Devoir 3

Exercice 1. *a) Montrer que le polynôme $P_1(T) = T^3 - 7T + 7$ a trois racines réelles x_1, x_2 et x_3 vérifiant $x_1 > x_2 > 0 > x_3$. Calculer le degré de l'extension $M = \mathbb{Q}(x_1)$ de $\mathbb{Q}$.*

b) Montrer que l'extension $M/\mathbb{Q}$ est galoisienne, et décrire son groupe de Galois.

c) On note $\pm y_1$, $\pm y_2$ et $\pm y_3$ les racines de $P_2(T) = T^6 - 7T^2 + 7$, numérotées de façon que $x_i = y_i^2$, et L le corps $\mathbb{Q}(y_1, y_2, y_3)$.

i) Montrer que y_3 n'appartient pas à $\mathbb{Q}(y_1, y_2)$.

ii) Montrer que y_2 n'appartient pas à $\mathbb{Q}(y_1)$.

iii) Calculer le degré de M sur L.

iv) L'extension $L/\mathbb{Q}$ est-elle galoisienne? Abélienne?

d) On note G le groupe $Aut(L)$. Montrer que, pour $i \in \{1, 2, 3\}$, il existe deux éléments τ_i et τ'_i de G tels que, pour $j \neq i$, on ait

$$\tau_i(y_i) = -y_i, \quad \tau'_i(y_i) = y_i, \quad \tau_i(y_j) = y_j, \quad \tau'_i(y_j) = -y_j.$$

Montrer qu'il existe un élément τ de G tel que

$$\forall i \in \{1, 2, 3\}, \quad \tau(y_i) = -y_i.$$

Donner la liste des sous-corps N de L contenant M et tels que $[L : N] = 2$.

e) Montrer qu'il existe un élément σ de G tel que

$$\sigma(y_1) = y_2, \quad \sigma(y_2) = y_3, \quad \sigma(y_3) = y_1,$$

et calculer

$$\tau_1\sigma\tau_3, \quad \tau_1\sigma^2\tau_1, \quad \tau'_3\sigma\tau'_2.$$

f) Montrer que $\sqrt{-7}$ appartient à L et déterminer le groupe $Aut(L/\mathbb{Q}(\sqrt{-7}))$.

g) On pose $\theta = y_1 + y_2 + y_3$. Calculer le degré de θ sur $\mathbb{Q}$ (on pourra étudier les images de θ sous l'action de G). Quelle est la structure du groupe $Aut(L/\mathbb{Q}(\theta))$? Est-il distingué dans G ?

h) Indiquer combien de sous-corps de $\mathbb{Q}(\theta)$ contiennent $\sqrt{-7}$.

Preuve :

(a) La fonction $t \mapsto P_1(t)$ atteint son minimum sur $\mathbb{R}^+$ au point $\sqrt{7/3}$, où elle vaut

$$\frac{7}{3\sqrt{3}}(3\sqrt{3} - 2\sqrt{7}) < 0.$$

Comme $P_1(0)$ et $P_1(1)$ sont positifs et $P_1(-4) = -29$ est négatif, P_1 a trois racines réelles distinctes, dont une seule est négative. Si une des racines de P_1 était rationnelle, ce serait un entier divisant 7, ce qui ne laisse que 4 possibilités, dont aucune n'est racine de P_1. On en déduit que P_1 est irréductible sur $\mathbb{Q}$, et le degré de M sur $\mathbb{Q}$ est 3. On aurait aussi pu invoquer le critère d'Eisenstein pour le nombre premier 7.

(b) Le discriminant $\Delta = -(4(-7)^3 + 27.7^2) = 49$ est un carré sur $\mathbb{Q}$. L'exercice 17 de la feuille 3 permet d'en déduire que l'extension M/Q est galoisienne. Le groupe de Galois agit sur les trois racines de P_1 comme le groupe alterné: les deux automorphismes non triviaux de M permutent circulairement x_1, x_2 et x_3.

(c) (i) Le corps $\mathbb{Q}(y_1, y_2)$ est inclus dans $\mathbb{R}$ et ne peut donc contenir y_3 qui est imaginaire pur.

(ii) L'automorphisme de M qui envoie x_1 sur x_2 se prolonge en un automorphisme ψ de L qui envoie y_1 sur $\pm y_2$ et y_2 sur $\pm y_3$. Si $y_2 \in \mathbb{Q}(y_1)$, il existe une fraction rationnelle R à coefficients dans $\mathbb{Q}$ telle que $R(y_1) = y_2$. En appliquant ψ, on trouve $R(\pm y_2) = \pm y_3$, donc $y_3 \in \mathbb{Q}(y_1, y_2)$, en contradiction avec la question précédente.

(iii) Le même raisonnement qu'au b) montre que $y_1 \notin M$ et $\mathbb{Q}(y_1)$ est quadratique sur M, donc de degré 6 sur $\mathbb{Q}$ (on peut aussi voir par le critère d'Eisenstein que P_2 est irréductible sur $\mathbb{Q}$). Les questions 2 b) et 2 a) montrent que $\mathbb{Q}(y_1, y_2)$ est une extension quadratique de $\mathbb{Q}(y_1)$ et L est une extension quadratique de $\mathbb{Q}(y_1, y_2)$. En conclusion, L/M est de degré 8 et $L/\mathbb{Q}$ de degré 24.

(iv) L est le corps de décomposition de P_2, c'est donc une extension galoisienne de $\mathbb{Q}$. Si elle était abélienne, tous ses sous-corps seraient galoisiens. Ce n'est pas le cas, puisque $\mathbb{Q}(y_1)$ ne contient pas le conjugué y_3 de y_1.

(d) Le groupe $\mathrm{Gal}(L/M)$ est d'ordre 8. Pour tout élément τ de ce groupe, on a $\tau(x_i) = x_i$, donc $\tau(y_i) = \epsilon_i y_i$, avec $\epsilon_i = \pm 1$ pour $i \in \{1, 2, 3\}$. L'application qui à τ associe le triplet $(\epsilon_1(\tau), \epsilon_2(\tau), \epsilon_3(\tau))$ induit donc un isomorphisme de $\mathrm{Gal}(L/M)$ sur $\{\pm 1\}^3$. Par exemple, le τ_1 de l'énoncé est l'image réciproque de $(-1, 1, 1)$ et le τ de l'énoncé est l'image réciproque de $(-1, -1, -1)$. Les 7 éléments non triviaux de $\mathrm{Gal}(L/M)$ sont les τ_i, les τ_i' et τ. Leurs corps fixes sont les 7 sous-corps de L contenant M et de degré 4 sur M. Le corps fixe de τ_1 est $\mathbb{Q}(y_2, y_3)$, celui de τ_1' est $\mathbb{Q}(y_1, y_2 y_3)$. Enfin, le corps fixe de τ est $M(y_1 y_2, y_2 y_3)$.

(e) L'élément ψ de G construit à la question 3 b) envoie y_1 sur $\epsilon_2 y_2$, y_2 sur $\epsilon_3 y_3$ et y_3 sur $\epsilon_1 y_1$. En le composant à gauche par l'élément de $\mathrm{Gal}(L/M)$ qui envoie y_i sur $\epsilon_i y_i$, on trouve l'élément σ de G cherché. Un élément de G est uniquement caractérisé par son action sur les y_i. On en déduit

$$\tau_1 \sigma \tau_3 = \tau_3 \sigma \tau_2 = \tau_2 \sigma \tau_1 = \tau_3' \sigma \tau_2' = \tau_2' \sigma \tau_1' = \tau_1' \sigma \tau_3' = \sigma.$$

Quant à $\tau_1 \sigma^2 \tau_1 = \tau_2' \sigma^2$, il n'a rien de remarquable...

(f) On a $x_1 x_2 x_3 = -7$, et $y_1 y_2 y_3 = \pm\sqrt{-7} \in L$. L'image de $\sqrt{-7}$ par σ est donc $\sqrt{-7}$. Le groupe de Galois de $L/\mathbb{Q}(\sqrt{-7})$ a 12 éléments, soit

$$H = \{Id, \sigma, \sigma^2, \tau_i', \tau_i'\sigma, \tau_i'\sigma^2\}.$$

(g) Les 8 images $\pm y_1 \pm y_2 \pm y_3$ sont distinctes, puisque une égalité entre elles donnerait une relation linéaire entre y_1, y_2 et y_3 sur $\mathbb{Q}$. On en déduit que θ est de degré 8 sur $\mathbb{Q}$, et le groupe de Galois $\mathrm{Gal}(L/\mathbb{Q}(\theta)$ a 3 éléments: c'est $\{Id, \sigma, \sigma^2\}$, qui est cyclique d'ordre 3. On a vu plus haut que $\tau_1 \sigma^2 \tau_1^{-1} = \tau_1 \sigma^2 \tau_1 = \tau_2' \sigma^2$ n'est pas dans ce sous-groupe, qui n'est donc pas distingué.

(h) Un sous-corps de $\mathbb{Q}(\theta)$ qui contient $\sqrt{-7}$ correspond à un sous-groupe de H qui contient $\{Id, \sigma, \sigma^2\}$. Un tel sous-groupe, s'il n'est pas réduit à $\{Id, \sigma, \sigma^2\}$, contient l'un des τ_i', par exemple τ_1', donc il contient aussi $\tau_2' = \sigma \tau_1' \sigma^2$ et $\tau_3' = \tau_1' \tau_2'$. Finalement, le groupe contient H tout entier, et il n'y a aucun corps intermédiaire entre $K(\theta)$ et $\mathbb{Q}(\sqrt{-7})$.

Exercice 2. ***Transcendance de*** π

(1) Soit f un polynôme à coefficients réels de degré m. Montrez que pour tout nombre complexe z, l'intégrale complexe

$$I(f; z) = \int_0^1 z e^{z(1-u)} f(zu) dz$$

vérifie

$$I(f; z) = e^z \sum_{j=0}^{m} f^{(j)}(0) - \sum_{j=0}^{m} f^{(j)}(z)$$

ainsi que la majoration

$$|I(f; z)| \leq |z| e^{|z|} \sup_{u \in [0,1]} |f(zu)|$$

(2) Soit f un polynôme à coefficients entiers. Montrez que pour tout $n \geq 0$, il existe un polynôme f_n à coefficients entiers tel que $f^{(n)} = n! f_n$.

(3) Pour un polynôme f et $g : \mathbb{C} \to \mathbb{C}$ une fonction, on note $\sum_{f(\alpha)=0} g(\alpha)$ la somme $g(\alpha_1) + \cdots + g(\alpha_n)$ où les α_i sont les racines de f répétées autant de fois que leur multiplicité. Montrez que si f est à coefficients entiers de coefficient a, alors pour tout $n \geq 0$, $a^n \sum_{f(\alpha)=0} \alpha^n$ appartient à $\mathbb{Z}$.

Indication: on pourra introduire une matrice dont la trace est $a^n \sum_{f(\alpha)=0} \alpha^n$.

(4) *Soit f un polynôme à coefficients entiers tel que $f(0) \neq 0$ et de coefficient dominant a. Pour p un nombre premier, soit $g(x) = x^{p-1} f^p(x)$ et $J_p = \sum_{f(\alpha)=0} I(g; \alpha)$. Montrez qu'il existe un entier M tel que*

$$\frac{a^{m-p}}{(p-1)!} J_p = a^{m-p} N f(0)^p + pM$$

où $N = \sum_{f(\alpha)=0} e^\alpha$. En déduire que N n'est pas un entier non nul.

(5) *On veut montrer que π est transcendant. On raisonne par l'absurde: soit f un polynôme irréductible à coefficients entiers tel que $f(i\pi) = 0$ dont on note $\alpha_1, \cdots, \alpha_n$ les racines.*

(a) *En développant l'égalité $\prod_{f(\alpha)=0}(1 + e^\alpha)$ montrez que*

$$\sum_{\epsilon \in \{0,1\}^n} exp(\sum \epsilon_j \alpha_j) = 0.$$

(b) *Soit $Q(X) = \prod_{\epsilon \in \{0,1\}^n}(X - \sum \epsilon_j \alpha_j)$. Montrer que $Q(X) \in \mathbb{Q}[X]$.*

(c) *En utilisant la question (4), aboutissez à une contradiction.*

Preuve : (1) On intègre par partie soit

$$\begin{aligned} I(f; z) &= [-e^{z(1-u)} f(zu)]_0^1 + \int_0^1 e^{z(1-u)} z f'(zu) du \\ &= -f(z) + e^z f(0) + I(f'; z); \end{aligned}$$

d'où le résultat par récurrence sur le degré de f. Pour obtenir la majoration de $|I(f; z)|$, il suffit d'intégrer sur $[0, 1]$, l'inégalité

$$|z e^{z(1-u)} f(zu)| \leq |z| e^{|z|} \sum_{u \in [0,1]} |f(zu)|,$$

valable pour tout $u \in [0, 1]$.

(2) Par linéarité, il suffit de considérer le cas de $f = X^m$; $f^{(m)} = m(m-1) \cdots (m-n+1) X^{m-n}$. Le polynôme $f_n := C_n^m X^{m-n}$ est à coefficients entiers et vérifie $f^{(n)} = n! f_n$.

(3) Soit m le degré de f et notons A la matrice compagnon du polynôme f/a. Par construction $aA \in \mathbb{M}_m(\mathbb{Z})$ de sorte que $a^n A^n$ est aussi à coefficients entiers ainsi que sa trace. Or les valeurs propres de $a^n A^n$ sont les $(a\alpha)^n$, α parcourant les racines de f avec multiplicités.

(4) On a

$$J_p = N\Big(\sum_n g^{(n)}(0)\Big) - \sum_n \Big(\sum_{f(\alpha)=0} g^{(n)}(\alpha)\Big).$$

Si $f(\alpha) = 0$, α est un zéro d'ordre p de g et donc $g^{(n)}(\alpha) = 0$ pour tout $n < p$. D'autre part si $n \geq p$, d'après ce qui précède, $g_n = g^{(n)}/p!$ est un polynôme à coefficients entiers de degré $m - n$ et

$$a^{m-n} \sum_{f(\alpha)=0} g^{(n)}(\alpha)$$

est entier, multiple de $p!$. En 0, on a $g^{(n)}(0) = 0$ pour $n < p - 1$ et pour $n \geq p$ alors que

$$g^{(p-1)}(0) = (p-1)! f(0)^p$$

Ainsi, il existe un entier M tel que

$$\frac{a^{m-p}}{(p-1)!} J_p = a^{m-p} N f(0)^p + pM$$

Le second membre de cette égalité est entier et si p ne divise pas $aNf(0)$, il n'est pas multiple de p; il est en particulier non nul et donc au moins égal à 1 en valeur absolue. Ainsi

$$|J_p| \geq (p-1)! a^{p-m} = (p-1)! p^{1-p \deg f}$$

Or la majoration de l'intégrale I dans (1) implique qu'il existe un réel $c > 0$ tel que $|J_p| \leq c^p$ pour tout p. Quand p tend vers l'infini, la formule de Stirling rend ces deux inégalités incompatibles, d'où le résultat.

(5) (a) c'est clair

(b) Les $\sum \epsilon_j \alpha_j = 0$ sont les racines du polynôme

$$P_0 = \prod_{\epsilon \in [0,1]^n} (X - \sum_j \epsilon_j \alpha_j)$$

dont les coefficients s'expriment comme des polynômes symétriques en les α_j: ce sont donc des polynômes en les fonctions symétriques élémentaires des α_j, donc en les coefficients de f. Ce sont donc des nombres rationnels.

(c) Soit un entier N tel que $NP_0 \in \mathbb{Z}[X]$ et soit $q \geq 1$ la multiplicité del a racine 0 dans P_0. On pose $P := NF_0/X^q$: c'est un polynôme à coefficients entiers avec $P(0) \neq 0$. De plus on a

$$0 \sum_{\epsilon \in [0,1]^n} \exp(\sum_j \epsilon_j \alpha_j) = q + \sum_{P(\beta)=0} e^\beta$$

ce qui contredit (4).