Feuille d'exercices 2

Remarque : Tous les exercices ne seront pas traités en séance de TD, j'indiquerai au fur et à mesure sur la page du forum (http ://cours-jussieu-nombres.monforum.com/cours-et-td-2009-vf7.html) les exercices que nous aurons abordés.

1 Approximations rationnelles

Exercice 1.1. ***Dirichlet***

(1) Soient $x_{i,j}$ avec $1 \leq i \leq n$ et $1 \leq j \leq m$ des réels et soit $Q > 1$ un entier. Montrer qu'il existe alors des entiers $q_1, \cdots, q_m, p_1, \cdots, p_n$ tels que

$$1 \leq \max\{|q_1|, \cdots, |q_m|\} \leq Q^{n/m}$$

$$|x_{i,1}q_1 + \cdots + x_{i,m}q_m - p_i| \leq \frac{1}{Q} \qquad \forall 1 \leq i \leq n.$$

(2) Supposons que

$$(x_{1,1}q_1 + \cdots, +x_{1,m}q_m, \cdots, x_{n,1}q_1 + \cdots + x_{n,m}q_m)$$

n'appartiennent jamais à $\mathbb{Z}^n$ pour tout $(q_1, \cdots, q_m) \in \mathbb{Z}^m$. Montrer qu'il existe alors une infinité de $(m+n)$-uplets premiers entre eux dans leur ensemble, tels que, pour $q = \max\{|q_1|, \cdots, |q_m|\} > 0$, on a

$$|x_{i,1}q_1 + \cdots + x_{i,m}q_m - p_i| \leq \frac{1}{Q} \qquad \forall 1 \leq i \leq n.$$

Exercice 1.2. *a) Soit $f(X,Y) = aX^2 + bXY + cY^2 \in \mathbb{R}[X,Y]$ un polynôme homogène de degré 2 à coefficients réels de discriminant positif*

$$\Delta = b^2 - 4ac > 0.$$

Soit $\epsilon > 0$. Montrer qu'il existe $(x,y) \in \mathbb{Z}^2$ avec $(x,y) \neq (0,0)$ tel que

$$|f(x,y)| \leq \sqrt{\Delta/5} + \epsilon.$$

b) Soit Δ un nombre réel positif. Donner un exemple d'un polynôme homogène f de degré 2 dont le discriminant est Δ tel que

$$\min\big\{|f(x,y)| \ ; \ (x,y) \in \mathbb{Z} \times \mathbb{Z}, \ (x,y) \neq (0,0)\big\} = \sqrt{\Delta/5}.$$

c) Soit Δ un nombre réel positif. Donner un exemple d'un polynôme homogène $f(X,Y) = aX^2 + bXY + cY^2$ de degré 2 dont le discriminant $b^2 - 4ac$ est Δ et tel que

$$\min\big\{|f(x,y)| \ ; \ (x,y) \in \mathbb{Z} \times \mathbb{Z}, \ (x,y) \neq (0,0)\big\} = \sqrt{\Delta/8}.$$

d) Donner un exemple d'un polynôme homogène f de degré 2 de discriminant $\Delta > 0$ tel que

$$\min\big\{|f(x,y)| \ ; \ (x,y) \in \mathbb{Z} \times \mathbb{Z}, \ (x,y) \neq (0,0)\big\} = 0.$$

Exercice 1.3. *a) Soit θ un nombre réel dans l'intervalle $0 < \theta < 3$. Montrer que les deux propriétés suivantes sont équivalentes.*

(i) Il existe une constante $c_1 > 0$ telle que, pour tout nombre rationnel p/q, on ait

$$\left|\sqrt[3]{2} - \frac{p}{q}\right| \geq \frac{c_1}{q^\theta}.$$

(ii) Il existe une constante $c_2 > 0$ telle que, pour tout couple (x,y) d'entiers $\neq (0,0)$, on ait

$$|x^3 - 2y^3| \geq c_2|y|^{3-\theta}.$$

b) Montrer qu'il existe une constante $c_3 > 0$ telle que, pour une infinité de couple (x,y) d'entiers, on ait

$$|x^3 - 2y^3| \leq c_3|y|.$$

2 Irrationnalité autour de e et π

Exercice 2.4. *On rappelle que pour tout $a \in \mathbb{R}$, $e^a = \sum_{n=0}^{\infty} \frac{a^n}{n!}$.*

(1) On suppose qu'il existe $a, b \in \mathbb{N}$ tels que $e = a/b$ ($b \neq 0$ avec a et b premiers entre eux). En étudiant $\alpha = (k!)(e - u_k)$ pour $k > b$, montrez que l'on aboutit à une contradiction.

(2) Montrez que e n'est pas racine d'un polynôme de degré 2 à coefficients rationnels.

(3) Montrez que $e^{\sqrt{2}} + e^{-\sqrt{2}}$ est irrationnel.

(4) Montrez que e^2 n'est pas racine d'un polynôme de degré 2 à coefficients rationnels.

(5) Montrez que $e^{\sqrt{3}}$ est irrationnel.

(6) Soit $(b_n)_{n\geq 0}$ une suite bornée de nombres entiers ; montrez que les conditions suivantes sont équivalentes :

(i) il existe $N > 0$ tel que $b_n = 0$ pour tout $n \geq N$;

(ii) le nombre $\nu_1 = \sum_{n\geq 0} \frac{b_n}{n!}$ est rationnel ;

(iii) Le nombre $\nu_2 = \sum_{n\geq 0} \frac{b_n 2^n}{n!}$ est rationnel.

Exercice 2.5. π^2 est irrationnel *: Soit $f_n(x) = \frac{x^n(1-x)^n}{n!}$.*

(a) Montrez que pour tout $m \geq 0$, $f_n^{(m)}(0) \in \mathbb{Z}$.

(b) On suppose qu'il existe $a, b \in \mathbb{N}$ premiers entre eux et $b \neq 0$ tels que $\pi^2 = a/b \in \mathbb{Q}$ et on pose

$$G_n(x) = b^n[\pi^{2n} f_n(x) - \pi^{2n-2} f_n''(x) + \cdots + (-1)^n f_n^{(2n)}(x)].$$

Montrez que $G_n(0)$ et $G_n(1)$ sont des entiers.

(c) Montrez que

$$\pi \int_0^1 a^n \sin(\pi x) f_n(x) dx = G_n(0) + G_n(1)$$

et conclure.

3 Autour de la transcendance de e et π

Exercice 3.6. *e et π sont transcendants :*

(1) ***Formule de Hermite*** *: commençons par quelques généralités.*

(a) Soit $D : \mathbb{R}[X] \to \mathbb{R}[X]$ l'application linéaire de dérivation. Montrez que $(\mathrm{Id} - D)$ est un opérateur inversible d'inverse $(\mathrm{Id} - D)^{-1} = \sum_{k\geq 0} D^k$.

(b) Pour $g \in \mathbb{R}[X]$ montrez qu'une primitive de $e^{-t}g(t)$ est $-e^{-t}(\mathrm{Id} - D)^{-1}(g)$ et déduisez-en la formule d'Hermite pour tout z complexe :

$$I(g; z) = \int_0^1 z e^{z(1-u)} g(zu) du = e^z \sum_{i=0}^{+\infty} g^{(i)}(0) - \sum_{i=0}^{+\infty} g^{(i)}(z).$$

(c) Montrez que $|I(g; z)| \leq |z|e^{|z|} \sup_{u\in[0,1]} |g(zu)|$.

(d) Soit f un polynôme à coefficients entiers ; montrez que pour tout $k \geq 0$, il existe un polynôme f_k à coefficients entiers tel que $f^{(k)} = k! f_k$.

(2) ***Transcendance de*** *e :*

(a) à l'aide de $g_p(x) = \frac{x^{p-1} f(x)^p}{(p-1)!}$ où $f(x) = \prod_{i=1}^n (x - i)$, construisez pour tout $i = 1, \cdots, n$, une suite de rationnels $(\frac{a_{p,i}}{b_p})_{p\in\mathcal{P}}$ qui converge vers e^i.

(b) On suppose qu'il existe des entiers $a_0, \cdots, a_n \in \mathbb{Z}$ tels que $a_0 + a_1 e + \cdots + a_n e^n = 0$ avec $a_0 a_n \neq 0$. On pose pour tout $p \in \mathbb{N}$, $J_p = a_0 I(g_p; 0) + \cdots + a_n I(g_p; n)$. Montrez que :

(i) $J_p \in \mathbb{Z}$;

(ii) J_p tend vers 0 quand p tend vers $+\infty$;

(iii) si p est un nombre premier assez grand, $J_p \not\equiv 0 \mod p$.

(c) *Déduisez de ce qui précède que e est transcendant.*

(3) ***Transcendance de π :***

(a) *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 $\mathbb{Z}$.*

(b) *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 des entiers Q, R tels que*

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

où $N = \sum_{f(\alpha)=0} e^\alpha$. En déduire que si $N \in \mathbb{Z}$ alors il est nul.

(c) *On suppose qu'il existe un polynôme f à coefficients entiers tel que $f(i\pi) = 0$ dont on note $\alpha_1, \cdots, \alpha_n$ les racines.*

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

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

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

(iii) *Déduisez de ce qui précède que π est transcendant.*

Exercice 3.7. *Déduire du théorème de Gel'fond-Schneider la transcendance de chacun des nombres*

$$2^{\sqrt{2}}, \quad 2^i, \quad e^\pi, \quad e^{\pi\sqrt{2}}, \quad \cos(\pi\sqrt{2}), \quad \frac{\log 3}{\log 2}, \quad \frac{\pi}{\log 2}.$$

Exercice 3.8. *On considère un nombre complexe non nul a, un nombre complexe irrationnel b, et une détermination non nulle $\log a$ du logarithme de a. Chacun des trois nombres a, b et $a^b = e^{b \log a}$ peut être algébrique ou transcendant, ce qui fait a priori 8 possibilités, mais le théorème de Gel'fond–Schneider montre que l'une de ces possibilités est exclue : les trois nombres en question ne peuvent pas tous être algébriques. Donner un exemple de chacune des 7 autres situations (on pourra utiliser les théorèmes de Hermite–Lindemann et Gel'fond–Schneider).*

4 Extensions de corps, groupes de Galois

Exercice 4.9. *Montrer que si a et b sont deux éléments non nuls d'un corps K de caractéristique différente de 2, $K(\sqrt{a})$ est égal à $K(\sqrt{b})$ si et seulement si b/a est un carré dans K.*

Exercice 4.10. *Soit $K = \mathbb{Q}(i + \sqrt{2})$. Montrer que K est galoisien sur $\mathbb{Q}$. Calculer le degré de K sur $\mathbb{Q}$ et le groupe de Galois de $K/\mathbb{Q}$. Donner la liste des sous-corps de K.*

Exercice 4.11. *Soit $L = \mathbb{Q}(\sqrt{5})$ et $M = \mathbb{Q}(\sqrt{2 + \sqrt{5}})$. Déterminer les degrés des extensions $L/\mathbb{Q}$, $M/\mathbb{Q}$ et M/L. Indiquer lesquelles de ces extensions sont galoisiennes. Déterminer les polynômes minimaux de $\sqrt{2 + \sqrt{5}}$ sur $\mathbb{Q}$ et sur L.*

Exercice 4.12. *Soit a et b deux rationnels, donnez une condition suffisante pour que le polynôme $X^4 + aX^2 + b$ soit irréductible sur $\mathbb{Q}$. Donnez une CNS pour qu'alors son corps de rupture soit galoisien sur $\mathbb{Q}$. En particulier que se passe-t-il si on suppose que $a^2 - 4b$ est positif mais pas un carré rationnel, et b négatif.*

Exercice 4.13. *Soit $K = \mathbb{Q}(\sqrt[3]{2})$, L la clôture galoisienne de K sur $\mathbb{Q}$. Calculer le degré de L sur $\mathbb{Q}$, le groupe de Galois de L/K. Donner la liste des sous-corps de L.*

Exercice 4.14. *On rappelle que, si L/K est une extension cubique de corps de caractéristique différente de 3, L est engendré par une racine α d'un polynôme de $K[X]$ de la forme $X^3 + pX + q$. Montrer que si la caractéristique est aussi différente de 2, l'extension L/K est galoisienne si et seulement si le discriminant $\Delta = -(4p^3 + 27q^2)$ est un carré dans K.*

Exercice 4.15. *Soit G le groupe de Galois de $X^5 - 2$. Quel est le cardinal de G ? Est-il abélien, résoluble ?*

Exercice 4.16. *Quel est le degré du corps de décomposition du polynôme $(X^3 - 5)(X^3 - 7)$ sur $\mathbb{Q}$?*

Exercice 4.17. *Déterminez le groupe de Galois de $X^6 - 5$ sur $\mathbb{Q}$, $\mathbb{R}$.*

Exercice 4.18. *Trouvez un élément primitif de $\mathbb{Q}[\sqrt{3}, \sqrt{7}]$.*

Exercice 4.19. *Soit G le groupe de Galois de $(X^3 - 5)(X^4 - 2)$ sur $\mathbb{Q}$.*
1) Donner un ensemble de générateurs de G ainsi que l'ensemble de relations entre eux.
2) G est-il un groupe cyclique, diédral, symétrique ?

Exercice 4.20. *Trouvez un élément primitif du corps de décomposition de $(X^2 - 2)(X^2 - 5)(X^2 - 7)$.*

Exercice 4.21. *Soit ζ un racine primitive 12-ième de l'unité. Combien y a-t-il d'extension comprises entre $\mathbb{Q}[\zeta^3]$ et $\mathbb{Q}[\zeta]$.*

Exercice 4.22. *Soit ζ une racine primitive 5-ième de l'unité.*
(1) Décrivez le groupe de Galois de $K = \mathbb{Q}[\zeta]/\mathbb{Q}$ et montrez que K contient un unique sous-corps de degré 2 sur $\mathbb{Q}$ à savoir $\mathbb{Q}[\zeta + \zeta^4]$.
(2) Donnez le polynôme minimal de $\zeta + \zeta^4$ sur $\mathbb{Q}$.
(3) Donnez le groupe de Galois de $(X^2 - 5)(X^5 - 1)$.
(4) Donnez le groupe de Galois de $(X^2 + 3)(X^5 - 1)$.

Exercice 4.23. *Notons K le corps $\mathbb{Q}(\sqrt{-15})$, f son automorphisme non trivial, et α un élément de K tel que le polynôme $X^3 - \alpha$ soit irréductible sur K. Pourquoi existe-t-il de tels α ? On note L le corps de décomposition de ce polynôme, et $\{\theta, j\theta, j^2\theta\}$ ses différentes racines dans L.*
1) Pourquoi sont-elles de cette forme ?
2) Montrer que L est une extension galoisienne de K de degré 6, et que L contient $\sqrt{5}$.
3) Montrer qu'il existe deux $K-$automorphismes σ et τ de L tels que

$$\sigma(\sqrt{5}) = \sqrt{5}, \quad \sigma(\theta) = j\theta, \quad \tau(\sqrt{5}) = -\sqrt{5}, \quad \tau(\theta) = \theta.$$

4) Déterminer l'ordre des éléments σ et τ du groupe $Gal(L/K)$ et calculer $\tau\sigma\tau^{-1}$. Etablir la liste des extensions de K contenues dans L.
5) On suppose désormais que $N_{K/\mathbb{Q}}(\alpha)$ est le cube d'un nombre rationnel b (on admettra que c'est possible). Déterminer les différents conjugués de θ sur $\mathbb{Q}$. Montrer que l'extension $L/\mathbb{Q}$ est galoisienne de degré 12. Prouver qu'il est possible de prolonger l'automorphisme f de K en un automorphisme ϕ de L tel que $\phi(\sqrt{5}) = \sqrt{5}$ et $\phi(\theta) = b/\theta$. Calculer ϕ^2, $\phi\sigma\phi^{-1}$ et $\phi\tau\phi^{-1}$. Montrer que $\mathbb{Q}(\sqrt{5})$ admet une extension de degré 3 contenue dans L et galoisienne sur $\mathbb{Q}$.

Exercice 4.24. *Montrer que si K est un corps de caractéristique p non nulle, le corps $M = K(X, Y)$ des fractions rationnelles en deux indéterminées à coefficients dans K est une extension de degré p^2 de son sous-corps $L = K(X^p, Y^p)$. Montrer que si α est un élément de M qui n'est pas dans L, son polynôme minimal sur L est de degré p. En déduire que le mot "séparable" dans l'énoncé du théorème de l'élément primitif n'est pas inutile.*

Exercice 4.25. *On note L le corps de décomposition dans $\mathbb{C}$ du polynôme $P = T^4 - 3T - 3$.*
a) Montrer que le polynôme P est irréductible sur $\mathbb{Q}$, et qu'il admet dans $\mathbb{C}$ deux racines réelles x et y, et un couple $(z, \overline{z})$ de racines complexes conjuguées l'une de l'autre.
b) Notons $T^2 + aT + b$ et $T^2 - aT + b'$ les polynômes unitaires de degré 2 qui divisent P dans $\mathbb{R}[X]$. Montrer que a est une racine du polynôme $X^6 + 12X^2 - 9$, et calculer le degré de a^2 sur $\mathbb{Q}$.
c) Montrer que $[L : \mathbb{Q}]$ est un multiple de 12.
d) Montrer que le groupe alterné $\mathcal{A}_4$ est le seul sous-groupe d'indice 2 du groupe symétrique $\mathcal{S}_4$.
e) Montrer qu'il existe un automorphisme de L qui échange z et $\overline{z}$ et qui laisse x fixe. Déterminer le groupe de Galois de $L/\mathbb{Q}$. Combien L a-t'il de sous-corps ?

Exercice 4.26. *Montrez en réduisant modulo 2 et 3, que le groupe de Galois de $X^5 - X - 1$ est $\mathcal{S}_5$.*

Exercice 4.27. *(1) Soit $E \subset F$ une extension quadratique et soit $x \in F\backslash E$ tel que $x^2 \in E$. Si $a \in F$ est un carré montrez que ou bien a est un carré dans E ou bien ax^2 est un carré dans E.*

(2) Soient $p_1, \cdots, p_n$ des nombres premiers distincts. On considère les propriétés suivantes :

(a_n) le corps $\mathbb{Q}[\sqrt{p}_1, \cdots, \sqrt{p}_n]$ est de degré 2^n sur $\mathbb{Q}$;

(b_n) $x \in \mathbb{Q}$ est un carré dans $\mathbb{Q}[\sqrt{p}_1, \cdots, \sqrt{p}_n]$ si et seulement s'il existe une partie $I \subset \{1, \cdots, n\}$ telle que $x \prod_{i\in I} p_i$ est un carré dans $\mathbb{Q}$.

(i) Montrez que $(a_n) \wedge (b_n) \Rightarrow (a_{n+1})$.

(ii) Montrer que $(a_n) \wedge (b_{n-1}) \Rightarrow (b_n)$.

(iii) En déduire que (a_n) et (b_n) sont vraies pour tout n.

(iv) Montrez que la famille $\sqrt{2}, \sqrt{3}, \cdots$ des racines carrées des nombres premiers, est libre sur $\mathbb{Q}$.

Exercice 4.28. *Soit $P(X) = a_nX^n + \cdots + a_0 \in \mathbb{C}[X]$; on veut prouver que P est totalement décomposé dans $\mathbb{C}[X]$.*

(1) Montrer que $Q(X) = (X^2 + 1)P(X)\bar{P}(X) \in \mathbb{R}[X]$.

(2) On note D le corps de décomposition sur $\mathbb{R}$ de Q et on note G le groupe de Galois de $D/\mathbb{R}$ de cardinal 2^nm avec m impair.

(i) Montrer que $n \geq 1$.

(ii) En notant que tout polynôme réel de degré impair admet au moins une racine réelle, montrer, en utilisant le théorème de Sylow, que $m = 1$.

(iii) En notant que tout nombre complexe est le carré d'un nombre complexe, montrer, en utilisant le théorème de Sylow, que $n = 1$.

(iv) Montrer que $D = \mathbb{C}$ et conclure.

Exercice 4.29. *a) Montrer que $P_1(T) = T^3 - 7T + 7$ 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 $\sqrt{-7}$.

5 Solutions

1.1 (1) Considérons les points $(\{x_{1,1}a_1+\cdots,+x_{1,m}a_m\},\cdots,\{x_{n,1}a_1+\cdots+x_{n,m}a_m\})$ où les a_j sont des entiers tels que $0\le a_j<Q^{n/m}$. Il y a au moins Q^n tels points qui par définition de $\{x\}$ appartiennent à l'hypercube $|x|_\infty\le 1$ de $\mathbb{R}^n$, tout comme le point $(1,\cdots,1)$ ce qui donne donc Q^n+1 points de l'hypercube unité $B_{\infty,n}$. On divise $B_{\infty,n}$ en Q^n petits cubes disjoints de coté $1/Q$ de sorte qu'il existe 2 points parmi les Q^n+1 ci-dessus qui appartiennent au même petit cube soit par exemple

$$(x_{1,1}a_1+\cdots,+x_{1,m}a_m-b_1,\cdots,x_{n,1}a_1+\cdots+x_{n,m}a_m-b_n)\text{ et}$$
$$(x_{1,1}a'_1+\cdots,+x_{1,m}a'_m-b'_1,\cdots,x_{n,1}a'_1+\cdots+x_{n,m}a'_m-b'_n)$$

avec $(a_1,\cdots,a_m)\neq(a'_1,\cdots,a'_m)$. Le résultat est alors obtenu pour $q_i=a_i-a'_i$ et $p_i=b_i-b'_i$.

(2) En effet vu l'hypothèse $|x_{i,1}q_1+\cdots+x_{i,m}q_m-p_i|\neq 0$ de sorte que quand Q grandit, on obtient de nouveaux $(m+n)$-uplets.

Remarque : les résultats précédents peut se reformuler ainsi : il existe un point $(v,w)=(q_1,\cdots,q_m,p_1,\cdots,p_n)\in\mathbb{Z}^{m+n}$ tel que

$$1\le|v|_\infty<Q^{n/m}\text{ et }|\mathcal{L}(v)-w|_\infty\le Q^{-1}<|v|_\infty^{-m}$$

où pour $(v_1,\cdots,v_m)\in\mathbb{R}^n$, $\mathcal{L}(v)=(L_1(v),\cdots,L_n(v))$ avec $L_i(v)=x_{i,1}v_1+\cdots+x_{i,m}v_m$. Minkowski a montré, cf. [**?**] p.36, qu'il existe un point entier (v,w) avec $v\neq 0$ tel que

$$|\mathcal{L}(v)-w|_\infty^n<C_{m,n}|v|_\infty^{-m}\qquad C_{m,n}=\frac{m^nn^m}{(m+n)^{m+n}}\frac{(m+n)!}{m!n!}<1.$$

1.2 (a) On considère le polynôme $P(T)=aT^2+bT+c=a(T-\alpha)(T-\beta)$ avec $\alpha,\beta\in\mathbb{R}$ tels que $0<\alpha-\beta=\frac{\sqrt{\Delta}}{a}=\delta$. Soit $t=p/q\in\mathbb{Q}$, tel que d'après le lemme d'Hurwitz $|\frac{p}{q}-\alpha|\le\frac{1}{q^2\sqrt{5}}<\epsilon'$ de sorte que $|\frac{p}{q}-\beta|\le\delta+\epsilon$ et donc $|ap^2+bpq+cq^2|=|q^2P(p/q)|\le(\sqrt{\Delta}+a\epsilon')/\sqrt{5}\le\sqrt{\Delta/5}+\epsilon$ avec $\epsilon=a\epsilon'/\sqrt{5}$.

(b) Prenons $\sqrt{\Delta/5}(X^2-XY-Y^2)$ qui est de discriminant $\sqrt{\Delta}$; avec les notations précédentes $\alpha=\Phi$ le nombre d'or et $\beta=-\Phi^{-1}$. Soit F_n la suite de Fibonacci définie par récurrence par $F_0=0$, $F_1=1$ et $F_n=F_{n-1}+F_{n-2}$ de sorte que $F_n^2-F_nF_{n-1}-F_{n-1}^2=(-1)^{n-1}$ et donc le minimum de ce polynôme est $\sqrt{\Delta/5}$.

(c) On considère $\sqrt{\Delta/8}(X^2-2XY-Y^2)$ dont le discriminant est $\sqrt{\Delta}$. On considère la suite G_n définie par récurrence $G_0=0$, $G_1=1$ et $G_n=2G_{n-1}+G_{n-2}$. Par récurrence on a $G_n^2-2G_nG_{n-1}-G_{n-1}^2=(-1)^{n-1}$. de sorte que le minimum est $\sqrt{\Delta/8}$.

(d) Le polynôme $\sqrt{\Delta/4}(X^2-2XY+Y^2)$ convient.

1.3 a) On écrit $x^3-2y^3=y^3(\frac{x}{y}-\sqrt[3]{2})(\frac{x}{y}-j\sqrt[3]{2})(\frac{x}{y}-j^2\sqrt[3]{2})$ avec pour $\frac{x}{y}$ réel, $|\frac{x}{y}-j\sqrt[3]{2}|\ge\frac{\sqrt[3]{2}}{2}$ et donc

$$|x^3-2y^3|\ge\frac{\sqrt[3]{4}}{4}|\frac{x}{y}-\sqrt[3]{2}|$$

de sorte que (i) implique (ii) avec $c_1=c_2\frac{4}{\sqrt[3]{4}}$. Réciproquement si $|\frac{x}{y}-\sqrt[3]{2}|\le 1$ alors $|\frac{x}{y}-j\sqrt[3]{2}|\le|\sqrt[3]{2}+1-j\sqrt[3]{2}|=c_0$ et

$$|x^3-2y^3|\le y^3|\frac{x}{y}-\sqrt[3]{2}|c_0^2$$

de sorte que (ii) implique (i) avec $c_1=\min(1,c_2/c_0^2)$.

b) D'après Hurwitz, il existe une infinité de p/q tel que $|\sqrt[3]{2}-\frac{x}{y}|\le\frac{1}{y^2\sqrt{5}}$ ce qui en raisonnant comme dans a) donne le résultat.

2.4 Comme d'habitude, l'argument final proviendra du fait élémentaire suivant : toute suite d'entiers relatifs qui converge vers 0 est nulle à partir d'un certain rang. Dans cet exercice le schéma de la preuve est le suivant : soit à montrer qu'une série convergente $\sum_{n=0}^\infty u_n$ est irrationnel. On raisonne par l'absurde et on écrit pour une suite $k(N)$ d'entiers strictement croissante

$$\frac{p}{q}-\sum_{n=0}^{k(N)}u_n=\sum_{n>k(N)}u_n\tag{1}$$

égalité que l'on multiplie par un entier a_N tel que

(a) $a_N p/q \in \mathbb{Z}$;
(b) $a_N u_n \in \mathbb{Z}$ pour tout $n = 0, \cdots, k(N)$;
(c) $(a_N \sum_{n>k(N)} u_n)_N$ est une suite $(r_N)_N$ de réels non nuls telle qu'il existe N_0 tel que pour tout $N \geq N_0$, $|r_N| < 1$.

La contradiction découle alors du fait que le membre de gauche de (1) est une suite d'entiers qui, au vu du membre de droite, à partir d'un certain rang et non nulle et de valeur absolue strictement plus petite que 1 ce qui est impossible.

Remarque : afin d'assurer la dernière condition de (c), on pourra se ramener à une suite convergeant vers 0. En ce qui concerne la condition (a), il suffit de multiplier a_N par q ce qui ne modifie pas les conditions (b) et (c).

(1) La suite considérée est $u_n = \frac{1}{n!}$. On prend $k(N) = N$ et $a_N = N!$; les conditions (a) et (b) sont évidentes. En ce qui concerne (c), la non nullité découle du fait que l'on a une série à termes strictement positifs ; la majoration suivante

$$r_N = (N+1)^{-1} + (N+1)^{-1}(N+2)^{-1} + \cdots \leq \sum_{i=1}^{+\infty} (N+1)^{-i} = 1/N$$

montre la convergence de r_N vers 0 d'où le résultat.

(2) Si e est solution d'une équation de degré 2 alors il existe $a, b, c \in \mathbb{Z}$ tels que $ae + \frac{b}{e} = c$; quitte à multiplier cette équation par -1, on suppose $a > 0$. La suite considérée est alors $u_n = \frac{a+(-1)^n b}{n!}$ avec $p = c$ et $q = 1$. Si b est négatif (resp. positif), on prend $k(N) = 2N$ (resp. $k(N) = 2N+1$) avec $a_N = k(N)!$. Les conditions (a) et (b) sont évidentes ; la non nullité de r_N découle du fait que comme la suite $\frac{(-1)^n}{n!}$ vérifie le critère des séries alternée, $\sum_{n>k(N)} b\frac{(-1)^n}{n!}$ est du signe de $b(-1)^n$ est donc strictement positif. En ce qui concerne la convergence vers 0, le résultat découle de la majoration $|\frac{a+(-1)^n b}{n!}| \leq \frac{|a|+|b|}{n!}$ et on conclut comme dans (1).

(3) On a

$$\frac{e^{\sqrt{2}} + e^{-\sqrt{2}}}{2} = \sum_{n=0}^{\infty} \frac{2^n}{(2n)!}$$

ce qui nous amène à considérer $u_n = \frac{2^n}{(2n)!}$. On pose $k(N) = N$ et $a_N = q\frac{(2N)!}{2^N}$. La condition (a) est claire tandis que pour (b) cela découle de l'égalité pour tout $0 \leq m \leq N$,

$$\frac{(2N)!}{2^{N-m}(2m)!} = \frac{N!}{m!}(2m+1)\cdots(2N-1) \in \mathbb{N}.$$

En ce qui concerne (c), la non nullité découle du fait que la série est à termes positifs et la convergence vers 0 découle de la majoration grossière $\frac{2^k(2N)!}{(2n+2k)!} \leq (N+1)^k$ et du fait que $\sum_{k=1}^{\infty}(N+1)^{-k} = 1/N$.

(4) Il suffit de montrer comme dans (c) qu'une égalité de la forme $ae^2 + be^{-2} = c$ avec $a, b, c \in \mathbb{Z}$ est impossible. A l'image de (2), on considère $u_n = \frac{a+(-1)^n}{n!}2^n$. On suppose $a > 0$ et on pose pour $b < 0$ (resp. $b > 0$) $k(N) = 2^N$ (resp. $k(N) = 2^n + 1$). On rappelle que la valuation 2-adique de $n!$ est égale à

$$v_2(n!) = \lfloor \frac{n}{2} \rfloor + \lfloor \frac{n}{2^2} \rfloor + \lfloor \frac{n}{2^3} \rfloor \cdots < n$$

de sorte que pour $n = 2^i$ (resp. $n = 2^i + 1$), on a $v_2(n!) = n-1$ (resp. $v_2(n!) = n-2$). On pose alors $\frac{2^n}{n!} = \frac{2^{\alpha_n}}{p_n}$ avec donc $\alpha_n > 0$ égal à 1 (resp. 2) si $n = 2^i$ (resp. $n = 2^i + 1$) ; notons par ailleurs que si $n > m$ alors $p_m | p_n$. On pose alors $a_N = 2^i \frac{k(N)!}{2^{k(N)}}$ avec $i = 0$ (resp. $i = 1$) si $b < 0$ (resp. $b > 0$). La condition (a) est clairement vérifiée tandis que (b) découle du fait que $2^i \frac{k(N)!}{2^{k(N)}} \frac{2^n}{n!} \in \mathbb{Z}$ d'après la discussion précédente. La non nullité dans (c) découle du théorème des séries alternées qui nous dit que $b\sum_{n>k(N)} \frac{(-2)^n}{n!}$ est du signe de $b(-1)^{k(N)}$ et donc strictement positif, cf. (2). En ce qui concerne la convergence vers 0 elle découle de la majoration grossière $\frac{2^r}{(k(N)+1)\cdots(k(N)+r)} \leq (\frac{k(N)}{2})^{-r}$ avec $\sum_{r\geq 1}(\frac{k(N)}{2})^{-r} = (k(N)/2 - 1)^{-1}$ qui tend bien vers 0 quand N tend vers l'infini.

(5) Comme dans (3), on montre l'irrationnalité de

$$\frac{e^{\sqrt{3}} + e^{-\sqrt{3}}}{2} = \sum_{n=0}^{\infty} \frac{3^n}{(2n)!}$$

ce qui nous amène à considérer $u_n = \frac{3^n}{(2n)!}$. Contrairement à ce qui se passait dans (3), $\frac{(2N)!}{3^N}\frac{3^m}{(2m)!}$ pour $m < N$ n'est pas forcément entier ; évidemment pour tout $p \neq 3$, la valuation p-adique de ce rationnel est positive, mais pour $p = 3$ il est possible quelle soit négative. L'idée est donc de rendre la valuation 3-adique de $(2N)!$ maximale et donc de prendre $k(N) = 3^N$. En effet comme dans (4), on a :

$$v_3((2n)!) = \lfloor\frac{2n}{3}\rfloor + \lfloor\frac{2n}{3^2}\rfloor + \lfloor\frac{2n}{3^3}\rfloor \cdots < n,$$

et pour $n = 3^N$, on obtient $v_3((23^N)!) = 3^N - 1 = k(N) - 1$. On écrit alors pour tout n, $\frac{3^n}{(2n)!}$ sous la forme $\frac{3^{\alpha_n}}{p_n}$ avec $3 \wedge p_n = 1$ et $\alpha_n > 0$; par ailleurs on a $p_m | p_n$ pour tout $m < n$. Ainsi pour $a_N = q\frac{(23^N)!}{3^{3^N}}$, les conditions (a) et (b) sont clairement vérifiées. En ce qui concerne (c), la non nullité découle de la positivité des u_n et en ce qui concerne la convergence elle découle de la majoration grossière

$$\frac{3^k}{(2n+1)(2n+2)\cdots(2n+2k-1)(2n+2k)} \leq \frac{1}{n^{2k}}.$$

(6) L'implication (i) ⇒ (ii) et (iii) est évidente tandis que (ii) ⇒ (i) découle comme dans (1) du procédé général pour $u_n = b_n/n!$ avec $k(N) = N$ et $a_N = N!$.

L'implication (iii) ⇒ se montre selon le même procédé : pour $u_n = b_n 2^n/n!$ on pose $k(N) = 2^N$ avec $a_N = qk(N)!/2^{k(N)}$. La condition (a) est claire tandis que (b) se prouve comme dans (4), en remarquant que $\frac{k(N)!}{2^{k(N)}}\frac{2^n}{n!} \in \mathbb{Z}$. La condition de non nullité dans (c) découle du fait que la série est à termes positifs tandis que la convergence vers 0 se prouve comme dans (4).

2.5 (a) $f_n^{(m)}(0) = 0$ pour $m < n$ et $m > 2n$. En écrivant $x^n(1-x)^n = \sum_k c_k x^k$, on a $f^{(m)}(0) = \frac{m!}{n!}c_m$ pour $m \geq n$.

(b) En remarquant que $f_n(1-x) = f_n(x)$ on a le même résultat en 1 d'où le résultat.

(c) C'est une simple intégration par parties et la conclusion découle de la majoration de l'intégrale par $\pi a^n/n!$ dont la limite est nulle pour n tendant vers l'infini ($0 < f(x) \leq 1/n!$). Un entier plus petit que $1/2$ est nul ce qui ne se peut pas car l'intégrale n'est pas nulle pour n fixé.

3.6 (1-a) Notons tout d'abord que pour tout $f \in \mathbb{R}[X]$, $(\sum_{k\geq 0} D^k)(f)$ est une somme finie car pour tout $k > \deg f$, $D^k f = 0$ de sorte que l'opérateur $\sum_{k\geq 0} D^k$ est bien définie. Par ailleurs comme pour tout $f \in \mathbb{R}[X]$, $(\mathrm{Id} - D)(\sum_{k=0}^n D^k)f = f - D^{n+1}f$, on a bien $(\mathrm{Id} - D)(\sum_{k\geq 0} D^k) = \mathrm{Id}$.

(1-b) Bien entendu l'intérêt de la question précédente est d'exprimer une primitive de $e^{-t}g(t) = e^{-t}(f - f')$ avec $g = (\mathrm{Id} - D)f$ par $-e^{-t}f(t)$ avec $f = (\mathrm{Id} - D)^{-1}g$. La formule de Hermite s'en déduit immédiatement après le changement de variable $t = zu$.

(1-c) On a $|\mathrm{Re}\left((1-u)z\right)| \leq |z|$ et donc $|ze^{z(1-u)}g(zu)| \leq |z|e^{|z|}\sum_{u\in[0,1]}|g(zu)|$, d'où le résultat.

(1-d) Par linéarité, il suffit de considérer le cas de $f = X^m$; $f^{(m)} = m(m-1)\cdots(m-n+1)X^{m-n}$. Si $m < n$ alors $f^{(m)}$ est le polynôme nul et pour $m \geq n$, il suffit de poser $f_n := \binom{m}{n}X^{m-n}$.

(2-a) On écrit $I(g_p; i) = e^i \sum_{k\geq p-1}\frac{k!}{(p-1)!}h_k(0) - \sum_{k\geq p}\frac{k!}{(p-1)!}h_k(i)$, où h_k est le polynôme à coefficients entiers construit à la question précédente à partir du polynôme $x^{p-1}f(x)^p$. On pose alors $b_p = \sum_{k\geq p-1}\frac{k!}{(p-1)!}h_k(0) \in \mathbb{Z}$ et $a_{p,i} := \sum_{k\geq p}\frac{k!}{(p-1)!}h_k(i) \in \mathbb{Z}$ avec en outre $a_{p,i} \equiv 0 \mod p$ et $b_p \equiv f(0)^p = (-1)^n n!$.

En outre d'après (1-c), on a $I(g_p; i) \leq e^i\frac{c_i^p}{(p-1)!}$ où $c_i = \sup_{u\in[0,i]}|f(u)|$ de sorte que $I(g_p; i)$ tend vers 0 quand p tend vers $+\infty$.

(2-b-i) On a $J_p = b_p(a_0 + a_1 e + \cdots + a_n e^n) - \sum_{i=1}^n b_{p,i}a_i = -\sum_{i=0}^n a_{p,i}a_i \in \mathbb{Z}$; où on a posé $a_{p,0} = b_p$.

(2-b-ii) D'après (2-a), chacun des $I(g_p; i)$ tend vers 0 quand $p \to +\infty$ et donc comme n est fixé, J_p aussi.

(2-b-iii) soit $p > n$ premier de sore que $a_{p,0} \not\equiv 0 \mod p$ alors que pour tout $i = 1, \cdots, n$, $a_{p,i} \equiv 0 \mod p$ et donc $J_p \not\equiv 0 \mod p$.

(2-c) D'après 2-b, pour p premier assez grand, J_p est un entier qui tend vers 0 et dont la congruence modulo p est non nulle ce qui est absurde.

(3-a) On peut évoquer le théorème sur les polynômes symétriques : le polynôme symétrique $\sum_{f(\alpha)=0}\alpha^n$ est un polynôme $Q(\sigma_1, \cdots, \sigma_m)$ où les σ_i sont les polynômes symétriques élémentaires des racines de f, i.e. $f(X) = aX^m - a\sigma_1 X^{m-1} + \cdots + (-1)^m a\sigma_m$. En outre le degré de Q est égal au degré partiel de $\sum_{f(\alpha)=0}\alpha^n$ c'est à dire

n (et de poids le degré total soit ici encore n). Comme pour tout $1 \leq i \leq m$, $a\sigma_i \in \mathbb{Z}$, on en déduit alors que $a^n Q(\sigma_1, \cdots, \sigma_m) \in \mathbb{Z}$, d'où le résultat.
Remarque : une autre technique consiste à considérer la matrice compagnon A 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.

(3-b) 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 $n \geq p$, $g^{(n)}(0)$ est divisible par $p!$ alors que

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

Ainsi, il existe des entiers Q, R tels que

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

Si N est un entier alors le second membre de cette égalité est entier qui, si p est un premier $> aNf(0)$, 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 1-c 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.

(3-c-i) Cela découle directement du fait que $e^{i\pi} = -1$.

(3-b-ii) 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.

(3-b-iii) Soit un entier M tel que $MP_0 \in \mathbb{Z}[X]$ et soit $q \geq 1$ la multiplicité de la racine 0 dans P_0. On pose $P := MF_0/X^q$: 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 3-b.

3.7 i) 2 est algébrique et $\sqrt{2}$ (resp. i) est algébrique irrationnel de sorte que $2^{\sqrt{2}}$ (resp. 2^i) est transcendant.

ii) On écrit e^{π} sous la forme $e^{-i \log e^{i\pi}}$ avec $e^{i\pi} = -1$ algébrique et $-i$ algébrique non rationnel ; même argument pour $e^{\pi\sqrt{2}}$.

iii) Si $\cos(\pi\sqrt{2})$ était algébrique alors $i \sin(\pi\sqrt{2})$ aussi et donc aussi $e^{i\pi\sqrt{2}}$ ce qui n'est pas en raisonnant comme dans ii).

iv) Si $\log 3/\log 2$ était rationnel de la forme p/q alors $3^q = 2^p$ ce qui n'est pas et donc comme 3 et 2 sont algébriques, $\log 3/\log 2$ est transcendant.

v) Même raisonnement que dans iv) en écrivant $i\pi = log(e^{i\pi})$.

3.8 En utilisant tout d'abord le théorème de Gel'fond-Schneider :
- $a = 2$ et $b = \sqrt{2}$ donne a et b algébriques et a^b transcendant ;
- $a = 1$ et $b = \log 3/\log 2$ donne a et $a^b = 3$ algébriques et b transcendant ;
- $a = e^\pi$ et $b = i$ donne b et $a^b = -1$ algébriques et a transcendant ;

En utilisant Hermite Lindeman :
- $a = 1$ et $b = 1/\log 2$ donne a algébrique avec b et $a^b = 2$ transcendants ;
- $a = e$ et $b = \log 2$ donne a et b transcendants avec $a^b = 2$ algébrique ;
- $a = e$ et $b = \pi$ donne (en utilisant aussi Gel'fond-Schneider) a, b et $a^b = e^\pi$ transcendants ;
- $a = e$ et $b = \sqrt{2}$ donne a et a^b transcendants avec b algébrique.

4.9 Il est clair que, si $b/a = x^2$ est un carré dans K, on a $\sqrt{b} = \pm x\sqrt{a}$ et $K(\sqrt{a}) = K(\sqrt{b})$. Réciproquement, si ces deux corps sont égaux et différents de K, on peut écrire par exemple $\sqrt{b} = x + y\sqrt{a}$ avec x et y dans K. On en déduit $(b - x^2 - ay^2)^2 = 4x^2y^2a$. Comme a n'est pas un carré dans K, cela implique $2xy = 0$ et $b = x^2 + ay^2$. Comme b n'est pas un carré et la caractéristique n'est pas 2, $2y \neq 0$. On en déduit que $x = 0$ et $b/a = y^2$ est un carré dans K. Reste le cas $K(\sqrt{a}) = K(\sqrt{b}) = K$ pour lequel b et a sont des carrés, et leur quotient aussi.

4.10 Comme $-1/2$ n'est pas un carré dans $\mathbb{Q}$, l'exercice précédent montre que $\mathbb{Q}(i)$ et $\mathbb{Q}(\sqrt{2})$ sont deux extensions quadratiques distinctes de $\mathbb{Q}$. Le composé $L = \mathbb{Q}(i, \sqrt{2})$ est donc une extension galoisienne de degré 4 de $\mathbb{Q}$. On peut décrire l'action du groupe de Galois $\mathrm{Gal}(L/\mathbb{Q}) = \{Id, \tau_1, \tau_2, \tau_3\}$ sur i et $\sqrt{2}$:

$$\tau_1(i) = -i,\ \tau_1(\sqrt{2}) = \sqrt{2},\ \tau_2(i) = i,\ \tau_2(\sqrt{2}) = -\sqrt{2},\ \tau_3(i) = -i,\ \tau_3(\sqrt{2}) = -\sqrt{2}.$$

Seul Id laisse fixe l'élément $\alpha = i + \sqrt{2}$ de L. On en déduit que le corps engendré par α est L tout entier, c'est-à-dire $L = K$.

4.11 Comme 5 n'est pas un carré dans $\mathbb{Q}$, $L/\mathbb{Q}$ est une extension quadratique. Montrons que $2 + \sqrt{5}$ n'est pas un carré dans L : en effet, si $(x + y\sqrt{5})^2 = 2 + \sqrt{5}$, son conjugué vérifie $(x - y\sqrt{5})^2 = 2 - \sqrt{5}$ et en faisant le produit, on obtient

$$(x^2 - 5y^2)^2 = 4 - 5 = -1$$

mais -1 n'est pas un carré dans $\mathbb{Q}$, une contradiction. L'extension M/L est donc quadratique, et $[M : \mathbb{Q}] = [M : L][L : \mathbb{Q}] = 4$.. Le générateur $\alpha = \sqrt{2 + \sqrt{5}}$ de M sur $\mathbb{Q}$ vérifie $(\alpha^2 - 2)^2 = 5$, son polynôme minimal sur $\mathbb{Q}$ est donc $(X^2 - 2)^2 - 5 = X^4 - 4X^2 - 1$. Les deux racines imaginaires de ce polynôme ne peuvent appartenir à M qui est inclus dans $\mathbb{R}$. On en déduit que l'extension $M/\mathbb{Q}$ n'est pas galoisienne. D'autre part, une extension quadratique est toujours galoisienne, c'est donc le cas de M/L et $L/\mathbb{Q}$. Le polynôme minimal de α sur L est simplement $X^2 - 2 - \sqrt{5}$.

4.12 (i) Le discriminant $\Delta = a^2 - 4b$ ne doit pas être un carré, sinon le polynôme serait réductible. Le corps quadratique $\mathbb{Q}(\sqrt{\Delta})$ contient alors $(-a + \sqrt{\Delta})/2$ et $(-a - \sqrt{\Delta})/2$, dont les racines carrées sont les racines de $X^4 + aX^2 + b$. Ces racines engendrent des extensions quadratiques de $\mathbb{Q}(\sqrt{\Delta})$ qui coïncident si et seulement si le quotient

$$\frac{-a - \sqrt{\Delta}}{-a + \sqrt{\Delta}} = \frac{a^2 - \Delta}{(-a + \sqrt{\Delta})^2} = b\left(\frac{2}{-a + \sqrt{\Delta}}\right)^2$$

est un carré dans $\mathbb{Q}(\sqrt{\Delta})$, ce qui équivaut à dire que b lui-même est un carré dans $\mathbb{Q}(\sqrt{\Delta})$. L'équation $b = (x + y\sqrt{\Delta})^2$ implique que x ou y est nul, et b est un carré ou Δ fois un carré dans $\mathbb{Q}$.

Ainsi $X^4 + aX^2 + b$ est réductible si et seulement si $(-a + \sqrt{\Delta})/2$ est un carré dans $\mathbb{Q}(\sqrt{\Delta})$. Dans le cas contraire le corps de rupture associé est galoisien si et seulement si b eou Δb est un carré dans $\mathbb{Q}$.

(ii) Ainsi si δ est positif sans être un carré dans $\mathbb{Q}$ et si b est négatif alors ni b ni Δb ne sont des carrés dans $\mathbb{Q}$ de sorte que $X^4 + aX^2 + b$ est irréductible mais son corps de rupture n'est pas galoisien.

(iii) Par exemple, pour $b = 1$ et $a = -1$: le polynôme $X^4 - X^2 + 1$ est irréductible et son corps de rupture est galoisien sur $\mathbb{Q}$.

4.13 Le corps L est le corps de décomposition de X^3-2. Comme X^3-2 est irréductible, K est de degré 3. Les autres racines ne sont pas réelles : le polynôme $X^2+\sqrt[3]{2}X+\sqrt[3]{4}$ est donc irréductible sur K et ses racines engendrent une extension quadratique $L=K(j)$ de K, et $[L:\mathbb{Q}]=6$. Le groupe de Galois est un sous-groupe du groupe des permutations des trois racines : c'est $\mathcal{S}_3$ tout entier. Ce groupe a 6 sous-groupes : les deux sous-groupes triviaux, correspondant aux corps $\mathbb{Q}$ et L, les trois sous-groupes d'ordre 2 correspondant aux trois corps cubiques $K=\mathbb{Q}(\sqrt[3]{2})$, $K'=\mathbb{Q}(\rho\sqrt[3]{2})$ et $K''=\mathbb{Q}(\rho^2\sqrt[3]{2})$, enfin le groupe alterné, d'ordre 3, correspond au corps quadratique $\mathbb{Q}(\rho)=\mathbb{Q}(\sqrt{-3})$.

4.14 Notons $L=K(\alpha)$ et $M=K(\alpha,\beta,\gamma)$, où α, β et γ sont les racines de X^3+pK+q. Le corps de rupture $L=K(\alpha)$ est séparable sur K puisque la caractéristique ne divise pas le degré. Sa clôture galoisienne est M. Posons

$$\delta=(\alpha-\beta)(\alpha-\gamma)(\beta-\gamma).$$

On a $\delta^2=\Delta=-(4p^3+27q^2)\in K$. Si $M=L$, δ appartient à L et son degré sur K est inférieur ou égal à 2 : il appartient en fait à K et Δ est un carré dans K. Au contraire, si $M\neq L$, il existe un automorphisme non trivial σ de M sur K. Cet automorphisme doit laisser fixe α et échanger β et γ, on a donc

$$\sigma(\delta)=(\sigma(\alpha)-\sigma(\beta))(\sigma(\alpha)-\sigma(\gamma))(\sigma(\beta)-\sigma(\gamma))=(\alpha-\gamma)(\alpha-\beta)(\gamma-\beta)=-\delta.$$

Comme la caractéristique est différente de 2, on a $\sigma(\delta)=-\delta\neq\delta$, et δ n'est pas dans K, c'est-à-dire que Δ n'est pas un carré dans K.

4.15 On note $\zeta=e^{\frac{2i\pi}{5}}$ et $\alpha=\sqrt[5]{2}$ dont les polynômes minimaux sont respectivement $\Phi_5(X)=X^4+X^3+X^2+X+1$ et X^5-2. Le corps de décomposition de X^5-2 est $L=\mathbb{Q}[\zeta,\alpha]$ qui contient entr'autre les corps $\mathbb{Q}[\zeta]$ et $\mathbb{Q}[\alpha]$ qui sont respectivement de degré 4 et 5 sur $\mathbb{Q}$. On en déduit alors que $[L:\mathbb{Q}]$ est divisible par 5 et 4 et donc par 20. Par ailleurs ζ est au plus de degré 4 sur $\mathbb{Q}[\alpha]$ de sorte que $[L:\mathbb{Q}]\leq 20$. Ainsi d'après le théorème de Galois, G est de cardinal 20.

Pour tout $\sigma\in G$, on a $\sigma(\alpha)\in\{\alpha,\zeta\alpha,\zeta^2\alpha,\zeta^3\alpha,\zeta^4\alpha\}$ et $\sigma(\zeta)\in\{\zeta,\zeta^2,\zeta^3,\zeta^4\}$. Comme G est de cardinal 20, alors pour tout $0\leq k\leq 4$ et $1\leq l\leq 4$, il existe $\sigma\in G$ tel que $\sigma(\alpha)=\alpha\zeta^k$, $\sigma(\zeta)=\zeta^l$.

Soit alors σ (resp. τ) tel que $\sigma(\alpha)=\alpha\zeta$ (resp. $\tau(\alpha)=\alpha$) et $\sigma(\zeta)=\zeta$ (resp. $\tau(\zeta)=\zeta^2$) de sorte que σ est d'ordre 5 (resp. d'ordre 4) et que tout élément de G s'écrit de manière unique sous la forme $\sigma^k\tau^l$ avec $0\leq k\leq 4$ et $0\leq l\leq 3$.

Clairement G n'est pas abélien car $\mathbb{Q}[\alpha]/\mathbb{Q}$ n'est pas galoisien. Par contre il est résoluble car tout groupe de cardinal 20 l'est (le plus petit groupe non résoluble est $\mathcal{A}_5$).
Remarque : En fait $G\simeq\mathbb{Z}/5\mathbb{Z}\ltimes_\psi\mathbb{Z}/4\mathbb{Z}$ où $\psi:\mathbb{Z}/4\mathbb{Z}\to(\mathbb{Z}/5\mathbb{Z})^\times$ avec $\psi(1)$ est la multiplication par 2. On peut déterminer tous les sous-groupes de G et donc toutes les sous-extensions de L, on obtient alors

sous-groupe	corps intermédiaires	degré sur $\mathbb{Q}$
$\{1\}$	$\mathbb{Q}[\zeta,\alpha]$	20
$\{1,\tau^2\}$	$\mathbb{Q}[\alpha,\zeta^2+\zeta^3]$	10
$\{1,\sigma\tau^2\sigma^{-1}\}$	$\mathbb{Q}[\zeta\alpha,\zeta^2+\zeta^3]$	10
$\{1,\sigma^2\tau^2\sigma^{-2}\}$	$\mathbb{Q}[\zeta^2\alpha,\zeta^2+\zeta^3]$	10
$\{1,\sigma^3\tau^2\sigma^{-3}\}$	$\mathbb{Q}[\zeta^3\alpha,\zeta^2+\zeta^3]$	10
$\{1,\sigma^4\tau^2\sigma^{-4}\}$	$\mathbb{Q}[\zeta^4\alpha,\zeta^2+\zeta^3]$	10
$<\tau>$	$\mathbb{Q}[\alpha]$	5
$<\sigma\tau\sigma^{-1}>$	$\mathbb{Q}[\zeta\alpha]$	5
$<\sigma^2\tau\sigma^{-2}>$	$\mathbb{Q}[\zeta^2\alpha]$	5
$<\sigma^3\tau\sigma^{-3}>$	$\mathbb{Q}[\zeta^3\alpha]$	5
$<\sigma^4\tau\sigma^{-4}>$	$\mathbb{Q}[\zeta^4\alpha]$	5
$<\sigma>$	$\mathbb{Q}[\zeta]$	4
$<\sigma,\tau^2>$	$\mathbb{Q}[\zeta^2+\zeta^3]$	2
G	$\mathbb{Q}$	1

4.16 Si E_1 et E_2 sont deux extensions galoisiennes de F alors E_1E_2 et $E_1 \cap E_2$ sont galoisiennes sur F et on a la suite exacte suivante

$$\mathrm{Gal}(E_1E_2/F) \hookrightarrow \mathrm{Gal}(E_1/F) \times \mathrm{Gal}(E_2/F) \twoheadrightarrow \mathrm{Gal}(E_1 \cap E_2/F)$$

où la dernière flèche n'est un morphisme que si $\mathrm{Gal}(E_1 \cap E_2/F)$ est abélien et où l'image de la première est exactement les éléments du groupe produit qui s'envoie sur l'élément neutre de $\mathrm{Gal}(E_1 \cap E_2/F)$. Ici on a $E_1 \cap E_2 = \mathbb{Q}[j]$ où j est une racine cubique primitive de l'unité de sorte que le degré cherché est 18. On vérifie alors que $\mathrm{Gal}(E_1E_2/F)$ s'identifie aux éléments $\mathrm{d}(\sigma_1, \sigma_2) \in \mathfrak{S}_3 \times \mathfrak{S}_3$ tels que $\epsilon(\sigma_1) = \epsilon(\sigma_2)$ où ϵ désigne la signature.

4.17 Soit L le corps de décomposition de $X^6 - 5$: $L = \mathbb{Q}[\zeta, \alpha]$ avec $\alpha^6 = 5$, $\alpha \in \mathbb{R}$ et ζ est une racine primitive 3-ième de l'unité de sorte que $-\zeta$ est une racine primitive 6-ième de l'unité. Le degré $[L : \mathbb{Q}]$ est donc égal à 12 et $G \simeq D_6$ engendré par (26)(35) et (123456). Sur $\mathbb{R}$ le groupe de galois est $\mathbb{Z}/2\mathbb{Z}$.

4.18 Comme 3/7 n'est pas un carré dans $\mathbb{Q}$, on en déduit $\mathbb{Q}[\sqrt{3}] \cap \mathbb{Q}[\sqrt{7}] = \mathbb{Q}$ et donc que $[\mathbb{Q}[\sqrt{3}, \sqrt{7}] : \mathbb{Q}] = 4$ avec pour base $1, \sqrt{3}, \sqrt{7}, \sqrt{21}$. Le groupe de Galois est isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ avec $(i,j)(\sqrt{3}) = (-1)^i\sqrt{3}$ et $(i,j)(\sqrt{7}) = (-1)^j\sqrt{7}$. En particulier on remarque que $x = \sqrt{3} + \sqrt{7}$ possède 4 conjugués distincts deux à deux (utilisez que la famille $\sqrt{3}$ et $\sqrt{7}$ est libre sur $\mathbb{Q}$). On peut par ailleurs trouver son polynôme minimal en procédant selon le principe général suivant : soit A et B deux polynômes irréductibles unitaires sur $\mathbb{Q}$. Le système en d'équations $A(X) = B(Y - X) = 0$ possède comme solutions les couples $(x_a, x_b + x_a)$ où x_a (resp. x_b) décrit les solutions de $A(X) = 0$ (resp. $B(X) = 0$). On considère alors les polynômes $A(X)$ et $B(Y - X)$ comme des polynômes à valeurs dans $K[Y]$ et on introduit leur résultant qui est un polynôme en Y dont les zéros sont d'après ce qui précède, exactement les sommes des zéros de A avec ceux de B.

Dans notre cas on a $A(X) = X^2 - 3$ et $B(X) = X^2 - 7$. Le résultant en question est donné par le déterminant

$$\begin{vmatrix} 1 & 0 & -3 & 0 \\ 0 & 1 & 0 & -3 \\ 1 & -2Y & Y^2 - 7 & 0 \\ 0 & 1 & -2Y & Y^2 - 7 \end{vmatrix}$$

soit après calcul $Y^4 - 20y^2 + 16$

4.19 Le corps de décomposition de $X^4 - 2$ est $E_1 = \mathbb{Q}[i, \alpha]$ avec $\alpha^4 = 2$ qui est de degré 8 sur $\mathbb{Q}$ et de groupe de Galois D_4. Le corps de décomposition de $X^3 - 5$ est $E_2 = \mathbb{Q}[j, \beta]$ qui est de degré 6 et de groupe de Galois $\mathfrak{S}_3$ sur $\mathbb{Q}$. Comme les extensions $E_i/\mathbb{Q}$ sont galoisiennes le degré de $[E_1E_2 : \mathbb{Q}] = [E_1 : \mathbb{Q}].[E_2 : \mathbb{Q}]/[E_1 \cap E_2 : \mathbb{Q}]$ et on est donc ramené à étudier $E_1 \cap E_2$ qui est donc de degré sur $\mathbb{Q}$ un diviseur de 6 et 8 et donc égal à 1 ou 2. Il faut donc étudier les extensions de degré 2 contenues dans E_1 et E_2 ce qui revient à étudier les sous-groupes d'indice 2 dans les groupes de Galois respectifs. En ce qui concerne E_2, le seul sous-groupe d'indice 2 de $\mathfrak{S}_3$ est $\mathcal{A}_3$ (utilisez que la signature est le seul morphisme non trivial de $\mathfrak{S}_3 \twoheadrightarrow \mathbb{Z}/2\mathbb{Z}$) et donc $\mathbb{Q}[j]$ est la seule extension quadratique contenue dans E_2. En ce qui concerne E_1, les sous-groupes H d'indice 2 de D_4 sont soit $D_4^+ \simeq \mathbb{Z}/4\mathbb{Z}$ correspondant aux rotations ; sinon $H \cap D_4^+$ ne peut pas être réduit à l'identité c'est donc le sous-groupe d'indice 2 de D_4^+ égal à $\pm\mathrm{Id}$ et H est alors égal à $\{\pm\mathrm{Id}, \sigma_D, \sigma_{D^\perp}\} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ où σ_D est la réflexion par rapport à la droite D (diagonale ou médiatrice du carré). Les corps correspondant sont alors $\mathbb{Q}[i]$, $\mathbb{Q}[\sqrt{2}]$ et $\mathbb{Q}[i\sqrt{2}]$. Comme $2/-3$, $2/3$ et $-1/-3$ ne sont pas dans $(\mathbb{Q}^\times)^2$, les extensions précédentes sont distinctes deux à deux et $E_1 \cap E_2 = \mathbb{Q}$. Ainsi le groupe de Galois est le groupe produit $D_4 \times D_3$.

4.20 Comme 2/5 n'est pas un carré de $\mathbb{Q}$, $\mathbb{Q}[\sqrt{2}, \sqrt{5}]/\mathbb{Q}$ est de degré 4 de groupe de Galois $\mathbb{Z}/2\mathbb{Z}/2$: les extensions quadratiques contenue dans $\mathbb{Q}[\sqrt{2}, \sqrt{5}]$ sont $\mathbb{Q}[\sqrt{2}]$, $\mathbb{Q}[\sqrt{5}]$ et $\mathbb{Q}[\sqrt{10}]$ correspondant aux trois sous-groupes d'indices 2 de $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Celles-ci sont toutes distinctes de $\mathbb{Q}[\sqrt{7}]$ de sorte que le groupe de Galois est $(\mathbb{Z}/2\mathbb{Z})^3$ donné par $\sigma_{\epsilon_1,\epsilon_2,\epsilon_3}(\alpha_i) = \epsilon_i\alpha_i$ où $\epsilon_i = \pm 1$ et $\alpha_1 = \sqrt{2}$, $\alpha_2 = \sqrt{5}$ et $\alpha_3 = \sqrt{7}$. On remarque ainsi que les images de $x = \sqrt{2} + \sqrt{5} + \sqrt{7}$ par les éléments du groupe de Galois sont toutes distinctes, ce qui prouve que x est générateur.

4.21 On a $\mathbb{Q}[\zeta] = \mathbb{Q}[\zeta', i]$ où ζ' est une racine primitive 3-ième de l'unité et $\pm i = \zeta^3$ ...

4.22 (1) Le groupe de galois est $(\mathbb{Z}/5\mathbb{Z})^\times$, cyclique de cardinal 4 engendré par $\sigma_0 := 2$; il possède donc un unique sous-groupe H d'indice 2 à savoir le groupe engendré par 2^2. Le sous-corps correspondant est donc engendré par $\sum_{\sigma\in H}\sigma(\zeta) = \zeta + \zeta^4$.

(2) On a $\sigma_0(\zeta+\zeta^4) = \zeta^2+\zeta^3$ et

$$(\zeta+\zeta^4)(\zeta^2+\zeta^3) = -1 \qquad (\zeta+\zeta^4)+(\zeta^2+\zeta^3) = -1$$

de sorte que le polynôme minimal de $\zeta+\zeta^4$ est X^2+X-1. Par ailleurs les racines de ce polynôme sont $\frac{-1\pm\sqrt{5}}{2}$ de sorte que $\mathbb{Q}[\zeta+\zeta^4] = \mathbb{Q}[\sqrt{5}]$.

(3) On a d'après (2), $\mathbb{Q}[\sqrt{5},\zeta] = \mathbb{Q}[\zeta]$.

(4) On a $\mathbb{Q}[\sqrt{5}]\cap\mathbb{Q}[i\sqrt{3}] = \mathbb{Q}$ de sorte que d'après (1), on a $\mathbb{Q}[\zeta]\cap\mathbb{Q}[i\sqrt{3}] = \mathbb{Q}$ de sorte que le groupe de Galois est le produit direct de ceux de X^2+3 et X^5-1, soit $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$.

4.23 (1) Un polynôme de degré 3 est irréductible si et seulement s'il n'a pas de racine. Il s'agit donc de montrer que tous les éléments de $\mathbb{Q}(\sqrt{-15})$ ne sont pas des cubes. Mais si $\alpha = x+y\sqrt{-15} = \theta^3$ avec $\theta\in\mathbb{Q}(\sqrt{-15}$, alors $f(\alpha) = f(\theta)^3$ et la quantité

$$x^2+15y^2 = N(\alpha) = \alpha f(\alpha) = N(\theta)^3$$

est le cube d'un rationnel. Il suffit de prendre par exemple $y=0$ et x non cube pour trouver un α qui convient. Si θ' est une autre racine, on a $(\theta'/\theta)^3 = 1$. Alors θ et θ' différent par une racine cubique de l'unité, j ou j^2.

(2) Comme L est défini comme corps de décomposition en caractéristique nulle, L/K est forcément galoisienne, et son degré est un multiple de $3 = [K(\theta)/K]$ et de $[K(j):K] = 2$ car $j\notin K$: en effet si $K = \mathbb{Q}(\sqrt{-15})$ et $\mathbb{Q}(j) = \mathbb{Q}(\sqrt{-3})$ sont deux extensions quadratiques distinctes de $\mathbb{Q}$ car $\frac{-15}{-3} = 5$ n'est pas un carré dans $\mathbb{Q}$. Donc j est quadratique sur K, donc pas dans $K(\theta)$, donc quadratique sur $K(\theta)$, et $L = K(\theta)(\rho)$ est de degré 6 sur K. Au passage, on a vu que L contenait $\frac{\sqrt{-15}}{\sqrt{-3}} = \sqrt{5}$.

(3) Le groupe de Galois du corps de décomposition est un sous-groupe du groupe des permutations des racines du polynôme. Ici le groupe est d'ordre 6, et il y a trois racines : $\mathrm{Gal}(L/K)$ s'identifie au groupe des permutations de $\{\theta, j\theta, j^2\theta\}$. Il existe en particulier σ qui envoie θ sur $j\theta$ et $j\theta$ sur $j^2\theta$. On en déduit $\sigma(j) = \sigma(\frac{j\theta}{\theta}) = \frac{j^2\theta}{j\theta} = j$, donc aussi $\sigma(\sqrt{-3}) = \sigma(1+2j) = 1+2\sigma(j) = \sqrt{-3}$. Comme on a par définition $\sigma(\sqrt{-15}) = \sqrt{-15}$, on en déduit $\sigma(\sqrt{5}) = \frac{\sigma(\sqrt{-15})}{\sigma(\sqrt{-3})} = \sqrt{5}$. De même, la permutation τ qui échange $j\theta$ et $j^2\theta$ en laissant fixe θ vérifie $\tau(j) = \frac{\tau(j\theta)}{\tau(\theta)} = j^{-1} = j^2$, donc $\tau(\sqrt{-3}) = -\sqrt{-3}$ et $\tau(\sqrt{5}) = \frac{\tau(\sqrt{-15})}{\tau(\sqrt{-3})} = -\sqrt{5}$.

(4) La permutation σ est circulaire, elle est d'ordre 3. De même, τ est une transposition, d'ordre 2. On voit que $\tau\sigma\tau^{-1}$ permute les trois racines circulairement, dans l'autre sens : $\tau\sigma\tau^{-1} = \sigma^{-1} = \sigma^2$. On peut écrire

$$\mathrm{Gal}(L/K) = \{Id, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau\}.$$

Ce groupe a 4 sous-groupes non triviaux, $\{Id,\sigma,\sigma^2\}$ est d'ordre 3 et a pour corps fixe $K(\sqrt{5})$, et les trois groupes d'ordre 2 $\{Id,\tau\}$, $\{Id,\sigma\tau\}$ et $\{Id,\sigma^2\tau\}$ ont pour corps fixes respectifs $K(\theta)$, $K(\rho^2\theta)$ et $K(\rho\theta)$, ce qui complète, avec K et L, la liste des corps intermédiaires entre K et L.

(5) On a $t = \alpha+f(\alpha)\in\mathbb{Q}$ et $N_{K/\mathbb{Q}}(\alpha) = \alpha\overline{\alpha} = b^3\in\mathbb{Q}$. On en déduit que θ est racine du polynôme à coefficients rationnels

$$P(X) = (X^3-\alpha)(X^3-f(\alpha)) = X^6 - tX^3 + b^3.$$

Sur K, ce polynôme se décompose en deux facteurs dont on sait qu'ils sont irréductibles (b^3/α n'est pas plus un cube que α dans K). Toute factorisation de P sur $\mathbb{Q}$ serait encore valable sur K, or les facteurs ont des coefficients qui ne sont pas dans $\mathbb{Q}$ (en effet, si α appartenait à $\mathbb{Q}$, α^2 serait un cube et donc α aussi (dans le groupe $\mathbb{Q}^\times/(\mathbb{Q}^\times)^3$) tous les éléments non triviaux sont d'ordre 3), ce qui contredit le fait que $X^3-\alpha$ est irréductible sur K) ; on en déduit que P est irréductible sur $\mathbb{Q}$.

Les racines du polynôme P sont

$$\{\theta, j\theta, j^2\theta, b/\theta, jb/\theta, j^2b/\theta\}$$

et appartiennent toutes à L. D'autre part, le corps de décomposition de P sur $\mathbb{Q}$ contient θ, donc α, donc K, donc $L = K(\theta, j\theta)$. On vient de prouver que c'est L, qui est donc une extension galoisienne de degré 12 de $\mathbb{Q}$. $\mathrm{Gal}(L/K)$ est un sous-groupe (distingué) d'indice 2 de $\mathrm{Gal}(L/\mathbb{Q})$.

Soit ψ un élément quelconque de $\mathrm{Gal}(L/\mathbb{Q})$ qui n'est pas dans $\mathrm{Gal}(L/K)$. Par construction, la restriction de ψ à K n'est pas l'identité, c'est donc f. On en déduit que ψ échange les deux facteurs de P sur K, et donc l'image $\gamma = \psi(b/\theta)$ de b/θ par ψ est θ, $j\theta$ ou $j^2\theta$. Choisissons un élément κ de $\mathrm{Gal}(L/K)$ tel que $\kappa(\theta) = \gamma$. Si l'image de $\sqrt{5}$ par $\psi^{-1}\kappa$ est $\sqrt{5}$, $\phi = \psi^{-1}\kappa$ présente les propriétés requises. Sinon, $\phi = \tau\psi^{-1}\kappa$ convient.

On a $\phi^2(\theta) = \phi(b/\theta) = b/\phi(\theta) = \theta$. Donc ϕ^2 est un élément de $\mathrm{Gal}(L/K)$ qui laisse fixe $\sqrt{5}$ et θ : c'est l'identité. On a encore $\phi(\sqrt{-15}) = f(\sqrt{-15}) = -\sqrt{-15}$, donc $\phi(\sqrt{-3}) = \frac{\phi(\sqrt{-15})}{\phi(\sqrt{5})} = -\sqrt{-3}$, d'où $\phi(j) = j^2$. On en déduit que

$$\phi\sigma\phi^{-1}(\theta) = \phi\sigma(\frac{b}{\theta}) = \phi(\frac{b}{j\theta}) = \frac{\theta}{j^2} = j\theta,$$

donc $\phi\sigma\phi^{-1}$ est un élément de $\mathrm{Gal}(L/K)$ qui envoie $\sqrt{5}$ sur $\sqrt{5}$ et θ sur $j\theta$, donc $\phi\sigma\phi^{-1} = \sigma$. De même, on montre que $\phi\tau\phi^{-1} = \tau$, et ϕ commute à tous les éléments de $\mathrm{Gal}(L/K)$, et à lui-même, donc ϕ est dans le centre de $\mathrm{Gal}(L/\mathbb{Q})$: le sous-groupe $\{Id, \phi\}$ est distingué, et le corps fixe de ϕ est un sous-corps M de L galoisien sur $\mathbb{Q}$. Comme $[L : M] = 2$, M est de degré 6 sur $\mathbb{Q}$. Comme $\phi(\sqrt{5}) = \sqrt{5}$, $R = \mathbb{Q}(\sqrt{5})$ est inclus dans M qui est donc une extension de degré 3 de R.

4.24 Montrons d'abord que si a est un élément d'un corps L de caractéristique p non nulle qui n'a pas de racine p-ième dans L, le polynôme $U = T^p - a$ est irréductible sur L. En effet, si b est une racine de U dans une extension N de L, le polynôme U se factorise comme $(T-b)^p$ dans $N[T]$. Si donc $U = PQ$ est un factorisation non triviale de U en polynômes unitaires de $L[X]$, on a $P = (T-b)^k$, avec $0 < k < p$. Le coefficient constant $\pm b^k$ de P appartient à L. Comme b^p appartient aussi à L, il en est de même de $b = (b^k)^u.(b^p)^v$, une contradiction.

En reprenant les notations de l'exercice et en posant $N = K(X, Y^p)$, on déduit de ce qui précède que N/L et M/N sont de degré p. Si $\alpha = R(X, Y)$ est un élément quelconque de M, sa puissance p-ième s'écrit $S(X^p, Y^p)$, où S est la fraction rationnelle obtenue en élevant à la puissance p-ième chacun des coefficients de R. Donc α^p est dans L, et le degré de α sur L est au plus p. On en déduit que M/L n'est pas monogène, d'où le résultat.

4.25 (a) Le critère d'Eisenstein s'applique à P pour le nombre premier $p = 3$, donc P est irréductible sur $\mathbb{Q}$. La dérivée $P'(t) = 4t^3 - 3$ s'annule exactement une fois sur $\mathbb{R}$, au point $\vartheta = \sqrt[3]{\frac{3}{4}}$. Comme $P(\vartheta) = -9\vartheta/4 - 3 < 0$, et $\lim_{t\to\pm\infty} P(t) = +\infty$, la fonction $P(t)$ s'annule exactement deux fois sur $\mathbb{R}$. Les deux autres racines de P dans $\mathbb{C}$ sont conjuguées (au sens habituel...) l'une de l'autre.

(b) La décomposition de P en éléments irréductibles de $\mathbb{R}[T]$, s'écrit

$$(T - x)(T - y)(T^2 + aT + b).$$

Le coefficient de T^2 est nul, donc $(T - x)(T - y) = T^2 - aT + b'$. L'identification donne

$$a^2 = b + b' \qquad a(b - b') = 3 \qquad bb' = -3$$

on tire $a^6 = a^2(b^2 + 2bb' + b'^2)$ de la première équation et $9 = a^2(b^2 - 2bb' + b'^2)$ de la seconde. On a donc $a^6 - 9 = a^2(4bb') = -12a^2$, d'où le résultat. Comme a^2 est racine d'un polynôme de degré 3, il est de degré au plus 3. Pour montrer que a^2 est de degré 3, on peut montrer que le polynôme $X^3 + 12X^2 - 9$ est irréductible sur $\mathbb{Q}$, ce qui résulte du fait qu'aucun des entiers ±1, ±3 ou ±9 qui divisent son coefficient constant n'en est une racine.

(c) Le degré de L est un multiple de celui de chacun de ses éléments. Or x est de degré 4 et a^2 est de degré 3, d'où le résultat.

(d) Les classes de conjugaison de $\mathcal{S}_n$ sont en bijection avec les partitions de l'entier n. Pour $n = 4$, la permutation identique forme la seule classe de conjugaison de cardinal 1, les permutations (12), (123), (1234) et (12)(34) sont des représentants des autres classes, de cardinal respectif 6, 8, 6 et 3. Un sous-groupe d'indice 2 est forcément distingué, et formé de certaines de ces classes. La seule somme qui donne 12 est 1 + 8 + 3, qui donne le groupe alterné $\mathcal{A}_4$.

(e) Comme L est une extension normale de $\mathbb{Q}$, il est laissé stable par tout automorphisme de $\mathbb{C}$, en particulier la conjugaison complexe, qui laisse x et y et échange z et $\overline{z}$. Cette permutation est une transposition, c'est-à-dire que considéré comme sous-groupe du groupe des permutations des racines de P, le groupe de Galois de $L/\mathbb{Q}$ n'est pas inclus dans $\mathcal{A}_4$; Or, on a vu au c), que son cardinal $[L : \mathbb{Q}]$ vaut 12 ou 24. la question précédente permet donc de conclure $\mathrm{Gal}(L/\mathbb{Q}) = \mathcal{S}_4$. Reste à compter le nombre de sous-groupes de $\mathcal{S}_4$. Il y en a 1 d'ordre 24, un d'ordre

12, 3 d'ordre 8 (les 2-Sylow sont conjugués entre eux). Il y a 4 sous-groupes d'ordre 6, conjugués à $\mathcal{S}_3$. Les groupes d'ordre ' sont de 3 sortes : les cycliques, au nombre de 3, les conjugués de $\{Id, (12), (34), (12)(34)\}$, au nombre de 3, et le groupe de Klein $\{Id, (12)(34), (13)(24), (14)(23)$. Enfin, il y a 4 groupes d'ordre 3, 9 groupes d'ordre 2 et 1 groupe d'ordre 1, soit un total de $1 + 1 + 3 + 4 + (3 + 3 + 1) + 4 + 9 + 1 = 30$ sous-corps.

4.26 $X^5 - X - 1$ n'a pas de racines dans $\mathbb{F}_2$ mais il en a dans $\mathbb{F}_4$ comme on peut par exemple le voir calculant le pgcd de $X^5 - X - 1$ avec $X^4 - X$. Ainsi $X^5 - X - 1$ se factorise en un produit de deux facteurs irréductibles de degré 2 et 3. On en déduit alors que G contient une permutation de type $(12)(345)$ et donc en passant au cube, une transposition.

Modulo 3, $X^5 - X - 1$ reste irréductible, de sorte que G contient un 5-cycle.

Par ailleurs comme 5 est premier quitte à prendre une puissance du 5-cycle trouvé, on peut supposer le 5-cycle et la transposition respectivement égale à (12) et (12345). On conclut en remarquant que $\mathcal{S}_n$ est engendré par (12) et $(12 \cdots n)$.

4.27 (1) On a $F = E[x]$; supposons donc $a = \alpha^2$ avec $\alpha x \notin E$. On a alors $F = E[\alpha x]$ et il existe $e_1, e_2 \in E$ tels que $x = e_1(\alpha x) + e_2$ et donc $(x - e_2)^2 \in E$ soit $e_2 = 0$ ce qui implique $\alpha \in E$.

(2) (i) c'est trivial

(ii) Cela découle directement de (1)

(iii) (iv) immédiat.

4.28 (1) C'est clair.

(2) (i) D contient $\mathbb{C}$ et donc 2 divise $[D : \mathbb{R}]$.

(ii) Un polynôme de degré impair possède toujours une racine réelle d'après le théorème des valeurs intermédiaires en remarquant qu'en $\pm\infty$ les limites sont infinies de signes opposés. Soit d'après le théorème de Sylow, le 2-Sylow G_2 : l'extension $L = D^{G_2}/\mathbb{R}$ est donc de degré m sur $\mathbb{R}$, le polynôme minimal d'un élément primitif est de degré m et irréductible sur $\mathbb{R}$ d'où $m = 1$.

(iii) Soit H le groupe de Galois de $D/\mathbb{C}$; c'est un 2-groupe que nous supposons non trivial. Or dans un 2-groupe non trivial il existe $Q \subset H$ tel que $H/Q \simeq \mathbb{Z}/2\mathbb{Z}$ de sorte que D^Q est une extension de degré 2 de $\mathbb{C}$ et donc de la forme $\mathbb{C}[\alpha]$ avec $\alpha^2 \in \mathbb{C}$. Or tout nombre complexe a une racine carrée complexe et donc $\alpha \in \mathbb{C}$, contradiction.

(iv) On en déduit donc que $D = \mathbb{C}$ i.e. $\mathbb{C}$ est algébriquement clos.

4.29 (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 $\mathbb{Q}$ de sorte 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 $\mathbb{Q}(y_1, y_2y_3)$. Enfin, le corps fixe de τ est $M(y_1y_2, y_2y_3)$.

(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 $x_1x_2x_3 = -7$, et $y_1y_2y_3 = \pm\sqrt{-7} \in L$. 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 $\mathbb{Q}(\sqrt{-7})$.