Constructions à la règle et au compas : correction

Exercice 1.
$\sqrt[3]{2}$ est racine du polynôme $X^3 - 2 \in \mathbf{Q}[X]$. Ce dernier est irréductible (par exemple d'après le critère d'Eisenstein) : c'est donc le polynôme minimal de $\sqrt[3]{2}$ sur $\mathbf{Q}$. Cela montre que le nombre algébrique $\sqrt[3]{2}$ est de degré 3 : il ne peut donc être constructible à la règle et au compas.

Exercice 2.

1. Pour tout ω, on a $\cos(3\omega) = 4\cos^3(\omega) - 3\cos(\omega)$. On a donc bien
$$4\cos^3(\theta/3) - 3\cos(\theta/3) - \cos(\theta) = 0 \text{ soit } \left(2\cos(\theta/3)\right)^2 - 3\left(2\cos(\theta/3)\right) - 2\cos\theta = 0.$$
2. En particulier, $2\cos(\pi/9)$ est racine de $X^3 - 3X - 1$. Il s'agit de montrer que ce polyôme est irréductible dans $\mathbf{Q}[X]$: en effet, on aura alors $\mu_{\mathbf{Q}}^{2\cos(\pi/9)}(X) = X^3 - 3X - 1$, ce qui montre que $2\cos(\pi/9)$ (et donc $\cos(\pi/9)$) est de degré 3 et donc non constructible. On ne peut donc pas construire à la règle et au compas un angle de $\pi/9$.
   Le polynôme $X^3 - 3X - 1$ n'a pas de racine entière (pour $r \notin \{0, \pm 1\}$, $|r|^3 > 3|r| + 1$ et on vérifie à la main que ces trois nombres ne sont pas racines) ; comme il est unitaire et que $\mathbf{Z}$ est intégralement clos, cela implique qu'il n'a pas de racine dans $\mathbf{Q}$ et, étant de degré 3, il est bien irréductible dans $\mathbf{Q}[X]$.

Exercice 3.

1. Dans $\mathbf{F}_2[X]$, le polynôme $X^4 + X + 1$ est irréductible : en effet, il n'a pas de racine et ne peut pas s'écrire comme produit de deux irréductibles de degré 2 (il n'y a qu'un seul irréductible de degré 2, $X^2 + X + 1$, et $X^4 + X + 1 \neq (X^2 + X + 1)^2 = X^4 + X^2 + 1$). Le polynôme unitaire $X^4 + X + 1$ est donc irréductible dans $\mathbf{Q}[X]$.
2. Par hypothèse, il existe une suite d'extensions $\mathbf{Q} = K_0 \subset K_1 \subset \cdots \subset K_m$ avec $x \in K_m$ et $[K_{i+1} : K_i] = 2$. On peut supposer que $x \notin K_{m-1}$. Alors le polynôme minimal de x sur K_{m-1} est de degré 2, et divise P dans $K_{m-1}[X]$.
3. Soit $P = (X^2 + aX + b)(X^2 + cX + d)$ la décomposition de la question précédente. En développant et en identifiant les coefficients, on a donc
$$\begin{cases} a + c &= 0 \\ b + ac + d &= 0 \\ ad + bc &= 1 \\ bd &= 1. \end{cases} \Leftrightarrow a \neq 0 \text{ et } \begin{cases} c &= -a \\ b + d &= a^2 \\ d - b &= 1/a \\ bd &= 1. \end{cases}$$
   Les deuxième et troisième équations entraînent $2d = a^2 + 1/a$ et $2b = a^2 - 1/a$. La quatrième équation s'écrit donc $4 = (a^2 + 1/a)(a^2 - 1/a)$ ou encore $a^4 - a^{-2} = 4$. Le coefficient a est donc bien racine de $Q(X) = X^6 - 4X^2 - 1$.
4. Par construction, $Q \in \mathbf{Q}[X]$ a une racine a constructible, dont le degré $\deg \mu_{\mathbf{Q}}^a$ est de ce fait une puissance de 2 inférieure à 6.
   On vérifie facilement que Q n'a pas de racine entière. Puisqu'il est unitaire et que $\mathbf{Z}$ est intégralement clos, cela entraîne qu'il n'a pas de racine dans $\mathbf{Q}$. On a donc $\deg_{\mathbf{Q}}^a \in \{2, 4\}$.

Que $\deg^a_{\mathbf{Q}}$ vaille 2 ou 4, on a trouvé une décomposition $Q = Q_2Q_4$ de Q en produit de deux polynômes unitaires, l'un de degré 2 et l'autre de degré 4. Puisque Q n'a pas de racine, Q_2 est irréductible.

Comme on a en outre $Q(X) = Q(-X) = Q_2(-X)Q_4(-X)$, Q_2 doit diviser $Q_2(-X)$ ou $Q_4(-X)$.

– Si Q_2 divise $Q_2(-X)$, alors $Q_2 = Q_2(-X)$, et ceci impose que Q_2 soit de la forme $X^2 + n$ ($n \in \mathbf{Q}$).

– Sinon, Q_2 divise $Q_4(-X)$, donc $Q_2(X)$ et $Q_2(-X)$ divisent $Q_4(X)$. On peut alors écrire $Q = Q_2(X)Q_2(-X)\tilde{Q}(X)$, ce qui entraîne $\tilde{Q}(X) = \tilde{Q}(-X)$, et donc $\tilde{Q}(X) = X^2 + n$ ($n \in \mathbf{Q}$).

Dans les deux cas, $-n \in \mathbf{Q}$ doit être le carré d'une racine (complexe) de Q, donc doit être entier sur $\mathbf{Z}$. Comme $\mathbf{Z}$ est intégralement clos, $n \in \mathbf{Z}$ et Q possède un facteur irréductible de la forme $X^2 + n$ ($n \in \mathbf{Z}$).

5. Soit α une racine carrée (complexe) de n. Alors α est racine de Q ; donc $n = \alpha^2$ est racine de $X^3 - 4X - 1$, qui n'a pas de racine entière, d'où une contradiction. Donc x n'est pas constructible.

Exercice 4.

1. Le polynôme minimal de ζ_n est Φ_n, qui est de degré $\varphi(n)$. Donc si ζ_n est constructible, alors $\varphi(n)$ est une puissance de 2.
2. Soit $n = 2^k p_1^{\alpha_1} \dots p_s^{\alpha_s}$ la décomposition en nombres premiers de n ($k \in \mathbf{N}$, $\alpha_i \geq 1$). Alors
$$\varphi(n) = \varphi(2^k)\varphi(p_1^{\alpha_1}) \dots \varphi(p_s^{\alpha_s}) = 2^{k-1}\ (p_1 - 1)p_1^{\alpha_1 - 1} \cdots (p_n - 1)p_n^{\alpha_n - 1}.$$
Donc si $\varphi(n)$ est une puissance de 2 si et seulement si pour tout $1 \leq i \leq s$, $\alpha_i = 1$ et $p_i - 1$ est une puissance de 2. Autrement dit, $\varphi(n)$ est une puissance de 2 si et seulement si la partie impaire de n est un produit de nombres premiers de Fermat [1]différents.
3. Soit n et m premiers entre eux. On peut trouver une relation de Bézout : $un + vm = 1$. Si ζ_m et ζ_n sont constructibles, il en va alors de même de $\zeta_{mn} = \zeta_{mn}^{un}\zeta_{mn}^{vn} = \zeta_m^u\zeta_n^v$.
Réciproquement, si ζ_{mn} est constructible, alors $\zeta_n = \zeta_{mn}^m$ et $\zeta_n = \zeta_{mn}^n$ le sont aussi.
4. Pour construire ζ_{2^k}, il suffit de construire des bissectrices successives (en partant de l'angle π).
5. (a) i. Notons qu'un automorphisme de corps de $\mathbf{Q}(\zeta_p)$ doit automatiquement être l'identité sur $\mathbf{Q}$ (car il l'est sur 0 et 1) : les notions de morphismes d'anneaux (ou de corps) et de $\mathbf{Q}$-algèbres sont les mêmes.
En outre, comme $\mu_{\mathbf{Q}}^{\zeta_p} = \Phi_p$, on a $\mathbf{Q}(\zeta_p) \simeq \mathbf{Q}[X]/(\Phi_p(X))$. Cela en détermine les endomorphismes de $\mathbf{Q}$-algèbres : on a une bijection (cf. TD 1, exercice 2)
$$\begin{array}{ccc} \mathrm{Hom}_{\mathbf{Q}\text{-Alg}}(\mathbf{Q}(\zeta_p), \mathbf{Q}(\zeta_p)) & \to & \left\{ z \in \mathbf{Q}(\zeta_p) \,\middle|\, \Phi_p(z) = 0 \right\} \\ \varphi & \mapsto & \varphi(\zeta_p). \end{array}$$
Il y a donc un unique morphisme (de corps ou de $\mathbf{Q}$-algèbres, c'est pareil) $\sigma_n : \mathbf{Q}(\zeta_p) \to \mathbf{Q}(\zeta_p)$ envoyant ζ_p sur ζ_p^n. Cet endomorphisme est en outre injectif

1. Montrons la question subsidiaire. Par définition, un nombre premier de Fermat peut se mettre sous la forme $p = 2^r + 1$. Écrivons $r = r_0 r_1$, où r_0 est une puissance de 2 et r_1 est impaire. Alors
$$p = 2^{r_0 r_1} + 1 = (2^{r_0})^{r_1} + 1 = (2^{r_0} + 1)((2^{r_0})^{r_1 - 1} - (2^{r_0})^{r_1 - 2} + \cdots - 2^{r_0} + 1).$$
La primalité de p entraîne donc $r_1 = 1$, et $r = r_0$ est une puissance de 2.

($\mathbf{Q}(\zeta_p)$ est un corps) donc, $\mathbf{Q}(\zeta_p)$ étant un $\mathbf{Q}$-espace vectoriel de dimension finie, c'est un automorphisme.

ii. C'est évident car ζ_p^n ne dépend que de la classe de n modulo p.

iii. De manière générale, on vérifie immédiatement que l'ensemble des points fixes d'un automorphisme de corps est un sous-corps.

(b) i. Le polynôme annulateur de ζ_p est Φ_p, de degré $\varphi(p) = p-1$. La famille $(\zeta_p, \zeta_p^2, \dots, \zeta_p^{p-1})$ est donc une $\mathbf{Q}$-base de $\mathbf{Q}(\zeta_p)$.
Soit $x \in \mathbf{Q}(\zeta_p)$ un élément fixe par τ_0. Décomposons-le dans la base que nous avons choisie : $x = a_1\zeta_p + \cdots + a_{p-1}\zeta_p^{p-1}$, avec des rationnels a_i.

On a alors pour tout $k \in \mathbf{N}$, $\tau_0^k(x) = a_1\zeta_p^{u^k} + \cdots + a_{p-1}\zeta_p^{(p-1)u^k} = x$. Puisque l'on a pris soin de prendre u générateur de $(\mathbf{Z}/p\mathbf{Z})^\times$, cela signifie que la multiplication par u est un automorphisme de $(\mathbf{Z}/p\mathbf{Z})^\times$, d'ordre $p-1$ exactement. Donc pour tout $j \in \{1, \dots, p-1\}$, il existe $k \in \{1, \dots, p-1\}$ tel que $\zeta_p^{ju^k} = \zeta_p$, et alors, en identifiant les coefficients de x dans la base, on a $a_j = a_1$. Donc en fait x est de la forme $a_1(\zeta_p + \cdots + \zeta_p^{p-1}) = -a_1 \in \mathbf{Q}$.

ii. C'est évident, il suffit de le vérifier pour ζ_p.

iii. On va démontrer que si $\varphi : \mathrm{L} \to \mathrm{L}$ est un automorphisme involutif (*i.e.* tel que $\varphi^2 = \mathrm{id}$) d'un corps de caractéristique nulle, le sous-corps fixe

$$\mathrm{K} = \left\{ x \in \mathrm{L} \,\middle|\, \varphi(x) = x \right\}$$

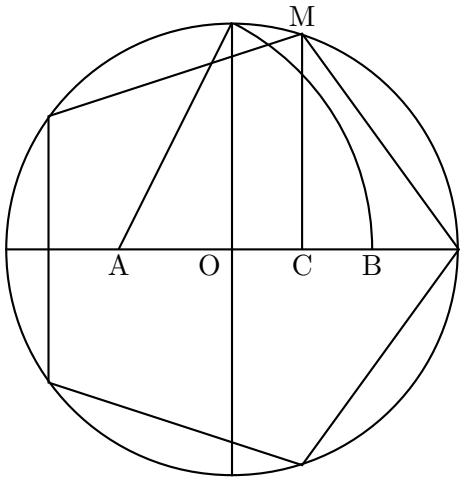
est tel que L/K est une extension de degré 1 (dans le cas où $\varphi = \mathrm{id}_\mathrm{L}$) ou 2. Il suffira ensuite d'appliquer ce résultat à $\mathrm{L} = \mathrm{K}_{m+1}$ et $\varphi = \tau_m$ (ce qui entraîne $\mathrm{K} = \mathrm{K}_m$).

Le morphisme $\varphi : \mathrm{L} \to \mathrm{L}$, vu comme application K-linéaire, est diagonalisable (il est annulé par $\mathrm{X}^2 - 1$ qui est scindé à racines simples, car la caractéristique n'est pas 2) de spectre inclus dans $\{\pm 1\}$. L'espace propre associé à la valeur propre 1 est K. Supposons qu'il existe $z \in \mathrm{L}$ non nul tel que $\varphi(z) = -z$. Tout autre $z' \in \mathrm{L}$ tel que $\varphi(z') = -z'$ vérifie alors $\varphi(z'/z) = \varphi(z')/\varphi(z) = z'/z$, c'est-à-dire $z'/z \in \mathrm{K}$. On a donc montré que l'espace propre associé à la valeur propre -1, s'il existe, est une droite. Au final, on a bien $\dim_\mathrm{K} \mathrm{L} \in \{1, 2\}$.

iv. Puisque p est un nombre premier de Fermat, $p = 2^\mathrm{N} + 1$, et $u^{2^\mathrm{N}} \equiv 1 \pmod{p}$, donc $\tau_\mathrm{N} = \mathrm{id}$. Ainsi, $\mathbf{Q}(\zeta_p) = \mathrm{K}_\mathrm{N}$, et d'après la question précédente, ceci prouve que ζ_p est constructible.

6. On a ainsi prouvé une sorte de réciproque à la question 2, à savoir que le polygone régulier à n côtés est constructible si et seulement si n est de la forme $2^k p_1 \dots p_i$, où les p_j sont des premiers de Fermat distincts. Notons que les seuls nombres premiers de Fermat actuellement connus sont 3, 5, 17, 257 et 65 537.

7. Afin de construire ζ_5, nous allons donner une formule explicite pour $\cos(2\pi/5)$. On sait déjà que $\zeta_5 + \zeta_5^4 = 2\cos(2\pi/5)$ et que $\zeta_5^2 + \zeta_5^3 = 2\cos(4\pi/5)$, et donc que $2\cos(2\pi/5) + 2\cos(4\pi/5) + 1 = 0$. De plus, le produit $\cos(2\pi/5)\cos(4\pi/5)$ vaut $\frac{1}{2}(\cos(2\pi/5) + \cos(4\pi/5))$, donc $\cos(2\pi/5)$ et $\cos(4\pi/5)$ sont racines de $\mathrm{X}^2 + \mathrm{X}/2 - 1/4$. Si l'on remarque que $\cos(4\pi/5) < 0 < \cos(2\pi/5)$, on a donc $\cos(2\pi/5) = \frac{-1+\sqrt{5}}{4}$, que l'on écrira encore $\frac{1}{2}\left(\frac{-1}{2} + \sqrt{\frac{5}{4}}\right)$. Cette écriture permet rapidement de construire le pentagone régulier à la règle et au compas.



Remarque. Les questions précédentes montrent que l'heptadécagone régulier est également constructible à la règle et au compas, un résultat dû à C. F. Gauß en 1796. [2] On a en fait la formule explicite :

$$\cos\left(\frac{2\pi}{17}\right) = -\frac{1}{16} + \frac{\sqrt{17}}{16} + \frac{1}{8}\sqrt{\frac{17-\sqrt{17}}{2}} + \frac{1}{4}\sqrt{\frac{17+3\sqrt{17}}{4} - \frac{1}{2}\sqrt{\frac{17-\sqrt{17}}{2}} - \frac{1}{2}\sqrt{\frac{17+\sqrt{17}}{2}}},$$

ce qui rend toute construction à la règle et au compas un peu plus délicate.

2. Notons que Gauß avait 19 ans.