Partiel Algèbre 2

Responsable : Mr O. DEBARRE

Exercice 1. Soit K un corps. Montrer que la clôture algébrique de K dans le corps $K(X)$ est K.

Exercice 2. Soit $K \hookrightarrow L$ une extension algébrique de corps et soit $Q \in L[X]$ un polynôme irréductible. Montrer qu'il existe un polynôme irréductible $P \in K[X]$ tel que Q divise P (dans $L[X]$).

Exercice 3. On pose $a := \sqrt{5+\sqrt{21}}$ et on note $K = \mathbf{Q}(a)$.

a) Quel est le degré de l'extension $\mathbf{Q} \hookrightarrow K$?

b) Montrer que l'extension $\mathbf{Q} \hookrightarrow K$ est galoisienne (*Indication :* on pourra montrer que $b := \sqrt{5-\sqrt{21}}$ est dans K).

c) Déterminer le groupe de Galois de l'extension $\mathbf{Q} \hookrightarrow K$.

d) Déterminer tous les sous-corps de K (*Indication :* on pourra calculer $(a \pm b)^2$ pour les écrire simplement).

e) L'extension $\mathbf{Q} \hookrightarrow \mathbf{Q}(\sqrt{5+\sqrt{15}})$ est-elle galoisienne ?

Exercice 4. On rappelle que si M est une matrice carrée à coefficients dans un corps algébriquement clos $\overline{K}$, il existe un *unique* couple (D_M, N_M) de matrices carrées à coefficients dans $\overline{K}$ telles que $M = D_M + N_M$, $D_M N_M = N_M D_M$, D_M est diagonalisable et N_M est nilpotente.

a) Si M est à coefficients réels, montrer qu'il en est de même pour D_M et N_M.

b) Si M est à coefficients rationnels, montrer qu'il en est de même pour D_M et N_M (*Indication :* on pourra utiliser la théorie de Galois).

Exercice 5. Soit $K \hookrightarrow L$ une extension algébrique de corps. On suppose que tout polynôme de $K[X]$ a une racine dans L. On veut montrer que L est une clôture algébrique de K.

a) Montrer la conclusion si on suppose de plus que tout polynôme de $K[X]$ est *scindé* dans L.

b) Montrer la conclusion si on suppose de plus que le corps K est *parfait* (*Indication :* si $P \in K[X]$, on pourra appliquer le théorème de l'élément primitif à un corps de décomposition de P et considérer le polynôme minimal d'un générateur).

c) On suppose à partir de maintenant que la caractéristique de K est $p > 0$. Montrer que

$$M := \{x \in L \mid \exists n \in \mathbf{N}^* \quad x^{p^n} \in K\}$$

est un sous-corps parfait de L.

d) En déduire que L est un corps parfait.

e) Montrer que tout polynôme de $M[X]$ a une racine dans L. Conclure.

Corrigé du partiel Algèbre 2

Responsable : Mr O. DEBARRE

Exercice 1. *Soit K un corps. Montrer que la clôture algébrique de K dans le corps $K(X)$ est K.*

Il s'agit de montrer que tout $F \in K(X)$ algébrique sur K est dans K. Mais si $F = P/Q \in K(X) - K$, on a la relation non triviale $FQ(X) - P(X) = 0$ qui montre que X est algébrique sur $K(F)$, donc que $K(X)$ est une extension algébrique de $K(F)$. Si F est algébrique sur K, $K(F)$ est une extension algébrique de K, donc $K(X)$ est algébrique sur K, ce qui est absurde.

Exercice 2. *Soit $K \hookrightarrow L$ une extension algébrique de corps et soit $Q \in L[X]$ un polynôme irréductible. Montrer qu'il existe un polynôme irréductible $P \in K[X]$ tel que Q divise P (dans $L[X]$).*

Soit x une racine de Q dans un corps de rupture M de Q, de sorte que Q est le polynôme minimal de x sur L. Comme x est algébrique sur L et que $K \hookrightarrow L$ est une extension algébrique, x est algébrique sur K. Soit $P \in K[X]$ son polynôme minimal. Alors $P \in L[X]$ et $P(x) = 0$, donc $Q \mid P$.

Exercice 3. *On pose $a := \sqrt{5+\sqrt{21}}$ et on note $K = \mathbf{Q}(a)$.*

a) Quel est le degré de l'extension $\mathbf{Q} \hookrightarrow K$?

On a des extensions $\mathbf{Q} \subset \mathbf{Q}(\sqrt{21}) \subset K$. Il suffit donc de montrer $a \notin \mathbf{Q}(\sqrt{21})$. Supposons donc $a = u+v\sqrt{21}$, avec $u, v \in \mathbf{Q}$. On a

$$5 + \sqrt{21} = u^2 + 21v^2 + 2uv\sqrt{21},$$

d'où on déduit $uv = 1/2$ et $5 = u^2 + \frac{21}{4u^2}$, d'où $u^4 - 5u^2 + 21/4 = 0$, qui n'a pas de racine rationnelle puisque ses racines sont $\pm\sqrt{(5 \pm 2)/2}$.

b) Montrer que l'extension $\mathbf{Q} \hookrightarrow K$ est galoisienne.

On a $ab = 2$, donc $b \in K$. Le polynôme minimal de a est de degré 4 et divise $P(X) := (X^2 - 5)^2 - 21$. Il lui est donc égal et les conjugués de a sont $\pm a$ et $\pm b$, qui sont tous dans K. Le corps K est donc le corps de décomposition de P : c'est une extension galoisienne de $\mathbf{Q}$.

c) Déterminer le groupe de Galois de l'extension $\mathbf{Q} \hookrightarrow K$.

Ce groupe G est d'ordre 4. Il agit transitivement sur l'ensemble $\{a, -a, b, -b\}$ des conjugués de a et un élément est entièrement déterminé par l'image de a (à cause de la relation $b = 2/a$). C'est donc le sous-groupe de Klein composé de l'identité et des doubles transpositions. Il est isomorphe à $(\mathbf{Z}/2\mathbf{Z})^2$.

d) Déterminer tous les sous-corps de K.

Tout sous-corps de K contient K. Ces sous-corps correspondent donc, par la théorie de Galois, aux sous-groupes du groupe de Galois. Il y en a donc 5 (on remarque que $(a + b)^2 = 6$ et $(a - b)^2 = 14$) : $\mathbf{Q}$, K, $\mathbf{Q}(a^2) = \mathbf{Q}(\sqrt{21})$, $\mathbf{Q}(a + b) = \mathbf{Q}(\sqrt{6})$, $\mathbf{Q}(a - b) = \mathbf{Q}(\sqrt{14})$.

e) L'extension $\mathbf{Q} \hookrightarrow \mathbf{Q}(\sqrt{5+\sqrt{15}})$ est-elle galoisienne ?

On vérifie comme en a) qu'elle est de degré 4. Notons comme avant $a := \sqrt{5+\sqrt{15}}$ et $b := \sqrt{5-\sqrt{15}}$, de sorte que les conjugués de a sont $\pm a$ et $\pm b$. Si l'extension $\mathbf{Q} \hookrightarrow \mathbf{Q}(a)$ est galoisienne, on note G son groupe de Galois ; il est d'ordre 4. La sous-extension $\mathbf{Q} \hookrightarrow \mathbf{Q}(\sqrt{15})$ correspond à un élément $g \in G$ d'ordre 2 qui fixe a^2 mais pas a, donc $g(a) = -a$ et $g(b) = \pm b$. Si $g(b) = b$, on a $b \in \mathbf{Q}(\sqrt{15})$, mais on montre de la même façon qu'en a) que c'est absurde. Donc $g(b) = -b$. Alors $g(ab) = g(a)g(b) = ab$, donc $ab \in \mathbf{Q}(\sqrt{15})$. Mais $ab = \sqrt{10}$ et on montre encore que c'est absurde. Donc l'extension $\mathbf{Q} \hookrightarrow \mathbf{Q}(\sqrt{5+\sqrt{15}})$ n'est pas galoisienne.

Exercice 4. *On rappelle que si M est une matrice carrée à coefficients dans un corps algébriquement clos $\overline{K}$, il existe un* unique *couple (D_M, N_M) de matrices carrées à coefficients dans $\overline{K}$ telles que $M = D_M + N_M$, $D_M N_M = N_M D_M$, D_M est diagonalisable et N_M est nilpotente.*

a) Si M est à coefficients réels, montrer qu'il en est de même pour D_M et N_M.

Si M est réelle, on a $M = \overline{M} = \overline{D} + \overline{N}$, et $\overline{D}\,\overline{N} = \overline{N}\,\overline{D}$, $\overline{D}$ est diagonalisable et $\overline{N}$ est nilpotente. Par l'unicité de la décomposition, on a $D = \overline{D}$ et $N = \overline{N}$, c'est-à-dire que D et N sont réelles.

b) Si M est à coefficients rationnels, montrer qu'il en est de même pour D_M et N_M.

On peut voir M comme étant à coefficients dans $\overline{\mathbf{Q}}$, de sorte que D et N sont aussi à coefficients dans $\overline{\mathbf{Q}}$ d'après le rappel. Soit $K \subset \overline{\mathbf{Q}}$ l'extension (finie) de $\mathbf{Q}$ engendrée par les coefficients des matrices D_M et N_M et soit $K \subset L \subset \overline{\mathbf{Q}}$ sa clôture normale. D'après le cours, L est une extension finie galoisienne de $\mathbf{Q}$. Comme dans le a), l'unicité de la décomposition entraîne que les coefficients de D_M et de N_M sont invariants par l'action de $\mathrm{Gal}(L/\mathbf{Q})$. Ils sont donc dans $\mathbf{Q}$.

Exercice 5. *Soit $K \hookrightarrow L$ une extension algébrique de corps. On suppose que tout polynôme de $K[X]$ a une racine dans L. On veut montrer que L est une clôture algébrique de K.*

a) Montrer la conclusion si on suppose de plus que tout polynôme de $K[X]$ est scindé dans L.

On peut utiliser l'exerc. 2) : soit $Q \in L[X]$ un polynôme irréductible, par l'exerc. 2), il existe un polynôme irréductible $P \in K[X]$ tel que Q divise P dans $L[X]$. Mais P est scindé dans L par hypothèse, donc aussi L. Comme tout élément de $L[X]$ est produit de polynômes irréductibles, on a montré que L est une clôture algébrique de K.

b) Montrer la conclusion si on suppose de plus que le corps K est parfait.

Par a), il suffit de montrer que tout polynôme $P \in K[X]$ est scindé dans L. Soit $K \hookrightarrow M$ un corps de décomposition de P. Comme K est parfait, l'extension $K \hookrightarrow M$ est finie et séparable donc engendrée par un élément $x \in M$ (théorème de l'élément primitif). Soit $Q \in K[X]$ le polynôme minimal de x ; il a par hypothèse une racine y dans L. Les corps $M = K(x)$ et $K(y)$ sont alors des corps de rupture du polynôme irréductible Q, donc ils sont K-isomorphes. Comme P est scindé dans M, il est scindé dans $K(y) \subset L$.

c) On suppose à partir de maintenant que la caractéristique de K est $p > 0$. Montrer que $M := \{x \in L \mid \exists n \in \mathbf{N}^* \quad x^{p^n} \in K\}$ est un sous-corps parfait de L.

On vérifie facilement que c'est un sous-corps de L. Montrons $M^p = M$. Soit $a \in M$ et $n > 0$ tel que $a^{p^n} \in K$. Le polynôme $X^{p^{n+1}} - a^{p^n} \in K[X]$ a alors une racine b dans L ; elle vérifie $b^{p^{n+1}} = a^{p^n} \in K$, donc $b \in M$, et, en prenant les racines p^n-ièmes, $b^p = a$. Donc $a \in M^p$.

d) En déduire que L est un corps parfait.

Soit $L \hookrightarrow L'$ une extension algébrique. L'extension $M \hookrightarrow L'$ est algébrique, donc séparable puisque M est parfait, donc l'extension $L \hookrightarrow L'$ est séparable. Ceci montre que L est parfait (on vient en fait de montrer que toute extension algébrique d'un corps parfait est encore un corps parfait). On peut aussi raisonner directement avec la définition en utilisant l'exerc. 2).

e) Montrer que tout polynôme de $M[X]$ a une racine dans L. Conclure.

Soit $P(X) = a_k X^k + \cdots + a_1 X + a_0 \in M[X]$. Il existe $n > 0$ tel que

$$P_n(X) = a_k^{p^n} X^k + \cdots + a_1^{p^n} X + a_0^{p^n} \in K[X]$$

Ce polynôme a, par hypothèse, une racine $a \in L$. Comme L est parfait par d), on peut écrire $a = b^{p^n}$ avec $b \in L$. On a alors

$$0 = a_k^{p^n} (b^{p^n})^k + \cdots + a_1^{p^n} b^{p^n} + a_0^{p^n} = P(b)^{p^n}$$

donc $P(b) = 0$. Tout polynôme de $M[X]$ a donc une racine dans L, et M est parfait par c). Par b), L est une clôture algébrique de M, donc de K.