Constructions à la Règle et au Compas

Matthieu Boyer

Cours TalENS 6 2025-2026

Table des matières

Ce cours est basé sur `https://mathcircle.berkeley.edu/sites/default/files/handouts/2021/BMC_Adv_Constructions.pdf`

1 Positionnement du Problème

Définition 1.1 Dans toute la suite, on désignera par règle un outil permettant de tracer et de prolonger des lignes droites infiniement parfaites passant par deux points, et par compas un outil permettant de tracer des cercles parfaits à partir de leur centre et d'un rayon.

On s'intéresse au problème de construire des figures juste avec ces deux outils. C'est la manière fondamentale qu'avait Euclide de faire des preuves : étant donné une série d'axiomes, de constructions réalisables a priori, on sait définir la liste des constructions réalisables en général.

Proposition 1.2 Sont constructibles :

1. La bissectrice d'un segment ;
2. La perpendiculaire à une droite passant par un point sur la droite ;
3. La perpendiculaire à une droite passant par un point hors de la droite ;
4. La bissectrice d'un angle ;
5. La parallèle à une droite passant par un point hors de la droite ;
6. Un triangle semblable à un autre triangle avec un côté prescrit ;
7. La subdivision d'un segment en n parts égales pour $n \geq 1$.

Plus formellement, on va chercher à savoir quels nombres, quelles longueurs sont constructibles. Ici, on identifiera le plan euclidien avec l'ensemble $\mathbb{C}$ des nombres complexes, mais ce n'est pas nécessaire pour comprendre.

Définition 1.3 Le plan Euclidien est l'espace vectoriel $\mathbb{R}^2$ muni de la base $(0,1),(1,0)$ et du produit scalaire la rendant orthonormale.

En particulier, on notera

Définition 1.4 — Axiomatique. On se suppose capable de faire les constructions suivantes :

- R Étant donnés deux points z_1, z_2 on peut tracer la droite passant par ces points.
- C Étant donné un point z_1 et deux points distincts z_2, z_3, on peut tracer le cercle $\mathcal{B}(z_1, |z_2 - z_3|)$ de centre z_1 et de rayon $|z_2 - z_3|$.
- P_{ll} Étant données deux droites distinctes construites comme ci-dessus, on peut construire leur point d'intersection.
- P_{lc} Étant donnés une droite et un cercle construits comme ci-dessus, on peut construire leurs points d'intersections.
- P_{cc} Étant donnés deux cercles distincts construites comme ci-dessus, on peut construire leurs points d'intersections.

Définition 1.5 Le point $z \in \mathbb{C}$ est constructible s'il existe une suite finie d'opérations R, C, $\mathrm{P}_{\mathrm{ll,\ lc,\ cc}}$ qui commence avec les points $0, 1$ et qui termine en z. On note $\mathfrak{C}$ l'ensemble des nombres constructibles.

■ **Exemple 1.6** Tout entier m dans $\mathbb{Z}$ est constructible. Tout entier Gaussien $m + in \in \mathbb{Z}[i]$ est constructible. Les points $\frac{1}{2} \pm i\frac{\sqrt{3}}{2}$ sont constructibles. ■

Proposition 1.7 z est constructible si et seulement si son conjugué (symmétrique par rapport à la droite portant le segment $[0,1]$) l'est.

Théorème 1.8 Le n-gone régulier est constructible si et seulement si le point $\xi_n = e^{2i\pi/n}$ l'est.

La question qu'on se pose est donc la suivante : comment peut-on calculer $\mathfrak{C}$?

2 Al-Jabr

On va chercher une description algébrique de $\mathfrak{C}$, afin de savoir ce qui est constructible.

2.1 Structures

Définition 2.1 Un groupe $(G, \cdot)$ est un ensemble G muni d'une opération $\cdot$

- Associative : $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ pour tous $a, b, c \in G$;
- Unifère : il existe un élément $e \in G$ tel que $e \cdot g = g \cdot e = g$ pour tout $g \in G$;
- Inversible : pour $g \in G$, il existe $g^{-1} \in G$ tel que $g \cdot g^{-1} = g^{-1} \cdot g = e$.

Un morphisme de groupes est une application préservant l'opération de groupe. On parle de monomorphisme si elle est injective, epimorphisme si elle est surjective, et d'isomorphisme si elle est bijective.

■ **Exemple 2.2** $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ sont des groupes pour l'addition. Ce ne sont pas des groupes pour la multiplication.
On note $\mathfrak{S}_A$ le groupe des bijections $A \to A$ muni de la composition. Pour $A = [\![1, n]\!]$ on le note $\mathfrak{S}_n$. ■

Théorème 2.3 — Cayley Tout groupe G est isomorphe à un sous-groupe de $\mathfrak{S}_G$.

Définition 2.4 Un anneau est un groupe abélien pour l'addition de neutre 0 muni d'une multiplication associative, commutative, unifère pour 1 et distributive sur l'addition.

■ **Exemple 2.5** $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ sont des anneaux, $\mathbb{Z}/n\mathbb{Z}$ est un anneau pour l'addition et la multiplication modulo n. ■

Définition 2.6 Si R est un anneau, on note l'ensemble des polynômes à coefficients dans R d'indéterminée X par

$$R[X] = \left\{P = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n \,\middle|\, n \geq 0, a_i \in R\right\}$$

C'est aussi un anneau. Si $\alpha \in R$ et $P \in R[X] = \sum a_iX^i$, on note $P(\alpha) = \sum a_i\alpha^i$.

Définition 2.7 Un anneau est dit intègre s'il n'y a pas de diviseur de 0, i.e. d'éléments non nuls dont le produit est nul.

■ **Exemple 2.8** $\mathbb{R}$ est intègre, $\mathbb{Z}/5\mathbb{Z}$ est intègre, $\mathbb{Z}/6\mathbb{Z}$ ne l'est pas. ■

Définition 2.9 Un corps est un anneau avec $1 \neq 0$ dont tous les éléments non nuls sont inversibles.

■ **Exemple 2.10** $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ sont des corps. ■

Théorème 2.11 $\mathbb{Z}/p\mathbb{Z}$ est un corps si et seulement si p est premier.

Théorème 2.12 L'ensemble $\mathfrak{C}$ est un corps. De plus :

1. $z = a + ib \in \mathfrak{C}$ si et seulement si $a \in \mathfrak{C}$ et $b \in \mathfrak{C}$ pour $a, b \in \mathbb{R}$;
2. $z \in \mathfrak{C} \Rightarrow \sqrt{z} \in \mathfrak{C}$.

R Tout nombre complexe a deux racines carrées opposées, le deuxième point implique donc que les deux racines sont constructibles.

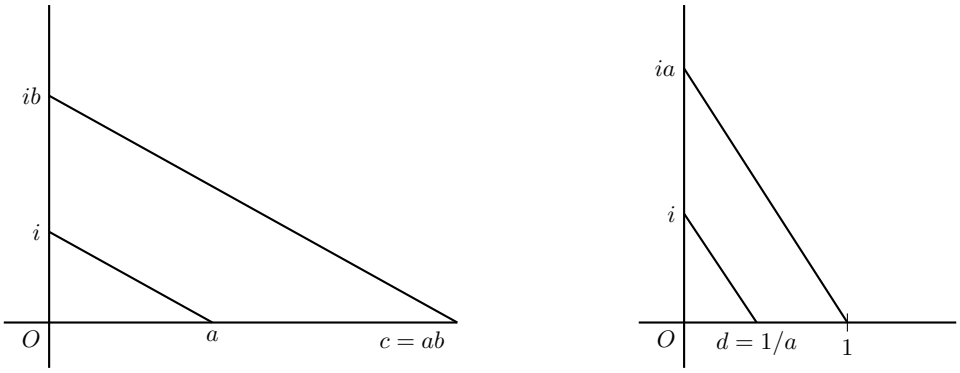
Démonstration. Pour montrer que $\mathfrak{C}$ est un corps, nous devons montrer qu'il contient 0 et 1, qu'il est stable par addition et multiplication, qu'il contient l'opposé de chacun de ses éléments, et qu'il contient l'inverse multiplicatif de chacun de ses éléments non nuls.

- Par définition, $0 \in \mathfrak{C}$ et $1 \in \mathfrak{C}$.
- Soit $0 \neq z \in \mathfrak{C}$, $L(0, z)$ et $C(0, |z|)$ s'intersectent en $\pm z$. Donc $-z \in \mathfrak{C}$.
- Soient $z, w \in \mathfrak{C}$, alors la ń règle du parallélogramme ż nous indique comment construire $z + w$ lorsque $0, z$ et w ne sont pas colinéaires : $C(z, |w|)$ et $C(w, |z|)$ ont $z + w$ comme l'un de leurs points d'intersection. Lorsque $0, z$ et w sont colinéaires, il est encore plus facile de construire $z + w$. Ainsi $z + w \in \mathfrak{C}$.

Jusqu'ici, nous avons prouvé que $\mathfrak{C}$ est un groupe additif (et que $1 \in \mathfrak{C}$).

Prouvons maintenant le premier point : Ensuite, si $z = a + ib \in \mathfrak{C}$, projetons orthogonalement z sur les axes x et y (ce qui est manifestement constructible). Nous obtenons $a \in \mathfrak{C}$ et $ib \in \mathfrak{C}$. Comme $C(0, |ib|)$ coupe l'axe des abscisses en b, on a $b \in \mathfrak{C}$. Réciproquement, si $a \in \mathfrak{C}$ et $b \in \mathfrak{C}$ (où $a, b \in \mathbb{R}$), alors $C(0, |b|)$ coupe l'axe des ordonnées en ib. Ainsi $ib \in \mathfrak{C}$ et par conséquent $z = a + ib \in \mathfrak{C}$ d'après ce que nous avons déjà démontré.

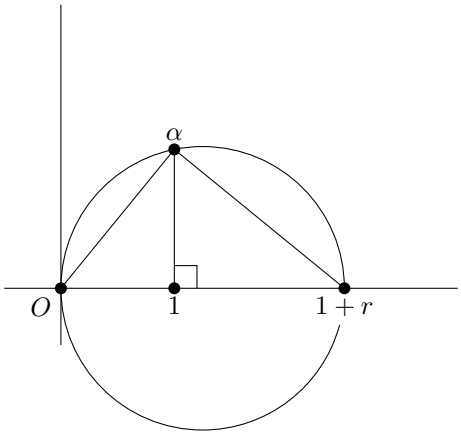
Pour prouver que $\mathfrak{C}$ est stable par multiplication et passage à l'inverse, nous allons d'abord prouver un résultat intermédiaire : $\mathfrak{C} \cap \{x \in \mathbb{R} \mid x > 0\}$ est stable par multiplication et passage à l'inverse. L'illustration suivante montre pourquoi cela est vrai. À partir de a ou b, nous construisons ia ou ib, puis nous traçons les droites parallèles appropriées, et nous raisonnons enfin avec des triangles semblables.



Il en découle immédiatement que $\mathfrak{C} \cap \mathbb{R}$ est un corps.

Nous pouvons maintenant montrer que $\mathfrak{C}$ est stable par multiplication et par l'inverse : Soient $z = a + ib \in \mathfrak{C}$ et $w = c + id \in \mathfrak{C}$. Alors $zw = (ac - bd) + i(ad + bc)$. En utilisant l'affirmation (a), puis le fait que $\mathfrak{C} \cap \mathbb{R}$ est un corps, et enfin de nouveau l'affirmation (a), il s'ensuit que $zw \in \mathfrak{C}$. De même, si $z \neq 0$, alors $\frac{1}{z} = \frac{a}{a^2+b^2} - i\frac{b}{a^2+b^2}$, et en utilisant le même raisonnement, nous voyons que $\frac{1}{z} \in \mathfrak{C}$.

Il ne reste plus qu'à prouver l'affirmation (b) : Soit $0 \neq z \in \mathfrak{C}$. Écrivons $z = re^{i\theta}$ avec $0 < r = |z| \in \mathbb{R}$. Nous devons construire $w = \sqrt{r}e^{i\theta/2}$. Puisque $z \in \mathfrak{C}$, il est clair que nous pouvons construire un angle de mesure θ. Comme nous pouvons diviser cet angle en deux (bissectrice), nous pouvons construire un angle de mesure $\theta/2$. Il est alors également clair que si nous pouvons construire $\sqrt{r}$, alors nous pouvons construire $w = \sqrt{z}$ et nous aurons terminé. Vous pouvez vérifier qu'il est possible de construire α comme dans la figure suivante et (en utilisant des triangles semblables) que le segment joignant 1 à α a pour longueur $\sqrt{r}$.



Par conséquent $\sqrt{z} \in \mathfrak{C}$ et la démonstration est terminée. ■

2.2 Polynômes

Dans cette partie R est un corps et on s'intéresse à des polynômes sur $R[X]$.

Définition 2.13 Le degré d'un polynôme P est la plus haute puissance de X dans P. On le note $\deg P$.

Définition 2.14 La division euclidienne de P' par P est l'unique couple (Q, R) tel que $P' = PQ + R$. On dit que P divise Q dans $R[X]$ quand $R = 0$. On note ceci $P \mid Q$. Un polynôme est irréductible s'il n'a pas de diviseur de degré > 0 autre que lui même.

Théorème 2.15 Si $\deg P > 0$, alors $(t-\alpha) \mid P$ si et seulement si $P(\alpha) = 0$. On dit que α est une racine de P.

Théorème 2.16 Dans $\mathbb{C}$, il n'y a pas de polynôme irréductible de degré > 2.

2.3 Extensions et Algébricité

Dans la suite, L et K sont des corps.

Définition 2.17 On dit que L est une extension du corps K quand $K \subseteq L$, ce qu'on note $L : K$. On appelle le degré de l'extension $L : K$ ou degré de L sur K la dimension de L comme K espace vectoriel, on la note $[L : K]$.

Définition 2.18 Soit K un corps et $X \subseteq K$. Le sous-corps de K engendré par X est le plus petit sous-corps de K contenant X. On le note $K(X)$.

Si $L : K$ est une extension de corps et $Y \subseteq L$, on note $K(Y)$ le sous-corps de L engendré par $K \cup Y$.

L'extension $L : K$ est dite simple si $L = K(\alpha)$ pour un certain $\alpha \in L$.

Par exemple, $\mathbb{Q}(\sqrt{2}) = \{p + q\sqrt{2} \mid p, q \in \mathbb{Q}\}$ et $\mathbb{R}(i) = \mathbb{C}$. L'extension $\mathbb{Q}(i, \sqrt{5}) : \mathbb{Q}$ est simple.

Définition 2.19 Soit $L : K$ une extension de corps. $\alpha \in L$ est algébrique sur K s'il existe un polynôme à coefficients dans K non nul dont α est racine. Sinon, α est dit transcendent.

$L : K$ est une extension algébrique si tout élément de L est algébrique sur K.

Définition 2.20 Soit $L : K$ une extension et $\alpha \in L$ algébrique sur K. Il existe un unique polynôme monique de plus petit degré dont α est racine. On l'appelle le polynôme minimal de α sur K et on le note m_α.

Théorème 2.21 On a $[K(\alpha) : K] = \infty$ si α est transcendent sinon $[K(\alpha) : K] = \deg m_\alpha$.

Proposition 2.22 Si $K_0 \subseteq K_1 \subseteq \cdots \subseteq K_n$ sont des corps, alors

$$[K_n : K_0] = \prod_{i=0}^{n-1} [K_{i+1} : K_i].$$

Proposition 2.23 Si $L : K$ est une extension de degré 2, alors $L = K(\sqrt{(}\alpha))$ pour $\alpha \in K$.

Définition 2.24 La clôture pythagoréenne $\mathbb{Q}^{py}$ de $\mathbb{Q}$ est le plus petit sous-corps de $\mathbb{C}$ stable par racine.

Théorème 2.25 $\mathfrak{C} = \mathbb{Q}^{py}$

Démonstration. On vérifie simplement l'inclusion $\mathfrak{C} \subseteq \mathbb{Q}^{py}$. Tout $z \in \mathfrak{C}$ est obtenue par une suite finie de constructions à partir de 0 et 1. Chaque point construit peut se voir comme une solution d'un système d'équations qui s'expriment avec des opérations de corps et des racines carrées à partir des points précédents. ■

Théorème 2.26 On a $z \in \mathfrak{C}$ si et seulement si il existe une suite d'extensions de $\mathbb{Q}$ par des sous-corps K_i de $\mathbb{C}$ tel que $z \in K_n$ et $[K_i : K_{i-1}] = 2$

Démonstration. Pour montrer que la condition est suffisante, on vérifie par récurrence que $K_i \subseteq \mathfrak{C}$. Puisque $K_i = K_{i-1}(\sqrt{\alpha})$ pour un certain $\alpha \in K_{i-1}$, $\alpha \in \mathfrak{C}$. De plus $\sqrt{\alpha} \in \mathfrak{C}$ et donc $K_i \subseteq \mathfrak{C}$.

Réciproquement, puisque $\mathfrak{C} = \mathbb{Q}^{py}$, z peut s'obtenir par une suite finie d'opérations de corps et de racines. Chaque étape dans cette suite peut se faire soit au sein d'un même corps soit par une extension de la forme $K_i = K_{i-1}(\sqrt{\alpha})$ qui produit une extension de degré 2. ■

Corollaire 2.27 Si $\alpha \in \mathfrak{C}$, alors $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg m_\alpha = 2^m$ pour $m \geq 0$.

2.4 Quelques résultats en conséquence

Proposition 2.28 Le cube ne peut pas être doublé à la règle et au compas.

Démonstration. Doubler le cube équivaut à construire $\alpha = \sqrt[3]{2} \in \mathbb{R}$, donc le polynôme minimal est $X^3 - 2$. En particulier, $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$ et donc $\alpha \notin \mathfrak{C}$. ■

Proposition 2.29 La quadrature du cercle est impossible à la règle et au compas.

Démonstration. La quadrature du cercle équivaut à la construction de $\sqrt{\pi}$. Si $\sqrt{\pi} \in \mathfrak{C}$ alors $\pi \in \mathfrak{C}$ et donc π est algébrique, ce qui n'est pas vrai. ■

Proposition 2.30 La trisection de l'angle n'est pas faisable à la règle et au compas.

Démonstration. L'angle de mesure $2\pi/3$ n'est pas trisectable. Cela reviendrait à construire $\xi_9 = e^{2i\pi/9}$. Si $\xi_9 \in \mathfrak{C}$, alors $\alpha = \xi_9 + \xi_9^{-1} \in \mathfrak{C}$. Or, α est une racine de $X^3 - 3X + 1 \in \mathbb{Q}[X]$, qui est irréductible sur $\mathbb{Q}$ et est donc son polynôme minimal, qui n'est pas de degré une puissance de 2. ■

Proposition 2.31 Soit $n > 2$ un entier. Le n-gone régulier peut être construit à la règle et au compas si et seulement si $n = 2^r p_1 \dots p_s$ où $r \geq 0$, $s \geq 0$ et les p_i sont des premiers de Fermat de la forme $p = 2^{2^k} + 1$.