Constructions à la règle et au compas

Dans toute cette feuille, *constructible* signifie *constructible à la règle et au compas.*

Exercice 1. (Un algébrique de degré 4 non constructible)
Soit P le polynôme $X^4 + X + 1$ et x une racine de P dans $\mathbf{C}$. Le but de cet exercice est de montrer que x n'est pas constructible.

1. Montrer que P est irréductible sur $\mathbf{Q}$.
2. On suppose par l'absurde que x est constructible. Montrer qu'il existe une extension finie de $\mathbf{Q}$, formée de nombres constructibles, sur laquelle P se factorise en produit de deux polynômes de degré 2.
3. Montrer que parmi les coefficients de ces deux polynômes se trouve une racine de
$$Q(X) = X^6 - 4X^2 - 1.$$
4. Montrer que dans $\mathbf{Q}[X]$, Q possède un facteur (irréductible) de degré 2, puis un facteur de degré 2 de la forme $X^2 + n$, pour un entier relatif n.
5. Conclure.

Exercice 2. (Constructibilité des polygones réguliers)
Pour tout entier $n \geq 2$, on note $\zeta_n = e^{2i\pi/n}$. On s'intéresse ici à la constructibilité du nombre ζ_n ou plus géométriquement à celle de l'angle $2\pi/n$ ou encore du n-gone régulier.

1. Montrer que ζ_{2^k} est constructible pour tout k dans $\mathbf{N}^*$.
2. Soit n et m dans $\mathbf{N}^*$ premiers entre eux ; montrer que ζ_n et ζ_m sont constructibles si et seulement si ζ_{nm} l'est.
3. Un nombre premier p est dit *de Fermat* si $p-1$ est une puissance de 2. Montrer que les nombres premiers de Fermat sont de la forme $2^{2^m} + 1$. Quels sont les premiers nombres premiers de Fermat ?
4. Soit $p \geq 3$ un nombre premier. Montrer que si ζ_p est constructible, alors p est de Fermat.
5. Le but de cette (longue) question est de démontrer la réciproque de la question précédente. Soit donc $p = 2^{2^m} + 1$ un nombre premier de Fermat.
   (a) Soit n dans $\mathbf{N}^*$ premier à p.
      i. Montrer qu'il existe un unique automorphisme du corps $\mathbf{Q}(\zeta_p)$ qui envoie ζ_p sur ζ_p^n ; on le note σ_n.
      ii. Montrer que σ_n ne dépend que de la classe de n modulo p.
      iii. Montrer que l'ensemble des points fixes de σ_n dans $\mathbf{Q}(\zeta_p)$ forme un sous-corps de $\mathbf{Q}(\zeta_p)$.
   (b) Soit u dans $\mathbf{N}^*$ premier à p dont la classe modulo p engendre $(\mathbf{Z}/p\mathbf{Z})^\times$; pour tout m dans $\mathbf{N}$, on note τ_m l'automorphisme $\sigma_{u^{2^m}}$ et K_m le sous-corps de $\mathbf{Q}(\zeta_p)$ formé des points fixes de τ_m.
      i. En choisissant une base de $\mathbf{Q}(\zeta_p)$ sur $\mathbf{Q}$ adéquate, montrer que K_0 est égal à $\mathbf{Q}$.
      ii. Montrer qu'on a pour tout m dans $\mathbf{N}$: $\tau_{m+1} = \tau_m \circ \tau_m$.

iii. Montrer que pour tout m dans $\mathbf{N}$, K_{m+1} est une extension de degré au plus 2 de K_m.

iv. Déduire de ce qui précède que ζ_p est constructible.

6. Décrire une construction explicite du pentagone régulier à la règle et au compas.
7. Déterminer, pour $n \in \{1, \ldots, 20\}$, si l'angle de n degrés est constructible. En déduire un nouvel exemple d'angle constructible et non trisectable.

Exercice 3. (Constructibilité des polygones réguliers, suite et fin)
Dans l'étude de la constructibilité des polygones réguliers, le cas laissé ouvert par l'exercice précédent est celui des ζ_{p^i}, où p est un nombre premier impair et $i \geq 2$. Le but de cet exercice est de pallier ce manque.
Si n est un entier quelconque, on appelle *n-ième polynôme cyclotomique* le polynôme

$$\Phi_n(\mathrm{X}) = \prod_k (\mathrm{X} - \zeta_n^k),$$

où k décrit l'ensemble des éléments de $\{1, \ldots, n\}$ premiers avec n.

0. Dans cette question uniquement, on admet que Φ_n est un élément irréductible de $\mathbf{Z}[\mathrm{X}]$. Montrer que les nombres ζ_{p^i}, pour p premier impair et $i \geq 2$, ne sont jamais constructibles.

Les trois prochaines questions démontrent le même résultat sans rien admettre sur Φ_n.

1. Soit p un nombre premier impair. Écrire explicitement les polynômes Φ_p et Φ_{p^2}. Montrer le résultat admis à la question 0 quand $n = p$.
2. Montrer que si n et m sont entiers, la constructibilité de ζ_{nm} entraîne celle de ζ_n. En déduire que la non-constructibilité de ζ_{p^2} entraîne celle de tous les ζ_{p^i}, pour $i \geq 2$.
3. En utilisant le critère d'Eisenstein, montrer que $\Phi_{p^2}(\mathrm{X}+1)$ est irréductible. En déduire la non-constructibilité de ζ_{p^2}.
4. Pour quels entiers n le nombre ζ_n est-il constructible ?

Exercice 4. (Clôture quadratique)
On dit qu'un corps L est *quadratiquement clos* si tout polynôme de degré 2 à coefficients dans L admet une racine dans L. Si L/K est une extension, on dit que L est une *clôture quadratique* de K si L est quadratiquement clos et si aucun sous-corps $\mathrm{K} \subset \mathrm{L}' \subsetneq \mathrm{L}$ ne l'est.

1. Soit K un corps. Démontrer qu'une clôture quadratique de K existe et qu'elle est unique à isomorphisme près.
2. Décrire des clôtures quadratiques de $\mathbf{Q}$, $\mathbf{R}$ et $\mathbf{C}$.
3. Soit $\mathbf{F}_q$ un corps fini de caractéristique différente de 2. Montrer que tout polynôme de degré 2 de $\mathbf{F}_q$ a une racine dans $\mathbf{F}_{q^2}$. En déduire une clôture quadratique de $\mathbf{F}_q$. Est-elle algébriquement close ?