La règle et le compas

Vidéo ■ partie 1. Constructions
Vidéo ■ partie 2. Nombres constructibles
Vidéo ■ partie 3. Éléments de théorie des corps
Vidéo ■ partie 4. Corps et nombres constructibles
Vidéo ■ partie 5. Applications aux problèmes grecs

Vous avez à votre disposition une règle et un compas et bien sûr du papier et un crayon ! Avec si peu de matériel s'ouvre à vous un monde merveilleux rempli de géométrie et d'algèbre.

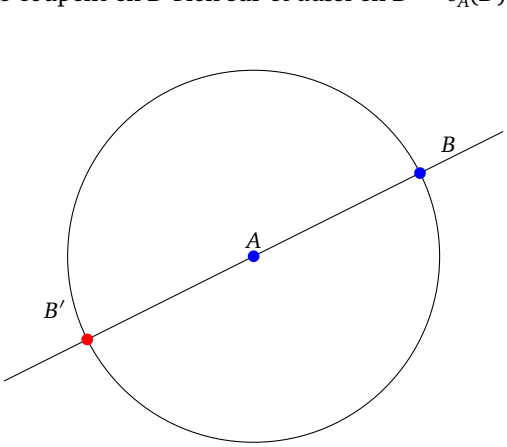
1. Constructions et les trois problèmes grecs

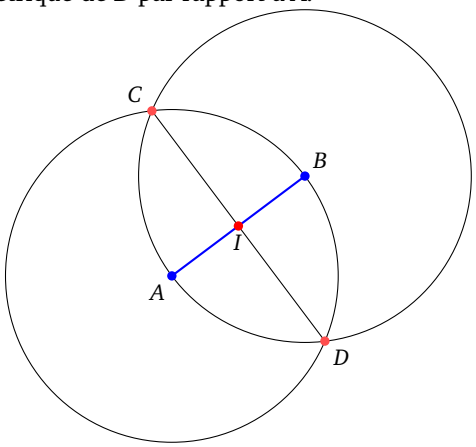
Nous allons voir dans cette première partie que tout un tas de constructions sont possibles. Mais le but de ce cours est de répondre à trois problèmes qui datent des mathématiciens grecs : la trisection des angles, la duplication du cube ainsi que le célèbre problème de la quadrature du cercle.

1.1. Premières constructions géométriques

Nous avons à notre disposition un compas et une règle (non graduée). On démarre par des constructions élémentaires.

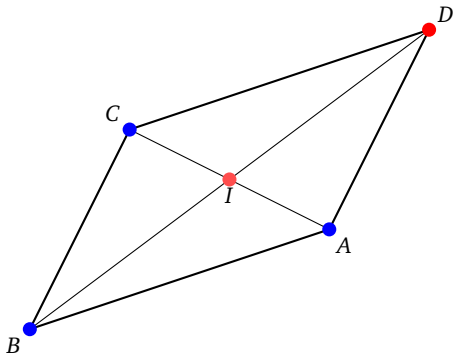
- Si A, B sont deux points donnés du plan, alors on peut construire, à la règle et au compas, le ***symétrique*** de B par rapport à A. Pour cela, il suffit juste de tracer la droite (AB) et le cercle de centre A passant par B. Cette droite et ce cercle se coupent en B bien sûr et aussi en $B' = s_A(B)$, le symétrique de B par rapport à A.

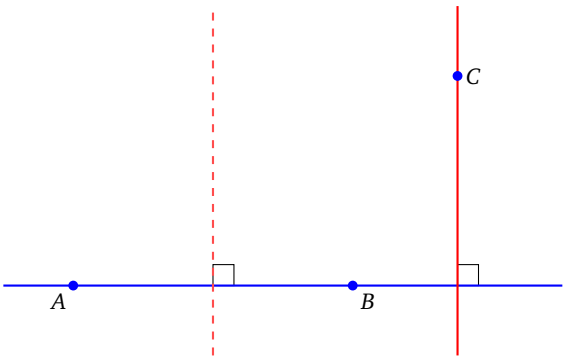




- Si A, B sont deux points donnés du plan, alors on peut construire la ***médiatrice*** de $[AB]$. Pour cela, tracer le cercle centré en A passant par B et aussi le cercle centré en B passant par A. Ces deux cercles s'intersectent en deux points C, D. Les points C, D appartiennent à la médiatrice de $[AB]$. Avec la règle on trace la droite (CD) qui est la médiatrice de $[AB]$.
- En particulier cela permet de construire le ***milieu*** I du segment $[AB]$. En effet, c'est l'intersection de la droite (AB) et de la médiatrice (CD) que l'on vient de construire.

- Si A, B, C sont trois points donnés alors on peut construire la ***parallèle*** à la droite (AB) passant par C. Tout d'abord construire le milieu I de $[AC]$. Puis construire D le symétrique de B par rapport à I. La figure $ABCD$ est un ***parallélogramme***, donc la droite (CD) est bien la parallèle à la droite (AB) passant par C.



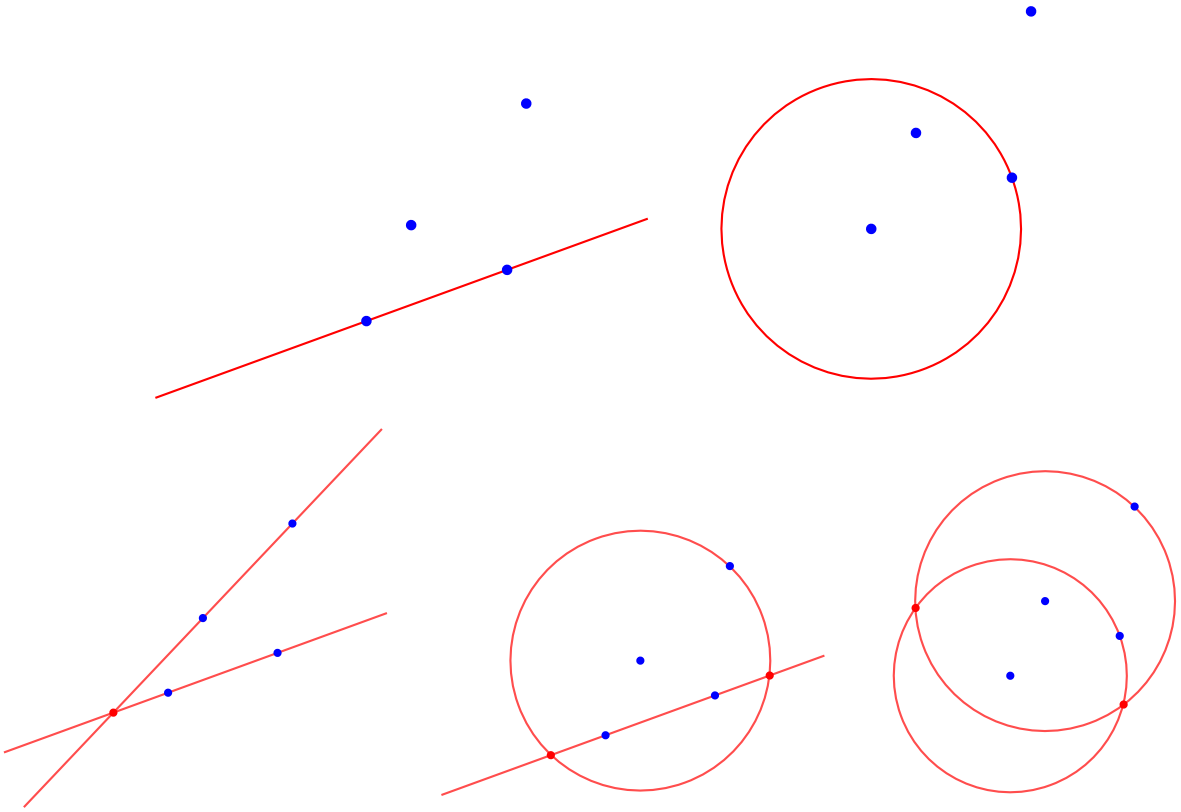


- Pour construire la ***perpendiculaire*** à (AB) passant par un point C, on construit d'abord deux points de la médiatrice de $[AB]$, puis la parallèle à cette médiatrice passant par C.

1.2. Règles du jeu

Il est peut-être temps d'expliquer ce que l'on est autorisé à faire. Voici les règles du jeu : partez de points sur une feuille. Vous pouvez maintenant tracer d'autres points, à partir de cercles et de droites en respectant les conditions suivantes :

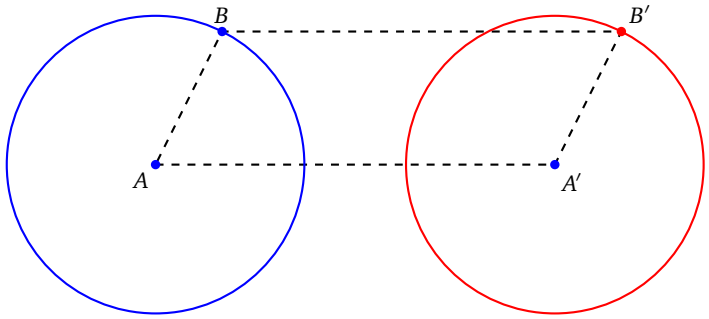
- vous pouvez tracer une droite entre deux points déjà construits,
- vous pouvez tracer un cercle dont le centre est un point construit et qui passe par un autre point construit,
- vous pouvez utiliser les points obtenus comme intersections de deux droites tracées, ou bien intersections d'une droite et d'un cercle tracé, ou bien intersections de deux cercles tracés.



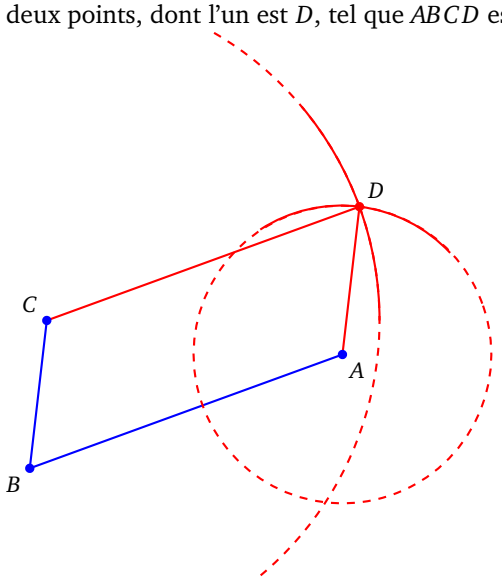
- Une remarque importante : la règle est une règle simple, qui n'est pas graduée.
- Convention pour les couleurs : les points donnés à l'avance sont les points bleus. Les constructions se font en rouge (rouge pâle pour les constructions qui viennent en premier, rouge vif pour les constructions qui viennent en dernier).

1.3. Conserver l'écartement du compas

- On peut ***conserver l'écartement du compas***. C'est une propriété importante qui simplifie les constructions.
  Si l'on a placé des points A, B, A' alors on peut placer la pointe en A avec un écartement de longueur AB. C'est-à-dire que l'on peut mesurer le segment $[AB]$, puis soulever le compas en gardant l'écartement pour tracer le cercle centré en A' et d'écartement AB.
  Cette opération se justifie de la façon suivante : on pourrait construire le point B' tel que $A'ABB'$ soit un parallélogramme et ensuite tracer le cercle centré en A' passant par B'.



- En conservant l'écartement du compas, nous pouvons plus facilement construire les parallélogrammes, avec seulement deux traits de compas. Donnons-nous trois points A, B, C. On mesure l'écartement $[AB]$, on trace le cercle centré en C de rayon AB. Puis on mesure l'écartement $[BC]$ et on trace le cercle centré en A de rayon BC. Ces deux cercles se recoupent en deux points, dont l'un est D, tel que $ABCD$ est un parallélogramme.

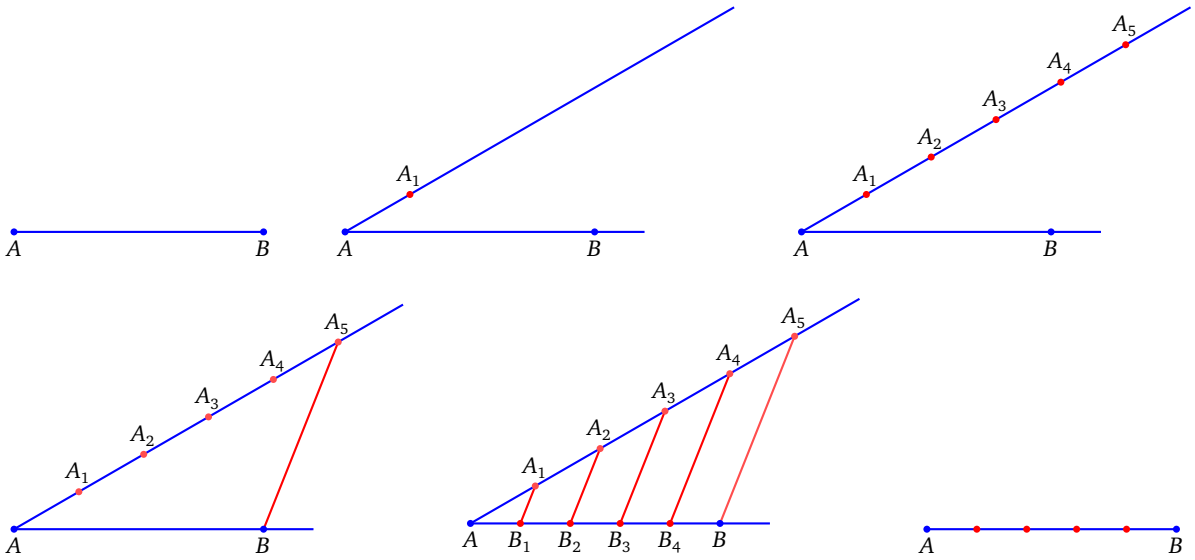


1.4. Thalès et Pythagore

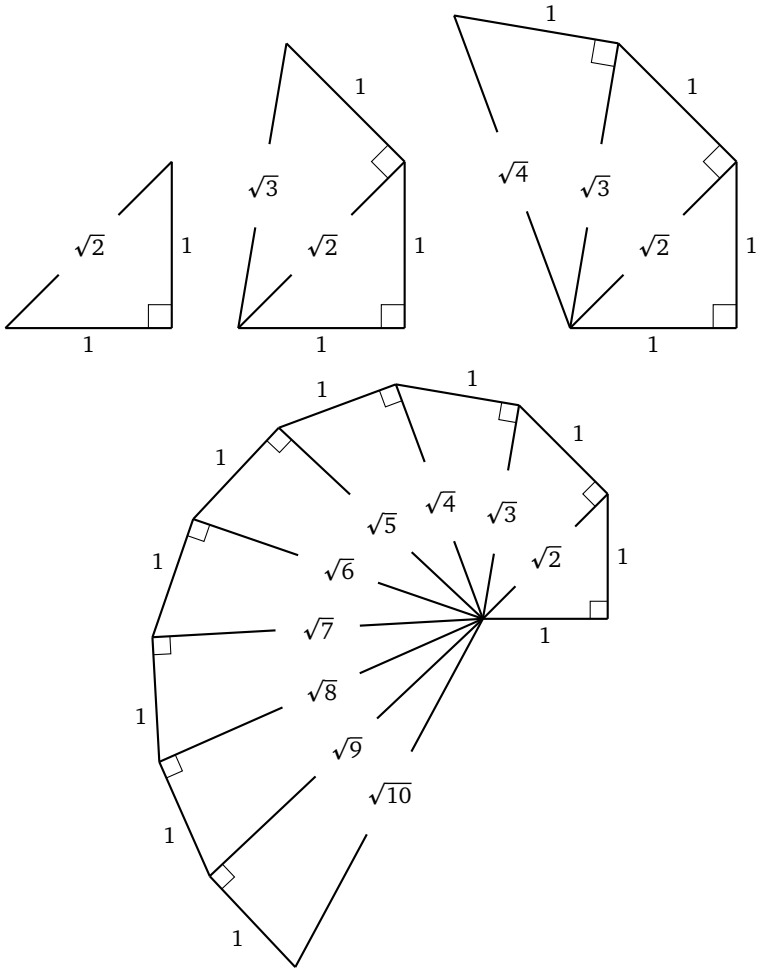
Voyons comment le théorème de Thalès nous permet de diviser un segment en n morceaux.
Fixons n un entier. Voici les étapes pour diviser un segment $[AB]$ en n parts égales.

1. Tracer une droite $\mathscr{D}$ quelconque, passant par A, autre que la droite (AB).
2. Prendre un écartement quelconque du compas. Sur la droite $\mathscr{D}$ et en partant de A, tracer n segments de même longueur. On obtient des points $A_1, A_2, \ldots, A_n$.
3. Tracer la droite (A_nB). Tracer les parallèles à cette droite passant par A_i. Ces droites recoupent le segment $[AB]$ en des points $B_1, B_2, \ldots, B_{n-1}$ qui découpent l'intervalle $[AB]$ en n segments égaux.

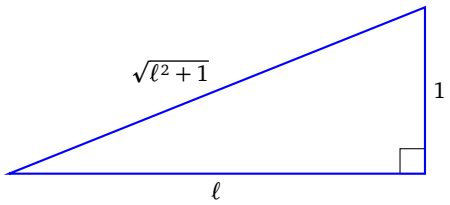
Cette construction fonctionne grâce au théorème de Thalès.



Voyons maintenant comment le théorème de Pythagore va nous permettre de faire apparaître des racines carrées. Supposons que l'on parte d'un segment de longueur 1. Il est facile de construire un segment de longueur $\sqrt{2}$: c'est la longueur de la diagonale du carré de côté 1. Repartons du segment diagonal de longueur $\sqrt{2}$: on construit un triangle rectangle avec un côté de longueur 1, et l'hypoténuse a alors pour longueur $\sqrt{3}$ (voir le calcul plus bas). Repartant de ce segment, on construit un « escargot » avec des segments de longueurs $\sqrt{4}$, $\sqrt{5}$...



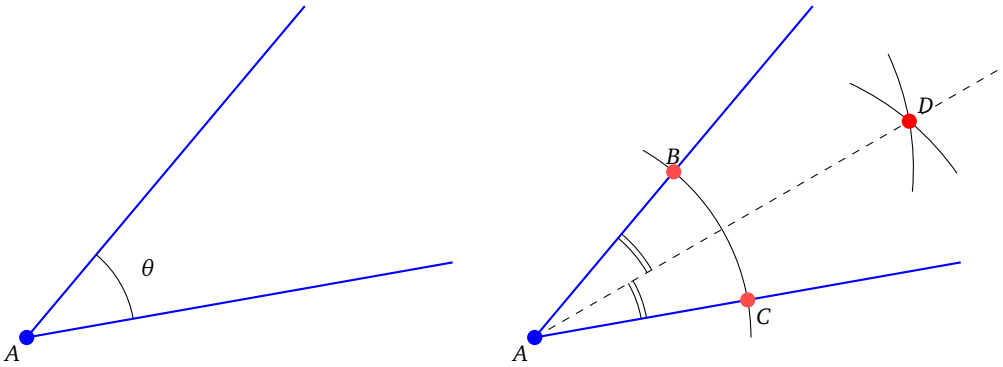
Tout ceci se justifie par le théorème de Pythagore : dans un triangle rectangle ayant un côté de longueur ℓ et un autre de longueur 1, l'hypoténuse est de longueur $\sqrt{\ell^2+1}$. En partant de $\ell_1 = 1$, on trouve $\ell_2 = \sqrt{\ell_1^2+1} = \sqrt{2}$, puis $\ell_3 = \sqrt{\ell_2^2+1} = \sqrt{3}$, $\ell_4 = \sqrt{4} = 2$, et plus généralement $\ell_n = \sqrt{n}$.



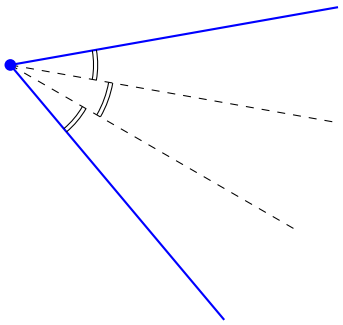
Voici maintenant trois questions qui datent de la Grèce antique et qui vont nous occuper le reste du chapitre.

1.5. La trisection des angles

Considérons un angle θ, c'est-à-dire la donnée d'un point A et de deux demi-droites issues de ce point. Nous savons diviser cet angle en deux à l'aide d'une règle et d'un compas : il suffit de tracer la bissectrice. Pour cela on fixe un écartement de compas et on trace un cercle centré en A : il recoupe les demi-droites en des points B et C. On trace maintenant deux cercles centrés en B puis C (avec le même rayon pour les deux cercles). Si D est un point de l'intersection de ces deux cercles alors la droite (AD) est la bissectrice de l'angle.

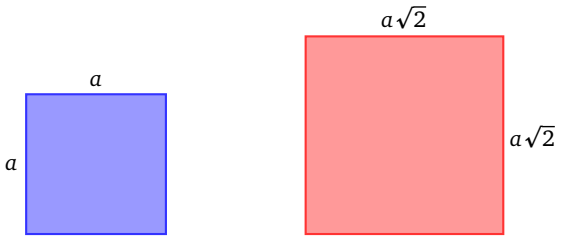


Problème de la trisection. Peut-on diviser un angle donné en trois angles égaux à l'aide de la règle et du compas ?



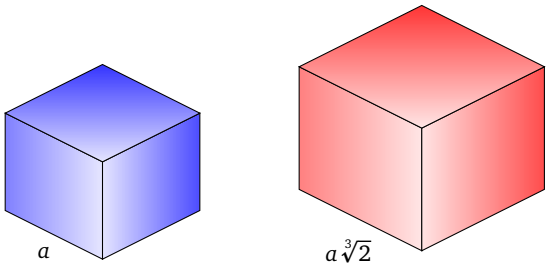
1.6. La duplication du cube

Commençons par un problème assez simple : étant donné un carré, construire (à la règle et au compas) un carré dont l'aire est le double. C'est facile, car cela revient à savoir tracer un côté de longueur $a\sqrt{2}$ à partir d'un côté de longueur a. En fait la diagonale de notre carré original a la longueur voulue $a\sqrt{2}$. Partant de cette longueur, on construit un carré dont l'aire est $(a\sqrt{2})^2 = 2a^2$: son aire est bien le double de celle du carré de départ.



$S = a^2$ $S = 2a^2$

Posons nous la question dans l'espace : étant donné un cube, peut-on construire un second cube dont le volume est le double de celui du premier ? Si le premier cube a ses côtés de longueur a, alors le second doit avoir ses côtés de longueur $a\sqrt[3]{2}$. La question se formule alors de la manière suivante :

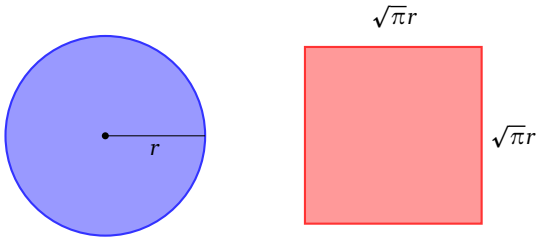


$V = a^3$ $V = 2a^3$

Problème de la duplication du cube. Étant donné un segment de longueur 1, peut-on construire à la règle et au compas un segment de longueur $\sqrt[3]{2}$?

1.7. La quadrature du cercle

Problème de la quadrature du cercle. Étant donné un cercle, peut-on construire à la règle et au compas un carré de même aire ?



$S = \pi r^2$ $S = \pi r^2$

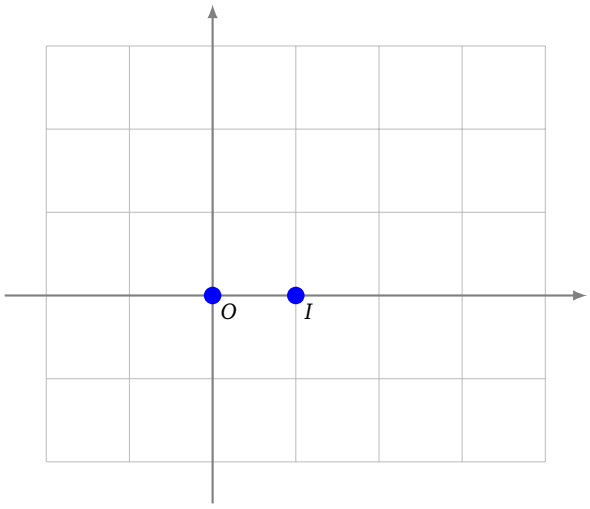
Cela revient à construire un segment de longueur $\sqrt{\pi}$ à la règle et au compas, à partir d'un segment de longueur 1.

2. Les nombres constructibles à la règle et au compas

Pour résoudre les trois problèmes grecs, il va falloir les transformer complètement. D'une question géométrique nous allons passer à une question algébrique. Dans cette partie on ramène le problème de la construction de points dans le plan à la construction de points sur la droite numérique réelle.

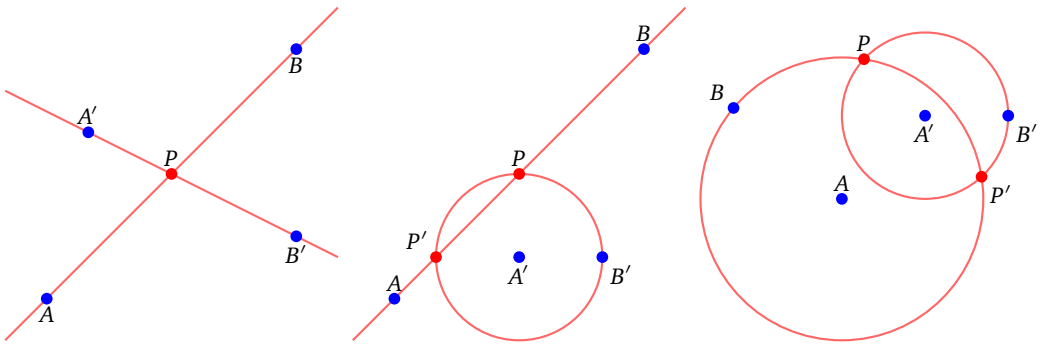
2.1. Nombre constructible

On considère le plan euclidien $\mathscr{P}$ muni d'un repère orthonormé, que l'on identifiera à $\mathbb{R}^2$ (ou $\mathbb{C}$). On définit des ensembles de points $\mathscr{C}_i \subset \mathscr{P}$ par récurrence.

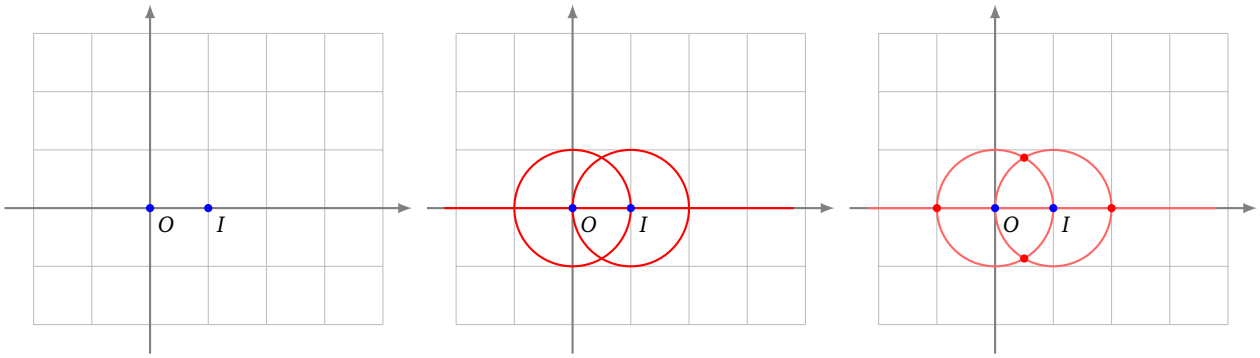


- On se donne au départ seulement deux points : $\mathscr{C}_0 = \{O, I\}$ où $O = (0,0)$ et $I = (1,0)$.
- Fixons $i \geqslant 0$, et supposons qu'un certain ensemble de points $\mathscr{C}_i$ soit déjà construit. Alors on définit $\mathscr{C}_{i+1}$ par récurrence, comme l'ensemble des ***points élémentairement constructibles*** à partir de $\mathscr{C}_i$. C'est-à-dire : $P \in \mathscr{C}_{i+1}$ si et seulement si
  0. $P \in \mathscr{C}_i$
  1. ou $P \in (AB) \cap (A'B')$ avec $A, B, A', B' \in \mathscr{C}_i$,
  2. ou $P \in (AB) \cap \mathscr{C}(A', A'B')$ avec $A, B, A', B' \in \mathscr{C}_i$,
  3. ou $P \in \mathscr{C}(A, AB) \cap \mathscr{C}(A', A'B')$ avec $A, B, A', B' \in \mathscr{C}_i$.

On a noté $\mathscr{C}(A, r)$ le cercle de centre A et de rayon r.
Il faut comprendre cette construction ainsi : si A, B, A', B' ont été construits et sont dans $\mathscr{C}_i$ alors, à partir de ces points, on peut tracer plusieurs objets à la règle et au compas : par exemple la droite (AB) – à l'aide de la règle – ou le cercle de centre A' et de rayon de longueur $A'B'$ en plaçant la pointe du compas en A' avec un écartement faisant passer le cercle par B'. Si cette droite (AB) et ce cercle $\mathscr{C}(A', A'B')$ s'intersectent alors les points d'intersection sont par définition dans $\mathscr{C}_{i+1}$.
Voici les trois situations possibles. Les points A, B, A', B' en bleu sont dans $\mathscr{C}_i$, et les points P en rouge sont dans $\mathscr{C}_{i+1}$.



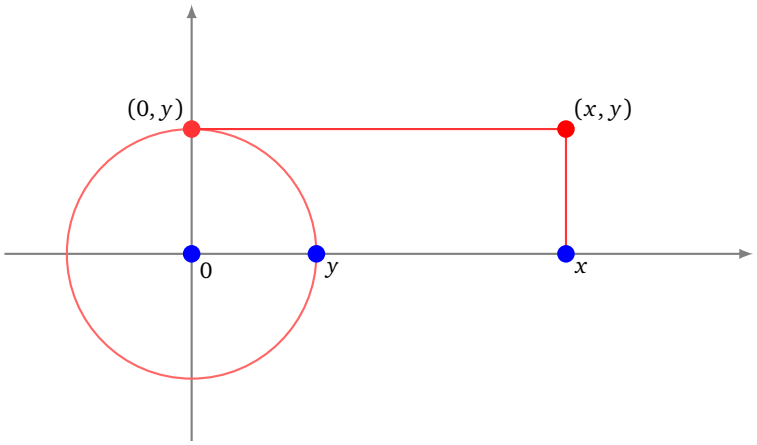
Voici la première étape. Partant de $\mathscr{C}_0$ (en bleu à gauche), on peut tracer une droite et deux cercles (au milieu), ce qui donne pour $\mathscr{C}_1$ quatre points supplémentaires (en rouge à droite).



Pour $\mathscr{C}_2$ on repartirait de tous les points (rouges ou bleus) de $\mathscr{C}_1$, et on tracerait tous les cercles ou droites possibles (il y en a beaucoup !), et les points d'intersection formeraient l'ensemble $\mathscr{C}_2$.

Définition 1.
- $\mathscr{C} = \bigcup_{i \geqslant 0} \mathscr{C}_i$ est l'ensemble des ***points constructibles***. Autrement dit $\mathscr{C} = \mathscr{C}_0 \cup \mathscr{C}_1 \cup \mathscr{C}_2 \cup \cdots$ De plus $P \in \mathscr{C}$ si et seulement s'il existe $i \geqslant 0$ tel que $P \in \mathscr{C}_i$.
- $\mathscr{C}_{\mathbb{R}} \subset \mathbb{R}$ est l'ensemble des abscisses des points constructibles : ce sont les ***nombres (réels) constructibles***.
- $\mathscr{C}_{\mathbb{C}} \subset \mathbb{C}$ est l'ensemble des affixes des points constructibles : ce sont les ***nombres complexes constructibles***.

Attention ! Même si deux points A, B sont constructibles et que l'on peut tracer la droite (AB), pour autant les points de (AB) ne sont pas tous constructibles. Seuls les points d'intersection de (AB) avec d'autres objets construits sont constructibles.
Déterminer les points constructibles $\mathscr{C}$ ou déterminer les nombres constructibles $\mathscr{C}_{\mathbb{R}}$ sont deux problèmes équivalents. En effet, si (x, y) est un point constructible alors par projection sur l'axe des abscisses nous obtenons le réel constructible x, et de même pour y projection sur l'axe des ordonnées, puis report sur l'axe des abscisses. Réciproquement on peut passer de deux nombres constructibles $x, y \in \mathbb{R}$ à un point constructible (x, y) dans le plan. Voici comment : partant du point $(y, 0)$ on construit $(0, y)$ sur l'axe des ordonnées par un coup de compas en reportant y. Une fois que $(x, 0)$ et $(0, y)$ sont construits, il est facile de construire (x, y).



2.2. Premières constructions algébriques

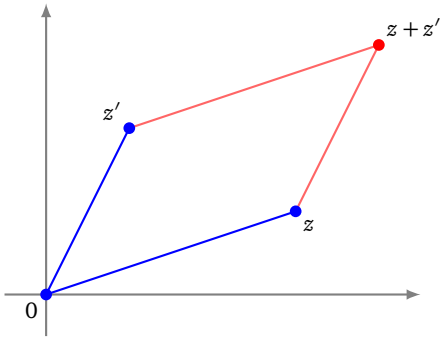
Proposition 1.
Si x, x' sont des réels constructibles alors :

1. *$x + x'$ est constructible,*
2. *$-x$ est constructible,*
3. *$x \cdot x'$ est constructible.*
4. *Si $x' \neq 0$, alors x/x' est constructible.*

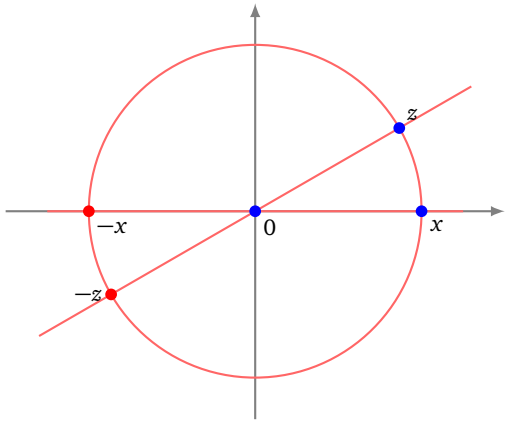
Tous ces résultats sont valables si l'on remplace x, x' par des nombres complexes z, z'.

Démonstration. 1. La construction pour le réel $x+x'$ est facile en utilisant le report du compas (on reporte la longueur x' à partir de x). Une autre méthode est de construire d'abord le milieu $\frac{x+x'}{2}$ puis le symétrique de 0 par rapport à ce milieu : c'est $x+x'$.

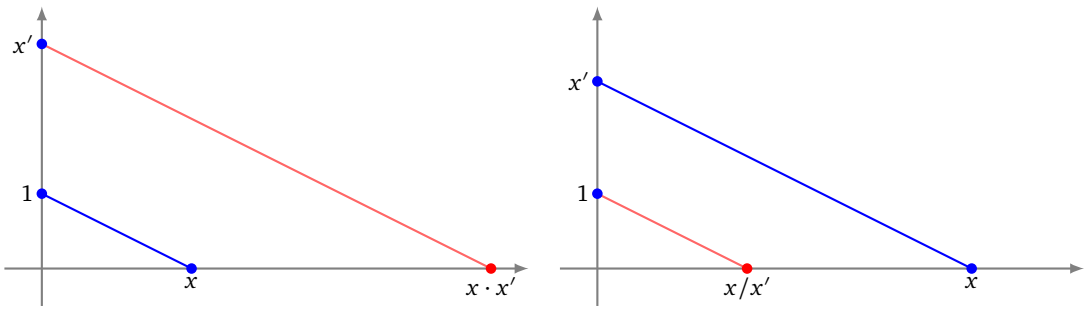
La somme de deux nombres complexes $z+z'$ correspond à la construction d'un parallélogramme de sommets $0, z, z', z+z'$: les points d'affixes 0, z, z' étant supposés constructibles, on construit un parallélogramme de sorte que $z+z'$ soit le quatrième sommet.



2. L'opposé du réel x (resp. du complexe z) s'obtient comme symétrique par rapport à l'origine : tracez la droite passant par 0 et x (resp. z) ; tracez le cercle de centre 0 passant par x (resp. z) ; ce cercle recoupe la droite en $-x$ (resp. $-z$).

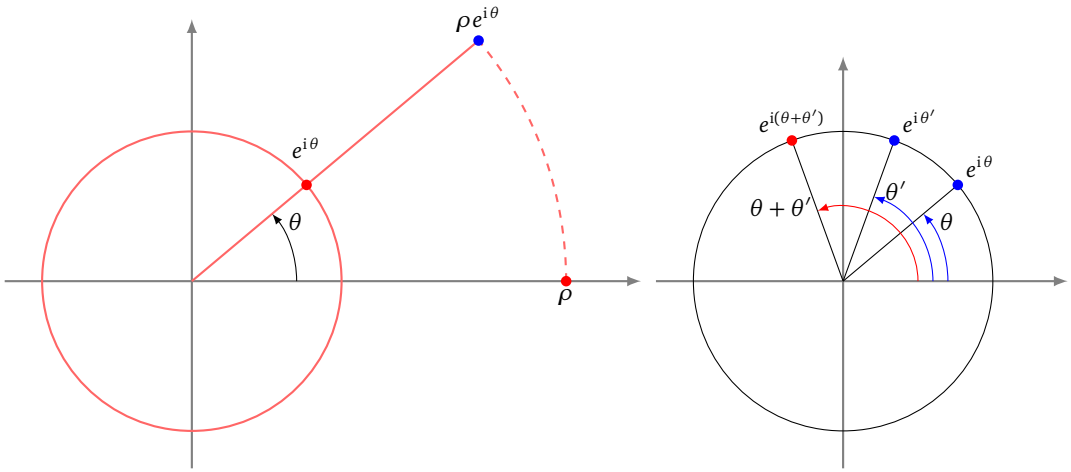


3. Commençons par le produit de deux nombres réels $x \cdot x'$. On suppose construits les points $(x,0)$ et $(0,x')$ (dessin de gauche). On trace la droite $\mathscr{D}$ passant par $(x,0)$ et $(0,1)$. On construit ensuite – à la règle et au compas – la droite $\mathscr{D}'$ parallèle à $\mathscr{D}$ et passant par $(0,x')$. Le théorème de Thalès prouve que $\mathscr{D}'$ recoupe l'axe des abscisses en $(x \cdot x', 0)$.



4. Pour le quotient la méthode est similaire (dessin de droite).

5. Il reste à s'occuper du produit et du quotient de deux nombres complexes. Tout d'abord, si $z = \rho e^{i\theta}$ est un nombre complexe constructible, alors ρ est constructible (considérer le cercle centré à l'origine qui passe par z ; il recoupe l'axe des abscisses en $(\rho, 0)$). Le nombre $e^{i\theta}$ est aussi constructible : c'est l'intersection de la droite passant par l'origine et z avec le cercle unité. Réciproquement avec ρ et $e^{i\theta}$ on construit facilement $z = \rho e^{i\theta}$.



Maintenant si $z = \rho e^{i\theta}$ et $z' = \rho' e^{i\theta'}$ alors $z \cdot z' = (\rho \cdot \rho') e^{i(\theta+\theta')}$. Le réel $\rho \cdot \rho'$ est constructible comme nous l'avons vu au-dessus. Il reste à construire le nombre complexe $e^{i(\theta+\theta')}$, qui correspond à la somme de deux angles θ et θ'. Cela se fait simplement, à partir du cercle unité, en reportant au compas la mesure d'un angle à partir de l'extrémité de l'autre.

Pour le quotient la méthode est similaire.

□

Corollaire 1.

$$\mathbb{N} \subset \mathscr{C}_{\mathbb{R}} \qquad \mathbb{Z} \subset \mathscr{C}_{\mathbb{R}} \qquad \mathbb{Q} \subset \mathscr{C}_{\mathbb{R}}$$

Autrement dit, tous les rationnels (et en particulier tous les entiers) sont des nombres réels constructibles.

La preuve découle facilement de la proposition :

Démonstration.
- Puisque 1 est un nombre constructible alors $2 = 1 + 1$ est constructible, mais alors $3 = 2 + 1$ est constructible et par récurrence tout entier $n \geqslant 0$ est un élément de $\mathscr{C}_{\mathbb{R}}$.
- Comme tout entier $n \geqslant 0$ est constructible alors $-n$ l'est aussi ; donc tous les entiers $n \in \mathbb{Z}$ sont constructibles.
- Enfin pour $\frac{p}{q} \in \mathbb{Q}$, comme les entiers p, q sont constructibles, alors le quotient $\frac{p}{q}$ est constructible et ainsi $\mathbb{Q} \subset \mathscr{C}_{\mathbb{R}}$.

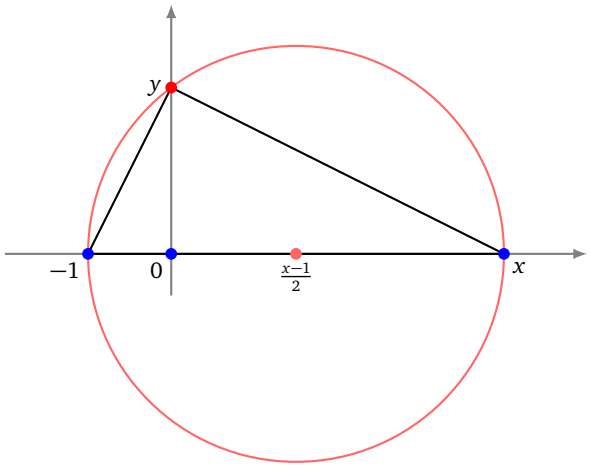
□

Nous allons voir que $\mathscr{C}_{\mathbb{R}}$ contient davantage de nombres que les rationnels.

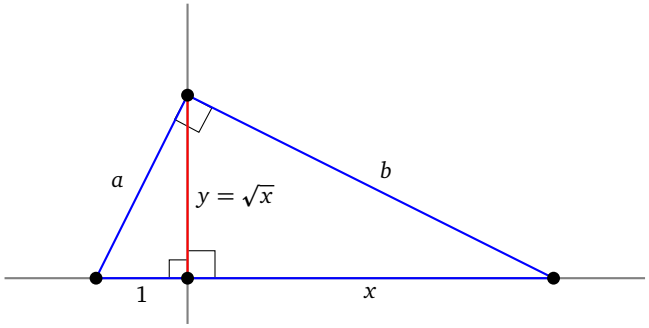
Proposition 2.
Si $x \geqslant 0$ est un nombre constructible, alors $\sqrt{x}$ est constructible.

Remarques :

1. La réciproque est vraie. En effet si $x' = \sqrt{x}$ est un nombre constructible, alors par la proposition 1 : $x' \cdot x'$ est constructible. Or $x' \cdot x' = \sqrt{x} \cdot \sqrt{x} = x$, donc x est constructible.
2. On peut en déduire aussi que si $z \in \mathbb{C}$ est constructible alors les racines carrées (complexes) de z sont constructibles. On utilise pour cela la racine carrée du module et la bissection de l'argument comme on l'a vue au paragraphe 1.5.
3. En particulier $\sqrt{2}$, $\sqrt{3}$, … sont des nombres constructibles (comme on l'avait vu en première partie).



Démonstration.
Soient les nombres constructibles $0, -1, x$ placés sur l'axe des abscisses. Traçons le cercle dont le diamètre est $[-1, x]$ (cela revient à construire le centre du cercle $\frac{x-1}{2}$; voir la proposition 1). Ce cercle recoupe l'axe des ordonnées en $y \geqslant 0$.



On applique le théorème de Pythagore dans trois triangles rectangles, pour obtenir :

$$\begin{cases} a^2 + b^2 &= (1+x)^2 \\ 1 + y^2 &= a^2 \\ x^2 + y^2 &= b^2. \end{cases}$$

On en déduit $a^2 + b^2 = (1+x)^2 = 1 + x^2 + 2x$ d'une part et $a^2 + b^2 = 1 + x^2 + 2y^2$ d'autre part. Ainsi $1 + x^2 + 2x = 1 + x^2 + 2y^2$ d'où $y^2 = x$. Comme $y \geqslant 0$ alors $y = \sqrt{x}$.
Une autre méthode consiste à remarquer que le triangle de sommets $(0,0), (-1,0), (0,y)$ et le triangle de sommets $(0,0), (x,0), (0,y)$ sont semblables donc $\frac{x}{y} = \frac{y}{1}$, d'où $x = y^2$, donc $y = \sqrt{x}$.

□

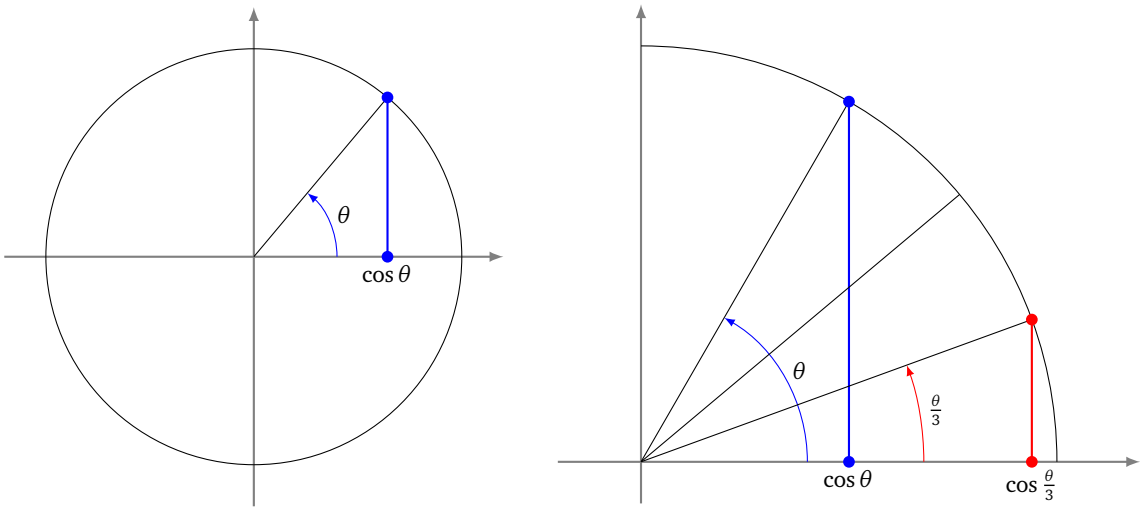
2.3. Retour sur les trois problèmes grecs

Avec le langage des nombres constructibles les problèmes historiques s'énoncent ainsi :

- ***La duplication du cube.*** Est-ce que $\sqrt[3]{2}$ est un nombre constructible ?
- ***La quadrature du cercle.*** Est-ce que π est un nombre constructible ?
- ***La trisection des angles.*** Étant donné un réel constructible $\cos\theta$, est-ce que $\cos\frac{\theta}{3}$ est aussi constructible ?

Si vous n'êtes pas convaincu voici les preuves :

- Si on a un cube de volume a^3, alors il faut construire un cube de volume $2a^3$. Fixons a un réel constructible. Que $\sqrt[3]{2}$ soit aussi constructible équivaut à $a\sqrt[3]{2}$ constructible. Un segment de longueur $a\sqrt[3]{2}$ définit bien un cube de volume $2a^3$. On aurait résolu la duplication du cube.
- Soit construit un cercle de rayon r, donc d'aire πr^2. Que π soit constructible équivaut à $\sqrt{\pi}$ constructible. Construire un segment de longueur $\sqrt{\pi}r$, correspond à un carré d'aire πr^2, donc de même aire que le cercle initial. Nous aurions construit un carré de même aire que le cercle ! On aurait résolu la quadrature du cercle.
- Remarquons que construire un angle géométrique de mesure θ est équivalent à construire le nombre réel $\cos\theta$ (voir la figure de gauche). Partons d'un angle géométrique θ, c'est-à-dire partons d'un réel $\cos\theta$ constructible. Construire $\cos\frac{\theta}{3}$ est équivalent à construire un angle géométrique de mesure $\frac{\theta}{3}$. On aurait résolu la trisection des angles.



2.4. Les ensembles

Une dernière motivation à propos des nombres constructibles concerne les ensembles. Nous avons les inclusions d'ensembles :

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}.$$

Le passage d'un ensemble à un ensemble plus grand se justifie par la volonté de résoudre davantage d'équations :

- passage de $\mathbb{N}$ à $\mathbb{Z}$, pour résoudre des équations du type $x + 7 = 0$,
- passage de $\mathbb{Z}$ à $\mathbb{Q}$, pour résoudre des équations du type $5x = 4$,
- passage de $\mathbb{Q}$ à $\mathbb{R}$, pour résoudre des équations du type $x^2 = 2$,
- passage de $\mathbb{R}$ à $\mathbb{C}$, pour résoudre des équations du type $x^2 = -1$.

Mais en fait le passage de $\mathbb{Q}$ à $\mathbb{R}$ est un saut beaucoup plus « grand » que les autres : $\mathbb{Q}$ est un ensemble dénombrable (il existe une bijection entre $\mathbb{Z}$ et $\mathbb{Q}$) alors que $\mathbb{R}$ ne l'est pas.
Nous allons définir et étudier deux ensembles intermédiaires :

$$\mathbb{Q} \subset \mathscr{C}_{\mathbb{R}} \subset \overline{\mathbb{Q}} \subset \mathbb{R}$$

où

- $\mathscr{C}_{\mathbb{R}}$ est l'ensemble des nombres réels constructibles à la règle et au compas,
- $\overline{\mathbb{Q}}$ est l'ensemble des nombres algébriques : ce sont les réels x qui sont solutions d'une équation $P(x) = 0$, pour un polynôme P à coefficients dans $\mathbb{Q}$.

3. Éléments de théorie des corps

La théorie des corps n'est pas évidente et mériterait un chapitre entier. Nous résumons ici les grandes lignes utiles à nos fins. Il est important de bien comprendre le paragraphe suivant ; les autres paragraphes peuvent être sautés lors de la première lecture.

3.1. Les exemples à comprendre

Premier exemple. Soit l'ensemble

$$\mathbb{Q}(\sqrt{2}) = \left\{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\right\}.$$

C'est un sous-ensemble de $\mathbb{R}$, qui contient par exemple 0, 1, $\frac{1}{3}$ et tous les éléments de $\mathbb{Q}$, mais aussi $\sqrt{2}$ (qui n'est pas rationnel !), $\frac{1}{2} - \frac{2}{3}\sqrt{2}$.
Voici quelques propriétés :

- Soient $a + b\sqrt{2}$ et $a' + b'\sqrt{2}$ deux éléments de $\mathbb{Q}(\sqrt{2})$. Alors leur somme $(a + b\sqrt{2}) + (a' + b'\sqrt{2})$ est encore un élément de $\mathbb{Q}(\sqrt{2})$. De même $-(a + b\sqrt{2}) \in \mathbb{Q}(\sqrt{2})$.
- Plus surprenant, si $a + b\sqrt{2}, a' + b'\sqrt{2} \in \mathbb{Q}(\sqrt{2})$ alors $(a + b\sqrt{2}) \times (a' + b'\sqrt{2}) = aa' + 2bb' + (ab' + a'b)\sqrt{2}$ est aussi un élément de $\mathbb{Q}(\sqrt{2})$. Enfin l'inverse d'un élément non nul $a + b\sqrt{2}$ est $\frac{1}{a+b\sqrt{2}} = \frac{1}{a^2-2b^2}(a - b\sqrt{2})$: c'est encore un élément de $\mathbb{Q}(\sqrt{2})$.

Ces propriétés font de $\mathbb{Q}(\sqrt{2})$ un ***corps***. Comme ce corps contient $\mathbb{Q}$ on parle d'une ***extension*** de $\mathbb{Q}$. De plus, il est étendu avec un élément du type $\sqrt{\delta}$: on parle alors d'une ***extension quadratique***. Notez que, même si $\delta \in \mathbb{Q}$, $\sqrt{\delta}$ n'est généralement pas un élément de $\mathbb{Q}$.

Deuxième série d'exemples. On peut généraliser l'exemple précédent : si K est lui-même un corps et δ est un élément de K alors

$$K(\sqrt{\delta}) = \left\{a + b\sqrt{\delta} \mid a, b \in K\right\}$$

est un corps. On vérifie comme ci-dessus que la somme et le produit de deux éléments restent dans $K(\sqrt{\delta})$, ainsi que l'opposé et l'inverse.
Cela permet de construire de nouveaux corps : partant de $K_0 = \mathbb{Q}$, on choisit un élément, disons $\delta_0 = 2$ et on obtient le corps plus gros $K_1 = \mathbb{Q}(\sqrt{2})$. Si on prend $\delta_1 = 3$ alors $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$ et donc $K_2 = K_1(\sqrt{3})$ est un nouveau corps (qui contient K_1). Le corps K_2 est :

$$K_2 = K_1(\sqrt{3}) = \mathbb{Q}(\sqrt{2})(\sqrt{3}) = \left\{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{2}\sqrt{3} \mid a, b, c, d \in \mathbb{Q}\right\}.$$

On pourrait continuer avec $\delta_2 = 11$ et exprimer chaque élément de $\mathbb{Q}(\sqrt{2})(\sqrt{3})(\sqrt{11})$ comme une somme de 8 éléments $a_1 + a_2\sqrt{2} + a_3\sqrt{3} + a_4\sqrt{11} + a_5\sqrt{2}\sqrt{3} + a_6\sqrt{2}\sqrt{11} + a_7\sqrt{3}\sqrt{11} + a_8\sqrt{2}\sqrt{3}\sqrt{11}$ avec les $a_i \in \mathbb{Q}$.
En partant de $K_1 = \mathbb{Q}(\sqrt{2})$, on aurait pu considérer $\delta_1 = 1 + \sqrt{2}$ et $K_2 = K_1(\sqrt{1+\sqrt{2}}) = \mathbb{Q}(\sqrt{2})(\sqrt{1+\sqrt{2}})$. Chaque élément de K_2 peut s'écrire comme une somme de 4 éléments $a + b\sqrt{2} + c\sqrt{1+\sqrt{2}} + d\sqrt{2}\sqrt{1+\sqrt{2}}$.

Une propriété. Il faut noter que chaque élément de $\mathbb{Q}(\sqrt{2})$ est racine d'un polynôme de degré au plus 2 à coefficients dans $\mathbb{Q}$. Par exemple $3 + \sqrt{2}$ est annulé par $P(X) = (X-3)^2 - 2 = X^2 - 6X + 7$. Les nombres qui sont annulés par un polynôme à coefficients rationnels sont les ***nombres algébriques***. Plus généralement, si K est un corps et $\delta \in K$, alors tout élément de $K(\sqrt{\delta})$ est annulé par un polynôme de degré 1 ou 2 à coefficients dans K. On en déduit que chaque élément de $\mathbb{Q}(\sqrt{2})(\sqrt{3})$ (ou de $\mathbb{Q}(\sqrt{2})(\sqrt{1+\sqrt{2}})$) est racine d'un polynôme de $\mathbb{Q}[X]$ de degré 1, 2 ou 4. Et chaque élément de $\mathbb{Q}(\sqrt{2})(\sqrt{3})(\sqrt{11})$ est racine d'un polynôme de $\mathbb{Q}[X]$ de degré 1, 2, 4 ou 8, etc.

Nous allons maintenant reprendre ces exemples d'une manière plus théorique.

3.2. Corps

Un corps est un ensemble sur lequel sont définies deux opérations : une addition et une multiplication.

Définition 2.
Un ***corps*** $(K, +, \times)$ est un ensemble K muni des deux opérations $+$ et $\times$, qui vérifient :

0. $+$ et $\times$ sont des lois de composition interne, c'est à dire $x + y \in K$ et $x \times y \in K$ (pour tout $x, y \in K$).
1. $(K, +)$ est un groupe commutatif, c'est-à-dire :
   - Il existe $0 \in K$ tel que $0 + x = x$ (pour tout $x \in K$).
   - Pour tout $x \in K$ il existe $-x$ tel que $x + (-x) = 0$.
   - $+$ est associative : $(x + y) + z = x + (y + z)$ (pour tout $x, y, z \in K$).
   - $x + y = y + x$ (pour tout $x, y \in K$).
2. $(K \setminus \{0\}, \times)$ est un groupe commutatif, c'est-à-dire :
   - Il existe $1 \in K \setminus \{0\}$ tel que $1 \times x = x$ (pour tout $x \in K$).
   - Pour tout $x \in K \setminus \{0\}$, il existe x^{-1} tel que $x \times x^{-1} = 1$.
   - $\times$ est associative : $(x \times y) \times z = x \times (y \times z)$ (pour tout $x, y, z \in K \setminus \{0\}$).
   - $x \times y = y \times x$ (pour tout $x, y \in K \setminus \{0\}$).
3. $\times$ est distributive par rapport à $+$: $(x + y) \times z = x \times z + y \times z$ (pour tout $x, y, z \in K$).

Voici des exemples classiques :
- $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ sont des corps. L'addition et la multiplication sont les opérations usuelles.
- Par contre $(\mathbb{Z}, +, \times)$ n'est pas un corps. (Pourquoi ?)

Voici des exemples qui vont être importants pour la suite :
- $\mathbb{Q}(\sqrt{2}) = \left\{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\right\}$ est un corps (avec l'addition et la multiplication habituelles des nombres réels). Voir les exemples introductifs.
- $\mathbb{Q}(\mathrm{i}) = \left\{a + \mathrm{i}\, b \mid a, b \in \mathbb{Q}\right\}$ est un corps (avec l'addition et la multiplication habituelles des nombres complexes).

- Par contre $\{a+b\pi \mid a,b\in\mathbb{Q}\}$ n'est pas un corps (où $\pi=3,14\ldots$). (C'est une conséquence du fait que π n'est pas un nombre algébrique comme on le verra plus loin.)

La proposition 1 de la première partie se reformule avec la notion de corps en :

Proposition 3.
L'ensemble des nombre réels constructibles $(\mathscr{C}_{\mathbb{R}},+,\times)$ est un corps inclus dans $\mathbb{R}$.

On a aussi que $(\mathscr{C}_{\mathbb{C}},+,\times)$ est un corps inclus dans $\mathbb{C}$.

3.3. Extension de corps

Nous cherchons des propositions qui lient deux corps, lorsque l'un est inclus dans l'autre. Les résultats de ce paragraphe seront admis.

Proposition 4.
Soient K,L deux corps avec $K\subset L$. Alors L est un espace vectoriel sur K.

Définition 3.
L est appelé une ***extension*** de K. Si la dimension de cet espace vectoriel est finie, alors on l'appelle le ***degré*** de l'extension, et on notera :
$$[L:K]=\dim_K L.$$
Si ce degré vaut 2, nous parlerons d'une ***extension quadratique***.

Proposition 5.
Si K,L,M sont trois corps avec $K\subset L\subset M$ et si les extensions ont un degré fini alors :
$$[M:K]=[M:L]\times[L:K].$$

Exemple 1. • $\mathbb{Q}(\sqrt{2})$ est une extension de $\mathbb{Q}$. De plus, comme $\mathbb{Q}(\sqrt{2})=\{a+b\sqrt{2}\mid a,b\in\mathbb{Q}\}$, alors $\mathbb{Q}(\sqrt{2})$ est un espace vectoriel (sur $\mathbb{Q}$) de dimension 2 : en effet $(1,\sqrt{2})$ en est une base. Attention : ici 1 est un vecteur et $\sqrt{2}$ est un autre vecteur. Le fait que $\sqrt{2}\notin\mathbb{Q}$ se traduit en : ces deux vecteurs sont linéairement indépendants sur $\mathbb{Q}$. C'est un peu déroutant au début !
- $\mathbb{C}$ est une extension de degré 2 de $\mathbb{R}$ car tout élément de $\mathbb{C}$ s'écrit $a+\mathrm{i}\,b$. Donc les vecteurs 1 et i forment une base de $\mathbb{C}$, vu comme un espace vectoriel sur $\mathbb{R}$.
- Notons $\mathbb{Q}(\sqrt{2},\sqrt{3})=\mathbb{Q}(\sqrt{2})(\sqrt{3})=\{a+b\sqrt{3}\mid a,b\in\mathbb{Q}(\sqrt{2})\}$. Alors $\mathbb{Q}\subset\mathbb{Q}(\sqrt{2})\subset\mathbb{Q}(\sqrt{2},\sqrt{3})$. Calculer le degré des extensions. Expliciter une base sur $\mathbb{Q}$ de $\mathbb{Q}(\sqrt{2},\sqrt{3})$.

Pour $x\in\mathbb{R}$, on note $\mathbb{Q}(x)$ le plus petit corps contenant $\mathbb{Q}$ et x : c'est le ***corps engendré*** par x. C'est cohérent avec la notation pour les extensions quadratiques $\mathbb{Q}(\sqrt{\delta})$, qui est bien le plus petit corps contenant $\sqrt{\delta}$.
Par exemple, si $x=\sqrt[3]{2}=2^{\frac{1}{3}}$, alors il n'est pas dur de calculer que
$$\mathbb{Q}(\sqrt[3]{2})=\left\{a+b\sqrt[3]{2}+c\sqrt[3]{2}^2\mid a,b,c\in\mathbb{Q}\right\}.$$
En effet $\mathbb{Q}(\sqrt[3]{2})$ contient $x,x^2,x^3,\ldots$ mais aussi $\frac{1}{x},\frac{1}{x^2},\ldots$ Mais comme $x^3=2\in\mathbb{Q}$ et $\frac{1}{x}=\frac{x^2}{2}$, alors $a+bx+cx^2$, avec $a,b,c\in\mathbb{Q}$, engendrent tous les éléments de $\mathbb{Q}(x)$. Conclusion : $[\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}]=3$.

3.4. Nombre algébrique

L'ensemble des ***nombres algébriques*** est
$$\overline{\mathbb{Q}}=\{x\in\mathbb{R}\mid \text{ il existe } P\in\mathbb{Q}[X] \text{ non nul tel que } P(x)=0\}.$$

Proposition 6.
$\overline{\mathbb{Q}}$ est un corps.

Démonstration. L'addition et la multiplication définies sur $\overline{\mathbb{Q}}$ sont celles du corps $(\mathbb{R},+,\times)$. Ainsi beaucoup de propriétés découlent du fait que l'ensemble des réels est un corps (on parle de sous-corps).
La première chose que l'on doit démontrer, c'est que $+$ et $\times$ sont des lois de composition interne, c'est-à-dire que si x et y sont des nombres réels algébriques alors $x+y$ et $x\times y$ le sont aussi. Ce sera prouvé dans le corollaire 2.

1. $(\overline{\mathbb{Q}}, +)$ est un groupe commutatif, car :
   - $0 \in \overline{\mathbb{Q}}$ (prendre $P(X) = X$) et $0 + x = x$ (pour tout $x \in \overline{\mathbb{Q}}$).
   - Si $x \in \overline{\mathbb{Q}}$ alors $-x \in \overline{\mathbb{Q}}$ (si $P(X)$ est un polynôme qui annule x alors $P(-X)$ annule $-x$).
   - $+$ est associative : cela découle de l'associativité sur $\mathbb{R}$.
   - $x + y = y + x$: idem.
2. $(\overline{\mathbb{Q}} \setminus \{0\}, \times)$ est un groupe commutatif, car :
   - $1 \in \overline{\mathbb{Q}} \setminus \{0\}$ et $1 \times x = x$ (pour tout $x \in \overline{\mathbb{Q}} \setminus \{0\}$).
   - Si $x \in \overline{\mathbb{Q}} \setminus \{0\}$ alors $x^{-1} \in \overline{\mathbb{Q}} \setminus \{0\}$: en effet, si $P(X)$ est un polynôme de degré n annulant x, alors $X^n P(\frac{1}{X})$ est un polynôme annulant $\frac{1}{x}$.
   - $\times$ est associative : cela découle de l'associativité sur $\mathbb{R} \setminus \{0\}$.
   - $x \times y = y \times x$: idem.
3. $\times$ est distributive par rapport à $+$: cela découle de la distributivité sur $\mathbb{R}$.

□

Si $x \in \overline{\mathbb{Q}}$ est un nombre algébrique, alors le plus petit degré, parmi tous les degrés des polynômes $P \in \mathbb{Q}[X]$ tels que $P(x) = 0$, est le ***degré algébrique*** de x. Par exemple, calculons le degré algébrique de $\sqrt{2}$: un polynôme annulant ce nombre est $P(X) = X^2 - 2$ et il n'est pas possible d'en trouver de degré 1, donc le degré algébrique de $\sqrt{2}$ vaut 2. Plus généralement $\sqrt{\delta}$ avec $\delta \in \mathbb{Q}$ est de degré algébrique égal à 1 ou 2 (de degré algébrique 1 si $\sqrt{\delta} \in \mathbb{Q}$, de degré 2 sinon). Par contre $\sqrt[3]{2}$ est de degré 3, car il est annulé par $P(X) = X^3 - 2$ mais pas par des polynômes de degré plus petit.

Proposition 7. *1. Soit L une extension finie du corps $\mathbb{Q}$. Si $x \in L$, alors x est un nombre algébrique.*

2. Si x un nombre algébrique alors $\mathbb{Q}(x)$ est une extension finie de $\mathbb{Q}$.

3. Si x est un nombre algébrique alors le degré de l'extension $[\mathbb{Q}(x) : \mathbb{Q}]$ et le degré algébrique de x coïncident.

Démonstration. 1. Soit L une extension finie de $\mathbb{Q}$, et soit $n = [L : \mathbb{Q}]$. Fixons $x \in L$. Les $n+1$ éléments $(1, x, x^2, \ldots, x^n)$ forment une famille de $n+1$ vecteurs dans un espace vectoriel de dimension n. Donc cette famille est liée. Il existe donc une combinaison linéaire nulle non triviale, c'est-à-dire il existe $a_i \in \mathbb{Q}$ non tous nuls tels que $\sum_{i=0}^{n} a_i x^i = 0$. Si l'on définit $P(X) = \sum_{i=0}^{n} a_i X^i$, alors $P(X) \in \mathbb{Q}[X]$, $P(X)$ n'est pas le polynôme nul et $P(x) = 0$. C'est exactement dire que x est un nombre algébrique.

2. Soit $P(X) = \sum_{i=0}^{n} a_i X^i$ non nul qui vérifie $P(x) = 0$. En écartant le le cas trivial $x = 0$, on peut donc supposer que $a_0 \neq 0$ et $a_n \neq 0$. Alors $x^n = -\frac{1}{a_n} \sum_{i=0}^{n-1} a_i x^i$ et $\frac{1}{x} = \frac{1}{a_0} \sum_{i=1}^{n} a_i x^{i-1}$. Ce qui prouve que $x^n \in \text{Vect}(1, x, \ldots, x^{n-1})$ et $\frac{1}{x} \in \text{Vect}(1, x, \ldots, x^{n-1})$. De même pour tout $k \in \mathbb{Z}$, $x^k \in \text{Vect}(1, x, \ldots, x^{n-1})$, donc $\mathbb{Q}(x) \subset \text{Vect}(1, x, \ldots, x^{n-1})$. Ce qui prouve que $\mathbb{Q}(x)$ est un espace vectoriel de dimension finie sur $\mathbb{Q}$.

3. Ce sont à peu près les mêmes arguments. Si $m = [\mathbb{Q}(x) : \mathbb{Q}]$ alors il existe $a_i \in \mathbb{Q}$ non tous nuls tels que $\sum_{i=0}^{m} a_i x^i = 0$. Donc il existe un polynôme non nul de degré m annulant x. Donc le degré algébrique de x est inférieur ou égal à m.
   Mais s'il existait un polynôme $P(X) = \sum_{i=0}^{m-1} b_i X^i$ non nul de degré strictement inférieur à m qui annulait x, alors nous aurions une combinaison linéaire nulle non triviale $\sum_{i=0}^{m-1} b_i x^i = 0$. Cela impliquerait que $x^{m-1} \in \text{Vect}(1, x, \ldots, x^{m-2})$ et plus généralement que $\mathbb{Q}(x) \subset \text{Vect}(1, x, \ldots, x^{m-2})$, ce qui contredirait le fait que $\mathbb{Q}(x)$ soit un espace vectoriel de dimension m sur $\mathbb{Q}$.
   Bilan : le degré algébrique de x est exactement $[\mathbb{Q}(x) : \mathbb{Q}]$.

□

Corollaire 2.
Si x et y sont des nombres réels algébriques alors $x + y$ et $x \times y$ aussi.

Démonstration. Comme x est un nombre algébrique alors $L = \mathbb{Q}(x)$ est une extension finie de $K = \mathbb{Q}$. Posons $M = \mathbb{Q}(x, y) = \big(\mathbb{Q}(x)\big)(y)$. Comme y est un nombre algébrique alors M est une extension finie de $\mathbb{Q}(x)$. Par la proposition 5 $M = \mathbb{Q}(x, y)$ est une extension finie de $K = \mathbb{Q}$.
Comme $x + y \in \mathbb{Q}(x + y) \subset \mathbb{Q}(x, y)$ et que $\mathbb{Q}(x, y)$ est une extension finie de $\mathbb{Q}$ alors par la proposition 7, $x + y$ est un nombre algébrique.
C'est la même preuve pour $x \times y \in \mathbb{Q}(x \times y) \subset \mathbb{Q}(x, y)$. □

4. Corps et nombres constructibles

Cette partie est la charnière de ce chapitre. Nous expliquons à quoi correspondent algébriquement les opérations géométriques effectuées à la règle et au compas.

4.1. Nombre constructible et extensions quadratiques

Voici le résultat théorique le plus important de ce chapitre. C'est Pierre-Laurent Wantzel qui a démontré ce théorème en 1837, à l'âge de 23 ans.

Théorème 1 (Théorème de Wantzel)**.**
Un nombre réel x est constructible si et seulement s'il existe des extensions quadratiques

$$\mathbb{Q} = K_0 \subset K_1 \subset \cdots \subset K_r$$

telles que $x \in K_r$.

Chacune des extensions est quadratique, c'est-à-dire $[K_{i+1} : K_i] = 2$. Autrement dit, chaque extension est une extension quadratique de la précédente : $K_{i+1} = K_i(\sqrt{\delta_i})$ pour un certain $\delta_i \in K_i$. Donc en partant de $K_0 = \mathbb{Q}$, les extensions sont :

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt{\delta_0}) \subset \mathbb{Q}(\sqrt{\delta_0})(\sqrt{\delta_1}) \subset \cdots$$

Démonstration. Il y a un sens facile : comme on sait construire les racines carrées des nombres constructibles (voir la proposition 2) alors on sait construire tout élément d'une extension quadratique $K_1 = \mathbb{Q}(\sqrt{\delta_0})$, puis par récurrence tout élément de K_2, K_3,...

Passons au sens difficile. Rappelons-nous que les points constructibles sont construits par étapes $\mathscr{C}_0$, $\mathscr{C}_1$, $\mathscr{C}_2$,...
L'ensemble $\mathscr{C}_{j+1}$ s'obtient à partir de $\mathscr{C}_j$ en ajoutant les intersections des droites et des cercles que l'on peut tracer à partir de $\mathscr{C}_j$. Nous allons voir que ce passage correspond à une suite d'extensions quadratiques.
Soit donc K le plus petit corps contenant les coordonnées des points de $\mathscr{C}_j$. Nous considérons P un point de $\mathscr{C}_{j+1}$. Ce point P est l'intersection de deux objets (deux droites ; une droite et un cercle ; deux cercles). Distinguons les cas :

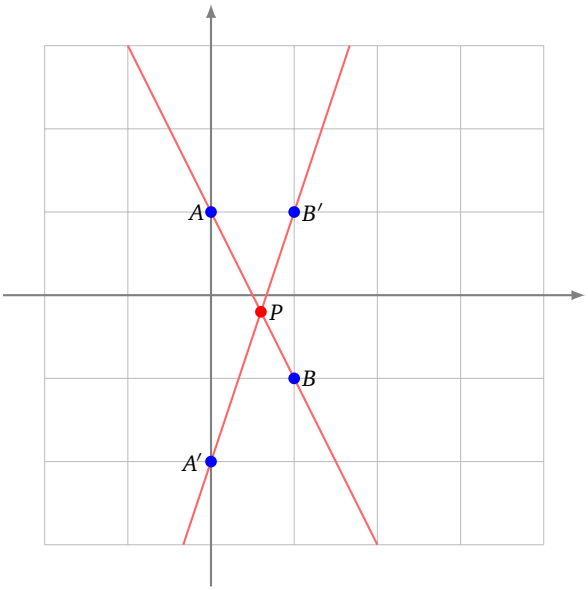
- *P est l'intersection de deux droites.* Ces droites passent par des points de $\mathscr{C}_j$ donc elles ont pour équations $ax+by = c$ et $a'x + b'y = c'$ et il est important de noter que l'on peut prendre a, b, c, a', b', c' comme étant des éléments de K. Par exemple une équation de la droite passant par $A(x_A, y_A)$ et $B(x_B, y_B)$ (avec $x_A, y_A, x_B, y_B \in K$) est $y = \frac{y_B - y_A}{x_B - x_A}(x - x_A) + y_A$, ce qui donne bien une équation à coefficients dans K. Les coordonnées de P sont donc
$$\left(\frac{cb' - c'b}{ab' - a'b}, \frac{ac' - a'c}{ab' - a'b}\right).$$
Comme K est un corps alors l'abscisse et l'ordonnée de ce P sont encore dans K. Dans ce cas il n'y a pas besoin d'extension : le plus petit corps contenant les coordonnées des points de $\mathscr{C}_j$ et de P est K.
- *P appartient à l'intersection d'une droite et d'un cercle.* Notons l'équation de la droite $ax + by = c$ avec $a, b, c \in K$ et $(x - x_0)^2 + (y - y_0)^2 = r^2$ l'équation du cercle. On note que x_0, y_0, r^2 (mais pas nécessairement r) sont des éléments de K car les coordonnées du centre et d'un point du cercle sont dans K. Il reste à calculer les intersections de la droite et du cercle : en posant
$$\delta = -2x_0a^3by_0 + 2y_0a^2cb - b^2{y_0}^2a^2 + b^2r^2a^2 + 2a^3x_0c - a^4{x_0}^2 - a^2c^2 + a^4r^2 \in K,$$
on trouve deux points (x, y), (x', y') avec
$$x = -\frac{b}{a}\frac{1}{a^2+b^2}\left(-x_0ab + y_0a^2 + cb - \frac{c}{b}(a^2+b^2) + \sqrt{\delta}\right) \quad \text{et} \quad y = \frac{c - ax}{b},$$
$$x' = -\frac{b}{a}\frac{1}{a^2+b^2}\left(-x_0ab + y_0a^2 + cb - \frac{c}{b}(a^2+b^2) - \sqrt{\delta}\right) \quad \text{et} \quad y' = \frac{c - ax'}{b}.$$
Les coordonnées sont bien de la forme $\alpha + \beta\sqrt{\delta}$ avec $\alpha, \beta \in K$ et c'est le même $\delta \in K$ pour x, y, x', y'. Donc les coordonnées de P sont bien dans l'extension quadratique $K(\sqrt{\delta})$.
- *P appartient à l'intersection de deux cercles.* On trouve aussi deux points (x, y), (x', y') et x, y, x', y' sont aussi de la forme $\alpha + \beta\sqrt{\delta}$ pour un certain $\delta \in K$ fixé et $\alpha, \beta \in K$. Les formules sont plus longues à écrire et on se contentera ici de faire un exemple (voir juste après).

En résumé, dans tous les cas, les coordonnées de P sont dans une extension quadratique du corps K, qui contient les coefficients qui servent à construire P.

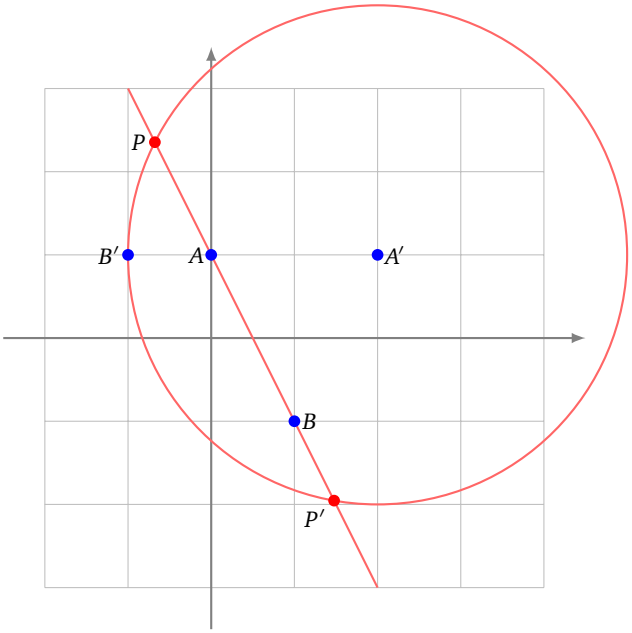
Voici comment terminer la démonstration par une récurrence sur j. Soit K le plus petit corps contenant les coordonnées des points de $\mathscr{C}_j$. On suppose par récurrence que K s'obtient par une suite d'extensions quadratiques de $\mathbb{Q}$. Soit P_1 un point de C_{j+1}, alors nous venons de voir que le corps $K_1 = K(d_1)$ correspondant est une extension quadratique de K. Ensuite soit P_2 un autre point, toujours dans C_{j+1}, cela donne une autre extension quadratique $K_2 = K(\delta_2)$ de K, mais on considère plutôt $K_2' = K(d_1, d_2) = K_1(d_2)$ comme une extension (au plus) quadratique de K_1.
On fait de même pour tous les points de C_{j+1} et on construit une extension $K(d_1, d_2, ..., d_p)$ de K qui correspond à toutes les coordonnées des points de C_{j+1}. Par construction c'est bien une suite d'extension quadratique de K donc de $\mathbb{Q}$. □

Exemple 2.
Donnons les extensions nécessaires dans chacun des trois cas de la preuve sur un exemple concret.

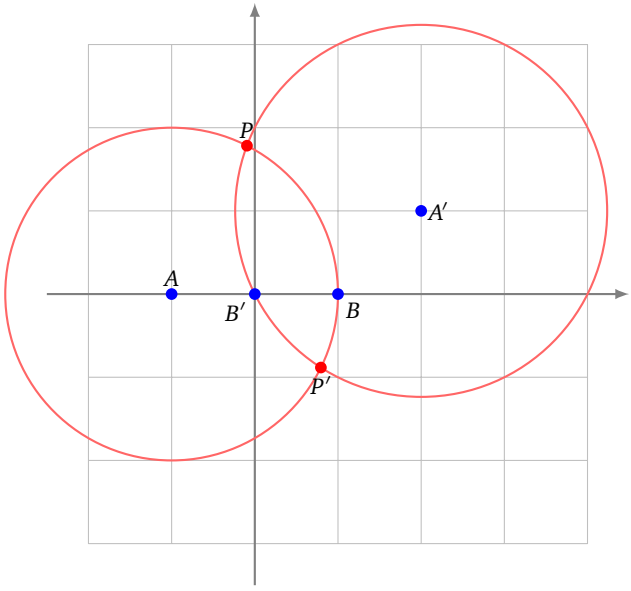
1. P est l'intersection de deux droites (AB) et $(A'B')$ avec par exemple $A(0,1)$, $B(1,-1)$, $A'(0,-2)$, $B'(1,1)$ dont les coordonnées sont dans $K = \mathbb{Q}$. Les équations sont $2x + y = 1$ et $3x - y = 2$; le point d'intersection P a pour coordonnées $(\frac{3}{5}, -\frac{1}{5})$, donc l'abscisse et l'ordonnée sont dans $\mathbb{Q}$. Il n'y a pas besoin d'étendre le corps.



2. P et P' sont les intersections de la droite passant par $A(0,1)$ et $B(1,-1)$ et du cercle de centre $A'(2,1)$ passant par le point $B'(-1,1)$ (et donc de rayon 3). Les équations sont alors $2x + y = 1$ et $(x-2)^2 + (y-1)^2 = 9$. Les deux solutions sont les points :
$$\left(\frac{1}{5}\left(2 - \sqrt{29}\right), \frac{1}{5}\left(1 + 2\sqrt{29}\right)\right), \left(\frac{1}{5}\left(2 + \sqrt{29}\right), \frac{1}{5}\left(1 - 2\sqrt{29}\right)\right).$$
Donc si on pose $\delta = 29$ (qui est bien un rationnel) alors les coordonnées des points d'intersection sont de la forme $\alpha + \beta\sqrt{\delta}$ $(\alpha, \beta \in \mathbb{Q})$, c'est-à-dire appartiennent à l'extension quadratique $\mathbb{Q}(\sqrt{29})$.



3. Soient le cercle $\mathscr{C}((-1,0),2)$ (qui a pour centre $A(-1,0)$ et passe par $B(1,0)$) et le cercle $\mathscr{C}((2,1),\sqrt{5})$ (qui a pour centre $A'(2,1)$ et passe par $B'(0,0)$). Les équations sont $(x+1)^2+y^2=4$, $(x-2)^2+(y-1)^2=5$. Les deux points d'intersection sont :
$$\left(\frac{1}{20}\left(7-\sqrt{79}\right),\frac{3}{20}\left(3+\sqrt{79}\right)\right),\left(\frac{1}{20}\left(7+\sqrt{79}\right),\frac{3}{20}\left(3-\sqrt{79}\right)\right).$$
Encore une fois, pour le rationnel $\delta=79$, les abscisses et ordonnées des points d'intersection sont de la forme $\alpha+\beta\sqrt{\delta}$ avec $\alpha,\beta\in\mathbb{Q}$; l'extension quadratique qui convient est donc $\mathbb{Q}(\sqrt{79})$.



4.2. Corollaires

La conséquence la plus importante du théorème de Wantzel est donnée par l'énoncé suivant. C'est ce résultat que l'on utilisera dans la pratique.

Corollaire 3.
Tout nombre réel constructible est un nombre algébrique dont le degré algébrique est de la forme 2^n, $n\geqslant 0$.

Démonstration. Soit x un nombre constructible. Par le théorème de Wantzel, il existe des extensions quadratiques $\mathbb{Q}=K_0\subset K_1\subset\cdots\subset K_r$ telles que $x\in K_r$. Donc x appartient à une extension de $\mathbb{Q}$ de degré fini. Ainsi, par la proposition 7, x est un nombre algébrique.

On sait de plus que $[K_{i+1} : K_i] = 2$, donc par la proposition 5, nous avons $[K_r : \mathbb{Q}] = 2^r$. Il nous reste à en déduire le degré algébrique $[\mathbb{Q}(x) : \mathbb{Q}]$. Comme $\mathbb{Q}(x) \subset K_r$, alors nous avons toujours par la proposition 5 que : $[K_r : \mathbb{Q}(x)] \times [\mathbb{Q}(x) : \mathbb{Q}] = [K_r : \mathbb{Q}] = 2^r$. Donc $[\mathbb{Q}(x) : \mathbb{Q}]$ divise 2^r et est donc de la forme 2^n. □

Voici une autre application plus théorique du théorème de Wantzel, qui caractérise les nombres constructibles.

Corollaire 4.
$\mathscr{C}_\mathbb{R}$ est le plus petit sous-corps de $\mathbb{R}$ stable par racine carrée, c'est-à-dire tel que :
- *$(x \in \mathscr{C}_\mathbb{R}$ et $x \geqslant 0) \Rightarrow \sqrt{x} \in \mathscr{C}_\mathbb{R}$,*
- *si K est un autre sous-corps de $\mathbb{R}$ stable par racine carrée alors $\mathscr{C}_\mathbb{R} \subset K$.*

La preuve est à faire en exercice.

5. Applications aux problèmes grecs

Nous allons pouvoir répondre aux problèmes de la trisection des angles, de la duplication du cube et de la quadrature du cercle, tout cela en même temps ! Il aura fallu près de 2 000 ans pour répondre à ces questions. Mais pensez que, pour montrer qu'une construction est possible, il suffit de l'exhiber (même si ce n'est pas toujours évident). Par contre pour montrer qu'une construction n'est pas possible, c'est complètement différent. Ce n'est pas parce que personne n'a réussi une construction qu'elle n'est pas possible ! Ce sont les outils algébriques qui vont permettre de résoudre ces problèmes géométriques.
Rappelons le corollaire au théorème de Wantzel, qui va être la clé pour nos problèmes.

Corollaire 5. *1. Si un nombre réel x est constructible alors x est un nombre algébrique. C'est-à-dire qu'il existe un polynôme $P \in \mathbb{Q}[X]$ tel que $P(x) = 0$.*

2. De plus le degré algébrique de x est de la forme 2^n, $n \geqslant 0$. C'est-à-dire que le plus petit degré, parmi tous les degrés des polynômes $P \in \mathbb{Q}[X]$ vérifiant $P(x) = 0$, est une puissance de 2.

5.1. L'impossibilité de la duplication du cube

La duplication du cube ne peut pas s'effectuer à la règle et au compas.

Cela découle du fait suivant :

Théorème 2.
$\sqrt[3]{2}$ n'est pas un nombre constructible.

Démonstration. $\sqrt[3]{2}$ est une racine du polynôme $P(X) = X^3 - 2$. Ce polynôme est unitaire et irréductible dans $\mathbb{Q}[X]$, donc $\sqrt[3]{2}$ est un nombre algébrique de degré 3. Ainsi son degré algébrique n'est pas de la forme 2^n. Bilan : $\sqrt[3]{2}$ n'est pas constructible. □

5.2. L'impossibilité de la quadrature du cercle

La quadrature du cercle ne peut pas s'effectuer à la règle et au compas.

C'est une reformulation du théorème suivant, dû à Ferdinand von Lindemann (en 1882) :

Théorème 3.
π n'est pas un nombre algébrique (donc n'est pas constructible).

Comme π n'est pas constructible, alors $\sqrt{\pi}$ n'est pas constructible non plus (c'est la contraposée de $x \in \mathscr{C}_\mathbb{R} \implies x^2 \in \mathscr{C}_\mathbb{R}$).
Nous ne ferons pas ici la démonstration que π n'est pas un nombre algébrique, mais c'est une démonstration qui n'est pas si difficile et abordable en première année.

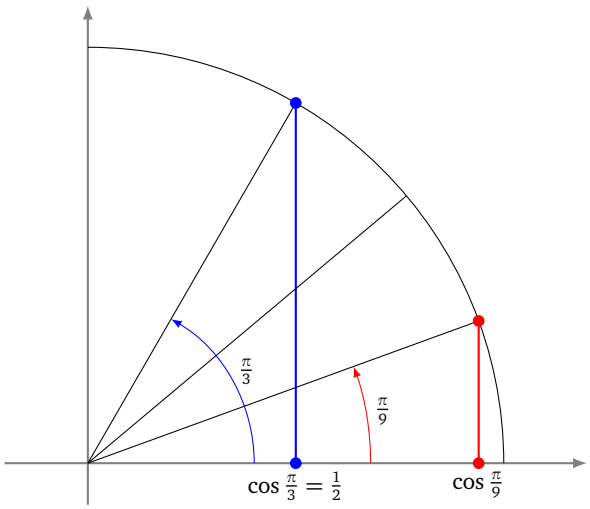
5.3. L'impossibilité de la trisection des angles

La trisection des angles ne peut pas s'effectuer à la règle et au compas.

Plus précisément nous allons exhiber un angle que l'on ne peut pas couper en trois.

Théorème 4.
L'angle $\frac{\pi}{3}$ est constructible mais ne peut pas être coupé en trois car $\cos\frac{\pi}{9}$ *n'est pas un nombre constructible.*

Bien sûr l'angle $\frac{\pi}{3}$ est constructible car $\cos\frac{\pi}{3} = \frac{1}{2}$. La preuve de la non constructibilité de l'angle $\frac{\pi}{9}$ fait l'objet d'un exercice : $\cos\frac{\pi}{9}$ est un nombre algébrique de degré algébrique 3, donc il n'est pas constructible.



La trisection n'est donc pas possible en général, mais attention, pour certains angles particuliers c'est possible : par exemple les angles π ou $\frac{\pi}{2}$!

Pour aller plus loin voici quelques références :

- *Théorie des corps. La règle et le compas.* J.-L. Carrega, Hermann, 2001.
  Un livre complet sur le sujet !
- *Nombres constructibles.* V. Vassallo, Ph. Royer, IREM de Lille, 2002.
  Avec un point de vue pour le collège et le lycée.
- *Sur les nombres algébriques constructibles à la règle et au compas.* A. Chambert-Loir, Gazette des mathématiciens 118, 2008.
  Vous trouverez dans cet article une réciproque du corollaire au théorème de Wantzel, prouvée de façon « élémentaire », c'est-à-dire sans faire usage de la théorie de Galois.

Auteurs du chapitre Arnaud Bodin.
Relu par Vianney Combet.