Théorème de Gauss-Wantzel

1 Constructions à la règle et au compas

Théorème 1 *(Théorème de Pilau Wantzel) Un nombre réel est constructible à la règle et au compas si, et seulement si, il existe une tour d'extensions quadratiques* $\mathbb{Q} = L_0 \subset L_1 \subset \ldots \subset L_k$ *telles que* L_{i+1} *soit une extension quadratique de* L_i.

2 Le théorème de Gauss-Wantzel

Note historique : Gauss a démontré le sens direct une trentaine d'années avant la publication par Wantzel de son théorème qui est une des clés de voûte du sens réciproque.

Théorème 2 *Un polygone régulier* P_n *à* n *côtés est constructible à la règle et au compas si et seulement si* $n = 2^i \Pi_{j=1}^r p_j$ *où les* p_j *sont des nombres premiers de Fermat distincts.*

Fait 1 *Dire que* P_n *est constructible à la règle et au compas est équivalent à dire que* $cos(2\pi/n)$ *est constructible à la règle et au compas.*

Fait 2 *Preuve :* $sin(x) = \sqrt{1 - cos(2\pi/n)^2}$.

Fait 3 *Le polygone régulier à* 2^i *côté est constructible.*

Fait 4 *Si* P_n *est constructible et* P_m *est constructible avec* m, n *premiers entre eux alors* P_{mn} *est constructible.*

Fait 5 *Si* P_n *est constructible et* $m|n$ *alors* P_m *est constructible.*

Fait 6 *Si* $n = \Pi_{i=1}^r p_i^{\alpha_i}$ *alors* P_n *est constructible si et seulement si chacun des* $P_{p_i^{\alpha_i}}$ *est constructible.*

Preuve du sens direct : par les faits qui précèdent on peut se limiter au cas $n = p_j^{\alpha_j}$ *tel que* P_n *soit constructible à la règle et au compas. Alors* $cos(2\pi/n)$ *est constructible et par suite comme* $Q(\omega)$ *où* ω *est une racine primitive* $n - eme$ *de l'unité est constructible. Or le polynôme minimal de cette racine est le polynôme cyclotomique. Or son degré est* $p_j^{\alpha_j - 1}(p_j - 1)$. *Par le théorème de Wantzel ce nombre doit être une puissance de 2. Pour des raisons arithmétiques,* p_j *est forcément un nombre premier de Fermat.*

Preuve du sens réciproque : $n = 2^k + 1$. *Il faut trouver une tour d'extension quadratiques qui permet de construire* ω. *Considérons* $\mathbb{Q}(\omega)$ *qui est de degré* 2^k *sur* $\mathbb{Q}$. *Soit* G *le groupe des automorphismes de corps de* $\mathbb{Q}(\omega)$. *Remarquons qu'un tel automorphisme envoie nécessairement* ω *sur* ω^k. *L'application*

$$\Psi : x \in G \mapsto k, x(\omega) = \omega^k$$

est un isomorphisme de groupe sur $(Z/pZ)^*$ *donc en particulier* G *est cyclique et engendré par un élément* σ, *qui envoie* ω *sur* ω^2 *puis* ω^4. *Les* $\sigma^{2^{k-i}}(\mathbb{Q}(\omega))$ *forment une suite de corps décroissants qui contiennent* $\mathbb{Q}$. *Chaque extension est de degré au plus* 2 *et exactement* 2 *car* $Q(\omega)$ *est de degré* $2^k + 1$. *Ainsi* P_n *est constructible.*

3 Les questions téléphonées

Nombre premier de Fermat, précisez la forme.
$2^k+1 = 2^{2^p}+1$, *car* 2^k+1 *premier, or* $2^{b2^a}+1 = c^a+1 = (c+1)(\sum(-1)^k c^{a-1-k}$.
Cyclicité du groupe $(Z/pZ)^*$ *?* $\phi(p) = p-1$.

Références

— *Francinou, Gianella.*