# Constructions à la règle et au compas : correction

**Exercice 1.**

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 $\mathbf{Q}[X]$.

   Si l'on ne pense pas à cette astuce, il est toujours possible de s'en sortir avec moins de subtilité : une éventuelle racine rationnelle $a/b$ de $X^4+X+1$ aurait un dénominateur $b$ divisant le coefficient dominant et un numérateur $a$ divisant le coefficient constant. Ces deux coefficients étant égaux à 1, il n'y a qu'à vérifier que $\pm 1$ n'est pas racine de $X^4+X+1$ (ce qui est immédiat) pour s'assurer qu'il n'a pas de racine rationnelle. Pour obtenir l'irréductibilité, il ne reste donc plus qu'à exclure une factorisation

   $$X^4+X+1 = (X^2+aX+b)(X^2+cX+d)$$

   en deux polynômes du second degré à coefficients entiers (en effet, le lemme de Gauß implique qu'un polynôme entier unitaire est réductible sur $\mathbf{Q}$ si et seulement s'il l'est sur $\mathbf{Z}$). En développant et en identifiant les coefficients, on obtient le système

   $$a+c=0, \qquad b+ac+d=0, \qquad ad+bc=1, \qquad bd=1,$$

   qui n'a pas de solution sur $\mathbf{Z}$ (la première équation entraîne $c=-a$, la dernière entraîne $b=d=\pm 1$, donc la deuxième équation devient $a^2=\pm 2$, ce qui est impossible pour $a \in \mathbf{Q}$).

2. Par hypothèse, il existe une suite d'extensions $\mathbf{Q} = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_m$ 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

   $$\begin{cases} a+c &= 0 \\ b+ac+d &= 0 \\ ad+bc &= 1 \\ bd &= 1. \end{cases} \iff a \neq 0 \text{ et } \begin{cases} c &= -a \\ b+d &= a^2 \\ d-b &= 1/a \\ bd &= 1. \end{cases}$$

   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 $\deg \mu_a$ 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, cela entraîne qu'il n'a pas de racine dans $\mathbf{Q}$. Le degré de l'algébrique $a$ est donc 2 ou 4.

   Que ce degré 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, on a donc une factorisation sur $\mathbf{Q}$ de la forme $Q = (X^2+n)R$. Comme Q est unitaire, on a affaire à une factorisation en polynômes unitaires dans $\mathbf{Q}[X]$. D'après le lemme de Gauß, les deux facteurs sont bien dans $\mathbf{Z}[X]$. En particulier, $n \in \mathbf{Z}$.

5. Soit $\alpha$ une racine carrée (complexe) de $n$. Alors $\alpha$ 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 2.**

1. Pour construire $\zeta_{2^k}$, il suffit de construire des bissectrices successives (en partant de l'angle plat $\pi$).
2. Soit $n$ et $m$ premiers entre eux. On peut trouver une relation de Bézout : $un + vm = 1$. Si $\zeta_m$ et $\zeta_n$ 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 $\zeta_{mn}$ est constructible, alors $\zeta_n = \zeta_{mn}^m$ et $\zeta_n = \zeta_{mn}^n$ le sont aussi.
3. 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 un nombre impair. 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.
   Les premiers nombres premiers de Fermat sont

$$F_0 = 2^{2^0}+1 = 3, \quad F_1 = 2^{2^1}+1 = 5, \quad F_2 = 2^{2^2}+1 = 17, \quad F_3 = 2^{2^3}+1 = 257 \quad \text{et } 2^{2^4}+1 = 65\,537$$

   et poussèrent apparemment Fermat (à partir de 1640) à croire que $F_m = 2^{2^m}+1$ était toujours un nombre premier. Non seulement c'est déjà faux pour $F_5 = 4\,294\,967\,297 = 641 \cdot 6\,700\,417$ (Euler, 1732), mais on ne connaît à l'heure aucun autre nombre premier de Fermat.
4. Le résultat vu en cours incite à déterminer le degré de $\zeta_p$, c'est-à-dire le degré de son polynôme minimal. Racine de l'unité, $\zeta_p$ est annulée par le polynôme $X^p - 1$. Celui-ci n'est pas irréductible, puisqu'il admet 1 comme racine rationnelle. Cependant, le polynôme quotient

$$P = \frac{X^p - 1}{X - 1} = X^{p-1} + X^{p-2} + \cdots + X + 1,$$

   lui, est irréductible, d'après une application aussi classique qu'astucieuse du critère d'Eisenstein au polynôme

$$P(X+1) = \frac{(X+1)^p - 1}{(X+1) - 1} = X^{p-1} + \binom{p}{1}X^{p-2} + \cdots + \binom{p}{p-2}X + \binom{p}{p-1}$$

   (cf. par exemple TD 0, exercice 10, question 4). Ainsi, $\zeta_p$ est un algébrique de degré $p-1$. S'il est constructible, ce degré doit être une puissance de 2, et $p$ doit donc être un nombre de Fermat.
5. (a) i. Remarquons d'abord que $\mathbf{Q}(\zeta_n)$ est, par définition, le plus petit sous-corps de $\mathbf{C}$ contenant à la fois $\mathbf{Q}$ et $\zeta_n$. Supposons que $\varphi$ et $\psi$ soient deux automorphismes de $\mathbf{Q}(\zeta_p)$ envoyant $\zeta_p$ sur $\zeta_p^u$.
   De manière générale, si $\varphi$ et $\psi$ sont deux morphismes de corps $K \to K'$, on montre directement que

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

est un sous-corps de K.

Dans notre cas, $\varphi$ et $\psi$ coïncident par hypothèse sur $\zeta_p$. Ils ne peuvent pas faire autrement que coïncider sur $\mathbf{Q}$ (un morphisme de corps doit envoyer 1 sur 1, donc il doit coïncider avec l'identité sur le *sous-corps premier*, c'est-à-dire le sous-corps engendré par 1, qui est isomorphe à $\mathbf{Q}$ en caractéristique nulle et à $\mathbf{F}_p$ en caractéristique $p$). Ils coïncident donc bien sur $\mathbf{Q}(\zeta_n)$, et l'unicité est démontrée.

Pour démontrer l'existence d'un tel morphisme, on procède en deux étapes :

– On commence par construire un morphisme $\mathbf{Q}(\zeta_p) \to \mathbf{C}$ vérifiant l'hypothèse, sans se préoccuper de son image.
Puisque $X^{p-1}+\cdots+X+1$ est le polynôme minimal de $\zeta_p$, le corps $\mathbf{Q}(\zeta_p)$ est isomorphe à $\mathbf{Q}[X]/(X^{p-1}+\cdots+X+1)$. Plus précisément, le morphisme d'évaluation

$$\begin{array}{rccc}\widetilde{\varphi}_{\zeta_p} = \text{év}_{\zeta_p} : & \mathbf{Q}[X] & \to & \mathbf{C} \\ & P(X) & \mapsto & P(\zeta_p)\end{array}$$

est un morphisme d'anneaux dont l'image est exactement $\mathbf{Q}[\zeta_p] = \mathbf{Q}(\zeta_p)$ et dont le noyau est $(X^{p-1}+\cdots+X+1)$ (c'est la définition du polynôme minimal) donc il induit un isomorphisme

$$\begin{array}{rccc}\varphi_{\zeta_p} : & \mathbf{Q}[X]/(X^{p-1}+\cdots+X+1) & \to & \mathbf{Q}(\zeta_p) \\ & [X] & \mapsto & \zeta_p\end{array}.$$

Mais les racines de ce polynôme [1] sont précisément les racines $p$-ièmes de l'unité différentes de 1, c'est-à-dire les $(\zeta_p^k)_{k=1}^{p-1}$. On peut donc faire exactement la même construction que précédemment et obtenir un isomorphisme

$$\begin{array}{rccc}\varphi_{\zeta_p^u} : & \mathbf{Q}[X]/(X^{p-1}+\cdots+X+1) & \to & \mathbf{Q}(\zeta_p^u) \\ & [X] & \mapsto & \zeta_p^u\end{array}.$$

En particulier, le morphisme $\sigma_u : \varphi_{\zeta_p^u} \circ \varphi_{\zeta_p}^{-1} : \mathbf{Q}(\zeta_p) \to \mathbf{Q}(\zeta_p^u) \subseteq \mathbf{C}$ convient.

(Évidemment, on vient ici de refaire la preuve, vue en cours, de l'unicité du corps de rupture d'un polynôme irréductible.)

– Il faut maintenant expliquer pourquoi le morphisme $\sigma_u : \mathbf{Q}(\zeta_p) \to \mathbf{C}$ que l'on vient de construire est en fait un automorphisme du corps $\mathbf{Q}(\zeta_p)$. Déjà, $\sigma_u(\zeta_p) = \zeta_p^u$ appartient à $\mathbf{Q}(\zeta_p)$. Puisque $\sigma_u(\zeta_p) \in \mathbf{Q}(\zeta_p)$, il en va de même pour tous les $\sigma_u(x)$, $x \in \mathbf{Q}(\zeta_p)$ : en effet, un tel élément $x$ peut s'écrire

$$x = Q(\zeta_p) = \zeta_p^n + q_{n-1}\zeta_p^{n-1} + \cdots + q_0.$$

On a donc (en se souvenant que $\forall q \in \mathbf{Q}, \sigma_u(q) = q$) :

$$\sigma_u(x) = \sigma_u\left(\zeta_p^n + q_{n-1}\zeta_p^{n-1} + \cdots + q_0\right) = (\zeta_p^u)^n + q_{n-1}(\zeta_p^u)^{n-1} + \cdots + q_0 = Q(\zeta_p^u),$$

donc $\sigma_u(x) = Q(\zeta_p^u) \in \mathbf{Q}(\zeta_p)$.
Le morphisme $\sigma_u$ est donc bien un morphisme de $\mathbf{Q}(\zeta_p)$ dans lui-même. Cela entraîne directement que c'est un automorphisme : il est injectif et $\mathbf{Q}$-linéaire comme tout morphisme de corps [2] ; comme $\mathbf{Q}(\zeta_p)$ est un $\mathbf{Q}$-espace vectoriel de dimension finie, cela entraîne bien $\sigma_u \in \operatorname{Aut}\mathbf{Q}(\zeta_p)$.

1. Les autres racines du polynôme minimal d'un élément algébrique $x$ sont appelés les *conjugués* de $x$, ce qui généralise le cas de l'extension $\mathbf{C}/\mathbf{R}$, où un élément $z \in \mathbf{C}\setminus\mathbf{R}$ a pour polynôme minimal sur $\mathbf{R}$ le polynôme $X^2 - 2(\text{Ré}\, z)X + |z|^2$, et donc pour conjugué... le nombre complexe conjugué $\overline{z}$.

2. Il vaudrait mieux dire tout morphisme de corps *de caractéristique nulle*. Un morphisme de corps en caractéristique $p$ est $\mathbf{F}_p$-linéaire.

**Remarque.** La première partie du raisonnement (qui construit des morphismes $\mathbf{Q}(\alpha) \to \mathbf{C}$ envoyant $\alpha$ sur un de ses conjugués) est extrêmement générale. Pour la seconde (qui montre que ce morphisme envoie bien $\mathbf{Q}(\alpha)$ sur lui-même), nous n'avons utilisé qu'un seul argument spécifique au cas $\alpha = \zeta_p$, à savoir que $\sigma_u(\zeta_p) \in \mathbf{Q}(\zeta_p)$. Le lecteur se convaincra facilement que, de même, si $\varphi(\alpha) \in \mathbf{Q}(\alpha)$, alors $\varphi$ est un automorphisme de $\mathbf{Q}(\alpha)$. Cependant, cette condition n'est pas automatique. On pourra vérifier, par exemple qu'il existe un unique morphisme de corps $\mathbf{Q}(\sqrt[3]{2}) \to \mathbf{C}$ envoyant $\sqrt[3]{2}$ sur $e^{2i\pi/3}\sqrt[3]{2}$, mais que celui-ci n'envoie pas $\mathbf{Q}(\sqrt[3]{2})$ sur lui-même.

ii. C'est évident car $\zeta_p^n$ 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 $\zeta_p$ est $X^{p-1}+\cdots+X+1$, de degré $p-1$. On en déduit donc que la famille $(1, \zeta_p, \ldots, \zeta_p^{p-2})$ est une $\mathbf{Q}$-base de $\mathbf{Q}(\zeta_p)$. Il nous sera plus commode d'en choisit une autre, légèrement différente. Déjà, l'égalité

$$1 + \zeta_p + \cdots + \zeta_p^{p-1} = 0$$

exprime 1 comme combinaison linéaire des $(\zeta_p^k)_{k=1}^{p-1}$ et, réciproquement, exprime $\zeta_p^{p-1}$ comme combinaison linéaire des $(\zeta_p^k)_{k=0}^{p-2}$. La famille $(\zeta_p, \zeta_p^2, \ldots, \zeta_p^{p-1})$ est donc également une $\mathbf{Q}$-base de $\mathbf{Q}(\zeta_p)$. Pour simplifier encore la rédaction, on peut même choisir de permuter ces vecteurs de base : au lieu de numéroter les $(\zeta_p^k)_{k=1}^{p-1}$ (ce qui revient à numéroter les éléments $\overline{k}$ du groupe cyclique $(\mathbf{Z}/p\mathbf{Z})^\times$) par $k$ croissant, on utilise l'élément $u \in \mathbf{Z}$ dont la classe modulo $p$ engendre $(\mathbf{Z}/p\mathbf{Z})^\times$. Ainsi, on a

$$\left\{\overline{u}, \overline{u^2}, \ldots, \overline{u^{p-1}}\right\} = \left\{\overline{1}, \overline{2}, \ldots, \overline{p-1}\right\} = (\mathbf{Z}/p\mathbf{Z})^\times$$

donc

$$\left\{\zeta_p^u, \zeta_p^{u^2}, \ldots, \zeta_p^{u^{p-1}}\right\} = \left\{\zeta_p, \zeta_p^2, \ldots, \zeta_p^{p-1}\right\}$$

et l'on peut utiliser la $\mathbf{Q}$-base $\left(\zeta_p^u, \zeta_p^{u^2}, \ldots, \zeta_p^{u^{p-1}}\right)$.

Soit $x \in \mathbf{Q}(\zeta_p)$ un élément fixe par $\tau_0$. Décomposons-le dans la base que nous avons choisie : $x = a_1\zeta_p^u + a_2\zeta_p^{u^2} \cdots + a_{p-1}\zeta_p^{u^{p-1}}$, avec des rationnels $a_i$.

Puisque $\tau_0 = \sigma_u$ vérifie $\tau_0(\zeta_p) = \zeta_p^u$, on a

$$\tau_0\left(\zeta_p^{u^k}\right) = \tau_0(\zeta_p)^{u^k} = \left(\zeta_p^u\right)^{u^k} = \zeta_p^{u^{k+1}}$$

donc

$$\tau_0(x) = a_{p-1}\zeta_p^u + a_1\zeta_p^{u^2} + \cdots + a_{p-2}\zeta_p^{u^{p-1}}.$$

Ainsi, si $\tau_0(x) = x$, on a $\forall k \in [\![1, p-1]\!]$, $a_k = a_1$, donc $x$ est un multiple rationnel de $\zeta_p^u + \cdots + \zeta_p^{u^{p-1}} = \zeta_p^1 + \cdots + \zeta_p^{p-1} = -1$ et appartient à $\mathbf{Q}$.

ii. C'est évident, il suffit de le vérifier pour $\zeta_p$.

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

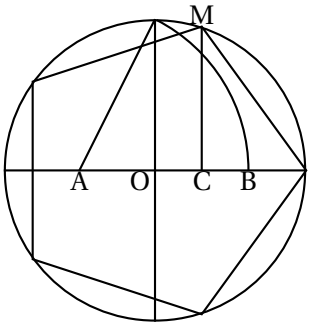
$$K = \left\{x \in L \,\middle|\, \varphi(x) = x\right\}$$

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

Le morphisme $\varphi : L \to L$, vu comme application K-linéaire, est diagonalisable (il est annulé par $X^2 - 1$ 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 $z \in L$ non nul tel que $\varphi(z) = -z$. Tout autre $z' \in L$ tel que $\varphi(z') = -z'$ vérifie alors $\varphi(z'/z) = \varphi(z')/\varphi(z) = z'/z$, c'est-à-dire $z'/z \in K$. 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 $\dim_K L \in \{1, 2\}$.

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

6. Afin de construire $\zeta_5$, 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 $X^2 + X/2 - 1/4$. 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.[3] 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.

7. Du côté positif, on sait construire un triangle régulier et un pentagone régulier. Outre les angles de 120° et 72° que cela nous apporte directement, la question 2 entraîne que $\zeta_{15}$ (et donc le pentadécagone régulier) est constructible, donc l'angle de 24° aussi. Par bissections, on peut donc construire les angles de 3°, 6°, 9°, 12°, 15° et 18°.

Du côté négatif, on a vu en cours que l'angle de 20° n'est pas constructible. Or, si l'on sait construire un angle de mesure $\alpha$, il est facile de construire les angles de mesure multiple de $\alpha$ (du point de vue algébrique, cela revient à dire que si $e^{i\theta}$ est constructible, $e^{in\theta} = (e^{i\theta})^n$ l'est aussi, mais c'est encore plus évident du point de vue géométrique : il suffit de reporter l'angle $n$ fois sur le cercle unité...) Cela démontre donc par la contraposée que les angles de mesure 1°, 2°, 4°, 5°, 10° et 20° ne sont pas constructibles. Mais il y a mieux : comme tout cela a un sens modulo un tour complet, un angle de $n$ degrés, avec $n$ inversible modulo 360

3. Notons que Gauß avait 19 ans.

permettrait également de construire l'angle de 1°. Par bissections successives, il en va de même d'un angle de $2^k n$ degrés. On vérifie directement que cela tranche les cas restants.

Finalement, sont constructibles les angles suivants :

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| ~~1°~~ | ~~2°~~ | $\boxed{3°}$ | ~~4°~~ | ~~5°~~ | $\boxed{6°}$ | ~~7°~~ | ~~8°~~ | $\boxed{9°}$ | ~~10°~~ |
| ~~11°~~ | $\boxed{12°}$ | ~~13°~~ | ~~14°~~ | $\boxed{15°}$ | ~~16°~~ | ~~17°~~ | $\boxed{18°}$ | ~~19°~~ | ~~20°~~ |

et l'on constate notamment que l'angle de 3° est constructible mais pas trisectable.

**Exercice 3.**

0. Si $\Phi_{p^i}$ est irréductible, c'est le polynôme minimal de $\zeta_{p^i}$. Il s'ensuit que $\zeta_{p^i}$ est algébrique de degré $\varphi(p^i)$, le nombre de $k \in [\![1,n]\!]$ premiers avec $p^i$, qui est également le cardinal de $(\mathbf{Z}/p^i\mathbf{Z})^\times$. Mais on sait (ou l'on vérifie) que $\varphi(p^i) = p^i - p^{i-1} = p^{i-1}(p-1)$. Ainsi, si $i \geq 2$, $\varphi(p^i)$ est divisible par $p$ et ne peut pas être une puissance de 2, ce qui entraîne que $\zeta_{p^i}$ n'est pas constructible.

1. Les racines $\zeta_n^k$ du polynôme cyclotomique sont exactement les *racines primitives $n$-ièmes de l'unité,* c'est-à-dire les racines $n$-ièmes de l'unité qui ne sont pas des racines $d$-ièmes pour un $d$ divisant strictement $n$.

   Quand $n = p$ est un nombre premier, ce sont toutes les racines de l'unité non triviales, c'est-à-dire différentes de 1. On a donc

   $$\Phi_p(X) = \frac{\prod_{k=1}^{p}(X-\zeta_p^k)}{X-1} = \frac{X^p-1}{X-1} = X^{p-1}+X^{p-2}+\cdots+X+1,$$

   dont on a déjà montré à la question 4 de l'exercice précédent qu'il était irréductible.

   Si $n = p^2$, les racines $n$-ièmes de l'unité non primitives sont les racines $p$-ièmes. On a donc

   $$\Phi_{p^2}(X) = \frac{X^{p^2}-1}{X^p-1} = \Phi_p(X^p) = X^{p(p-1)}+X^{p(p-2)}+\cdots+X^p+1.$$

2. On a déjà utilisé ce fait aux questions 2 et 7 de l'exercice précédent : si $\zeta_{mn}$ est constructible, il en va de même de $\zeta_n = \zeta_{mn}^m$. Ainsi, la constructibilité de $\zeta_{p^i}$ entraîne celle de $\zeta_{p^2}$ (c'est le cas $n = p^2$, $m = p^{i-2}$) et, par contraposée, il va bien nous suffire de démontrer la non-constructibilité de $\zeta_{p^2}$.

3. Comme dans le cas de $\Phi_p$, $\Phi_{p^2}$ est irréductible si et seulement si $\Phi_{p^2}(X+1)$ l'est. Or,

   $$\begin{aligned}\Phi_{p^2}(X+1) &= \Phi_p((X+1)^p)\\ &= \Phi_p(Y+1) \qquad \text{pour } Y = X^p + \binom{p}{1}X^{p-1}+\cdots+\binom{p}{p-1}X\\ &= Y^{p-1}+\binom{p}{1}Y^{p-2}+\cdots+\binom{p}{p-2}X+\binom{p}{p-1}.\end{aligned}$$

   Comme Y est un polynôme unitaire et sans terme constant en X, le critère d'Eisenstein s'applique ($\Phi_{p^2}(X+1)$ est congru à $X^{p(p-1)}$ modulo $p$, et son coefficient constant est $\binom{p}{p-1} = p$).

   Le polynôme $\Phi_{p^2}$ est un polynôme irréductible qui annule $\zeta_{p^2}$ : c'en est donc le polynôme minimal. Il s'ensuit que $\zeta_{p^2}$ est un algébrique de degré $\deg\Phi_{p^2} = p(p-1)$, qui n'est pas une puissance de 2. Ce nombre n'est donc pas constructible.

4. En rassemblant les différents résultats que nous avons montrés, on obtient donc (en notant $n = \prod p^{v_p}$ la décomposition en facteurs premiers de $n$) :
   - que $\zeta_n$ est constructible si et seulement si chacun des $\zeta_{p^{v_p}}$ l'est (exercice précédent, question 2) ;

– que $\zeta_{2^{v_2}}$ est toujours constructible (exercice précédent, question 1) ;
– que, pour $p$ impair, $\zeta_p$ est constructible si et seulement si $p$ est de Fermat (exercice précédent) ;
– que, pour $p$ impair et $v_p \geq 2$, $\zeta_{p^{v_p}}$ n'est jamais constructible (question précédente).

En résumé, $\zeta_n$ (ou le $n$-gone régulier, ou l'angle $2\pi/n$) est constructible si et seulement si $n$ est le produit d'une puissance de 2 et de nombres premiers de Fermat tous distincts ou, pour reprendre la fin des *Disquitiones Arithmeticae* de Gauß :

> [...] sive brevius, requiritur, ut N neque ullum factorem primum qui non est formae $2^m+1$, implicet, neque etiam ullum factorem primum formae $2^m+1$ pluries. Huiusmodi valores ipsius N infra 300 reperiuntur hi 38 :
> 2, 3, 4, 5, 6, 8, 10, 12, 15, 16, 17, 20, 24, 30, 32, 34, 40, 48, 51, 60, 64, 68, 80, 85, 96, 102, 120, 128, 136, 160, 170, 192, 204, 255, 256, 257, 272.

Ce résultat est parfois appelé *théorème de Gauß-Wantzel* (le fait que la condition soit suffisante étant due à Gauß (1801) et son aspect nécessaire découlant directement de la caractérisation vue en cours des nombres constructibles, due à Pierre-Laurent Wantzel (1837)).

Cet énoncé ne doit pas cacher que, vu l'étendue de notre ignorance sur les nombres premiers de Fermat, il serait difficile de considérer le problème comme définitivement clos. Il est même assez frappant de constater que, bien qu'on ne sache pas construire à la règle et au compas plus de polygones réguliers que le jeune Gauß, on semble assez loin de pouvoir démontrer que son résultat est optimal...

**Exercice 4.**

1. Évidemment, cette question fait penser à l'existence et à l'unicité à isomorphisme près de la clôture algébrique. On va d'ailleurs utiliser ce fait pour notre preuve. Plus précisément, si $\Omega$ est une clôture algébrique de K, on définit l'ensemble $\mathrm{L}_\Omega$ des éléments $x \in \Omega$ pour lesquels il existe une suite de corps
$$\mathrm{K}_0 = \mathrm{K} \subseteq \mathrm{K}_1 \subseteq \cdots \subseteq \mathrm{K}_n$$
tels que $\mathrm{K}_i/\mathrm{K}_{i-1}$ soit une extension de degré 2 et $x \in \mathrm{K}_n$.

   On va alors montrer :
   – que $\mathrm{L}_\Omega$ est quadratiquement clos ;
   – que si $\mathrm{K} \subseteq \mathrm{L}' \subseteq \Omega$ est une extension intermédiaire telle que $\mathrm{L}'$ soit quadratiquement clos, alors $\mathrm{L}' \supseteq \mathrm{L}_\Omega$ ;
   – que si $\mathrm{L}'$ est une clôture quadratique de K, alors l'extension $\mathrm{L}'/\mathrm{K}$ est algébrique.

   Les deux premiers points montrent que $\mathrm{L}_\Omega$ est une clôture quadratique de K et même que c'est la seule clôture quadratique de K incluse dans $\Omega$.

   Les deux derniers points montrent l'unicité à isomorphisme près. En effet, si $\mathrm{L}'/\mathrm{K}$ est une clôture quadratique, on peut choisir une clôture algébrique $\Omega'$ de $\mathrm{L}'$. Puisque l'extension $\mathrm{L}'/\mathrm{K}$ est algébrique, il en est de même de $\Omega'/\mathrm{L}'$, et $\Omega'$ est une clôture algébrique de K. D'après le deuxième point, on a donc $\mathrm{L}' = \mathrm{L}(\Omega')$. Toutes les clôtures quadratiques de K sont donc de la forme $\mathrm{L}_\Omega$ pour une clôture algébrique $\Omega$ de K. Or, on voit directement à l'aide de la définition que si $\varphi : \Omega \to \Omega'$ est un isomorphisme K-linéaire entre deux clôtures algébriques, celui-ci vérifie $\varphi(\mathrm{L}_\Omega) = \mathrm{L}(\Omega')$ : deux clôtures quadratiques de K sont donc bien isomorphes.

   Démontrons donc successivement ces trois points.
   – Montrons que $\mathrm{L}_\Omega$ est quadratiquement clos. Soit donc $\mathrm{P} \in \mathrm{L}_\Omega[\mathrm{X}]$ un polynôme de degré 2, que l'on peut supposer unitaire. Écrivons $\mathrm{P} = \mathrm{X}^2 + b\mathrm{X} + c$. Les coefficients $b$ et $c$ appartiennent à $\mathrm{L}_\Omega$ donc on peut trouver des tours d'extensions quadratiques
$$\mathrm{K} = \mathrm{K}_0 \subseteq \mathrm{K}'_1 \subseteq \mathrm{K}'_2 \subseteq \cdots \subseteq \mathrm{K}_{n'} \ni b$$
$$\mathrm{K} = \mathrm{K}_0 \subseteq \mathrm{K}''_1 \subseteq \mathrm{K}''_2 \subseteq \cdots \subseteq \mathrm{K}_{n''} \ni c.$$

Comme $K'_{i+1}/K'_i$ est quadratique, un simple argument de degré montre que pour tout $\beta_{i+1} \in K'_{i+1} \setminus K'_i$, on a $K'_{i+1} = K'_i[\beta_{i+1}]$. L'argument étant le même pour la deuxième suite, on peut trouver des éléments $\beta_1, \ldots, \beta_{n'}$ et $\gamma_1, \ldots, \gamma_{n''}$ dans $L_\Omega$ tels que $K'_i = K[\beta_1, \ldots, \beta_i]$ et $K''_j = K[\gamma_1, \ldots, \gamma_j]$. La tour d'extensions

$$\begin{aligned} K \subseteq K_1 = K[\beta_1] \subseteq K_2 = K[\beta_1, \beta_2] \subseteq \cdots \subseteq K_{n'} = K[\beta_1, \ldots, \beta_{n'}] \\ \subseteq K_{n'+1} = K[\beta_1, \ldots, \beta_{n'}, \gamma_1] \subseteq \cdots \subseteq K_{n'+n''} = K[\beta_1, \ldots, \beta_{n'}, \gamma_1, \ldots, \gamma_{n''}] \end{aligned}$$

vérifie manifestement $\forall i \in [\![1, n' + n'']\!], [K_i : K_{i-1}] \in \{1, 2\}$. En outre, $K_{n'+n''}$ contient les éléments $b$ et $c$.

Le corps $K_{n'+n''}$ est donc le dernier étage d'une tour d'extensions quadratiques et contient les coefficients de P. Ainsi, P a ses racines soit dans $K_{n'+n''}$ soit dans une extension quadratique de $K_{n'+n''}$. Dans tous les cas, P a ses racines dans $L_\Omega$, ce qui achève la preuve.

– Démontrons maintenant le second point : soit $K \subseteq L' \subseteq \Omega$ une extension intermédiaire quadratiquement close. Soit $x \in L_\Omega$. Par construction, on peut trouver une tour d'extensions quadratiques

$$K_0 = K \subseteq K_1 \subseteq \cdots \subseteq K_n$$

telles que $x \in K_n$. Montrons par récurrence que $K_i \subseteq L'$ : l'initialisation est claire, $L'$ étant par définition une extension de $K_0$. Si maintenant $K_i \subseteq L'$, soit $y \in K_{i+1}$. Par hypothèse, $y$ est algébrique sur $K_i$, de degré 1 ou 2. Si $y \in K_i$, il appartient également à $L'$. S'il est de degré 2 sur $K_i$, il admet un polynôme minimal $\mu_y \in K_i[X]$. Puisque $L'$ est quadratiquement clos, $\mu_y$ admet une racine dans $L'$ ; comme le degré de $\mu_y$ est 2, cela entraîne que $\mu_y$ est scindé sur $L'$, et donc que toutes ses racines appartiennent à $L'$. On a donc $y \in L'$, ce qui clôt la récurrence. Ainsi, on a en particulier montré que $x \in L'$, et on a donc bien $L' \supseteq L_\Omega$.

– Soit $L'$ une clôture quadratique de K. On pose

$$M = \left\{ x \in L' \,\middle|\, x \text{ soit algébrique sur } K \right\}.$$

D'après le cours, M est un sous-corps de $L'$ (contenant K). Montrons qu'il est quadratiquement clos. Soit donc $P \in M[X]$ un polynôme de degré 2. Puisque $L'$ est quadratiquement clos, il existe une racine $\alpha \in L'$ de P. Cet élément $\alpha \in L$ est donc algébrique sur M. Or, comme M/K est par définition une extension algébrique, le fait que $\alpha$ soit algébrique sur M entraîne qu'il est algébrique sur K. On a donc $\alpha \in M$, ce qui prouve que M est quadratiquement clos. Par définition de la clôture quadratique, cela entraîne que $M = L'$, et donc que $L'/K$ est bien une extension algébrique.

2. Vu la description précédente, le corps des nombres constructibles est une clôture quadratique de **Q**. **C** est une clôture quadratique de **R** : algébriquement clos, il est évidemment quadratiquement clos, et tout sous-corps de **C** quadratiquement clos contenant **R** soit également contenir une racine de $X^2 + 1$, donc être égal à **C** lui-même. Quant à **C**, de même que tout corps algébriquement clos (ou même uniquement quadratiquement clos), il est égal à sa propre clôture quadratique.

3. Soit $P \in \mathbf{F}_q[X]$ un polynôme de degré 2. S'il a une racine dans $\mathbf{F}_q$, il en a évidemment une dans $\mathbf{F}_{q^2}$. Si ce n'est pas le cas, il a tautologiquement une racine dans le sous-corps $\mathbf{F}_q[\alpha]$ de sa clôture algébrique, où $\alpha$ est une des racines de P. Mais, comme $\mathbf{F}_q$ n'a, à isomorphisme près, qu'une unique extension de degré 2, à savoir $\mathbf{F}_{q^2}$, on a bien $\alpha \in \mathbf{F}_{q^2}$. Cela démontre directement que l'union croissante

$$L = \bigcup_{n \geq 0} \mathbf{F}_{q^{2^n}}$$

forme un corps quadratiquement clos.

Comme en outre chaque élément $x \in \mathbf{F}_{q^{2^n}}$ vit au dernier étage d'une tour

$$\mathbf{F}_q \subseteq \mathbf{F}_{q^2} \subseteq \mathbf{F}_{q^4} \subseteq \cdots \subseteq \mathbf{F}_{q^{2^n}}$$

d'extensions quadratiques, il doit appartenir à tout sous-corps de L quadratiquement clos. L s'identifie donc bien à la clôture quadratique de $\mathbf{F}_q$.

En revanche, cette clôture quadratique L ne contient par construction que des éléments dont le degré sur $\mathbf{F}_q$ est une puissance de 2. Comme toute clôture algébrique $\overline{\mathbf{F}}_q$ de $\mathbf{F}_q$ soit contenir des éléments de degré 3 sur $\mathbf{F}_q$ (car $\mathbf{F}_q$ possède une extension de degré 3, à savoir $\mathbf{F}_{q^3}/\mathbf{F}_q$), L ne peut pas être algébriquement clos.