

# Théorème de Wantzel

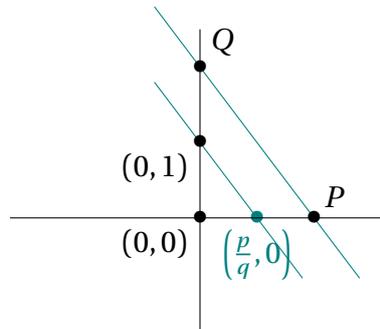
Une application sympathique de la théorie des corps en géométrie. Les arguments sont assez simples et donnent lieu à de jolies applications.

**Notation 1.** On note  $\mathbb{E}$  l'ensemble des nombres constructibles. Tout au long du développement, on se permettra de confondre points et coordonnées.

**Lemme 2.**  $\mathbb{E}$  contient le corps  $\mathbb{Q}$ .

[GOZ]  
p. 49

*Démonstration.* Tout élément  $z \in \mathbb{Z}$  est constructible. Soit  $(p, q) \in \mathbb{Z}^* \times \mathbb{N}^*$ . Les points  $P = (p, 0)$  et  $Q = (0, q)$  sont constructibles. On considère la droite  $(d)$ , parallèle à  $(PQ)$  passant par  $(0, 1)$ . Cette droite est constructible, et son point d'intersection avec la droite passant par les points  $(0, 0)$  et  $(1, 0)$  est  $(\frac{p}{q}, 0)$  par le théorème de Thalès.

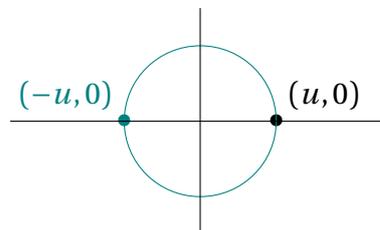


Donc  $\frac{p}{q} \in \mathbb{E}$ . Comme  $0 \in \mathbb{E}$ , on a bien  $\mathbb{Q} \subseteq \mathbb{E}$ . □

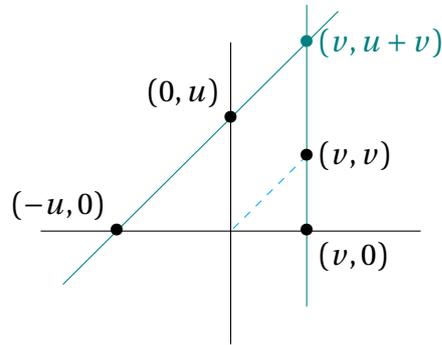
**Lemme 3.**  $\mathbb{E}$  est un sous-corps de  $\mathbb{R}$  stable par racine carrée.

*Démonstration.* Soient  $u, v \in \mathbb{E}$ . Commençons par montrer que  $\mathbb{E}$  est un sous-corps de  $\mathbb{R}$ .

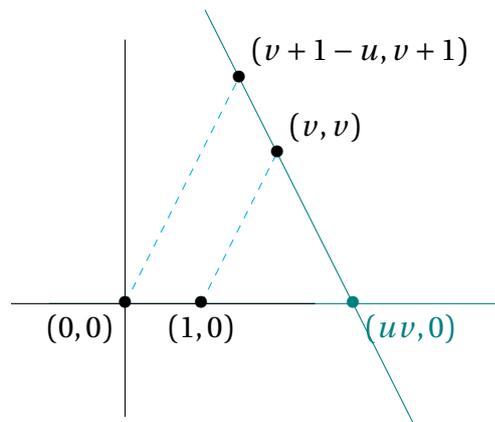
— Le point  $(u, 0)$  est constructible donc son symétrique  $(-u, 0)$  l'est aussi. Donc  $-u \in \mathbb{E}$ .



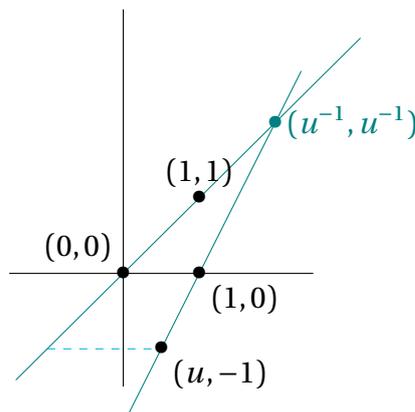
— La droite passant par les points  $(0, u)$  et  $(-u, 0)$  et la droite passant par les points  $(v, 0)$  et  $(v, v)$  ont pour point d'intersection  $(v, u + v)$  (par le théorème de Thalès). Donc  $u + v \in \mathbb{E}$ .



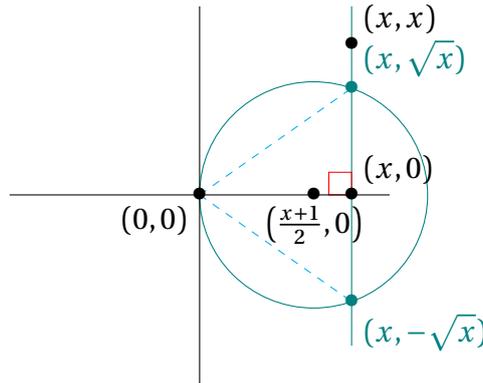
- D'après ce qui précède,  $v + 1$  et  $v + 1 - u$  appartiennent à  $\mathbb{E}$ . La droite passant par les points  $(v + 1 - u, v + 1)$  et  $(u, v)$  et la droite passant par les points  $(0, 0)$  et  $(1, 0)$  ont pour point d'intersection  $(uv, 0)$  (par le théorème de Thalès). Donc  $uv \in \mathbb{E}$ .



- On suppose  $u \neq 0$ . La droite passant par les points  $(1, 0)$  et  $(u, -1)$  et la droite passant par les points  $(0, 0)$  et  $(1, 1)$  ont pour point d'intersection  $(u^{-1}, u^{-1})$  (par le théorème de Thalès). Donc  $u^{-1} \in \mathbb{E}$ .



Ainsi,  $\mathbb{E}$  est un sous-corps de  $\mathbb{R}$ , qui contient  $\mathbb{Q}$  par le Lemme 2. Maintenant, soit  $x \in \mathbb{E}$  avec  $x > 0$ . Comme  $\mathbb{E}$  est un sous-corps de  $\mathbb{R}$ , on a  $\frac{x+1}{2} \in \mathbb{E}$ . Le cercle de centre  $(\frac{x+1}{2}, 0)$  passant par  $(0, 0)$  et la droite passant par les points  $(x, 0)$  et  $(x, -\sqrt{x})$  ont pour point d'intersection  $(x, \sqrt{x})$  et  $(x, -\sqrt{x})$  par le théorème de Pythagore. Donc  $\sqrt{x} \in \mathbb{E}$ .



□

**Théorème 4** (Wantzel). Soit  $\alpha \in \mathbb{R}$ . Alors,  $\alpha \in \mathbb{E}$  si et seulement s'il existe une suite finie  $(L_0, \dots, L_p)$  de sous-corps de  $\mathbb{R}$  vérifiant :

- (i)  $L_0 = \mathbb{Q}$ .
- (ii)  $\forall i \in \llbracket 0, p-1 \rrbracket$ ,  $L_{i+1}$  est une extension quadratique (de degré 2) de  $L_i$ .
- (iii)  $\alpha \in L_p$ .

*Démonstration.* On suppose  $\alpha$  constructible. Alors, il existe un point  $M$  tel que  $\alpha$  est l'abscisse de  $M$ .  $M$  s'obtient à l'aide d'un nombre fini de constructions de points  $M_1, \dots, M_m$ . Pour tout  $i \in \llbracket 1, m \rrbracket$ , on note  $(x_i, y_i)$  les coordonnées de  $M_i$ . De ce fait, on a une tour d'extension

[ULM18]  
p. 103

$$\underbrace{K_0}_{=\mathbb{Q}} \subseteq K_1 \subseteq \dots \subseteq K_m$$

avec  $\alpha \in K_m$  et pour tout  $i \in \llbracket 1, m-1 \rrbracket$ ,  $K_{i+1} = K_i(x_i, y_i)$ . Soit  $i \in \llbracket 1, m-1 \rrbracket$ . Montrons que  $[K_{i+1} : K_i] \leq 2$ . On a différents cas possibles :

- $M_i$  est l'intersection de deux droites passant par des nombres constructibles de  $K_i$ . Alors, les coordonnées  $(x_i, y_i)$  de  $M_i$  sont solution d'un système d'équations de la forme

$$\begin{cases} ax + by = c \\ a'x + b'y = c' \end{cases}$$

avec  $a, b, c, a', b', c' \in K_i$  par construction. Donc,  $x_i, y_i \in K_i$  et ainsi,  $[K_{i+1} : K_i] = 1$ .

- $M_i$  est l'intersection d'une droite et d'un cercle passant par des points dont les coordonnées sont des nombres constructibles de  $K_i$  et de rayon un nombre constructible de  $K_i$ . Alors, les coordonnées  $(x_i, y_i)$  de  $M_i$  sont solution d'un système d'équations de la forme

$$\begin{cases} ax + by = c \\ (x - a')^2 + (y - b')^2 = c' \end{cases}$$

avec  $a, b, c, a', b', c' \in K_i$  par construction. Raisonnons selon la nullité de  $a$ .

— Si  $a \neq 0$ , la première équation donne

$$x = -\frac{by + c}{a}$$

et en réinjectant dans la deuxième équation, on obtient que  $y_i$  est racine d'un polynôme de degré 2. Ainsi,  $[K_i(y_i) : K_i] \leq 2$ . Puisque  $x_i = -\frac{by_i + c}{a} \in K_i(y_i)$ , on a bien  $[K_{i+1} : K_i] \leq 2$ .

— Si  $a = 0$ , alors  $y_i = \frac{c}{b} \in K_i$  (on ne peut pas avoir  $b = 0$  dans ce cas). Or, cette fois-ci c'est  $x_i$  qui est racine d'un polynôme de degré 2. On peut conclure de la même manière que ci-dessus.

—  $M_i$  est l'intersection de deux cercles passant par des points dont les coordonnées sont des nombres constructibles de  $K_i$  et de rayon un nombre constructible de  $K_i$ . Alors, les coordonnées  $(x_i, y_i)$  de  $M_i$  sont solution d'un système d'équations de la forme

$$\begin{cases} (x - a)^2 + (y - b)^2 = c \\ (x - a')^2 + (y - b')^2 = c' \end{cases}$$

avec  $a, b, c, a', b', c' \in K_i$  par construction. On soustrait la deuxième équation à la première, pour obtenir le système équivalent :

$$\begin{cases} -2(a - a')x - 2(b - b')y = c - c' - (a^2 - a'^2) - (b^2 - b'^2) \\ (x - a')^2 + (y - b')^2 = c' \end{cases}$$

ce qui nous ramène au cas précédent.

Il suffit alors d'extraire de la suite  $(K_0, \dots, K_m)$  une sous-suite  $(L_0, \dots, L_p)$  strictement croissante (au sens de l'inclusion) en ne conservant dans la suite initiale que les corps extension quadratique du précédent (avec  $L_0 = K_0$  et  $L_p = K_n$ ). On obtient une suite de sous-corps de  $\mathbb{R}$  (par le Lemme 3) qui remplit les trois conditions annoncées.

Réciproquement, supposons l'existence d'une suite  $(L_0, \dots, L_p)$  de sous-corps de  $\mathbb{R}$  répondant aux trois conditions de l'énoncé. Montrons par récurrence que

$$\forall j \in \llbracket 0, p \rrbracket, L_j \subseteq \mathbb{E}$$

— Initialisation :  $L_0 = \mathbb{Q}$  : cela résulte du Lemme 2.

— Hérédité : Supposons  $L_j \subseteq \mathbb{E}$  pour  $j \in \llbracket 0, p - 1 \rrbracket$ . Soit  $x \in L_{j+1}$ . Comme, par hypothèse,

$$[L_{j+1} : L_j] = 2$$

la famille  $(1, x, x^2)$  est  $L_j$ -liée :

$$\exists a, b, c \in L_j \text{ non tous nuls tels que } ax^2 + bx + c = 0$$

— Si  $a = 0$ , alors,  $x = -\frac{c}{b} \in L_j$ . Donc  $x \in \mathbb{E}$ .

— Si  $a \neq 0$ , alors,  $x = \frac{1}{2a}(-b \pm \sqrt{b^2 - 4ac})$ . Donc, comme  $\mathbb{E}$  est un sous-corps de  $\mathbb{R}$  stable par racine carrée (cf. Lemme 3),  $x \in \mathbb{E}$ .

Ainsi,  $L_{j+1} \subseteq \mathbb{E}$ . En conclusion,  $L_p \subseteq \mathbb{E}$ , donc  $\alpha$  est constructible. □

*Remarque 5.* La réciproque et la conclusion du sens direct du théorème sont mieux rédigées dans [GOZ], à mon avis.

**Corollaire 6.** Si  $\alpha \in \mathbb{R}$  est constructible, il existe  $e \in \mathbb{N}$  tel  $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2^e$ .

[GOZ]  
p. 52

*Démonstration.* Soit  $\alpha \in \mathbb{E}$ . D'après le théorème précédent, il existe une suite finie  $(L_0, \dots, L_p)$  de sous-corps de  $\mathbb{R}$  vérifiant :

- (i)  $L_0 = \mathbb{Q}$ .
- (ii)  $\forall i \in \llbracket 0, p-1 \rrbracket$ ,  $L_{i+1}$  est une extension quadratique (de degré 2) de  $L_i$ .
- (iii)  $\alpha \in L_p$ .

Par le théorème de la base télescopique,

$$[L_p : \mathbb{Q}] = 2^p$$

et par ce même théorème,

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

et en particulier,  $[\mathbb{Q}(\alpha) : \mathbb{Q}]$  est un diviseur de  $2^p$  : ce qu'on voulait. □

**Application 7** (Duplication du cube). Soit un cube de volume  $\mathcal{V}$  dont on suppose son arête  $a$  constructible. Il est impossible de dessiner, à la règle et au compas, l'arête d'un cube de volume  $2\mathcal{V}$ .

*Démonstration.* On a  $\mathcal{V} = a^3$  et donc  $2\mathcal{V} = 2a^3$ . L'arête d'un cube est la racine cubique de son volume. Il faut donc construire le nombre

$$\alpha = \sqrt[3]{2a^3} = a\sqrt[3]{2}$$

Le polynôme  $P = X^3 - 2$  est irréductible sur  $\mathbb{Q}$  (par le critère d'Eisenstein) et annule  $\alpha$  : c'est son polynôme minimal sur  $\mathbb{Q}$ . On a ainsi

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$$

donc  $\alpha$  n'est pas constructible par le Corollaire 6. □

# Bibliographie

## **Théorie de Galois**

[GOZ]

Ivan GOZARD. *Théorie de Galois. Niveau L3-M1*. 2<sup>e</sup> éd. Ellipses, 1<sup>er</sup> avr. 2009.

<https://www.editions-ellipses.fr/accueil/4897-15223-theorie-de-galois-niveau-l3-m1-2e-edition-9782729842772.html>.

## **Anneaux, corps, résultants**

[ULM18]

Felix ULMER. *Anneaux, corps, résultants. Algèbre pour L3/M1/agrégation*. Ellipses, 28 août 2018.

<https://www.editions-ellipses.fr/accueil/9852-20186-anneaux-corps-resultants-algebre-pour-l3-m1-agregation-9782340025752.html>.