Théorème de Wantzel

CloudSea

Cadre

Soit $\mathcal{C}$ le corps des nombres constructibles à la règle et au compas.
$t \in \mathcal{C}$ si et seulement si t appartient à une tour d'extensions $\mathbb{Q} = K_0 \subseteq \cdots \subseteq K_n$ où $[K_{i+1} : K_i] = 2$ pour tout i

Recasages :
- [[125 Extensions de corps]]
- [[127 Nombres remarquables]]
- [[148 Dimension d'un espace vectoriel]]
- [[191 Géométrie]]

Référence : Invitation à l'algèbre Janneret

lemme : Soit $\mathcal{P}$ un ensemble de points et K le sous corps de $\mathcal{C}$ engendré par les coordonnées des points de $\mathcal{P}$, soit $M = (x, y)$ un point constructible en une étape à partir de $\mathcal{P}$. Alors $[K(x, y) : K] = 1$ ou 2

Déroulé du développement

lemme : Soit $\mathcal{P}$ un ensemble de points et K le sous corps de $\mathcal{C}$ engendré par les coordonnées des points de $\mathcal{P}$, soit $M = (x, y)$ un point constructible en une étape à partir de $\mathcal{P}$. Alors $[K(x, y) : K] = 1$ ou 2

Montrer le lemme, en déduire le sens direct

1er cas, M est l'intersection de deux droites engendrées par $\mathcal{P}$

Soient $M_i = (a_i, b_i)$ $1 \leq i \leq 4$ tels que $M_1 \neq M_2$ et $M_3 \neq M_4$ et tels que $D_1 = (M_1M_2)$, $D_2 = (M_3M_4)$ s'intersectent en M.
On a $M \in D_1$ ssi $(a_2 - a_1)(y - b_1) = (b_2 - b_1)(x - a_1)$. Or $M_1 \neq M_2$ donc $a_2 - a_1$ ou

$b_2 - b_1$ est non nul, donc l'équation précédente se ré écrit $y = \alpha_1 x + \beta_1$ ou $x = \alpha_1 y + \beta_1$ avec $\alpha_1, \beta_1 \in K$. Donc en substituant x ou y dans l'équation $M \in D_2$, on montre que x et y sont solution d'une équation linéaire à coefficients dans K, donc $x, y \in K$, donc $[K(x, y) : K] = 1$

2e cas, M est l'intersection d'une droite et un cercles engendrés par $\mathcal{P}$

Soit $D = (M_1 M_2)$ où $M_i = (a_i, b_i)$ et $M_1 \neq M_2$, et soit C le cercle de centre $M_3 = (a_3, b_3)$ et de rayon r où r est la distance entre deux points distincts de $\mathcal{P}$. On suppose que D et C s'intersectent en M.
Comme dans le cas 1, on a $x = \alpha y + \beta$ ou $y = \alpha x + \beta$. Supposons par exemple que $x = \alpha y + \beta$. Et comme $M \in C$, on a $(x - a_3)^2 + (y - b_3)^2 = r^2$ avec $r^2 \in K$
En substituant x dans la 2e équation, on montre que y est solution d'une équation de degré 2 à coefficients dans K, donc $[K(y) : K] = 1$ ou 2. Puis comme x dépend affinement de y on a $x \in K(y)$, donc $[K(x, y) : K] = [K(y) : K] = 1$ ou 2

3e cas, M est l'intersection de deux cercles engendrés par $\mathcal{P}$

Soient C_1 et C_2 deux cercles de centres différents qui s'intersectent en M, de centres (a_1, b_1) et (a_2, b_2) et de rayons r_1 et r_2.
On a donc le système d'équations

$$\begin{cases} (x - a_1)^2 + (y - b_1)^2 = r_1^2 \\ (x - a_2)^2 + (y - b_2)^2 = r_2^2 \end{cases}$$

En soustrayant la 1ere équation à la 2e on obtient

$$\begin{cases} (x - a_1)^2 + (y - b_1)^2 = r_1^2 \\ 2(a_1 - a_2)x + 2(b_1 - b_2)y + a_2^2 - a_1^2 + b_2^2 - b_1^2 = r_2^2 - r_1^2 \end{cases}$$

Donc on est ramené au cas 2, donc on a bien $[K(x, y) : K] = 1$ ou 2

En déduire le sens direct

Soit $t \in \mathcal{C}$ et $M_1, \cdots, M_n = (t, 0)$ une suite de points qui mène à la construction de t
Soit K_i le corps engendré par les coordonnées de $M_1, \cdots M_i$ et $K_0 = \mathbb{Q}$, on a montré que pour tout $i < n$ $[K_{i+1} : K_i] = 1$ ou 2. Donc en ne gardant que les K_i tels que $[K_i : K_{i-1}] = 2$, on obtient bien une tour d'extension quadratique dont le dernier terme est K_n

Montrer que si K est un sous corps de $\mathcal{C}$ et L une extension quadratique de K alors $L \subseteq \mathcal{C}$

L est une extension quadratique de K donc $L = K(\alpha)$ où α est algébrique sur K de degré 2 donc α est racine d'un polynôme $X^2 + bX + c$. Donc $\alpha = \dfrac{-b \pm \sqrt{\Delta}}{2}$, donc $L = K(\sqrt{\Delta})$. Donc comme $\mathcal{C}$ est un corps stable par racine carrée, on a $\sqrt{\Delta} \in \mathcal{C}$, donc $L \subseteq \mathcal{C}$

En déduire la réciproque

Si t appartient à une tour d'extensions quadratiques $K_0 = \mathbb{Q} \subseteq \cdots \subseteq K_n$, alors en appliquant le résultat précédent successivement à $K = K_i$ et $L = K_{i+1}$ pour $i = 0$ à $n-1$, on obtient $K_n \subseteq \mathcal{C}$ et donc $t \in \mathcal{C}$

Détail de certains points

Détailler l'argument du sens direct

Soient $i_1, \cdots i_p$ les indices tels que $[K_i : K_{i-1}] = 2$ on considère la tour d'extensions $\mathbb{Q} \subseteq K_{i_1} \subseteq \cdots \subseteq K_{i_p}$
Soit $1 \leq k \leq p$, par construction on a $[K_{i_k} : K_{i_{k-1}}] = [K_{i_k} : K_{i_k - 1}] \cdots [K_{i_{k-1}+1} : K_{i_{k-1}}] = 2 \times 1 \times \cdots \times 1 = 2$, et $[K_n : K_{i_p}] = [K_n : K_{n-1}] \cdots [K_{i_p+1} : K_{i_p}] = 1 \times \cdots \times 1 = 1$, donc $K_{i_p} = K_n$, donc on obtient bien une tour d'extensions quadratiques dont le dernier terme est K_n

Montrer que $\mathcal{C}$ est stable par racine carrée (a faire à la fin si le temps)

Soit $a \in \mathcal{C}$ tel que $a > 0$, on considère les points $A = (a, 0)$ et $B = (-1, 0)$. On trace le cercle dont $[AB]$ est un diamètre. Il coupe Oy en un point $C = (0, y)$, on va montrer que $y = \sqrt{a}$
En faisant Pythagore trois fois, on obtient

$$\begin{cases} BC^2 = OB^2 + OC^2 \\ AC^2 = OA^2 + OC^2 \\ AB^2 = AC^2 + BC^2 \end{cases}$$

Donc on a

$$\begin{aligned} AB^2 = OA^2 + 2OC^2 + OB^2 &\Leftrightarrow (a+1)^2 = a^2 + 2y^2 + 1 \\ &\Leftrightarrow a^2 + 2a + 1 = a^2 + 2y^2 + 1 \\ &\Leftrightarrow a = y^2 \\ &\Leftrightarrow y = \sqrt{a} \end{aligned}$$

Version révisions

Soit $\mathcal{C}$ le corps des nombres constructibles à la règle et au compas, on se propose de montrer que $t \in \mathcal{C}$ si et seulement si t appartient à une tour d'extensions $\mathbb{Q} = K_0 \subseteq \cdots \subseteq K_n$ où $[K_{i+1} : K_i] = 2$ pour tout i

Soit $\mathcal{P}$ un ensemble de points et K le sous corps de $\mathcal{C}$ engendré par les coordonnées des points de $\mathcal{P}$, soit $M = (x, y)$ un point constructible en une étape à partir de $\mathcal{P}$, on va montrer que $[K(x, y) : K] = 1$ ou 2

1. 1er cas : M est l'intersection de deux droites
   1.1 Montrer que x ou y est solution d'une équation de degré 1, et appartient donc à K
   1.2 En déduire que l'autre aussi en faisant une substitution

2. 2e cas : M est l'intersection d'une droite et d'un cercle
   2.1 Montrer que x ou y est racine d'un polynôme de degré 2, disons que c'est x
   2.2 En déduire que $[K(x) : K] = 1$ ou 2
   2.3 Montrer que $y \in K(x)$ et conclure

3. 3e cas : M est l'intersection de deux cercles
   3.1 Se ramener au cas 2 en soustrayant les deux équations de cercle

4. En déduire le sens direct du théorème de Wantzel
5. Montrer que si L est une extension quadratique de K un sous corps de $\mathcal{C}$, alors $L \subseteq \mathcal{C}$
6. En déduire la réciproque