Théorie des Nombres - TD7
Extensions de corps

Exercice 1 :

a) Soit $x \in \mathbb{R}$ tel qu'il existe une constante $K > 0$ et une suite de rationnels $(\frac{p_n}{q_n})_{n\in\mathbb{N}}$ deux-à-deux distincts tels que $|x - \frac{p_n}{q_n}| \leq \frac{K}{q_n^n}$. Montrer que x est transcendant (sur $\mathbb{Q}$).

b) Soit $(a_n)_{n\in\mathbb{N}}$ une suite bornée d'entiers relatifs, telle que $a_n \neq 0$ pour une infinité de n. Soit $b \in \mathbb{N}$, $b \geq 2$. On définit $\theta := \sum_{n\geq 0} \frac{a_n}{b^{n!}}$. Montrer que θ est transcendant.

c) En déduire qu'il existe une famille explicite non dénombrable de nombres transcendants.

Solution de l'exercice 1.

a) Supposons x algébrique (sur $\mathbb{Q}$). Alors il existe un polynôme $P(X) = a_d X^d + \cdots + a_0 \in \mathbb{Z}[X]$ tel que $P(x) = 0$. Puisque P n'a qu'un nombre fini de racines, il existe $\epsilon > 0$ tel que P ne s'annule pas sur $[x - \epsilon; x + \epsilon] \setminus \{x\}$. Donc si $\frac{p}{q} \neq x \in \mathbb{Q} \cap [x - \epsilon; x + \epsilon]$, $P(\frac{p}{q}) \neq 0$, donc

$$|P(\frac{p}{q})| = \left|\frac{a_d p^d + a_{d-1}p^{d-1}q + \ldots a_0 q^d}{q^d}\right| \neq 0\,.$$

Or le numérateur de cette fraction est un entier non nul, donc

$$|P(\frac{p}{q})| \geq \frac{1}{q^d}\,.$$

En outre, le théorème des accroissements finis assure qu'il existe $M \in \mathbb{R}$ tel que pour $\frac{p}{q} \in \mathbb{Q} \cap [x - \epsilon; x + \epsilon]$,

$$|P(\frac{p}{q})| = |P(\frac{p}{q}) - P(x)| \leq M|x - \frac{p}{q}|\,.$$

Donc finalement pour $\frac{p}{q} \neq x \in \mathbb{Q} \cap [x - \epsilon; x + \epsilon]$, $\frac{1}{Mq^d} \leq |x - \frac{p}{q}|$. Or la suite $(\frac{p_n}{q_n})$ converge vers x, donc pour tout n assez grand, on a

$$\frac{1}{Mq_n^d} \leq |x - \frac{p_n}{q_n}| \leq \frac{K}{q_n^n}\,.$$

Ceci est contradictoire puisque (q_n) tend vers l'infini. Donc on en déduit que x n'est pas algébrique, donc x est transcendant.

b) Notons $A := \max\{|a_n|, n \in \mathbb{N}\}$. Soit $N \in \mathbb{N}$ tel que $a_N \neq 0$. Posons $p_N := \sum_{n=0}^{N} a_n b^{N!-n!}$ et $q_N := b^{N!}$. Alors $\theta - \frac{p_N}{q_N} = \sum_{j=1}^{\infty} \frac{a_{N+j}}{b^{(N+j)!}}$. Or pout tout $j \geq 2$, on a $(N + j)! - (N + 1)! \geq j$, donc

$$\left|\sum_{j=1}^{\infty} \frac{a_{N+j}}{b^{(N+j)!}}\right| \leq \frac{A}{b^{(N+1)!}} \sum_{j\geq 0} \frac{1}{b^j} \leq \frac{A(1 - \frac{1}{b})}{b^{(N+1)!}}\,.$$

Donc

$$\left|\theta - \frac{p_N}{q_N}\right| \leq \frac{A(1 - \frac{1}{b})}{b^{(N+1)!}} = \frac{A(1 - \frac{1}{b})}{q_N^{N+1}} \leq \frac{A(1 - \frac{1}{b})}{q_N^N}\,.$$

On conclut alors avec la question précédente que x est transcendant.

c) Grâce à la question précédente, il suffit de remarquer que l'ensemble des suites bornées d'entiers relatifs à support infini est non dénombrable, ce qui est clair puisque l'ensemble $\{1, 2\}^{\mathbb{N}}$ est déjà non dénombrable.

Exercice 2 : Soit K un corps de caractéristique différente de 2, et $a, b \in K^*$.
Montrer que $K(\sqrt{a}) = K(\sqrt{b})$ si et seulement si $\frac{a}{b} \in (K^*)^2$.
Que se passe-t-il en caractéristique 2 ?

Solution de l'exercice 2.
- On suppose que $\frac{a}{b} \in (K^*)^2$. Alors il existe $x \in K^*$ tel que $b = x^2 a$. Alors $\sqrt{b} = \pm x\sqrt{a}$. Donc il est clair que $K(\sqrt{a}) = K(\sqrt{b})$.
- On suppose que $K(\sqrt{a}) = K(\sqrt{b})$. Alors il existe $x, y \in K$ tels que $\sqrt{b} = x + y\sqrt{a}$. On a donc $\sqrt{b} - x = y\sqrt{a}$, donc en élevant au carré, on a $b - 2x\sqrt{b} + x^2 = ay^2$. Donc $2x\sqrt{b} = b + x^2 - ay^2$. On a donc deux cas possibles : soit $\sqrt{b} \in K$, auquel cas $\sqrt{a} \in K$ et le résultat est évident. Soit $\sqrt{b} \notin K$, alors $2x\sqrt{b} = 0$, donc $x = 0$ (car $2 \in K^*$), donc $\sqrt{a} = y\sqrt{b}$, $y \in K$, ce qui conclut.
- Remarquons qu'en caractéristique 2, l'implication de la gauche vers la droite n'est pas vérifiée en général : par exemple, considérer $K = \mathbb{F}_2(T^2)$, $a = T^2$ et $b = 1+T^2$. Alors $K(\sqrt{a}) = K(\sqrt{b}) = \mathbb{F}_2(T)$, alors que $\frac{b}{a} = 1 + \frac{1}{T^2}$ n'est pas un carré dans K (puisque T^2 n'est pas un carré dans K).

Exercice 3 : Montrer que pour tout $b, c \in \mathbb{R}$ tels que $b^2 < 4c$, si $P = X^2 + bX + c$, alors on a un isomorphisme de corps

$$\mathbb{R}[X]/(P) \cong \mathbb{C}\,.$$

Cet isomorphisme est-il canonique ?

Solution de l'exercice 3. L'hypothèse $b^2 < 4c$ assure que le discriminant de P est négatif, donc P n'a pas de racine réelle, donc P est irréductible dans $\mathbb{R}[X]$. Donc $\mathbb{R}[X]/(P)$ est un corps de rupture de P, i.e. $\mathbb{R}[X]/(P) \cong \mathbb{R}[\alpha]$, où $\alpha \in \mathbb{C}$ est une racine de P. Par conséquent, le morphisme canonique de $\mathbb{R}$-algèbre $\phi : \mathbb{R}[X] \to \mathbb{C}$ qui envoie X sur α (et donc $Q(X) \in \mathbb{R}[X]$ sur $Q(\alpha)$) se factorise en un morphisme de corps (injectif) :

$$\mathbb{R}[X]/(P) \to \mathbb{C}\,.$$

Or les deux corps sont des extensions de degré 2 de $\mathbb{R}$, donc c'est un isomorphisme. Cet isomorphisme n'est pas canonique, puisqu'il nécessite le choix d'une racine α de P. Un autre choix conduirait à l'isomorphisme induit par $X \mapsto \overline{\alpha}$.

Exercice 4 : Soit K un corps et x algébrique sur K, de degré impair. Montrer que x^2 est algébrique sur K et que $K(x^2) = K(x)$.

Solution de l'exercice 4. Il est clair que $K(x^2) \subset K(x)$, donc x^2 est algébrique sur K. En outre, x est annulé par le polynôme $X^2 - x^2$ à coefficients dans $K(x^2)$. Donc x est de degré au plus 2 sur $K(x^2)$, i.e. $[K(x) : K(x^2)] = 1$ ou 2. Or par multiplicativité des degrés, on a $[K(x) : K] = [K(x) : K(x^2)][K(x^2) : K]$ et $[K(x) : K]$ est impair par hypothèse, donc $[K(x) : K(x^2)] = 1$, i.e. $K(x^2) = K(x)$.

Exercice 5 : Soit L/K une extension finie de corps de degré m. Soit $P \in K[X]$ un polynôme irréductible de degré d premier à m. Montrer que P est irréductible dans $L[X]$.

Solution de l'exercice 5. On considère un facteur irréductible Q de P dans $L[X]$, et M un corps de rupture de Q sur L, i.e. $M = L(x)$ avec x racine de Q. On a alors les inclusions suivantes : $K \subset L \subset M = L(x)$ et $K \subset K(x) \subset M = L(x)$. En outre, $K(x)$ est un corps de rupture de P sur K, donc $[K(x) : K] = d$. Par multiplicativité des degrés, on obtient $\deg(Q)m = [M : L][L : K] = [M : K] = [M : K(x)][K(x) : K] = [M : K(x)]d$. Donc d divise $m\deg(Q)$. Or d et m sont premiers entre eux, donc d divise $\deg(Q)$, donc $d = \deg(Q)$, donc $P = Q$, donc P est irréductible sur L.

Exercice 6 :

a) Soient $d_1, \ldots, d_r \in \mathbb{N}$. Montrer que $d_1! \ldots d_r!$ divise $(d_1 + \cdots + d_r)!$.

b) Si K est un corps et $f \in K[X]$ de degré d, montrer que le degré d'une extension de décomposition de f divise $d!$.

Solution de l'exercice 6.

a) On peut montrer ce résultat de diverses manières. Voici une façon de le démontrer : on montre par récurrence sur r que le quotient $\frac{(d_1+\cdots+d_r)!}{d_1!\ldots d_r!}$ est égal au nombre $C(d_1,\ldots,d_r)$ de façons de partitionner un ensemble de $d_1+\cdots+d_r$ éléments en r sous-ensembles (disjoints) de cardinaux respectifs $d_1,\ldots,d_r$. Pour $r=1$, c'est évident. Pour $r=2$, c'est l'interprétation combinatoire du coefficient binomial. Supposons le résultat connu pour r et montrons le pour $r+1$. On a clairement $C(d_1,\ldots,d_{r+1}) = \binom{d_1+\cdots+d_{r+1}}{d_{r+1}} C(d_1,\ldots,d_r)$ (se donner une partition en $r+1$ sous-ensembles de cardinaux $d_1,\ldots,d_{r+1}$ revient à choisir d_{r+1} élément parmi $d_1+\cdots+d_{r+1}$ puis une partition en r sous-ensembles de cardinaux $d_1,\ldots,d_r$ des $d_1+\cdots+d_r$ éléments restants). Alors l'hypothèse de réccurrence assure que $C(d_1,\ldots,d_{r+1}) = \binom{d_1+\cdots+d_{r+1}}{d_{r+1}} \frac{(d_1+\cdots+d_r)!}{d_1!\ldots d_r!} = \frac{(d_1+\cdots+d_{r+1})!}{d_1!\ldots d_{r+1}!}$. Cela conclut la preuve.

b) Soit $P_1 \in K[X]$ un facteur irréductible de f. Notons d_1 le degré de P_1 et K_1 un corps de décomposition de P_1 sur K. On construit alors par récurrence des polynômes P_i et des corps K_i tels que P_{i+1} est un facteur irréductible, de degré d_{i+1}, du polynôme $\frac{f}{P_1\ldots P_i}$ dans $K_i[X]$, et K_{i+1} est un corps de décomposition de P_{i+1} sur K_i. Alors par construction, il existe un entier r tel que K_r soit un corps de décomposition de f, et tel que $d_1+\cdots+d_r = d$.

Supposons que l'on sache montrer le résultat souhaité pour un polynôme f irréductible, alors on sait que $[K_{i+1}:K_i]$ divise $d_i!$. Donc $[K_r:K] = \prod_{i=0}^{r-1}[K_{i+1}:K_i]$ divise $d_1!\ldots d_r!$. Donc la question a) assure que $[K_r:K]$ divise $d! = (d_1+\cdots+d_r)!$, d'où le résultat pour f.

Il suffit donc de se limiter au cas où f est irréductible dans $K[X]$, de degré d. On traite ce cas par récurrence sur le degré. Dans ce cas, on considère un corps de rupture L/K de f et $\alpha \in L$ une racine de f. Alors $[L:K]=d$ et on pose $g(X) := \frac{f(X)}{X-\alpha} \in L[X]$. Puisque $\deg(g) = d-1$, on sait par récurrence (en utilisant le raisonnement précédent pour se ramener au cas des facteurs irréductibles successifs de g) que si K' désigne un corps de décomposition de g sur L, alors $[K':L]$ divise $(d-1)!$. Donc $[K':K] = [K':L][L:K]$ divise $d(d-1)! = d!$. Or il est clair que K' est un corps de décomposition de f sur K, donc on a bien montré que le degré d'un corps de décomposition de f sur K divisait $d!$.

Exercice 7 : Soit k un corps de caractéristique $p>0$. Soit $a \in k$.
Montrer que le polynôme $X^p - X - a \in k[X]$ est scindé ou irréductible.

Solution de l'exercice 7. Remarquons d'abord que si l'on note $P(X) = X^p - X - a$, alors on a $P(X+1) = P(X) \in k[X]$.
Supposons d'abord que $P(X)$ ait une racine $\alpha \in k$. Alors pour tout entier $0 \leq n \leq p-1$, $\alpha+n \in k$ est racine de P grâce à la remarque précédente. Or les $\alpha+n$, n variant entre 0 et $p-1$, sont deux-à-deux distincts, donc le polynome $P(X)$ admet p racines distinctes dans k. Or il est de degré p, donc il est scindé sur k.
Supposons maintenant que $P(X)$ soit réductible dans $k[X]$. Alors $P = QR$, où $Q, R \in k[X]$ sont des polynômes unitaires de degrés respectifs $q, r \geq 1$. Notons α une racine de Q (dans un corps de décompostion de Q). Comme remarqué plus haut, les racines de Q sont de la forme $\alpha+n_i$, où $0 \leq n_i \leq p-1$. Par conséquent, le coefficient de degré $q-1$ de Q s'écrit $-\sum_{i=1}^{q}(\alpha+n_i) = -q\alpha - \sum_{i=1}^{q} n_i$. Ce nombre est dans k, or $\sum_{i=1}^{q} n_i \in k$, donc $q\alpha \in k$, donc $\alpha \in k$ car $1 \leq q < p$. Donc P a une racine dans k, ce qui conclut la preuve.

Exercice 8 :

a) Montrer que pour tout $n \geq 1$, pour $p_1,\ldots,p_n$ nombres premiers distincts, l'extension $\mathbb{Q}[\sqrt{p_1},\ldots,\sqrt{p_n}]/\mathbb{Q}$ est de degré 2^n.

[Indication : on pourra montrer le même résultat pour $p_1,\ldots,p_n$ deux-à-deux premiers entre eux et sans facteurs carrés (pas forcément premiers)].

b) En déduire que la famille $(\sqrt{p_n})_{n\in\mathbb{N}}$ des racines carrées des nombres premiers est libre sur $\mathbb{Q}$.

c) Plus généralement, montrer que la famille des racines carrées des entiers naturels sans facteur carré est libre sur $\mathbb{Q}$.

Solution de l'exercice 8.

a) On raisonne par récurrence sur le nombre n de nombres premiers. On montre en fait un résultat un peu plus fort (par récurrence) : pour tout $n \geq 1$, pour $p_1, \ldots, p_n$ entiers distincts sans facteur carré et deux-à-deux premiers entre eux, l'extension $\mathbb{Q}[\sqrt{p_1}, \ldots, \sqrt{p_n}]/\mathbb{Q}$ est de degré 2^n.
   - pour $n = 1$, il est clair que l'extension $\mathbb{Q}[\sqrt{p_1}]/\mathbb{Q}$ est de degré 2.
   - pour $n > 1$: soient $p_1, \ldots, p_n$ n entiers distincts deux-à-deux premiers entre eux et sans facteur carré. Supposons l'extension $\mathbb{Q}[\sqrt{p_1}, \ldots, \sqrt{p_n}]/\mathbb{Q}[\sqrt{p_1}, \ldots, \sqrt{p_{n-1}}]$ triviale. En utilisant l'exercice 2 et l'hypothèse de récurrence (appliquée à $p_1, \ldots, p_{n-1}$ et $p_1, \ldots, p_{n-2}, p_n$), il existe $x \in \mathbb{Q}[\sqrt{p_1}, \ldots, \sqrt{p_{n-2}}]$ tel que $p_n = x^2 p_{n-1}$. Alors $\sqrt{p_{n-1}p_n} \in \mathbb{Q}[\sqrt{p_1}, \ldots, \sqrt{p_{n-2}}]$. Cela contredit l'hypothèse de récurrence appliquée aux $n-1$ entiers $p_1, \ldots, p_{n-2}, p_{n-1}p_n$. Cela conclut la preuve.

b) C'est une conséquence immédiate de la question précédente.

c) On montre le fait suivant par récurrence sur n : si $p_1, \ldots, p_n$ sont n entiers sans facteur carré deux-à-deux premiers entre eux, alors la famille $(1, \sqrt{p_1}, \sqrt{p_2}, \sqrt{p_1p_2}, \ldots, \sqrt{p_1 \ldots p_n})$, formée des racines de tous les produits possibles de nombres choisis parmi les p_i, est libre sur $\mathbb{Q}$.

   On propose deux preuves de ce fait.
   - Preuve utilisant la première question : on montre en fait que la famille $(1, \sqrt{p_1}, \sqrt{p_2}, \sqrt{p_1p_2}, \ldots, \sqrt{p_1 \ldots p_n})$ est une base de $\mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_n})$ sur $\mathbb{Q}$. Puisque cette famille est formée de 2^n éléments, la première question assure qu'il suffit de montrer qu'elle est génératrice. Et ceci est évident par récurrence sur n.
   - Preuve directe : pour $n = 1$, la propriété est claire. Montrons l'hérédité : soient $n > 1$ et $p_1, \ldots, p_n$ des entiers sans facteur carré deux-à-deux premiers entre eux. Supposons la famille $(1, \sqrt{p_1}, \sqrt{p_2}, \sqrt{p_1p_2}, \ldots, \sqrt{p_1 \ldots p_n})$ liée : alors il existe une relation linéaire non triviale entre ces nombres. Quitte à séparer les éléments de cette famille faisant intervenir un facteur $\sqrt{p_n}$ des autres, cette relation s'écrit $\alpha + \beta\sqrt{p_n} = 0$, avec $\alpha, \beta \in \mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_{n-1}})$. Par hypothèse de récurrence, le terme β est non nul. On en déduit donc que $\sqrt{p_n} \in \mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_{n-1}})$, donc $\sqrt{p_n}$ s'écrit sous la forme $\sqrt{p_n} = a + b\sqrt{p_{n-1}}$, avec $a, b \in \mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_{n-2}})$. On élève au carré, il reste $p_n = a^2 + b^2 p_{n-1} + 2ab\sqrt{p_{n-1}}$. Par l'hypothèse de récurrence appliquée à $(p_1, \ldots, p_{n-1})$, cette relation implique que $ab = 0$. Si $a = 0$, alors $p := p_{n-1}p_n$ est un carré dans $\mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_{n-2}})$. Si $b = 0$, alors $p := p_{n-1}$ est un carré dans $\mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_{n-2}})$. Dans les deux cas, on a donc un entier p sans facteur carré, premier à tous les p_i ($1 \leq i \leq n-2$) et tel que la famille $(1, \sqrt{p_1}, \sqrt{p_2}, \sqrt{p_1p_2}, \ldots, \sqrt{p_1 \ldots p_{n-2}p})$ soit liée. Cela contredit l'hypothèse de récurrence appliquée aux $n-1$ entiers $(p_1, \ldots, p_{n-2}, p)$. Par conséquent, la famille $(1, \sqrt{p_1}, \sqrt{p_2}, \sqrt{p_1p_2}, \ldots, \sqrt{p_1 \ldots p_n})$ est libre sur $\mathbb{Q}$.

   Il est alors clair que la propriété démontrée répond à la question, puisque toute famille finie de racines carrées d'entiers sans facteur carré est contenue dans une famille de la forme précédente, à savoir $(1, \sqrt{p_1}, \sqrt{p_2}, \sqrt{p_1p_2}, \ldots, \sqrt{p_1 \ldots p_n})$ où les p_i sont sans facteurs carrés et deux-à-deux premiers entre eux (on peut même supposer les p_i premiers et deux-à-deux distincts).

Exercice 9 : Soit K un corps. Soient $P = a_n X^n + \cdots + a_0$ et $Q = b_m X^m + \cdots + b_0$ deux polynômes à coefficients dans K, de degrés respectifs n et m. On définit le résultant $\mathrm{Res}(P, Q)$ de P et Q comme

le déterminant de la matrice de taille $m+n$

$$\begin{pmatrix} a_n & 0 & \dots & 0 & b_m & 0 & \dots & 0 \\ a_{n-1} & a_n & \ddots & \vdots & b_{m-1} & b_m & \ddots & \vdots \\ \vdots & a_{n-1} & \ddots & 0 & \vdots & b_{m-1} & \ddots & 0 \\ a_0 & \vdots & \ddots & a_n & b_0 & \vdots & \ddots & b_m \\ 0 & a_0 & & a_{n-1} & 0 & b_0 & & b_{m-1} \\ \vdots & \ddots & \ddots & \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & \dots & 0 & a_0 & 0 & \dots & 0 & b_0 \end{pmatrix}.$$

a) Montrer que $\mathrm{Res}(P,Q)$ est le déterminant de l'application linéaire $(A,B) \mapsto AP+BQ$ entre des espaces vectoriels de polynômes que l'on précisera.

b) En déduire que $\mathrm{Res}(P,Q)=0$ si et seulement si P et Q ne sont pas premiers entre eux.

c) Application : trouver un élément primitif pour l'extension $\mathbb{Q}[\sqrt{2},\sqrt{3}]$, ainsi que son polynôme minimal. Mêmes questions pour l'extension $\mathbb{Q}[\sqrt{p},\sqrt{q}]$ où p et q sont des nombres premiers distincts.

Solution de l'exercice 9.

a) On considère l'application linéaire $\varphi : K[X]_{m-1} \times K[X]_{n-1} \to K[X]_{m+n-1}$ définie par $\varphi(A,B) := AP+BQ$, où $K[X]_d$ désigne le K-espace vectoriel des polynômes à coefficients dans K et de degré $\leq d$. On munit l'espace vectoriel $K[X]_{m-1} \times K[X]_{n-1}$ de la base

$$((X^{m-1},0),\dots,(X,0),(1,0),(0,X^{n-1}),\dots,(0,X),(0,1))$$

et l'espace vectoriel $K[X]_{m+n-1}$ de la base $(X^{m+n-1},\dots,X,1)$. On voit alors immédiatement que dans ces bases, la matrice de φ est exactement celle définie plus haut.

b) Grâce à la question précédente, $\mathrm{Res}(P,Q)=0$ si et seulement si φ n'est pas injective.

Supposons que P et Q ne soient pas premiers entre eux : il existe alors $R,S,T \in K[X]$ polynômes non constants tels que $P=RS$ et $Q=RT$. Alors on a $TP+(-S)Q=0$, i.e. $\varphi(T,-S)=0$, donc φ n'est pas injective.

Réciproquement, supposons que φ ne soit pas injective. Alors il existe $(A,B) \in \mathrm{Ker}(\varphi) \setminus \{0\}$: $AP+BQ=0$, i.e. $AP=-BQ$. Puisque le degré de A est strictement inférieur à celui de Q, Q ne divise pas A. Divisons A et Q par leur PGCD, on obtient alors $\widetilde{A}P=-B\widetilde{Q}$, avec $\widetilde{Q}$ non constant, divisant Q et premier à $\widetilde{A}$. Fixons alors $f \in K[X]$ un facteur irréductible de $\widetilde{Q}$. Alors f divise $\widetilde{A}P$ et ne divise pas $\widetilde{A}$. Donc f divise P, i.e. f est un facteur commun à P et Q dans $K[X]$.

c) L'extension $\mathbb{Q}[\sqrt{2},\sqrt{3}]/\mathbb{Q}$ est clairement de degré 4. Cette extension est galoisienne (c'est un corps de décomposition de $(X^2-2)(X^2-3)$ sur $\mathbb{Q}$), de groupe de Galois $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. L'action du groupe de Galois sur les générateurs est la suivante : $(1,0).\sqrt{2}=-\sqrt{2}$, $(1,0).\sqrt{3}=\sqrt{3}$, $(0,1).\sqrt{2}=\sqrt{2}$, $(0,1).\sqrt{3}=-\sqrt{3}$. En particulier, l'élément $\alpha := \sqrt{2}+\sqrt{3} \in \mathbb{Q}[\sqrt{2},\sqrt{3}]$ a ses quatre conjugués distincts, donc $\mathbb{Q}(\alpha)=\mathbb{Q}[\sqrt{2},\sqrt{3}]$. Par conséquent, $\alpha=\sqrt{2}+\sqrt{3}$ est un élément minimal.

Calculons son polynôme minimal avec la méthode du résultant : la question précédente assure que si $P,Q \in \mathbb{Q}[X]$, le résultant des polynômes $P(X), Q(Y-X) \in \mathbb{Q}(Y)[X]$ est un polynôme dans $\mathbb{Q}[Y]$ dont les racines $y \in \overline{\mathbb{Q}}$ sont exactement les x_1+x_2, où x_1 est une racine de P et x_2 est une racine de Q dans $\overline{\mathbb{Q}}$. Ainsi les quatre racines de $R(Y) := \mathrm{Res}(X^2-2,(Y-X)^2-3) \in \mathbb{Q}[Y]$ sont-elles exactement les quatre conjugués de α : $\pm\sqrt{2}\pm\sqrt{3}$. La calcul explicite donne ici :

$$R(Y) = \begin{vmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & -2Y & 1 \\ -2 & 0 & Y^2-3 & -2Y \\ 0 & -2 & 0 & Y^2-3 \end{vmatrix} = Y^4-10Y^2+1\,.$$

Ce polynôme annule α, il est unitaire et de degré 4, c'est donc le polynôme minimal de α sur $\mathbb{Q}$. En général, pour $\mathbb{Q}[\sqrt{p}, \sqrt{q}]$, le même raisonnement montre qu'un élément primitif est $\sqrt{p} + \sqrt{q}$ et que son polynôme minimal est

$$P(X) = X^4 - 2(p+q)X^2 + (p-q)^2 \in \mathbb{Q}[X]\,.$$

Exercice 10 : Soit L/K une extension algébrique de corps.

a) On suppose que $L = K(x)$, pour un $x \in L$. On note P le polynôme minimal de x sur K.
   i) Soit une extension intermédiaire $K \subset M \subset L$. Montrer qu'il existe un facteur unitaire Q de P dans $L[X]$ tel que M soit le corps engendré sur K par les coefficients de Q.
   ii) En déduire que L/K n'a qu'un nombre fini de sous-extensions.

b) On suppose que L/K n'a qu'un nombre fini de sous-extensions.
   i) Montrer que L/K est finie.
   ii) Montrer que si K est un corps fini, alors il existe $x \in L$ tel que $L = K(x)$.
   iii) On suppose K infini. Montrer que pour tout $x, y \in L$, il existe $\lambda \in K$ tel que $K(x,y) = K(x + \lambda y)$. En déduire qu'il existe $x' \in L$ tel que $L = K(x')$.

Solution de l'exercice 10.

a) i) On remarque que l'extension L/M est engendrée par x, i.e. $L = M(x)$. Notons Q le polynôme minimal de x sur M. Alors Q divise P dans $M[X]$, donc en particulier Q est un facteur unitaire de P dans $L[X]$. Il est alors clair que M est engendré sur K par les coefficients de Q.

   ii) Dans $L[X]$, le polynôme P n'admet qu'un nombre fini de facteurs unitaires (puisque dans une clôture algébrique fixée $\overline{L}$ de L, P se décompose en produit de $X - x_i$, $x_i \in \overline{L}$, et tout facteur unitaire de P dans $L[X]$ est un produit de certains de ces $X - x_i$). Par conséquent, la question précédente assure que L/K n'a qu'un nombre fini de sous-extensions.

b) i) Supposons L/K infinie. On choisit $x \in L \setminus K$. Puisque x est algébrique sur K, l'extension $L/K(x)$ est infinie (car $K(x)$ est une extension finie de K), donc on conclut par récurrence à l'existence d'une tour infinie d'extensions intermédiaires. Cela contredit l'hypothèse de finitude du nombre d'extensions intermédiaires. Par conséquent, L/K est finie.

   ii) Si K est un corps fini, L est aussi un corps fini, et on sait alors que le groupe L^* est cyclique. On choisit un générateur $x \in L^*$ de ce groupe. Il est alors clair que $L = K(x)$.

   iii) Si K est infini et $x, y \in L$, alors quand λ décrit K, les extensions intermédiaires $K(x + \lambda y)$ ne peuvent être deux-à-deux distinctes. Donc il existe $\lambda \neq \mu \in K$ tels que $K(x + \lambda y) = K(x + \mu y)$. En particulier, $(x + \lambda y) - (x - \mu u) \in K(x + \lambda y)$, i.e. $(\lambda - \mu)y \in K(x + \lambda y)$, donc $y \in K(x + \lambda y)$, donc $x \in K(x + \lambda y)$. Finalement, on a bien $K(x,y) \subset K(x + \lambda y)$.
   L'extension L/K est finie, donc de type finie : il existe $x_1, \ldots, x_n \in L$ tels que $L = K(x_1, \ldots, x_n)$. On applique alors la première partie de la question (par récurrence) pour en déduire qu'il existe $\lambda_2, \ldots, \lambda_n \in K$ tels que $L = K(x_1 + \lambda_2 x_2 + \cdots + \lambda_n x_n)$, ce qui conclut.

Exercice 11 : Soit k un corps. Soit $q(X_1, \ldots, X_n) \in k[X_1, \ldots, X_n]$ une forme quadratique (un polynôme homogène de degré 2). On suppose que q admet un zéro non trivial dans une extension K/k de degré impair de k. L'objectif est de montrer que q a un zéro non trivial dans k (théorème de Springer).

a) Montrer que l'on peut supposer $K = k[\alpha]$ monogène de degré $d > 1$ impair.

b) Si f est le polynôme minimal de α sur k, montrer qu'il existe $g_1, \ldots, g_n \in k[X]$ de degrés $< d$, premiers entre eux dans leur ensemble, tels que f divise $q(g_1(X), \ldots, g_n(X))$ dans $k[X]$.

c) En déduire l'existence d'une extension K'/k de degré impair $< d$ telle que q a un zéro non trivial dans K'.

d) Conclure.

e) Que dire d'un polynôme homogène de degré 3 admettant un zéro non trivial dans une extension de degré 2 ?

Solution de l'exercice 11.

a) L'extension K/k est finie, donc de type fini. Il existe donc une tour finie d'extensions intermédiaires

$$k = k_0 \subset k_1 \subset \cdots \subset k_{n-1} \subset k_n = K$$

telle que k_{i+1}/k_i soit monogène pour tout i. La formule de multiplicativité des degrés assure alors que pour tout i, $[k_{i+1} : k_i]$ est impair. Par récurrence, on peut donc supposer K/k monogène. Et si $d = 1$, la conclusion est immédiate.

b) On note $(x_1, \ldots, x_n)$ une solution non triviale de $q(X_1, \ldots, X_n) = 0$ dans K^n. Puisque $K \cong k[X]/(f)$, il existe des polynômes $h_i \in k[X]$ de degrés $< d = \deg(f)$ tels que pour tout i, $x_i = h_i(\alpha)$. On a alors $q(h_1(\alpha), \ldots, h_n(\alpha)) = 0$. Puisque q est homogène et les $x_i = h_i(\alpha)$ non tous nuls, si on définit les polynômes g_i comme les quotients des h_i par le PGCD de $(h_1, \ldots, h_n)$, on dispose alors de polynômes $g_i(X)$ premiers entre eux dans leur ensemble tels que $q(g_1(\alpha), \ldots, g_n(\alpha)) = 0$. Par conséquent le polynôme $q(g_1(X), \ldots, g_n(X)) \in k[X]$ annule α, donc il est divisible par f.

c) Par la question précédente, on peut écrire

$$q(g_1(X), \ldots, g_n(X)) = fh \in k[X]\,.$$

Calculons le degré de h. On sait que $\deg(f) = d$. On note $m < d$ le degré maximal des g_i. Il est clair que $q(g_1(X), \ldots, g_n(X))$ est de degré au plus $2m$. Le coefficient de degré $2m$ de ce polynôme est de la forme $q(a_{1,m}, \ldots, a_{n,m})$, où $a_{i,m}$ est le coefficient (éventuellement nul) de degré m dans $g_i(X)$. Par définition de m, le n-uplet $(a_{1,m}, \ldots, a_{n,m})$ n'est pas nul, donc on a l'alternative suivante : soit $q(a_{1,m}, \ldots, a_{n,m}) = 0$, auquel cas il suffit de prendre $K' = k$. Soit $q(a_{1,m}, \ldots, a_{n,m}) \neq 0$, alors $q(g_1(X), \ldots, g_n(X))$ est de degré exactement $2m$. Donc h est de degré $2m - d$, qui est un nombre impair strictement inférieur à d. Il existe donc un facteur irréductible $P \in k[X]$ de h qui soit de degré impair d'. Considérons le corps $K' := k[X]/(P)$, extension de degré $d' < d$ impair de k. Montrons que q a un zéro non trivial dans K'. Par construction, si on note $\overline{X}$ la classe de X dans K', on a $q(g_1(\overline{X}), \ldots, g_n(\overline{X})) = 0$. Si tous les $g_i(\overline{X})$ sont nuls, cela implique que $P(X)$ divise tous les $g_i(X)$ dans $k[X]$, ce qui est exclu. Par conséquent, le n-uplet $(g_1(\overline{X}), \ldots, g_n(\overline{X})$ est non nul, ce qui termine cette question.

d) Par récurrence sur le degré (impair) de l'extension K, on conclut que q a un zéro non trivial dans k^n. Cela termine la preuve.

e) Dans ce cas, le même raisonnement que précédemment permet de se ramener à un polynôme de degré 3 en une variable admettant une racine dans une extension de degré 2. Or on sait qu'un tel polynôme admet une racine dans le corps de base, ce qui permet de conclure que le polynôme homogène initial admet une racine non triviale dans k^n.