Sur les nombres constructibles à la règle et au compas

Antoine Chambert-Loir

Université de Rennes 1, IRMAR (UMR 6625 du CNRS), Campus de Beaulieu, 35042 Rennes Cedex
Courriel : antoine.chambert-loir@univ-rennes1.fr

***Résumé.* —** Le but de cette note est de montrer que le critère classique pour qu'un nombre complexe soit constructible à la règle et au compas peut être établi sans faire usage de la théorie de Galois.

Dans toute cette note, nous identifions le corps $\mathbf{C}$ des nombres complexes au plan réel $\mathbf{R}^2$. Si $a, b \in \mathbf{C}$ sont des nombres complexes, on désigne par (ab) la droite passant par a et b et par $\mathscr{C}(a,b)$ le cercle de centre a qui passe par b.

Soit S une partie de $\mathbf{C}$ contenant 0 et 1. On dit qu'un nombre complexe z est *élémentairement constructible* (sous-entendu : à la règle et au compas) à partir de S s'il existe des points a, b, a', b' dans S tels qu'une des assertions suivantes soit vérifiée :

- les droites (ab) et $(a'b')$ ne sont pas parallèles et se croisent en z ;
- le cercle $\mathscr{C}(a,b)$ et la droite $(a'b')$ se rencontrent en z ;
- les cercles $\mathscr{C}(a,b)$ et $\mathscr{C}(a',b')$ se rencontrent en z.

On dit qu'un nombre complexe z est *constructible* (sous-entendu : à la règle et au compas) à partir de S s'il existe des points $z_1, \dots, z_n = z$ tels que, pour tout entier i tel que $1 \leqslant i \leqslant n$, z_i soit élémentairement constructible à partir de $S \cup \{z_1, \dots, z_{i-1}\}$.

Enfin, on dit qu'un nombre complexe z est constructible s'il l'est à partir de $\{0, 1\}$.

La construction classique d'une droite parallèle à une droite donnée et passant par un point donné, jointe au théorème de Thalès, implique facilement que si z, z' sont des nombres complexes constructibles (à partir d'une partie S, parfois sous-entendue dans la suite), il en est de même de $z + z'$, $z - z'$, zz' et, si $z' \neq 0$, z/z'.

De même, en traçant les droites passant par un point et perpendiculaires aux axes de coordonnées, on voit qu'un nombre complexe est constructible si et seulement s'il en est de même de sa partie réelle et de sa partie imaginaire. La valeur absolue d'un nombre constructible est constructible.

Soit z un nombre réel positif qui est constructible et traçons trois points B, H, C sur une droite, dans cet ordre, aux distances $BH = 1$ et $HC = z$. La perpendiculaire à (BC) passant par H et le cercle de diamètre BC se croisent en deux points, disons A et A'. Alors, $AH = \sqrt{z}$, ce qui démontre que la racine carrée d'un nombre réel positif constructible est elle-même constructible. En résolvant les équations pour la partie réelle et la partie réelle des racines carrées d'un nombre complexe, on constate que les racines carrées d'un nombre complexe constructible sont encore constructibles.

En écrivant les équations qui définissent les intersections droite–droite, droite–cercle et cercle–cercle, on constate que si un nombre complexe z est élémentairement constructible à partir d'une partie S, il satisfait une équation polynomiale de degré $\leqslant 2$ dont les coefficients appartiennent au sous-corps de $\mathbf{C}$ engendré par S. Inversement,

les solutions d'une telle équation s'expriment à l'aide d'une racine carrée. Renvoyant aux textes standard d'algèbre de base ou de théorie des corps pour plus de détails, les considérations précédentes impliquent le théorème suivant.

Théorème 1. — *Un nombre complexe z est constructible si et seulement s'il existe des sous-corps $\mathbf{Q} = F_0, \dots, F_n$ de $\mathbf{C}$ tels que $z \in F_n$ et tels que pour tout $i \in \{1, \dots, n\}$, F_i soit une extension quadratique de F_{i-1}.*

Remarque 1.1. — Soit S une partie de $\mathbf{C}$ contenant $\{0,1\}$. L'ensemble des nombres complexes qui sont constructibles à partir de S est le plus petit sous-corps de $\mathbf{C}$ contenant S qui soit stable par extraction de racine carrée.

Les corollaires suivants font référence aux définitions de base en théorie des corps, dont celle d'une extension finie, ainsi qu'à la multiplicativité des degrés. Pour tout cela, nous renvoyons aux textes d'algèbre de base. Rappelons tout de même que, par définition, un nombre algébrique est un nombre complexe z qui est racine d'un polynôme unitaire à coefficients rationnels. Il existe alors un tel polynôme M_z, et un seul, dont le degré est minimal ; c'est le polynôme minimal de z et son degré est appelé le degré de z ; les racines complexes de M_z sont appelées les *conjugués* de z.

Corollaire 1.2. — *Si un nombre complexe z est constructible, c'est un nombre algébrique et son degré est une puissance de* 2.

Démonstration. — Avec les notations du théorème 1, F_n est une extension finie de $\mathbf{Q}$ de degré 2^n, en particulier une extension algébrique. Puisque $z \in F_n$, c'est un nombre algébrique. De plus, $\mathbf{Q}(z)$ est une sous-extension de F_n dont le degré est précisément celui de z. Par multiplicativité des degrés, le degré de z divise 2^n, donc est une puissance de 2. □

Corollaire 1.3. — *Si un nombre complexe z est constructible, il en est de même de ses conjugués.*

Démonstration. — Soit z' un conjugué de z dans $\mathbf{C}$. Il existe un unique homomorphisme de corps $f_0 \colon \mathbf{Q}(z) \to \mathbf{C}$ tel que $f_0(z) = z'$. On peut l'étendre par récurrence en un homomorphisme de corps $f_n \colon F_n \to \mathbf{C}$. En considérant la suite de corps $(f_n(F_i))$, on voit que z' est constructible. □

Corollaire 1.4. — *Si un nombre complexe z est constructible, le corps engendré par ses conjugués est une extension finie de $\mathbf{Q}$ dont le degré est une puissance de* 2.

Démonstration. — Soit z une nombre complexe constructible, de conjugués $z_1, \dots, z_d$, où d est le degré de z. Il suffit de démontrer que chaque extension $\mathbf{Q}(z_1, \dots, z_{i-1}) \subset \mathbf{Q}(z_1, \dots, z_i)$ est de degré une puissance de 2, le degré de l'extension $\mathbf{Q} \subset \mathbf{Q}(z_1, \dots, z_d)$ étant le produit des degrés de ces extensions intermédiaires. Comme chaque z_i est constructible, il suffit de démontrer alors que pour tout sous-corps K de $\mathbf{C}$ et tout nombre complexe constructible z, l'extension $K \subset K(z)$ est finie de degré une puissance de 2.

Comme dans le théorème 1, choisissons une suite d'extensions quadratiques $\mathbf{Q} = F_0 \subset F_1 \subset \cdots \subset F_n$ telle que $z \in F_n$ et considérons la suite d'extensions composées $K = KF_0 \subset KF_1 \subset \cdots \subset KF_n$. Pour tout $i \in \{1, \ldots, n\}$, il existe un élément $a_i \in F_i$, de degré 2 sur F_{i-1} tel que $F_i = F_{i-1}(a_i)$. Par suite, $KF_i = KF_{i-1}(a_i)$. Comme le polynôme minimal de a_i sur KF_{i-1} divise celui de a_i sur F_{i-1}, il est de degré 1 ou 2 ; autrement dit, l'extension $KF_{i-1} \subset KF_i$ est de degré 1 ou 2. Par multiplicativité des degrés, le degré de l'extension $K \subset KF_n$ est une puissance de 2. Comme $z \in KF_n$, il en est de même du degré de la sous-extension $K \subset K(z)$, ce qui conclut la démonstration du corollaire. □

Ce dernier corollaire permet de démontrer que la réciproque du corollaire 1.2 n'est pas vraie. Il y a des polynômes $P \in \mathbf{Q}[X]$ de degré 4, irréductibles sur $\mathbf{Q}$, dont la résolvante cubique Q est encore irréductible sur $\mathbf{Q}$; on peut prendre par exemple $P = X^4 - X - 1$. Le corps F_P engendré par les racines complexes de P contient les racines de Q, qui sont toutes de degré 3. Par conséquent, le degré de F_P est un multiple de 3, donc n'est pas une puissance de 2.

Cependant, il est bien connu que la réciproque du corollaire 1.4 est vraie, donc fournit une condition nécessaire et suffisante pour qu'un nombre complexe soit constructible.

Théorème 2. — *Un nombre complexe est constructible si et seulement si c'est un nombre algébrique et que le corps engendré par ses conjugués est une extension finie de* $\mathbf{Q}$ *de degré une puissance de* 2.

La démonstration de ce théorème est souvent faite au moyen de théorie de Galois. La démonstration qui suit figure en exercice dans [**1, 2**] et est plus élémentaire ; elle s'inspire d'une preuve classique du théorème de d'Alembert-Gauß, voir par exemple [**3**] et constitue la seule partie peut-être originale de cette note.

Démonstration. — Soit z un nombre algébrique, de degré d, de conjugués $z_1, \ldots, z_d$. Supposons que le degré du corps $F = \mathbf{Q}(z_1, \ldots, z_d)$ soit une puissance de 2. Puisque ce corps contient $\mathbf{Q}(z_1)$, dont le degré est d, cela entraîne déjà que d est une puissance de 2. Raisonnons maintenant par récurrence sur d.

Soit $c \in \mathbf{Q}$. Soit $\mathscr{P}$ l'ensemble des paires $\{i, j\}$ d'entiers distincts satisfaisant $1 \leqslant i, j \leqslant d$. Pour toute telle paire $p = \{i, j\}$, posons $z_{p,c} = z_i + z_j + c z_i z_j$ et soit Q_c le polynôme $\prod_{p \in \mathscr{P}} (X - z_{p,c})$. On le considère comme un polynôme en X dont les coefficients sont des polynômes en $z_1, \ldots, z_d$. Toute permutation des z_i induit une permutation de l'ensemble des paires $\mathscr{P}$ et laisse donc le polynôme Q_c inchangé. Par conséquent, les coefficients de Q_c sont des polynômes symétriques en $z_1, \ldots, z_d$ (à coefficients dans $\mathbf{Q}$). D'après le théorème fondamental sur les fonctions symétriques,[(1)] ce sont des fonctions polynomiales à coefficients rationnels en les coefficients du polynôme minimal de z_1, donc des nombres rationnels. Autrement dit, $Q_c \in \mathbf{Q}[X]$.

[(1)] Pour être précis, il faudrait d'abord raisonner en remplaçant les z_i par des indéterminées Z_i, définissant ainsi un polynôme Q_c^* dont les coefficients sont des éléments de $\mathbf{Q}[Z_1, \ldots, Z_d]$, appliquer le théorème fondamental sur les polynômes symétriques à Q_c^* et évaluer enfin en $(z_1, \ldots, z_d)$.

Toute racine de Q_c engendre une extension de $\mathbf{Q}$ contenue dans F ; son degré est donc une puissance de 2. Ainsi, les degrés $d_1, \dots, d_e$, des facteurs irréductibles $Q_{c,1}, \dots, Q_{c,e}$ de Q_c sont des puissances de 2, disons $d_i = 2^{a_i}$. On a $d_1 + \cdots + d_e = \frac{1}{2}d(d-1)$. Notons aussi $d = 2^a$; l'exposant de 2 au membre de droite de la relation précédente est égal à $a-1$; au membre de gauche, il est au moins égal à $\min(a_1, \dots, a_e)$. Cela entraîne qu'au moins l'un de $a_1, \dots, a_e$, disons a_s, est inférieur ou égal à $a-1$. En d'autre mots, d_s divise $d/2$.

Les racines de $Q_{c,s}$ sont de la forme $z_{i,j,c}$; leur degré est une puissance de 2 qui divise $d/2 < d$. Elles engendrent un sous-corps de F, sous-corps dont le degré est donc aussi une puissance de 2. Par l'hypothèse de récurrence, les racines de $Q_{c,s}$ sont constructibles. Cela démontre qu'il existe une paire $p \in \mathscr{P}$ telle que $z_{p,c}$ soit constructible.

Jusqu'à présent, le nombre rationnel c était fixé, mais ce qui précède vaut pour tout c. Puisque le corps des nombres rationnels est infini, mais que l'ensemble $\mathscr{P}$ est fini, il existe deux nombres rationnels distincts c et c', et une paire $p = \{i, j\}$ comme ci-dessus, tels que $z_{p,c} = z_i + z_j + c z_i z_j$ et $z_{p,c'} = z_i + z_j + c' z_i z_j$ soient tous deux constructibles. Puisque les nombres constructibles forment un corps, il s'ensuit que $z_i + z_j$ et $z_i z_j$ sont constructibles. Alors z_i et z_j, étant les racines du polynôme quadratique $(X - z_i)(X - z_j)$ à coefficients constructibles, sont aussi des nombres constructibles (*cf.* les commentaires qui précèdent l'énoncé du théorème 1). Puisque $z_1, \dots, z_d$ sont conjugués de z_i, le corollaire 1.3 entraîne qu'ils sont tous constructibles, ce qu'il fallait démontrer. □

Références

[1] Antoine Chambert-Loir. *Algèbre corporelle*. Éditions de l'École polytechnique, 2005.

[2] Antoine Chambert-Loir. *A Field guide to Algebra*. Undergraduate Texts in Mathematics. Springer-Verlag, New York, 2005.

[3] Pierre Samuel. *Théorie algébrique des nombres*. Méthodes. Hermann, 1971.