Examen Algèbre 2

Responsable : Mr O. DEBARRE

Exercice 1. Le polynôme $X^5 - 5X^2 + 1 \in \mathbf{Q}[X]$ est-il résoluble par radicaux ?

Exercice 2. Soient $u_1, \ldots, u_n$ des éléments de $\mathbf{Z}^n$ linéairement indépendants dans l'espace vectoriel $\mathbf{Q}^n$ et soit $M \subset \mathbf{Z}^n$ le sous-groupe abélien qu'ils engendrent.

a) Montrer que le cardinal du groupe quotient $\mathbf{Z}^n/M$ est égal à la valeur absolue du déterminant des vecteurs $u_1, \ldots, u_n$ dans la base canonique de $\mathbf{Z}^n$.

b) Dans le cas $n = 3$ et $u_1 = (2, 1, 1)$, $u_2 = (1, 2, 1)$ et $u_3 = (1, 1, 2)$, déterminer le groupe $\mathbf{Z}^3/M$.

Exercice 3. Soit A un anneau noethérien. Montrer que tout morphisme surjectif d'anneaux $u : A \to A$ est bijectif (*Indication :* on pourra considérer les noyaux des itérés de u).

Exercice 4. Soit A un anneau intégralement clos de corps des fractions K et soit $K \hookrightarrow L$ une extension algébrique de corps. Montrer qu'un élément de L est entier sur A si et seulement si son polynôme minimal sur K est à coefficients dans A.

Exercice 5. Soit K un corps. Dans l'anneau $A := K[X, Y, Z]$, on note I l'idéal (XY, YZ, ZX).

a) Trouver une décomposition primaire minimale de I. Quels sont les idéaux premiers associés ? Lesquels sont immergés ? Quelle est la décomposition de $V(I)$ en composantes irréductibles ? Quelle est la dimension de l'anneau A/I ?

b) Mêmes questions pour l'idéal $J = (X^2, XY, YZ, ZX)$.

Exercice 6. Soit A un anneau noethérien.

a) Soient I et J des idéaux de A. Montrer que $I = (I : J)$ si et seulement si J n'est contenu dans aucun idéal premier associé à I.

b) Montrer que l'ensemble des éléments nilpotents de A est l'intersection des idéaux premiers associés à l'idéal (0), tandis que l'ensemble des diviseurs de 0 est la réunion de ces mêmes idéaux.

Exercice 7. Soit A une $\mathbf{Z}$-algèbre de type fini.

a) Soit $\mathfrak{m}$ un idéal maximal de A. Dans toute la suite, on note $\mathbf{Z} \cap \mathfrak{m}$ l'image inverse de $\mathfrak{m}$ par l'application canonique $\mathbf{Z} \to A$. Montrer que l'anneau quotient $\mathbf{Z}/(\mathbf{Z} \cap \mathfrak{m})$ est soit $\mathbf{Z}$, soit un corps fini.

b) Montrer que le corps $A/\mathfrak{m}$ est un espace vectoriel de dimension finie sur le corps de fractions de $\mathbf{Z}/(\mathbf{Z} \cap \mathfrak{m})$ (*Indication :* on pourra utiliser le Nullstellensatz faible).

c) Si $\mathbf{Z} \cap \mathfrak{m} = 0$, montrer qu'on arrive à une contradiction. En déduire que le corps $A/\mathfrak{m}$ est fini.

d) Soit $f \in A$ un élément non nilpotent et soit $\mathfrak{n}$ un idéal maximal de l'anneau de fractions (non nul) A_f. Montrer que le corps $A_f/\mathfrak{n}$ est fini.

e) En déduire que $A/A \cap \mathfrak{n}$ est un corps fini.

f) Montrer que l'intersection de tous les idéaux maximaux de A est $\sqrt{(0)}$.

g) En déduire que les points fermés sont denses dans toute partie fermée de $\mathrm{Spec}(A)$.

Corrigé de l'examen Algèbre 2

Responsable : Mr O. DEBARRE

Exercice 1. *Le polynôme $X^5 - 5X^2 + 1 \in \mathbf{Q}[X]$ est-il résoluble par radicaux ?*

Montrons tout d'abord que ce polynôme P est irréductible. Posons $X = Y - 1$; on a $P(X) = (Y - 1)^5 - 5(Y - 1)^2 + 1$. On peut appliquer le critère d'Eisenstein avec $p = 5$ pour en déduire que P est irréductible dans $\mathbf{Q}[X]$. Son groupe de Galois G s'identifie alors à un sous-groupe de $\mathfrak{S}_5$ qui opère transitivement sur l'ensemble des 5 racines. Son cardinal est donc divisible par 5 (on peut aussi arguer que si x est une racine de P dans un corps de rupture, le cardinal de G, qui est le degré du corps de décomposition de P, est divisible par le degré $[\mathbf{Q} : \mathbf{Q}(x)] = 5$ de la sous-extension $\mathbf{Q} \subset \mathbf{Q}(x)$). Par le théorème de Sylow, G contient un élément d'ordre 5, qui est nécessairement un 5-cycle.

D'autre part, une étude de fonction montre que P a exactement 3 racines réelles. La conjugaison complexe, qui est dans G, opère comme une transposition.

Le sous-groupe $G \subset \mathfrak{S}_5$ contient un 5-cycle et une transposition. Il est donc égal à $\mathfrak{S}_5$ donc n'est pas résoluble. Le polynôme $X^5 - 5X^2 + 1 \in \mathbf{Q}[X]$ n'est donc pas résoluble par radicaux.

Exercice 2. *Soient $u_1, \ldots, u_n$ des éléments de $\mathbf{Z}^n$ linéairement indépendants dans l'espace vectoriel $\mathbf{Q}^n$ et soit $M \subset \mathbf{Z}^n$ le sous-groupe abélien qu'ils engendrent.*

a) Montrer que le cardinal du groupe quotient $\mathbf{Z}^n/M$ est égal à la valeur absolue du déterminant des vecteurs $u_1, \ldots, u_n$ dans la base canonique de $\mathbf{Z}^n$.

On applique le théorème de la base adaptée : il existe une base $(e_1, \ldots, e_n)$ de $\mathbf{Z}^n$ et des entiers strictement positifs $d_1 \mid \cdots \mid d_n$ tels que $(d_1e_1, \ldots, d_ne_n)$ soit une base de M. Le groupe $\mathbf{Z}^n/M$ est alors isomorphe à $(\mathbf{Z}/d_1\mathbf{Z}) \times \cdots \times (\mathbf{Z}/d_n\mathbf{Z})$. D'autre part, les matrices de changement de base de la base canonique de $\mathbf{Z}^n$ à la base $(e_1, \ldots, e_n)$, et de la base $(u_1, \ldots, u_n)$ de M à la base $(d_1e_1, \ldots, d_ne_n)$, sont toutes deux de déterminant ± 1. Le résultat en découle.

b) Dans le cas $n = 3$ et $u_1 = (2, 1, 1)$, $u_2 = (1, 2, 1)$ et $u_3 = (1, 1, 2)$, déterminer le groupe $\mathbf{Z}^3/M$.

Comme expliqué dans le cours, on réduit la matrice $\begin{pmatrix} 2 & 1 & 1 \\ 1 & 2 & 1 \\ 1 & 1 & 2 \end{pmatrix}$ par opérations élémentaires. On obtient (aux signes près) la matrice $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 4 \end{pmatrix}$ (les coefficients peuvent se calculer directement à partir des mineurs). Le groupe $\mathbf{Z}^3/M$ est donc $\mathbf{Z}/4\mathbf{Z}$.

Exercice 3. *Soit A un anneau noethérien. Montrer que tout morphisme surjectif d'anneaux $u : A \to A$ est bijectif.*

Comme A est noethérien, la suite croissante d'idéaux $(\mathrm{Ker}(u^n))_{n \geq 0}$ stationne : il existe un entier N tel que $\mathrm{Ker}(u^N) = \mathrm{Ker}(u^{N+1})$. Montrons que u est injectif. Soit $y \in A$ tel que $u(y) = 0$. Comme u est surjectif, u^N est surjectif et il existe $x \in A$ tel que $y = u^N(x)$. On a alors $0 = u(y) = u^{N+1}(x)$, donc $x \in \mathrm{Ker}(u^{N+1}) = \mathrm{Ker}(u^N)$. On en déduit $0 = u^N(x) = y$.

Exercice 4. *Soit A un anneau intégralement clos de corps des fractions K et soit $K \hookrightarrow L$ une extension algébrique de corps. Montrer qu'un élément de L est entier sur A si et seulement si son polynôme minimal sur K est à coefficients dans A.*

Supposons $x \in L$ entier sur A, de polynôme minimal P sur K. Comme x est aussi racine d'un polynôme unitaire $Q \in A[X]$, le polynôme P divise Q, donc toutes les racines de P (dans un corps de décomposition) sont aussi racines de Q et sont ainsi entières sur A. Il en est alors de même des coefficients de P, puisque ce sont les polynômes symétriques en les racines. Puisque ces coefficients sont dans K et que A est intégralement clos, ils sont dans A. On peut aussi utiliser le lemme 8.25 du cours qui donne directement $P \in A[X]$.

Inversement, si le polynôme minimal de $x \in L$ est à coefficients dans A, il est clair par définition que x est entier sur A.

Exercice 5. *Soit K un corps. Dans l'anneau $A := K[X,Y,Z]$, on note I l'idéal (XY, YZ, ZX).*

a) Trouver une décomposition primaire minimale de I. Quels sont les idéaux premiers associés ? Lesquels sont immergés ? Quelle est la décomposition de $V(I)$ en composantes irréductibles ? Quelle est la dimension de l'anneau A/I ?

L'idéal I n'est pas primaire : on a $XY \in I$ mais $X \notin I$ et $Y \notin \sqrt{I}$. On a $(I : Y) = (X, Z) = (I : Y^2)$ (il y a un petit raisonnement à faire), donc

$$I = ((Y) + I) \cap ((X) + I) = (Y, XZ) \cap (X, YZ).$$

L'idéal $I' = (Y, XZ)$ n'est pas primaire : on a $XZ \in I'$ mais $X \notin I'$ et $Z \notin \sqrt{I'}$. De nouveau, $(I' : Z) = (Y) = (I' : Z^2)$, donc

$$I' = ((Z) + I') \cap ((X) + I') = (Y, Z) \cap (Y, X).$$

On obtient

$$I = (X, Y) \cap (Y, Z) \cap (Z, X).$$

Tous ces idéaux sont premiers (par exemple, $K[X,Y,Z]/(X,Y)$ est isomorphe à $K[Z]$ donc est intègre). Ce sont tous les idéaux premiers associés à I, donc ils sont tous minimaux (aucun n'est immergé). On a aussi

$$V(I) = V(X,Y) \cup V(Y,Z) \cup V(Z,X),$$

qui est la décomposition en composantes irréductibles de $V(I)$. On a

$$\dim(A/I) = \dim(V(I)) = \max(\dim(V(X,Y)), \dim(V(Y,Z)), \dim(V(Z,X))) = 1$$

puisque, par exemple,

$$\dim(V(X,Y)) = \dim(A/(X,Y)) = \dim(K[Z]) = 1.$$

b) Mêmes questions pour l'idéal $J = (X^2, XY, YZ, ZX)$.

L'idéal J n'est pas primaire : on a $YZ \in J$ mais $Y \notin J$ et $Z \notin \sqrt{J}$. On a $(J : Z) = (X, Y) = (J : Z^2)$, donc

$$J = ((Y) + J) \cap ((Z) + J) = (Y, X^2, ZX) \cap (Z, X^2, XY).$$

Posons $J' = (Z, X^2, XY)$. On a vu dans le cours $(X^2, XY) = (X) \cap (X^2, Y)$, donc

$$J' = (X, Z) \cap (X^2, Y, Z)$$

et

$$J = (X, Y) \cap (X, Z) \cap (X^2, Y, Z).$$

Les idéaux premiers associés sont (X, Y), (X, Z) et (X, Y, Z). Seul le dernier est immergé. On a encore $\dim(A/J) = 1$.

Exercice 6. *Soit A un anneau noethérien.*

a) Soient I et J des idéaux de A. Montrer que $I = (I : J)$ si et seulement si J n'est contenu dans aucun idéal premier associé à I.

Soit $I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n$ une décomposition primaire minimale de I. Posons $\mathfrak{p}_j = \sqrt{\mathfrak{q}_j}$, de sorte que $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ sont les idéaux premiers associés à I.

Montrons la contraposée. Si $I \not\subset (I : J)$, il existe $x \notin I$ tel que $xJ \subset I$. Il existe alors j tel que $x \notin \mathfrak{q}_j$. Pour tout $y \in J$, on a $xy \in I \subset \mathfrak{q}_j$, donc $y \in \mathfrak{p}_j$. On a montré $J \subset \mathfrak{p}_j$.

Inversement, supposons $J \subset \mathfrak{p}_j$. Il existe $x \in A$ tel que $\mathfrak{p}_j = (I : x)$, c'est-à-dire $xJ \subset x\mathfrak{p}_j \subset I$. On a donc $x \in (I : J)$, mais $x \notin I$, puisqu'on aurait sinon $\mathfrak{p}_j = (I : x) = A$.

b) Montrer que l'ensemble des éléments nilpotents de A est l'intersection des idéaux premiers associés à l'idéal (0), *tandis que l'ensemble des diviseurs de 0 est la réunion de ces mêmes idéaux.*

Soit $(0) = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n$ une décomposition primaire minimale. En prenant les radicaux, on obtient

$$\sqrt{(0)} = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_n,$$

ce qui répond à la première question, puisque $\sqrt{(0)}$ est l'ensemble des éléments nilpotents de A.

Soit $x \in A$. Appliquons a) avec $I = (0)$ et $J = (x)$. On a $(0) \not\subset ((0) : (x))$ si et seulement s'il existe $y \neq 0$ tel que $xy = 0$, c'est-à-dire si et seulement si x est un diviseur de zéro. Par a), c'est le cas si et seulement si x est dans un des $\mathfrak{p}_j$.

Exercice 7. *Soit A une $\mathbf{Z}$-algèbre de type fini.*

a) Soit $\mathfrak{m}$ un idéal maximal de A. Dans toute la suite, on note $\mathbf{Z} \cap \mathfrak{m}$ l'image inverse de $\mathfrak{m}$ par l'application canonique $\mathbf{Z} \to A$. Montrer que l'anneau quotient $\mathbf{Z}/(\mathbf{Z} \cap \mathfrak{m})$ est soit $\mathbf{Z}$, soit un corps fini.

L'idéal $\mathbf{Z} \cap \mathfrak{m}$ de $\mathbf{Z}$ est premier, donc il est soit nul, soit engendré par un nombre premier.

b) Montrer que le corps $A/\mathfrak{m}$ est un espace vectoriel de dimension finie sur le corps de fractions de $\mathbf{Z}/(\mathbf{Z} \cap \mathfrak{m})$.

Il existe $a_1, \ldots, a_n \in A$ tel que tout élément de A peut s'écrire comme un polynôme en $a_1, \ldots, a_n$ à coefficients dans $\mathbf{Z}$. Tout élément de $A/\mathfrak{m}$ peut alors s'écrire comme polynôme en $\bar{a}_1, \ldots, \bar{a}_n$ à coefficients dans $\mathbf{Z}/(\mathbf{Z} \cap \mathfrak{m})$. Le corps $A/\mathfrak{m}$ est donc une extension de type fini du corps des fractions de $\mathbf{Z}/(\mathbf{Z} \cap \mathfrak{m})$. Par le Nullstellensatz faible, c'est une extension finie.

c) Si $\mathbf{Z} \cap \mathfrak{m} = 0$, montrer qu'on arrive à une contradiction. En déduire que le corps $A/\mathfrak{m}$ est fini.

Si $\mathbf{Z} \cap \mathfrak{m} = 0$, on prend une base $(e_1, \ldots, e_m)$ du $\mathbf{Q}$-espace vectoriel $A/\mathfrak{m}$ et des générateurs $\bar{a}_1, \ldots, \bar{a}_n$ de la $\mathbf{Z}$-algèbre $A/\mathfrak{m}$. Il existe un entier q tel que $q\bar{a}_1, \ldots, q\bar{a}_n \in \mathbf{Z}e_1 \oplus \cdots \oplus \mathbf{Z}e_m$, de sorte que

$$\mathbf{Q}e_1 \oplus \cdots \oplus \mathbf{Q}e_m = A/\mathfrak{m} \subset \mathbf{Z}[1/q]e_1 \oplus \cdots \oplus \mathbf{Z}[1/q]e_m,$$

ce qui est absurde. Le corps $\mathbf{Z}/(\mathbf{Z} \cap \mathfrak{m})$ est donc fini, ainsi que le corps $A/\mathfrak{m}$, puisque c'en est une extension finie.

d) Soit $f \in A$ un élément non nilpotent et soit $\mathfrak{n}$ un idéal maximal de l'anneau de fractions (non nul) A_f. Montrer que le corps $A_f/\mathfrak{n}$ est fini.

L'anneau A_f est encore une $\mathbf{Z}$-algèbre de type fini (avec les notations de b), elle est engendrée par $a_1, \ldots, a_n, 1/f$, donc le corps $A_f/\mathfrak{n}$ est fini.

e) En déduire que $A/A \cap \mathfrak{n}$ est un corps fini.

Le sous-anneau (intègre) $A/A \cap \mathfrak{n}$ du corps fini $A_f/\mathfrak{n}$ est aussi fini, donc c'est un corps (fini).

f) Montrer que l'intersection de tous les idéaux maximaux de A est $\sqrt{(0)}$.

L'idéal $A \cap \mathfrak{n}$ de A est donc maximal, et ne contient pas f, donc $f \notin \bigcap_{\mathfrak{m} \subset A \text{ maximal}} \mathfrak{m}$.

g) En déduire que les points fermés sont denses dans toute partie fermée de $\operatorname{Spec}(A)$.

Si I est un idéal de A, on applique ce qui précède à la $\mathbf{Z}$-algèbre de type fini A/I : l'intersection des idéaux maximaux de A contenant I est le radical de I.