Devoir à la maison n°2

Un corrigé

Exercice 1. Soit $\mathbb{F}_3$ le corps fini à 3 éléments et α une racine septième de l'unité (dans un corps de rupture du polynôme $X^7 - 1 \in \mathbb{F}_3[X]$, il existe - au moins - une racine septième de l'unité). On pose $K = \mathbb{F}_3(\alpha)$.

1) L'élément $\alpha \in K$ est *algébrique* sur $\mathbb{F}_3$ car il vérifie $\alpha^7 = 1$. Donc le corps $\mathbb{F}_3(\alpha)$ est une extension finie de $\mathbb{F}_3$. C'est un $\mathbb{F}_3$-espace vectoriel de dimension finie, il a donc un nombre fini d'éléments : K est un corps fini.

2) Pour déterminer K, il suffit de trouver son cardinal. D'après ce qui précède, $\#K = 3^m$ où m est le degré de l'extension $K/\mathbb{F}_3$. Maintenant, il s'agit de calculer m. Si $\alpha = 1$, alors $\mathbb{F}_3(\alpha) = \mathbb{F}_3$.

   Supposons $\alpha \neq 1$. Comme $\alpha^7 - 1 = (\alpha - 1)(1 + \alpha + \ldots + \alpha^6) = 0$ dans K, on a $1 + \alpha + \ldots + \alpha^6 = 0$. Notons P le polynôme cyclotomique $1 + X + \ldots + X^6 \in \mathbb{F}_3[X]$. Il annule α, c'est donc un multiple du polynôme minimal de α sur $\mathbb{F}_3$. Montrer que c'est le polynôme minimal revient à montrer que P est irréductible dans $\mathbb{F}_3[X]$.

   D'après l'exercice 9 de la feuille 4, P est irréductible dans $\mathbb{F}_3[X]$ si et seulement s'il n'a aucune racine dans toutes les extensions de $\mathbb{F}_3$ de degré au plus $\frac{\deg P}{2} = 3$. Il n'y a que trois possibilités pour ces extensions : $L_1 = \mathbb{F}_3, L_2 = \mathbb{F}_{3^2}, L_3 = \mathbb{F}_{3^3}$.

   Raisonnons par l'absurde : supposons que P ait une racine x dans un de ces corps L_d ($1 \leq d \leq 3$). Comme $x \neq 0$, x est un élément du groupe multiplicatif L_d^* du corps. D'après un résultat du cours, puisque L_d est fini, ce groupe est cyclique d'ordre $3^d - 1$. De plus, $x^7 = 1$ donc x est d'ordre 7. Par le théorème de Lagrange, 7 divise $3^d - 1$. Pour $d = 1, 2$ ou 3, c'est impossible. Ainsi le polynôme P est irréductible dans $\mathbb{F}_3[X]$ et c'est le polynôme minimal de α sur $\mathbb{F}_3$. Le degré de l'extension $K/\mathbb{F}_3$ est $m = \deg(P) = 6$.

   En conclusion, K est le corps fini $\mathbb{F}_{3^6}$ à 3^6 éléments.

   Remarque 0. On ne travaille pas dans un sous-corps de $\mathbb{C}$ donc on n'a pas $\alpha = \mathrm{e}^{2\mathrm{i}\pi/17}$!

   Remarque 1. D'après le cours, le polynôme cyclotomique $\Phi_7(X) = 1 + X + \ldots + X^6$ est irréductible dans $\mathbb{Q}[X]$. Mais cela ne nous dit rien de son irréductibilité dans $\mathbb{F}_3[X]$!

   Remarque 2. Pour vérifier que P n'a aucune racine dans ces corps, on pouvait également procéder comme en TD en construisant les corps $\mathbb{F}_{3^2}$ et $\mathbb{F}_{3^3}$ comme quotients de $\mathbb{F}_3[X]$ par un polynôme irréductible du bon degré (par exemple avec $X^2 + 1$ et $X^3 + 2X + 1$, irréductibles sur $\mathbb{F}_3$). Mais les calculs sont beaucoup plus longs.

Exercice 2. Soit n un entier ≥ 3.

1) Notons $\zeta = \mathrm{e}^{2\mathrm{i}\pi/n}$ et $\alpha = \cos(2\pi/n)$. On a $\alpha = \frac{\zeta + \zeta^{-1}}{2}$ donc α est dans $\mathbb{Q}(\zeta)$. On a ainsi les extensions de corps :

$$\begin{array}{c} \mathbb{Q}(\zeta) \\ | \\ \mathbb{Q}(\alpha) \\ | \\ \mathbb{Q}. \end{array}$$

D'après le cours, l'extension $\mathbb{Q}(\zeta)/\mathbb{Q}$ est de degré $\varphi(n)$. Déterminons le degré de l'extension $\mathbb{Q}(\zeta)/\mathbb{Q}(\alpha)$.

Le polynôme $P(X) = (X-\zeta)(X-\zeta^{-1}) = X^2 - 2\alpha X + 1$ est à coefficients dans $\mathbb{Q}(\alpha)[X]$. De plus, il annule ζ. Enfin, il est irréductible dans $\mathbb{Q}(\alpha)$: sinon, ses racines ζ et ζ^{-1} seraient dans $\mathbb{Q}(\alpha)$ ce qui est impossible car $\mathbb{Q}(\alpha) \subset \mathbb{R}$ et $\zeta \notin \mathbb{R}$ ($n \geq 3$). Donc P est le polynôme minimal de ζ sur $\mathbb{Q}(\alpha)$. Comme il est de degré 2, on en déduit $[\mathbb{Q}(\zeta) : \mathbb{Q}(\alpha)] = 2$. Par le théorème de multiplicativité du degré, on a donc :

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] = \frac{\varphi(n)}{2}.$$

2) Soit $x \in \mathbb{Q}$ écrit sous forme irréductible $\frac{a}{b}$ avec a et b entiers premiers entre eux et $b > 0$. On suppose $b \geq 3$. Comme précédemment, on a les extensions de corps :

$$\begin{array}{c} \mathbb{Q}(\mathrm{e}^{2\pi \mathrm{i} a/b}) \\ | \\ \mathbb{Q}(\cos(2\pi a/b)) \\ | \\ \mathbb{Q} \end{array}$$

et comme précédemment, on montre que $[\mathbb{Q}(\mathrm{e}^{2\pi \mathrm{i} a/b}) : \mathbb{Q}(\cos(2\pi a/b))] = 2$ (l'extension n'est pas de degré 1 car $b \geq 3$). De plus, $\mathrm{e}^{2\pi \mathrm{i}/b}$ est une racine primitive b-ème de l'unité. Comme a et b sont premiers entre eux, il en est de même de $\mathrm{e}^{2\pi \mathrm{i} a/b}$. Les corps $\mathbb{Q}(\mathrm{e}^{2\pi \mathrm{i}/b})$ et $\mathbb{Q}(\mathrm{e}^{2\pi \mathrm{i} a/b})$ sont donc égaux. Or, $[\mathbb{Q}(\mathrm{e}^{2\pi \mathrm{i}/b}) : \mathbb{Q}] = \varphi(b)$. Finalement, on obtient :

$$[\mathbb{Q}(\cos(2\pi a/b)) : \mathbb{Q}] = \frac{\varphi(b)}{2}.$$

3) Supposons $n \geq 5$. Notons $\beta = \sin(\frac{2\pi}{n})$. On commence par se ramener à la question précédente ! On a l'identité trigonométrique $\sin(\frac{2\pi}{n}) = \cos(\frac{\pi}{2} - \frac{2\pi}{n}) = \cos(2\pi\left(\frac{n-4}{4n}\right))$. Maintenant, écrivons $\frac{n-4}{4n}$ sous forme irréductible.

- Si $\mathrm{pgcd}(n, 8) = 1$, alors n est impair et le pgcd de $4n$ et $n-4$ est 1. D'après la question 2), le degré $[\mathbb{Q}(\beta) : \mathbb{Q}]$ est $\varphi(4n)/2$. Comme 4 et n sont premiers entre eux, d'après les propriétés de l'indicatrice d'Euler[1], $\varphi(4n) = \varphi(4)\varphi(n) = 2\varphi(n)$. D'où $[\mathbb{Q}(\beta) : \mathbb{Q}] = \varphi(n)$.
- Si $\mathrm{pgcd}(n, 8) = 2$, alors $n = 2k$ avec k impair et on voit que le pgcd de $4n$ et $n-4$ est 2. Donc comme $\frac{n-4}{4n} = \frac{n/2-2}{2n}$, le degré de l'extension est donc $\varphi(2n)/2$. On a $\varphi(2n) = \varphi(4k) = \varphi(4)\varphi(k) = 2\varphi(k)$. De plus, $\varphi(n) = \varphi(2k) = \varphi(2)\varphi(k) = \varphi(k)$. Donc $\varphi(2n) = 2\varphi(n)$ et le degré est $[\mathbb{Q}(\beta) : \mathbb{Q}] = \varphi(n)$.
- Si $\mathrm{pgcd}(n, 8) = 4$, alors $n = 4k$ avec k impair et on voit que le pgcd de $4n$ et $n-4$ est 8. Comme $\frac{n-4}{4n} = \frac{(n-4)/8}{n/2}$, le degré est donc $\varphi(n/2)/2$. On a $\varphi(n) = \varphi(4k) = \varphi(4)\varphi(k) = 2\varphi(k)$ et $\varphi(n/2) = \varphi(2k) = \varphi(k)$ d'où $\varphi(n/2) = \varphi(n)/2$. Finalement, le degré est $[\mathbb{Q}(\beta) : \mathbb{Q}] = \varphi(n)/4$.
- Si $\mathrm{pgcd}(n, 8) > 4$, alors $n = 8k$ avec k quelconque et le pgcd de $4n$ et $n-4$ est 4. Comme $\frac{n-4}{4n} = \frac{(n-4)/4}{n}$, le degré de l'extension est $[\mathbb{Q}(\beta) : \mathbb{Q}] = \varphi(n)/2$.

4) Notons $\beta = \sin(2\pi/5)$. Comme $\mathrm{pgcd}(5, 4) = 1$, d'après ce qui précède, l'extension $Q(\beta)/\mathbb{Q}$ est de degré $\varphi(5) = 4$, donc le polynôme minimal de β sur $\mathbb{Q}$ est de degré 4. D'après la formule $\sin(5x) = 16\sin(x)^5 - 20\sin(x)^3 + 5\sin(x)$ appliquée à $x = 2\pi/5$, on a $16\beta^5 - 20\beta^3 + 5\beta = 0$, d'où

$$16\beta^4 - 20\beta^2 + 5 = 0.$$

Le polynôme $P = 16X^4 - 20X^2 + 5 \in \mathbb{Q}[X]$ annule β ; il divise le polynôme minimal et il est de même degré que celui-ci. C'est donc le polynôme minimal de β sur $\mathbb{Q}$.

Remarque. On pouvait également voir que P est irréductible en appliquant le critère d'Eisenstein.

[1] Si n et m sont premiers entre eux, alors $\varphi(nm) = \varphi(n)\varphi(m)$

Exercice 3. Notons $z = \mathrm{e}^{\frac{2i\pi}{17}}$ et $K = \mathbb{Q}(z)$.

1) (a) D'après le cours, l'extension $K/\mathbb{Q}$ est de degré $\varphi(17) = 16$ et une base de K sur $\mathbb{Q}$ est $\{z, z^2, \ldots, z^{16}\}$.

(b) D'après le cours, l'extension $K/\mathbb{Q}$ est galoisienne de groupe de Galois isomorphe à $(\mathbb{Z}/17\mathbb{Z})^*$. Or, $(\mathbb{Z}/17\mathbb{Z})^*$ est cyclique car c'est le groupe multiplicatif du corps fini $\mathbb{Z}/17\mathbb{Z}$ (17 est premier). Donc G est cyclique isomorphe au groupe additif $\mathbb{Z}/16\mathbb{Z}$ et d'ordre 16.

(c) Soit g un générateur de G ; il est d'ordre 16. Soit G_i le sous-groupe de G engendré par g^{2^i} $(0 \leq i \leq 4)$. L'élément g^{2^i} est d'ordre $\frac{16}{\mathrm{pgcd}(2^i,2^4)} = \frac{2^4}{2^i} = 2^{4-i}$. Donc le groupe G_i est d'ordre 2^{4-i}.

Par la correspondance de Galois, la suite de sous-groupes $\{e\} = G_4 \subset G_3 \subset G_2 \subset G_1 \subset G_0 = G$ donne les extensions de corps suivantes :

$$\begin{array}{c} K_4 = K^{G_4} = K \\ | \\ K_3 = K^{G_3} \\ | \\ K_2 = K^{G_2} \\ | \\ K_1 = K^{G_1} \\ | \\ K_0 = K^G = \mathbb{Q}. \end{array}$$

Calculons $[K_{i+1} : K_i]$. Par multiplicativité du degré, c'est $\dfrac{[K_{i+1} : \mathbb{Q}]}{[K_i : \mathbb{Q}]}$. Or, $[K_i : \mathbb{Q}] = \dfrac{[K : \mathbb{Q}]}{[K : K_i]} = \dfrac{|G|}{|G_i|}$ d'après la correspondance. Donc $[K_i : \mathbb{Q}] = 2^i$. On en déduit $[K_{i+1} : K_i] = \frac{2^{i+1}}{2^i} = 2$.

(d) Un automorphisme σ de $K/\mathbb{Q}$ (c'est-à-dire un élément du groupe de Galois G) est déterminé par sa valeur en z. De plus, comme $z^{17} = 1$, $\sigma(z)$ est une racine 17ème de l'unité. Donc il existe k avec $0 \leq k \leq 16$ tel que $g^8(z) = z^k$. De plus, $g^{16} = \mathrm{id}$ donc

$$z = g^{16}(z) = g^8(g^8(z)) = g^8(z^k) = (g^8(z))^k = z^{k^2}$$

d'où $z^{k^2-1} = 1$. Alors z étant d'ordre 17, 17 divise $k^2 - 1 = (k-1)(k+1)$, d'où puisque 17 est premier, $\overline{k} = \overline{1}$ ou $\overline{k} = \overline{-1}$. Si $\overline{k} = \overline{1}$, alors $g^8 = \mathrm{id}$ ce qui est impossible car g est d'ordre 16. Donc $\overline{k} = \overline{-1}$ et $g^8(z) = z^{-1}$.

D'après la correspondance de Galois, pour voir que $\cos(\frac{2\pi}{17})$ est dans $K_3 = K^{G_3}$, il faut et il suffit de montrer que $g^{2^3}(\cos(\frac{2\pi}{17})) = \cos(\frac{2\pi}{17})$. Or, $g^8(\cos(\frac{2\pi}{17})) = g^8(\frac{z+\overline{z}}{2}) = g^8(\frac{z+z^{-1}}{2}) = \frac{1}{2}(z^{-1} + z) = \cos(\frac{2\pi}{17})$. Donc $\cos(\frac{2\pi}{17})$ appartient au corps K_3.

On obtient ainsi $\mathbb{Q}(\cos(\frac{2\pi}{17})) \subset K_3$. Maintenant d'après l'exercice 2, l'extension $\mathbb{Q}(\cos(\frac{2\pi}{17}))/\mathbb{Q}$ est de degré $\frac{\varphi(17)}{2} = 8$. Comme on sait que $[K_3 : \mathbb{Q}] = 2^3 = 8$, on obtient l'égalité de corps $K_3 = \mathbb{Q}(\cos(\frac{2\pi}{17}))$.

2) (a) On vérifie que la classe de 2 ne convient pas car $2^8 = 1$. Calculons les réductions modulo 17 des puissances successives de 3 :

$$\begin{array}{l|l} \overline{3} & \overline{3^9} = \overline{14} \\ \overline{3^2} = \overline{9} & \overline{3^{10}} = \overline{8} \\ \overline{3^3} = \overline{10} & \overline{3^{11}} = \overline{7} \\ \overline{3^4} = \overline{13} & \overline{3^{12}} = \overline{4} \\ \overline{3^5} = \overline{5} & \overline{3^{13}} = \overline{12} \\ \overline{3^6} = \overline{15} & \overline{3^{14}} = \overline{2} \\ \overline{3^7} = \overline{11} & \overline{3^{15}} = \overline{6} \\ \overline{3^8} = \overline{16} = \overline{-1} & \overline{3^{16}} = \overline{1} \end{array}$$

La classe de 3 est d'ordre 16 dans $(\mathbb{Z}/17\mathbb{Z})^*$ et engendre ce groupe.

On sait que le groupe de Galois G est isomorphe à $(\mathbb{Z}/17\mathbb{Z})^*$. Plus précisément, l'isomorphisme est donné par :

$$\begin{array}{ccc}(\mathbb{Z}/17\mathbb{Z})^* & \to & G \\ \overline{k} & \mapsto & (z \mapsto z^k)\end{array}$$

L'automorphisme g de $K/\mathbb{Q}$, défini par $g(z) = z^3$, est un générateur de G.

(b) On pose $a_1 = \sum_{i=0}^{7} g^{2i}(z)$ et $a_2 = g(a_1)$.

i. Comme $K_1 = K^{G_1}$, pour voir que a_1 appartient à K_1, il faut et il suffit de montrer que $g^2(a_1) = a_1$. Puisque $g^{16} = \mathrm{id}$, on a

$$g^2(a_1) = \sum_{i=0}^{7} g^{2(i+1)}(z) = \sum_{i=0}^{6} g^{2(i+1)}(z) + g^{16}(z) = \sum_{i=0}^{7} g^{2i}(z) = a_1$$

donc a_1 appartient à K_1.

En utilisant $g(z) = z^3$, on obtient les formules :

$$\begin{aligned} a_1 &= z + z^9 + z^{13} + z^{15} + z^{16} + z^8 + z^4 + z^2 \\ a_2 &= z^3 + z^{10} + z^5 + z^{11} + z^{14} + z^7 + z^{12} + z^6. \end{aligned}$$

Comme $\{z, \ldots, z^{16}\}$ est une $\mathbb{Q}$-base de K, on en déduit $a_2 \neq a_1$. Puisque $\mathbb{Q} = K^{G_1}$ et $g(a_1) \neq a_1$, a_1 n'est pas dans $\mathbb{Q}$. Enfin, $\mathbb{Q} \subsetneq \mathbb{Q}(a_1) \subset K_1$ et l'extension $K_1/\mathbb{Q}$ étant de degré 2, on obtient $K_1 = \mathbb{Q}(a_1)$.

ii. Par les formules précédentes, $1 + a_1 + a_2 = \Phi_{17}(z) = 0$ (où Φ_{17} désigne le 17ème polynôme cyclotomique).

iii. En remarquant que $z^k + z^{-k} = 2\cos(k\theta)$, on obtient

$$\begin{aligned} a_1 &= 2(\cos(\theta) + \cos(8\theta) + \cos(4\theta) + \cos(2\theta)) \\ a_2 &= 2(\cos(3\theta) + \cos(7\theta) + \cos(5\theta) + \cos(6\theta)). \end{aligned}$$

Comme $\theta = \frac{2\pi}{17}$, on a les inégalités

$$0 < \theta < 2\theta < 3\theta < 4\theta < \frac{\pi}{2} < 5\theta < 6\theta < 7\theta < 8\theta < \pi$$

Le cosinus est strictement décroissant sur $[0, \pi]$ donc $\cos(k\theta) > 0$ pour $k = 1, 2, 3, 4$ et $\cos(k\theta) < 0$ pour $k = 5, 6, 7, 8$. De plus

$$a_2 = 2(2\cos(9\theta/2)\cos(3\theta/2) + \cos(5\theta) + \cos(7\theta))$$

Comme $0 < 3\theta/2 < \pi/2 < 9\theta/2 < \pi$, le produit $\cos(9\theta/2)\cos(3\theta/2)$ est strictement négatif. Donc $a_2 < 0$.

iv. En développant le produit, en utilisant la formule rappelée puis en regroupant les termes (on a $\cos(k\theta) = \cos((17-k)\theta)$ pour tout k), on obtient $a_1 + a_2 = 4a_1a_2 = -4$.

v. Les racines de l'équation du second degré $X^2 + X - 4 = 0$ sont a_1 et a_2. Donc $\{a_1, a_2\} = \{\frac{-1-\sqrt{17}}{2}, \frac{-1+\sqrt{17}}{2}\}$. Comme $a_2 < 0$, on obtient :

$$a_1 = \frac{-1+\sqrt{17}}{2} \text{ et } a_2 = \frac{-1-\sqrt{17}}{2}.$$

En particulier, on voit que $K_1 = K(a_1) = \mathbb{Q}(\sqrt{17})$.

(c) On pose $b_1 = \sum_{i=0}^{3} g^{4i}(z)$ et $b_2 = g^2(b_1)$.

i. Comme $K_2 = K^{G_2}$, voir que b_1 appartient à K_2 revient à montrer que $g^4(b_1) = b_1$, ce qui s'obtient à l'aide des formules

$$\begin{aligned} b_1 &= z + z^{13} + z^{16} + z^4 \\ b_2 &= z^9 + z^{15} + z^8 + z^2. \end{aligned}$$

Comme $\{z, \ldots, z^{16}\}$ est une $\mathbb{Q}$-base de K, on a $b_2 \neq b_1$ donc $b_1 \notin K_1 = K^{G_1}$. Enfin, $K_1 \subsetneq K_1(b_1) \subset K_2$ et comme l'extension K_2/K_1 étant de degré 2, on obtient $K_2 = K_1(b_1)$.

ii. A l'aide des formules précédentes, on a directement $b_1 + b_2 = a_1$.

iii. Un calcul similaire à celui de 2)b)iii donne $b_1 = 2(\cos(\theta) + \cos(4\theta))$ et $b_2 = 2(\cos(2\theta) + \cos(8\theta))$. Par décroissance du cosinus sur $[0, \pi]$, on obtient $b_2 < b_1$.

iv. En effectuant le produit et regroupant les termes, on obtient

$$b_1 b_2 = 2 \sum_{k=1}^{8} \cos(k\theta) = a_1 + a_2 = -1.$$

v. Les racines de l'équation du second degré $X^2 - a_1 X - 1 = 0$, à coefficients dans K_1, sont b_1 et b_2. Ainsi, $\{b_1, b_2\} = \{\frac{a_1 - \sqrt{a_1^2+4}}{2}, \frac{a_1 + \sqrt{a_1^2+4}}{2}\}$. Comme $b_1 > b_2$,

$$b_1 = \frac{1}{2}(a_1 + \sqrt{a_1^2 + 4}) \text{ et } b_2 = 12(a_1 - \sqrt{a_1^2 + 4}).$$

vi. On pose $b_3 = \sum_{i=0}^{3} g^{4i+1}(z)$ et $b_4 = g^2(b_3)$. Par la même méthode, on obtient les relations suivantes :

$$\begin{aligned} b_3 &= z + z^3 + z^5 + z^{14} + z^{12} \\ b_4 &= z^{10} + z^{11} + z^7 + z^6 \\ b_3 + b_4 &= a_2 \\ b_3 &= 2(\cos(3\theta) + \cos(5\theta)) \\ b_4 &= 2(\cos(7\theta) + \cos(6\theta)) \\ b_3 b_4 &= 2\textstyle\sum_{k=1}^{8} \cos(k\theta) = -1 \end{aligned}$$

Les racines de l'équation $X^2 - a_2 X - 1 = 0$ sont $\frac{1}{2}(a_2 + \sqrt{4 + a_2^2})$ et $\frac{1}{2}(a_2 - \sqrt{4 + a_2^2})$. Comme $b_3 > b_4$, on obtient

$$b_3 = \frac{1}{2}(a_2 + \sqrt{4 + a_2^2}) \text{ et } b_4 = \frac{1}{2}(a_2 - \sqrt{4 + a_2^2}).$$

(d) On pose $c_1 = \sum_{i=0}^{1} g^{8i}(z)$ et $c_2 = g^4(c_1)$.

i. Comme $K_3 = K^{G_3}$, voir que c_1 appartient à K_3 revient à montrer que $g^8(c_1) = c_1$, ce qui s'obtient à l'aide des formules

$$\begin{aligned} c_1 &= z + z^{16} \\ c_2 &= z^{13} + z^4. \end{aligned}$$

Comme $\{z, \ldots, z^{16}\}$ est une $\mathbb{Q}$-base de K, on a $c_2 \neq c_1$ donc $c_1 \notin K_2 = K^{G_2}$. Enfin, $K_2 \subsetneq K_2(c_1) \subset K_3$ et comme l'extension K_3/K_2 est de degré 2, on obtient $K_3 = K_2(c_1)$.

ii. A l'aide des formules précédentes, on a directement $c_1 + c_2 = b_1$.

iii. Un calcul donne $c_1 = 2\cos(\theta)$ et $c_2 = 2\cos(4\theta)$. Par décroissance du cosinus sur $[0, \pi]$, on obtient $c_2 < c_1$.

iv. En effectuant le produit et regroupant les termes, on obtient

$$c_1 c_2 = 2(\cos(3\theta) + \cos(5\theta)) = b_3.$$

v. Les racines de l'équation du second degré $X^2 - b_1 X + b_3 = 0$, à coefficients dans K_2, sont c_1 et c_2. Ainsi, $\{c_1, c_2\} = \{\frac{1}{2}(b_1 - \sqrt{b_1^2 - 4b_3}), \frac{1}{2}(b_1 + \sqrt{b_1^2 - 4b_3})\}$. Comme $c_1 > c_2$,

$$c_1 = \frac{1}{2}(b_1 + \sqrt{b_1^2 - 4b_3}) \text{ et } c_2 = \frac{1}{2}(b_1 - \sqrt{b_1^2 - 4b_3}).$$

(e) Finalement, $\cos(\theta) = \frac{1}{2}c_1 = \frac{1}{4}(b_1 + \sqrt{b_1^2 - 4b_3})$. Or

$$b_1 = \frac{1}{2}(a_1 + \sqrt{a_1^2 + 4}) = \frac{1}{2}(a_1 + \sqrt{8 - a_1})) = \frac{1}{4}(-1 + \sqrt{17} + \sqrt{4(8 - a_1)})$$

d'où

$$b_1 = \frac{1}{4}(-1 + \sqrt{17} + \sqrt{34 - 2\sqrt{17}}).$$

De même,

$$b_3 = \frac{1}{2}(a_2 + \sqrt{a_2^2 + 4}) = \frac{1}{4}(-1 - \sqrt{17} + \sqrt{34 + 2\sqrt{17}}).$$

En développant, on trouve

$$b_1^2 = \frac{1}{16}(62 + 2(-1 + \sqrt{17})\sqrt{34 - 2\sqrt{17}} - 4\sqrt{17})$$

et finalement $\cos\left(\frac{2\pi}{17}\right)$ vaut

$$\frac{1}{16}\left(-1 + \sqrt{17} + \sqrt{34 - 2\sqrt{17}} + \sqrt{68 + 12\sqrt{17} + 2(-1 + \sqrt{17})\sqrt{34 - 2\sqrt{17}} - 16\sqrt{34 + 2\sqrt{17}}}\right).$$

Autour de la formule de Gauss

Constructions à la règle et au compas. Voici la définition mathématique précise de la notion de point du plan constructible (sous-entendu, à la règle et au compas).

Points constructibles en une étape. Soit E un sous-ensemble du plan euclidien, qu'on assimile ici à $\mathbb{R}^2$. On dit qu'un point $P = (x, y)$ est constructible en une étape à partir de E si et seulement si P est un point de E ou si P est dans l'intersection de deux objets quelconques parmi :

- l'ensemble des droites distinctes qui passent par deux éléments distincts de E ;
- l'ensemble des cercles distincts centrés en un point de E et dont le rayon est la distance de deux quelconques points de E.

Points constructibles en n étapes. Partant des mêmes données, on définit, naturellement et par récurrence, l'ensemble des points constructibles en n étapes à partir de E : pour $n = 1$, c'est la construction précédente ; sinon, c'est l'ensemble des points constructibles en une étape à partir de l'ensemble des points constructibles en $n-1$ étapes (à partir de E). Enfin, un point est dit constructible à partir de E s'il l'est en n étapes pour un certain n.

Nombres constructibles. Un nombre réel x est dit constructible si le point $(x, 0)$ du plan l'est à partir de $E = \{O = (0, 0), I = (0, 1), J = (1, 0)\}$. Les nombres constructibles forment un sous-corps de $\mathbb{R}$.

Critère pour qu'un nombre soit constructible. Savoir quels sont les nombres et les figures constructibles à la règle et au compas était un problème central des mathématiques dès l'Antiquité. Jusqu'au dix-neuvième siècle, on démontra l'impossibilité de réaliser certaines constructions (quadrature

du cercle, trisection de l'angle). La théorie des extensions de corps fournit le bon cadre mathématique pour étudier la constructibilité. C'est Wantzel (1837) qui donne finalement un critère pour qu'un nombre réel x soit constructible : il faut et il suffit qu'il existe une tour d'extension quadratique $\mathbb{Q} = K_0 \subset K_1 \subset \ldots \subset K_n$ (cela signifie que les extensions successives sont de degré 2) avec $x \in K_n$.

Le polygone régulier à 17 côtés. D'après l'exercice 3, le nombre $\cos(\frac{2\pi}{17})$ est donc constructible à la règle et au compas. Maintenant, il est facile de se convaincre qu'un polygone régulier à n côtés est constructible si et seulement si $\cos(\frac{2\pi}{n})$ l'est. Muni de la formule de Gauss, d'une règle, d'un compas et de beaucoup de patience, vous pouvez donc construire le polygone régulier à 17 côtés...

Tous les polygones sont-ils constructibles ? Une question naturelle est de savoir si tous les polygones réguliers sont constructibles. En 1801, Gauss en obtient la liste : ce sont les polygones à n côtés, où n est soit une puissance de 2, soit le produit d'une puissance de 2 et de nombres de Fermat premiers. Les nombres de Fermat sont ceux de la forme $F_k = 2^{2^k} + 1$. Parmi eux, on ne connaît actuellement que cinq nombres premiers : $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$, $F_4 = 65537$. On conjecture qu'il n'en existe pas d'autres.

Pour en savoir plus : Consulter n'importe quel bon ouvrage sur la théorie des corps et la théorie de Galois.