Annexe

Extension de $\mathbb{Q}$ avec les nombres constructibles

D'après le mémoire de Master de Madame Barny

1 Points et nombres constructibles

1.1 Définitions

Il nous faut tout d'abord définir avec précision ce que l'on entend par point constructible à la règle et au compas.

Définition 1 *Soit P un plan euclidien et $\mathcal{B}$ un sous-ensemble fini de P ayant au moins 2 éléments. Les éléments de B sont appelés points de base.*

- *Un point M de P est dit constructible à la règle et au compas à partir de $\mathcal{B}$ s'il existe une suite finie de points de P se terminant par M: $M_1, \ldots, M_n = M$ telle que pour tout $1 \leq i \leq n$ M_i est un point d'intersection*
  - *soit de deux droites*
  - *soit d'une droite et d'un cercle*
  - *soit de deux cercles.*

  Ces droites et cercles étants obtenus à l'aide de l'ensemble

  $$E_i = \mathcal{B} \cap \{M_1, \ldots, M_{i-1}\}$$

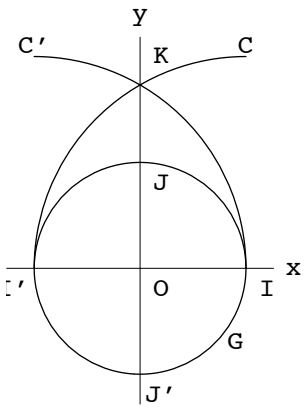
  de la façon suivante:

  - *chaque droite passe par 2 points distincts de E_i*
  - *chaque cercle est centré en un point de E_i et a pour rayon la distance entre deux points de E_i.*
- *Une droite passant par deux points constructibles est dite constructible*
- *Un cercle centr en un point constructible est ayant pour rayon la distance entre deux points constructibles est dit constructible.*

Il serait agréable de pouvoir repérer les points de P et en particulier les points constructibles. Pour cela, il nous faudrait un repère afin de pouvoir identifier les coordonnées.

Intéressons-nous au cas où l'ensemble $\mathcal{B}$ est le plus simple possible c'est-à-dire réduit à deux points de base que l'on notera O et I. Dans ce chapitre nous prendrons donc $\mathcal{B} = \{O, I\}$. Nous dirons simplement "constructible" pour dire "constructible à la règle et au compas à partir de B".

Nous allons mettre en évidence certains points constructibles. Considérons le cercle Γ de centre O et de rayon OI, il coupe la droite (OI) en un point noté I'. Considérons le cercle C de centre I et de rayon II' ainsi que le cercle C' de centre I' et de rayon II'. Désignons par K un point d'intersection de ces deux cercles. La droite (OK) est perpendiculaire à la droite (OI), elle coupe le cercle Γ en J et J'.



Sur cet exemple nous avons mis en évidence certains points constructibles: O, I, I', K, J, J' ainsi qu'un repère orthonormé (O, I, J) du plan P. Nous notons (Ox) et (Oy) les axes correspondants à ce repère. Grâce à lui, chaque point du plan P et notamment les points constructibles pourront être repérés par leurs coordonnées. Nous donnons la définition suivante:

Définition 2 *Un nombre réel est dit constructible si c'est une des coordonnées dans le repère (O, I, J) d'un point constructible.*

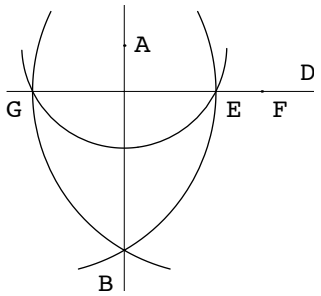
Par exemple, les nombres réels $0,\ -1,\ 1$ sont constructibles car ce sont les abscisses dans (O, I, J) des points constructibles $O,\ I,\ I'$. $\sqrt{3}$ est également constructible, c'est l'ordonnée dans (O, I, J) du point K. En effet, ce point a une abscisse nulle et se trouve sur le cercle C d'equation $(x-1)^2 + y^2 = 4$.

1.2 Résultats élémentaires

Afin de simplifier les constructions ultérieures, nous signalons ici quelques résultats élémentaires.

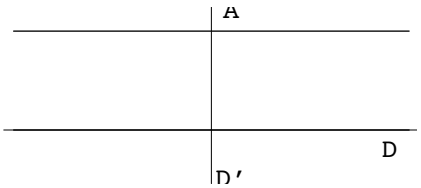
1. *Si D est une droite constructible et A un point constructible, la parallèle D passant par A est une droite constructible.*

La droite D étant constructible, elle contient au moins deux points constructibles E et F. Le cercle de centre A et de rayon AE coupe D en G. A partir de G et E comme centres, on construit les cercles de rayon GE qui se coupent en B. La droite AB est la perpendiculaire cherchée. (Cette construction suppose $A \neq E$, si $A = E$ on utilise F à la place de E.)



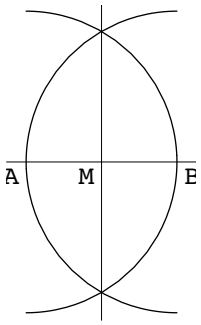
2. *Si D est une droite constructible et A un point constructible, la parallèle D passant par A est une droite constructible.*

   On utilise deux fois le résultat précédent. Une fois pour construire la perpendiculaire D' en A à D, une autre fois pour construire la perpendiculaire en A à D' qui est la droite cherchée.



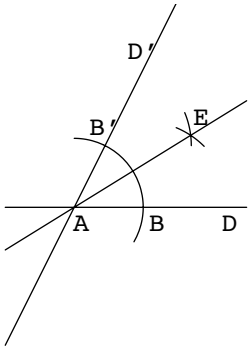
3. *Si A et B sont deux points constructibles, le milieu et la médiatrice du segment $[AB]$ sont constructibles.*

   Les cercles de centre A et B, de rayon AB permettent de construire la médiatrice du segment AB, celle-ci coupe la droite AB au milieu M du segment AB.



4. *Si D et D' sont deux droites constructibles concourantes, les bissectrices des angles déterminés par ces deux droites sont constructibles.*

   Si A est le point d'intersection de D et D', on considère le cercle de centre A et de rayon OI (par exemple) qui coupe D et D' en B et B'. Les cercles de centres B et B' et de rayon OI se coupent en E. La droite AE est une des bissectrices cherchées.

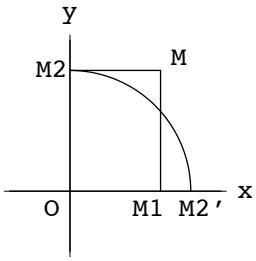


5. *Soit $t \in \mathbb{R}$, t est un nombre constructible si et seulement si le point de l'axe Ox d'abscisse t est constructible. (Même résultat en remplaçant Ox par Oy et abscisse par ordonnée.)*

   Si le point de l'axe Ox d'abscisse t est constructible, t est un nombre constructible par définition. Inversement, si t est un nombre constructible, c'est une des coordonnées d'un point constructible M. Les projections orthogonales M_1 et M_2 de M sur les axes de coordonnées sont des points constructibles d'après 1).

   (a) Si t est l'abscisse de M, c'est l'abscisse de M_1 et le résultat est établi.

   (b) Si t est l'ordonnée de M, c'est l'ordonnée de M_2, c'est aussi l'abscisse du point M_2' de Ox obtenu grâce au cercle de centre O et de rayon OM_2.



6. *Si A est un point constructible et t un nombre constructible, le cercle de centre A et de rayon $|t|$ est constructible.*

   Le point M de l'axe Ox d'abscisse t est constructible d'après 5). Ce cercle de centre A et de rayon $|t|$ est alors le cercle de centre A et de rayon OM.

1.3 Le corps des nombres constructibles

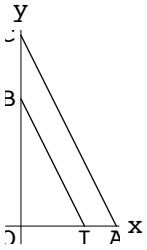
Théorème 1 *L'ensemble $\mathcal{C}$ des nombres constructibles est un sous-corps de $\mathbb{R}$ stable par racine carrée.*

Démonstration. Un sous-corps k de $\mathbb{R}$ est dit stable par racine carrée si pour tout α de k tel que $\alpha \geq 0$ on a $\sqrt{\alpha} \in k$. Nous savons déjà que 0 et 1, qui sont les abscisses de O et I, sont dans $\mathcal{C}$.

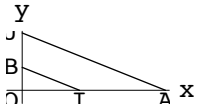
1. Si $u \in \mathcal{C}$ alors $-u \in \mathcal{C}$. En effet, si A est le point de l'axe Ox d'abscisse u, en utilisant le cercle de centre O passant par A on construit le point A' de Ox d'abscisse $-u$.

2. Si u et v sont dans $\mathcal{C}$ alors $u+v \in \mathcal{C}$. En effet, soit, A et B les points de l'axe Ox tels que $\overline{OA} = u$ et $\overline{AB} = v$. A est constructible d'après 5) et B est constructible d'après 6) en utilisant le cercle de centre A et de rayon $|v|$. On a $\overline{ON} = u + v$ et ainsi $u + v \in \mathcal{C}$.

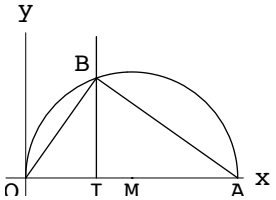
3. Si u et v sont dans $\mathcal{C}$ alors $uv \in \mathcal{C}$. Ecartons le cas trivial où $uv = 0$; soit A sur Ox tel que $\overline{OA} = u$ et B sur Oy tel que $\overline{OB} = v$. La parallèle à IB passant par A coupe Oy en C. D'après Thalès, on a $\frac{\overline{OC}}{\overline{OB}} = \frac{\overline{OA}}{\overline{OI}}$, d'où $\overline{OC} = uv$.



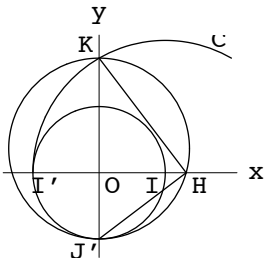
4. Si $u \in \mathcal{C}$, $u \neq 0$, alors $\frac{1}{u} \in \mathcal{C}$. En effet, soit A sur Ox tel que $\overline{OA} = u$. La parallèle à AJ passant par I coupe Oy en B. D'après Thalès on a: $\frac{\overline{OB}}{\overline{OJ}} = \frac{\overline{OI}}{\overline{OA}}$ d'où $\overline{OB} = \frac{1}{u}$.



5. Si $u \in \mathcal{C}$, $u \geq 0$, alors $\sqrt{u} \in \mathcal{C}$. Supposons $u > 0$, soit A le point de l'axe Ox tel que $\overline{IA} = u$, soit M le milieu du segment OA; la perpendiculaire en I à Ox coupe le cercle de centre M et de rayon OM en un point B d'ordonnée positive. le triangle OBA étant rectangle nous avons $IB^2 = OI.IA$; ainsi $IB = \sqrt{u}$ et $\sqrt{u}$ est l'ordonnée du point constructible B.



Remarques. Rappelons que $\mathbb{Q}$ est le plus petit sous-corps de $\mathbb{R}$. En effet, si k est un sous-corps de $\mathbb{R}$, on a $1 \in k$, la stabilité de k par l'addition nous donne $\mathbb{N} \subset k$, la stabilité pour l'opposé nous donne $\mathbb{Z} \subset k$, et la stabilité pour le produit et l'inverse nous donne $\mathbb{Q} \subset k$. Il en résulte que l'on a $\mathbb{Q} \subset \mathcal{C} \subset \mathbb{R}$. Sachant que le corps $\mathcal{C}$ contient $\mathbb{Q}$ et est stable par racine carrée, nous pouvons donner de nombreux exemples de nombres constructibles: $-\frac{2}{3}$, $\sqrt{2}$, $\sqrt[4]{3}$, $\frac{2+3\sqrt{2}+\sqrt{5}}{\sqrt{3}}$. De plus, en utilisant les constructions faites dans la démonstration du théorème précédent, on peut effectivement construire à la règle et au compas les points de l'axe Ox ayant pour abscisses les nombres précédents.
A titre d'exemple, construisons le point de l'axe Ox d'abscisse $\sqrt[4]{3}$. Il nous faut d'abord faire apparaître $\sqrt{3}$. On peut pour cela utiliser la dernière construction du théorème, on peut également remarquer en utilisant la figure du 1.1) que $OK = \sqrt{3}$. (On applique le théorème de Pythagore dans le triangle $I'OK$: $I'K^2 = I'O^2 + OK^2$). La dernière construction du théorème nous invite alors à considérer le cercle de centre le milieu du segment $[J'K]$ et de diamètre $J'K$ qui coupe l'axe Ox au point d'abscisse positive H tel que $OH^2 = OK.OJ'$ d'où $OH = \sqrt[4]{3}$.



2 Caractérisation des nombres constructibles: le résultat de Wantzel.

C'est en 1837 que P.L. Wantzel caractérisa les nombres réels constructibles. Nous donnons ici cette caractérisation sous une forme un peu plus moderne.
(O, I, J) désigne toujours le repère orthonormé du plan euclidien P, construit à partir des points de base O et I. Si M est un point de coordonnées x et y dans ce repère, on note $M(x, y)$.

Lemme 1 *1. Si D est une droite de P passant par les points distincts $A(a_1, a_2)$ et $B(b_1, b_2)$ alors D a une équation de la forme $\alpha x + \beta y + \gamma = 0$ avec $\alpha, \beta, \gamma \in \mathbb{Q}(a_1, a_2, b_1, b_2)$.*

2. Soient $A(a_1, a_2)$, $B(b_1, b_2)$, $C(c_1, c_2)$ des points de P; le cercle de centre A et de rayon BC a une équation de la forme $x^2 + y^2 - 2\alpha x - 2\beta y + \gamma = 0$ avec $\alpha, \beta, \gamma \in \mathbb{Q}(a_1, a_2, b_1, b_2, c_1, c_2)$.

Démonstration.
1. Si $a_1 = b_1$, D a pour équation $x - a_1 = 0$, sinon, D a pour équation $y - a_2 = (x - a_1)\frac{b_2 - a_2}{b_1 - a_1}$ qui se met sous la forme $\alpha x + \beta y + \gamma = 0$ avec $\alpha, \beta, \gamma \in \mathbb{Q}(a_1, a_2, b_1, b_2)$.

2. Le cercle de centre A et de rayon BC a pour équation: $(x-a_1)^2+(y-a_2)^2=(c_1-b_1)^2+(c_2-b_2)^2$ qui se met sous la forme $x^2+y^2-2\alpha x-2\beta y+\gamma=0$ avec $\alpha,\beta,\gamma\in\mathbb{Q}(a_1,a_2,b_1,b_2,c_1,c_2)$.

Théorème 2 *Soit $t\in\mathbb{R}$; t est un nombre constructible si et seulement si il existe un entier $p\geq 1$ et une suite de sous-corps de $\mathbb{R}$, $L_1,L_2,\ldots,L_p$, tels que:*

- $L_1=\mathbb{Q}$
- *pour* $1\leq j\leq p-1\quad L_j\subset L_{j+1}$ *et* $[L_{j+1},L_j]=2$
- $t\in L_p$

Démonstration.

- Si t est constructible, t est l'abscisse d'un point constructible M de l'axe Ox.

  Soit $M_1,M_2,\ldots,M_n=M$ la suite des points successivement construits pour obtenir M. On peut supposer que M_1 et M_2 sont les points de base O et I. Par exemple, pour construire J au 1.1) la suite de points était O,I,I',K,J. Pour $i=1,2,\ldots,n$, appelons x_i et y_i les coordonnées dans (O,I,J) du point M_i. On a en particulier: $x_1=y_1=0,\ x_2=1,\ y_2=0,\ x_n=t,\ y_n=0$.Posons

  $K_1=\mathbb{Q}(x_1,y_1)$

  $K_2=\mathbb{Q}(x_1,y_1,x_2,y_2)$

  $\ldots$

  $K_i=\mathbb{Q}(x_1,y_1,\ldots,x_i,y_i)$

  $\ldots$

  $K_n=\mathbb{Q}(x_1,y_1,\ldots,x_n,y_n)$.

  On a $K_1\subset K_2\subset\ldots\subset K_i\subset K_{i+1}\subset\ldots\subset K_n,\ K_1=K_2=\mathbb{Q},\ t=x_n\in K_n$. Nous allons établir que pour tout $i=1,2,\ldots,n-1\quad K_{i+1}=K_i$ ou $[K_{i+1},K_i]=2$. Le résultat est évident pour $i=1$ car $K_1=K_2=\mathbb{Q}$. Supposons donc $i\geq 2$. Trois cas se présentent pour le point M_{i+1} suivant qu'il est à l'intersection de deux droites, d'une droite et d'un cercle ou de deux cercles définis par les points précédents $M_1,\ldots,M_i$. Mais d'après le lemme précédent, ces droites et ces cercles ont des équations à coefficients dans $K_i=\mathbb{Q}(x_1,y_1,\ldots,x_i,y_i)$.

  1. Si M_{i+1} est à l'intersection de deux droites, x_{i+1} et y_{i+1} sont alors solutions d'un système de la forme $\left\{\begin{array}{l}\alpha x+\beta y+\gamma=0\\ \alpha' x+\beta' y+\gamma'=0\end{array}\right.$ avec $\alpha,\beta,\gamma,\alpha',\beta',\gamma'$ dans K_i. En résolvant ce système du 1$^{\text{er}}$ degré on constate que x_{i+1} et y_{i+1} sont aussi dans K_i, d'où $K_{i+1}=K_i(x_{i+1},y_{i+1})=K_i$.
  2. Si M_{i+1} est à l'intersection d'une droite et d'un cercle, x_{i+1} et y_{i+1} sont alors solutions d'un système de la forme $\left\{\begin{array}{l}\alpha x+\beta y+\gamma=0\\ x^2+y^2-2\alpha' x-2\beta' y+\gamma'=0\end{array}\right.$ avec $\alpha,\beta,\gamma,\alpha',\beta',\gamma'$ dans K_i.
     - Si $\beta\neq 0$, on a $y=-\frac{1}{\beta}(\alpha x+\gamma)$ que l'on reporte dans la seconde équation pour former l'équation aux abscisses. Cette équation est du second degré à coefficients dans $\mathbb{K}_i$ et x_{i+1} est racine de cette équation.

∗ si $x_{i+1} \in K_i$ alors $y_{i+1} = -\frac{1}{\beta}(\alpha\ x_{i+1} + \gamma) \in K_i$ et $K_{i+1} = K_i$

∗ si $x_{i+1} \notin K_i$ alors x_{i+1} est algébrique sur K_i et de degré 2 et on a:

$$K_{i+1} = K_i(x_{i+1}, y_{i+1}) = K_i(x_{i+1}) \text{ et } [K_{i+1}, K_i] = 2.$$

– Si $\beta = 0$, alors $\alpha \neq 0$, on procède de même en formant l'équation aux ordonnées.

3. Si M_{i+1} est à l'intersection de deux cercles, x_{i+1} et y_{i+1} sont alors solutions d'un système de la forme $\begin{cases} x^2 + y^2 - 2\alpha x - 2\beta y + \gamma = 0 \\ x^2 + y^2 - 2\alpha' x - 2\beta' y + \gamma' = 0 \end{cases}$ avec $\alpha, \beta, \gamma, \alpha', \beta', \gamma'$ dans K_i. Ce système est équivalent au système $\begin{cases} x^2 + y^2 - 2\alpha x - 2\beta y + \gamma = 0 \\ 2(\alpha - \alpha')x + 2(\beta - \beta')y - (\gamma - \gamma') = 0 \end{cases}$ et on est ainsi ramené au cas précédent.

Nous avons ainsi construit une suite de sous-corps de $\mathbb{R}$: $K_1 \subset K_2 \subset \ldots \subset K_n$ telle que $K_1 = \mathbb{Q}$, $t \in K_n$ et pour $1 \leq i \leq n-1$ $K_{i+1} = K_i$ ou $[K_{i+1}, K_i] = 2$. Nous pouvons rendre cette suite strictement croissante en supprimant les corps superflus. On obtient alors une suite $L_1 \subset L_2 \subset \ldots \subset L_p$ avec $L_1 = \mathbb{Q}$, $t \in L_p$ et pour $1 \leq j \leq p-1$ $[L_{j+1}, L_j] = 2$.

- Réciproquement, supposons que $L_1 \subset L_2 \subset \ldots \subset L_p$ soit une suite de sous-corps de $\mathbb{R}$ vérifiant les conditions du théorème. Nous allons montrer par récurrence sur j $1 \leq j \leq p$ que $L_j \subset \mathcal{C}$. Il en résultera bien que t est un nombre constructible.

  – $L_1 \subset \mathcal{C}$ car on a $L_1 = \mathbb{Q}$ et on sait que $\mathbb{Q} \subset \mathcal{C}$.

  – Supposons que $L_j \subset \mathcal{C}$ et montrons que $L_{j+1} \subset \mathcal{C}$. Soit $a \in L_{j+1}$. La famille $1, a, a^2$ est liée sur L_j car $[L_{j+1}, L_j] = 2$, il existe donc α, β, γ dans L_j non tous nuls tels que $\alpha a^2 + \beta a + \gamma = 0$.

  ∗ si $\alpha = 0$ alors $a = -\frac{\gamma}{\beta} \in L_j \subset \mathcal{C}$

  ∗ si $\alpha \neq 0$ alors $a = \frac{-\beta \pm \sqrt{\beta^2 - 4\alpha\gamma}}{2\alpha}$ et $a \in \mathcal{C}$ car $\mathcal{C}$ est un corps stable par racine carrée comme nous l'avons démontré au théorème 1.□

Nous allons nous intéresser plus particulièrement à une corollaire de ce théorème. C'est ce corollaire qui nous permettra de répondre facilement aux trois problèmes grecs que nous étudierons au chapitre suivant. Afin de pouvoir y faire référence facilement, nous appelerons ce corollaire "le résultat de Wantzel".

Théorème 3 *Tout nombre constructible est algébrique sur $\mathbb{Q}$ et son degré est une puissance de 2.*

Si $t \in \mathbb{R}$ est constructible, d'après le théorème précédent il existe une suite de sous-corps de $\mathbb{R}$, $L_1 \subset L_2 \subset \ldots L_p$ telle que $L_1 = \mathbb{Q}$, $t \in L_p$ et pour $1 \leq j \leq p-1$ $[L_{j+1}, L_j] = 2$. On a donc

$$[L_p, \mathbb{Q}] = [L_p, L_{p-1}] \times [L_{p-1}, L_{p-2}] \times \ldots \times [L_2, \mathbb{Q}] = 2^{p-1}.$$

On a aussi $\mathbb{Q} \subset \mathbb{Q}(t) \subset L_p$, d'où $2^{p-1} = [L_p, \mathbb{Q}] = [L_p, \mathbb{Q}(t)] \times [\mathbb{Q}(t), \mathbb{Q}]$. Nous retenons de ceci que $[\mathbb{Q}(t), \mathbb{Q}]$ est un diviseur de 2^{p-1}, c'est donc une puissance de 2 que nous notons 2^q. Considérons la famille $1, t, t^2, \ldots, t^{2^q}$, c'est donc une famille à $2^q + 1$éléments, elle est donc liée dans le $\mathbb{Q}$-espace vectoriel $\mathbb{Q}(t)$, il existe alors $\alpha_0, \alpha_1, \ldots, \alpha_{2^q}$ dans $\mathbb{Q}$ non tous nuls tels que $\alpha_0 + \alpha_1 t + \ldots + \alpha_{2^q} t^{2^q} = 0$. Ceci montre que t est algébrique sur $\mathbb{Q}$ et le degré de t sur $\mathbb{Q}$ est $[\mathbb{Q}(t), \mathbb{Q}] = 2^q$.□

Le résultat de Wantzel est très utile pour montrer qu'un nombre réel n'est pas constructible. Donnons quelques exemples.

Nous avons démontré dans le chapitre 1 que π n'était pas algébrique sur $\mathbb{Q}$. Il en résulte que π n'est pas un nombre constructible.

Considérons le polynôme X^3-2, si ce polynôme se décomposait dans $\mathbb{Q}[X]$, un des facteurs de la décomposition serait du premier degré et ainsi le polynôme aurait une racine dans $\mathbb{Q}$. Ceci n'est pas possible car les racines du polynôme $\sqrt[3]{2}, j\sqrt[3]{2}, -j^2\sqrt[3]{2}$ ne sont pas dans $\mathbb{Q}$. Ainsi X^3-2 est irréductible dans $\mathbb{Q}[X]$ et c'est donc le polynôme minimal de $\sqrt[3]{2}$ sur $\mathbb{Q}$. Il en résulte que $\sqrt[3]{2}$ est algébrique sur $\mathbb{Q}$ et de degré 3. Compte tenu du résultat de Wantzel, $\sqrt[3]{2}$ n'est pas un nombre constructible.

On peut se demander si la réciproque du résultat de Wantzel est exacte. A savoir, si t est un nombre réel algébrique sur $\mathbb{Q}$ dont le degré est une puissance de 2, est-il constructible?
Nous allons donner un contre-exemple montrant que cette réciproque est fausse. Nous considérons pour cela le polynôme $P(x)=x^4-x-1$. Nous allons démontrer que ce polynôme est irréductible dans $\mathbb{Q}[x]$ et qu'il possède une racine réelle non constructible. Cette racine sera alors un exemple de nombre réel algébrique sur $\mathbb{Q}$ et de degré 4 qui n'est pas constructible.
$P(x)$ se décompose dans $\mathbb{R}[x]$ en un produit de deux polynômes du second degré

$$x^4-x-1=(x^2+ax+b)(x^2+a'x+b'),\quad a,b,a',b'\in\mathbb{R}$$

avec $\left\{\begin{array}{l} a+a'=0\\ b+b'+aa'=0\\ ab'+a'b=-1\\ bb'=-1\end{array}\right.$ $\left\{\begin{array}{l} a=-a'\\ b+b'=a^2\\ a(b'-b)=-1\\ bb'=-1\end{array}\right.$ b et b' sont alors racines de $t^2-a^2t-1=0$.

a et a' sont opposés, on peut donc supposer par exemple $a>0$ d'où $b'<b$, on a alors: $\left\{\begin{array}{l} b=\frac{a^2+\sqrt{a^4+4}}{2}\\ b'=\frac{a^2-\sqrt{a^4+4}}{2}\end{array}\right.$

et $b'-b=-\sqrt{a^4+4}$, $\quad a\sqrt{a^4+4}=1$.

- Le polynôme x^2+ax+b a pour discriminant

  $$\Delta_1=a^2-4b=a^2-2(a^2+\sqrt{a^4+4})=-a^2-2\sqrt{a^4+4}<0.$$

  Il a donc 2 racines complexes conjuguées.

- Le polynôme $x^2+a'x+b'$ a pour discriminant

  $$\Delta_2=a'^2-4b'=a^2-2(a^2-\sqrt{a^4+4})=-a^2+2\sqrt{a^4+4}>0.$$

  Il a donc deux racines réelles notées α et β.

- A partir de $a\sqrt{a^4+4}=1$, on obtient $a^2(a^4+4)=1$ et ainsi a^2 est racine du polynôme t^3+4t-1. Il est facile de vérifier que ce polynôme n'a pas de racine dans $\mathbb{Q}$ et ainsi il est irréductible dans $\mathbb{Q}[x]$. Ainsi a^2 est algébrique sur $\mathbb{Q}$ et de degré 3. Le résultat de Wantzel nous dit alors que a^2 n'est pas un nombre constructible d'où il résulte que a n'est pas non plus un nombre constructible.

- On a $\alpha+\beta=-a'=a$. Comme a n'est pas constructible on peut affirmer que l'une au moins des racines α et β n'est pas constructible. Ainsi le polynôme $P(x)$ possède au moins une racine réelle non constructible. Il nous reste à établir que ce polynôme est irréductible dans $\mathbb{Q}[x]$.

- a n'étant pas constructible, n'est pas dans $\mathbb{Q}$ et la décomposition $P(x) = (x^2+ax+b)(x^2+a'x+b')$ n'est pas une décomposition dans $\mathbb{Q}[x]$. Comme de plus le polynôme $x^2 + ax + b$ n'a pas de racine réelle aucune décomposition de $P(x)$ ne peut se faire dans $\mathbb{Q}[x]$. $P(x)$ est donc irréductible dans $\mathbb{Q}[x]$.