Chapitre 3 : Constructibilité à la règle et au compas des polygones réguliers

I. Introduction

On se place dans un plan $(\mathcal{P})$.

I. Introduction

On se place dans un plan $(\mathcal{P})$.

Soit $\mathcal{E}$ un ensemble de points du plan contenant deux points distincts O et A et soit B tel que le triplet (O, A, B) forme un repère orthonormal. On note (x, y) les coordonnées dans ce repère.

I. Introduction

On se place dans un plan $(\mathcal{P})$.

Soit $\mathcal{E}$ un ensemble de points du plan contenant deux points distincts O et A et soit B tel que le triplet (O, A, B) forme un repère orthonormal. On note (x, y) les coordonnées dans ce repère.

Soit $n \in \mathbb{N} \setminus \{0; 1; 2\}$.

I. Introduction

On se place dans un plan $(\mathcal{P})$.

Soit $\mathcal{E}$ un ensemble de points du plan contenant deux points distincts O et A et soit B tel que le triplet (O, A, B) forme un repère orthonormal. On note (x, y) les coordonnées dans ce repère.

Soit $n \in \mathbb{N} \setminus \{0; 1; 2\}$. On note $\mathcal{R}_n$ le *polygone régulier à n côtés de centre O et de sommet A*.

On se place dans un plan $(\mathcal{P})$.

Soit $\mathcal{E}$ un ensemble de points du plan contenant deux points distincts O et A et soit B tel que le triplet (O, A, B) forme un repère orthonormal. On note (x, y) les coordonnées dans ce repère.

Soit $n \in \mathbb{N} \setminus \{0; 1; 2\}$. On note $\mathcal{R}_n$ le *polygone régulier à n côtés de centre O et de sommet A*. Nous allons montrer le résultat suivant :

I. Introduction

On se place dans un plan $(\mathcal{P})$.

Soit $\mathcal{E}$ un ensemble de points du plan contenant deux points distincts O et A et soit B tel que le triplet (O, A, B) forme un repère orthonormal. On note (x, y) les coordonnées dans ce repère.

Soit $n \in \mathbb{N} \setminus \{0; 1; 2\}$. On note $\mathcal{R}_n$ le *polygone régulier à n côtés de centre O et de sommet A*. Nous allons montrer le résultat suivant :

Théorème de Gauss-Wantzel

Le polygone régulier $\mathcal{R}_n$ est constructible à partir de $\{O, A\}$ ssi

I. Introduction

On se place dans un plan $(\mathcal{P})$.

Soit $\mathcal{E}$ un ensemble de points du plan contenant deux points distincts O et A et soit B tel que le triplet (O, A, B) forme un repère orthonormal. On note (x, y) les coordonnées dans ce repère.

Soit $n \in \mathbb{N} \setminus \{0; 1; 2\}$. On note $\mathcal{R}_n$ le *polygone régulier à n côtés de centre O et de sommet A*. Nous allons montrer le résultat suivant :

Théorème de Gauss-Wantzel

Le polygone régulier $\mathcal{R}_n$ est constructible à partir de $\{O, A\}$ ssi n est le produit d'une puissance de deux et

I. Introduction

On se place dans un plan $(\mathcal{P})$.

Soit $\mathcal{E}$ un ensemble de points du plan contenant deux points distincts O et A et soit B tel que le triplet (O, A, B) forme un repère orthonormal. On note (x, y) les coordonnées dans ce repère.

Soit $n \in \mathbb{N} \setminus \{0; 1; 2\}$. On note $\mathcal{R}_n$ le *polygone régulier à n côtés de centre O et de sommet A*. Nous allons montrer le résultat suivant :

Théorème de Gauss-Wantzel

Le polygone régulier $\mathcal{R}_n$ est constructible à partir de $\{O, A\}$ ssi n est le produit d'une puissance de deux et de nombres de Fermat <u>premiers</u> et <u>deux à deux distincts</u>.

I. Introduction

On se place dans un plan $(\mathcal{P})$.

Soit $\mathcal{E}$ un ensemble de points du plan contenant deux points distincts O et A et soit B tel que le triplet (O, A, B) forme un repère orthonormal. On note (x, y) les coordonnées dans ce repère.

Soit $n \in \mathbb{N} \setminus \{0; 1; 2\}$. On note $\mathcal{R}_n$ le *polygone régulier à n côtés de centre O et de sommet A*. Nous allons montrer le résultat suivant :

Théorème de Gauss-Wantzel

Le polygone régulier $\mathcal{R}_n$ est constructible à partir de $\{O, A\}$ ssi n est le produit d'une puissance de deux et de nombres de Fermat premiers et deux à deux distincts.

Si $m \in \mathbb{N}$,

I. Introduction

On se place dans un plan $(\mathcal{P})$.

Soit $\mathcal{E}$ un ensemble de points du plan contenant deux points distincts O et A et soit B tel que le triplet (O, A, B) forme un repère orthonormal. On note (x, y) les coordonnées dans ce repère.

Soit $n \in \mathbb{N} \setminus \{0; 1; 2\}$. On note $\mathcal{R}_n$ le *polygone régulier à n côtés de centre O et de sommet A*. Nous allons montrer le résultat suivant :

Théorème de Gauss-Wantzel

Le polygone régulier $\mathcal{R}_n$ est constructible à partir de $\{O, A\}$ ssi n est le produit d'une puissance de deux et de nombres de Fermat premiers et deux à deux distincts.

Si $m \in \mathbb{N}$, le $m^{\text{ème}}$ nombre de Fermat est le nombre $F_m := 1 + 2^{2^m}$.

II. Nombres complexes constructibles

Soit $z = a + ib \in \mathbb{C}$.

II. Nombres complexes constructibles

Soit $z = a + ib \in \mathbb{C}$.

Définition 1

On dit que z est constructible à partir de $\mathcal{E}$ si $(a, b) \in \mathcal{K}_{\mathcal{E}}$.

Soit $z = a + ib \in \mathbb{C}$.

Définition 1

On dit que z est <u>constructible à partir de $\mathcal{E}$</u> si $(a, b) \in \mathcal{K}_{\mathcal{E}}$.

On note $\mathcal{F}_{\mathcal{E}}$ l'ensemble des nombres complexes constructibles à partir de $\mathcal{E}$.

Soit $z = a + ib \in \mathbb{C}$.

Définition 1

On dit que z est constructible à partir de $\mathcal{E}$ si $(a, b) \in \mathcal{K}_{\mathcal{E}}$.

On note $\mathcal{F}_{\mathcal{E}}$ l'ensemble des nombres complexes constructibles à partir de $\mathcal{E}$.

Proposition 2

$\mathcal{F}_{\mathcal{E}}$ est un sous-corps de $\mathbb{C}$ contenant $\mathbb{Q}(\mathcal{E})$.

II. Nombres complexes constructibles

Soit $z = a + ib \in \mathbb{C}$.

Définition 1

On dit que z est constructible à partir de $\mathcal{E}$ si $(a, b) \in \mathcal{K}_{\mathcal{E}}$.

On note $\mathcal{F}_{\mathcal{E}}$ l'ensemble des nombres complexes constructibles à partir de $\mathcal{E}$.

Proposition 2

$\mathcal{F}_{\mathcal{E}}$ est un sous-corps de $\mathbb{C}$ contenant $\mathbb{Q}(\mathcal{E})$. De plus, si $z \in \mathcal{F}_{\mathcal{E}}$ et si $\omega \in \mathbb{C}$ vérifie $\omega^2 = z$,

II. Nombres complexes constructibles

Soit $z = a + ib \in \mathbb{C}$.

Définition 1

On dit que z est constructible à partir de $\mathcal{E}$ si $(a, b) \in \mathcal{K}_{\mathcal{E}}$.

On note $\mathcal{F}_{\mathcal{E}}$ l'ensemble des nombres complexes constructibles à partir de $\mathcal{E}$.

Proposition 2

$\mathcal{F}_{\mathcal{E}}$ est un sous-corps de $\mathbb{C}$ contenant $\mathbb{Q}(\mathcal{E})$. De plus, si $z \in \mathcal{F}_{\mathcal{E}}$ et si $\omega \in \mathbb{C}$ vérifie $\omega^2 = z$, alors $\omega \in \mathcal{F}_{\mathcal{E}}$.

De la proposition 2 et du critère nécessaire et suffisant de constructibilité à partir de $\mathcal{E}$, on déduit :

De la proposition 2 et du critère nécessaire et suffisant de constructibilité à partir de $\mathcal{E}$, on déduit :

Théorème 3

$z \in \mathcal{F}_{\mathcal{E}}$ ss'il existe une suite

$$K_0 \subset \cdots \subset K_N,$$

$N \in \mathbb{N}$, de sous-corps de $\mathbb{C}$

II. Nombres complexes constructibles

De la proposition 2 et du critère nécessaire et suffisant de constructibilité à partir de $\mathcal{E}$, on déduit :

Théorème 3

$z \in \mathcal{F}_{\mathcal{E}}$ ss'il existe une suite

$$K_0 \subset \cdots \subset K_N,$$

$N \in \mathbb{N}$, de sous-corps de $\mathbb{C}$ telle que

- $K_0 = \mathbb{Q}(\mathcal{E})$,
- $z \in K_N$,
- si $N \geq 1$, pour tout $i \in \{1, \ldots, N\}$, $[K_i : K_{i-1}] \in \{1; 2\}$.

De la proposition 2 et du critère nécessaire et suffisant de constructibilité à partir de $\mathcal{E}$, on déduit :

Théorème 3

$z \in \mathcal{F}_{\mathcal{E}}$ ss'il existe une suite

$$K_0 \subset \cdots \subset K_N,$$

$N \in \mathbb{N}$, de sous-corps de $\mathbb{C}$ telle que

- $K_0 = \mathbb{Q}(\mathcal{E})$,
- $z \in K_N$,
- si $N \geq 1$, pour tout $i \in \{1, \ldots, N\}$, $[K_i : K_{i-1}] \in \{1; 2\}$.

Corollaire 4 (Critère de Wantzel)

Si $z \in \mathcal{F}_{\mathcal{E}}$, alors z est algébrique sur $\mathbb{Q}(\mathcal{E})$ de degré une puissance de deux.

III. Constructibilité du polygone régulier $\mathcal{R}_n$

III. Constructibilité du polygone régulier $\mathcal{R}_n$

Lemme 5

$\mathcal{R}_n$ est constructible à partir de $\{O, A\}$

Lemme 5

$\mathcal{R}_n$ est constructible à partir de $\{O, A\}$ ssi $\zeta_n := e^{\frac{2i\pi}{n}} \in \mathcal{F}_{\{O,A\}}$.

III. Constructibilité du polygone régulier $\mathcal{R}_n$

Lemme 5

$\mathcal{R}_n$ est constructible à partir de $\{O, A\}$ ssi $\zeta_n := e^{\frac{2i\pi}{n}} \in \mathcal{F}_{\{O,A\}}$.

Remarque :

III. Constructibilité du polygone régulier $\mathcal{R}_n$

Lemme 5

$\mathcal{R}_n$ est constructible à partir de $\{O, A\}$ ssi $\zeta_n := e^{\frac{2i\pi}{n}} \in \mathcal{F}_{\{O,A\}}$.

Remarque : ζ_n est algébrique sur $\mathbb{Q} = \mathbb{Q}(\{O, A\})$.

Lemme 5

$\mathcal{R}_n$ est constructible à partir de $\{O, A\}$ ssi $\zeta_n := e^{\frac{2i\pi}{n}} \in \mathcal{F}_{\{O,A\}}$.

Remarque : ζ_n est algébrique sur $\mathbb{Q} = \mathbb{Q}(\{O, A\})$.

On note

$$\Phi_n := \prod_{\substack{1 \leq k \leq n \\ \mathrm{pgcd}(k,n)=1}} \left(X - \zeta_n^k\right) = \prod_{\substack{1 \leq k \leq n \\ \mathrm{pgcd}(k,n)=1}} \left(X - e^{\frac{2ik\pi}{n}}\right) \in \mathbb{C}[X]$$

Lemme 5

$\mathcal{R}_n$ est constructible à partir de $\{O, A\}$ ssi $\zeta_n := e^{\frac{2i\pi}{n}} \in \mathcal{F}_{\{O,A\}}$.

Remarque : ζ_n est algébrique sur $\mathbb{Q} = \mathbb{Q}(\{O, A\})$.

On note

$$\Phi_n := \prod_{\substack{1 \leq k \leq n \\ \mathrm{pgcd}(k,n)=1}} (X - \zeta_n^k) = \prod_{\substack{1 \leq k \leq n \\ \mathrm{pgcd}(k,n)=1}} \left(X - e^{\frac{2ik\pi}{n}}\right) \in \mathbb{C}[X]$$

le $n^{\text{ème}}$ *polynôme cyclotomique*.

III. Constructibilité du polygone régulier $\mathcal{R}_n$

Lemme 5

$\mathcal{R}_n$ est constructible à partir de $\{O, A\}$ ssi $\zeta_n := e^{\frac{2i\pi}{n}} \in \mathcal{F}_{\{O,A\}}$.

Remarque : ζ_n est algébrique sur $\mathbb{Q} = \mathbb{Q}(\{O, A\})$.

On note

$$\Phi_n := \prod_{\substack{1 \leq k \leq n \\ \mathrm{pgcd}(k,n)=1}} (X - \zeta_n^k) = \prod_{\substack{1 \leq k \leq n \\ \mathrm{pgcd}(k,n)=1}} \left(X - e^{\frac{2ik\pi}{n}}\right) \in \mathbb{C}[X]$$

le $n^{\text{ème}}$ *polynôme cyclotomique*.

Rappel :

Lemme 5

$\mathcal{R}_n$ est constructible à partir de $\{O, A\}$ ssi $\zeta_n := e^{\frac{2i\pi}{n}} \in \mathcal{F}_{\{O,A\}}$.

Remarque : ζ_n est algébrique sur $\mathbb{Q} = \mathbb{Q}(\{O, A\})$.

On note

$$\Phi_n := \prod_{\substack{1 \leq k \leq n \\ \mathrm{pgcd}(k,n)=1}} (X - \zeta_n^k) = \prod_{\substack{1 \leq k \leq n \\ \mathrm{pgcd}(k,n)=1}} \left(X - e^{\frac{2ik\pi}{n}}\right) \in \mathbb{C}[X]$$

le $n^{\text{ème}}$ *polynôme cyclotomique*.

Rappel : $\Phi_n \in \mathbb{Z}[X]$

III. Constructibilité du polygone régulier $\mathcal{R}_n$

Lemme 5

$\mathcal{R}_n$ est constructible à partir de $\{O, A\}$ ssi $\zeta_n := e^{\frac{2i\pi}{n}} \in \mathcal{F}_{\{O,A\}}$.

Remarque : ζ_n est algébrique sur $\mathbb{Q} = \mathbb{Q}(\{O, A\})$.

On note

$$\Phi_n := \prod_{\substack{1 \leq k \leq n \\ \mathrm{pgcd}(k,n)=1}} (X - \zeta_n^k) = \prod_{\substack{1 \leq k \leq n \\ \mathrm{pgcd}(k,n)=1}} \left(X - e^{\frac{2ik\pi}{n}}\right) \in \mathbb{C}[X]$$

le $n^{\text{ème}}$ *polynôme cyclotomique*.

Rappel : $\Phi_n \in \mathbb{Z}[X]$ et Φ_n est irréductible sur $\mathbb{Q}$.

III. Constructibilité du polygone régulier $\mathcal{R}_n$

Lemme 5

$\mathcal{R}_n$ est constructible à partir de $\{O, A\}$ ssi $\zeta_n := e^{\frac{2i\pi}{n}} \in \mathcal{F}_{\{O,A\}}$.

<u>Remarque :</u> ζ_n est algébrique sur $\mathbb{Q} = \mathbb{Q}(\{O, A\})$.

On note

$$\Phi_n := \prod_{\substack{1 \leq k \leq n \\ \mathrm{pgcd}(k,n)=1}} (X - \zeta_n^k) = \prod_{\substack{1 \leq k \leq n \\ \mathrm{pgcd}(k,n)=1}} \left(X - e^{\frac{2ik\pi}{n}}\right) \in \mathbb{C}[X]$$

le $n^{\text{ème}}$ *polynôme cyclotomique*.

<u>Rappel :</u> $\Phi_n \in \mathbb{Z}[X]$ et Φ_n est irréductible sur $\mathbb{Q}$.

Proposition 6

On a $\mu_{\zeta_n, \mathbb{Q}} = \Phi_n$:

III. Constructibilité du polygone régulier $\mathcal{R}_n$

Lemme 5

$\mathcal{R}_n$ est constructible à partir de $\{O, A\}$ ssi $\zeta_n := e^{\frac{2i\pi}{n}} \in \mathcal{F}_{\{O,A\}}$.

<u>Remarque :</u> ζ_n est algébrique sur $\mathbb{Q} = \mathbb{Q}(\{O, A\})$.

On note

$$\Phi_n := \prod_{\substack{1 \leq k \leq n \\ \mathrm{pgcd}(k,n)=1}} (X - \zeta_n^k) = \prod_{\substack{1 \leq k \leq n \\ \mathrm{pgcd}(k,n)=1}} \left(X - e^{\frac{2ik\pi}{n}}\right) \in \mathbb{C}[X]$$

le $n^{\text{ème}}$ *polynôme cyclotomique*.

<u>Rappel :</u> $\Phi_n \in \mathbb{Z}[X]$ et Φ_n est irréductible sur $\mathbb{Q}$.

Proposition 6

On a $\mu_{\zeta_n,\mathbb{Q}} = \Phi_n$: ζ_n est donc algébrique sur $\mathbb{Q}$ de degré $\varphi(n)$

III. Constructibilité du polygone régulier $\mathcal{R}_n$

Lemme 5

$\mathcal{R}_n$ est constructible à partir de $\{O, A\}$ ssi $\zeta_n := e^{\frac{2i\pi}{n}} \in \mathcal{F}_{\{O,A\}}$.

Remarque : ζ_n est algébrique sur $\mathbb{Q} = \mathbb{Q}(\{O, A\})$.

On note

$$\Phi_n := \prod_{\substack{1 \leq k \leq n \\ \mathrm{pgcd}(k,n)=1}} (X - \zeta_n^k) = \prod_{\substack{1 \leq k \leq n \\ \mathrm{pgcd}(k,n)=1}} \left(X - e^{\frac{2ik\pi}{n}}\right) \in \mathbb{C}[X]$$

le $n^{\text{ème}}$ *polynôme cyclotomique*.

Rappel : $\Phi_n \in \mathbb{Z}[X]$ et Φ_n est irréductible sur $\mathbb{Q}$.

Proposition 6

On a $\mu_{\zeta_n,\mathbb{Q}} = \Phi_n$: ζ_n est donc algébrique sur $\mathbb{Q}$ de degré $\varphi(n)$ (où φ est la fonction indicatrice d'Euler).

IV. Théorème de Gauss-Wantzel : sens direct

On commence par montrer :

IV. Théorème de Gauss-Wantzel : sens direct

On commence par montrer :

Proposition 7

Si $\mathcal{R}_n$ est constructible à partir de $\{O, A\}$, alors n est le produit d'une puissance de deux et de nombres de Fermat premiers deux à deux distincts.

On commence par montrer :

Proposition 7

Si $\mathcal{R}_n$ est constructible à partir de $\{O, A\}$, alors n est le produit d'une puissance de deux et de nombres de Fermat premiers deux à deux distincts.

La preuve de la proposition 7 utilise :

On commence par montrer :

Proposition 7

Si $\mathcal{R}_n$ est constructible à partir de $\{O, A\}$, alors n est le produit d'une puissance de deux et de nombres de Fermat premiers deux à deux distincts.

La preuve de la proposition 7 utilise :

Lemme 8

Soit $k \in \mathbb{N} \setminus \{0\}$ tel que l'entier $1 + 2^k$ soit premier.

IV. Théorème de Gauss-Wantzel : sens direct

On commence par montrer :

Proposition 7

Si $\mathcal{R}_n$ est constructible à partir de $\{O, A\}$, alors n est le produit d'une puissance de deux et de nombres de Fermat premiers deux à deux distincts.

La preuve de la proposition 7 utilise :

Lemme 8

Soit $k \in \mathbb{N} \setminus \{0\}$ tel que l'entier $1 + 2^k$ soit premier. Alors k est une puissance de 2 et $1 + 2^k$ est donc un nombre de Fermat.

V. Théorème de Gauss-Wantzel : sens réciproque

Nous allons ensuite montrer :

Nous allons ensuite montrer :

Théorème 9

Si n est le produit d'une puissance de deux et de nombres de Fermat premiers deux à deux distincts, alors $\mathcal{R}_n$ est constructible à partir de $\{O, A\}$.

V. Théorème de Gauss-Wantzel : sens réciproque

Preuve :

V. Théorème de Gauss-Wantzel : sens réciproque

Preuve : On suppose que

$$n = 2^d \prod_{s=1}^{M} F_{m_s},$$

avec $d \in \mathbb{N}$, $m_1, \ldots, m_s \in \mathbb{N}$ deux à deux distincts et, pour tout $s \in \{1, \ldots, M\}$, F_{m_s} premier.

V. Théorème de Gauss-Wantzel : sens réciproque

Preuve : On suppose que

$$n = 2^d \prod_{s=1}^{M} F_{m_s},$$

avec $d \in \mathbb{N}$, $m_1, \ldots, m_s \in \mathbb{N}$ deux à deux distincts et, pour tout $s \in \{1, \ldots, M\}$, F_{m_s} premier.

On a :

V. Théorème de Gauss-Wantzel : sens réciproque

Preuve : On suppose que

$$n = 2^d \prod_{s=1}^{M} F_{m_s},$$

avec $d \in \mathbb{N}$, $m_1, \ldots, m_s \in \mathbb{N}$ deux à deux distincts et, pour tout $s \in \{1, \ldots, M\}$, F_{m_s} premier.

On a :

Lemme 10

Soient k_1 et k_2 deux entiers naturels non nuls premiers entre eux.

V. Théorème de Gauss-Wantzel : sens réciproque

Preuve : On suppose que

$$n = 2^d \prod_{s=1}^{M} F_{m_s},$$

avec $d \in \mathbb{N}$, $m_1, \ldots, m_s \in \mathbb{N}$ deux à deux distincts et, pour tout $s \in \{1, \ldots, M\}$, F_{m_s} premier.

On a :

Lemme 10

Soient k_1 et k_2 deux entiers naturels non nuls premiers entre eux. Alors $\zeta_{k_1 k_2} \in \mathcal{F}_{\{O,A\}}$ ssi $\zeta_{k_1}, \zeta_{k_2} \in \mathcal{F}_{\{O,A\}}$.

V. Théorème de Gauss-Wantzel : sens réciproque

Preuve : On suppose que

$$n = 2^d \prod_{s=1}^{M} F_{m_s},$$

avec $d \in \mathbb{N}$, $m_1, \ldots, m_s \in \mathbb{N}$ deux à deux distincts et, pour tout $s \in \{1, \ldots, M\}$, F_{m_s} premier.

On a :

Lemme 10

Soient k_1 et k_2 deux entiers naturels non nuls premiers entre eux. Alors $\zeta_{k_1 k_2} \in \mathcal{F}_{\{O,A\}}$ ssi $\zeta_{k_1}, \zeta_{k_2} \in \mathcal{F}_{\{O,A\}}$.

Et :

V. Théorème de Gauss-Wantzel : sens réciproque

Preuve : On suppose que

$$n = 2^d \prod_{s=1}^{M} F_{m_s},$$

avec $d \in \mathbb{N}$, $m_1, \ldots, m_s \in \mathbb{N}$ deux à deux distincts et, pour tout $s \in \{1, \ldots, M\}$, F_{m_s} premier.

On a :

Lemme 10

Soient k_1 et k_2 deux entiers naturels non nuls premiers entre eux. Alors $\zeta_{k_1 k_2} \in \mathcal{F}_{\{O,A\}}$ ssi $\zeta_{k_1}, \zeta_{k_2} \in \mathcal{F}_{\{O,A\}}$.

Et :

Lemme 11

$\forall m \in \mathbb{N}$, $\zeta_{2^m} \in \mathcal{F}_{\{O,A\}}$.

On est ainsi ramené à montrer :

On est ainsi ramené à montrer :

Théorème 12

Soit p un entier de Fermat premier, alors $\zeta_p \in \mathcal{F}_{\{O,A\}}$.

VI. Groupe de Galois d’une extension

VI. Groupe de Galois d'une extension

Soient L un corps et K un sous-corps de L.

VI. Groupe de Galois d'une extension

Soient L un corps et K un sous-corps de L. Soit $\psi : L \to L$ une application.

VI. Groupe de Galois d'une extension

Soient L un corps et K un sous-corps de L. Soit $\psi : L \to L$ une application.

Définition 13

On dit que ψ est un <u>endomorphisme de L sur K</u> si

Soient L un corps et K un sous-corps de L. Soit $\psi : L \to L$ une application.

Définition 13

On dit que ψ est un endomorphisme de L sur K si

- ψ est un morphisme de corps,

VI. Groupe de Galois d'une extension

Soient L un corps et K un sous-corps de L. Soit $\psi : L \to L$ une application.

Définition 13

On dit que ψ est un endomorphisme de L sur K si

- ψ est un morphisme de corps,
- ψ est une application K-linéaire.

Soient L un corps et K un sous-corps de L. Soit $\psi : L \to L$ une application.

Définition 13

On dit que ψ est un endomorphisme de L sur K si

- ψ est un morphisme de corps,
- ψ est une application K-linéaire.

On dit que ψ est un automorphisme de L sur K

VI. Groupe de Galois d'une extension

Soient L un corps et K un sous-corps de L. Soit $\psi : L \to L$ une application.

Définition 13

On dit que ψ est un endomorphisme de L sur K si

- ψ est un morphisme de corps,
- ψ est une application K-linéaire.

On dit que ψ est un automorphisme de L sur K si ψ est un endomorphisme de L sur K bijectif,

VI. Groupe de Galois d'une extension

Soient L un corps et K un sous-corps de L. Soit $\psi : L \to L$ une application.

Définition 13

On dit que ψ est un endomorphisme de L sur K si

- ψ est un morphisme de corps,
- ψ est une application K-linéaire.

On dit que ψ est un automorphisme de L sur K si ψ est un endomorphisme de L sur K bijectif, et on note $\mathrm{Gal}(L/K)$ l'ensemble des automorphismes de L sur K.

VI. Groupe de Galois d'une extension

Soient L un corps et K un sous-corps de L. Soit $\psi : L \to L$ une application.

Définition 13

On dit que ψ est un endomorphisme de L sur K si

- ψ est un morphisme de corps,
- ψ est une application K-linéaire.

On dit que ψ est un automorphisme de L sur K si ψ est un endomorphisme de L sur K bijectif, et on note $\mathrm{Gal}(L/K)$ l'ensemble des automorphismes de L sur K.

Remarque :

VI. Groupe de Galois d'une extension

Soient L un corps et K un sous-corps de L. Soit $\psi : L \to L$ une application.

Définition 13

On dit que ψ est un endomorphisme de L sur K si

- ψ est un morphisme de corps,
- ψ est une application K-linéaire.

On dit que ψ est un automorphisme de L sur K si ψ est un endomorphisme de L sur K bijectif, et on note $\mathrm{Gal}(L/K)$ l'ensemble des automorphismes de L sur K.

Remarque :

- Si $[L : K] < \infty$, ψ est un endomorphisme de L sur K ssi $\psi \in \mathrm{Gal}(L/K)$.

VI. Groupe de Galois d'une extension

Soient L un corps et K un sous-corps de L. Soit $\psi : L \to L$ une application.

Définition 13

On dit que ψ est un endomorphisme de L sur K si

- ψ est un morphisme de corps,
- ψ est une application K-linéaire.

On dit que ψ est un automorphisme de L sur K si ψ est un endomorphisme de L sur K bijectif, et on note $\mathrm{Gal}(L/K)$ l'ensemble des automorphismes de L sur K.

Remarque :

- Si $[L : K] < \infty$, ψ est un endomorphisme de L sur K ssi $\psi \in \mathrm{Gal}(L/K)$.
- ψ est un endomorphisme de L sur K ssi $\forall k \in \mathbb{N}$, $\forall P \in K[X_1, \ldots, X_k]$, $\forall a_1, \ldots, a_k \in L$,

VI. Groupe de Galois d'une extension

Soient L un corps et K un sous-corps de L. Soit $\psi : L \to L$ une application.

Définition 13

On dit que ψ est un endomorphisme de L sur K si

- ψ est un morphisme de corps,
- ψ est une application K-linéaire.

On dit que ψ est un automorphisme de L sur K si ψ est un endomorphisme de L sur K bijectif, et on note $\mathrm{Gal}(L/K)$ l'ensemble des automorphismes de L sur K.

Remarque :

- Si $[L : K] < \infty$, ψ est un endomorphisme de L sur K ssi $\psi \in \mathrm{Gal}(L/K)$.
- ψ est un endomorphisme de L sur K ssi $\forall k \in \mathbb{N}$, $\forall P \in K[X_1, \dots, X_k]$, $\forall a_1, \dots, a_k \in L$,

$$\psi\big(P(a_1, \dots, a_k)\big) = P\big(\psi(a_1), \dots, \psi(a_k)\big).$$

Supposons que ψ soit un endomorphisme de L sur K. Alors :

Supposons que ψ soit un endomorphisme de L sur K. Alors :

- Si $L = K(a_1, \ldots, a_l)$, alors ψ est déterminé par $\psi(a_1), \ldots, \psi(a_l)$,

Supposons que ψ soit un endomorphisme de L sur K. Alors :

- Si $L = K(a_1, \ldots, a_l)$, alors ψ est déterminé par $\psi(a_1), \ldots, \psi(a_l)$,
- Si $P(x) = 0$ avec $P \in K[X]$ et $x \in L$, alors $P\big(\psi(x)\big) = 0$.

Supposons que ψ soit un endomorphisme de L sur K. Alors :

- Si $L = K(a_1, \dots, a_l)$, alors ψ est déterminé par $\psi(a_1), \dots, \psi(a_l)$,
- Si $P(x) = 0$ avec $P \in K[X]$ et $x \in L$, alors $P\big(\psi(x)\big) = 0$.

Proposition et Définition 14

$(\mathrm{Gal}(L/K), \circ)$ est un groupe,

Supposons que ψ soit un endomorphisme de L sur K. Alors :

- Si $L = K(a_1, \ldots, a_l)$, alors ψ est déterminé par $\psi(a_1), \ldots, \psi(a_l)$,
- Si $P(x) = 0$ avec $P \in K[X]$ et $x \in L$, alors $P\big(\psi(x)\big) = 0$.

Proposition et Définition 14

$(\mathrm{Gal}(L/K), \circ)$ est un groupe, appelé groupe de Galois de L sur K.

Supposons que ψ soit un endomorphisme de L sur K. Alors :

- Si $L = K(a_1, \ldots, a_l)$, alors ψ est déterminé par $\psi(a_1), \ldots, \psi(a_l)$,
- Si $P(x) = 0$ avec $P \in K[X]$ et $x \in L$, alors $P\big(\psi(x)\big) = 0$.

Proposition et Définition 14

$(\mathrm{Gal}(L/K), \circ)$ est un groupe, appelé groupe de Galois de L sur K.

Soit $n \in \mathbb{N} \setminus \{0\}$.

VI. Groupe de Galois d'une extension

Supposons que ψ soit un endomorphisme de L sur K. Alors :

- Si $L = K(a_1, \dots, a_l)$, alors ψ est déterminé par $\psi(a_1), \dots, \psi(a_l)$,
- Si $P(x) = 0$ avec $P \in K[X]$ et $x \in L$, alors $P\big(\psi(x)\big) = 0$.

Proposition et Définition 14

$(\mathrm{Gal}(L/K), \circ)$ est un groupe, appelé <u>groupe de Galois de L sur K</u>.

Soit $n \in \mathbb{N} \setminus \{0\}$.

Théorème 15

Le groupe $\mathrm{Gal}\,(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ est isomorphe à $(\mathbb{Z}/n\mathbb{Z})^\times$.

Conséquence : Soit $p = 1 + 2^{2^m}$ un nombre de Fermat premier, $m \in \mathbb{N}$.

Conséquence : Soit $p = 1 + 2^{2^m}$ un nombre de Fermat premier, $m \in \mathbb{N}$.
Alors

$$\mathrm{Gal}\left(\mathbb{Q}(\zeta_p)/\mathbb{Q}\right)$$

est cyclique d'ordre $p - 1$.

Conséquence : Soit $p = 1 + 2^{2^m}$ un nombre de Fermat premier, $m \in \mathbb{N}$. Alors

$$\mathrm{Gal}\left(\mathbb{Q}(\zeta_p)/\mathbb{Q}\right)$$

est cyclique d'ordre $p - 1$.

Soit ρ un générateur de $\mathrm{Gal}\left(\mathbb{Q}(\zeta_p)/\mathbb{Q}\right)$.

Conséquence : Soit $p = 1 + 2^{2^m}$ un nombre de Fermat premier, $m \in \mathbb{N}$. Alors

$$\mathrm{Gal}\left(\mathbb{Q}(\zeta_p)/\mathbb{Q}\right)$$

est cyclique d'ordre $p - 1$.

Soit ρ un générateur de $\mathrm{Gal}\left(\mathbb{Q}(\zeta_p)/\mathbb{Q}\right)$. On note

$$G_k := \langle \rho^{2^k} \rangle$$

pour $k \in \{0, \dots, 2^m\}$,

Conséquence : Soit $p = 1 + 2^{2^m}$ un nombre de Fermat premier, $m \in \mathbb{N}$.
Alors

$$\mathrm{Gal}\left(\mathbb{Q}(\zeta_p)/\mathbb{Q}\right)$$

est cyclique d'ordre $p - 1$.

Soit ρ un générateur de $\mathrm{Gal}\left(\mathbb{Q}(\zeta_p)/\mathbb{Q}\right)$. On note

$$G_k := \langle \rho^{2^k} \rangle$$

pour $k \in \{0, \ldots, 2^m\}$, et on a

$$\left\{\mathrm{id}_{\mathbb{Q}(\zeta_p)}\right\} = G_{2^m} \subset G_{2^m-1} \subset \cdots \subset G_1 \subset G_0 = \mathrm{Gal}\left(\mathbb{Q}(\zeta_p)/\mathbb{Q}\right).$$

Proposition 16

Soit $S \subset \mathrm{Gal}(L/K)$.

Proposition 16

Soit $S \subset \mathrm{Gal}(L/K)$. L'ensemble

$$L^S := \{x \in L \mid \forall \psi \in S, \psi(x) = x\}$$

est un sous-corps de L contenant K.

VI. Groupe de Galois d'une extension

Proposition 16

Soit $S \subset \mathrm{Gal}(L/K)$. L'ensemble

$$L^S := \{x \in L \mid \forall \psi \in S, \psi(x) = x\}$$

est un sous-corps de L contenant K.

Conséquence :

Proposition 16

Soit $S \subset \mathrm{Gal}(L/K)$. L'ensemble

$$L^S := \{x \in L \mid \forall \psi \in S, \psi(x) = x\}$$

est un sous-corps de L contenant K.

Conséquence : On avait

$$\left\{\mathrm{id}_{\mathbb{Q}(\zeta_p)}\right\} = G_{2^m} \subset G_{2^m-1} \subset \cdots \subset G_1 \subset G_0 = \mathrm{Gal}\left(\mathbb{Q}(\zeta_p)/\mathbb{Q}\right).$$

Proposition 16

Soit $S \subset \mathrm{Gal}(L/K)$. L'ensemble

$$L^S := \{x \in L \mid \forall \psi \in S, \psi(x) = x\}$$

est un sous-corps de L contenant K.

Conséquence : On avait

$$\left\{\mathrm{id}_{\mathbb{Q}(\zeta_p)}\right\} = G_{2^m} \subset G_{2^m-1} \subset \cdots \subset G_1 \subset G_0 = \mathrm{Gal}\left(\mathbb{Q}(\zeta_p)/\mathbb{Q}\right).$$

Si l'on note

$$L_i := \mathbb{Q}(\zeta_p)^{G_i}$$

pour $i \in \{0, \dots, 2^m\}$,

Proposition 16

Soit $S \subset \mathrm{Gal}(L/K)$. L'ensemble

$$L^S := \{x \in L \mid \forall \psi \in S, \psi(x) = x\}$$

est un sous-corps de L contenant K.

Conséquence : On avait

$$\left\{\mathrm{id}_{\mathbb{Q}(\zeta_p)}\right\} = G_{2^m} \subset G_{2^m-1} \subset \cdots \subset G_1 \subset G_0 = \mathrm{Gal}\left(\mathbb{Q}(\zeta_p)/\mathbb{Q}\right).$$

Si l'on note

$$L_i := \mathbb{Q}(\zeta_p)^{G_i}$$

pour $i \in \{0, \ldots, 2^m\}$, on obtient une suite

$$L_0 \subset L_1 \subset \cdots \subset L_{2^m-1} \subset L_{2^m} = \mathbb{Q}(\zeta_p)$$

de sous-corps de $\mathbb{Q}(\zeta_p)$ contenant $\mathbb{Q}$.

VII. Théorème de Gauss-Wantzel : sens réciproque

On considère la suite d'extensions

$$L_0 \subset L_1 \subset \cdots \subset L_{2^m-1} \subset L_{2^m} = \mathbb{Q}(\zeta_p).$$

On considère la suite d'extensions

$$L_0 \subset L_1 \subset \cdots \subset L_{2^m-1} \subset L_{2^m} = \mathbb{Q}(\zeta_p).$$

Théorème 17

On a

On considère la suite d'extensions

$$L_0 \subset L_1 \subset \cdots \subset L_{2^m-1} \subset L_{2^m} = \mathbb{Q}(\zeta_p).$$

Théorème 17

On a

- $L_0 = \mathbb{Q}\ (= \mathbb{Q}(\{O, A\})\,),$

On considère la suite d'extensions

$$L_0 \subset L_1 \subset \cdots \subset L_{2^m-1} \subset L_{2^m} = \mathbb{Q}(\zeta_p).$$

Théorème 17

On a

- $L_0 = \mathbb{Q} \ (= \mathbb{Q}(\{O, A\})\,)$,
- $\zeta_p \in L_{2^m} = \mathbb{Q}(\zeta_p)$,

On considère la suite d'extensions

$$L_0 \subset L_1 \subset \cdots \subset L_{2^m-1} \subset L_{2^m} = \mathbb{Q}(\zeta_p).$$

Théorème 17

On a

- $L_0 = \mathbb{Q}\ (= \mathbb{Q}(\{O, A\})\,)$,
- $\zeta_p \in L_{2^m} = \mathbb{Q}(\zeta_p)$,
- pour tout $i \in \{1, \ldots, 2^m\}$, $[L_i : L_{i-1}] = 2$.

VII. Théorème de Gauss-Wantzel : sens réciproque

On considère la suite d'extensions

$$L_0 \subset L_1 \subset \cdots \subset L_{2^m-1} \subset L_{2^m} = \mathbb{Q}(\zeta_p).$$

Théorème 17

On a

- $L_0 = \mathbb{Q}\ (= \mathbb{Q}(\{O, A\})\,)$,
- $\zeta_p \in L_{2^m} = \mathbb{Q}(\zeta_p)$,
- pour tout $i \in \{1, \ldots, 2^m\}$, $[L_i : L_{i-1}] = 2$.

Conséquence : $\zeta_p \in \mathcal{F}_{\{O,A\}}$.

VIII. Théorème de Gauss-Wantzel

VIII. Théorème de Gauss-Wantzel

Théorème de Gauss-Wantzel

Soit $n \in \mathbb{N} \setminus \{0; 1; 2\}$. Le polygone régulier $\mathcal{R}_n$ est constructible à partir de $\{O, A\}$ ssi n est le produit d'une puissance de deux et de nombres de Fermat premiers et deux à deux distincts.

Exemples :

VIII. Théorème de Gauss-Wantzel

Théorème de Gauss-Wantzel

Soit $n \in \mathbb{N} \setminus \{0; 1; 2\}$. Le polygone régulier $\mathcal{R}_n$ est constructible à partir de $\{O, A\}$ ssi n est le produit d'une puissance de deux et de nombres de Fermat premiers et deux à deux distincts.

Exemples :

- Le triangle équilatéral est constructible.

VIII. Théorème de Gauss-Wantzel

Théorème de Gauss-Wantzel

Soit $n \in \mathbb{N} \setminus \{0;1;2\}$. Le polygone régulier $\mathcal{R}_n$ est constructible à partir de $\{O, A\}$ ssi n est le produit d'une puissance de deux et de nombres de Fermat premiers et deux à deux distincts.

Exemples :

- Le triangle équilatéral est constructible.
- Le carré est constructible.

VIII. Théorème de Gauss-Wantzel

Théorème de Gauss-Wantzel

Soit $n \in \mathbb{N} \setminus \{0; 1; 2\}$. Le polygone régulier $\mathcal{R}_n$ est constructible à partir de $\{O, A\}$ ssi n est le produit d'une puissance de deux et de nombres de Fermat premiers et deux à deux distincts.

Exemples :

- Le triangle équilatéral est constructible.
- Le carré est constructible.
- Le pentagone régulier est constructible.

VIII. Théorème de Gauss-Wantzel

Théorème de Gauss-Wantzel

Soit $n \in \mathbb{N} \setminus \{0; 1; 2\}$. Le polygone régulier $\mathcal{R}_n$ est constructible à partir de $\{O, A\}$ ssi n est le produit d'une puissance de deux et de nombres de Fermat premiers et deux à deux distincts.

Exemples :

- Le triangle équilatéral est constructible.
- Le carré est constructible.
- Le pentagone régulier est constructible.
- L'hexagone régulier est constructible.

VIII. Théorème de Gauss-Wantzel

Théorème de Gauss-Wantzel

Soit $n \in \mathbb{N} \setminus \{0;1;2\}$. Le polygone régulier $\mathcal{R}_n$ est constructible à partir de $\{O, A\}$ ssi n est le produit d'une puissance de deux et de nombres de Fermat premiers et deux à deux distincts.

Exemples :

- Le triangle équilatéral est constructible.
- Le carré est constructible.
- Le pentagone régulier est constructible.
- L'hexagone régulier est constructible.
- L'heptagone régulier n'est pas constructible.

VIII. Théorème de Gauss-Wantzel

Théorème de Gauss-Wantzel

Soit $n \in \mathbb{N} \setminus \{0; 1; 2\}$. Le polygone régulier $\mathcal{R}_n$ est constructible à partir de $\{O, A\}$ ssi n est le produit d'une puissance de deux et de nombres de Fermat premiers et deux à deux distincts.

Exemples :

- Le triangle équilatéral est constructible.
- Le carré est constructible.
- Le pentagone régulier est constructible.
- L'hexagone régulier est constructible.
- L'heptagone régulier n'est pas constructible.
- L'octogone régulier est constructible.

Théorème de Gauss-Wantzel

Soit $n \in \mathbb{N} \setminus \{0; 1; 2\}$. Le polygone régulier $\mathcal{R}_n$ est constructible à partir de $\{O, A\}$ ssi n est le produit d'une puissance de deux et de nombres de Fermat premiers et deux à deux distincts.

Exemples :

- Le triangle équilatéral est constructible.
- Le carré est constructible.
- Le pentagone régulier est constructible.
- L'hexagone régulier est constructible.
- L'heptagone régulier n'est pas constructible.
- L'octogone régulier est constructible.
- Le nonagone (ou ennéagone) régulier n'est pas constructible.

VIII. Théorème de Gauss-Wantzel

Théorème de Gauss-Wantzel

Soit $n \in \mathbb{N} \setminus \{0; 1; 2\}$. Le polygone régulier $\mathcal{R}_n$ est constructible à partir de $\{O, A\}$ ssi n est le produit d'une puissance de deux et de nombres de Fermat premiers et deux à deux distincts.

Exemples :

- Le triangle équilatéral est constructible.
- Le carré est constructible.
- Le pentagone régulier est constructible.
- L'hexagone régulier est constructible.
- L'heptagone régulier n'est pas constructible.
- L'octogone régulier est constructible.
- Le nonagone (ou ennéagone) régulier n'est pas constructible.
- Le décagone régulier est constructible.

Exemples :

- Le hendécagone régulier n'est pas constructible.
- Le dodécagone régulier est constructible.
- Le tridécagone régulier n'est pas constructible.
- Le tétradécagone régulier n'est pas constructible.
- Le pentadécagone régulier est constructible.
- L'hexadécagone régulier est constructible.
- L'heptadécagone régulier est constructible.
- L'octadécagone régulier n'est pas constructible.
- L'ennéadécagone régulier n'est pas constructible.
- L'icosagone régulier est constructible.