Nombres constructibles

Parimaths, 23 avril 2016

Quelques problèmes anciens (datant du Vème siècle avant J.-C.)

Est-il possible de réaliser ces constructions à la règle et au compas ?

- *La quadrature du cercle* (1882)
  Construire un carré ayant la même aire qu'un cercle donné.
- *La duplication du cube/problème de Délos* (1837)
  Construire l'arête d'un cube ayant un volume deux fois plus grand que le volume d'un cube donné.
- *La trisection de l'angle*(1837)
  Construire les demi-droites partageant un angle quelconque en trois angles égaux.
- *Le problème des polygones réguliers*(1837)
  Construire, pour chaque $n > 2$, un polygone regulier ayant n côtés.

Exercice 1

Trouver des méthodes (à la règle et au compas) d'addition, de multiplication, de division et d'extraction de racine carrée.

Points constructibles

Un point M du plan euclidien est dit constructible s'il existe une suite finie $M_1, \dots, M_n$ de points du plan telle que $M_n = M$ et, pour tout i, M_i est un point d'intersection de droites ou cercles constructibles c.à.d. obtenus à l'aide de l'ensemble $\{O, I, M_1, \dots, M_{i-1}\}$.

Un angle dessiné par deux droites constructibles est dit constructible.

Exercice 2

Soit D et E des droites constructibles, A et B des points constructibles. Montrer que :

- Le point J$(1,\frac{\pi}{2})$ est constructible.
- La perpendiculaire à D passant par A est constructible.
- La parallèle à D passant par A est constructible.
- Le milieu et la médiatrice du segment [AB] sont constructibles.
- Les bissectrices des angles déterminés par ces D et E sont constructibles.

Nombres constructibles

Un nombre réel t est dit constructible si c'est une des coordonnées dans le repère (O,I,J) d'un point constructible.

Exercice 3

Montrer que : t est constructible ⇔ le point de l'axe Ox d'abscisse t est constructible.

Exercice 4*

Montrer que l'ensemble C des nombres constructibles est le plus petit sous-corps de $\mathbb{R}$ stable par racine carrée et contenant $\mathbb{Q}$.

Extensions de corps

Soit K un corps. Un corps L est dit une extension du corps K s'il existe une application ψ de K dans L non nulle qui respecte l'addition et la multiplication (morphisme de corps).

Exercice 5 Montrer que ψ est injective et que K peut être vu comme un sous-corps de L.

Soit $K \subset L$ une extension de corps (cette notation a un sens d'après l'exercice précédent). Et $a_1, \dots, a_n \in$L, on note K($a_1, \dots, a_n$) le plus petit sous-corps de L contenant K et $a_1, \dots, a_n$.

Exercice 6 Déterminer $\mathbb{Q}(1)$; $\mathbb{Q}(2/3)$; $\mathbb{Q}(\sqrt{2})$; $\mathbb{Q}(\sqrt{3})$; $\mathbb{Q}(\sqrt{2},\sqrt{3})$; $\mathbb{R}(i)$

Exercice 7 Soit $K \subset L$ une extension de corps. Montrer que L est un espace vectoriel sur K.

La dimension de L en tant qu'espace vectoriel sur K est notée [L : K].

Exercice 8

Soit $K \subset L$ et $L \subset M$ deux extensions de corps. Montrer que $K \subset M$ est une extension de corps et que [M : K] = [M : L].[L : K].

Un élément $a \in L$ est dit algébrique sur K s'il existe un polynôme non nul $P \in K[X]$ tel que P(a) = 0. Sinon, il est transcendant sur K.

Exercice 9*

Soit $a \in L$ un élément algébrique sur K. Montrer que

- n=[K(a) : K] est fini.
- Il existe un unique polynôme $P \in K[X]$ de degré n, unitaire et tel que P(a) = 0.
- Il n'existe pas de polynôme non nul Q de degré strictement inférieur tel que Q(a) = 0.
- $K(a) = \{\alpha_0 + \alpha_1 a + \cdots + \alpha_{n-1}a^{n-1} / \alpha_0, \dots, \alpha_{n-1} \in K\}$.

Le polynôme P est dit polynôme minimal de a. On dit que a est algébrique de degré n sur K.

Le théorème de Wantzel

Exercice 10* Supposons [L : K] = 2. Montrer que $\exists a \in K, L = K(\sqrt{a})$.

Lemme 1 (très calculatoire)

Soit $A(a_1, a_2), B(b_1, b_2), C(c_1, c_2)$ des points distincts. (AB) est décrite par une équation de type $\alpha x + \beta y + \gamma = 0$, où $\alpha, \beta, \gamma \in \mathbb{Q}(a_1, a_2, b_1, b_2)$ et le cercle de centre A et de rayon BC est décrit par une équation de type $x^2 + y^2 - 2\alpha x - 2\beta y + \gamma = 0,\ \alpha, \beta, \gamma \in \mathbb{Q}(a_1, a_2, b_1, b_2, c_1, c_2)$.

Exercice 11* (Théorème de Wantzel, 1837)

Soit $t \in \mathbb{R}$, t est un nombre constructible si et seulement si il existe une suite finie $L_1, \dots, L_p$ de sous-corps de $\mathbb{R}$ telle que :

- L1 = $\mathbb{Q}$,
- Pour $1 \leq j \leq p-1,\ L_j \subset L_{j+1}\ et\ [L_{j+1} :\ L_j\ ] = 2$,
- $t \in L_p$.

Exercice 12

Montrer que tout nombre constructible est algébrique sur $\mathbb{Q}$ de degré une puissance de 2. Réciproque ? On pourra examiner le polynôme $X^4 + 2X - 2$.

Retour aux problèmes anciens

Exercice 13 Déduire du théorème de Wantzel que la duplication du cube est impossible.

Exercice 14 Montrer que l'angle θ est constructible $\Leftrightarrow \cos\theta$ constructible.

Puis que $\frac{\pi}{3}$ n'est pas «trissectable».

Exercice 15$^{\infty}$ (Lindemann, 1882) Montrer que e et π sont transcendants sur $\mathbb{Q}$.

Exercice 16 En déduire que la quadrature du cercle est impossible.

Un nombre est dit "de Fermat" s'il est de la forme $2^{2^k}+1$ avec $k \in \mathbb{N}$. On ne connait aujourd'hui que cinq nombres premiers de Fermat : 3, 5,17,257 et 65537.

Exercice 17$^{\frac{\infty}{2}}$ (Gauss, 1801, Wantzel, 1837). Montrer qu'un polygone régulier à n côtés est constructible si et seulement si n est le produit d'une puissance de 2 et d'un nombre quelconque de nombres premiers de Fermat distincts.

Exercice 18

Montrer que l'angle de $\frac{\pi}{2^n}$ est constructible pour tout $n \in \mathbb{N}$.

Exercice 19

Soient m et n tel que $m \wedge n = 1$. Montrer que

- L'angle de $\frac{\pi}{mn}$ est constructible $\Leftrightarrow \frac{\pi}{m}$ et $\frac{\pi}{n}$ le sont.
- L'exercice 17 se réduit à montrer que, pour $n = p^a$ avec p premier, le polygone régulier à n côtés est constructible $\Leftrightarrow$p = 2 ou a = 1 et p est un nombre de Fermat.

Problèmes bonus

Exercice 20*

Soit α algébrique sur $\mathbb{Q}$. Notons $\mathbb{Q}_\alpha = \{P(\alpha), P \in \mathbb{Q}[X]\}$, et φ: $\begin{matrix}\mathbb{Q}[X] \to \mathbb{Q}_\alpha \\ P \mapsto P(\alpha)\end{matrix}$

Notons μ_α le polynôme minimal de α (cf. exercice 9), et d son degré. Montrer que :

- φ est un morphisme d'anneau
- $Ker(\varphi) = \mu_\alpha\mathbb{Z}$
- $\mathbb{Q}_\alpha = Vect\left(1, \alpha, \dots, \alpha^{d-1}\right)$
- $\mathbb{Q}_\alpha$ est un corps (on pensera à Bézout…)
- Si α et β sont algébriques, $\alpha+\beta$ et $\alpha\beta$ le sont aussi.

Exercice 21 Montrer que l'ensemble des nombres algébriques sur $\mathbb{Q}$ est dénombrable.

Exercice 22*

- Montrer que $\exists!\,(T_n) \in \mathbb{Z}[X]^{\mathbb{N}}, \forall n \in \mathbb{N}, \forall t \in \mathbb{R}, T_n(2\cos(t)) = 2\cos(nt)$. Déterminer le coefficient dominant de T_n.
- Trouver les rationnels r tels que $\cos(r\pi) \in \mathbb{Q}$.
- En déduire les entiers $n \geq 3$ tels qu'il existe un polygone régulier à n côtés dans le plan complexe dont les sommets ont des coordonnées rationnelles.

Exercice 23**(reprise de l'exercice 15)

Montrons par l'absurde que e est transcendant. Soit $P = b_0 + \cdots + b_r X^r \in \mathbb{Z}[X]$ avec $P(e) = 0$. Soit p un nombre premier avec $p > \max(|b_0|, r)$.

Notons $Q(X) = x^{p-1}(x-1)^p \ldots (x-r)^p$, n le degré de Q et $\forall k \in \mathbb{N}, I(k) = \int_0^k e^{k-t} Q(t) dt$.

- Montrer par plusieurs IPP que $\forall k \in \mathbb{N}, I(k) = e^k \sum_{i=0}^n Q^{(i)}(0) - \sum_{i=0}^n Q^{(i)}(k)$
- Notons J=$b_0 I(0) + \cdots + b_r I(r)$, Montrer que $J = -\sum_{k=0}^r b_k \sum_{i=0}^n Q^{(i)}(k)$
- Vérifier que J est un entier, évaluer chaque terme puis J modulo p!
- En déduire que $|J| \geq (p-1)!$
- Par ailleurs, majorer brutalement J.
- Conclure, quant p tend vers l'infini.

Lemme 2 : Inégalité des accroissements finis

Soit f dérivable sur [a,b] et M un majorant de f'. Montrer que $f(b) - f(a) \leq M(b-a)$.

Exercice 24 (Liouville)

Soit $S \in \mathbb{Q}[X]$, irréductible (sur $\mathbb{Q}[X]$) avec $n = \deg(S) \geq 2$.

- Donner un exemple de tel polynôme.
- Montrer que S n'admet pas de racine rationnelle.
- Montrer que $\exists C \in \mathbb{N}^*$, tel que $\forall p, q \in \mathbb{Z} * \mathbb{N}^*, |S\left(\frac{p}{q}\right)| \geq \frac{1}{Cq^n}$
- Soit α une racine de S. Avec le lemme 2, montrer que $\exists K > 0$ tel que $\forall p, q \in \mathbb{Z} * \mathbb{N}^*$ tel que $\frac{p}{q} \in [\alpha - 1, \alpha + 1]$, on a $|\alpha - \frac{p}{q}| \geq \frac{K}{q^n}$
- Soit $\forall n \in \mathbb{N}, L_n = \sum_{k=0}^n 10^{-k!}$. Montrer que (L_n) converge. On note L sa limite.
- Prouver que L est irrationnel, et que $\forall n, |L - L_n| \leq 2.10^{-(n+1)!}$.
- Conclure que L est transcendant.

Exercice 25* (Lambert 1761, raisonnement d'Ivan Niven)

Supposons π rationnel : on note $\pi = \frac{a}{b}$ et $I_n = \int_0^\pi \frac{x^n(a-bx)^n}{n!} \sin(x) dx$.

- Intégrer par partie 2n fois pour montrer que $\forall n, I_n \in \mathbb{Z}$.
- Encadrer I_n et faire tendre n vers l'infini puis conclure que π est irrationnel.

Exercice 26**(retour sur l'exercice 19)

Soit $n = p^\alpha$, où un polygone régulier à n côtés est constructible. Notons $\omega = e^{\frac{2i\pi}{p^\alpha}}$ et $\mu(X) \in \mathbb{Z}[X]$ le p^α-ième polynôme cyclotomique. Montrer que (on peut admettre le troisième point)

- $\exists m \in \mathbb{N}, \left[\mathbb{Q}\left(cos\frac{2\pi}{p^\alpha}\right) : \mathbb{Q}\right] = 2^m$
- $\left[\mathbb{Q}(\omega) : \mathbb{Q}\left(cos\frac{2\pi}{p^\alpha}\right)\right] = 2$
- $\mu(X)$ est irréductible et de degré $p^{\alpha-1}(p-1)$, et que $\mu(\omega) = 0$
- $2^{m+1} = p^{\alpha-1}(p-1)$
- Conclure que $\alpha = 1$ et p est de Fermat