Feuille d'exercices 1

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-2007-vf6.html) les exercices que nous aurons abordés.

1 Quelques équations diophantiennes simples

Exercice 1. *On considère l'équation $y^2 = x^3 + 7$:*

(i) Montrez qu'il n'y a pas de solutions avec x pair;

(ii) En écrivant l'équation sous la forme $y^2 + 1 = x^3 + 8 = (x+2)(x^2 - 2x + 4)$ montrez qu'il n'existe pas de solutions entières.

Exercice 2. *Soit $A = \mathbb{Z}[i\sqrt{2}] = \{a + ib\sqrt{2} \ / \ (a,b) \in \mathbb{Z}^2\}$. On définit pour $z = a + ib\sqrt{2} \in A$, $N(z) = a^2 + 2b^2$.*

(a) Montrez que A est euclidien et donc factoriel.

(b) Soient $(x,y) \in \mathbb{Z}^2$, vérifiant l'équation $y^2 + 2 = x^3$. Montrez que x est impair puis que dans B, $y + i\sqrt{2}$ et $y - i\sqrt{2}$ sont premiers entre eux. En déduire qu'il existe $(a,b) \in \mathbb{Z}^2$ tels que $x = a^2 + 2b^2$ et $y + i\sqrt{2} = (a + ib\sqrt{2})^3$, puis décrire les solutions de l'équation précédente.

(c) Étudiez l'ensemble $S = \{n \in \mathbb{N} \ / \ \exists (x,y) \in \mathbb{Z}^2, \ n = x^2 + 2y^2\}$.
Indication: on utilisera que -2 est un carré dans $\mathbb{Z}/p\mathbb{Z}$ si et seulement si $p \equiv 1, 3 \mod 8$.

(d) Étudiez de même l'ensemble $\{n \in \mathbb{Z} \ / \ \exists (x,y) \in \mathbb{Z}^2, \ n = x^2 - 2y^2\}$.

Exercice 3. *Étude de l'équation de Pell-Fermat: $x^2 - Ny^2 = 1$.*

(i) Traitez le cas $N \leq 0$.

(ii) Montrez que dans le cas où N est un carré parfait, les solutions triviales $x = \pm 1, y = 0$ sont les seules.

(iii) On suppose donc $N > 1$ et N n'est pas un carré parfait. En utilisant l'anneau $\mathbb{Z}[\sqrt{N}]$, montrez l'égalité:

$$(x_1^2 - Ny_1^2)(x_2^2 - Ny_2^2) = (x_1x_2 + Ny_1y_2)^2 - N(x_1y_2 + x_2y_1)^2$$

En déduire que s'il existe un solution non triviale (x_0, y_0) à l'équation de Pell-Fermat, alors il en existe une infinité (x_n, y_n) définie par récurrence:

$$\begin{cases} x_{n+1} = x_0x_n + Ny_0y_n \\ y_{n+1} = x_0y_n + x_ny_0 \end{cases}$$

Calculez par exemple pour $N = 2$, les 3 premiers termes de cette suite en remarquant que $(3,2)$ est solution.

(iv) Montrez pour (x_1, y_1) et (x_2, y_2) des solutions positives de l'équation, les équivalences

$$x_1 < x_2 \Leftrightarrow y_1 < y_2 \Leftrightarrow (x_1 + y_1\sqrt{N}) < (x_2 + y_2\sqrt{N})$$

En déduire que s'il existe des solutions non triviales alors il existe une solution minimale (x_0, y_0) pour une relation d'ordre que l'on définira. Montrez ensuite que les solutions sont les (x_n, y_n) définies ci-dessus.

(v) On veut montrer l'existence d'une solution non triviale. Montrez qu'il existe une infinité de rationnels p/q tels que $|\sqrt{N} - p/q| < 1/q^2$.

Indication: commencez par remarquer que p ou $p-1$ est la partie entière de $q\sqrt{N}$, puis appliquez le principe des chaussettes et des tiroirs ($n+1$ chaussettes rangées dans n tiroir, implique qu'un tiroir contient au moins

deux chaussettes), où les chaussettes sont les $n\sqrt{N} - [n\sqrt{N}]$ pour $0 < n \leq q$ et les tiroirs sont les intervalles $[k/q, (k+1) : q]$ pour $0 \leq k < q$.

En déduire qu'il existe une infinité de couples $(p, q) \in \mathbb{N}^2$ premiers entre eux tels que $-1-2\sqrt{N} < p^2 - Nq^2 < 1+2\sqrt{N}$. En utilisant à nouveau le principe des tiroirs, montrez qu'il existe un entier $l < 1+2\sqrt{N}$, $p_1 \equiv p_2 \mod l$, $q_1 \equiv q_2 \mod l$ tels que $p_1^2 - Nq_1^2 = p_2^2 - Nq_2^2 = \pm l$, et en déduire l'existence d'une solution non triviale.

(vi) Soit p la période du développement de $\sqrt{N}$ en fractions continues et soit $\delta_p = N_p/D_p$ sa réduite d'ordre p, alors on rappelle que

$$(\delta_p - \sqrt{N})(\delta_p + \sqrt{N}) = \frac{(-1)^p}{D_p^2} \tag{1}$$

D'autre part il n'existe pas de fraction a/b plus simple que δ_p, i.e. $a < N_p$ et $b < D_p$ tels que $(a/b - \sqrt{N})(a/b + \sqrt{N}) = \frac{\pm 1}{D_p^2}$.

- *Montrez que pour p pair, (N_p, D_p) est une solution minimale de l'équation de Pell-Fermat $x^2 - Ny^2 = 1$ puis que toute solution (x, y) est de la forme $\begin{pmatrix} x_n \\ y_n \end{pmatrix} = A^n \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ avec $A = \begin{pmatrix} N_p & ND_p \\ D_p & N_p \end{pmatrix}$.*
- *Pour p impair, montrez que $(N_p^2 + ND_p^2, 2N_pD_p)$ est la solution minimale de l'équation de Pell-Fermat $x^2 - Ny^2 = 1$ puis que toute solution (x, y) est de la forme $\begin{pmatrix} x_n \\ y_n \end{pmatrix} = A^{2n} \begin{pmatrix} 1 \\ 0 \end{pmatrix}$.*

(vii) Résoudre les questions suivantes:

- *$x^2 - 7y^2 = 1$;*
- *$x^2 - 19y^2 = 1$;*
- *m est dit triangulaire s'il est de la forme $1 + 2 + \cdots + n$. Trouvez les nombres triangulaires qui sont des carrés.*
- *un problème de Sam Loyd: "... je vis les hommes de Harold groupés en 13 grands carrés tous égaux. Harold se porta au milieu de ses hommes et à son signal ils se réunirent en un seul et énorme carré..." Quel était le nombre des hommes de Harold?*
- *Soient $A = (0, 0)$ et $B = (4, 0)$. Trouvez l'ensemble des points M du réseau $\mathbb{Z}^2$ tels que $|MA - MB| = 2$.*

2 Nombres transcendants: premiers exemples

Exercice 1. e **est irrationnel**: *on considère la suite (u_n) définie par récurrence: $u_0 = 1$ et $u_{n+1} = u_n + \frac{1}{(n+1)!}$.*

(a) Montrez que (u_n) converge; on notera e sa limite.

(b) 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.

Exercice 2. 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.

Exercice 3. e **est transcendant**: *(a) Soit $P \in \mathbb{R}[X]$ de degré m; montrez que*

$$I_P(t) = \int_0^t e^{t-u} P(u) du = e^t \sum_{i=0}^{m} P^{(i)}(0) - \sum_{i=0}^{m} P^{(i)}(t).$$

(b) Soient $a_0, \cdots, a_n \in \mathbb{Z}$ tels que $a_0 + a_1 e + \cdots + a_n e^n = 0$ avec $a_0 \neq 0$ et $a_n \neq 0$. On pose pour tout $0 < p \in \mathbb{N}$: $f(x) = x^{p-1}(x-1)^p \cdots (x-n)^p$ ainsi que $J_p = a_0 I_f(0) + \cdots + a_n I_f(n)$. Montrez que $J_p \in \mathbb{Z}$ puis que si p est un nombre premier assez grand, J_p est divisible par $(p-1)!$ mais pas par $p!$.

(c) Montrez qu'il existe une constante c indépendante de p, telle que $|J_p| \leq c^p$ et conclure.

Exercice 4. Approximation des réels par des rationnels

(i) Soient $p/q \neq a/b$ des rationnels distincts. Montrez que $|p/q - a/b| \geq 1/bq$.

(ii) (a) Soit $P \in \mathbb{Z}[X]$ un polynôme de degré n ne possédant aucune racine rationnelle (i.e. $\forall x \in \mathbb{Q}$, $P(x) \neq 0$). Soit $x \in \mathbb{R}$ un irrationnel tel que $P(x) = 0$. Montrez que pour tout $\delta > 0$ et tout $p/q \in \mathbb{Q}$ avec p et q premiers entre eux et $q > 0$, tel que $|p/q - x| \leq \delta$, il existe une constante $K(x, \delta)$ qui ne dépend que de x et de δ telle que $|p/q - x| \geq K(x)/q^n$.

*(b) Soit $x = \sum_{i=1}^{+\infty} 10^{-i!}$. Justifiez cette écriture et montrez que x est irrationnel. On considère alors $I_x = \{P \in \mathbb{Q}[X],\ P(x) = 0\} = (\mu_x)$ avec $\mu_x \in \mathbb{Z}[X]$ qu'on appelle le polynôme minimal de x sur $\mathbb{Q}$. **On suppose** que μ_x est non nul et on note n son degré. Montrez que μ_x n'a pas de racines rationnelles. En considérant les rationnels $x_k = \sum_{i=1}^{k} 10^{-i!}$ pour $k \geq n$, montrez que l'on aboutit à une contradiction.*

(iii) Soit $x \in \mathbb{R}$ un irrationnel. Soit alors (p_n/q_n) une suite de rationnels écrite sous forme réduite (i.e. p_n et q_n premiers entre eux et $q_n > 0$), convergeant vers x. Montrez que (q_n) tend vers l'infini.

Citons le théorème de Thue-Siegel-Dyson-Roth: soit x algébrique de degré d, alors pour tout $\epsilon > 0$, il existe $K(x, \epsilon)$ tel que pour tout p/q on ait

$$|x - p/q| > \frac{K(x, \epsilon)}{q^{f(d)+\epsilon}}$$

où:

- $f(d) = d/2 + 1$ (Thue);
- $f(d) = 2\sqrt{d}$ (Siegel);
- $f(d) = \sqrt{2d}$ (Dyson et Gelfond);
- $f(d) = 2$ (Roth)

A titre de réflexion, vous pouvez réfléchir à l'argumentaire suivant: soit f une fonction sur $\mathbb{N}$ telle que $f(q) \to +\infty$ quand $q \to +\infty$. On note X_f l'ensemble des réels x de $[0, 1]$ admettant une suite d'approximations p_n/q_n avec $|x - p_n/q_n| \leq 1/f(q_n)$, alors

$$X_f = \bigcap_{q_0}^{\infty} \bigcup_{q \geq q_0} \bigcup_{0 \leq p \leq q} [\frac{p}{q} - \frac{1}{f(q)}, \frac{p}{q} + \frac{1}{f(q)}]$$

L'intersection étant décroissante et les ensembles de mesure finie, il vient

$$\mu(X_f) = \lim_{q_0 \to \infty} \mu\Big(\bigcup_{q \geq q_0} \bigcup_{0 \leq p \leq q} [\frac{p}{q} - \frac{1}{f(q)}, \frac{p}{q} + \frac{1}{f(q)}] \Big) \leq \lim_{q_0 \to \infty} \sum_{q \geq q_0} \frac{2(q+1)}{f(q)}$$

En particulier si la série $\sum_{q \geq 1} q/f(q)$ converge alors $\mu(X_f) = 0$ ce qui est le cas pour $f(q) = q^\alpha$ avec $\alpha > 2$.

Exercice 5. ***Transcendance de*** π

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

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

vérifie

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

ainsi que la majoration

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

(ii) *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 $f^{(n)} = n!f_n$.*

(iii) *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 $a^n \sum_{f(\alpha)=0} \alpha^n$.

(iv) *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*

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

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

(v) *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.

Exercice 6. ***Construction à la règle et au compas***

Soit Σ un ensemble de points du plan $\mathbb{R}^2$; on dit qu'un point P est constructible à la règle et au compas à partir de Σ s'il existe un entier n et une suite de points $P_1, \cdots, P_n = P$ tels que pour tout $i \in \{1, \cdots, n\}$, notant $\Sigma_i = \Sigma \cup \{P_1, \cdots, P_{i-1}\}$, il existe 4 points $A, B, A', B' \in \Sigma_i$ tels que l'une des propriétés suivantes soit vérifiée:

- P_i est le point d'intersection des droites non parallèles (AB), $(A'B')$;

- P_i est l'un des deux points d'intersection de la droite (AB) et du cercle de centre A' passant par B';

- P_i est l'un des points d'intersection des cercles centrés en A, A' et passant respectivement par B, B'.

Un réel x est dit constructible à partir de Σ si le point $(x, 0)$ de $\mathbb{R}^2$ l'est. Un nombre complexe z est dit constructible à partir de Σ si le point si sa partie réelle et imaginaire l'est.

(1) *Soit Σ une partie de $\mathbb{R}^2$ contenant $0, 1$ et soit C_Σ l'ensemble des points constructibles à partir de Σ. Montrez que si $x, y \in C_\Sigma$ alors $x + y, x - y, xy, x/y, \sqrt{x}$ sont aussi dans C_Σ.*

(2) *Désormais $\Sigma = \{0, 1\}$. Montrez qu'un réel x est constructible si et seulement s'il existe un entier n et une suite de sous-corps de $\mathbb{R}$: $\mathbb{Q} = E_0 \subset E_1 \subset \cdots, E_n$ tels que pour tout i, $[E_i : E_{i-1}] = 2$ et $x \in E_n$.*

(3) *En déduire que si x est constructible, alors x est algébrique de degré une puissance de 2.*

(4) Que pensez-vous des problèmes de la duplication du cube, de la trisection des angles et de la quadrature du cercle.

(5) Montrez que $x \in \mathbb{R}$ est constructible si et seulement si le sous-corps de $\mathbb{C}$ engendré par x et ses conjugués est de degré une puissance de 2: autrement dit si le corps de décomposition de x est de degré une puissance de 2.

(6) Montrez que les polygones réguliers constructibles sont les $2^s p_1 \cdots p_r$ où les p_i sont des nombres premiers de Fermat.

(7) Montrez que la règle ne sert à rien.

(8) Que pouvez-vous dire de la construction à la règle seule? Peut-on toujours construire le milieu de deux points, le centre d'un cercle, l'isobarycentre d'un triangle...?

3 Extensions de corps, groupes de Galois

Exercice 1. *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 2. *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 3. *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. Soit a et b deux rationnels tels que $a^2 - 4b$ soit positif mais pas un carré rationnel, et b négatif. Montrer que le polynôme $X^4 + aX^2 + b$ est irréductible sur $\mathbb{Q}$ et que son corps de rupture n'est pas galoisien sur $\mathbb{Q}$.*

Exercice 4. *Trouver a et b entiers tels que le polynôme $X^4 + aX^2 + b$ soit irréductible sur $\mathbb{Q}$ et que son corps de rupture soit galoisien sur $\mathbb{Q}$.*

Exercice 5. *Soit $K = \mathbb{Q}(\sqrt[3]{2})$, L la clôture galoisienne de K sur 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 6. *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 7. *Soit G le groupe de Galois de $X^5 - 2$. Quel est le cardinal de G? Est-il abélien, résoluble?*

Exercice 8. *Quel est le degré du corps de rupture du polynôme $(X^3 - 5)(X^3 - 7)$ sur $\mathbb{Q}$?*

Exercice 9. *Déterminez le groupe de Galois de $X^6 - 5$ sur $\mathbb{Q}$, $\mathbb{R}$.*

Exercice 10. *Trouvez un élément primitif de $\mathbb{Q}[\sqrt{3}, \sqrt{7}]$.*

Exercice 11. *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 12. *Trouvez un élément primitif du corps de rupture de $(X^2 - 2)(X^2 - 5)(X^2 - 7)$.*

Exercice 13. *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 14. *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 15. *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* $\{\theta, \rho\theta, \rho^2\theta\}$ *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*

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

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 16. 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 $\sqrt{-7}$.

Exercice 17. *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 18. *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 19. *(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 20. *Soit $P(X) = a_n X^n + \cdots + a_0 \in \mathbb{C}[X]$; 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 $2^n m$ 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.