Devoir à la maison n°2

SOIGNEZ LA RÉDACTION !

Exercice 1. Soient $\mathbb{F}_3$ le corps fini à 3 éléments et α une racine 7ème de l'unité (une telle racine existe dans un corps de rupture du polynôme $X^7 - 1 \in \mathbb{F}_3[X]$). On considère le corps $K = \mathbb{F}_3(\alpha)$.

1) Montrer que K est un corps fini.
2) Trouver le polynôme minimal de α sur $\mathbb{F}_3$ et déterminer le corps K.
   Indications : on pourra utiliser le résultat de l'exercice 9 de la feuille 4 ; pour simplifier les calculs, on rappelle que le groupe multiplicatif F^* d'un corps fini F est cyclique d'ordre...).

Exercice 2. Soit n entier ≥ 3.

1) Montrer que le degré de l'extension $\mathbb{Q}(\cos(\frac{2\pi}{n}))/\mathbb{Q}$ est $\frac{\varphi(n)}{2}$, où φ désigne la fonction indicatrice d'Euler.
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 $b \geq 3$. Calculer le degré de l'extension $\mathbb{Q}(\cos(\frac{2\pi a}{b}))/\mathbb{Q}$.
3) Pour $n \geq 5$, en déduire que le degré de l'extension $\mathbb{Q}(\sin(\frac{2\pi}{n}))/\mathbb{Q}$ est :

$$\begin{array}{ll} \varphi(n) & \text{si } \operatorname{pgcd}(n,8) < 4 \\ \frac{\varphi(n)}{4} & \text{si } \operatorname{pgcd}(n,8) = 4 \\ \frac{\varphi(n)}{2} & \text{si } \operatorname{pgcd}(n,8) > 4. \end{array}$$

4) Application : déterminer le polynôme minimal de $\sin(\frac{2\pi}{5})$ sur $\mathbb{Q}$.
   Indication : on rappelle la formule $\sin(5x) = 16\sin(x)^5 - 20\sin(x)^3 + 5\sin(x)$ pour tout x réel.

Exercice 3. Il s'agit de redémontrer la formule de Gauss (1796) :

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

à l'aide de la théorie de Galois. Notons $z = \mathrm{e}^{\frac{2i\pi}{17}}$ et $K = \mathbb{Q}(z)$.

1) (a) Quel est le degré de l'extension $K/\mathbb{Q}$? Donner une base de K comme $\mathbb{Q}$-espace vectoriel.
   (b) Montrer que l'extension $K/\mathbb{Q}$ est galoisienne de groupe de Galois G cyclique. Quel est son ordre ?
   (c) Soit g un générateur de G. Pour $i \in \{0,1,2,3,4\}$ on note G_i le sous-groupe de G engendré par g^{2^i}. Quel est l'ordre de G_i ? En déduire une tour de corps $\mathbb{Q} \subset K_1 \subset K_2 \subset K_3 \subset K$ dans laquelle les extensions successives sont de degré 2.
   (d) Montrer que $g^8(z) = z^{-1}$. En déduire que $\cos\left(\frac{2\pi}{17}\right) \in K_3$ et $K_3 = \mathbb{Q}(\cos\left(\frac{2\pi}{17}\right))$.

   Ainsi, on peut théoriquement exprimer $\cos\left(\frac{2\pi}{17}\right)$ à l'aide de racines carrées de racines carrées de racines carrées.
2) **Cette partie est calculatoire et peut prendre du temps. Aussi, avant de l'aborder, traitez en priorité et en profondeur la question 1 qui est plus importante**.
   Maintenant, place aux calculs ! On note $\theta = \frac{2\pi}{17}$.

(a) Donner le plus petit entier n tel que la classe de n modulo 17 engendre $(\mathbb{Z}/17\mathbb{Z})^*$. En déduire un générateur g de G.

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

i. Montrer que a_1 appartient à K_1 et $a_2 \neq a_1$. En déduire $K_1 = \mathbb{Q}(a_1)$.

ii. Montrer que $a_1 + a_2 = -1$.

iii. Exprimer a_1 et a_2 en fonction de θ. En déduire $a_2 < 0$.

iv. Montrer que $a_1 a_2 = -4$. Pour cela, on rappelle que $\cos(\alpha)\cos(\beta) = \frac{1}{2}\left(\cos(\alpha+\beta) + \cos(\alpha-\beta)\right)$.

v. Donner les expressions algébriques de a_1 et a_2.

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

i. Montrer que b_1 appartient à K_2 et $b_2 \neq b_1$. En déduire $K_2 = K_1(b_1)$.

ii. Montrer que $b_1 + b_2 = a_1$.

iii. Exprimer b_1 et b_2 en fonction de θ. En déduire $b_2 < b_1$.

iv. Montrer que $b_1 b_2 = -1$.

v. Donner les expressions de b_1 et b_2 en fonction de a_1.

vi. On pose $b_3 = \displaystyle\sum_{i=0}^{3} g^{4i+1}(z)$ et $b_4 = g^2(b_3)$. Par la même méthode, exprimer b_3 et b_4 en fonction de a_2.

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

i. Montrer que c_1 appartient à K_3 et $c_2 \neq c_1$. En déduire $K_3 = K_2(c_1)$.

ii. Montrer que $c_1 + c_2 = b_1$.

iii. Exprimer c_1 et c_2 en fonction de θ. En déduire $c_2 < c_1$.

iv. Montrer que $c_1 c_2 = b_3$.

v. Donner les expressions de c_1 et c_2 en fonction de b_1 et b_3.

(e) Démontrer la formule de Gauss.

$$\cos\frac{P}{17} = -\tfrac{1}{16} + \tfrac{1}{16}\sqrt{17} + \tfrac{1}{16}\sqrt{(34-2\sqrt{17})} - \tfrac{1}{8}\sqrt{\{(17+3\sqrt{17}) - \sqrt{(34-2\sqrt{17})} - 2\sqrt{(34+2\sqrt{17})}\}};$$

les cosinus des multiples de cet angle ont une forme semblable, les sinus ont un radical de plus. Il y a certainement bien lieu de s'étonner que la divisibilité du cercle en 3 et 5 parties ayant été connue dès le temps d'*Euclide*, on n'ait rien ajouté à ces découvertes dans un intervalle de deux mille ans, et que tous les géomètres aient annoncé comme certain, qu'excepté ces divisions et celles qui s'en déduisent (les divisions en 2^μ, 15, 5.2^μ, 5.2^μ, 15.2^μ parties), on ne pouvait en effectuer aucune par des constructions géométriques.

Gauss, *Recherches arithmétiques*