Lectures dirigées – Nombres constructibles

Taddéo Rocq & Giovanni Lebaron, sous la direction d'Antoine Dequay

ENS Rennes
2023–2024

Quelques grands problèmes de géométrie de l'Antiquité :

- Quadrature du cercle
- Duplication du cube
- Trisection de l'angle
- Construction des polygones réguliers

Quelques grands problèmes de géométrie de l'Antiquité :

- Quadrature du cercle
- Duplication du cube
- Trisection de l'angle
- Construction des polygones réguliers

Résolus au XIX$^{\text{ème}}$ siècle, soit plus de 2000 ans après.

L'ensemble des nombres constructibles

Définitions de base

On se donne un ensemble fini $\mathcal{B}$ de points du plan, appelés *points de base*.

On se donne un ensemble fini $\mathcal{B}$ de points du plan, appelés *points de base*.

À partir de ces points, on est autorisés à construire :

- la droite passant par deux points de $\mathcal{B}$,
- le cercle de centre un point de $\mathcal{B}$ et de rayon la distance entre deux points de $\mathcal{B}$.

On se donne un ensemble fini $\mathcal{B}$ de points du plan, appelés *points de base*.

À partir de ces points, on est autorisés à construire :

- la droite passant par deux points de $\mathcal{B}$,
- le cercle de centre un point de $\mathcal{B}$ et de rayon la distance entre deux points de $\mathcal{B}$.

Tout point obtenu par itération de ce procédé sera dit *constructible* (à la règle non graduée et au compas).

On se donne un ensemble fini $\mathcal{B}$ de points du plan, appelés *points de base*.

À partir de ces points, on est autorisés à construire :

- la droite passant par deux points de $\mathcal{B}$,
- le cercle de centre un point de $\mathcal{B}$ et de rayon la distance entre deux points de $\mathcal{B}$.

Tout point obtenu par itération de ce procédé sera dit *constructible* (à la règle non graduée et au compas).

Un nombre réel sera dit *constructible* lorsque c'est l'une des coordonnées d'un point constructible.

Dans toute la suite, on prendra $\mathcal{B} = \{O, I\}$. On peut déjà construire un repère orthonormé (O, I, J) en reportant correctement la longueur unité.

Dans toute la suite, on prendra $\mathcal{B} = \{O, I\}$. On peut déjà construire un repère orthonormé (O, I, J) en reportant correctement la longueur unité.

Sont également réalisables à la règle non graduée et au compas :

Dans toute la suite, on prendra $\mathcal{B} = \{O, I\}$. On peut déjà construire un repère orthonormé (O, I, J) en reportant correctement la longueur unité.

Sont également réalisables à la règle non graduée et au compas :

- perpendiculaires et parallèles,

Dans toute la suite, on prendra $\mathcal{B} = \{O, I\}$. On peut déjà construire un repère orthonormé (O, I, J) en reportant correctement la longueur unité.

Sont également réalisables à la règle non graduée et au compas :

- perpendiculaires et parallèles,
- médiatrices et milieux,

Dans toute la suite, on prendra $\mathcal{B} = \{O, I\}$. On peut déjà construire un repère orthonormé (O, I, J) en reportant correctement la longueur unité.

Sont également réalisables à la règle non graduée et au compas :

- perpendiculaires et parallèles,
- médiatrices et milieux,
- bissectrices,

Dans toute la suite, on prendra $\mathcal{B} = \{O, I\}$. On peut déjà construire un repère orthonormé (O, I, J) en reportant correctement la longueur unité.

Sont également réalisables à la règle non graduée et au compas :

- perpendiculaires et parallèles,
- médiatrices et milieux,
- bissectrices,
- projections orthogonales.

L'ensemble des nombres constructibles

Structure algébrique

À partir de deux nombres constructibles x et y, on peut construire...

L'ensemble des nombres constructibles

Structure algébrique

À partir de deux nombres constructibles x et y, on peut construire...

- $x + y$,

L'ensemble des nombres constructibles

Structure algébrique

À partir de deux nombres constructibles x et y, on peut construire...

- $x + y$,
- $x - y$,

À partir de deux nombres constructibles x et y, on peut construire...

- $x + y$,
- $x - y$,
- xy,

L'ensemble des nombres constructibles

Structure algébrique

À partir de deux nombres constructibles x et y, on peut construire...

- $x + y$,
- $x - y$,
- xy,
- x/y si $y \neq 0$.

À partir de deux nombres constructibles x et y, on peut construire...

- $x + y$,
- $x - y$,
- xy,
- x/y si $y \neq 0$.

Si $x \geq 0$ est constructible, on peut également construire $\sqrt{x}$.

À partir de deux nombres constructibles x et y, on peut construire...

- $x + y$,
- $x - y$,
- xy,
- x/y si $y \neq 0$.

Si $x \geq 0$ est constructible, on peut également construire $\sqrt{x}$.

Théorème

L'ensemble des nombres constructibles est un sous-corps de $\mathbb{R}$, stable par racine carrée.

Théorème de Wantzel

Quelques rappels sur les corps

On se donne deux corps quelconques K et L.

On se donne deux corps quelconques K et L.

On dit que K est une *extension* de L lorsque $K \subseteq L$. Ceci fait de L un $K-$espace vectoriel, et on appelle *degré* de L sur K la quantité :

$$[L : K] = \dim_K(L).$$

On se donne deux corps quelconques K et L.

On dit que K est une *extension* de L lorsque $K \subseteq L$. Ceci fait de L un $K-$espace vectoriel, et on appelle *degré* de L sur K la quantité :

$$[L : K] = \dim_K(L).$$

Si $K \subseteq L \subseteq M$ sont des corps, alors :

$$[M : K] = [M : L]\,[L : K]\,.$$

Une suite de corps $K_1 \subseteq \cdots \subseteq K_n$ sera appelée *tour d'extensions*.

On se donne deux corps quelconques K et L.

On dit que K est une *extension* de L lorsque $K \subseteq L$. Ceci fait de L un $K-$espace vectoriel, et on appelle *degré* de L sur K la quantité :

$$[L : K] = \dim_K(L).$$

Si $K \subseteq L \subseteq M$ sont des corps, alors :

$$[M : K] = [M : L]\,[L : K]\,.$$

Une suite de corps $K_1 \subseteq \cdots \subseteq K_n$ sera appelée *tour d'extensions*.

On dira que $K_i \subseteq K_{i+1}$ est une extension *quadratique* si $[K_{i+1} : K_i] = 2$.
On parlera dans ce cas de ***tour d'extensions quadratiques***.

Si $a \in L$, on dira que a est *algébrique* sur K lorsqu'il existe un polynôme $P \in K[X]$ non nul tel que $P(a) = 0$.

Si $a \in L$, on dira que a est *algébrique* sur K lorsqu'il existe un polynôme $P \in K[X]$ non nul tel que $P(a) = 0$.

On appelle alors *polynôme minimal* de a sur K l'unique polynôme unitaire de degré minimal μ_a vérifiant les conditions ci-dessus.

Si $a \in L$, on dira que a est *algébrique* sur K lorsqu'il existe un polynôme $P \in K[X]$ non nul tel que $P(a) = 0$.

On appelle alors *polynôme minimal* de a sur K l'unique polynôme unitaire de degré minimal μ_a vérifiant les conditions ci-dessus.

Exemple : $\sqrt{2}$ est algébrique sur $\mathbb{Q}$ et son polynôme minimal est $X^2 - 2$.

Si $a \in L$, on dira que a est *algébrique* sur K lorsqu'il existe un polynôme $P \in K[X]$ non nul tel que $P(a) = 0$.

On appelle alors *polynôme minimal* de a sur K l'unique polynôme unitaire de degré minimal μ_a vérifiant les conditions ci-dessus.

Exemple : $\sqrt{2}$ est algébrique sur $\mathbb{Q}$ et son polynôme minimal est $X^2 - 2$.

On notera $K(a)$ le plus petit sous-corps de L contenant K et a.
Si a est algébrique sur L, alors :

$$[K(a) : K] = \deg(\mu_a)$$

Théorème (Wantzel, 1837)

Soit $t \in \mathbb{R}$. Alors t est constructible si, et seulement s'il existe une tour d'extensions quadratiques :

$$\mathbb{Q} = L_1 \subseteq \cdots \subseteq L_n$$

avec $L_n \subseteq \mathbb{R}$ et $t \in L_n$.

Théorème de Wantzel

Un corollaire important

Corollaire

Si $t \in \mathbb{R}$ est constructible, alors t est algébrique sur $\mathbb{Q}$ et le degré de son polynôme minimal est une puissance de 2.

On appellera ce corollaire le « résultat de Wantzel ».

Théorème de Wantzel

Retour sur les problèmes de l'Antiquité

En 1882, Ferdinand von Lindemann montre que π est transcendant.
La quadrature du cercle est donc impossible à la règle et au compas.

Théorème de Wantzel

Retour sur les problèmes de l'Antiquité

En 1882, Ferdinand von Lindemann montre que π est transcendant.
La quadrature du cercle est donc impossible à la règle et au compas.

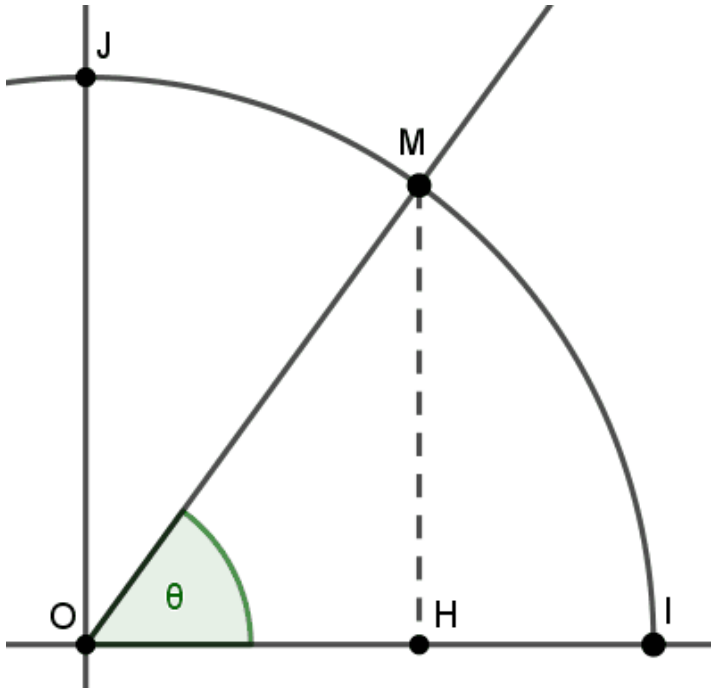
On peut également déduire du résultat de Wantzel que la duplication du cube et la trisection de l'angle sont impossibles à la règle non graduée et au compas.

Théorème de Gauss

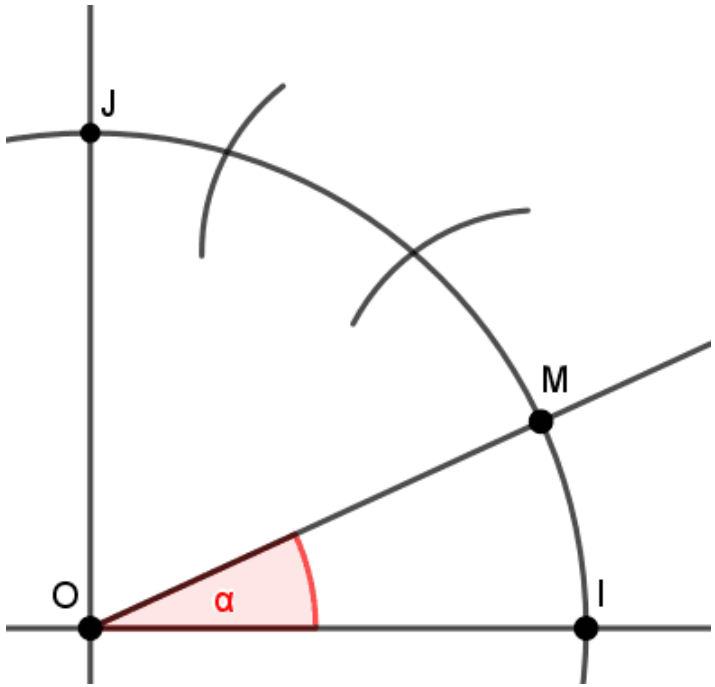
Le quatrième problème

Question. Quels sont les polygones réguliers constructibles à la règle non graduée et au compas ?

Soit $\theta \in \mathbb{R}$. On dit que l'angle $\widehat{\theta} = (\overrightarrow{OI}, \overrightarrow{OM})$ est *constructible* lorsque le point M est constructible, c'est-à-dire lorsque $\cos(\theta)$ est un nombre réel constructible.



Soit $n \geq 3$ un entier. On dit que le polygone régulier à n côtés est *constructible* lorsque l'angle $\widehat{\alpha} = \widehat{2\pi/n}$ est constructible (il suffit de le reporter au compas sur le cercle unité par la suite).



Lemme 1

Soient $m, n \geq 1$ deux entiers premiers entre eux. Alors $\widehat{\frac{2\pi}{mn}}$ est constructible si, et seulement si, $\widehat{\frac{2\pi}{m}}$ et $\widehat{\frac{2\pi}{n}}$ le sont.

Lemme 2

Soit $n \geq 3$ un entier dont la décomposition en facteurs premiers s'écrit :

$$n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}.$$

Alors le polygone régulier à n côtés est constructible si, et seulement si, pour tout $k \in \{1, \ldots, r\}$, $\widehat{\dfrac{2\pi}{p_k^{\alpha_k}}}$ est constructible.

Lemme 3

Les angles de la forme $\widehat{\frac{2\pi}{2^k}}$ avec $k \in \mathbb{N}$ sont constructibles.

Théorème de Gauss

Caractérisation des polygones réguliers constructibles

On appelle *nombres de Fermat* les entiers de la forme :

$$F_k = 1 + 2^{2^k}$$

Théorème de Gauss

Caractérisation des polygones réguliers constructibles

On appelle *nombres de Fermat* les entiers de la forme :

$$F_k = 1 + 2^{2^k}$$

Proposition

Soient $p \geq 3$ un nombre premier et $\alpha \geq 1$ un entier. Alors $\widehat{\frac{2\pi}{p^\alpha}}$ est constructible si, et seulement si, p est de Fermat et $\alpha = 1$.

On appelle *nombres de Fermat* les entiers de la forme :

$$F_k = 1 + 2^{2^k}$$

Proposition

Soient $p \geq 3$ un nombre premier et $\alpha \geq 1$ un entier. Alors $\widehat{\frac{2\pi}{p^\alpha}}$ est constructible si, et seulement si, p est de Fermat et $\alpha = 1$.

($\Rightarrow$) C'est le sens « facile ». On montre que $p = 1 + 2^m$ pour un certain entier $m \geq 1$ à l'aide du théorème de Wantzel, puis que m est lui-même une puissance de 2.

Théorème de Gauss

Caractérisation des polygones réguliers constructibles

($\Leftarrow$) Ça se complique *un peu*.

($\Leftarrow$) Ça se complique *un peu*. On suppose que p est un nombre premier de Fermat, en l'occurrence de la forme $p = 1 + 2^n$, et on veut montrer que $\cos(2\pi/p)$ est constructible.

($\Leftarrow$) Ça se complique *un peu*. On suppose que p est un nombre premier de Fermat, en l'occurrence de la forme $p = 1 + 2^n$, et on veut montrer que $\cos(2\pi/p)$ est constructible.

On s'intéresse à l'ensemble des racines primitives $p^{\text{èmes}}$ de l'unité :

$$\mathbb{U}_p \setminus \{1\} = \{\omega, \dots, \omega^{p-1}\}$$

avec $\omega = \exp\left(\frac{2\pi i}{p}\right) = \cos\left(\frac{2\pi}{p}\right) + i \sin\left(\frac{2\pi}{p}\right)$.

On étudie le corps $K = \mathbb{Q}(\omega)$, et on s'intéresse plus particulièrement au groupe de ses automorphismes.

Théorème de Gauss

Caractérisation des polygones réguliers constructibles

On étudie le corps $K = \mathbb{Q}(\omega)$, et on s'intéresse plus particulièrement au groupe de ses automorphismes.

Le polynôme minimal de ω sur $\mathbb{Q}$ est le $p^{\text{ème}}$ polynôme cyclotomique :

$$\Phi_p = X^{p-1} + X^{p-2} + \ldots + X + 1$$

On étudie le corps $K = \mathbb{Q}(\omega)$, et on s'intéresse plus particulièrement au groupe de ses automorphismes.

Le polynôme minimal de ω sur $\mathbb{Q}$ est le $p^{\text{ème}}$ polynôme cyclotomique :

$$\Phi_p = X^{p-1} + X^{p-2} + \ldots + X + 1$$

ce dont on déduit $[K : \mathbb{Q}] = p - 1 = 2^n$.

Théorème de Gauss

Caractérisation des polygones réguliers constructibles

Si $g \in \mathrm{Aut}(K)$, alors :

- $g(1) = 1$,
- puis $g(n) = n$ pour tout $n \in \mathbb{N}$,
- puis $g(n) = n$ pour tout $n \in \mathbb{Z}$,
- puis $g(q) = q$ pour tout $q \in \mathbb{Q}$!

Si $g \in \mathrm{Aut}(K)$, alors :

- $g(1) = 1$,
- puis $g(n) = n$ pour tout $n \in \mathbb{N}$,
- puis $g(n) = n$ pour tout $n \in \mathbb{Z}$,
- puis $g(q) = q$ pour tout $q \in \mathbb{Q}$!

Donc g est entièrement déterminé par $g(\omega)$.

Si $g \in \mathrm{Aut}(K)$, alors :

- $g(1) = 1$,
- puis $g(n) = n$ pour tout $n \in \mathbb{N}$,
- puis $g(n) = n$ pour tout $n \in \mathbb{Z}$,
- puis $g(q) = q$ pour tout $q \in \mathbb{Q}$!

Donc g est entièrement déterminé par $g(\omega)$.

On montre sans difficulté que $g(\omega) = \omega^k$ pour un certain $k \in \{1, \ldots, p-1\}$, ce qui fournit un isomorphisme :

$$\mathrm{Aut}(K) \cong \mathbb{F}_p^\times$$

Si $g \in \mathrm{Aut}(K)$, alors :

- $g(1) = 1$,
- puis $g(n) = n$ pour tout $n \in \mathbb{N}$,
- puis $g(n) = n$ pour tout $n \in \mathbb{Z}$,
- puis $g(q) = q$ pour tout $q \in \mathbb{Q}$!

Donc g est entièrement déterminé par $g(\omega)$.

On montre sans difficulté que $g(\omega) = \omega^k$ pour un certain $k \in \{1, \dots, p-1\}$, ce qui fournit un isomorphisme :

$$\mathrm{Aut}(K) \cong \mathbb{F}_p^\times$$

et on sait que $\mathbb{F}_p^\times$ est un groupe cyclique, donc $\mathrm{Aut}(K)$ l'est aussi.

Pourquoi tout ça ?

Pourquoi tout ça ?

- on souhaite montrer que $\cos(2\pi/p)$ est constructible ;

Pourquoi tout ça ?

- on souhaite montrer que $\cos(2\pi/p)$ est constructible ;
- on rappelle que $p - 1 = 2^n$ avec $n \geq 1$;

Pourquoi tout ça ?

- on souhaite montrer que $\cos(2\pi/p)$ est constructible ;
- on rappelle que $p - 1 = 2^n$ avec $n \geq 1$;
- on va construire une tour d'extensions quadratiques adaptée afin d'appliquer le théorème de Wantzel.

Pourquoi tout ça ?

- on souhaite montrer que $\cos(2\pi/p)$ est constructible ;
- on rappelle que $p - 1 = 2^n$ avec $n \geq 1$;
- on va construire une tour d'extensions quadratiques adaptée afin d'appliquer le théorème de Wantzel.

On note g un générateur du groupe cyclique $\mathrm{Aut}(K)$.

Pourquoi tout ça ?

- on souhaite montrer que $\cos(2\pi/p)$ est constructible ;
- on rappelle que $p - 1 = 2^n$ avec $n \geq 1$;
- on va construire une tour d'extensions quadratiques adaptée afin d'appliquer le théorème de Wantzel.

On note g un générateur du groupe cyclique $\mathrm{Aut}(K)$.

Idée : considérer les sous-groupes $G_i = \left\langle g^{2^i} \right\rangle$ pour $i \in \{0, \ldots, n\}$.

Pourquoi tout ça ?

- on souhaite montrer que $\cos(2\pi/p)$ est constructible ;
- on rappelle que $p - 1 = 2^n$ avec $n \geq 1$;
- on va construire une tour d'extensions quadratiques adaptée afin d'appliquer le théorème de Wantzel.

On note g un générateur du groupe cyclique $\mathrm{Aut}(K)$.

Idée : considérer les sous-groupes $G_i = \left\langle g^{2^i} \right\rangle$ pour $i \in \{0, \ldots, n\}$.
Ceci donne une suite d'inclusions strictes :

$$\{\mathrm{id}\} = G_n \subsetneq \cdots \subsetneq G_1 \subsetneq G_0 = G.$$

Théorème de Gauss

Caractérisation des polygones réguliers constructibles

Idée : s'intéresser aux points fixes des générateurs.

Idée : s'intéresser aux points fixes des générateurs.

De la suite d'inclusions strictes :

$$\{1_K\} = G_n \subsetneq \cdots \subsetneq G_1 \subsetneq G_0$$

on obtient une suite strictement croissante de sous-corps :

$$K_0 \subsetneq K_1 \subsetneq \cdots \subsetneq K_n = K$$

où l'on a posé $K_i = \left\{ z \in K \;\middle|\; g^{2^i}(z) = z \right\}$.

On montre facilement que $K_0 = \mathbb{Q}$.

Théorème de Gauss

Caractérisation des polygones réguliers constructibles

On montre facilement que $K_0 = \mathbb{Q}$.

Mais surtout ! $K_{n-1} = \mathbb{Q}\left(\cos\left(\frac{2\pi}{p}\right)\right)$.

Théorème de Gauss

Caractérisation des polygones réguliers constructibles

On montre facilement que $K_0 = \mathbb{Q}$.

Mais surtout ! $K_{n-1} = \mathbb{Q}\left(\cos\left(\frac{2\pi}{p}\right)\right)$.

On montre que $\cos(2\pi/p)$ est un point fixe de $g^{2^{n-1}}$:

$$\cos\left(\frac{2\pi}{p}\right) \in K_{n-1}.$$

Théorème de Gauss

Caractérisation des polygones réguliers constructibles

On montre facilement que $K_0 = \mathbb{Q}$.

Mais surtout ! $K_{n-1} = \mathbb{Q}\left(\cos\left(\frac{2\pi}{p}\right)\right)$.

On montre que $\cos(2\pi/p)$ est un point fixe de $g^{2^{n-1}}$:

$$\cos\left(\frac{2\pi}{p}\right) \in K_{n-1}.$$

On sait aussi que $g^{2^{n-1}}(q) = q$ pour tout $q \in \mathbb{Q}$, d'où :

$$\mathbb{Q}\left(\cos\left(\frac{2\pi}{p}\right)\right) \subseteq K_{n-1}.$$

Théorème de Gauss

Caractérisation des polygones réguliers constructibles

L'inclusion $\mathbb{Q}\left(\cos\left(\frac{2\pi}{p}\right)\right) \subseteq K_{n-1}$ est en fait une égalité.

Théorème de Gauss

Caractérisation des polygones réguliers constructibles

L'inclusion $\mathbb{Q}\left(\cos\left(\frac{2\pi}{p}\right)\right) \subseteq K_{n-1}$ est en fait une égalité.

En effet :

$$\omega + \omega^{-1} = \exp\left(\frac{2\pi i}{p}\right) + \exp\left(-\frac{2\pi i}{p}\right) = 2\cos\left(\frac{2\pi}{p}\right)$$

Théorème de Gauss

Caractérisation des polygones réguliers constructibles

L'inclusion $\mathbb{Q}\left(\cos\left(\frac{2\pi}{p}\right)\right) \subseteq K_{n-1}$ est en fait une égalité.

En effet :

$$\omega + \omega^{-1} = \exp\left(\frac{2\pi i}{p}\right) + \exp\left(-\frac{2\pi i}{p}\right) = 2\cos\left(\frac{2\pi}{p}\right)$$

ce qui entraîne :

$$\left[K : \mathbb{Q}\left(\cos\left(\frac{2\pi}{p}\right)\right)\right] = \left[\mathbb{Q}(\omega) : \mathbb{Q}\left(\cos\left(\frac{2\pi}{p}\right)\right)\right] = 2$$

L'inclusion $\mathbb{Q}\left(\cos\left(\frac{2\pi}{p}\right)\right) \subseteq K_{n-1}$ est en fait une égalité.

En effet :

$$\omega + \omega^{-1} = \exp\left(\frac{2\pi i}{p}\right) + \exp\left(-\frac{2\pi i}{p}\right) = 2\cos\left(\frac{2\pi}{p}\right)$$

ce qui entraîne :

$$\left[K : \mathbb{Q}\left(\cos\left(\frac{2\pi}{p}\right)\right)\right] = \left[\mathbb{Q}(\omega) : \mathbb{Q}\left(\cos\left(\frac{2\pi}{p}\right)\right)\right] = 2$$

et comme $K_{n-1} \subsetneq K_n = K$:

$$\underbrace{\left[K : \mathbb{Q}\left(\cos\left(\frac{2\pi}{p}\right)\right)\right]}_{=2} = \underbrace{[K : K_{n-1}]}_{\geq 2}\left[K_{n-1} : \mathbb{Q}\left(\cos\left(\frac{2\pi}{p}\right)\right)\right].$$

Théorème de Gauss

Caractérisation des polygones réguliers constructibles

Bref.

Bref. On a donc une tour d'extensions :

$$\mathbb{Q} = K_0 \subsetneq K_1 \subsetneq \cdots \subsetneq K_{n-1} = \mathbb{Q}\left(\cos\left(\frac{2\pi}{p}\right)\right) \subsetneq K_n = K.$$

Bref. On a donc une tour d'extensions :

$$\mathbb{Q} = K_0 \subsetneq K_1 \subsetneq \cdots \subsetneq K_{n-1} = \mathbb{Q}\left(\cos\left(\frac{2\pi}{p}\right)\right) \subsetneq K_n = K.$$

On rappelle que $[K : \mathbb{Q}] = [\mathbb{Q}(\omega) : \mathbb{Q}] = p - 1 = 2^n$. Par conséquent :

$$2^n = [K : \mathbb{Q}] = [K_n : K_{n-1}] \cdots [K_1 : K_0]$$

Bref. On a donc une tour d'extensions :

$$\mathbb{Q} = K_0 \subsetneq K_1 \subsetneq \cdots \subsetneq K_{n-1} = \mathbb{Q}\left(\cos\left(\frac{2\pi}{p}\right)\right) \subsetneq K_n = K.$$

On rappelle que $[K : \mathbb{Q}] = [\mathbb{Q}(\omega) : \mathbb{Q}] = p - 1 = 2^n$. Par conséquent :

$$2^n = [K : \mathbb{Q}] = [K_n : K_{n-1}] \cdots [K_1 : K_0]$$

donc on a n extensions, chacune de degré une puissance de 2. Par le principe des tiroirs, chaque degré $[K_{i+1} : K_i]$ vaut 2.

Bref. On a donc une tour d'extensions :

$$\mathbb{Q} = K_0 \subsetneq K_1 \subsetneq \cdots \subsetneq K_{n-1} = \mathbb{Q}\left(\cos\left(\frac{2\pi}{p}\right)\right) \subsetneq K_n = K.$$

On rappelle que $[K : \mathbb{Q}] = [\mathbb{Q}(\omega) : \mathbb{Q}] = p - 1 = 2^n$. Par conséquent :

$$2^n = [K : \mathbb{Q}] = [K_n : K_{n-1}] \cdots [K_1 : K_0]$$

donc on a n extensions, chacune de degré une puissance de 2. Par le principe des tiroirs, chaque degré $[K_{i+1} : K_i]$ vaut 2.

On dispose ainsi d'une tour d'extensions quadratiques partant de $\mathbb{Q}$ dans laquelle se trouve $\cos(2\pi/p)$.

Bref. On a donc une tour d'extensions :

$$\mathbb{Q} = K_0 \subsetneq K_1 \subsetneq \cdots \subsetneq K_{n-1} = \mathbb{Q}\left(\cos\left(\frac{2\pi}{p}\right)\right) \subsetneq K_n = K.$$

On rappelle que $[K : \mathbb{Q}] = [\mathbb{Q}(\omega) : \mathbb{Q}] = p - 1 = 2^n$. Par conséquent :

$$2^n = [K : \mathbb{Q}] = [K_n : K_{n-1}] \cdots [K_1 : K_0]$$

donc on a n extensions, chacune de degré une puissance de 2. Par le principe des tiroirs, chaque degré $[K_{i+1} : K_i]$ vaut 2.

On dispose ainsi d'une tour d'extensions quadratiques partant de $\mathbb{Q}$ dans laquelle se trouve $\cos(2\pi/p)$. :)

Théorème de Gauss

Caractérisation des polygones réguliers constructibles

En résumé :

- les $\widehat{\frac{2\pi}{2^k}}$ sont tous constructibles
- les $\widehat{\frac{2\pi}{p^\alpha}}$ ($p \geq 3$ premier, $\alpha \geq 1$) qui sont constructibles sont exactement ceux pour lesquels p est de Fermat et $\alpha = 1$

Théorème de Gauss

Caractérisation des polygones réguliers constructibles

En résumé :

- les $\widehat{\frac{2\pi}{2^k}}$ sont tous constructibles
- les $\widehat{\frac{2\pi}{p^\alpha}}$ ($p \geq 3$ premier, $\alpha \geq 1$) qui sont constructibles sont exactement ceux pour lesquels p est de Fermat et $\alpha = 1$

Théorème (Gauss)

Le polygone régulier à $n \geq 3$ côtés est constructible si, et seulement si :

$$n = 2^\alpha \quad \text{ou} \quad n = 2^\alpha p_1 \cdots p_r$$

où $\alpha \in \mathbb{N}$ et $p_1, \ldots, p_r$ sont des nombres premiers de Fermat distincts.

Merci !

Merci pour votre attention !