102 – Groupe des nombres complexes de module 1. Sous-groupes des racines de l'unité. Applications.

Question.

Donner un nombre complexe de module 1 qui ne soit pas une racine de l'unité.

Réponse.

$e^{i\pi a}$ avec $a \notin \mathbb{Q}$.

Question.

Existe-t'il un nombre algébrique de module 1 qui ne soit pas une racine de l'unité ?

Réponse.

On a

$$\cos\theta = \frac{1-t^2}{1+t^2} \quad \text{et} \quad \sin\theta = \frac{2t}{1+t^2}$$

avec $t := \tan\left(\frac{\theta}{2}\right)$, d'où

$$e^{i\theta} = \frac{1-t^2}{1+t^2} + i\frac{2t}{1+t^2}.$$

Soit θ tel que $\tan\left(\frac{\theta}{2}\right) = \frac{1}{2}$, alors

$$\begin{aligned} e^{i\theta} &= \frac{1-\frac{1}{4}}{1+\frac{1}{4}} + i\frac{1}{1+\frac{1}{4}} \\ &= \frac{3}{5} + \frac{4}{5}i. \end{aligned}$$

Son polynôme minimal est

$$\left(\frac{5}{4}\left(X - \frac{3}{5}\right)\right)^2 + 1 = X^2 - \frac{6}{5}X + 1$$

après simplification. Ce n'est pas un polynôme de $\mathbb{Z}[X]$ donc ce n'est pas un polynôme cyclotomique, donc $e^{i\theta}$ n'est pas une racine de l'unité mais est bien un nombre algébrique.

Question.

$SO_2(\mathbb{R}) \simeq \mathbb{S}^1$, y a-t'il un analogue pour $SO_3(\mathbb{R})$?

Réponse.

Oui avec le groupe G des quaternions de module 1 : on a $G \simeq S^3$ et $G/\{-1,1\} \simeq SO_3(\mathbb{R})$.

Question.

Soit $P \in \mathbb{Z}[X]$ unitaire et irréductible tel que toutes ses racines soient de module ≤ 1. Montrer que $P = X$ ou que P est un polynôme cyclotomique.

Réponse.

Supposons $P \neq X$. Alors P est irréductible donc 0 n'est pas racine de P et, d'après le théorème de Kronecker, ses racines sont des racines de l'unité. De plus, les racines de P sont simples car P est irréductible (sinon il serait divisible par $P \wedge P'$ non trivial) et donc $P \mid X^N - 1$ pour un certain N.
Or

$$X^N - 1 = \prod_{d \mid N} \Phi_d$$

avec Φ_d irréductible sur $\mathbb{Z}$.
$P \neq 1$ donc $P = \Phi_k$ pour un certain k.

Question.

Qu'est-ce qu'un nombre constructible ?

Réponse.

On commence par définir la notion de point constructible dans un plan euclidien.
Un point P est constructible en une étape à partir de E si P est un point de E ou si P est dans l'intersection de deux objets distincts parmi :
- l'ensemble des droites qui passent par deux éléments distincts de E,
- l'ensemble des cercles centrés en un point de E et dont le rayon est la distance de deux points quelconques de E.

On note $C_1(E)$ l'ensemble des points constructibles en une étape à partir de E.
L'ensemble $C_n(E)$ des points constructibles en n étapes est défini par récurrence par $C_{n+1}(E) := C_1(C_n(E))$.

L'ensemble des points constructibles à partir de E est alors la réunion des $C_n(E)$ pour $n \in \mathbb{N}^*$.
Finalement, un nombre réel est constructible s'il est abscisse d'un point constructible à partir de $\{(0,0),(0,1)\}$.

Question.

La définition donnée précédemment suppose que l'on puisse reporter les longueurs avec le compas. Qu'est-ce qu'on obtient si on suppose que ce n'est plus le cas ?

Réponse.

En fait on peut reporter des longueurs sans utiliser de compas. En effet, ce problème revient à se donner trois points distincts A, B, C et à construire le cercle de centre C et de rayon AB. Cela revient à compléter ABC en un parallélogramme $ABCD$. Pour ce faire, on commence par tracer la diagonale AC et on place le milieu O de $[AC]$ en construisant sa médiatrice (ceci est possible en traçant la droite passant par l'intersection entre le cercle de centre C et de rayon AC et celui de centre A et de rayon AC). On trace alors la droite (BO) et on place le point D en traçant le cercle de centre O et de rayon OB.

Question.

Donner l'idée de la preuve du théorème de Wantzel.

Réponse.

– Constructible $\Rightarrow$ existence d'une tour d'extension quadratique :
  On montre facilement que le produit de deux nombres constructibles est constructible, ainsi que l'inverse d'un nombre constructible (par exemple avec Thalès). En partant du nombre 1 constructible, on peut alors construire $\mathbb{Q}$, et dès qu'on construit un nombre non rationnel on peut alors construire l'extension qu'il engendre. On va donc construire successivement des extensions de $\mathbb{Q}$.
  On suppose qu'on a construit une extension $\mathbb{K}/\mathbb{Q}$ et on regarde les extensions de $\mathbb{K}$ que l'on peut construire en une étape. On considère ainsi les intersections suivantes : entre deux droites, entre une droite et un cercle, entre deux cercles, sachant que les équations des droites et des cercles sont à coefficients dans $\mathbb{K}$. L'équation d'une droite étant de degré 1, l'intersection entre deux droites reste dans $\mathbb{K}$. L'équation d'un cercle étant de degré 2, l'intersection entre une droite et un cercle crée une extension quadratique réelle (ou reste dans $\mathbb{K}$). On peut aussi montrer que l'intersection entre deux cercles revient à l'intersection entre un des cercles et la droite passant par les points d'intersections entre ces deux cercles (car en écrivant l'égalité entre les équations de cercle, les carrés

disparaissent). Au final, on crée au plus une extension quadratique réelle en une étape.

- Existence d'une tour d'extension quadratique $\Rightarrow$ constructible :
  Il suffit de montrer que si un élément est racine d'un polynôme du second degré sur $\mathbb{K}$, alors il est constructible à partir de $\mathbb{K}$. Pour cela, on montre que l'on peut construire la racine carrée d'un nombre (par exemple en utilisant Pythagore et la relation $\frac{1}{2}\sqrt{(a+1)^2-(a-1)^2} = \sqrt{a}$) et on sait que les racines d'un polynôme du second degré s'exprime en fonction de radicaux.

Question.

Sachant construire le triangle et le pentagone réguliers, comment construire le polygone régulier à 15 côtés ?

Réponse.

Savoir construire un polygone régulier à m côtés revient à savoir construire l'angle $\widehat{\frac{2\pi}{m}}$. On cherche une relation de Bezout entre 3 et 5 : $2 \times 5 - 3 \times 3 = 1$, on a alors

$$\frac{\widehat{2\pi}}{15} = 2 \times \frac{\widehat{2\pi}}{3} - 3 \times \frac{\widehat{2\pi}}{5}.$$