Examen Algèbre 2

Responsable : Mr O. DEBARRE

Important : vous avez droit de consulter le cours et d'utiliser sans démonstration ses résultats. Si vous voulez utiliser des résultats hors du cours, il faut les démontrer (sauf mention explicite du contraire).

Exercice 1. Soit $K \hookrightarrow L$ une extension de corps galoisienne (finie) de groupe de Galois $\mathfrak{S}_n$, avec $n \geq 5$. Montrer que le degré sur K d'un élément de L est soit 1, soit 2, soit $\geq n$ (on admettra sans démonstration que le seul sous-groupe distingué strict de $\mathfrak{S}_n$ est $\mathfrak{A}_n$).

Exercice 2. Soit K un corps et soit $P \in K[X]$ un polynôme unitaire de degré n. On a défini en cours la matrice compagnon $C(P) \in \mathscr{M}_n(K)$. Soit $Q \in K[X]$ un polynôme unitaire. Calculer les invariants de similitude de la matrice par blocs

$$\begin{pmatrix} C(P) & 0 \\ 0 & C(Q) \end{pmatrix}.$$

Exercice 3. 1) Donner une décomposition primaire minimale pour l'idéal $(X^2 - 2, Y^2 - 2)$ dans $\mathbf{C}[X, Y]$. Y a-t-il des idéaux premiers immergés ?

2) Donner une décomposition primaire minimale pour l'idéal $(X^2 - 2, Y^2 - 2)$ dans $\mathbf{Q}[X, Y]$.

Problème. Dans tout ce problème, A est un anneau intégralement clos de corps de fractions K_A, que l'on suppose de caractéristique nulle, et $\iota : A \hookrightarrow B$ est une extension finie d'anneaux intègres.

I. Montrer que l'extension $K_A \hookrightarrow K_B$ entre corps de fractions est finie.

Pour les besoins des démonstrations, on introduit maintenant la clôture galoisienne $K_A \hookrightarrow L$ de $K_A \hookrightarrow K_B$ dans une clôture algébrique de K_B (prop. I.6.34 du cours). C'est une extension galoisienne finie de K_A contenant K_B. On note enfin $C \subset L$ la clôture intégrale de A dans L ; c'est une extension entière de A. On a donc le diagramme d'extensions suivant :

$$\begin{tikzcd} A \arrow[r, hook] \arrow[d, hook] & B \arrow[r, hook] \arrow[d, hook] & C \arrow[d, hook] \\ K_A \arrow[r, hook] & K_B \arrow[r, hook] & L. \end{tikzcd}$$

II. Soit $\mathfrak{p}$ un idéal premier de A. Le but de cette partie est de montrer que tous les idéaux premiers de C au-dessus de $\mathfrak{p}$ sont conjugués par l'action du groupe de Galois $\mathrm{Gal}(L/K_A)$.

Soient $\mathfrak{q}_1$ et $\mathfrak{q}_2$ des idéaux premiers de C au-dessus de $\mathfrak{p}$. On raisonne par l'absurde, en supposant

$$\forall \sigma \in \mathrm{Gal}(L/K_A) \qquad \mathfrak{q}_2 \neq \sigma(\mathfrak{q}_1).$$

1) Montrer

$$\forall \sigma \in \mathrm{Gal}(L/K_A) \qquad \mathfrak{q}_2 \not\subset \sigma(\mathfrak{q}_1).$$

2) Montrer qu'il existe $x \in \mathfrak{q}_2$ qui n'appartient à aucun des $\sigma(\mathfrak{q}_1)$, pour $\sigma \in \mathrm{Gal}(L/K_A)$.

3) Montrer $\prod_{\sigma \in \mathrm{Gal}(L/K_A)} \sigma(x) \in A$.

4) En déduire une contradiction.

III. Montrer que les fibres de l'application canonique $\iota^\sharp : \mathrm{Spec}(B) \to \mathrm{Spec}(A)$ sont finies, c'est-à-dire que pour tout idéal premier $\mathfrak{p}$ de A, il n'y a qu'un nombre fini d'idéaux premiers $\mathfrak{q}$ de B tels que $\mathfrak{q} \cap A = \mathfrak{p}$ (*Indication :* on pourra utiliser le résultat de la partie II).

IV. Montrer le « going-down » : si $\mathfrak{p}_1 \subset \mathfrak{p}_2$ sont des idéaux premiers de A et $\mathfrak{q}_2$ un idéal premier de B au-dessus de $\mathfrak{p}_2$, il existe un idéal premier $\mathfrak{q}_1$ de B au-dessus de $\mathfrak{p}_1$ tel que $\mathfrak{q}_1 \subset \mathfrak{q}_2$ (*Indication :* on pourra utiliser le résultat de la partie II).

V. Le but de cette partie est de montrer que l'application $\iota^\sharp : \mathrm{Spec}(B) \to \mathrm{Spec}(A)$ est ouverte, c'est-à-dire que l'image de toute partie ouverte de $\mathrm{Spec}(B)$ est une partie ouverte de $\mathrm{Spec}(A)$.

On rappelle que pour tout élément a d'un anneau A', on a posé en cours

$$D(a) = \{\mathfrak{r} \in \mathrm{Spec}(A') \mid a \notin \mathfrak{r}\}.$$

C'est un ouvert de $\mathrm{Spec}(A')$ et tout ouvert de $\mathrm{Spec}(A')$ est réunion d'ouverts de ce type.

1) Soit $b \in B$ et soit $P(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \in K_A[X]$ le polynôme minimal de b sur K_A. Montrer $P \in A[X]$.

2) Soit $\mathfrak{q} \in D(b)$. Montrer $\iota^\sharp(\mathfrak{q}) \in \bigcup_{i=0}^{n-1} D(a_i)$.

3) Supposons inversement $\mathfrak{p} \in \bigcup_{i=0}^{n-1} D(a_i)$. Notons R le sous-anneau $A[b]$ de B.

a) Supposons $b \in \sqrt{\mathfrak{p}R}$. Montrer qu'il existe $m \geq 1$ et $a'_0, \ldots, a'_{n-1} \in \mathfrak{p}$ tels que $b^m = \sum_{i=0}^{n-1} a'_i b^i$.

b) Montrer que X^m est divisible par $\bar{P}(X) = X^n + \bar{a}_{n-1}X^{n-1} + \cdots + \bar{a}_1X + \bar{a}_0$ dans $(A/\mathfrak{p})[X]$ et en déduire une contradiction.

c) On a donc $b \notin \sqrt{\mathfrak{p}R}$. Montrer qu'il existe un idéal premier $\mathfrak{q}_2$ de R contenant $\mathfrak{p}R$ tel que $b \notin \mathfrak{q}_2$.

d) Montrer qu'il existe $\mathfrak{q} \in \mathrm{Spec}(R)$ avec $\mathfrak{q} \subset \mathfrak{q}_2$ et $\mathfrak{q} \cap A = \mathfrak{p}$.

e) En déduire $\mathfrak{p} \in \iota^\sharp(D(b))$.

4) En déduire que l'application $\iota^\sharp : \mathrm{Spec}(B) \to \mathrm{Spec}(A)$ est ouverte.

Corrigé de l'examen Algèbre 2

Responsable : Mr O. DEBARRE

Exercice 1. *Soit $K \hookrightarrow L$ une extension de corps galoisienne (finie) de groupe de Galois $\mathfrak{S}_n$, avec $n \geq 5$. Montrer que le degré sur K d'un élément de L est soit 1, soit 2, soit $\geq n$.*

Soit x un élément de L. L'extension intermédiaire $K \subset K(x) \subset L$ correspond à un sous-groupe $H < \mathfrak{S}_n$ d'indice le degré d de x sur K. Le groupe $\mathfrak{S}_n$ opère transitivement par translation sur l'ensemble des classes $X := \mathfrak{S}_n/H$ et le noyau K de l'opération

$$\begin{array}{rcl} \varphi : \mathfrak{S}_n & \to & \mathrm{Aut}(X) \\ g & \mapsto & \big(g'H \mapsto gg'H\big) \end{array}$$

est contenu dans H (si $\varphi(g)$ est l'identité, on a $H = gH$, donc $g \in H$). Si $d > 2$, on a $[\mathfrak{S}_n : K] \geq d > 2$, et comme K est distingué dans $\mathfrak{S}_n$, il est trivial. On en déduit $n! = \mathrm{Card}(\mathfrak{S}_n) \leq \mathrm{Card}(\mathrm{Aut}(X)) = d!$, donc $d \geq n$.

Exercice 2. *Soit K un corps et soient P et Q des polynômes unitaires de $K[X]$. Calculer les invariants de similitude de la matrice par blocs $\begin{pmatrix} C(P) & 0 \\ 0 & C(Q) \end{pmatrix}$.*

Soit M cette matrice ; elle est d'ordre $m + n$, avec $m := \deg(Q)$. Les facteurs invariants de la matrice $XI_{m+n} - M \in \mathscr{M}(K[X])$ sont $(1, \dots, 1, P_1, \dots, P_s)$, où $P_1, \dots, P_s \in K[X]$ sont les invariants de similitude de M. De plus, pour tout $r \in \{1, \dots, m + n\}$, le produit des r premiers facteurs invariants est le pgcd des mineurs d'ordre r de $XI_{m+n} - M$. Or $C(P)$ contient une matrice I_{n-1} et $C(Q)$ contient une matrice I_{m-1}, toutes les deux « sous la diagonale », donc $XI_{m+n} - M$ contient une matrice I_{m+n-2}. On a donc $s \leq 2$.

D'autre part, pour tout $R \in K[X]$, on a

$$R(M) = \begin{pmatrix} R(C(P)) & 0 \\ 0 & R(C(Q)) \end{pmatrix}.$$

On a donc $R(M) = 0$ si et seulement si $R(C(P)) = R(C(Q)) = 0$. Comme le polynôme minimal de $C(P)$ est P, et celui de $C(Q)$ est Q, on a $R(M) = 0$ si et seulement si $P \vee Q \mid R$. Le polynôme minimal P_s de M est donc $P \vee Q$.

Enfin, le déterminant de M est PQ, donc $P_1 \cdots P_s = PQ$. On en déduit que les invariants de similitude de M sont $(P \wedge Q, P \vee Q)$.

Exercice 3. *1) Donner une décomposition primaire minimale pour l'idéal $(X^2 - 2, Y^2 - 2)$ dans $\mathbf{C}[X, Y]$. Y a-t-il des idéaux premiers immergés ?*

Cet idéal I définit dans $\mathbf{C}^2 = \mathrm{Specmax}(\mathbf{C}[X, Y])$ l'ensemble à quatre éléments $\{(\pm\sqrt{2}, \pm\sqrt{2})\}$. Donc son radical est

$$(1) \qquad (X + \sqrt{2}, Y + \sqrt{2}) \cap (X + \sqrt{2}, Y - \sqrt{2}) \cap (X - \sqrt{2}, Y + \sqrt{2}) \cap (X - \sqrt{2}, Y - \sqrt{2}).$$

où chacun des idéaux qui apparaissent est maximal. Inversement, si un polynôme P est dans cette intersection, on peut d'abord l'écrire $P = (X+\sqrt{2})Q+(Y+\sqrt{2})R$. Comme il est aussi dans $(X+\sqrt{2}, Y-\sqrt{2})$, il s'annule en $(-\sqrt{2}, \sqrt{2})$, donc R aussi. On en déduit $P = (X + \sqrt{2})Q + (Y + \sqrt{2})\big((X + \sqrt{2})S + (Y - \sqrt{2})T\big)$. En raisonnant de même avec Q, qui s'annule en $(\sqrt{2}, -\sqrt{2})$, on obtient $P \in I$. L'égalité (1) est donc une décomposition primaire de I. Tous les idéaux qui y interviennent sont maximaux et distincts. Elle est donc minimale et il n'y a pas d'idéal premier immergé.

2) Donner une décomposition primaire pour l'idéal $(X^2 - 2, Y^2 - 2)$ dans $\mathbf{Q}[X, Y]$.

On regroupe les idéaux par paires conjuguées sous l'action du groupe de Galois de $\mathbf{Q}(\sqrt{2})$ sur $\mathbf{Q}$. On a ainsi

$$I = (X^2 - 2, X - Y) \cap (X^2 - 2, X + Y).$$

Ces idéaux sont distincts. Ils sont maximaux dans $\mathbf{Q}[X, Y]$, puisque par exemple $\mathbf{Q}[X, Y]/(X^2 - 2, X - Y) \simeq \mathbf{Q}[X]/(X^2 - 2) \simeq \mathbf{Q}(\sqrt{2})$ est un corps, et distincts. C'est donc bien une décomposition primaire minimale de I.

Problème. *Dans tout ce problème, A est un anneau intégralement clos de corps de fractions K_A, que l'on suppose de caractéristique nulle, et $\iota : A \hookrightarrow B$ est une extension finie d'anneaux intègres.*

I. Montrer que l'extension $K_A \hookrightarrow K_B$ entre corps de fractions est finie.

La A-algèbre B est engendrée par un nombre fini d'éléments $b_1, \dots, b_n$. Le sous-corps $K_A(b_1, \dots, b_n)$ de K_B contient alors B ; c'est donc K_B. Chaque b_i est entier sur A, donc est algébrique sur K_A. L'extension de corps $K_A \hookrightarrow K_B$ est ainsi engendrée par un nombre fini d'éléments algébriques sur K_A : elle est finie.

II. Soit $\mathfrak{p}$ un idéal premier de A. Soient $\mathfrak{q}_1$ et $\mathfrak{q}_2$ des idéaux premiers de C au-dessus de $\mathfrak{p}$. On raisonne par l'absurde, en supposant

$$\forall \sigma \in \mathrm{Gal}(L/K_A) \qquad \mathfrak{q}_2 \neq \sigma(\mathfrak{q}_1).$$

1) Montrer $\forall \sigma \in \mathrm{Gal}(L/K_A) \qquad \mathfrak{q}_2 \not\subset \sigma(\mathfrak{q}_1)$.

Commençons par remarquer que l'image d'un élément de C par n'importe quel élément σ de $\mathrm{Gal}(L/K_A)$ est encore entière sur A (elle est racine du même polynôme unitaire à coefficients dans A), donc est dans C. En d'autres termes, on a $\sigma(C) = C$, et $\sigma(\mathfrak{q}_1)$ est bien encore un idéal premier de C.

On a $\sigma(\mathfrak{q}_1) \cap A = \sigma(\mathfrak{q}_1 \cap A) = \sigma(\mathfrak{p}_1) = \mathfrak{p}_1$, donc $\sigma(\mathfrak{q}_1)$ et $\mathfrak{q}_2$ sont des idéaux premiers distincts de C au-dessus de $\mathfrak{p}$. Par le lemme III.10.2 du cours, il ne peut y avoir d'inclusion entre les deux.

2) Montrer qu'il existe $x \in \mathfrak{q}_2$ qui n'appartient à aucun des $\sigma(\mathfrak{q}_1)$, pour $\sigma \in \mathrm{Gal}(L/K_A)$.

C'est un lemme classique : si un idéal I est contenu dans une réunion $\mathfrak{p}_1 \cup \dots \cup \mathfrak{p}_s$ d'idéaux premiers, il est contenu dans l'un d'eux. Comme ce résultat n'est pas dans le cours, nous allons le redémontrer, par récurrence sur s. On peut supposer $s \geq 2$ et que I n'est contenu dans aucune réunion de $s-1$ des $\mathfrak{p}_i$. On choisit alors pour chaque $j \in \{1, \dots, s\}$ un $a_j \in I - \bigcup_{i \neq j} \mathfrak{p}_i$; on a $a_j \in \mathfrak{p}_j$.

Posons $a := a_1 \cdots a_{s-1}$. On a $a \in \mathfrak{p}_1 \cap \dots \cap \mathfrak{p}_{s-1}$ et $a \notin \mathfrak{p}_s$, puisqu'aucun des facteurs n'est dans $\mathfrak{p}_s$ et que cet idéal est premier. Alors $a + a_s$ ne peut être dans $\mathfrak{p}_s$, puisque a_s y est mais pas a. Il ne peut être non plus dans aucun des $\mathfrak{p}_1, \dots, \mathfrak{p}_{s-1}$ puisque a y est mais pas a_s. Comme il est dans I, c'est absurde.

Dans notre cas, par 1), $\mathfrak{q}_2$ n'est contenu dans aucun des $\sigma(\mathfrak{q}_1)$, donc il n'est pas contenu dans leur réunion.

3) Montrer $\prod_{\sigma \in \mathrm{Gal}(L/K_A)} \sigma(x) \in A$.

Posons $y := \prod_{\sigma \in \mathrm{Gal}(L/K_A)} \sigma(x)$. Il est invariant sous l'action de $\mathrm{Gal}(L/K_A)$ donc est dans K_A. D'autre part, on a déjè remarqué plus haut que chaque $\sigma(x)$, donc aussi y, est dans C, donc entier sur A. Comme A est intégralement clos, on a $y \in A$.

4) En déduire une contradiction.

Parmi les éléments de $\mathrm{Gal}(L/K_A)$ se trouve l'identité. On a donc $y \in \mathfrak{q}_2$, puis $y \in \mathfrak{q}_2 \cap A = \mathfrak{p} \subset \mathfrak{q}_1$. Comme $\mathfrak{q}_1$ est un idéal premier, cela contredit le fait qu'aucun des $\sigma(x)$ n'est dans $\mathfrak{q}_1$ (car $\sigma(x) \in \mathfrak{q}_1$ est la même chose que $x \in \sigma^{-1}(\mathfrak{q}_1)$).

III. Montrer que les fibres de l'application canonique $\iota^\sharp : \mathrm{Spec}(B) \to \mathrm{Spec}(A)$ sont finies.

Grâce au lemme III.10.3 du cours, on sait que l'application $\mathrm{Spec}(C) \to \mathrm{Spec}(B)$ est surjective. La partie II montre que les fibres de la composée $\mathrm{Spec}(C) \to \mathrm{Spec}(B) \to \mathrm{Spec}(A)$ sont finies. On en déduit que les fibres de $\mathrm{Spec}(B) \to \mathrm{Spec}(A)$ sont aussi finies.

IV. Montrer le « going-down » : si $\mathfrak{p}_1 \subset \mathfrak{p}_2$ sont des idéaux premiers de A et $\mathfrak{q}_2$ un idéal premier de B au-dessus de $\mathfrak{p}_2$, il existe un idéal premier $\mathfrak{q}_1$ de B au-dessus de $\mathfrak{p}_1$ tel que $\mathfrak{q}_1 \subset \mathfrak{q}_2$.

Grâce au lemme III.10.3 du cours, il existe des idéaux premiers $\mathfrak{r}_2 \subset C$ au-dessus de $\mathfrak{q}_2$ et $\mathfrak{r}'_1 \subset C$ au-dessus de $\mathfrak{p}_1$. Par le going-up, on peut trouver $\mathfrak{r}'_2 \subset C$ contenant $\mathfrak{r}'_1$ au-dessus de $\mathfrak{p}_2$. Mais alors $\mathfrak{r}_2$ et $\mathfrak{r}'_2$ sont au-dessus de $\mathfrak{p}_2$, donc il existe (par la partie II) $\sigma \in \mathrm{Gal}(L/K_A)$ tel que $\sigma(\mathfrak{r}'_2) = \mathfrak{r}_2$. Posant $\mathfrak{r}_1 := \sigma(\mathfrak{r}'_1)$, on a $\mathfrak{r}_1 \subset \mathfrak{r}_2$ et $\mathfrak{r}_1 \cap A = \mathfrak{r}'_1 \cap A = \mathfrak{p}_1$. Posant $\mathfrak{q}_1 := \mathfrak{r}_1 \cap B$, on a $\mathfrak{q}_1 \cap A = \mathfrak{p}_1$ et $\mathfrak{q}_1 \subset \mathfrak{r}_2 \cap B = \mathfrak{q}_2$.

V. Le but de cette partie est de montrer que l'application $\iota^\sharp : \mathrm{Spec}(B) \to \mathrm{Spec}(A)$ est ouverte.

1) Soit $b \in B$ et soit $P(X) = X^n + a_{n-1}X^{n-1} + \dots + a_1 X + a_0 \in K_A[X]$ le polynôme minimal de b sur K_A. Montrer $P \in A[X]$.

Comme b est entier sur A, il existe un polynôme unitaire $Q \in A[X]$ tel que $Q(b) = 0$. Par définition du polynôme minimal, P divise Q. Comme A est intégralement clos, le lemme III.6.17 du cours entraîne que P est à coefficients dans A.

2) Soit $\mathfrak{q} \in D(b)$. Montrer $\iota^\sharp(\mathfrak{q}) \in \bigcup_{i=0}^{n-1} D(a_i)$.

Posons $\mathfrak{p} := \iota^\sharp(\mathfrak{q}) = \mathfrak{q} \cap A$. Si tous les a_i sont dans $\mathfrak{p}$, on a $b^n \in \mathfrak{q}$, donc $b \in \mathfrak{q}$ puisque $\mathfrak{q}$ est un idéal premier, ce qui contredit $\mathfrak{q} \in D(b)$. On a donc bien $\iota^\sharp(\mathfrak{q}) \in \bigcup_{i=0}^{n-1} D(a_i)$.

3) Supposons inversement $\mathfrak{p} \in \bigcup_{i=0}^{n-1} D(a_i)$. Notons R le sous-anneau $A[b]$ de B.

a) Supposons $b \in \sqrt{\mathfrak{p}R}$. Montrer qu'il existe $m \geq 1$ et $a'_0, \ldots, a'_{n-1} \in \mathfrak{p}$ tels que $b^m = \sum_{i=0}^{n-1} a'_i b^i$.

Cela résulte du fait que R est un A-module libre de base $(1, b, \ldots, b^{n-1})$ et que $b^m \in \mathfrak{p}R$ pour un $m \geq 1$.

b) Montrer que X^m est divisible par $\bar{P}(X) = X^n + \bar{a}_{n-1}X^{n-1} + \cdots + \bar{a}_1 X + \bar{a}_0$ dans $(A/\mathfrak{p})[X]$ et en déduire une contradiction.

Par définition du polynôme minimal, P divise le polynôme $X^m - \sum_{i=0}^{n-1} a'_i X^i \in A[X]$ dans $K_A[X]$, donc aussi dans $A[X]$ par le même lemme III.6.17 que ci-dessus. En passant modulo $\mathfrak{p}$, on obtient le résultat, puisque chaque a'_i est dans $\mathfrak{p}$. Comme $(A/\mathfrak{p})[X]$ est un anneau intègre, cela entraîne que tous les $\bar{a}_i$ sont nuls, ce qui contredit l'hypothèse $\mathfrak{p} \in \bigcup_{i=0}^{n-1} D(a_i)$.

c) On a donc $b \notin \sqrt{\mathfrak{p}R}$. Montrer qu'il existe un idéal premier $\mathfrak{q}_2$ de R contenant $\mathfrak{p}R$ tel que $b \notin \mathfrak{q}_2$. On pose $\mathfrak{p}_2 := \mathfrak{q}_2 \cap A$.

Comme $\sqrt{\mathfrak{p}R}$ est l'intersection des idéaux premiers de R contenant $\mathfrak{p}R$, il existe un tel idéal ne contenant pas b.

d) Montrer qu'il existe $\mathfrak{q} \in \mathrm{Spec}(R)$ avec $\mathfrak{q} \subset \mathfrak{q}_2$ et $\mathfrak{q} \cap A = \mathfrak{p}$.

Cela résulte du going-down appliqué à l'extension entière $A \hookrightarrow R$.

e) En déduire $\mathfrak{p} \in \iota^\sharp(D(b))$.

Comme B est entier sur R, il existe $\mathfrak{r} \in \mathrm{Spec}(B)$ au-dessus de $\mathfrak{q}$ (lemme III.10.3 du cours). On a $\mathfrak{r} \in D(b)$, puisque sinon $b \in \mathfrak{r} \cap R = \mathfrak{q} \subset \mathfrak{q}_2$. On a ainsi montré $\mathfrak{p} = \iota^\sharp(\mathfrak{r}) \in \iota^\sharp(D(b))$.

4) En déduire que l'application $\iota^\sharp : \mathrm{Spec}(B) \to \mathrm{Spec}(A)$ est ouverte.

On a montré que pour tout $b \in B$, on a $\iota^\sharp(D(b)) = \bigcup_{i=0}^{n-1} D(a_i)$. C'est donc un ouvert de $\mathrm{Spec}(A)$. Comme tout ouvert de $\mathrm{Spec}(B)$ est réunion d'ouvert du type $D(b)$, l'application $\iota^\sharp$ est ouverte.