Théorie des Nombres - TD2
Extensions algébriques de corps

Exercice 0 :

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 irrationnel.

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

Solution de l'exercice 0.

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

$$\left|\sum_{j=2}^{\infty} \frac{a_{N+j}}{b^{(N+j)!}}\right| \leq \frac{A}{b^{(N+1)!}} \sum_{j\geq 2} \frac{1}{b^{N+j}} \leq \frac{A}{b^{(N+1)!}b^N}\,.$$

Or on a $\frac{A}{b^{(N+1)!}b^N} \leq \frac{A}{b^{(N+1)!}}$, donc

$$\left|\theta - \frac{p_N}{q_N}\right| \leq \frac{2A}{b^{(N+1)!}} = \frac{2A}{q_N^{N+1}} \leq \frac{2A}{q_N^N}\,.$$

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 1 : 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 $\frac{a}{b} \in (K^*)^2$.

Solution de l'exercice 1.
- 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 2 : 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 2. 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 définition, $\mathbb{C}$ est un corps de rupture de $X^2 + 1$ sur $\mathbb{R}$. Par conséquent, il existe un isomorphisme de corps (au-dessus de $\mathbb{R}$)

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

défini par $\alpha \mapsto i$. Cet isomorphisme n'est pas canonique puisqu'il nécessite le choix d'une racine de P. Un autre choix conduirait à l'isomorphisme $\alpha \mapsto -i$.

Exercice 3 : Soit p un nombre premier, k un corps de caractéristique p. On définit

$$k^p := \{x^p, x \in k\}\,.$$

Montrer que k^p est un sous-corps de k et que l'extension k/k^p est normale. Est-elle séparable ?

Solution de l'exercice 3.
- Montrons que k^p est un sous-corps : k^p est clairement stable par produit, et aussi par somme puisque en caractéristique p, pour tout $x, y \in k$, $(x+y)^p = x^p + y^p$. La stabilité par inverse est claire. Enfin, k^p contient bien les éléments 0 et 1.
- Pour montrer que l'extension k/k^p est normale, il suffit de montrer que pour tout $x \in k$, le polynôme minimal de x sur k^p est scindé sur k. Or il est clair que x est racine du polynôme $X^p - x^p \in k^p[X]$, et on a l'égalité suivante dans $k[X]$ qui assure que ce polynôme est scindé dans $k[X]$:

$$X^p - x^p = (X - x)^p\,.$$

- Concernant la séparabilité, on remarque que pour tout $x \in k$, le polynôme minimal de x sur k^p divise $X^p - x^p$. Par conséquent, ce polynôme minimal est séparable si et seulement si il est égal à $X - x$, i.e. si et seulement si $x \in k^p$. Finalement, l'extension k/k^p est séparable si et seulement si elle est triviale, i.e. si et seulement si tout élément de k a une racine p-ième dans k.

Exercice 4 : On considère le polynôme suivant à coefficients entiers : $Q = X^9 + 9X^8 - X^3 + 3X^2 - 3X + 11$.

a) Décomposer la réduction de Q dans $\mathbb{F}_2[X]$ en facteurs irréductibles.

b) Décomposer la réduction de Q dans $\mathbb{F}_3[X]$ en facteurs irréductibles.

c) En déduire que Q est irréductible dans $\mathbb{Q}[X]$.

Solution de l'exercice 4.

a) Dans $\mathbb{F}_2[X]$, la réduction Q_2 de Q s'écrit $Q_2(X) = X^9 + X^8 + X^3 + X^2 + X + 1$. On remarque que 1 est racine de Q_2 dans $\mathbb{F}_2$. Donc $X + 1$ divise Q_2 et on vérifie que l'on a $Q_2(X) = (X + 1)(X^8 + X^2 + 1)$. Or en caractéristique 2, on a $X^8 + X^2 + 1 = (X^4 + X + 1)^2$. Enfin, vérifions que le polynôme $X^4 + X + 1$ est irréductible sur $\mathbb{F}_2$: on voit qu'il n'a pas de racine dans $\mathbb{F}_2$. Donc s'il n'est pas irréductible, il se décompose en produit de deux polynômes de degré 2 : $X^4 + X + 1 = (X^2 + aX + 1)(X^2 + bX + 1)$ avec $a, b \in \mathbb{F}_2$. En développant, on aboutit à une contradiction. Donc $X^4 + X + 1$ est irréductible sur $\mathbb{F}_2$. Donc finalement la décomposition de Q_2 en facteurs irréductibles dans $\mathbb{F}_2[X]$ est

$$Q_2(X) = (X + 1)(X^4 + X + 1)^2 .$$

b) Dans $\mathbb{F}_3[X]$, la réduction Q_3 de Q s'écrit $Q_3(X) = X^9 - X^3 - 1$. Or en caractéristique 3, on a $X^9 - X^3 - 1 = (X^3 - X - 1)^3$. Enfin, le polynôme $X^3 - X - 1$ est irréductible dans $\mathbb{F}_3[X]$, puisqu'il n'a pas de racine dans $\mathbb{F}_3$. Donc la décomposition de Q_3 en facteurs irréductibles dans $\mathbb{F}_3[X]$ est

$$Q_3(X) = (X^3 - X - 1)^3 .$$

c) La décomposition de Q en facteurs irréductibles dans $\mathbb{Q}[X]$ induit des décompositions de Q_2 et Q_3 avec des facteurs de même degré, ce qui est contradictoire avec les décompositions en facteurs irréductibles de Q_2 et Q_3.

Exercice 5 : 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 5. 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 6 : Soit $K := \mathbb{Q}(\sqrt[3]{2})$ et $L/\mathbb{Q}$ la clôture galoisienne de $K/\mathbb{Q}$.

a) Calculer le degré de $L/\mathbb{Q}$ et le groupe de Galois de $L/\mathbb{Q}$.

b) Donner la liste des sous-corps de L.

Solution de l'exercice 6.

a) Par définition, L est un corps de décomposition de X^3-2 sur $\mathbb{Q}$. Ce polynôme est irréductible sur $\mathbb{Q}$, donc $K/\mathbb{Q}$ est de degré 3. Or le polynôme X^3-2 se décompose dans $K[X]$ sous la forme

$$X^3-2=(X-\sqrt[3]{2})(X^2+\sqrt[3]{2}X+\sqrt[3]{4})\,.$$

Les deux racines de $X^2+\sqrt[3]{2}X+\sqrt[3]{4}$ ne sont pas réelles (ce sont $j\sqrt[3]{2}$ et $j^2\sqrt[3]{2}$ où j est une racine primitive 3-ième de l'unité). Donc le polynôme $X^2+\sqrt[3]{2}X+\sqrt[3]{4}$ est irréductible sur K. Or L est engendré sur K par une des racines de ce polynôme ($L=K(j\sqrt[3]{2})=K(j)$), donc L/K est de degré 2, donc $L/\mathbb{Q}$ est de degré 6.

Le groupe de Galois de $L/\mathbb{Q}$ permute les racines de X^3-2, donc c'est un sous-groupe de $\mathfrak{S}_3$. Or $[L:\mathbb{Q}]=6$, donc le groupe de Galois est d'ordre 6, donc il est égal à $\mathfrak{S}_3$ tout entier.

b) Pour décrire tous les sous-corps de $L/\mathbb{Q}$, il suffit de décrire tous les sous-groupes de $\mathfrak{S}_3$. Ce groupe a six sous-groupes : les deux sous-groupes triviaux, qui correspondent aux extensions $\mathbb{Q}/\mathbb{Q}$ et $L/\mathbb{Q}$; trois sous-groupes d'ordre 2, engendré par une transposition, qui correspondent aux corps cubiques $K/\mathbb{Q}$, $\mathbb{Q}(j\sqrt[3]{2})/\mathbb{Q}$ et $\mathbb{Q}(j^2\sqrt[3]{2})/\mathbb{Q}$ un sous-groupe d'ordre 3 engendré par le 3-cycle (c'est le sous-groupe alterné) correspondant au corps quadratique $\mathbb{Q}(j)=\mathbb{Q}(\sqrt{-3})$.

Exercice 7 : Soit L/K une extension de corps de degré 3. On suppose K de caractéristique différente de 3.

a) Montrer que L est engendré par une racine α d'un polynôme de $K[X]$ de la forme X^3+pX+q.

b) Rappeler le lien entre le discriminant d'un polynôme et ses racines.

c) Montrer que si la caractéristique de K est différente de 2, alors L/K est galoisienne si et seulement si le discriminant $\Delta:=-(4p^3+27q^2)$ est un carré dans K.

Solution de l'exercice 7.

a) Puisque L/K est de degré 3, il est clair que cette extension est monogène : choisissons $\alpha\in L\setminus K$. Alors $L=K(\alpha)$. Notons $P(X)\in K[X]$ le polynôme minimal de α sur K. Alors P est de degré 3, de la forme $P(X)=X^3+aX^2+bX+c$. Un calcul simple assure que

$$P(X)=\left(X+\frac{a}{3}\right)^3+\left(b-\frac{a^2}{3}\right)\left(X+\frac{a}{3}\right)+\left(c+\frac{2a^3}{27}-\frac{ab}{3}\right),$$

donc en posant $\beta:=\alpha+\frac{a}{3}\in L$, on a $L=K(\beta)$ et le polynôme minimal de β est $P(X-\frac{a}{3})=X^3+pX+q$, avec $p=b-\frac{a^2}{3}$ et $q=c+\frac{2a^3}{27}-\frac{ab}{3}$.

b) Si $P(X)\in K[X]$ est un polynôme unitaire de degré n, et si $x_1,\dots x_n$ sont les racines de P dans un corps de décomposition, posons $\delta(P):=\prod_{1\le i<j\le n}(x_j-x_i)$. Alors $\Delta(P)=\delta(P)^2$. On peut démontrer ce résultat à l'aide du résultant de P et P' (voir exercice 10).

c) Remarquons d'abord que l'extension L/K est séparable, puisque son degré est premier à la caractéristique de K. Notons M/K la clôture galoisienne de L/K, et $\alpha,\beta,\gamma\in M$ les racines de X^3+pX+q. Supposons que $L=K(\alpha)$. Par la question précédente, on a $\delta:=(\alpha-\beta)(\alpha-\gamma)(\beta-\gamma)\in M$ tel que $\Delta=\delta^2\in K$.

Supposons L/K galoisienne, i.e. $M=L$. Alors $\delta\in L$ et $\delta^2\in K$. Or $[L:K]=3$, donc $\delta\in K$ et $\Delta\in K^2$.

Réciproquement, supposons que $M\neq L$. Alors il existe un L-automorphisme $\sigma:M\to M$ non trivial. Alors nécessairement $\sigma(\alpha)=\alpha$, $\sigma(\beta)=\gamma$ et $\sigma(\gamma)=\beta$. Donc $\sigma(\delta)=-\delta$, donc puisque la caractéristique de K n'est pas 2, $\sigma(\delta)=-\delta\neq\delta$, donc $\delta\notin K$, donc $\Delta\notin K^2$.

Exercice 8 : Soit p un nombre premier et $q=p^r$. Soit n un entier positif. On considère l'extension de corps $L=\mathbb{F}_q(Y)/K=\mathbb{F}_q(Y^n)$.

a) Montrer que L/K est séparable si et seulement si n est premier à p.

b) Montrer que L/K est normale si et seulement si $q \equiv 1 \pmod{n}$.

Solution de l'exercice 8.

a) L'extension L/K est monogène, engendrée par $Y \in L$. Elle est donc séparable si et seulement si $Y \in L$ est séparable sur K.

Supposons d'abord que p ne divise pas n. Le polynôme $X^n - Y^n \in K[X]$ annule $Y \in L$, et ce polynôme est clairement séparable, donc Y est séparable sur K.

Supposons maintenant que $n = p.m$. Alors on dispose d'une extension intermédiaire $K \subset K' = \mathbb{F}_q(Y^p) \subset L$. Il suffit de montrer que L/K' est inséparable. Or $L = K'(Y)$ et Y est annulé par le polynôme $X^p - Y^p \in K'[X]$. Ce dernier polynôme se factorise sous la forme $X^p - Y^p = (X-Y)^p$ dans $L[X]$, ce qui assure que Y n'est pas séparable sur K' (l'extension L/K' n'est pas triviale).

b) Montrons d'abord le fait suivant : l'extension $\mathbb{F}_q(Y)/\mathbb{F}_q(Y^n)$ est de degré n, donc $X^n - Y^n$ est le polynôme minimal de Y dans cette extension. Pour cela, soit $P := \sum_{i=0}^{d} a_i(Y^n)X^i$ un polynôme non nul de degré $d < n$ à coefficients dans $\mathbb{F}_q(Y^n)$ ($a_i \in \mathbb{F}_q(Y)$). Supposons $P(Y) = 0$. Alors on a $\sum_{i=0}^{d} a_i(Y^n)Y^i = 0$, et quitte à réduire au même dénominateur, on peut supposer que $a_i(Y) \in \mathbb{F}_q[Y]$. Notons alors $\alpha_d Y^{kn}$ ($\alpha_d \in \mathbb{F}_q^*$ et $k \in \mathbb{N}$) le coefficient dominant de $a_d(Y^n)$. Alors

$$\alpha_d Y^{kn+d} + \text{termes de degré inférieur} = -\sum_{i=0}^{d-1} a_i(Y^n)Y^i \,.$$

Or dans le membre de droite, les seuls monômes apparaissant sont de la forme Y^{mn+i} avec $m \in \mathbb{N}$ et $0 \leq i \leq d-1$: aucun n'est de la forme Y^{kn+d}. Par conséquent, l'égalité précédente est contradictoire, donc $P(Y) \neq 0$. Donc cela assure que $X^n - Y^n$ est le polynôme minimal de Y sur $\mathbb{F}_q(Y^n)$.

Donc l'extension est normale si et seulement si toutes les racines de ce polynôme sont dans $\mathbb{F}_q(Y)$. Or ces racines sont les $\zeta_n^k.Y$, avec $0 \leq k \leq n-1$ (où ζ_n est une racine primitive n-ième de l'unité), donc l'extension est normale si et seulement si $\mathbb{F}_q(Y)$ contient les racines primitives n-ièmes de l'unité si et seulement si $\mathbb{F}_q$ contient les racines primitives n-ièmes de l'unité si et seulement si $q \equiv 1 \pmod{n}$.

Exercice 9 :

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 (on pourra utiliser l'exercice 1).

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 9.

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 1 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 $p_n = a^2 + b^2p_{n-1} + 2ab\sqrt{p_{n-1}}$. 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.

Exercice 10 : Soit K un corps. Soient $P = a_nX^n + \cdots + a_0$ et $Q = b_mX^m + \cdots + b_0$ 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 $m + n$

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

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 10.

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

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

et l'espace vectoriel $K[X]_{m+n-1}$ de la base $(X^{m+n-1}, \ldots, X, 1)$. 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 11 : Trouver un élément primitif du corps de décomposition de $(X^2-2)(X^2-3)(X^2-5)$.

Solution de l'exercice 11. Puisque $\frac{2}{3}$ n'est pas un carré dans $\mathbb{Q}$, l'extension $\mathbb{Q}[\sqrt{2},\sqrt{3}]/\mathbb{Q}$ est galoisienne de groupe $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$, et cette extension admet $\sqrt{2}+\sqrt{3}$ comme élément primitif (voir exercice précédent). Les extensions quadratiques de Q contenues dans $\mathbb{Q}[\sqrt{2},\sqrt{3}]$ sont $\mathbb{Q}[\sqrt{2}]$, $\mathbb{Q}[\sqrt{3}]$ et $\mathbb{Q}[\sqrt{6}]$. Elles sont toutes distinctes de $\mathbb{Q}[\sqrt{5}]$. Donc le groupe de Galois de $\mathbb{Q}[\sqrt{2},\sqrt{3},\sqrt{5}]/\mathbb{Q}$ est $(\mathbb{Z}/2\mathbb{Z})^3$, avec l'action de Galois évidente sur $\sqrt{2},\sqrt{3},\sqrt{5}$. Par conséquent, l'élément $\alpha:=\sqrt{2}+\sqrt{3}+\sqrt{5}$ a tous ses conjugués distincts, donc c'est un générateur de l'extension $\mathbb{Q}[\sqrt{2},\sqrt{3},\sqrt{5}]/\mathbb{Q}$.

Exercice 12 : Soit k un corps de caractéristique $p>0$.

a) Montrer que l'extension $k(X,Y)/k(X^p,Y^p)$ est finie normale mais pas séparable.

b) Montrer que cette extension n'est pas monogène.

Solution de l'exercice 12.

a) Cette extension est engendrée par deux éléments algébriques, elle est donc finie. En outre, c'est un corps de décomposition de $(T^p-X^p)(T^p-Y^p)\in k(X^p,Y^p)[T]$, donc c'est une extension normale. En revanche, l'élément $X\in k(X,Y)$ est annulé par $T^p-X^p\in k(X^p,Y^p)[T]$. Or ce polynôme est scindé sur $k(X,Y)$, via l'égalité $T^p-X^p=(T-X)^p\in k(X,Y)[T]$. Donc le polynôme minimal de X sur $k(X^p,Y^p)$ n'est pas séparable puisque c'est un diviseur de degré >1 de T^p-X^p, qui a donc une racine multiple. Donc l'extension considérée n'est pas séparable.

b) Soit $\alpha \in k(X,Y)$. Puisque le morphisme de Frobenius $x \mapsto x^p$ est un morphisme du corps k, on a $\alpha^p \in k(X^p, Y^p)$. Par conséquent, le polynôme minimal de α sur $k(X^p, Y^p)$ est de degré au plus p (il divise $X^p - \alpha^p$), donc l'extension $k(X^p, Y^p)[\alpha]/k(X^p, Y^p)$ est de degré au plus p. Or l'extension $k(X,Y)/k(X^p, Y^p)$ est clairement de degré p^2, donc cette extension n'est pas monogène.

Exercice 13 : 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 13.

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 $x \in L \setminus K$. Alors deux cas se présentent : soit x est transcendant sur K, et alors on a une tour infinie d'extensions intermédiaires 2-à-2 distinctes $L \supset K(x) \supset K(x^2) \supset K(x^3) \supset \cdots \supset K$; soit x est algébrique sur K et l'extension $L/K(x)$ est infinie, donc on conclut par récurrence à l'existence d'une tour infinie d'extensions intermédiaires. Dans les deux cas, on 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 14 : 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 une racine non triviale dans une extension de degré 2 ?

Solution de l'exercice 14.

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.

Exercice 15 : Soit K un corps infini, L/K une extension normale séparable finie (on dit qu'une telle extension est galoisienne). On note G le groupe des K-automorphismes du corps L (appelé groupe de Galois de l'extension L/K). Enfin, il existe $x \in L$ tel que $L = K(x)$ (théorème de l'élément primitif), et on note $f \in K[X]$ le polynôme minimal de x sur K.

a) Si $\sigma \in G$, on pose $R_\sigma(T) := \frac{f(T)}{(T-\sigma(x))f'(\sigma(x))} \in L(T)$. Montrer que :

i) pour tout $\sigma \in G$, $R_\sigma(T) \in L[T]$.

ii) $\sum_{\sigma\in G} R_\sigma(T) = 1$.

iii) si $\sigma \neq \tau$ dans G, alors $R_\sigma R_\tau \equiv 1 \pmod f$.

iv) pour tout $\sigma \in G$, $R_\sigma^2 \equiv R_\sigma \pmod f$.

b) On note M la matrice carré $(R_{\sigma\tau})_{(\sigma,\tau)\in G^2}$ à coefficients dans $L[T]$ indicée par G. On note $D(T) := \det(M) \in L[T]$. En calculant M^tM modulo f, montrer que $D(T)^2 \equiv 1 \pmod f$.

c) En déduire qu'il existe $y \in K$ tel que si on pose $\alpha := R_1(y) \in L$, alors la famille $(\sigma(\alpha))_{\sigma\in G}$ est une base de l'extension L/K (i.e. une base du K-espace vectoriel L).

Solution de l'exercice 15.

a) On note $n := [L : K] = \deg(f)$.

i) Remarquons que, puisque les $\sigma(x)$ (pour $\sigma \in G$) sont les conjugués de x dans L/K, dans $L[T]$ le polynôme f s'écrit

$$f(T) = \prod_{\sigma\in G} (X - \sigma(x)) .$$

Par conséquent, il est clair que $R_\sigma(T) \in L[T]$ est un polynôme de degré $n - 1$.

ii) On remarque que pour tout $\sigma, \tau \in G$, $R_\sigma(\tau(x)) = 0$ si $\sigma \neq \tau$ et $R_\sigma(\tau(x)) = 1$ si $\sigma = \tau$. Par conséquent, pour tout $\tau \in G$, $(\sum_{\sigma\in G} R_\sigma)(\tau(x)) = 1$. Or le polynôme $\sum_{\sigma\in G} R_\sigma$ est de degré au plus $n - 1$, et les conjugués $\tau(x)$, pour $\tau \in G$, sont deux-à-deux distincts (l'extension est séparable), donc au nombre de n, donc les égalités précédentes assurent que l'on a $\sum_{\sigma\in G} R_\sigma = 1$ dans $L[T]$.

iii) Si $\sigma \neq \tau$, on écrit

$$R_\sigma(T)R_\tau(T) = \frac{1}{f'(\sigma(x))f'(\tau(x))} \frac{f(T)}{(T - \sigma(x))(T - \tau(x))} f(T)$$

et on vérifie que $(T - \sigma(x))(T - \tau(x))$ divise $f(T)$ dans $L[T]$, ce qui assure que $f(T)$ divise $R_\sigma(T)R_\tau(T)$.

iv) Pour $\tau \in G$, il suffit de multiplier l'égalité $\sum_{\sigma\in G} R_\sigma = 1$ par R_τ pour obtenir $\sum_{\sigma\in G} R_\sigma R_\tau = R_\tau$. On utilise alors la question précédente pour voir que modulo f, le membre de gauche s'écrit $\sum_{\sigma\in G} R_\sigma R_\tau \equiv R_\tau^2 \pmod f$, d'où le résultat.

b) Calculons le coefficient $d_{\sigma,\tau}$ d'indices $(\sigma, \tau) \in G^2$ dans la matrice M^tM : par définition, ce dernier est égal à

$$d_{\sigma,\tau} = \sum_{\mu\in G} R_{\sigma\mu}R_{\tau\mu} .$$

Donc modulo f, en utilisant la question précédente, on obtient que $d_{\sigma,\tau} = \sum_{\mu\in G} R_\mu^2 \equiv 1 \pmod f$ si $\sigma = \tau$, et $d_{\sigma,\tau} \equiv 0 \pmod f$ si $\sigma \neq \tau$. Donc finalement on a $M^tM \equiv I_n \pmod f$, d'où en prenant le déterminant $D^2 \equiv 1 \pmod f$.

c) Par la question précédente, le polynôme $D(T) \in L[T]$ n'est pas le polynôme nul. Or le corps K est infini, donc il existe $y \in K$ tel que $D(y) \neq 0$. On pose alors $\alpha := R_1(y) \in L$. Pour montrer que la famille $(\sigma(\alpha))_{\sigma\in G}$ est une base, il suffit de montrer qu'elle est libre sur K (puisqu'elle est formée de $n = [L : K]$ vecteurs).

Soit $(\lambda_\sigma) \in K^n$ tels que $\sum_{\sigma\in G} \lambda_\sigma\sigma(\alpha) = 0$. Remarquons que $\sigma(R_\tau(T)) = R_{\sigma\tau}(T)$. Alors la relation précédente se réécrit ainsi : $\sum_{\sigma\in G} \lambda_\sigma R_\sigma(y) = \sum_{\sigma\in G} \lambda_\sigma\sigma(R_1(y)) = 0$. Soit alors $\tau \in G$: on a

$$\sum_{\sigma\in G} \lambda_\sigma R_{\tau\sigma}(y) = \sum_{\sigma\in G} \lambda_\sigma\tau(R_\sigma(y)) = \tau\left(\sum_{\sigma\in G} \lambda_\sigma R_\sigma(y)\right) = 0$$

où la deuxième égalité provient du fait que $\lambda_\sigma \in K$. Donc finalement pour tout $\tau \in G$, $\sum_{\sigma\in G} \lambda_\sigma R_{\tau\sigma}(y) = 0$, donc on dispose d'une relation linéaire entre les colonnes de la matrice

M évaluée en $T = y$. Or cette matrice est inversible puisque $D(y) \neq 0$, donc la relation linéaire précédente entre ses colonnes est triviale, donc $\lambda_\sigma = 0$ pour tout $\sigma \in G$. Cela assure donc que la famille $(\sigma(\alpha))_{\sigma \in G}$ est libre sur K, ce qui conclut la preuve.