C^{ij}(G)$.

Proof :

Let j be a natural number different from 0.
Let us show by induction that for all i in $\mathbb{N}^*$, $C^i\left(C^j(G)\right) \subseteq C^{ij}(G)$.
For $i = 1$:
$C^1\left(C^j(G)\right) := C^j(G) = C^{1\times j}(G)$.
So, the property is true for $i = 1$.

For i in $\mathbb{N}^*$:
Let us assume that the property is true for i in $\mathbb{N}^*$. What about $i+1$?
According to lemma 2, we have :

$$C^{i+1}\left(C^j(G)\right) := \left[C^i\left(C^j(G)\right), C^j(G)\right] \subseteq \left[C^{ij}(G), C^j(G)\right] \subseteq C^{ij+j}(G) = C^{(i+1)j}(G)$$

So, we can conclude that $C^{i+1}\left(C^j(G)\right) \subseteq C^{(i+1)j}(G)$.
So the property is true for $i+1$.

Hence, we have shown by induction that for all i in $\mathbb{N}^*$, we have : $C^i\left(C^j(G)\right) \subseteq C^{ij}(G)$.

Finally, we have shown the lemma.

■

Lemma 4 :

For all i in $\mathbb{N}$, we have : $D^i(G) \subseteq C^{2^i}(G)$.

Proof :

Let us show by induction that for all i in $\mathbb{N}$, $D^i(G) \subseteq C^{2^i}(G)$.
For $i = 0$:
We have :

$$D^0(G) := G := C^1(G) = C^{2^0}(G)$$

So, the property is true for $i = 0$.

For i in $\mathbb{N}$:
Let us assume that the property is true for i in $\mathbb{N}$. What about $i+1$?
So, we have :

$$D^{i+1}(G) := \left[D^i(G), D^i(G)\right] \subseteq \left[C^{2^i}(G), C^{2^i}(G)\right] \subseteq \left[C^{2^i}(G), G\right] := C^{2^{i+1}}(G)$$

So, we can conclude that $D^{i+1}(G) \subseteq C^{2^{i+1}}(G)$.
So, the property is true for $i+1$.

Hence, we have shown by induction that for all i in $\mathbb{N}$, $D^i(G) \subseteq C^{2^i}(G)$.

■

Proposition 14 :

Let n be a natural number.
If G is nilpotent of class less or equal than $2^n - 1$, then G is solvable of class less or equal than n.

Proof :

Let us assume that G is nilpotent of class less or equal than $2^n - 1$.
Then, we have $C^{2^n}(G) = \{e_G\}$. And so, according to lemma 4, $D^n(G) = \{e_G\}$.

So, we can conclude that G is solvable of class less or equal than n.

■

Corollary 5 :

Every nilpotent group is solvable.

Proof :

Let us assume that G is nilpotent.
Hence, there exists n in $\mathbb{N}$ such that nilpotency class of G is less or equal than $2^n - 1$.

So, according to proposition 14, G is solvable of class less or equal then n.

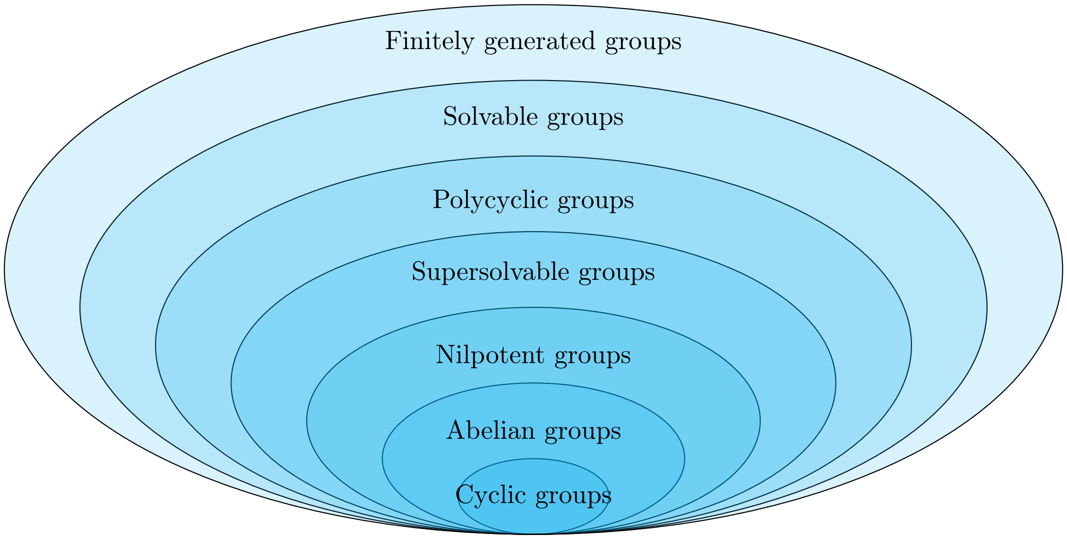
So, in particular, G is solvable.

■

Remark :
We can also show by induction that :
If G is nilpotent of class n in $\mathbb{N}$, then G is solvable of class less or equal than n.

Remark :
A solvable group is not necessary nilpotent (for example $\mathfrak{S}_3$ is solvable but not nilpotent).

So, if we restrict ourselves to finite groups, we can consider the following arrangement of classes of groups :



II.2.2 Schmidt's theorem

To conclude this subsection, we give a last result called "Schmidt's theorem" and demonstrate by Otto Schmidt in 1924.

Lemma 5 :

If G is a finite group with maximum subgroups trivially intersecting two to two, one of these maximum subgroups is normal.

Proof :

Let us assume that G is a finite group with maximum subgroups trivially intersecting two to two.
Let us prove this lemma by contradiction :
Let us assume that no maximum subgroup of G is normal. Then :

- For any maximal subgroup H of G, the normalizer of H is reduce to H (because H is not normal in G and $H \subseteq N_G(H)$), so the number of conjugate of H is equal to the index (greater or equal than 2) of $N_G(H) = H$.

- G is not a cyclic group (because if this is the case, then G is abelian and H is a strict normal subgroup of G and $N_G(H) = G$), hence :

  * The index of all maximal subgroups is upper bounded by $\dfrac{\text{Card}(G)}{2}$.

  * G is the union of all its maximal subgroups.

For H a maximal subgroups of G, the $H\backslash\{e_G\}$ form a partition of $G\backslash\{e_G\}$ (because maximum subgroups trivially intersecting two to two). By denoting $\widetilde{\Omega_i}$ the conjugacy classes of the $H\backslash\{e_G\}$ and c the number of conjugacy class, we have :

$$G\backslash\{e_G\} = \bigsqcup_{\substack{H \text{ normal} \\ \text{subgroup}}} H\backslash\{e_G\} = \bigsqcup_{i=1}^{c} \widetilde{\Omega_i}$$

Hence, by denoting h_i the index of the subgroups of the i^{th} conjugacy class and g the cardinal of G, we have the following equality :

$$g-1 = \sum_{i=1}^{c} \text{Card}\left(\widetilde{\Omega_i}\right) = \sum_{i=1}^{c} h_i\left(\text{Card}(H_i) - 1\right) = \sum_{i=1}^{c} h_i\left(\frac{g}{h_i} - 1\right) = \sum_{i=1}^{c}(g - h_i) = cg - \sum_{i=1}^{c} h_i \in \left[\frac{cg}{2}; c(g-2)\right]$$

So, we have : $\dfrac{cg}{2} \leq g - 1 \leq c(g-2)$, that is to say that c is in $\{1; 2\}$.
But, if $c = 1$, then $g - 1$ is in $\left[\dfrac{g}{2}; g-2\right]$ (which is impossible). And if $c = 2$, then $g - 1$ is in $[g; 2g-4]$ (which is also impossible). So, we have a contradiction.

Finally, we can conclude that one of the maximum subgroups of G is normal.

■

Theorem 5 : Schmidt's theorem :

If G is a finite group and all the proper subgroups of G are nilpotent, then G is solvable.

Proof :

Let us assume that G is a finite group and all the proper subgroups of G are nilpotent.
We already know that cyclic group are solvable. So, we can assume that G is not a cyclic group.

Let us show by induction the property :
For Card(G) = 1 :
We already know that $\{e_G\}$ is a solvable group.
So, the property is true for Card(G) = 1.

For Card(G) in $\mathbb{N}^*$:
Let us assume that the property is true for every group of order smaller than Card(G). What about Card(G)?
If one of the maximal subgroups M of G is normal, then G is solvable. Indeed, M and G/M are solvable (because M is nilpotent by hypothesis and G/M is a cyclic group of prime order), so according to proposition 3 of chapter 1, G is solvable.

Now, we can assume that G has not maximal subgroup who are normal.
According to the contraposition of lemma 5, the exists two maximal subgroups M and N of G such that $I := N \cap M \neq \{e_G\}$. Let us assume that M and N are chosen such that this intersection is of maximal order. There exist x in $M \backslash I$ who normalize I (because I is a proper subgroup of the nilpotent group M). By the same way, there exists y in $N \backslash I$ who normalize I.

Moreover, the subgroup $< I, x, y >$ is equal to G.
Indeed, if this is not the case, there exists a maximal subgroup R of G who contains $< I, x, y >$ and distinct from M (because y is in R but y is not in M). Hence, $M \cap R$ has an order greater than Card(I) (because $I \cup \{x\} \subseteq M \cap R$), which is not possible according to the construction of I.

The subgroup I is normal in G (because x and y normalize it). Moreover, proper subgroups of I and G/I are nilpotent and I is distinct from $\{e_G\}$ and G. Hence, I and G/I are of order smaller than Card(G).

Finally, according to the hypothesis, I and G/I are solvable. Thus, according to proposition 3 of chapter 1, G is solvable.
So, the property is true for Card(G) in $\mathbb{N}^*$.

Finally, we have shown Schmidt's theorem by induction.

■

Remark :
Kenkichi Iwasawa gave a more precise description of group G with the same hypothesis (more precisely, with the same hypothesis, G is nilpotent or of order $p^m q^n$ with p and q two distinct prime numbers and n, m in $\mathbb{N}^*$).

III Simple groups

We turn to groups which are in a sense the "opposite of solvable".

This section aims to give links between simple groups and solvable groups. More precisely, we will study $\mathfrak{A}_n$ and $\mathfrak{S}_n$ groups for $n \geq 5$ and give some recent developments.

III.1 Definition and properties

In this first subsection, we give the definition of a simple group and first links with solvable groups.

Definition 9 : Simple group :

We say that G is a **simple group**, when its only normal subgroups are $\{e_G\}$ and G.

Example 3 :

- Every cyclic group of prime order is simple, since it has no subgroups other than itself and the trivial group (and hence no other normal subgroup).
- Sporadic groups are simple.

The term "simple" means that such groups are not, in a sense, "reducible" to a more manageable group. The advantage of a normal non-trivial subgroup H of G is often to allow the construction of the quotient group G/H. The study of G is then reduced to that of H and G/H. This construction is not possible for a simple group and therefore one can not reduce one's study to that of a smaller cardinal quotient group.
Hence, simple groups play an important role in finite group theory. They are in a sense the fundamental units from which all finite groups are made.

Theorem 6 :

A solvable group is simple if, and only if, it is cyclic of prime order.

Proof :

- If G is a cyclic group of prime order, then it is simple (according to example 3) and also solvable (as it is abelian).
- If G is a simple solvable group, then there exists a finite series :

$$\{e_G\} := G_0 \subseteq G_1 \subseteq \cdots \subseteq G_n := G$$

  such that :

  - For all i in $[\![0; n-1]\!]$, G_i is a normal subgroup of G_{i+1}.
  - For all i in $[\![0; n-1]\!]$, G_{i+1}/G_i is an abelian group.

  We may assume that for all i in $[\![0; n-1]\!]$, $G_{i+1} \neq G_i$ (by deleting repeats).

  Then, G_{n-1} is a proper normal subgroup of G, which is simple, so $G_{n-1} = \{e_G\}$ and $G \cong G_n/G_{n-1}$ which is abelian.

So, G is a cyclic and simple group. But we know that the only cyclic and simple groups are cyclic groups of prime order. Hence, G is cyclic of prime order.

Finally, we have shown the theorem by double implication.

■

Remarks :

- A corollary of this theorem is that :
  If G is solvable and simple, then G is abelian.

- The contraposition of this corollary gives us that :
  If G is not abelian, then G is not solvable or G is not simple.
  In particular, sporadic groups are non abelian simple groups. Hence, we can conclude that sporadic groups are not solvable (we will see again this result by another way in the section V of this chapter).

Proposition 15 :

Every finite simple group is cyclic of prime order or of even order.

Proof :

Let us assume that G is a finite simple group.

- If, G is solvable, then according to theorem 6, G cyclic of prime order.

- If G is not solvable, according to contraposition of Feit-Thompson theorem, G has an even order.

■

Remark :
As sporadic groups are finite simple groups, they are cyclic of prime order or even order. But we know that they are not cyclic, hence they all have even order.

III.2 Study of $\mathfrak{A}_n$ and $\mathfrak{S}_n$ for $n \geq 5$

In this subsection, we are going to study with details $\mathfrak{A}_n$ and $\mathfrak{S}_n$ groups for $n \geq 5$. Results of this subpart will be used in the chapter IV during the study of general equation of degree n.

Indeed, we already know that $\mathfrak{S}_3$ and $\mathfrak{S}_4$ are solvable according to example 1 of chapter 1. And then, according to proposition 1, $\mathfrak{A}_3$ and $\mathfrak{A}_4$ are solvable too. Finally, $\mathfrak{S}_1$, $\mathfrak{A}_1$, $\mathfrak{S}_2$ and $\mathfrak{A}_2$ are solvable because they are abelian groups (as their cardinals are smaller than 5).

The following fundamental theorem is due to Galois :

Theorem 7 :

For all natural integer $n \geq 5$, $\mathfrak{A}_n$ is not a solvable group.

Proof :

Let us consider a natural integer $n \geq 5$.
Let us show that $D(\mathfrak{A}_n) = \mathfrak{A}_n$:
We know that $\mathfrak{A}_n$ is generated by 3-cycles, it is enough to show that a 3-cycle $(a\ b\ c)$ is an element of $D(\mathfrak{A}_n)$.

Let d and e be two elements of $[\![1;n]\!]$ distinct from a, b and c (which is possible because $n \geq 5$).
We have :

$$[(a\ c\ d), (b\ c\ e)] := (a\ d\ c)(b\ e\ c)(a\ c\ d)(b\ c\ e) = (a\ b\ c)$$

Then : $\mathfrak{A}_n \subseteq D(\mathfrak{A}_n)$.
As $D(\mathfrak{A}_n)$ is always included in $\mathfrak{A}_n$, we have finally : $\mathfrak{A}_n = D(\mathfrak{A}_n)$.

Hence, for all natural number n, $D^n(\mathfrak{A}_n) = \mathfrak{A}_n \neq \left\{\mathrm{Id}_{[\![1;n]\!]}\right\}$.

Finally, the derived series of $\mathfrak{A}_n$ is stationary to $\mathfrak{A}_n$.

Then, according to the characterisation of solvable groups by their derived series, we can conclude that $\mathfrak{A}_n$ is not solvable.

$\blacksquare$

Remark :
Another way to do is to show that for all natural number $n \geq 5$, $\mathfrak{A}_n$ is simple an then, if $\mathfrak{A}_n$ is solvable, it would be of prime order. However, for $n \geq 5$, $\dfrac{n!}{2}$ is not a prime number.

This result is very important because it is the basis of the theory of solving polynomial equations by radicals (as we will see in chapter 4). Indeed, this is this result that shows that general polynomial equations of degree greater of equal than 5 are not solvable by radicals.

Corollary 6 :

For all natural integer $n \geq 5$, $\mathfrak{S}_n$ is not a solvable group.

Proof :

Let us consider a natural integer $n \geq 5$.
Let us assume that $\mathfrak{S}_n$ is a solvable group.
Then, $\mathfrak{A}_n$ is also a solvable group (because $\mathfrak{A}_n$ is a subgroup of $\mathfrak{S}_n$).

However, according to theorem 7, $\mathfrak{A}_n$ is not a solvable group.

Hence, we have a contradiction.

Finally, we can conclude that $\mathfrak{S}_n$ is not a solvable group.

$\blacksquare$

III.3 Recent developments

The search for finite simple groups was completed in 1981. Galois had discovered the first : the alternating groups $\mathfrak{A}_n$ for $n \geq 5$. Émile Mathieu had discovered a few more in 1861. Their research (since Richard Brauer's speech in 1954 at the Congress of Mathematicians and Claude Chevalley's work at the same time) and the proof that those obtained were indeed the only ones, represented an enormous effort on the part of the mathematical community.

When put together end to end, the demonstration elements fill nearly 10,000 pages, the record length of a demonstration ! When we know that it is accepted that even the best mathematicians can make a mistake every 50 pages on average...

Some simple groups can be divided into infinite series and others are unique in their kind : sporadic simple groups ! Among these, the one called the **monster group**, or sometimes the **friendly giant** (for the beauty of its properties), is spectacular : it has about 10^{54} elements (specifically : $2^{46} \times 3^{20} \times 5^9 \times 7^6 \times 11^2 \times 13^3 \times 17 \times 19 \times 23 \times 29 \times 31 \times 41 \times 47 \times 59 \times 71$).

III.4 Links with Jordan-Hölder series

To conclude this section about simple groups, we give an extension with the link between solvable groups and Jordan-Hölder series.

Definition 10 : Composition series :

We call **composition series of** G, the finite series of subgroups :

$$\{e_G\} := G_0 \subseteq G_1 \subseteq \cdots \subseteq G_n := G$$

such that for all i in $[\![0; n-1]\!]$, G_i is a normal subgroup of G_{i+1}.

Example 4 :

The cyclic group $\mathbb{Z}/12\mathbb{Z}$ has $\{\overline{0}\} \lhd \mathbb{Z}/2\mathbb{Z} \lhd \mathbb{Z}/6\mathbb{Z} \lhd \mathbb{Z}/12\mathbb{Z}$, $\{\overline{0}\} \lhd \mathbb{Z}/2\mathbb{Z} \lhd \mathbb{Z}/4\mathbb{Z} \lhd \mathbb{Z}/12\mathbb{Z}$ and $\{\overline{0}\} \lhd \mathbb{Z}/3\mathbb{Z} \lhd \mathbb{Z}/6\mathbb{Z} \lhd \mathbb{Z}/12\mathbb{Z}$ as three different composition series.

For a cyclic group of order n, composition series correspond to ordered prime factorizations of n, and in fact yields a proof of the fundamental theorem of arithmetic.

Definition 11 : Jordan-Hölder series :

We call **Jordan-Hölder series of** G, every composition series of G which quotients are simple.

Example 5 :

The three series in the previous example are also Jordan-Hölder series of $\mathbb{Z}/12\mathbb{Z}$.

Remark :
Every finite group has at least one Jordan-Hölder series.

Theorem 8 :

If G is solvable and has a Jordan-Hölder series, then all the quotients are cyclic of prime order.

Proof :

Let us assume that G has a Jordan-Hölder series $\{e_G\} := G_0 \lhd G_1 \lhd \cdots \lhd G_n := G$.
Let G_{i+1}/G_i be a quotient of the previous Jordan-Hölder series.
G_{i+1} is a subgroup of G and G is solvable, hence G_{i+1} is solvable (according to proposition 1 of chapter 1).
So, G_{i+1}/G_i is a quotient of a solvable group and thus, it is solvable.
Moreover, G_{i+1}/G_i is a simple group (by definition of a Jordan-Hölder series).

Finally, G_{i+1}/G_i is a cyclic group of prime order (according to theorem 6).

■

Theorem 9 :

Let us assume that G is a finite group.
G is solvable if, and only if, it has a composition series which all quotients are cyclic of prime order.

Proof :

Let us assume that G is a finite group.

- Let us assume that G is solvable.
  Because G is finite, there exists a Jordan-Hölder series of G (and so in particular a composition series).
  And thus, according to theorem 8, all quotient of this composition series are cyclic of prime order.

- Let us assume that G has a composition series which all quotient are cyclic of prime order.
  Hence, all quotient are abelian, and thus, according to theorem 4, G is solvable.

Finally, we have shown the theorem by equivalence.

■

IV p-groups

This section aims to define p-groups and give basic properties in order to give applications to solvable groups.

In this whole section, p is a prime number and n is in $\mathbb{N}^*$.

IV.1 Some reminders about p-groups

In this first subpart, we give some reminders about p-groups without demonstration.

Definition 12 : p-group :

We call **p-group**, any finite group with order equal to a power of p.

Example 6 :

- $\mathbb{Z}/p\mathbb{Z}$ and $\mathbb{Z}/p^n\mathbb{Z}$ are p-groups.

- D_4 and $\mathbb{H}_8$ are two 2-groups.

- $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ is a 3-group.

Proposition 16 : Class equation for p-groups :

Let us assume that G act on a not empty finite set X.
If we denote $\text{Fix}_G(X) = \{x \in X \text{ st } \forall g \in G,\ gx = x\}$ the set of elements of X fixed under the action of G, then :

$$\text{Card}(X) \equiv \text{Card}(\text{Fix}_G(X))\ [p]$$

Proposition 17 :

If G is a non trivial p-group, then $Z(G) \neq \{e_G\}$.

IV.2 Application to solvable groups

Now, we will use the results of the previous subpart to give applications to solvable groups.

Proposition 18 :

All p-groups are solvable.

Proof :

Let us assume that G is a p-group of order p^n.
Now, let us show by induction that all p-groups are solvable :
For $n = 1$:
G has order p^1, hence G is cyclic of prime order.
Hence, G is a simple and solvable group.
So, the property is true for $i = 1$.

For n in $\mathbb{N}^*$:
Let us assume that all p-groups of order p^k with $k < n$ are solvable. What about a p-group of order p^n?
First of all, if G is abelian, than G is solvable. So, we can assume that G is not abelian.
We know that $Z(G)$ is a subgroup of G, so (by Lagrange's theorem), $\text{Card}(Z(G))$ divides $\text{Card}(G) = p^n$.

Moreover, G is a non-abelian p-group, so there exists k in $[\![1; n-1]\!]$ such that $\text{Card}(Z(G)) = p^k$.

Hence, $Z(G)$ is a p-group of order $p^k < p^n$, so by hypothesis, $Z(G)$ is a solvable group.

Moreover, $Z(G)$ is a normal subgroup of G and $\text{Card}(G/Z(G)) = p^{n-k} < p^n$, so by hypothesis, $G/Z(G)$ is also a solvable group.

So, we can conclude that G is a solvable group (according to proposition 3 of chapter 1).
So, the property is true for $n + 1$.

Hence, we have shown by induction that all p-groups are solvable.

■

Remark :
Another demonstration that all finite p-groups are solvable is that a finite p-group is a nilpotent group (more precisely, if $n \geq 2$, then a group of order p^n is nilpotent of class smaller than n) and based on the previous results, we find again the fact that p-groups are solvable.

Proposition 19 :

If G is a p-group of order p^n, then there exists a finite series of subgroups $\{e_G\} := G_0 \subseteq G_1 \subseteq \cdots \subseteq G_n := G$ such that for all i in $[\![0; n]\!]$, G_i is a normal subgroup of G and $\text{Card}(G_i) = p^i$.

Proof :

Let us assume that G is a p-group of order p^n.
We know that $Z(G) \neq \{e_G\}$ and $Z(G) \lhd G$.
So, $Z(G)$ is an abelian group of order equal to p^ℓ (with ℓ in $[\![1;n]\!]$) according to Lagrange's theorem.

Let x in $Z(G)\backslash\{e_G\}$.
So, $o(x)$ divides p^ℓ, then there exists i in $[\![1;\ell]\!]$ such that $o(x) = p^i$.

Let us consider $y := x^{p^{i-1}}$.
y has order p, because $x^{p^{i-1}} \neq e_G$ and $y^p := \left(x^{p^{i-1}}\right)^p = x^{p^i} := e_G$.

So, $\text{Card}(< y >) = p$ and $< y > \lhd G$ (because $< y > \subseteq Z(G)$).

Let us show the proposition by induction :
For $n = 0$:
$G := \{e_G\}$ and we just have the series $\{e_G\} := G_0 \lhd \{e_G\} := G$, where G_0 has order p^0.
So, the property is true for $n = 0$.

For n in $\mathbb{N}$:
Let us assume that the proposition is true for all p-groups of order p^k with $k < n$. What about a p-group of order p^n?
Let y in $Z(G)$ such that $\text{Card}(< y >) = p$. By hypothesis, the order of $G/ < y >$ is p^{n-1}, and so, there exists a finite series of subgroups $H_0 = \{e_{G/<y>}\} \subseteq \cdots \subseteq H_{k-1} := G/ < y >$ such that :

$$\forall i \in [\![0; k-1]\!],\ H_i \lhd G/ < y > \ \text{ and } |H_i| = p^i$$

Hence, if π is the natural projection from G to $G/ < y >$, we have :

$$\{e_G\} \subseteq \pi^{-1}(H_0) \subseteq \cdots \subseteq \pi^{-1}(H_{k-1})$$

Moreover :

$$\forall i \in [\![0; n-1]\!],\ \pi^{-1}(H_i) \lhd G \text{ and } \ \text{Card}(\pi^{-1}(H_i)) = \text{Card}(\text{Ker}(\pi))\,\text{Card}(H_i) = p^{i+1}$$

So, the property is true for n in $\mathbb{N}$.

Finally, we have shown by induction the proposition.

■

Corollary 7 :

All p-groups are supersolvable.

Proof :

Let us assume that G is a p-group or order p^n.
According to proposition 19, there exists a finite series $\{e_G\} := G_0 \subseteq G_1 \subseteq G_2 \subseteq \cdots \subseteq G_n := G$ such that for all i in $[\![0;n]\!]$, G_i is a normal subgroup of G and $\mathrm{Card}(G_i) = p^i$.

Hence :

- By hypothesis, for all i in $[\![0;n]\!]$, G_i is a normal subgroup of G.
- For all i in $[\![0:n-1]\!]$, $\mathrm{Card}(G_{i+1}/G_i) := \dfrac{p^{i+1}}{p^i} = p$.
  So, the quotient G_{i+1}/G_i is cyclic.

Finally, we can deduce that G is a supersolvable group (according to definition 4 of chapter 1).

■

V Perfect groups

We conclude this chapter with the study of perfect groups and their links with solvable groups. Here we will use results about simple and p-groups.

V.1 Definition

We begin with the definition of a perfect group and some basic examples.

Definition 13 : Perfect group :

We say that G is a **perfect group**, when $D(G) = G$.

Remark :
A characterization of a perfect group is that :
A group is perfect if, and only if its abelianization is trivial.

So, a perfect group is the "opposite" of an abelian group.

Example 7 :

- The trivial group is perfect.
- For all natural number $n \geq 5$, $\mathfrak{A}_n$ is a perfect group.
- Let us consider $\mathbb{K}$ a field and n in $\mathbb{N}^*$.
  If $n \geq 2$ and $\mathrm{car}(\mathbb{K}) = 2$, then $\mathrm{GL}_n(\mathbb{K})$ is a perfect group.

Remark :
We have even the following result :
In a finite non-abelian simple group, every element is a commutator (that is to say that every finite non-abelian simple group is perfect). In particular, sporadic groups are perfect (because the only abelian simple groups are cyclic groups), and then not solvable (and far enough to be abelian...).

The demonstration of this theorem, conjectured by Øystein Ore in 1951, was completed in 2010. The major part of this 1951 paper by Øystein Ore was devoted to showing that in the symmetric infinite group $\mathfrak{S}_{\mathbb{N}}$ every element is a commutator.

V.2 Application to solvable groups

Now, we will use the results of the previous subpart to give applications to solvable groups.

Proposition 20 :

Any non-trivial solvable group is not perfect.

Proof :

Let us assume that G is a non-trivial perfect group.
Then, for all natural number n in $\mathbb{N}$, $D^n(G) = G \neq \{e_G\}$.
So, the derived series of G is stationary to $G \neq \{e_G\}$ and thus, G is not solvable (according to the characterization of solvable group by its derived series).

Finally, by contraposition, we have shown the proposition.

■

Proposition 21 :

If $\text{Card}(G) < 60$, then G is solvable.

Proof :

Let us assume that $\text{Card}(G) < 60$.
According to Burnside's theorem, if $\text{Card}(G) = p^a q^b$ (with p and q two different prime numbers and a and b are to natural numbers), then G is solvable. Moreover, $\{e_G\}$ is a solvable group (because its abelian) and all finite p-group of order p^n (with p a prime number and n a natural number) are solvable. So, we just have to check the other cases.

The last cases is when $\text{Card}(G) = 2 \times 3 \times 5 = 30$ and $\text{Card}(G) = 2 \times 3 \times 7 = 42$.

- If $\text{Card}(G) = 42 = 7^1 \times 6$, then according to Sylow's theorems :

  $$n_7 \text{ divides } 6 \text{ and } n_7 \equiv 1 \ [7]$$

  Then, $n_7 = 1$ and thus, G has an unique 7-Sylow (denoted H).
  Hence, this 7-Sylow is normal in G and thus, G is not simple.

  Moreover, any group of order smaller than $\text{Card}(G)$ is solvable. Then, according to corollary 1 of chapter 1, G is solvable.

- If $\text{Card}(G) = 30 = 5^1 \times 6 = 3^1 \times 10$, then according to Sylow's theorems :

  $$n_5 \text{ divides } 6 \text{ and } n_5 \equiv 1 \ [5]$$

  $$n_3 \text{ divides } 10 \text{ and } n_3 \equiv 1 \ [3]$$

  Then, n_5 is in $\{1, 6\}$ and n_3 is in $\{1, 10\}$.

Moreover, we can not have $n_5 = 6$ and $n_3 = 10$ (because if it is the case, then there are too much elements). And so, there is at least a normal 3-Sylow or a normal 5-Sylow. Hence, G is not simple.

Moreover, any group of order smaller than $\text{Card}(G)$ is solvable. Then G is solvable (according to corollary 1 of chapter 1).

Finally, G is solvable.

■

Corollary 8 :

If $1 < \text{Card}(G) < 60$, then G is not perfect.

Proof :

Let us assume that $1 < \text{Card}(G) < 60$.
So G is not trivial and according to proposition 21, G is solvable.

Then G is a non-trivial solvable group and thus not perfect (according to proposition 20).

■

Remark :
According to the previous corollary, $\mathfrak{A}_5$ is the smallest non-trivial perfect group (unique up to an isomorphism).

Definition 14 : Quasi-perfect group :

We say that G is a **quasi-perfect group**, when its commutator subgroup $D(G)$ is perfect.

Remarks :

- Naturally, the concept of perfect group is stronger than the concept of quasi-perfect group.
- There exists also the concept of **superperfect group** (this concept is stronger than just the concept of perfect group).

Chapter 3

Non-graduated ruler and compass constructions

In this chapter, we will approach the concept of constructible numbers, which are the numbers that we can construct using only a non-graduated ruler and a compass. We will see that there is a strong link between constructible numbers and Galois theory.

First of all, we will give a definition of what is a constructible number and some examples. Secondly, we gill study links between constructability and Galois theory. The third section aims to study the construction of regular polygons. Finally, we will modify the rules by using other tools or methods of construction.

We shall consider the following question :

For which values of n can the regular n-gon be constructed by non-graduated ruler and compass ?

The ancient Greeks knew of constructions for 3-,5- and 15-gons and also knew how to construct a $2n$-gon given an n-gon by the obvious method of bisecting the angles. For about 2000 years little progress was made beyond the Greeks. Then, on 30 March 1796, Gauss made the remarkable discovery that the regular 17-gon could be constructed. In his *Disquistiones Arithmeticae* he stated necessary and sufficient conditions for constructibility of the regular n-gon.

I Definitions and basic constructions

This first section aims to give the first examples of constructible numbers and the basics constructions with non graduated ruler and compass.

We identify the usual plane $\mathbb{R}^2$ as the field of complex numbers $\mathbb{C}$.

In here, every constructions will start from 0 and 1. During our constructions, we are allowed to use the following actions :
$\underline{C1(\alpha, \beta)}$: From $\alpha \neq \beta$, we can draw the line l that goes through α and β.
$\underline{C2(\gamma, \alpha, \beta)}$: From $\alpha \neq \beta$ and γ, we can draw the circle C with center γ whose radius is the distance from α to β.
$\underline{P1}$: The point(s) of intersection of distinct lines ℓ_1 and ℓ_2 constructed as above.
$\underline{P2}$: The point(s) of intersection of a line ℓ and a circle C constructed as above.
$\underline{P3}$: The point(s) of intersection of distinct circles C_1 and C_2 constructed as above.

Definition 1 : Constructible number :

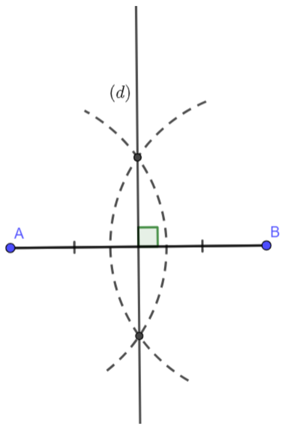
A complex number α is called **constructible number**, when there is a finite series of non-graduated ruler and compass constructions using $C1$, $C2$, $P1$, $P2$ and $P3$ that begins with 0 and 1 and ends with α.

For Euclid, a constructible number is a number associated with a constructible length. Nowadays, a constructible number is a number obtained as the coordinate of a constructible point from a grid. It is now known that the set of constructible numbers contains the set of rational numbers, but is strictly included in the set of algebraic numbers. In particular, we know that the number π (transcendent) is not constructible (squaring the circle) and that $\sqrt[3]{2}$ (an algebraic number) is not constructible either (doubling the cube).

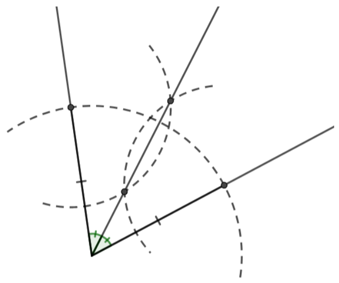
In geometry, the non-graduated ruler and the compass are the basic tools for working in plane geometry. They allow simple constructions such as those of axis or center of symmetry, parallel or perpendicular and are at the origin of the study of the so-called remarkable elements in a triangle. But some constructions remain unfeasible, such as the construction of a regular heptagon or the extraction of a cubic root.

Example 1 :

- The main construction of geometry is probably the tracing of the mediator of a segment. The mediator of the segment $[AB]$ is the line (d) that crosses perpendicularly $[AB]$ in its middle but it is also the set of equidistant points of the ends of the segment.
  It is enough to open the compass over a length greater than half of the length of the segment, then draw two circles with this radius, one centered on A, the other on B (we can only draw arcs of a circle). The intersection of the two circles consists of two points located equidistant from A and B, and thus define the mediator (this method also makes it possible to place a middle or to construct a perpendicular).



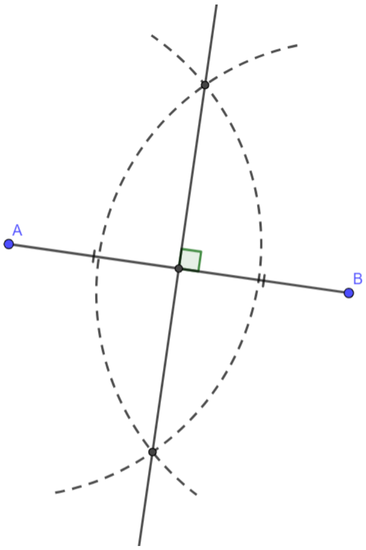
- The bisector of an angle, or more precisely, of an angular sector, is the axis of symmetry of that sector. It is enough to construct on each half-line two points equidistant from the top by constructing the points of intersection of the half-lines with the same circle centered at the top of the angle. By taking these two points as the centers of two circles of the same radius, two arcs of circle are constructed which intersect into two points, both of which belong to the desired bisector.



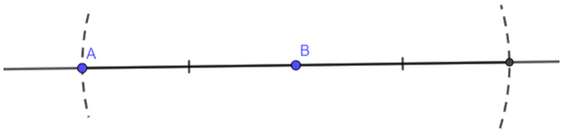
  It is therefore always possible to cut an angle into two equal parts using the non graduated ruler and the compass. But it is not always possible to cut an angle into equal three parts with a ruler and a compass : that's the problem of trisection of the angle.

Example 2 :

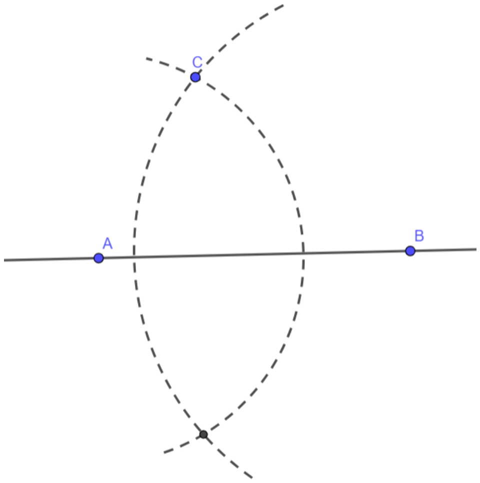
- The middle of the segment $[AB]$ is obtained by constructing the intersection point of the line (AB) with the mediator of the segment $[AB]$.



- The symmetric of point A with respect to B is obtained by constructing the point of intersection (different from A) between the line (AB) and the circle of center B passing through A.

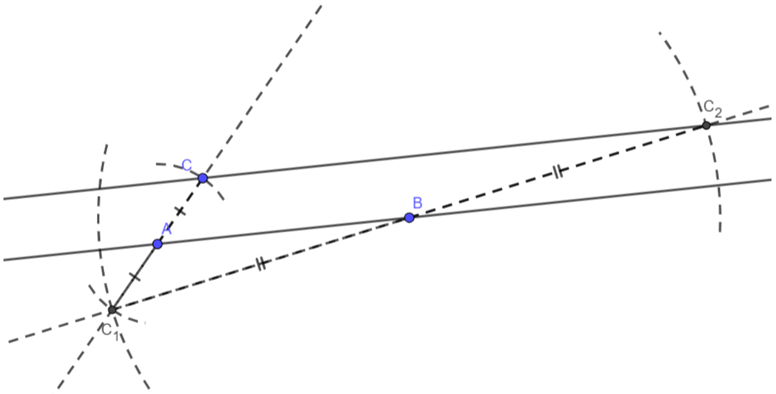


The symmetric of point C with respect to the line (AB) is obtained by constructing the point of intersection (different from C) between the circle of center A passing through C and the circle of center B passing through C (if point C is on the line (AB), then it is its own symmetric and no construction is required).

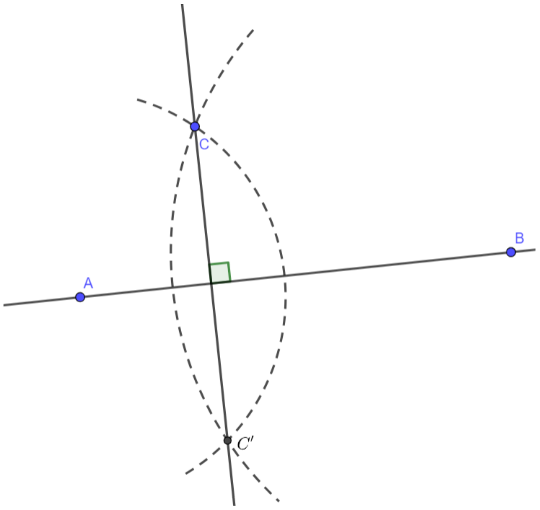


Example 3 :

- The parallel to the line (AB) passing through a point C is constructed using the right-of-middle property. We construct the symmetric C_1 of the point C with respect to A and then the symmetric C_2 of the point C_1 with respect to B. The desired line is the line (CC_2).



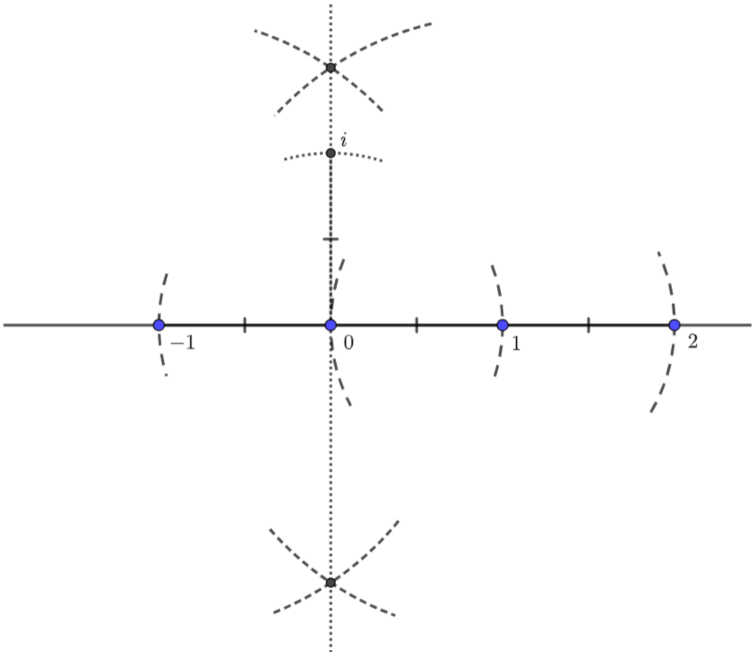
- The perpendicular to the line (AB) passing through a point C not situated on (AB) is the line (CC') joining point C to its symmetrical to the line (AB).
  If point C is located on (AB), it is sufficient to take the symmetric A' (or B') of point A (or B) with respect to C, then the perpendicular is the mediator of $[AA']$ (or $[BB']$).



Example 4 :

The will construct the points i and 2 :

- We start from 0 and 1.
- To build 2, we use $C2(1,0,1)$ and $P2$.
- To build i, we construct the perpendicular (d) going through 0 and finally we use $P2$ with (d) and $C2(0,0,1)$.



II Link between constructability and Galois theory

In this second section, we will study necessary and sufficient condition of constructability and the link with Galois theory and solvable groups.

In this whole section, we denote $\mathcal{C} := \{\alpha \in \mathbb{C} \text{ st } \alpha \text{ is constructible}\}$.

Theorem 1 :

The set $\mathcal{C}$ is a subfield of $\mathbb{C}$.
Furthermore, we have :

- $\alpha := a + ib$ is in $\mathcal{C}$ if, and only if, a and b are in $\mathcal{C} \cap \mathbb{R}$.
- If α is in $\mathcal{C}$, then any square root of α is in $\mathcal{C}$.

Proof :

- First of all, let us prove that $\mathcal{C}$ is a subgroup of $\mathbb{C}$ under addition :

  * By definition, 0 is in $\mathcal{C}$.

  * Let α be in $\mathbb{C}^*$.
    One construct the line connecting 0 and α by $C1(0,\alpha)$ and the circle of radius $|\alpha|$ centered at 0 by $C2(0,0,\alpha)$. These intersect in $\pm\alpha$, so that $-\alpha$ is constructible by $P2$.

  * Let (α,β) in $\mathcal{C}$.
    If $0,\alpha$ and β are collinear, then using $C1(\alpha,\beta)$ and $C2(\beta,0,\alpha)$, these intersect in $\alpha\pm\beta$ so that $\alpha+\beta$ is constructible by $P2$.
    If they are non collinear, then, using $C2(\beta,0,\alpha)$ and $C2(\alpha,0,\beta)$, one of the point of intersection is $\alpha+\beta$, so by $P3$, $\alpha+\beta$ is constructible.

  Finally, $\mathcal{C}$ is a subgroup of $\mathbb{C}$ under addition.

- We will now prove that if α is constructible and different from 0, then, $\dfrac{1}{\alpha}$ is also constructible.
  To do so, we will write $\alpha := re^{i\theta}$ and then $\dfrac{1}{\alpha} := \dfrac{1}{r}e^{-i\theta}$.
  To construct $e^{-i\theta}$, we can draw the line ℓ going through $e^{i\theta}$ and perpendicular to the $\mathbb{R}$-axis. Then, by using $P2(\ell,C)$ where C is $C2(0,0,1)$.

  Let's prove that for r in $\mathcal{C}\cap\mathbb{R}$, $\dfrac{1}{r}$ is in $\mathcal{C}$.
  Let us draw the triangle with vertices $0,r$ and i.
  If we draw the line d going through 1 and that is parallel with the line going through r and i, then $P1(d,(0,i))$ is the point $\dfrac{i}{r}$ thanks to Thales theorem.
  Now, thanks to $C_{\frac{1}{r}} := C2\left(0,\dfrac{i}{r}\right)$ and $P2\left((0,1),C_{\frac{1}{r}}\right)$, we construct $\dfrac{1}{r}$.
  Finally, if α is in $\mathcal{C}$, then $\dfrac{1}{\alpha}$ is also in $\mathcal{C}$.

- We will then prove that $\alpha = a+ib$ is in $\mathcal{C}$ if, and only if, a and b are in $\mathcal{C}\cap\mathbb{R}$:

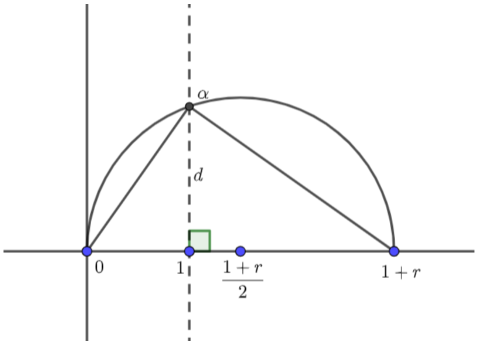
  * Let us assume that $\alpha = a+ib$ is in $\mathcal{C}$.
    We can draw perpendiculars from α to the $\mathbb{R}$-axis and imaginary-axis (those are constructed with $C1(0,1)$ and $C1(0,i)$). This shows that a and ib are constructible. By $C2(0,0,ib)$, this circle intersect the $\mathbb{R}$-axis in b, so that b is constructible by $P2$.

  * Let us assume that a and b are in $\mathcal{C}\cap\mathbb{R}$.
    Applying $C2(0,0,b)$ and $P2$ with the imaginary-axis shows that ib is constructible. Since we proved that $\mathcal{C}$ is a subgroup of $\mathbb{C}$, we have that $\alpha := a+ib$ is constructible.

- Now, let us complete the proof of $\mathcal{C}$ being a subfield of $\mathbb{C}$:
  Let us consider (α,β) in $\mathcal{C}^2$ with $\alpha := a+ib$ and $\beta := c+id$.
  Then we have $\alpha\beta = (ac-bd)+i(ad-bc)$ in $\mathcal{C}$ by what we have proved in the previous point.

- Finally, let us assume that α is constructible
  We can also assume that $\alpha \neq 0$ (because if this is the case, the result is trivial).
  If we write $\alpha := re^{i\theta}$ with $r := |\alpha| > 0$, then it suffices, to show that $\sqrt{r}e^{i\frac{\theta}{2}}$ is constructible.
  To prove this, one notes that the constructibility of α implies that θ is constructible (using the $\mathbb{R}$-axis and $C1(0, \alpha)$) and then we can bisect this angle to obtain $\dfrac{\theta}{2}$.
  Furthermore, using $C2(0, 0, \alpha)$ and $P2$ with the $\mathbb{R}$-axis, we have that r is constructible.

  We now have to prove that $\sqrt{r}$ is constructible, with r in $\mathcal{C} \cap \mathbb{R}_+$:



  Considering the graphic above (which is constructible because r is in $\mathcal{C}$ and thus $\dfrac{1+r}{2}$ is constructible and then we can apply $C2\left(\dfrac{1+r}{2}, 0, \dfrac{1+r}{2}\right)$), it is easily provable that α is constructible when r is in $\mathcal{C}$. Furthermore, the triangle with vertices $1, \alpha, 1+r$ is a right-angled triangle and the triangle with vertices $0, 1, \alpha$ is similar to the previous one. Hence we got that :

$$\frac{1}{d} = \frac{d}{r}$$

  where d is the distance between 1 and α.
  So, $d^2 = r$ and d is obviously constructible and thus, $d = \sqrt{r}$ is in $\mathcal{C}$.

Finally, we have shown the theorem.

■

Remark :

Hence, we can deduce that $\mathbb{Q}$ is a constructible set.
Indeed, every element of $\mathbb{Q}$ can be written as $\dfrac{p}{q}$ with p in $\mathbb{Z}$ and q in $\mathbb{N}^*$. Moreover, p and q are constructible numbers because $\mathbb{N}$ is clearly a constructible set, q in $\mathbb{N}^* \subsetneq \mathbb{N}$ and p is (or can be) the symmetric of a number included in $\mathbb{N}$. So, according to theorem 1, $\dfrac{p}{q}$ is constructible.

Example 5 :

- $2 + \sqrt{\dfrac{4\sqrt{5} - 3\sqrt{7}}{11}}$ is constructible.
- $\sqrt[3]{2}$ is not a constructible number.

Theorem 2 :

Let α in $\mathbb{C}$.
α is in $\mathcal{C}$ if, and only if, there are subfields of $\mathbb{C}$ such that :

$$\mathbb{Q} := F_0 \subseteq F_1 \subseteq \cdots \subseteq F_n \subseteq \mathbb{C}$$

and for all i in $[\![0; n-1]\!]$, $[F_{i+1} : F_i] = 2$ and α is in F_n.

Proof :

- Let's suppose we have $\mathbb{Q} := F_0 \subseteq F_1 \subseteq \cdots \subseteq F_n \subseteq \mathbb{C}$ where for all i in $[\![0; n-1]\!]$, $[F_{i+1} : F_i] = 2$ and α is in F_n.
  Thanks to Galois theory, $F_i = F_{i-1}(\beta_i)$ for β_i in F_{i-1} a square root of some α_i in F_{i-1}.

  Let us show by induction that for all i in $[\![0; n-1]\!]$, $F_i \subseteq \mathcal{C}$.
  For $i = 0$:
  We have already seen that $F_0 := \mathbb{Q} \subseteq \mathcal{C}$.
  So the property is true for $i = 0$.

  For i in $[\![0; n-2]\!]$:
  Let us assume that the property is true for i in $[\![0; n-2]\!]$. What about $i+1$?
  Then α_{i+1} is in F_i is constructible, which implies that β_{i+1}, a square root of α_{i+1}, is in $\mathcal{C}$ by theorem 1. Hence, any α in F_{i+1} is constructible and thus, $F_{i+1} \subseteq \mathcal{C}$.
  So, the property is true for $i+1$.

  Finally, we have shown by induction that for all i in $[\![0; n-1]\!]$, $F_i \subseteq \mathcal{C}$, and thus we can deduce that α is in $\mathcal{C}$.

- Conversely, let us assume that α is in $\mathcal{C}$.
  We need to create successive quadratic extensions that start from $\mathbb{Q}$ and eventually contain α. We will prove that there are extensions $\mathbb{Q} = F_0 \subseteq \cdots \subseteq F_n \subseteq \mathbb{C}$ where for all i in $[\![0; n-1]\!]$ $[F_{i+1} : F_i] = 2$ and such that F_n contains the real and the imaginary parts of all numbers constructed during the course of constructing α.

  Let us show this result by induction on the number N of times we use $P1, P2, P3$ in the construction of α.
  For $N = 0$:
  We have $\alpha = 0$ or $\alpha = 1$ in which case, we let $F_n = F_0 = \mathbb{Q}$.
  So the property is true for $N = 0$.

  For N in $\mathbb{N}$:

  * Let us assume that α is constructed in N in $\mathbb{N}$ steps, where the last step is $P1$, the intersection of ℓ_1 and ℓ_2.
    ℓ_1 was constructed from $C1(\alpha_1, \beta_1)$ and ℓ_2 from $C1(\alpha_2, \beta_2)$. By the inductive assumption, there are extensions $\mathbb{Q} := F_0 \subseteq \cdots \subseteq F_n \subseteq \mathbb{C}$ where for all i in $[\![0; n-1]\!]$, $[F_{i+1} : F_i] = 2$ and such that F_n contains the real and imaginary parts of $\alpha_1, \alpha_2, \beta_1$ and β_2.

One has that the line ℓ_1 has an equation of the form $a_1x + b_1y = c_1$ and goes through α_1 and β_1, hence we have that a_1, b_1, c_1 lie in F_n. We have the same thing for a_2, b_2 and c_2.
Hence, the imaginary and real parts of α give the unique solution of the following equation :

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} a_1 & b_1 \\ a_2 & b_2 \end{pmatrix}^{-1} \begin{pmatrix} c_1 \\ c_2 \end{pmatrix}$$

It follows that the real and imaginary parts of α lie in F_n.

$*$ Next suppose that the last step in the construction of α was $P2$, the intersection of a line ℓ and a circle C.
Thus ℓ is the line constructed with $C1(\alpha_1, \beta_1)$, and C is the circle constructed with $C2(\gamma, \alpha_2, \beta_2)$.
The five points $\alpha_1, \beta_1, \alpha_2, \beta_2$ and γ come from earlier step in the construction. Hence we got thanks to the inductive assumptions the extensions : $\mathbb{Q} := F_0 \subseteq \cdots \subseteq F_n \subseteq \mathbb{C}$ where for all i in $[\![0; n-1]\!]$, $[F_{i+1} : F_i] = 2$ and such that F_n contains the real and imaginary parts of these five points.
As above, ℓ is given by an equation of the form $a_1x + b_1y = c_1$ and C is given by an equation of the form $x^2 + y^2 + a_2x + b_2y = 0$ with a_1, b_1, a_2, b_2 in F_n.
Now suppose that $a_1 \neq 0$.
Then by dividing by a_1 in the equation of ℓ, we have that $x + by = c$ where $b := \dfrac{b_1}{a_1}$ and $c := \dfrac{c_1}{a_1}$.
Substituting $x = -by + c$ into the equation of C gives the quadratic equation :

$$(-by + c)^2 + y^2 + a_2(-by + c) + c_2 = 0$$

By the quadratic formula, the values of y involve the square root of an expression in F_n. If this lies in F_n, then so do x and y. If not, then it lies in a quadratic extension $F_n \subseteq F_{n+1}$.
Then, x and y also lie in F_{n+1}, which shows that the real and imaginary parts of α lie in a quadratic extension of F_n.
Now, if $a_1 = 0$ then $y = \dfrac{c_1}{b_1}$ and we have the same result.

$*$ Finally, let us assume that the last step in the construction of α is $P3$, the intersection of two circles $C1$ and $C2$.
As above, we can find $\mathbb{Q} := F_0 \subseteq \cdots \subseteq F_n \subseteq \mathbb{C}$ where for all i in $[\![0; n-1]\!]$, $[F_{i+1} : F_i] = 2$ such that α is in F_n and the circles $C1$ and $C2$ are given by the equations :

$$\begin{cases} x^2 + y^2 + a_1x + b_1y + c_1 = 0 \\ x^2 + y^2 + a_2x + b_2y + c_2 = 0 \end{cases}$$

where all the coefficient lie in F_n.
Furthermore, we know that the real and imaginary parts of α give a solution of the previous system, then by subtracting the equations, we get :

$$(a_1 - a_2)x + (b_1 - b_2)y + (c_1 - c_2) = 0$$

Since the circles are distinct but not disjoint, we easily see that the coefficient of x and y in the last equation don't vanish simultaneously. Thus, this equation define a line and then, if we combine this equation with the first equation of the previous system, we are in the previous case of the intersection of a circle and a line.

So, the property is true for $N + 1$.
Finally, we have shown by induction that α is constructible.

Finally, we have shown the theorem by double implication

■

Corollary 1 :

If α is in $\mathcal{C}$, then there exists m in $\mathbb{N}$ such that $[\mathbb{Q}(\alpha):\mathbb{Q}] = 2^m$.

Proof :

Let us assume that α is in $\mathcal{C}$.
Then according to theorem 1, $\mathbb{Q} := F_0 \subseteq \cdots \subseteq F_n \subseteq \mathbb{C}$ where for all i in $[\![0; n-1]\!]$, $[F_{i+1}:F_i] = 2$ and α is in F_n.
Hence by the normal basis theorem :

$$[F_n:\mathbb{Q}] = \prod_{i=0}^{n-1} [F_{i+1}:F_i] = \prod_{i=0}^{n-1} 2 = 2^n$$

Moreover, as α is in F_n and $\mathbb{Q} \subseteq F_n$, we have $\mathbb{Q}(\alpha) \subseteq F_n$ and thus according to the normal basis theorem :

$$[F_n:\mathbb{Q}] = [F_n:\mathbb{Q}(\alpha)][\mathbb{Q}(\alpha):\mathbb{Q}]$$

So $[\mathbb{Q}(\alpha):\mathbb{Q}]$ divides $[F_n:\mathbb{Q}]$ which is equal to 2^n, then we can conclude that there exists m in $\mathbb{N}$ such that $[\mathbb{Q}(\alpha):\mathbb{Q}] = 2^m$.

■

Remarks :

- That implies that every α in $\mathcal{C}$ is algebraic over $\mathbb{Q}$ and the degree of its minimal polynomial over $\mathbb{Q}$ is a power of 2. So, we have the inclusions : $\mathbb{Q} \subsetneq \mathcal{C} \subsetneq \mathcal{A}$ (because $\sqrt{2}$ is in $\mathcal{C}$ but not in $\mathbb{Q}$ and π is in $\mathcal{A}$ but not in $\mathcal{C}$), where $\mathcal{A}$ algebraic numbers.

- The contraposition of corollary of theorem 2 is very useful because to see if a number is not constructible, it suffices to examine the degree of its minimal polynomial over $\mathbb{Q}$ (as we will see in example 6).

Corollary 2 :

$\mathcal{C}$ is the smallest subfield of $\mathbb{C}$ that is closed under the operation of taking square roots.

Proof :

By theorem 1, we know that α is in $\mathcal{C}$ implies that any square root of α is in $\mathcal{C}$, hence $\mathcal{C}$ is a subfield of $\mathbb{C}$ that is closed under the operation of taking square roots.

Let F be a subfield of $\mathbb{C}$ close under taking square roots.
Let us assume that α is in $\mathcal{C}$.
By theorem 2, we have $\mathbb{Q} := F_0 \subseteq \cdots \subseteq F_n \subseteq \mathbb{C}$ where for all i in $[\![0; n-1]\!]$, $[F_{i+1}:F_i] = 2$ and α is in F_n.
The first part of the proof of theorem 2 shows that $F_n \subseteq F$ and thus, α belongs to F. Hence, $\mathcal{C} \subseteq F$.

Finally, $\mathcal{C}$ is the smallest subfield of $\mathbb{C}$ that is closed under the operation of taking square roots.

■

Theorem 3 :

Let α in $\mathbb{C}$ be algebraic over $\mathbb{Q}$, and let $\mathbb{L}$ be the splitting field of the minimal polynomial of α over $\mathbb{Q}$.
α is constructible if, and only if, $[\mathbb{L}:\mathbb{Q}]$ is a power of 2.

Proof :

Let α in $\mathbb{C}$ be algebraic over $\mathbb{Q}$, and let $\mathbb{L}$ be the splitting field of the minimal polynomial of α over $\mathbb{Q}$.

- Let us assume that $[\mathbb{L} : \mathbb{Q}]$ is a power of 2.
  One has that $\mathbb{Q} \subseteq \mathbb{L}$ is a Galois extension, which means that $\text{Card}(\text{Gal}(\mathbb{L}/\mathbb{Q})) = [\mathbb{L} : \mathbb{Q}]$ is a power of 2.

  Let m in $\mathbb{N}$ such that $\text{Card}(\text{Gal}(\mathbb{L}/\mathbb{Q})) = 2^m$.
  Thanks to proposition 18 of chapter 2, $\text{Gal}(\mathbb{L}/\mathbb{Q})$ is solvable and according to theorem 9, we have the following subgroups :

  $$\{e_G\} := G_0 \subseteq G_1 \subseteq \cdots \subseteq G_{m-1} \subseteq G_m := \text{Gal}(\mathbb{L}/\mathbb{Q})$$

  such that each G_i is normal in G_{i+1} of index 2 (since $\text{Card}(\text{Gal}(\mathbb{L}/\mathbb{Q})) = 2^m$ and each quotient is cyclic of prime order).

  According to Galois's correspondence, it gives :

  $$\mathbb{Q} := \mathbb{L}_{G_m} \subseteq \cdots \subseteq \mathbb{L}_{G_0} := \mathbb{L}$$

  where for all i in $[\![0; m-1]\!]$, $[\mathbb{L}_{G_{m-i-1}} : \mathbb{L}_{G_{m-i}}] = 2$.
  By the theorem 2, we conclude that α in $\mathbb{L}$ is constructible.

- Let us assume that α is constructible.
  We will start by showing that $\mathbb{Q} \subseteq \mathcal{C}$ is a normal extension.
  Let P be the minimal polynomial of α over $\mathbb{Q}$.
  Since α is constructible, theorem 2 gives the following extensions :

  $$\mathbb{Q} := F_0 \subseteq \cdots \subseteq F_n \subseteq \mathbb{C}$$

  where for all i in $[\![0; n-1]\!]$, $[F_i : F_{i-1}] = 2$ and α is in F_n.

  Let $\mathbb{M}$ be the Galois closure of $\mathbb{Q} \subseteq F_n$.
  Since $\mathbb{C}$ is closed, we can easily assume that $\mathbb{M} \subseteq \mathbb{C}$. Moreover, P splits completely in $\mathbb{M}$, since $\mathbb{M}$ is normal over $\mathbb{Q}$, P is irreducible over $\mathbb{Q}$, and α is in $F_n \subseteq \mathbb{M}$ is a root of P.

  Let β in $\mathbb{M}$ be a roots of P.
  Thanks to Galois theory, there is a field isomorphism $\sigma : \mathbb{L} \longrightarrow \mathbb{L}$ that is the identity over $\mathbb{Q}$ such that $\sigma(\alpha) = \beta$ (with σ in $\text{Gal}(\mathbb{M}/\mathbb{Q})$).
  Applying σ to the fields $\mathbb{Q} := F_0 \subseteq \cdots \subseteq F_n \subseteq M$ gives us :

  $$\mathbb{Q} = \sigma(\mathbb{Q}) := \sigma(F_0) \subseteq \cdots \subseteq \sigma(F_n)$$

  such that for all i in $[\![0; n-1]\!]$, $[\sigma(F_i) : \sigma(F_{i-1})] = [F_i : F_{i-1}] = 2$.

  By theorem 2, $\beta = \sigma(\alpha)$ in $\sigma(F_n)$ is constructible. This shows that P splits completely over $\mathcal{C}$.

  It follows that $\mathcal{C}$ contains a splitting field $\mathbb{L}$ of P over $\mathbb{Q}$ and by the primitive element theorem, we have $\mathbb{L} = \mathbb{Q}(\gamma)$ for some γ in $\mathbb{L}$. Since γ is in $\mathcal{C}$, corollary 1 implies that $[\mathbb{Q}(\gamma) : \mathbb{Q}] := [\mathbb{L} : \mathbb{Q}]$ is a power of 2.

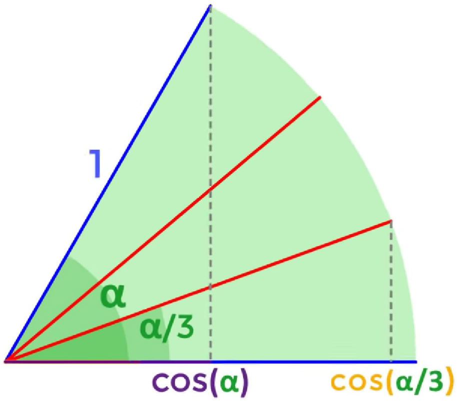
Finally, we have shown the theorem by double implication.

■

As we saw in the first section, many geometric constructions are possible with the non-graduated ruler and compass. However, not all of them are. Indeed, there are three major constructions known to the ancient Greeks that are not feasible with the non-graduated ruler and the compass :

Example 6 :

- Angle trisection :
  The problem of angle trisection is to divide a given angle into three equal angles (that is, to make its trisection).
  We consider a measurement angle α and try to construct a measurement angle $\frac{\alpha}{3}$. To do this, we can look at their cosine (in fact, if we know how to construct geometrically an angle, then we can construct its cosine):

  We have the following identity :

  $$\cos(\alpha) = 4\cos^3\left(\frac{\alpha}{3}\right) - 3\cos\left(\frac{\alpha}{3}\right)$$

  In other words, it is an equation of degree 3 which we do not know a priori to solve with the non-graduated ruler and the compass. This can be seen in an example:
  To get three angles of 20° from an angle of 60°, we have to "solve the equation" :

  $$\cos(60^\circ) = 4\cos^3(20^\circ) - 3\cos(20^\circ)$$

  So $X := \cos(20^\circ)$ checks the equation :

  $$4X^3 - 3X - \frac{1}{2} = 0$$

  Thus, X is a root of the polynomial $X^3 - \frac{3}{4}X - \frac{1}{8}$ and is its minimal polynomial. But the degree of this polynomial is not a power of 2, and so $\cos(20^\circ)$ is not a constructible number.
  Finally, it is impossible to trisect an angle of 60° and thus angle trisection is impossible.

- Doubling the cube :
  The problem of doubling the cube consists in constructing a cube with a volume twice that of a given cube using the non-graduated ruler and compass.
  We consider a cube of one unit per side. So its volume is 1 and we need to build a cube of volume 2. This cube must therefore have all its edges of length $\sqrt[3]{2}$. Is it a constructible number ?

To find out, we can apply the contraposition of corollary 1 :
A nullifying polynomial of $\sqrt[3]{2}$ is $X^3 - 2$ and it is its minimal polynomial. Now this polynomial is of degree 3, which is not a power of 2.
Thus, the number $\sqrt[3]{2}$ is not constructible with the non-graduated ruler and the compass and thus doubling the cube is impossible.

- Squaring the circle :
  This problem consists of constructing a square of the same area as a given disk using a non-graduated ruler and a compass.
  We consider a circle of radius 1. So its area is equal to π and we have to build a square of the same area. In other words, a square with all its sides of length $\sqrt{\pi}$.

  However, π is a transcendent number (demonstrated by Ferdinand von Lindemann in 1882 using the transcendence of e), so it is not algebraic over $\mathbb{Q}$ and thus not constructible.
  Thus, the number $\sqrt{\pi}$ is not constructible with the non-graduated ruler and the compass and thus the square of the circle is impossible.

III Construction of regular polygons

We will now develop the theory seen above to the construction of regular polygons with a non-graduated ruler and a compass. The main tool that will be used in this section is the cyclotomic extension $\mathbb{Q} \subseteq \mathbb{Q}(\zeta_n)$.

Definition 2 : Fermat number :

An odd prime p is called a **Fermat number**, when it can be written in the form :

$$p = 2^{2^n} + 1, \ n \in \mathbb{N}$$

Then the question becomes : when $F_n := 2^{2^n} + 1$ is a prime number ?
In 1640, Pierre de Fermat noticed that $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$ and $F_4 = 65537$ are all prime numbers. He conjectured that F_n is a prime number for all n in $\mathbb{N}$ but this was disproved by Euler in 1732. The only known Fermat prime numbers are those found by Fermat himself.

We can now characterize constructible regular n-gons as follows :

Theorem 4 : Gauss-Wantzel theorem :

Let n be a natural number greater than 2.

A regular n-gon can be constructed with a non-graduated ruler and a compass if, and only if, $n := 2^s \prod_{i=1}^{r} p_i$ (with s and r in $\mathbb{N}$) and $p_1, ..., p_r$ are r distinct Fermat prime numbers.

Proof :

Let us consider n a natural number greater than 2.
We can assume that a regular n-gon is constructible by non-graduated ruler and compass if, and only if, ζ_n is constructible.

One also has that $\mathbb{Q} \subseteq \mathbb{Q}(\zeta_n)$ is a Galois extension. By theorem 3, it follows that ζ_n is constructible if, and only if, $[\mathbb{Q}(\zeta_n) : \mathbb{Q}]$ is a power of 2, which means that $\varphi(n)$ is a power of 2 (where φ is the Euler's totient function).

- First, let us assume that $n := 2^s \prod_{i=1}^{r} p_i$ (with s and r in $\mathbb{N}$) and $p_1, ..., p_r$ are r distinct Fermat prime numbers.
  We have the following formula :

$$\varphi(n) = \begin{cases} \prod_{i=1}^{r} (p_i - 1) & \text{if } s = 0 \\ 2^{s-1} \prod_{i=1}^{r} (p_i - 1) & \text{if } s > 0 \end{cases}$$

  It follows that $\varphi(n)$ is a power of 2 since each p_i is a Fermat prime number. Hence, the regular n-gon is constructible.

- Let us assume that $\varphi(n)$ is a power of 2, and letthe factorization of n be $n = \prod_{i=1}^{s} q_i^{a_i}$, where $q_1, ..., q_s$ are distinct prime number and the exponents $a_1, ..., a_s$ are all greater of equal than 1. Then one has the following formula :

$$\varphi(n) = n \prod_{i=1}^{s} \left(1 - \frac{1}{q_i}\right) = \prod_{i=1}^{s} (q_i - 1) q_i^{a_i - 1}$$

  If q_i is odd, then we must have $a_i = 1$ since $\varphi(n)$ is a power of 2, and we also conclude that $q_i - 1$ must be a power of 2. However, if an odd prime p is of the form $2^k + 1$, then k must be a power of 2, that is to say, p is a Fermat prime number.

  Indeed, let us assume that there exists an odd number a and b a natural number such that $k := a2^b$.

  We denote $c := 2^{2^b}$.
  Then we have :

$$2^k + 1 = c^a + 1 = (c+1) \sum_{i=0}^{a-1} (-1)^i c^i$$

  It follows that $c + 1$ divides $2^k + 1$ and so, $c + 1 = 2^k + 1$ and $k = 2^b$.
  Hence, we have proven that the odd primes dividing n have exponent 1 and are Fermat prime numbers.

We have shown the theorem by double implication.

■

Example 7 :

- The hexacontahenagon (60-gon) is constructible since $60 = 2^2 \times 3 \times 5$.

- The tetracontadigon (42-gon) is not constructible since $42 = 2 \times 3 \times 7$ but 7 is not a Fermat prime number.

- Finally, there exist only 24 regular constructible n-gons which number of side is less or equal than 100.

Remark :

Thanks to theorem 4, we can affirm that all n-gon with n in $[\![3;10]\!]$ are constructible, except the heptagon (7-gon) and the nonagon (9-gon).

As example, we will construct a regular 5-gon :

Example 8 :

First of all, we will prove that :

$$\cos\left(\frac{2\pi}{5}\right)=\frac{\sqrt{5}-1}{4}$$

We have that $\cos\left(\frac{2\pi}{5}\right)=\mathrm{Re}(\zeta_5)$. Furthermore, ζ_5 and ζ_5^{-1} are conjugated, hence :

$$\begin{cases}\zeta_5+\zeta_5^{-1}=\alpha \quad \text{(with } \alpha \text{ in } \mathbb{R}) \\ \zeta_5\zeta_5^{-1}=1\end{cases}$$

Hence, ζ^5 is a root of $X^2-\alpha X+1$ in $\mathbb{Q}(\alpha)[X]$. Then, $\left[\mathbb{Q}\left(\zeta^5\right):\mathbb{Q}(\alpha)\right]=2$. Which means that $[\mathbb{Q}(\alpha):\mathbb{Q}]=2$. Furthermore, we have the following identity :

$$\zeta_5^4+\zeta_5^3+\zeta_5^2+\zeta_5+1=0$$

Dividing by ζ_5^2, we have :

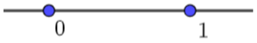
$$\zeta_5^2+\zeta_5^{-2}+\zeta_5+\zeta_5^{-1}+1=0$$

Since $\alpha^2=\zeta_5^2+\zeta_5^{-2}+2$, we have :

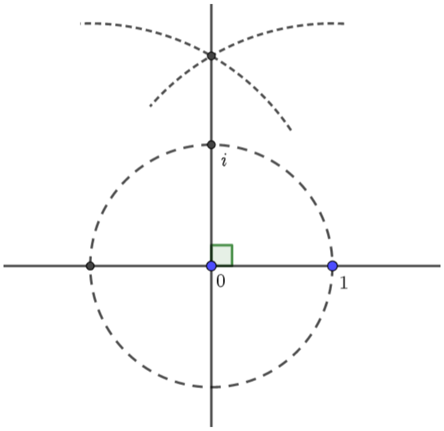
$$\alpha^2+\alpha-1=0$$

Hence, $\alpha=\frac{\sqrt{5}-1}{2}$ (since $\mathrm{Re}(\alpha)>0$).

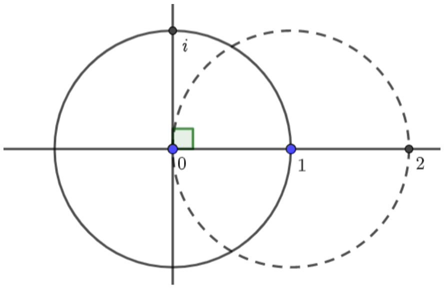
Now let's start the construction of the regular 5-gon :
We start with 0 and 1, and we draw the $\mathbb{R}$-axis.



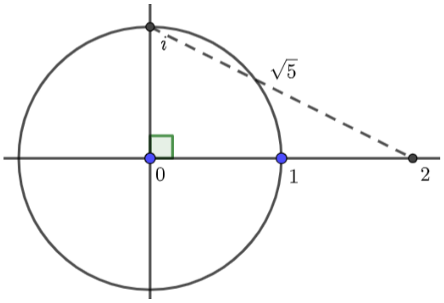
Then, we draw the line ℓ_1 going through 0 and perpendicular to the $\mathbb{R}$-axis and using $P2$ with ℓ_1 and the unit circle $C2(0,0,1)$, we construct i.



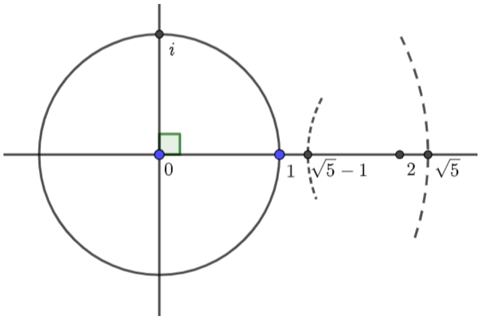
Now, we construct 2 using $P2$ with the $\mathbb{R}$-axis and $C2(1, 0, 1)$.



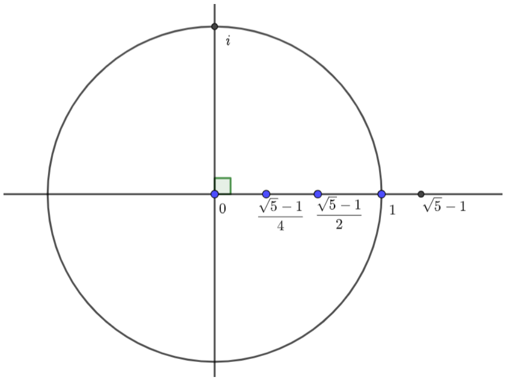
It follows that the length of the segment $[i, 2]$ is equal to $\sqrt{5}$ thanks to Pythagoras' theorem.



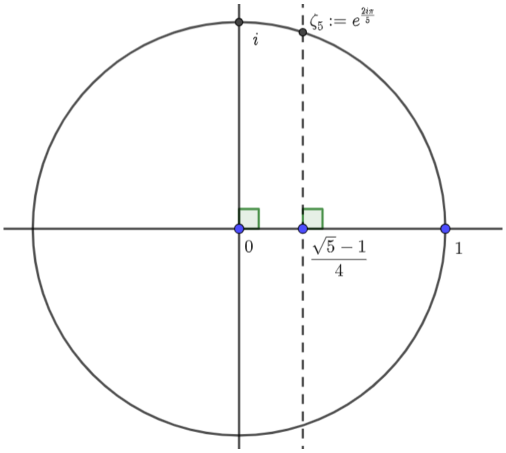
Using $P2$ with the $\mathbb{R}$-axis and $C2(0, i, 2)$, we construct $\sqrt{5}$. Then, using once again $P2$ with the $\mathbb{R}$-axis and $C2\left(\sqrt{5}, 0, 1\right)$ we construct the point $\sqrt{5} - 1$.



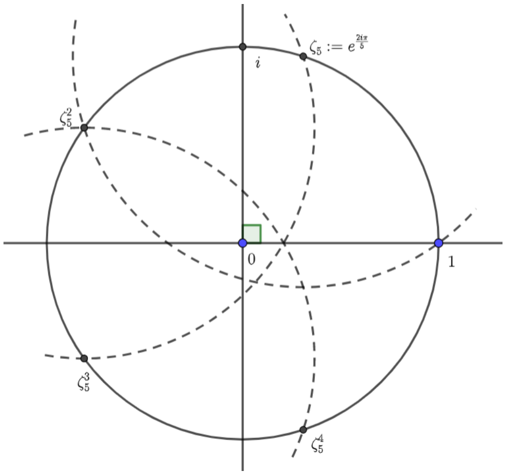
By constructing the middle of the segment $\left[0; \sqrt{5} - 1\right]$ as in example 2, and then the middle of the segment $\left[0; \dfrac{\sqrt{5} - 1}{2}\right]$, we construct $\alpha = \cos\left(\dfrac{2\pi}{5}\right) = \dfrac{\sqrt{5} - 1}{4}$.



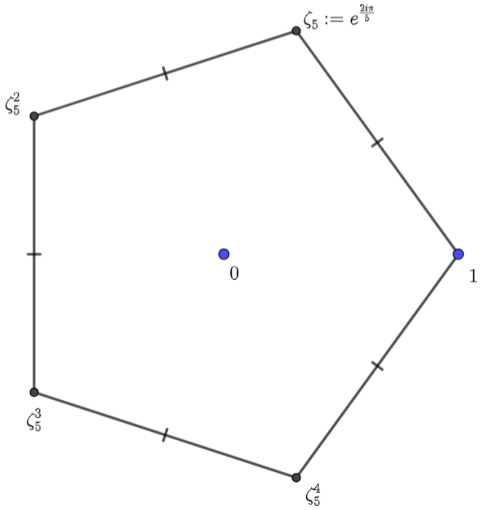
Now we draw the line going through α and perpendicular with the $\mathbb{R}$-axis as in example 1 and we construct the point ζ_5.



Hence, using $P3$ with the unit circle and $C2(\zeta_5, 1, \zeta_5)$ we are able to construct ζ_5^2. We repeat the process with the circles $C2(\zeta_5^2, 1, \zeta_5)$, $C2(\zeta_5^3, 1, \zeta_5)$, $C2(\zeta_5^4, 1, \zeta_5)$ to construct all the vertices of a regular 5-gon.



Finally, we just have to draw the segment connecting ζ_5^i with ζ_5^{i+1} with i in $[\![1;4]\!]$.



IV To go further...

So we have seen that with a non-graduated ruler and a compass it is possible to make elementary constructions (straights, circles, intersections, etc.), but also more complex constructions such as bisectors, middles, symmetrical points, etc. However, some constructions such as 9-gon, angle trisection, doubling the cube and the squaring of the circle are not possible. What if we modify the rules of the game by changing the tools we can use ?

- If we remove the non-graduated ruler from usable tools, keeping only the compass, then the answer is astonishing, but it does not change anything to the realizable constructions (except the actual tracing of the straight lines) ! It is indeed the Mohr-Mascheroni theorem :

  Theorem 5 : Mohr-Mascheroni theorem :

  Any geometric construction that can be performed by a compass and a non-graduated ruler can be performed by a compass alone (except the actual tracing of the straight lines).

  However, the construction steps are longer and more difficult, if only to trace the intersection of two straight lines !

- If we remove the compass this time to keep only the non-graduated ruler, then things are different ! Indeed, given base points, a point is constructible according to the non-graduated ruler when it is the point of intersection of two lines, each of these two lines passing through two points which are base points or points already constructed. And it is impossible with a non-graduated ruler alone to construct the middle of a segment and lead a parallel to a line through a point. However, the Poncelet-Steiner theorem allows us to find the usual Euclidean structure with an additional hypothesis :

  Theorem 6 : Poncelet-Steiner theorem :

  Whatever can be constructed by non-graduated ruler and compass together can be constructed by a non-graduated ruler alone, provided that a single circle and its centre are given.

  Thanks to this theorem, it is possible, for example, to make the parallel of a line passing through a given point constructible with the non-graduated ruler only.

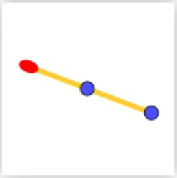
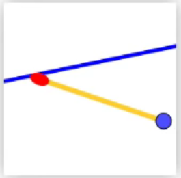
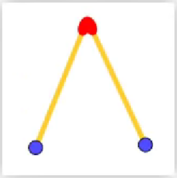
- We can also add tools : What is it possible to build with a graduated ruler with two graduations separated by a unit and a compass? The difference seems minimal, but the construction of a 9-gon, angle trisection and doubling the cube become feasible constructions ! However, squaring the circle is still inaccessible : the lengths that can be constructed with this new tool are still algebraic lengths...

- If we replace the non-graduated ruler and compass with an infinite collection of matches, then the basic constructions are quite different :

  ∗ If two points are close enough, then we can connect them with a match.

  ∗ If a point is close enough to a line, then we can place a match so that one end is on the point and the other end is on the straight.

  ∗ If two points are close enough, then an isosceles triangle can be constructed.

With these three basic operations, the constructible points are the same as with the non-graduated ruler and compass ! However, just to draw a square, you will need a lot of courage !

- Finally, we can get out of Euclid's geometry by using folds and origami. There are 7 fundamental folds in origami to create a straight line, a mediator, a perpendicular, etc. It is possible to construct by origami any constructible figure with the non-graduated ruler and the compass (because the axioms of Euclid's construction are verified with the 7 fundamental folds of origami). Then comes the following question: Is the geometry of origami strictly stronger than Euclidean geometry? The answer is affirmative because it is possible to construct a cubic root of a real number thanks to origami, which is not possible with the non-graduated ruler and the compass (the set of numbers constructible with the help of these 7 axioms is the smallest field containing the rational numbers and stable by the operations of calculating square root and cubic root). The angle trisection, doubling the cube and the 7-gon thus become realizable constructions with origami !

Chapter 4

Solution of general polynomial equations

The aim of this chapter is to use the Galois's correspondence to give a condition which must be satisfied by an equation solvable by radicals, namely : the associated Galois group must be a solvable group. We then construct a quintic polynomial whose Galois group is not solvable, which shows that quintic equation can not be solved by radicals. Solvability of the Galois group is also a sufficient condition for an equation to be solvable by radicals.

The first section aims to give a definition of radical extension and solvable polynomial equation by radicals which are very important for this chapter. The second section aims state and prove Abel-Ruffini theorem (which is the heart of this chapter). The third section is an application of both previous section by giving explicit formulae in degree 2,3 and 4. And finally, in a last section, we will talk about the inverse problem of Galois theory and more particularly Shafarevich's theorem.

For the whole chapter, we consider $\mathbb{K}$ a subfield of $\mathbb{C}$.

I Definitions and link with Galois theory

This first section aims to give the first definitions and some important properties which are very useful for the rest of this chapter.

It is with the help of Galois's correspondence and the results on the groups that Galois obtains a criterion of resolvability by radicals : "The novelty of this matter has demanded the use of new denominations, new characters", he says, adding further that his criterion has above all theoretical value because it is often insurmountable to calculate the Galois group of a particular polynomial : "In a word, calculations are impracticable". However, he points out, applications usually lead to "equations whose properties are known in advance..".

I.1 Radical extension

We need to formalise the idea of "solvability by radicals". We begin from the point of view of field extensions.

Definition 1 : Radical extension :

A field $\mathbb{L} \subseteq \mathbb{C}$ is called a **radical extension of** $\mathbb{K}$, when there exists an extension tower $(\mathbb{K}_i)_{i\in[\![0;r]\!]}$ (called **radical tower**) of extensions of $\mathbb{K}$ such that for all i in $[\![0; r-1]\!]$, $\mathbb{K}_{i+1}$ is an extension of $\mathbb{K}_i$ by a root of an element of $\mathbb{K}_i$ and $\mathbb{L} = \mathbb{K}_r$.

In other words :

$$\mathbb{K} := \mathbb{K}_0 \subseteq \mathbb{K}_1 \subseteq \cdots \subseteq \mathbb{K}_i := \mathbb{K}(a_1, ..., a_i) \subseteq \cdots \subseteq \mathbb{K}_r := \mathbb{K}(a_1, ..., a_r) = \mathbb{L}$$

where, for all i in $[\![1; r]\!]$, there exists n_i in $\mathbb{N}$ such that $a_i^{n_i}$ is in $\mathbb{K}_{i-1}$.

Remark :
The element a_i are said to from a **radical sequence** for $\mathbb{L}$.

Example 1 :

$\sqrt[12]{\sqrt[3]{1+i\sqrt[5]{7}}+i\sqrt{5}}$ belongs to a radical extension of $\mathbb{Q}$ (in fact, 360 complex numbers are defined by this formula !).

Informally, a radical extension is obtained by a sequence of adjunctions of n^{th} roots, for various n. For example, the radical expression :

$$\sqrt[3]{11}\sqrt[5]{\frac{7+\sqrt{3}}{2}}+\sqrt[4]{1+\sqrt[3]{4}}$$

is contained in a radical extension $\mathbb{Q}(\alpha,\beta,\gamma,\delta,\varepsilon)$ of $\mathbb{Q}$, where :

$$\alpha^3=11,\ \beta^2=3,\ \gamma^5=\frac{7+\beta}{2},\ \delta^3=4 \text{ and } \varepsilon^4=1+\delta$$

it is clear that any radical expression, in the sense of the introduction of this chapter, is contained in some radical extension.

A polynomial should be solvable by radicals provided all of its zeros are radical expressions over the ground field.

I.2 Solvable polynomial equations by radicals

This second subsection aims to define a solvable polynomial equation by radicals and a construction of a suitable radical extension.

I.2.1 Introduction to the problem

Definition 2 : Polynomial solvable by radicals on a field :

A polynomial P in $\mathbb{K}[X]$ is **solvable by radicals on** $\mathbb{K}$ (of characteristic zero), when there is a radical extension $\mathbb{L}$ of $\mathbb{K}$ containing the splitting field $\mathbb{N}$ of P.

There are several points to be made about this definition :

- The first is the restriction to characteristic zero : for technical reasons it is customary to use a slightly wider definition of solvability by radicals when fields of characteristic $p>0$ are under consideration. To keep our treatment simple we shall assume characteristic zero throughout this chapter.

- The second is to emphasize that $\mathbb{N}$ need not itself to be radical. We want everything in the splitting field to be expressible by radicals, but it is pointless to expect everything expressible by the same radicals to be inside the slitting field. If the extension $\mathbb{M}$ over $\mathbb{K}$ is radical and $\mathbb{L}$ is an intermediate field between $\mathbb{M}$ and $\mathbb{K}$, then $\mathbb{L}$ need not be radical.

- The third is that we require all zeros of P to be expressible by radicals. It is possible for some zeros to be expressible by radicals, whilst others are not (take a product of two polynomials, one solvable by radicals and one not). However, if an irreducible polynomial P has one zero expressible by radicals, then all zeros must be.

All elements of $\mathbb{L}$ may be expressed by radicals, but $\mathbb{L}$ may contain strictly $\mathbb{N}$. We demand that all the roots of P be in $\mathbb{L}$, and in the case of an irreducible polynomial on $\mathbb{K}$, we can show that it is equivalent to demand that a root of P be in $\mathbb{L}$.

We will show that if P is in $\mathbb{K}[X]$ is solvable by radicals on $\mathbb{K}$, of splitting field $\mathbb{N}$ on $\mathbb{K}$, $\text{Gal}(\mathbb{N}/\mathbb{K})$ is a solvable group. For this, we must first construct a suitable radical extension of $\mathbb{K}$ (and then show the reciprocity).

I.2.2 First construction

Let us consider a radical extension $\mathbb{L}$ of $\mathbb{K}$ containing $\mathbb{N}$, defined by a radical tower $T = (K_i)_{i \in [\![0;r]\!]}$ with the notations of the previous subsection.

Let us defined the tower $T' := (\mathbb{K}'_i)_{i \in [\![0;r+1]\!]}$ by $\mathbb{K}'_0 := \mathbb{K}$, $\mathbb{K}'_1 := \mathbb{K}(\zeta)$, where ζ is a n^{th} root of unity (with $n = \text{PPCM}(\{n_i,\ i \in [\![1;r]\!]\})$) and for all i in $[\![1;r]\!]$, $\mathbb{K}'_{i+1} := \mathbb{K}(\zeta, a_1, ..., a_i)$.

In this case, for all i in $[\![0;r]\!]$, $\mathbb{K}'_{i+1}$ is a normal extension of $\mathbb{K}'_i$, but we do not know if $\mathbb{L}' := \mathbb{K}'_{r+1}$ is a normal extension of $\mathbb{K}$ (for example, the radical tower $\mathbb{Q} \subseteq \mathbb{Q}\left(\sqrt{2}\right) \subseteq \mathbb{Q}\left(\sqrt[4]{2}\right)$ is not in this case).

Let us show that we can define a tower T'' further verifying this property.

I.2.3 Second construction

We denote P_i the minimal polynomial of a_i on $\mathbb{K}$ for all i in $[\![1;r]\!]$ and A_i the set of the conjugates in $\mathbb{C}$ of a_i on $\mathbb{K}$.

The extension $L'' := \mathbb{K}(\zeta, A_1, ..., A_r)$ is a normal extension of $\mathbb{K}$ (being the splitting field of $(X^n - 1)\displaystyle\prod_{i=1}^{r} P_i$). Let us show that it is again a radical extension of $\mathbb{K}$ and with the same shape that T' :

We just have to show that, for all i in $[\![1;r]\!]$ and for all a in A_i, a^{n_i} is in $\mathbb{K}\left(\zeta, \displaystyle\bigcup_{j<i} A_j\right)$:
Since a is a conjugate of a_i, there exists a $\mathbb{K}$-homomorphism $\sigma : \mathbb{K}(a_i) \longrightarrow \mathbb{C}$ such that $\sigma(a_i) = a$, and we can extend σ to a $\mathbb{K}$-homomorphism $\sigma' : \mathbb{K}\left(\zeta, \displaystyle\bigcup_{j\leq i} A_j\right) \longrightarrow \mathbb{C}$ such that $\sigma'(a_i) = a$.

Since $\mathbb{K}\left(\zeta, \displaystyle\bigcup_{j<i} A_j\right)$ is a normal extension of $\mathbb{K}$, being the splitting field of $(X^n - 1)\displaystyle\prod_{j=1}^{i-1} P_j$, and that $a_i^{n_i}$ belongs to its, the same is true for a^{n_i} which is conjugated to it since $a^{n_i} = (\sigma'(a_i))^{n_i} = \sigma'\left(a_i^{n_i}\right)$.

We will notice that we can refine the tower $\left(\mathbb{K}\left(\zeta, \displaystyle\bigcup_{j\leq i} A_j\right)\right)_{i \in [\![1;r]\!]}$ so that successive extensions are abelian (such as $K(\zeta)$ over $\mathbb{K}$) or cyclic (such as extensions by each conjugate of a_i).

I.3 Link between solvable groups and Galois theory

We now are able to see a first link between solvable groups and Galois theory with first some properties and then some examples and Galois's theorem.

Theorem 1 :

Let P in $\mathbb{K}[X]$ and $\mathbb{N}$ its splitting field.
If P is solvable by radicals, then $\text{Gal}(\mathbb{N}/\mathbb{K})$ is a solvable group.

Proof :

Let us consider P in $\mathbb{K}[X]$ and $\mathbb{N}$ its splitting field.
Let us assume that P is solvable by radicals.
According to the previous construction, there exists a radical extension $\mathbb{L}$ of $\mathbb{K}$ containing $\mathbb{N}$, defined by a radical tower $(K_i)_{i\in\llbracket 0;s\rrbracket}$ such that $\mathbb{K} := \mathbb{K}_0$, $\mathbb{K}_1 := \mathbb{K}(\zeta)$ an abelian extension of $\mathbb{K}$ and for all i in $\llbracket 1; s-1\rrbracket$, $\mathbb{K}_{i+1} := \mathbb{K}_i(x_i)$ a cyclic extension of $\mathbb{K}_i$ (where $x_i^{n_i}$ is in $\mathbb{K}_i$, ζ a primitive n^{th} root of unity, $n := \mathrm{PPCM}(n_1, ..., n_{s-1})$ and $\mathbb{L} := \mathbb{K}_s$ a normal extension of $\mathbb{K}$.

For all i in $\llbracket 0; s\rrbracket$, let us consider $G_i := \mathrm{Gal}(\mathbb{L}/\mathbb{K}_{s-i})$.
The sequence $(G_i)_{i\in\llbracket 0;s\rrbracket}$ verifies the conditions of definition 1 of chapter 1.
Indeed :

- By definition of G_i, $G_i \subseteq G_{i+1}$.
- By definition of G_i, G_i is a normal subgroup of G_{i+1}.
- $G_{i+1}/G_i \cong \mathrm{Gal}(\mathbb{K}_{s-i}/\mathbb{K}_{s-i-1})$ is abelian.

Hence, $\mathrm{Gal}(\mathbb{L}/\mathbb{K})$ is solvable.

So, according to proposition 2 of chapter 1, $\mathrm{Gal}(\mathbb{N}/\mathbb{K})$ is a solvable group (as a quotient of $\mathrm{Gal}(\mathbb{L}/\mathbb{K})$).

■

Thus, to find a polynomial not solvable by radicals it suffices to find one whose Galois groups is not solvable. There are two main ways of going this :

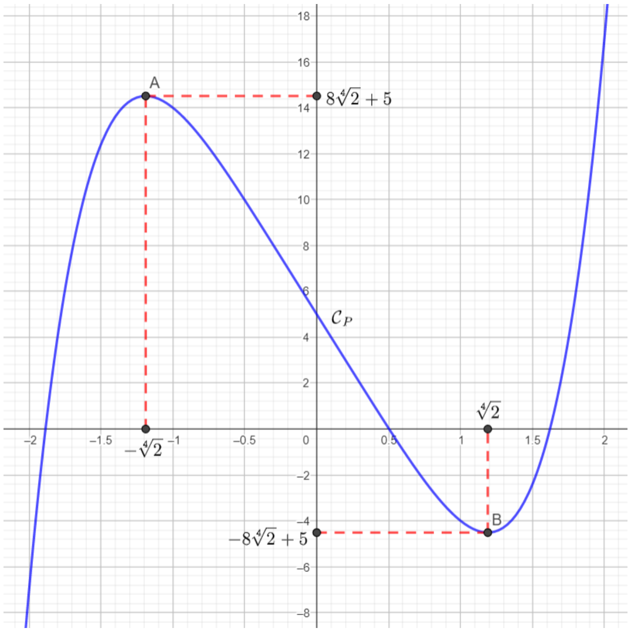
- One is to look at the so-called "general polynomial of degree n", but this has the disadvantage that it does not show that there are polynomials with rational coefficients which are not solvable by radicals.
- The alternative approach, which we shall adopt here, is to exhibit a specific polynomial with rational coefficients whose Galois group is not solvable. Since Galois groups are hard to calculate a little low cunning is necessary, together with knowledge of the symmetric group. We must also have recourse to the fundamental theorem of algebra.

Example 2 :

The polynomial $P := X^5 - 10X + 5$ in $\mathbb{Z}[X]$ is not solvable by radicals.
According to proposition 1, we just have to determine its Galois group and show that it is not solvable.

Let us consider $\mathbb{N}$ the splitting body of P in $\mathbb{C}$ and we denote $G := \mathrm{Gal}(\mathbb{N}/\mathbb{Q})$.
According to Eisenstein's criterion (with $p = 5$), P is irreducible over $\mathbb{Q}$. Moreover, there is three real roots and two conjugates complex roots denotes a and b.
Indeed, according to the study of the variations of P, we have the following variation table :

x	$-\infty$		$-\sqrt[4]{2}$		$\sqrt[4]{2}$		$+\infty$
$f'(x)$		$+$	0	$-$	0	$+$	
$f(x)$	$-\infty$	↗	$8\sqrt[4]{2}+5$	↘	$-8\sqrt[4]{2}+5$	↗	$+\infty$



Moreover, by the intermediate value theorem and Rolle's theorem, there exist exactly three real roots of the equation $P(X) = 0$ (one in $]-\infty; -\sqrt[4]{2}[$, another in $]-\sqrt[4]{2}; \sqrt[4]{2}[$ and the last in $]\sqrt[4]{2}; +\infty[$).
Finally, by the fundamental theorem of algebra, the equation $P(X) = 0$ admits 5 complex roots, and thus 2 non-real roots (who are conjugates because P has real coefficients).

The conjugacy of $\mathbb{C}$ induce an element of G exchanging a and b and fixing the three others roots of P. As $\text{Card}(G) = [\mathbb{N} : \mathbb{Q}] = [\mathbb{N} : \mathbb{Q}(a)][\mathbb{Q}(a) : \mathbb{Q}] = 5 \times [\mathbb{N} : \mathbb{Q}(a)]$, the group G has an order multiple of 5. Which implies, according to Cauchy's theorem, the existence of an element σ of order 5 of G.
Hence, G could be identify to a subgroup of $\mathfrak{S}_5$ containing a transposition and a 5-cycle. Finally, we can conclude that $G \cong \mathfrak{S}_5$.

Thus, G is isomorphic to $\mathfrak{S}_5$, and thus, G is not solvable and then P is not solvable by radicals.

We will now give a proposition how is useful to determine the Galois group of a certain class of polynomials :

Proposition 1 :

Let p be a prime number and P be an irreducible polynomial of degree p over $\mathbb{Q}$.
If P has precisely two non-real zeros in $\mathbb{C}$, then the Galois group of P over $\mathbb{Q}$ is the symmetric group $\mathfrak{S}_p$.

Proof :

Let us consider p a prime number and P an irreducible polynomial of degree p over $\mathbb{Q}$.
Let us assume that P has precisely two non-real zeros in $\mathbb{C}$.
By the fundamental theorem of algebra, $\mathbb{C}$ contains a splitting field $\mathbb{N}$ of P.
Let G the Galois group of P over $\mathbb{Q}$, considered as a permutation group on the zeros of P. These are distinct since the characteristic is zero, so that G is a subgroup of $\mathfrak{S}_p$.

When we construct a splitting field for P, we first adjoin an element of degree p, so that $[\mathbb{N} : \mathbb{Q}]$ is divisible by p. So, p also divides the order of G. By Cauchy's theorem, G has an element of order p. But the only elements of $\mathfrak{S}_p$ having order p are the p-cycles.

Complex conjugation is a $\mathbb{Q}$-automorphism of $\mathbb{C}$, and therefore induces a $\mathbb{Q}$-automorphism of $\mathbb{N}$. This leaves the $p-2$ real zeros of P fixed, while transposing the 2 non-real zeros. Therefore, G contains a 2-cycle.
By choice of notation, and if necessary taking a power of the p-cycle, we may assume that G contains the 2-cycle $(1\ 2)$ and the p-cycle $(1\ 2\ ...\ p)$. But these generate the whole of $\mathfrak{S}_p$, hence $\mathfrak{S}_p$ is included in G.

Hence, we have shown by double inclusion that $G = \mathfrak{S}_p$.

■

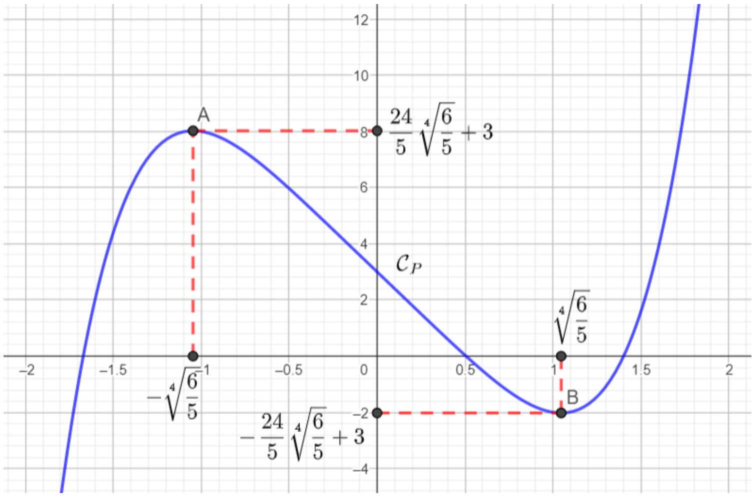
This criterion is very useful because we don't have to determine Galois group of a polynomial (which is very convenient !) in a certain class of polynomials. Let us give an example of application :

Example 3 :

The polynomial $P := X^5 - 6X + 3$ on $\mathbb{Q}$ is not solvable by radicals.
First, P is a polynomial a prime degree and P is irreducible over $\mathbb{Q}$ according to Eisenstein's criterion (with $p = 3$).

Secondly, let us study variations of P :

x	$-\infty$		$-\sqrt[4]{\frac{6}{5}}$		$\sqrt[4]{\frac{6}{5}}$		$+\infty$
$f'(x)$		$+$	0	$-$	0	$+$	
$f(x)$	$-\infty$	↗	$\frac{24}{5}\sqrt[4]{\frac{6}{5}}+3$	↘	$-\frac{24}{5}\sqrt[4]{\frac{6}{5}}+3$	↗	$+\infty$



Moreover, by the intermediate value theorem and Rolle's theorem, there exist exactly three real roots of the equation $P(X) = 0$.
Finally, by the fundamental theorem of algebra, the equation $P(X) = 0$ admits 5 complex roots, and thus exactly 2 non-real roots.

To conclude, according to proposition 2, we can affirm that Galois group of P over $\mathbb{Q}$ is $\mathfrak{S}_5$, and then P is not solvable by radicals (according to theorem 1).

Of course this is not the end of the story. There are more ways to killing a quintic than choking it with radicals. Having established the inadequacy of radicals for solving the problem, it is natural to look further afield.

On a mundane level, numerical methods can be used to find the zeros (real or complex) to any required degree of accuracy. This is a useful practical method (indeed the only practical method). The mathematical theory of such numerical methods can be far from mundane (but from the algebraic point of view it is unilluminating).

Another way of solving the problem is to say, in effect, "What is so special about radicals ?". Suppose for any real number a we define the **ultraradical** $\sqrt[*]{a}$ to be the real zero of $X^5 + X + a$. It was shown that the quintic equation can be solved by the use of radicals and ultraradicals.

Instead of inventing new tools we can refashion existing ones, Hermite made the remarkable discovery that the quintic equation can be solved in therms of elliptic modular functions, specials functions of classical mathematics which arose in a quite different context (integration of algebraic functions). The method is analogous to the well-known trigonometric solution of the cubic equation. In a triumph of mathematical unification Klein succeeded in connecting together the quintic equation, elliptic functions, and the rotation group of the regular icosahedron. The latter is isomorphic to the alternating group $\mathfrak{A}_5$ which we have seen plays a key part in the theory of the quintic equation. Klein's work helped to explain the unexpected appearance of elliptic functions in the theory of polynomial equations. These ideas were subsequently generalized by Poincaré to cover polynomials of arbitrary degree.

Theorem 2 : Galois's theorem :

Let P in $\mathbb{K}[X]$, $\mathbb{N}$ its splitting field and $G := \mathrm{Gal}(\mathbb{N}/\mathbb{K})$.
Let us assume that $\mathbb{K}$ contains a primitive n^{th} root of unity with $n := [\mathbb{N} : \mathbb{K}] = \mathrm{Card}(G)$.
If G is solvable, then P is solvable by radicals on $\mathbb{K}$.

Proof :

Let us consider P in $\mathbb{K}[X]$, $\mathbb{N}$ its splitting field and $G := \mathrm{Gal}(\mathbb{N}/\mathbb{K})$.
Let us assume that $\mathbb{K}$ contains a primitive n^{th} root of unity with $n := [\mathbb{N} : \mathbb{K}] = \mathrm{Card}(G)$ and that G is solvable.
According to theorem 9 of chapter 2, there exist a sequence $(G_i)_{i\in[\![0;r]\!]}$

$$\{e_G\} := G_0 \subseteq G_1 \subseteq \cdots \subseteq G_r := G$$

such that :

- For all i in $[\![0;r-1]\!]$, G_i is a normal subgroup of G_{i+1}.
- For all i in $[\![0;r-1]\!]$, G_{i+1}/G_i is a cyclic group of prime order.

Let us consider, for all i in $[\![0;r]\!]$, $K_i := I(G_i)$, where $I : \mathcal{G} \longrightarrow \mathcal{E}$ is the application who associates to a subgroup H of $\mathrm{Gal}(\mathbb{N}/\mathbb{K})$ the field of invariants $I(H)$.
We have $\mathbb{K}_0 := \mathbb{K}$ and for all i in $[\![0;r-1]\!]$:

$$\mathrm{Gal}(\mathbb{K}_i/\mathbb{K}_{i+1}) \cong \mathrm{Gal}(\mathbb{N}/\mathbb{K}_{i+1})/\,\mathrm{Gal}(\mathbb{N}/\mathbb{K}_i) \cong G_{i+1}/G_i$$

So, $\mathrm{Gal}(\mathbb{K}_i/\mathbb{K}_{i+1})$ is cyclic of prime order p_i and thus, there exists a_i in $\mathbb{K}_i$ such that $(a_i)^{p_i}$ is in $\mathbb{K}_{i+1}$ and $\mathbb{K}_i = \mathbb{K}_{i+1}(a_i)$.

By reversing the tower $(\mathbb{K}_i)_{i\in[\![0;r]\!]}$, we construct a radical extension of $\mathbb{K}$ containing the splitting field $\mathbb{N}$ of P and thus, P is solvable by radicals on $\mathbb{K}$ (according to definition 2).

■

II General polynomial of degree n

In this second section, we finally study the general polynomial of degree n and the famous Abel-Ruffini theorem.

The so called "general" polynomial is in fact a very special polynomial. It is one whose coefficients do not satisfy any algebraic relations. This property makes it simpler to work with than, say, polynomials over $\mathbb{Q}$, and in particular it is easier to calculate its Galois group. As a result, we can show that the general quintic polynomial is not solvable by radicals without assuming as much group theory as we did previously in this chapter. Effectively this implies that there is no general formula by which all quintic equations can be solved in therms of radicals. Since this does not a priori preclude the possibility that there might exist solutions by radicals of all quintic polynomials which can not be subsumed under a general formula, the results of this section are not as strong as those of the precedent section.

It transpires that the Galois group of the general polynomial of degree n is the whole symmetric group $\mathfrak{S}_n$. This immediately shows the insolubility of the general quintic. Our knowledge of the structure of $\mathfrak{S}_2$, $\mathfrak{S}_3$ and $\mathfrak{S}_4$ can be used to find methods of solving the general quadratic, cubic or quartic equation (as we will see in the next section).

II.1 Algebraically independent elements

First of all, we have to define the notion of algebraically independent elements.

Definition 3 : Algebraically independent elements on a field :

We consider $\mathbb{L}$ an extension of $\mathbb{K}$.
Elements $x_1, ..., x_n$ of $\mathbb{L}$ are called **algebraically independent elements on** $\mathbb{K}$, when the homomorphism $f : \mathbb{K}[X_1, ..., X_n] \longrightarrow \mathbb{L}$ such that $f|_{\mathbb{K}}$ is the inclusion of $\mathbb{K}$ in $\mathbb{L}$ and that for all i in $[\![1;n]\!]$, $f(X_i) = x_i$ is injective.

Remark :
In other words, there is no polynomial P different from $0_{\mathbb{K}[X_1,...,X_n]}$ such that $P(x_1, ..., x_n) = 0$.

Proposition 2 :

For all integer n in $\mathbb{N}^*$, there exists n algebraically independent complex numbers on $\mathbb{Q}$.

Proof :

Let us consider n an integer in $\mathbb{N}^*$.
Let us begin on $\mathbb{Q}$:
$\mathbb{Q}$ is a countable set. So, its algebraic closure $C(\mathbb{Q})$ in $\mathbb{C}$ is also a countable set, then its complementary is not empty : so we choose x_1 on it.

The extension of $C(\mathbb{Q})$ by x_1 is also a countable set, then its algebraic closure $C(C(\mathbb{Q})(x_1))$ in $\mathbb{C}$ is also a countable set then its complementary is not empty : so we choose x_2 on it.

By the same way, we can choose $x_3, x_4, ..., x_n$.
Thus, for all integer n in $\mathbb{N}^*$, there exists n algebraically independent complex numbers on $\mathbb{Q}$.

■

II.2 Galois group of a general polynomial of degree n

Let us consider $x_1, ..., x_n$ algebraically independent elements on $\mathbb{Q}$, $\mathbb{N} := \mathbb{Q}(x_1, ..., x_n)$ the generated by these elements and P the monic polynomial defined by :

$$P := \prod_{i=1}^{n} (X - x_i)$$

The polynomial equation $P(X) = 0$ is called **general polynomial of degree n over $\mathbb{Q}$**, and we denote :

$$P := X^n + \sum_{k=0}^{n-1} a_k X^k \text{ and } \mathbb{K} := \mathbb{Q}\left(a_0, ..., a_{n-1}\right)$$

Proposition 3 :

The Galois group $\mathrm{Gal}(\mathbb{N}/\mathbb{K})$ of a general polynomial of degree n is isomorphic to $\mathfrak{S}_n$.

Proof :

Any permutation s of $[\![1; n]\!]$ induces a $\mathbb{Q}$-automorphism σ of $\mathbb{N}$ defined by :

$$\forall i \in [\![1; n]\!], \;\; \sigma(x_i) = x_{\sigma(i)}$$

Hence, we can consider $\mathfrak{S}_n$ as a group of $\mathbb{Q}$-automorphisms of $\mathbb{N}$.

Let us consider $\mathbb{L} = I(\mathfrak{S}_\mathbf{n})$, where $I : \mathcal{G} \longrightarrow \mathcal{E}$ is the application who associates to a subgroup H of $\mathrm{Gal}(\mathbb{N}/\mathbb{K})$ the field of invariants $I(H)$.
According to Artin's theorem, $[\mathbb{N} : \mathbb{L}] = n!$. Moreover, as for all k in $[\![0; n]\!]$, a_k is in $\mathbb{L}$, we have $\mathbb{K} \subseteq \mathbb{L}$, and thus (as $\mathbb{N}$ is the splitting field of P over $\mathbb{K}$) $[\mathbb{N} : \mathbb{K}] \leq n!$.

Finally, we have $\mathbb{L} = \mathbb{K}$ and so $\mathrm{Gal}(\mathbb{N} : \mathbb{K}) = \mathrm{Gal}(\mathbb{N} : \mathbb{L}) \cong \mathfrak{S}_n$.

■

Theorem 3 : Abel–Ruffini theorem :

If $n \geq 5$, then a general polynomial of degree n is not solvable by radicals.

Proof :

Let us consider P a general polynomial of degree n.
Let us assume that $n \geq 5$.
According to proposition 3, the Galois group of P is isomorphic to $\mathfrak{S}_n$. Moreover, according to corollary 6 of chapter 2, $\mathfrak{S}_n$ is not solvable.

Finally, according to theorem 1, we can conclude that P is not solvable by radicals.

■

Remark :
This impossibility has already been proved by Ruffini in 1799 but his very long proof had not convinces his contemporaries, even after the modifications and simplifications of his proof.

Example 4 :

- The polynomial $X^5 - 4X + 2$ is not solvable by radicals (because its Galois group is $\mathfrak{S}_5$).
- $\Phi_7 := X^6 + X^5 + X^4 + X^3 + X^2 + X + 1$ is solvable by radicals (because its Galois group is $\mathbb{Z}/6\mathbb{Z}$).

III Explicit formulae for roots in degree 1,2,3 and 4

In this section, we give the explicit formulae in degree 1,2,3 and 4 and their demonstration.

The general polynomial of degree n has Galois group $\mathfrak{S}_n$, and we know that for $n \geq 4$, $\mathfrak{S}_n$ is solvable. Hence, theorem 2 implies that the general polynomial of degree $n \leq 4$ can be solved by radicals. The objective is to use the Galois group to find formulae for solutions of general polynomial of degree $n \geq 4$.

III.1 Linear and quadratic equations

First we consider the familiar cases of linear and quadratic equations.

Let us consider a linear equation : $X - s_1 = 0$.
Trivially, $t_1 = s_1$ is the solution (the only one according to the fundamental theorem of algebra) of this equation. Here, the Galois group is trivial, and adds little to the discussion except to confirm that the zero must lie in $\mathbb{K}$.

Let us consider a quadratic equation : $X^2 - s_1X + s_2 = 0$.
Let t_1 and t_2 be the solutions of this equation.
The Galois group $\mathfrak{S}_2$ consists of the identity and an application interchanging t_1 and t_2. Hence, $(t_1 - t_2)^2$ is fixed by $\mathfrak{S}_2$, so lies $\mathbb{K}(s_1, s_2)$.
Moreover, we have :

$$(t_1 - t_2)^2 = t_1^2 - 2t_1t_2 + t_2^2 = (s_1t_1 - s_2) - 2s_2 + (s_1t_2 - s_2) = s_1(t_1 + t_2) - 4s_2 = s_1^2 - 4s_2$$

Hence :

$$\begin{cases} t_1 - t_2 = & \pm\sqrt{s_1^2 - 4s_2} \\ t_1 + t_2 = & s_1 \end{cases}$$

Thus, we have the familiar relation :

$$t_1, t_2 \in \left\{ \frac{s_1 - \sqrt{s_1^2 - 4s_2}}{2} ; \frac{s_1 + \sqrt{s_1^2 - 4s_2}}{2} \right\}$$

III.2 Cubic equations

To give general solutions of cubic (and quartic equations), we will use Tschirnhaus' transformation. The Tschirnhaus' method, conceived and developed by Ehrenfried Walther von Tschirnhaus, is an attempt to solve the key point of equation theory, namely to find a general method for solving the polynomial equation. This method attempts to reduce the equation we want to solve to other equations of a lower degree. This method certainly fails for equations of degree greater than or equal to five that have an unsolvable Galois group.

Let us consider a cubic equation : $X^3 - s_1X^2 + s_2X - s_3 = 0$.
Let t_1, t_2 and t_3 be the solutions of this equation.
The Galois group $\mathfrak{S}_3$ has a series :

$$\{\mathrm{Id}_{[\![1;3]\!]}\} \lhd \mathfrak{A}_3 \lhd \mathfrak{S}_3$$

with abelian quotients.

Adjoin an element $j \neq 1$ such that $j^3 = 1$ and consider :

$$y := t_1 + jt_2 + j^2 t_3$$

An element of $\mathfrak{A}_3$ permute t_1, t_2 and t_3 cyclically, and therefore multiply y by a power of j. Hence y^3 is fixed by $\mathfrak{A}_3$. Similarly, if :

$$z := t_1 + j^2 t_2 + jt_3$$

then z^3 is fixed by $\mathfrak{A}_3$.

Now, any odd permutation in $\mathfrak{S}_3$ interchanges y^3 and z^3, so that $y^3 + z^3$ and $y^3 z^3$ are fixed by the whole of $\mathfrak{S}_3$, hence lie in $\mathbb{K}(s_1, s_2, s_3)$.

Moreover, by the Tschirnhaus' transformation $U := X - \frac{1}{3}s_1$, the general cubic polynomial takes the form $U^3 + pU + q$.
If we can find the zeros of this it is an easy matter to find them for the general cubic. Following the above procedure for this polynomial, we have explicitly :

$$y^3 + z^3 = -27q \text{ and } y^3 z^3 = -27p^3$$

from which it follows that y^3 and z^3 are the zeros of the quadratic polynomial $X^2 + 27qX - 27p^3$.

So, according to the previous subpart, we have :

$$\begin{aligned} y^3, z^3 &\in \left\{ \frac{-27q - \sqrt{(27q)^2 + 4 \times 27p^3}}{2} ; \frac{-27q + \sqrt{(27q)^2 + 4 \times 27p^3}}{2} \right\} \\ &= \left\{ 27\left(-\frac{q}{2} + \sqrt{\left(\frac{p}{3}\right)^3 + \left(\frac{p}{2}\right)^2} \right) ; 27\left(-\frac{q}{2} - \sqrt{\left(\frac{p}{3}\right)^3 + \left(\frac{p}{2}\right)^2} \right) \right\} \end{aligned}$$

Taking cube roots we know y and z. But since $s_1 = t_1 + t_2 + t_3$, it follows that :

$$t_1, t_2, t_3 \in \left\{ \frac{1}{3}(s_1 + y + z); \frac{1}{3}(s_1 + j^2 y + jz); \frac{1}{3}(s_1 + jy + j^2 z) \right\}$$

Remark :
It is also possible to show this result with many other methods. Indeed, we can do it with :

- The use of the discriminant.
- Algebraic methods : Cardan's method, Viète's substitution, Lagrange's method, etc.
- Factorisation.
- Geometric methods : Omar Khayyam's method or with angle trisection (a cubic equation with real coefficients can be solved geometrically using the non-graduated ruler, the compass and the angle trisection if, and only if, the equation admits three real solutions).

III.3 Quartic equations

Let us consider a quartic equation : $X^4 - s_1X^3 + s_2X^2 - s_3X + s_4 = 0$.
Let t_1, t_2, t_3 and t_4 be the solutions of this equation.
The Galois group $\mathfrak{S}_4$ has a series :

$$\left\{\mathrm{Id}_{[\![1;4]\!]}\right\} \lhd V_4 \lhd \mathfrak{A}_4 \lhd \mathfrak{S}_4$$

with abelian quotients.

It is therefore natural to consider the three expressions :

$$y_1 := (t_1 + t_2)(t_3 + t_4),\ y_2 := (t_1 + t_3)(t_2 + t_4) \text{ and } y_3 := (t_1 + t_4)(t_2 + t_3)$$

These are permuted amongst themselves by any permutation in $\mathfrak{S}_4$, so that all the elementary symmetric polynomials in y_1, y_2 and y_3 lie in $\mathbb{K}(s_1, s_2, s_3, s_4)$.

Moreover, by the Tschirnhaus' transformation $U := T - \frac{1}{4}s_1$, which reduces the quartic to the form $U^4 + pU^2 + qU + r$.
It is now the case that in the above procedure :

$$y_1 + y_2 + y_3 = 2p,\ y_1y_2 + y_1y_3 + y_2y_3 = p^2 - 4r \text{ and } y_1y_2y_3 = -q^2$$

The resolvent cubic then takes the form : $X^3 - 2pX^2 + (p^2 - 4r)X + q^2$ and its zeros are y_1, y_2 and y_3. Since $t_1 + t_2 + t_3 + t_4 = s_1$, we can find three quadratic polynomials whose zeros are $t_1 + t_2$ and $t_2 + t_3$, $t_1 + t_3$ and $t_2 + t_4$, $t_1 + t_4$ and $t_2 + t_3$. From these, we finally have t_1, t_2, t_3 and t_4 in the set :

$$\left\{\frac{1}{2}\left(\sqrt{-y_1} + \sqrt{-y_2} + \sqrt{-y_3}\right); \frac{1}{2}\left(\sqrt{-y_1} - \sqrt{-y_2} - \sqrt{-y_3}\right); \frac{1}{2}\left(-\sqrt{-y_1} + \sqrt{-y_2} - \sqrt{-y_3}\right); \frac{1}{2}\left(-\sqrt{-y_1} - \sqrt{-y_2} + \sqrt{-y_3}\right)\right\}$$

the square roots being chosen so that $\sqrt{-y_1}\sqrt{-y_2}\sqrt{-y_3} = -q$.

Remark :
It is also possible to have other expressions by using Ferrari's method, Lagrange's method or Descartes' method.

Remark :
Concerning the equations of degree greater or equal than 5, as their Galois group is not solvable by radical, we can not have a formula using radicals. However, it is possible to have a formula for the zeros of a quintic equation by using Tschirnhaus' transformation and **Bring's radical** (or also know as **ultraradical**) or with elliptic functions.

IV The inverse problem of Galois theory

To conclude this chapter, we give a recent development of Galois Theory.

Any finite group is Galois group of an extension of the field $\mathbb{Q}$? The answer to this question is not yet known. The study of the Galois groups of degree 2,3 and 4 polynomials allows us to affirm that any subgroup of $\mathfrak{S}_2$, $\mathfrak{S}_3$, and $\mathfrak{S}_4$ is a Galois group of an extension of $\mathbb{Q}$.

Jean-Pierre Serre pointed out in 1981 that, apart from the abelian groups, few finite groups were known for which the answer was known, always positive : the groups $\mathfrak{A}_n$ and $\mathfrak{S}_n$ (Hilbert 1954), the solvable groups (result of very difficult demonstration of Shafarevitch, 1954), the groups $\mathrm{PSL}(2, \mathbb{F}_p)$ for some p...

The situation has changed considerably in a few years. In 1985, it was known, thanks to the work of Belyi, Fried, Llorente, Matzat, Thomson, etc. that 18 of the 26 simple so-called "sporadic" groups are Galois groups of an extension of the field $\mathbb{Q}$. Many more results have appeared since then.

Proposition 4 :

Let G be a finite abelian group.
There exists a finite Galois extension $\mathbb{K}$ of $\mathbb{Q}$ of Galois group G.

Proof :

Let us consider G a finite abelian group.
According to the theorem of finitely generated abelian group, we know that $G \cong \prod_{i \in I} \mathbb{Z}/n_i\mathbb{Z}$ where each n_i are distinct or not (and I is a finite set).
Let us choose, for all i in I, a prime number p_i such that $p_i \equiv 1\ [n_i]$. According to Dirichlet's theorem on arithmetic progressions, we can choose all p_i the distinct.

We denote $N := \prod_{i \in I} p_i$ and $\zeta := e^{\frac{2i\pi}{N}}$.
We know that $\text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \cong (\mathbb{Z}/N\mathbb{Z})^\times$. Hence :

$$\text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \cong \prod_{i \in I} (\mathbb{Z}/p_i\mathbb{Z})^\times \cong \prod_{i \in I} \mathbb{Z}/(p_i - 1)\mathbb{Z}$$

But, for all i in I, there exists k_i in $\mathbb{Z}$ such that : $p_i - 1 = k_i n_i$. Then, $H := \prod_{i \in I} n_i\mathbb{Z}/(p_i - 1)\mathbb{Z}$ is a subgroup of $(\mathbb{Z}/N\mathbb{Z})^\times$.

So, if we denote H' the corresponding subgroup of $\text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$, then $\mathbb{K} := \{x \in \mathbb{Q}(\zeta) \text{ st } \forall \sigma \in H',\ \sigma(x) = x\}$ is a normal extension of $\mathbb{Q}$ (because H' is a normal subgroup of G) and $\text{Gal}(\mathbb{K}/\mathbb{Q}) \cong \left((\mathbb{Z}/N\mathbb{Z})^\times\right)/H \cong G$.

■

Example 5 :

Let us consider $G := \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$.
We have $n_1 = n_2 = 3$ and $n_3 = 5$. So, we can take $p_1 = 7$, $p_2 = 13$ and $p_3 = 13$, which gives $N = 1001$.

Moreover, we know that $(\mathbb{Z}/1001\mathbb{Z})^\times \cong (\mathbb{Z}/7\mathbb{Z})^\times \times (\mathbb{Z}/11\mathbb{Z})^\times \times (\mathbb{Z}/13\mathbb{Z})^\times \cong \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$.

And so, we have $H \cong 3\mathbb{Z}/6\mathbb{Z} \times 3\mathbb{Z}/12\mathbb{Z} \times 5\mathbb{Z}/10\mathbb{Z}$.

Finally, to conclude this section, we give Shafarevich's theorem without (its difficult) proof :

Theorem 4 : Shafarevich's theorem :

Any finite solvable group is the Galois group of some finite extension of the field $\mathbb{Q}$.

Remark :
It was first proved by Igor Shafarevich (1954), though Alexander Schmidt later pointed out a gap in the proof, which was fixed by Shafarevich in 1989.

Moreover, by using Feit-Thompson theorem, we have that all group of odd order is a Galois group over $\mathbb{Q}$. However, the question is still open for the other groups.

Conclusion

To conclude, we can see that the concept of a solvable group is central to algebra and is not limited to group theory. Indeed, we have seen that solvable groups include other types of groups such as simple groups or p-groups for example. This makes it possible to demonstrate interesting properties on these groups and in particular on their internal structures. But we can apply the theory of solvable groups to other areas of algebra, for example in geometry with the construction of some regular polygons, or even to Galois theory through the resolution of a general equation of degree greater than or equal to 5. This tool is therefore as versatile as it is powerful because it allows to solve very important mathematical problems that have resisted mathematicians for several centuries (if not a millennium).

Finally, it would be wrong to believe that solvable groups are limited to this kind of application. For example, another application is the Lie–Kolchin theorem which is a triangularisability result of the connected and solvable subgroups of the invertible matrix group $\mathrm{GL}_n(\mathbb{K})$, where $\mathbb{K}$ is an algebraically closed field for a given characteristic.

Bibliography

[1] *https://webusers.imj-prg.fr/ patrick.polo/M1Galois/ATGchdix.pdf.*

[2] Emil Artin. *Galois Theory.* NAPCO Inc., 1942.

[3] William Burnside. On groups of order $p^\alpha q^\beta$. 1904.

[4] William Burnside. On groups of order $p^\alpha q^\beta$ (second paper). 1905.

[5] Benoît Claudon. Deux théorèmes de burnside. 2009.

[6] David A. Cox. *Galois Theory.* Wiley-interscience, 2004.

[7] Jean Delcourt. *Théorie des groupes.* Dunod, 2019.

[8] Jean-Pierre Escofier. *Théorie de Galois.* Dunod, 2020.

[9] Georges Gras and Marie-Nicole. *Algèbre fondamentale - Arithmétique.* Ellipses, 2004.

[10] Ian Stewart. *Galois Theory.* Halsted Press, 1973.

[11] Wikipedia. https://en.wikipedia.org/wiki/Feit-Thompson theorem.

[12] Wikipedia. https://en.wikipedia.org/wiki/Solvable group.

[13] Wikipedia. https://fr.wikiversity.org/wiki/Théorie des groupes/Groupes résolubles.