Correction feuille 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.

Preuve : (i) Si x est pair, on a $y^2 \equiv -1 \mod 8$. En écrivant y impair sous la forme $2k+1$, on obtient $y^2 = 1 + 4k(k+1) \equiv 1 \mod 8$ contradiction.

(ii) On a $x^3 + 8 = (x+2)(x^2 - 2x + 4)$ avec x impair de la forme $2k+1$; $(x^2 - 2x + 4) = 4k^2 + 3$. On en déduit donc qu'il existe un p premier divisant $x^2 - 2x + 4$ avec $p \equiv 3 \mod 4$. Or si p premier divise $y^2 + 1$ alors $p \equiv 1 \mod 4$, d'où la contradiction.

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 B 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 $\{n \in \mathbb{Z} \ / \ \exists (x,y) \in \mathbb{Z}^2, \ n = x^2 - 2y^2\}$.

Preuve : (a) On raisonne comme dans $\mathbb{Z}[i]$; soit $N(a+ib\sqrt{2}) = a^2 + 2b^2$ la norme qui est une fonction multiplicative, et soit $z \in A^\times$; on a $zz' = 1$ soit $N(z)N(z') = 1$ et donc $N(z) = 1$, soit $z = \pm 1$.
Pour montrer que A est euclidien, on remarque à nouveau que z_1/z_2 peut s'écrire sous la forme $q + e$ avec $q \in A$ et $e \in \mathbb{C}$ de norme strictement plus petite que 1. Ainsi on a $z_1 = qz_2 + r$, avec $r = z_1 - qz_2 \in A$ et $N(r) < N(z_2)$.

(b) Si x est pair, on a $y^2 \equiv -2 \mod 8$, ce qui ne se peut pas, car les carrés dans $\mathbb{Z}/8\mathbb{Z}$, sont $0, 1, 4$. On factorise ensuite dans A: $x^3 = (y + i\sqrt{2})(y - i\sqrt{2})$ et soit δ un pgcd de $y + i\sqrt{2}$ et $y - i\sqrt{2}$; on a $\delta = (y + i\sqrt{2}, (i\sqrt{2})^3)$, or $i\sqrt{2}$ est irréductible car de norme 2, et la seule factorisation de 2 est 1×2, de sorte que $i\sqrt{2} = zz'$ implique que $N(z) = 1$ soit z inversible (ou z'). Or $i\sqrt{2}$ ne divise pas y car sinon y^2 serait pair et donc y pair soit x pair, ce qui n'est pas; ainsi $\delta = 1$. On en déduit donc que $(y \pm i\sqrt{2})$ sont des cubes parfaits: $(y \pm i\sqrt{2}) = (a \pm i\sqrt{2})^3$ et $x = a^2 + 2b^2$. En séparant partie réelle et imaginaire, on trouve alors $y = a^3 - 6ab^2$ et $1 = b(3a^2 - 2b^2)$ soit $b = \epsilon = \pm 1 = 3a^2 - 2$, ce qui donne $b = 1$ et $a = \pm 1$ soit $y = \pm 5$ et $x = 3$ qui est bien une solution de l'équation.

(c) On a à nouveau $n \in S$ si et seulement si il existe $z \in A$ tel que $n = N(z)$. On étudie à nouveau les irréductibles de B; p est irréductible si et seulement si $A/(p)$ est intègre, i.e. $X^2 + 2$ n'a pas de racine dans $\mathbb{Z}/p\mathbb{Z}$, i.e. si et seulement si -2 n'est pas un carré dans $\mathbb{Z}/p\mathbb{Z}$, i.e. si et seulement si $p \equiv 5, 7 \mod 8$. En raisonnant comme dans $\mathbb{Z}[i]$, on trouve que les irréductibles de A, outre les premiers $p \equiv 5, 7 \mod 8$, sont les $z \in A$ tels que $N(z)$ est premier: en effet si $N(z)$ est premier alors si $z = z_1 z_2$ alors $N(z_1) = 1$ et donc z_1 est inversible, réciproquement, si $N(z) = ab$ alors soit z_0 un diviseur irréductible dans A de a, il divise $z\bar{z}$ et donc z, quitte à conjuguer, de sorte que $z_0 = z$ et $N(z) = N(z_0)$ est premier.

Finalement pour déterminer l'ensemble S, on commence par remarquer que S est multiplicatif et que si n est tel que $v_p(n)$ est pair pour $p \equiv 5, 7 \mod 8$ alors $n \in S$. Réciproquement soit $p \equiv 1, 3 \mod 8$ qui divise $n = a^2 + 2b^2$.

Alors p est irréductible dans A et divise $n = z\bar{z}$ avec $z = a + i\sqrt{2}b$ et donc divise z de sorte que p^2 divise n; par récurrence immédiate on en déduit donc que $v_p(n)$ est pair.

(d) De la même façon, la détermination de S se fait via l'étude de $A = \mathbb{Z}[\sqrt{2}]$, dont la norme est $a^2 - 2b^2$, avec le morphisme de corps $c(a+b\sqrt{2}) = a-\sqrt{2}b$ de sorte que N est multiplicative. Soit $z \in A^\times$, on a alors $N(z) = \pm 1$. A nouveau A est euclidien pour le stathme $|N|$. On remarque que -1 est une norme $-1 = 1^2 - 2\times 1^2 = N(1+\sqrt{2})$. Si n est un diviseur de $x^2 - 2y^2$ avec x, y premiers entre eux, alors au signe près n est de la forme $u^2 - 2v^2$. En effet soit $x + \sqrt{2}y = \pi_1 \cdots \pi_r$ une décomposition en produit d'irréductibles; aucun des π_i n'appartient à $\mathbb{Z}$ car x et y sont premiers entre eux, de sorte que comme précédemment les $N(\pi_i)$ sont des premiers de $\mathbb{Z}$; on a alors $x^2 - 2y^2 = N(\pi_1)\cdots N(\pi_r)$ et n au signe près, est un produit de certains de ces $N(\pi_i)$ et donc n est de la forme $N(z) = u^2 - 2v^2$.
L'égalité $-(u^2 - 2v^2) = N((1+\sqrt{2})(u + v\sqrt{2})) = (u+2v)^2 - 2(u+v)^2$ permet de négliger le signe $\pm$. Ainsi un premier impair p est de la forme $x^2 - 2y^2$ si et seulement si 2 est un carré modulo p ce qui est équivalent à $p \equiv \pm$ mod 8.

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 que 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 l'ensemble des solutions sont les (x_n, y_n) définis 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 $0 \leq n \leq q$ 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* $A = (-2, 0)$ *et* $B = (2, 0)$*. Trouvez l'ensemble des points* M *du réseau* $\mathbb{Z}^2$ *tels que* $|MA - MB| = 2$*.*

Preuve : Evidemment, on se limite à chercher les solutions $x, y \geq 0$.

(i) Pour $N \leq -2$, les seules solutions sont clairement $x = 1$ et $y = 0$; pour $N = -1$, on obtient $(x, y) = (1, 0)$ ou $(0, 1)$.

(ii) Soit $N = d^2$; $x^2 - d^2y^2 = (x - dy)(x + dy) = 1$, soit $x + dy = 1 = x - dy$, d'où $x = 1$ et $y = 0$.

(iii) Soit $A = \mathbb{Z}[\sqrt{N}]$ et $N(a + b\sqrt{N}) = a^2 - Nb^2 = (a + b\sqrt{N})(a - b\sqrt{N})$. L'application N est multiplicative, d'où $N((a + b\sqrt{N})(c + d\sqrt{N})) = N(a + b\sqrt{N})N(c + d\sqrt{N})$ ce qui donne l'identité remarquable de l'énoncé.

Avec ces notations (x, y) est solution si et seulement si $N(x + y\sqrt{N}) = 1$, ainsi si (x_0, y_0) est solution alors (x_n, y_n) tel que $x_n + y_n\sqrt{N} = (x_0 + y_0\sqrt{N})^n$, est solution, ce qui donne la relation de récurrence de l'énoncé. On remarque simplement que la suite (x_n, y_n) prend une infinité de valeur car la solution (x_0, y_0) étant non triviale, $x_0 \geq 2$ et $y_0 \geq 1$ ce qui implique $x_{n+1} > x_n$ et $y_{n+1} > y_n$.

Avec $N = 2$ et $(x_0, y_0) = (3, 2)$, on obtient les premiers termes de la suite (x_n, y_n): $(17, 12)$, $(99, 70)$, $(577, 408)$.

(iv) Soient (x_1, y_1) et (x_2, y_2) des solutions positives; on a alors les équivalences:

$$x_1 < x_2 \Leftrightarrow x_1^2 < x_2^2 \Leftrightarrow 1 + Ny_1^2 < 1 + Ny_2^2 \Leftrightarrow y_1 < y_2 \Leftrightarrow x_1 + y_1\sqrt{N} < x_2 + y_2\sqrt{N}$$

On choisit alors la relation d'ordre suivante sur les solutions positives: $(x_1, y_1) \leq (x_2, y_2)$ si et seulement si $x_1 \leq x_2$. Parmi les solutions positives non triviales, soit donc (x_0, y_0) la solution minimale dont l'existence découle du fait que $\mathbb{N}$ est discret.

Soit alors (x, y) une solution (positive) et $n \geq 0$ tel que $x_n \leq x < x_{n+1}$; on a alors $y_n \leq y < y_{n+1}$ et donc $1 \leq \frac{x+y\sqrt{N}}{x_n+y_n\sqrt{N}} < x_0 + y_0\sqrt{N}$. Or $\frac{x+y\sqrt{N}}{x_n+y_n\sqrt{N}}$ est égal à $X + Y\sqrt{N}$ avec $X = xx_n - Nyy_n$ et $Y = yx_n - xy_n$ avec $X^2 - NY^2 = 1$. En outre, on a $X \geq 0$ car $x \geq y \geq 0$ et $x_n \geq y_n \geq 0$; de même $Y \geq 0$ car sinon $X + Y\sqrt{N} = \frac{1}{X+\sqrt{X^2+1}} < 1$ ce qui n'est pas. Ainsi (X, Y) est une solution positive et $X + Y\sqrt{N} < x_0 + y_0\sqrt{N}$ ce qui contredit la minimalité de (x_0, y_0).

(v) Commençons par montrer l'existence d'une infinité de rationnels p/q tels que $|\sqrt{N} - p/q| < 1/q^2$, soit $-1/q < q\sqrt{N} - p < 1/q$ et donc soit $p = [q\sqrt{N}]$ soit $p = [q\sqrt{N}] + 1$. On raisonne par l'absurde, en supposant la finitude de l'ensemble E de ces rationnels. Soit alors $\epsilon = \min_{p/q \in E} |\sqrt{N} - p/q|$. Comme $\sqrt{N} \notin \mathbb{Q}$, on a $\epsilon > 0$. Soit donc $q_0 > 0$ tel que $1/q_0 < \epsilon$, on va montrer qu'il existe $q \leq q_0$ et p tel que $|\sqrt{N} - p/q| < 1/qq_0 \leq 1/q^2$ ce qui est en contradiction avec le fait que l'on devrait avoir $|\sqrt{N} - p/q| \geq \epsilon$. Considérons donc les q_0-tiroirs $[k/q_0, (k + 1)/q_0]$ pour $k = 0, \cdots, q_0 - 1$, et les chaussettes $|q\sqrt{N} - [q\sqrt{N}]|$ pour $n = 1, \cdots, q_0$. Si une chaussette est dans le premier tiroir, c'est gagné. Plaçons-nous dans la situation contraire et soient $q_1 \neq q_2$ deux chaussettes dans le même tiroir, soit $|(q_1 - q_2)\sqrt{N} - [q_1\sqrt{N}] + [q_2\sqrt{N}]| < 1/q_0$. Ainsi en posant $q = |q_1 - q_2|$ et $p = [q_1\sqrt{N}] - [q_2\sqrt{N}]$, on a bien $|a\sqrt{N} - p| < 1/q_0$, d'où le résultat.

Des inégalités $-1/q^2 < \sqrt{N} - p/q < 1/q^2$ avec $p, q > 0$, on obtient $-1/q < q\sqrt{N} - p < 1/q$, soit $0 < p + q\sqrt{N} < 1 : q + 2q\sqrt{N}$ soit $-1 - 2\sqrt{N} < p^2 - Nq^2 < 1 + 2\sqrt{N}$. On obtient de la sorte une infinité de couples (p, q) avec p et q premiers entre eux, et $p^2 - Nq^2$ appartenant à l'intervalle $[-1 - 2\sqrt{N}, 1 + 2\sqrt{N}]$ dans lequel il y a un nombre fini d'entiers (de tiroirs). Selon le principe des tiroirs, il existe un entier l de l'intervalle précédent tel qu'il existe une infinité de couples (p, q) (les chaussettes) avec p et q premiers entre eux, tels que $p^2 - Nq^2 = l$. Comme ${}^s qrt N \notin \mathbb{Q}$, l n'est pas nul; si $l = \pm 1$ c'est gagné, sinon les nouveaux tiroirs sont les éléments de $\mathbb{Z}/l\mathbb{Z}$ et on place la chaussette (p, q) dans le tiroir $\bar{p}$. On en déduit donc l'existence d'une infinité de couples (p, q) comme ci-dessus, tels que tous les p ont la même congruence modulo l. En envoyant ces chaussettes (p, q) dans le tiroir $\bar{q}$, on obtient finalement l'existence d'un infinité de couples (p_i, q_i) tels que p_i et q_i sont premiers entre eux, $p_i^2 - Nq_i^2 = l$, tous les p_i ont la même congruence modulo l; de même que tous les q_i.

Soient alors (p_1, q_1) et (p_2, q_2) des éléments distincts de cet ensemble; on a $p_1^2 - Nq_1^2 = p_2^2 - Nq_2^2 = l$ et $p_1 \equiv p_2 \mod l$ et $q_1 \equiv q_2 \mod l$. Ainsi $p_1q_2 - p_2q_1$ est divisible par l. De l'égalité $(p_1p_2 - Nq_1q_2)^2 - N(p_1q_2 - p_2q_1)^2 = l^2$, on en déduit que l divise $p_1p_2 - Nq_1q_2$ et $(\frac{p_1p_2 - Nq_1q_2}{l}, \frac{p_1q_2 - p_2q_2}{l})$ est alors une solution non triviale de l'équation.

(vi) *cas pair*:(1 s'écrit $(N_p - \sqrt{N}D_p)(N_p + \sqrt{N}D_p) = 1$ de sorte que (N_p, D_p) est une solution. Elle est minimale du fait que N_p/D_p est la fraction la plus simple.

cas impair: en élevant au carré les deux membres de (1), on obtient

$$(N_p - \sqrt{N}D_p)^2(N_p + \sqrt{N}D_p)^2 = 1$$

ce qui donne $(N^2 + KD_p^2)^2 - K(2N_pD_p)^2 = 1$ et donc $(N^2 + KD_p^2, 2N_pD_p)$ est une solution. S'il existait (x_0', y_0') et $n \geq 2$ tels que

$$(x_0' + \sqrt{N}y_0')^n = N_p^2 + ND_p^2 + \sqrt{N}(2N_pD_p)$$

avec $x_0' < N_p$ et $y_0' < D_p$ alors on aurait

$$(\frac{x_0'}{y_0'} - \sqrt{N})(\frac{x_0'}{y_0'} + \sqrt{N}) = (\frac{1}{y_0'})^2$$

et x_0'/y_0' serait une meilleure fraction que N_p/D_p.

(vii) $x^2 - 7y^2 = 1$: ici on trouve la solution par tâtonnements en remplaçant successivement y par $1, 2, 3 \cdots$, on trouve la solution minimale $(8, 3)$ et la matrice $A = \begin{pmatrix} 8 & 21 \\ 3 & 8 \end{pmatrix}$, ce qui donne pour premières solutions $(1, 0)$, $(8, 3)$, $(127, 48)$, $(2024, 765)$.

$x^2 - 19y^2 = 1$: à la main on ne trouve rien rapidement, on calcule alors $\sqrt{19} = (4)(\overline{2, 1, 3, 1, 2, 8})$ soit $p = 6$ et $\delta_6 = \frac{170}{39}$, ce qui donne $A = \begin{pmatrix} 170 & 741 \\ 39 & 170 \end{pmatrix}$, ce qui donne pour premières solutions $(1, 0)$, $(170, 39)$, $(57799, 13260)$.

Les nombres triangulaires et carrés: $m^2 = \frac{n(n+1)}{2}$ soit $n^2 + n - 2m^2 = 0$ soit $n = \sqrt{-1 + \sqrt{8m^2 + 1}}2$ soit à trouver m tel que $8m^2 + 1$ est un carré. L'équation $x^2 - 8y^2 = 1$ a pour solution minimale $(3, 1)$, les nombres y_n sont donnés par

$$y_n = \frac{(3 + \sqrt{8})^n - (3 - \sqrt{8})^n}{2\sqrt{8}}$$

et donc

$$x_n = \frac{(3 + 2\sqrt{2})^{2n} + (3 - 2\sqrt{2})^{2n} - 2}{32}$$

ou encore avec $A = \begin{pmatrix} 3 & 8 \\ 1 & 3 \end{pmatrix}$, on trouve $1, 36, 1225, 41616....$

La bataille de Hasting 4-10-1066: Soit x^2 le nombre des hommes de Harold, on a donc $x^2 - 13y^2 = 1$ avec $\sqrt{13} = (3)(\overline{1, 1, 1, 1, 6})$, $p = 5$ et $\delta_5 = \frac{18}{5}$. Comme p est impair, la solution minimale est $x = 18^2 + 13.5^2 = 649$ et $y = 2.18.5 = 180$. Le nombre de soldats est donc 421000 (cela fait quand même beaucoup de monde!).

Coordonnées entières sur une hyperbole: l'équation en $M = (x, y)$ de l'hyperbole est

$$|\sqrt{(x+2)^2 + y^2} - \sqrt{(x-2)^2 + y^2}| = 2$$

ce qui équivaut à $3x^2 - y^2 = 3$. Une solution entière est alors telle que $y = 3z$ et l'équation devient $x^2 - 3z^2 = 1$. La solution minimale est $(2, 1)$ et les solutions $(\pm x_n, \pm y_n)$ sont

$$\begin{cases} x_n = \frac{(2+\sqrt{3})^n + (2-\sqrt{3})^n}{2} \\ y_n = \frac{(2+\sqrt{3})^n - (2-\sqrt{3})^n}{2}\sqrt{3} \end{cases}$$

Les premières solutions sont

$$(\pm 1, 0),\ (\pm 2, \pm 3),\ (\pm 7, \pm 12),\ (\pm 26, \pm 45)$$

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.*

Preuve : (a) évident (b) $\alpha = (k+1)^{-1} + (k+1)^{-1}(k+2)^{-1} + \cdots \leq \sum_{i=1}^{+\infty}(k+1)^{-i} = 1/k \notin \mathbb{N}$.

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.

Preuve : (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.

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.*

Preuve : (a) On traite le cas d'un monôme (évidemment) puis on conclura par linéarité:

$$\begin{aligned} \int_0^t e^{t-u} u^n du &= e^t[-e^{-u}u^n]_0^t + e^t \int_0^t e^{-u} n u^{n-1} du \\ &= -t^n + n \int_0^t e^{t-u} u^{n-1} du \end{aligned}$$

On peut par exemple raisonner par récurrence sur n, on obtient alors $\int_0^t e^{t-u} u^n du = e^t \sum_{k=0}^n [\frac{d^k}{dt^k} t^n]_0 - \sum_{k=0}^n \frac{d^k}{dt^k} t^n$ et on conclut par linéarité. (remplacer m par $+\infty$).

(b) On pose $m = np + p - 1$ de sorte que $J_p = \sum_{j=0}^{m} f^{(j)}(0)(a_0 + a_1 e + \cdots + a_n e^n) - \sum_{j=0}^{m}\sum_{k=0}^{n} f^{(j)}(k)$. Le résultat se déduit des faits suivants: le premier terme dans l'écriture de J_p ci-dessus est nul et les $f^{(j)}(k) \in \mathbb{Z}$.

En outre si $k > 0$, $f^{(j)}(k) = 0$ pour $j < p$ et $f^{(j)}(k)$ est un multiple de $p!$ pour $j \geq p$. Pour $k = 0$, $f^{(j)}(0) = 0$ pour $j < p - 1$ et $f^{(j)}(0)$ est divisible par $p!$ pour $j \geq p$ alors que $f^{(p-1)}(0) = (p-1)!(n!)^p(-1)^{np}$ qui ne sera pas divisible par p si $p > n$, d'où le résultat.

En particulier J_p n'est pas nul.

(c) On a $|f(x)| \leq (2n)^m$ pour $0 \leq x \leq n$ de sorte que

$$J_p \leq \sum_{k=0}^{n} |a_k| \int_0^k e^{k-u}|f(u)|du \leq \sum_k |a_k|(2n)^m(e^k - 1) \leq c[(2n)^{n+1}]^p$$

avec $c = e^n \sum |a_k|$, d'où le résultat.

Au final on a donc $|J_p| \geq (p-1)!$ car J_p est non nul et divisible par $(p-1)!$ et $|J_p| \leq c^p$. La contradiction provient du fait que $c^p/(p-1)!$ tend vers 0 lorsque p tend vers $+\infty$.

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.

Preuve : (1) $|pb - qa|$ est un entier non nul donc supérieur ou égal à 1.

(2) (a) L'inégalité des AF s'écrit: $|P(p/q) - P(x)| \leq K|x - p/q|$ où K est un majorant de la dérivée de P sur $[x - \delta, x + \delta]$. Comme $P(x) = 0$ et $P(p/q) \neq 0$, on obtient en réduisant au même dénominateur $1/q^n \leq |a_n p^n + a_{n-1}p^{n-1}q + \cdots + a_0 q^n| \leq K|p/q - x|$ d'où le résultat.

(b) Si μ_x avait une racine, en factorisant, on obtiendrait un polynôme de $\mathbb{Q}[X]$ qui s'annule en x et de degré strictement plus petit que celui de μ_x alors qu'il doit être divisible par ce dernier !

On a $0 \leq x - x_k \leq 210^{-(k+1)!}$ (on prend des 1 partout au lieu de les prendre espacés). On doit donc avoir $210^{n(k!)} \geq K10^{(k+1)!}$ pour tout k ce qui ne se peut pas. (x est donc transcendant)

(3) Soit M, d'après l'indication, on choisit 2ϵ égal au minimum des $x - p_n/q_n$ où $p_n/q_n \in [x-1, x+1]$ (si l'ensemble est vide, on prend $2\epsilon = 1$). Soit alors n_0 tel que pour tout $n \geq n_0$, $|p_n/q_n - x| \leq \epsilon$. On a alors pour tout $n \geq n_0$, $q_n \geq M$, d'où le résultat.

Le dénominateur q^n est alors un facteur cohérent d'estimation de la facilité avec laquelle un réel se laisse approcher par des rationnels. En particulier dans 2-a, le δ n'est pas important car si on se rapproche de x, les dénominateurs q grandissent de sorte que K/q^n sera plus petit que δ ...

(4) C'est le principe des tiroirs et des chaussettes; les chaussettes sont les x_q pour $1 \leq q \leq q_0$ ce qui donne q_0 chaussette. Si une de ces chaussettes est rangée dans tiroir I_0 il n'y a rien à faire. Dans le cas contraire, q_0 chaussettes rangées dans $q_0 - 1$ tiroirs cela donne 2 chaussettes dans le même tiroir, soit $x_{q_1}, x_{q_2} \in I_k$. On écrit $x_{q_1} - x_{q_2} = qx - p$ avec $q = q_1 - q_2$ et $p = E(q_2 x) - E(q_1 x)$. On a bien $0 \leq q \leq q_0$.

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

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

vérifie

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

ainsi que la majoration

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

(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

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

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.

Preuve : (1) On intègre par partie soit

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

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

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

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^nA^n est aussi à coefficients entiers ainsi que sa trace. Or les valeurs propres de a^nA^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 $n \ge p$, 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 $n \ge p$ alors que

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

Ainsi, il existe un entier M tel que

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

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

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

Or la majoration de l'intégrale I dans (1) implique qu'il existe un réel $c > 0$ tel que $|J_p| \le c^p$ 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 $q \ge 1$ la multiplicité del a racine 0 dans P_0. On pose $P := NF_0/X^q$: c'est un polynôme à coefficients entiers avec $P(0) \ne 0$. 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).

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...?

Preuve : (1) Ce sont des constructions classiques

(2) Rappelons qu'une équation d'une droite est de la forme $ax + by + c = 0$ tandis que celle d'un cercle est de la forme $x^2 + y^2 + Ax + By + C = 0$. Le point d'intersection de deux droites d'équations $ax + by + c = 0$ et $a'x + b'y + c' = 0$ avec $a, b, c, a', b', c' \in K$ est un point $(x, y) \in K^2$. Le point d'intersection d'une droite d'équation $ax + by + c = 0$ et d'un cercle $x^2 + y^2 + Ax + By + C = 0$ avec $a, b, c, A, B, C \in K$ est un point $(x, y) \in L^2$ où L est une extension de degré au plus deux de K. Le point d'intersection de deux cercles se ramène à celui d'une droite et d'un cercle, l'équation de la droite étant obtenue par soustraction des deux équations des cercles (c'est l'axe radial du faisceau de cercle engendré par ces deux cercles).

(3) C'est clair en utilisant la multiplicativité des degrés.

(4) Le polynôme $X^3 - 2$ n'a pas de racines dans $\mathbb{Q}$, il est donc irréductible et $\sqrt[3]{2}$ est donc de degré 3.

Le point $\sin\alpha$ est constructible à partir de $\cos\alpha$ car $\sin^2\alpha\alpha = 1 - \cos^2\alpha$. La question est donc de savoir si $\cos\alpha/3$ est constructible sur le corps $\mathbb{Q}[\cos\alpha]$. Or comme $\cos(3x) = 4\cos^3 x - 3\cos x$, alors $2\cos(\alpha/3)$ est racine du polynôme $X^3 - 3X + 2\cos\alpha$ les autres racines étant $\cos(\alpha/3 + 2\pi/3)$ et $\cos(\alpha/3 + 4\pi/3)$. Ainsi α est trisectable si et seulement si $X^3 - 3X + 2\cos\alpha$ est réductible sur $\mathbb{Q}[\cos\alpha]$, i.e. a une racine dans $\mathbb{Q}[\cos\alpha]$.

Considérons par exemple $\alpha = \pi/3$ et donc le polynôme $X^3 - 3X - 1$ et soit $a/b \in \mathbb{Q}$ une éventuelle racine. On obtient après réduction au même dénominateur avec $a \wedge b = 1$: $a^3 - 3a^2b - b^3 = 0$ soit $b = 1$ et $a = \pm 1$ ce qui n'est pas.

Le nombre π étant transcendant, la quadrature du cercle est impossible.

(5) Remarquons déjà que si z est constructible alors tout conjugué z' de z l'est aussi. Soit en effet $\mathbb{Q} \subset K_1 \subset \cdots, \subset K_n$ est tour d'extensions quadratiques avec $z \in K_n$ et soit $L/\mathbb{Q}$ une extension galoisienne de $\mathbb{Q}$ contenant K_n. Il existe alors $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ tel que $\sigma(z) = z'$ et alors $\mathbb{Q} \subset \sigma(K_1) \subset \cdots \subset \sigma(K_n)$ est une tour d'extension quadratiques avec $z' \in \sigma(K_n)$ et z' est donc constructible.

Soit alors L l'extension de $\mathbb{Q}$ engendrée par z et ses conjugués. D'après ce qui précède tout élément de L est constructible. Or d'après le théorème de l'élément primitif on a $L = \mathbb{Q}[\alpha]$ avec donc α constructible de sorte que $[L : \mathbb{Q}]$ est une puissance de 2.

Réciproquement soit $L/\mathbb{Q}$ une extension galoisienne de degré 2^n. Son groupe de Galois est donc d'ordre 2^n de sorte qu'il existe une suite de sous-groupe distingué

$$(0) = G_0 \subset G_1 \subset \cdots \subset G_n = G$$

avec $G_i/G_{i-1} \simeq \mathbb{Z}/2\mathbb{Z}$. On en déduit alors que la tour $\mathbb{Q} = L^{G_n} \subset L^{G_{n-1}} \subset \cdots \subset L^{G_0} = L$ est une tour d'extensions quadratiques.

Remarque: Pour voir l'existence de la suite de composition formée par les G_i, on raisonne par récurrence sur le cardinal de G. Le centre Z de G n'est pas trivial car G est un p-groupe pour $p = 2$. Si $Z \neq G$, on construit à partir d'une suite de composition de Z et de G/Z une pour G. Si $Z = G$, on considère $2G \neq G$ ainsi que $G/2G$ qui est une $\mathbb{Z}/2\mathbb{Z}$-espace vectoriel, et on procède de même.

(6) Notons $\mathcal{C}$ l'ensemble des nombres n tels que $e^{2i\pi/n}$ soit constructible. De manière élémentaire on a les propriétés suivantes:

- si $n \in \mathcal{C}$ alors $2n \in \mathcal{C}$;
- si $n \in \mathcal{C}$ et $m|n$ alors $m \in \mathcal{C}$;
- si $n, m \in \mathcal{C}$ et $n \wedge m = 1$ alors $nm \in \mathcal{C}$ (utiliser une relation de Bezout).

Il nous reste alors à montrer que si p impair appartient à $\mathcal{C}$ alors p est un nombre de Fermat et que pour tout p premier impair $p^2 \notin \mathcal{C}$: cela découle simplement de l'irréductibilité sur $\mathbb{Q}$ des polynômes cyclotomiques: $e^{2i\pi/p}$ (resp. $e^{2i\pi/p^2}$) est de degré $p-1$ (resp. $p(p-1)$) sur $\mathbb{Q}$ de polynôme minimal $\Phi_p(X) = \frac{X^p-1}{X-1}$ (resp. $\Phi_{p^2}(X) = \frac{X^{p^2}-1}{X^p-1}$.

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.*

Preuve : 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.

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.*

Preuve : 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 $L = K$.

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.*

Preuve : 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 $X^2 - 2 - \sqrt{5}$.

Exercice 4. *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.*

Preuve : (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 $\mathbb{Q}$.

Exercice 5. *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.*

Preuve : 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 $\mathbb{Q}(\rho) = \mathbb{Q}(\sqrt{-3})$.

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.*

Preuve : 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.

Exercice 7. *Soit G le groupe de Galois de X^5-2. Quel est le cardinal de G? Est-il abélien, résoluble?*

Preuve : 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

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

Preuve : 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 $\mathrm{d}(\sigma_1,\sigma_2)\in\mathcal{S}_3\times\mathcal{S}_3$ tels que $\epsilon(\sigma_1)=\epsilon(\sigma_2)$ où ϵ désigne la signature.

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

Preuve : 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 $\mathbb{Z}/2\mathbb{Z}$.

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

Preuve : Soit par exemple $x = \sqrt{3} + \sqrt{7}$. On peut par ailleurs trouver son polynôme minimal en procédant comme suit.

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 $Y^4 - 20y^2 + 16$

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?

Preuve : 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 $\mathcal{S}_3$ sur $\mathbb{Q}$. Le groupe de Galois est le groupe produit $D_4 \times D_3$: en effet $E_1 \cap E_2 = \mathbb{Q}$ car la seule autre alternative serait une extension quadratique de $\mathbb{Q}$ (car $2 = 5 \wedge 8$) et $\mathbb{Q}[j]$ (resp. $\mathbb{Q}[i]$) est l'unique sous-extension quadratique de E_2 (resp. E_1) car $\mathcal{A}_3$ (resp. $\mathbb{Z}/2\mathbb{Z}$) est l'unique sous-groupe d'indice 2 de $\mathcal{S}_3$ (resp. D_4).

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

Preuve : On vérifie aisément 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.

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 $\mathbb{Q}[\zeta]$.*

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

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 $(X^2 + 3)(X^5 - 1)$.

Preuve : (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 $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$.

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 $\{\theta, j\theta, j^2\theta\}$ 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 $\mathbb{Q}$.

Preuve : (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.

Exercice 16. *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.*

Preuve : 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.

Exercice 17. *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 ?

Preuve :

(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.

Exercice 18. *Montrez en réduisant modulo 2 et 3, que le groupe de Galois G de $X^5 - X - 1$ est $\mathcal{S}_5$.*

Preuve : $X^5 - X - 1$ 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 $(12\cdots n)$.

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 $\mathbb{Q}$.

Preuve : (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.

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.

Preuve : (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.

Exercice 21. *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 $\mathbb{Q}$ 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 $\mathbb{Q}(\sqrt{-7})$.