Polygones constructibles à la règle et au compas

Perrine Jouteur

Ce développement se place dans les leçons 102, 121, 125 et 191, et il est contenu dans le livre *Théorie de Galois* de Ivan Gozard. On pourra aussi profiter du livre *Géométrie* de Michèle Audin pour donner des exemples d'applications du développement. L'objectif est le théorème suivant, dû à Gauss :

Théorème 0.1
Soit n un nombre entier plus grand que 2. On peut construire le polygone régulier à n côtés si et seulement si l'un des deux cas suivant est respecté :
(i) ou bien n est une puissance de 2 ;
(ii) ou bien il existe $\alpha \in \mathbb{N}$, $p_1, \cdots, p_r$ des nombres de Fermat premiers et distincts tels que $n = 2^\alpha p_1 \cdots p_r$.

En fait, on ne va pas le démontrer entièrement. On va faire l'implication directe, et une partie de la réciproque.

1 Prérequis

On doit savoir ce qu'est un nombre constructible, un angle constructible, un polygone constructible. On doit aussi connaître la définition de nombre de Fermat. Tout est dans l'ordre dans Gozard.

Lemme 1.1 Soit F un sous-corps de $\mathbb{R}$. On note $U = F \times F$ l'ensemble des points à coordonnées dans F. On note D l'ensemble des droites passant par deux points distincts de U, et C l'ensemble des cercles de centre un point de U et de rayon la distance de deux points de U.
Alors
(i) Si d_1 et d_2 sont deux droites non parallèles de D, alors leur intersection est un point de U.
(ii) Si $d_1 \in D$ et $\gamma \in C$, qui s'intersectent en un point M, alors ou bien $M \in U$ ou bien il existe une extension quadratique G de F tel que $M \in G \times G$.
(iii) Si $\gamma_1, \gamma_2 \in C$ s'intersectent en un point M, alors ou bien $M \in U$ ou bien il existe une extension quadratique G de F tel que $M \in G \times G$.

Démonstration voir Gozard ■

Proposition 1.1 Soit $x \in \mathbb{R}$ un nombre constructible.
Alors il existe une suite finie de sous-corps de $\mathbb{R}$, $L_0 \subset L_1 \subset \cdots \subset L_p$ telle que
(i) $L_0 = \mathbb{Q}$,
(ii) $[L_{i+1} : L_i] = 2$ pour tout $i \in [\![0, p-1]\!]$,
(iii) $x \in L_p$.

Démonstration
Comme x est constructible, il existe une suite finie $M_0, \cdots, M_n$ de points du plan tels que $M_n = (t, 0)$ et pour tout i, M_i est constructible à partir de $(0,0), (1,0)$ et $M_0, \cdots, M_{i-1}$.
Notons, pour tout i, $M_i = (x_i, y_i)$, $K_0 = \mathbb{Q}$ et $K_{i+1} = K_i(x_{i+1}, y_{i+1})$.
D'après le lemme précédent, pour tout i, ou bien $[K_{i+1} : K_i] = 0$ ou bien $[K_{i+1} : K_i] = 2$. On n'a plus qu'à extraire une suite strictement croissante de la suite $(K_0, \cdots, K_n)$, en ne conservant que les extensions quadratiques, et c'est gagné. ■

On a ensuite besoin de connaître un peu les polynômes cyclotomiques et les racines de l'unité.

Proposition 1.2 Soit $n \in \mathbb{N}^*$. Soit ω_n une racine primitive $n$ième de l'unité. Alors le polynôme minimal de ω_n sur $\mathbb{Q}$ est le nième polynôme cyclotomique, et donc

$$[\mathbb{Q}(\omega_n) : \mathbb{Q}] = \phi(n).$$

De plus, on a $\mathbb{Q}(\omega_n) \cap \mathbb{R} = \mathbb{Q}(\cos(\frac{2\pi}{n}))$ et

$$[\mathbb{Q}(\omega_n) : \mathbb{Q}(\cos(\frac{2\pi}{n}))] = 2.$$

2 Le développement

Lemme 2.1 Soient n, m deux entiers premiers entre eux. Le polygone régulier à nm côtés est constructible si et seulement si les polygones réguliers à n et m côtés respectivement sont constructibles.

Démonstration
• Si le polygone régulier à mn côtés est constructible, alors on peut construire $\sin(\frac{2\pi}{mn})$ et $\cos(\frac{2\pi}{nm})$. Le point d'angle $\frac{2\pi}{nm}$, sur le cercle unité, est donc constructible. Partant de ce point, on peut réitérer pour construire le point, sur le cercle unité, d'angle $\frac{2\pi}{nm} \times 2$, et ainsi de suite jusqu'aux points d'angles $\frac{2\pi}{n}$ et $\frac{2\pi}{m}$ respectivement.

• Si les polygones à n et m côtés sont constructibles, alors les points d'angle $\frac{2\pi}{n}$ et $\frac{2\pi}{m}$ sont constructibles. Comme les entiers n et m sont premiers entre eux, il existe des entiers a, b tels que $an + mb = 1$. On peut construire l'angle $\frac{2\pi}{n}$ donc on peut aussi construire l'angle $\frac{2\pi}{n}b$, et de même on peut construire l'angle $\frac{2\pi}{m}a$. Et on peut enfin construire l'angle

$$\frac{2\pi}{n}b + \frac{2\pi}{m}a = \frac{2\pi}{nm}(an + mb) = \frac{2\pi}{nm}.$$

Remarque 2.1 Si on a un entier n plus grand que 2, avec sa décomposition en facteurs premiers : $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, en itérant le lemme précédant, on a que le polygone régulier à n côtés est constructible si et seulement si les polygones réguliers à $p_i^{\alpha_i}$ côtés sont tous constructibles.

Proposition 2.1
• Pour tout $\alpha \in \mathbb{N}^*$, le polygone régulier à 2^α côtés est constructible.
• Soit p un nombre premier impair, et $\alpha \in \mathbb{N}^*$. Si le polygone régulier à p^α côtés est constructible alors $\alpha = 1$ et p est un nombre premier de Fermat.

Démonstration
• Remarquons que si $\alpha = 1$, comme $\frac{2\pi}{2} = \pi$, construire le point d'angle π revient à construire le point $(-1, 0)$, ce qui est possible en un coup de compas.

Pour $\alpha \geq 2$, on procède par récurrence.
Si $\alpha = 2$, alors $\frac{2\pi}{4} = \frac{\pi}{2}$, et le point $(0, 1)$ se construit comme l'intersection du cercle unité avec la médiatrice du segment $[(-1, 0), (1, 0)]$. Donc le polygone à 4 côtés est constructible.

Supposons que le polygone à 2^α côtés soit constructible. Alors le point $A = (\cos(\frac{2\pi}{2^\alpha}), \sin(\frac{2\pi}{2^\alpha}))$ soit constructible. On peut construire le milieu B du segment $[(1, 0), A]$. Et B n'est pas confondu avec l'origine, sinon A serait le point $(-1, 0)$ et donc α serait égal à 1. Ainsi on peut construire le point d'intersection de la droite $((0, 0), B)$ avec le cercle unité. Ce point est d'angle moitié par rapport à l'angle de A, donc c'est $(\cos(\frac{2\pi}{2^{\alpha+1}}), \sin(\frac{2\pi}{2^{\alpha+1}}))$. Ainsi le polygone à $2^{\alpha+1}$ côtés est constructible.

• Supposons que le polygone à p^α côtés soit constructible. Ceci revient à dire que le nombre $\cos(\frac{2\pi}{p^\alpha})$ est constructible. Par la proposition 1.1, il existe $e \in \mathbb{N}$ tel que $[\mathbb{Q}(\cos(\frac{2\pi}{p^\alpha})) : \mathbb{Q}] = 2^e$.
Or on a vu en proposition 1.2 que l'extension $\mathbb{Q}(\cos(\frac{2\pi}{p^\alpha}))$ est de degré $\phi(p^\alpha)/2 = p^{\alpha-1}(p-1)/2$. D'où

$$p^{\alpha-1}(p-1) = 2^{e+1}.$$

Donc ou bien $p = 2$ et $\alpha = e + 2$, ou bien $\alpha = 1$ et $p - 1 = 2^{e+1}$. Comme on s'est placé dans le cas où p est impair, on a nécessairement $\alpha = 1$ et $p = 2^{e+1} + 1$. Ainsi p est un nombre premier de Fermat. ■

Remarque 2.2 En fait, la réciproque du deuxième point est vraie : le polygone à p^α côtés est constructible si et seulement si p est de Fermat et $\alpha = 1$. Pour la réciproque, on a besoin de la théorie de Galois.