Examen Algèbre 2

Responsable : Mr O. DEBARRE

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

Exercice. Soit A un anneau noethérien qui n'a qu'un seul idéal premier, que l'on note $\mathfrak{p}$.

a) Montrer qu'il existe un entier $n > 0$ tel que $\mathfrak{p}^n = (0)$.

b) Montrer que toute suite décroissante d'idéaux de A est stationnaire (*Indication :* on pourra procéder par récurrence sur un entier n tel que $\mathfrak{p}^n = (0)$).

Problème 1. Soit K un corps. Le but de cet problème est de donner une démonstration directe de l'égalité

$$\dim(K[X_1, \dots, X_n]) = n$$

pour tout entier n.

Soit A un anneau.

a) Soit x un élément de A. Montrer que $S_x := \{x^m(1 + ax) \mid m \in \mathbf{N},\ a \in A\}$ est une partie multiplicative de A.

b) Soit $\mathfrak{p}$ un idéal premier de A contenu dans un idéal maximal $\mathfrak{m}$ de A. Montrer que pour tout $x \in A$, on a $\mathfrak{m} \cap S_x \neq \varnothing$ et que pour tout $x \in \mathfrak{m} - \mathfrak{p}$, on a $\mathfrak{p} \cap S_x = \varnothing$.

c) Soit n un entier ≥ 0. Montrer que les propriétés suivantes sont équivalentes :

(i) $\dim(A) \leq n$;

(ii) pour tout $x \in A$, on a $\dim(S_x^{-1}A) \leq n - 1$.

d) Soit n un entier ≥ 0. En déduire que les propriétés suivantes sont équivalentes :

(i) $\dim(A) \leq n$;

(ii) pour tous $x_0, \dots, x_n \in A$, il existe $a_0, \dots, a_n \in A$ et $m_0, \dots, m_n \in \mathbf{N}$ tels que

$$x_0^{m_0}(x_1^{m_1}(\cdots(x_{n-2}^{m_{n-2}}(x_{n-1}^{m_{n-1}}(x_n^{m_n}(1 + a_n x_n) + a_{n-1}x_{n-1}) + a_{n-2}x_{n-2}) + \cdots) + a_1 x_1) + a_0 x_0) = 0.$$

e) On suppose que A est une K-algèbre et que toute famille $(x_0, \dots, x_n)$ d'éléments de A est algébriquement dépendante sur K. Montrer que l'on a $\dim(A) \leq n$ (*Indication :* on pourra ordonner les monômes intervenant dans une relation de dépendance algébrique entre $x_0, \dots, x_n$ selon l'ordre lexicographique).

f) En déduire $\dim(K[X_1, \dots, X_n]) = n$.

Problème 2. Soit $P(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in \mathbf{Z}[X]$ un polynôme unitaire à coefficients entiers. Notons $z_1, \dots, z_n$ ses racines complexes (non nécessairement simples) et $K := \mathbf{Q}(z_1, \dots, z_n) \subset \mathbf{C}$ le corps de décomposition de P et posons $G := \mathrm{Gal}(K/\mathbf{Q})$.

Soit p un nombre premier. Le but de ce problème est de comparer le groupe G au groupe de Galois $\bar{G}$ du polynôme

$$\bar{P}(X) = X^n + \bar{a}_{n-1}X^{n-1} + \cdots + \bar{a}_0 \in \mathbf{F}_p[X],$$

où $\bar{a}_i$ désigne la classe de l'entier a_i dans $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$.

Soit A le sous-anneau $\mathbf{Z}[z_1, \dots, z_n]$ de K.

a) Montrer que l'action du groupe G sur K laisse A stable.

b) Pour tout a dans A, on pose $N(a) = \prod_{g\in G} g(a)$. Montrer $N(a) \in \mathbf{Z}$.

c) Soit p un nombre premier. En déduire que l'idéal pA de A est distinct de A.

d) Soit $\mathfrak{m}$ un idéal maximal de A contenant pA. Montrer que $k := A/\mathfrak{m}$ est un corps de décomposition pour le polynôme $\bar{P}$ défini plus haut.

On pose $D_\mathfrak{m} := \{g \in G \mid g(\mathfrak{m}) = \mathfrak{m}\}$. Lorsque g décrit $G - D_\mathfrak{m}$, les $g(\mathfrak{m})$ décrivent un ensemble fini $\{\mathfrak{m}_1, \ldots, \mathfrak{m}_r\}$, peut-être vide, d'idéaux maximaux de A distincts deux à deux et distincts de $\mathfrak{m}$.

e) Montrer que $D_\mathfrak{m}$ est un sous-groupe de G.

f) Pour tout $i \in \{1, \ldots, r\}$, montrer que l'on a $\mathfrak{m} + \mathfrak{m}_i = A$.

g) Montrer $\mathfrak{m} + \mathfrak{m}_1 \cdots \mathfrak{m}_r = A$.

h) Montrer qu'il existe $x \in A$ dont la classe $\bar{x}$ dans k engendre l'extension $\mathbf{F}_p \subset k$.

i) Montrer qu'il existe $z \in A$ tel que $\bar{z} = \bar{x}$ et $g(z) \in \mathfrak{m}$ pour tout $g \in G - D_\mathfrak{m}$.

j) Montrer que le polynôme $\mu(X) := \prod_{g\in G}(X - g(z))$ est à coefficients dans $\mathbf{Z}$.

Tout $g \in D_\mathfrak{m}$ laisse stable A et $\mathfrak{m}$, donc définit un élément de $\bar{G}$ que l'on note $\bar{g}$.

k) Si $\sigma \in \bar{G}$, déduire de j) qu'il existe $g \in D_\mathfrak{m}$ tel que $\sigma(\bar{x}) = \bar{g}(\bar{x})$, puis que le morphisme

$$\begin{array}{rcl} \psi : D_\mathfrak{m} & \to & \bar{G} \\ g & \mapsto & \bar{g} \end{array}$$

est surjectif.

l) Si le polynôme $\bar{P}$ est séparable, montrer que ψ est un isomorphisme.

m) Quelle est la nature du groupe $\bar{G}$?

Corrigé de l'examen Algèbre 2

Responsable : Mr O. DEBARRE

Exercice. *Soit A un anneau noethérien qui n'a qu'un seul idéal premier, que l'on note $\mathfrak{p}$.*

a) Montrer qu'il existe un entier $n > 0$ tel que $\mathfrak{p}^n = (0)$.

Dans tout anneau, l'ensemble des éléments nilpotents est l'intersection des idéaux premiers, donc ici $\mathfrak{p}$. Tout élément de $\mathfrak{p}$ est donc nilpotent, et comme on est dans un anneau noethérien, il existe $n > 0$ tel que $\mathfrak{p}^n = (0)$.

b) Montrer que toute suite décroissante d'idéaux de A est stationnaire.

Si $n = 1$, l'anneau $A = A/\mathfrak{p}$ est un corps et c'est clair.

Si $n > 1$, on pose $A' = A/\mathfrak{p}^{n-1}$. C'est encore un anneau avec un seul idéal premier, $\mathfrak{p}' := \mathfrak{p}/\mathfrak{p}^{n-1}$, et $\mathfrak{p}'^{n-1} = (0)$. Si $(I_j)_{j\in\mathbf{N}}$ est une suite décroissante d'idéaux de A, on note $I'_j := (I_j+\mathfrak{p}^{n-1})/\mathfrak{p}^{n-1} \simeq I_j/(I_j\cap\mathfrak{p}^{n-1})$ l'image de I_j dans A'. Alors $(I'_j)_{j\in\mathbf{N}}$ est une suite décroissante d'idéaux de A'. Par hypothèse de récurrence, elle est stationnaire. De même, $(I_j\cap\mathfrak{p}^{n-1})_{j\in\mathbf{N}}$ est une suite décroissante de sous-A-modules du A-module $\mathfrak{p}^{n-1}$. Comme $\mathfrak{p}^n = (0)$ et que $\mathfrak{p}$ est un idéal maximal (donc $A/\mathfrak{p}$ est un corps), ce dernier est en fait un $A/\mathfrak{p}$-espace vectoriel, de dimension finie (car A étant noethérien, $\mathfrak{p}^{n-1}$ est de type fini), donc la suite $(I_j \cap \mathfrak{p}^{n-1})_{j\in\mathbf{N}}$ est aussi stationnaire, puisque deux sous-espaces vectoriels emboîtés de même dimension sont égaux. On a donc, pour $j \gg 0$, à la fois $I_j/(I_j\cap\mathfrak{p}^{n-1}) = I_{j+1}/(I_{j+1}\cap\mathfrak{p}^{n-1})$ et $I_j\cap\mathfrak{p}^{n-1} = I_{j+1}\cap\mathfrak{p}^{n-1}$, ce qui entraîne facilement $I_j = I_{j+1}$.

Problème 1. *Soit A un anneau.*

a) Soit x un élément de A. Montrer que $S_x := \{x^m(1+ax) \mid n \geq 0,\ a \in A\}$ est une partie multiplicative de A.

On a $1 \in S_x$ et $x^m(1+ax)x^n(1+bx) = x^{m+n}(1+(a+b+abx)x)$, donc S_x est une partie multiplicative.

b) Soit $\mathfrak{p}$ un idéal premier de A contenu dans un idéal maximal $\mathfrak{m}$ de A. Montrer que pour tout $x \in A$, on a $\mathfrak{m}\cap S_x \neq \varnothing$ et que pour tout $x \in \mathfrak{m}-\mathfrak{p}$, on a $\mathfrak{p}\cap S_x = \varnothing$.

Si $x \in \mathfrak{m}$, on a $x \in \mathfrak{m}\cap S_x$. Si $x \notin \mathfrak{m}$, on a $A = Ax + \mathfrak{m}$ et on peut écrire $1 = ax + y$, avec $a \in A$ et $y \in \mathfrak{m}$, et $y \in \mathfrak{m}\cap S_x$. Dans tous les cas, $\mathfrak{m}\cap S_x \neq \varnothing$.

Si $x \in \mathfrak{m}-\mathfrak{p}$ et $y = x^m(1+ax) \in \mathfrak{p}\cap S_x$, on a $1+ax \in \mathfrak{p}$ (car $\mathfrak{p}$ est premier et $x \notin \mathfrak{p}$) et $1 = (1+ax)-ax \in \mathfrak{m}$, ce qui est absurde.

c) Soit n un entier ≥ 0. Montrer que les propriétés suivantes sont équivalentes :

(i) $\dim(A) \leq n$;

(ii) *pour tout $x \in A$, on a* $\dim(S_x^{-1}A) \leq n-1$.

La dimension de $S_x^{-1}A$ est le supremum des longueurs des chaînes finies d'idéaux premiers de $S_x^{-1}A$, c'est-à-dire des chaînes d'idéaux premiers de A ne rencontrant pas S_x.

Supposons (i). Toute chaîne d'idéaux premiers de $S_x^{-1}A$ de longueur m correspond à une chaîne d'idéaux premiers de A de longueur m qui commence par un idéal premier $\mathfrak{p}_m$ de A qui n'est pas maximal (par b)). On peut donc ajouter à cette chaîne un idéal maximal de A contenant $\mathfrak{p}_m$, ce qui augmente la longueur de la chaîne de 1. On a donc $m \leq n-1$.

Inversement, supposons (ii). On veut montrer que toute chaîne finie d'idéaux premiers de A est de longueur $\leq n$. On peut supposer qu'une telle chaîne commence par un idéal maximal $\mathfrak{p}_m$ et qu'elle est de longueur $m > 0$ (sinon, il n'y a rien à montrer). Si $x \in \mathfrak{p}_m - \mathfrak{p}_{m-1}$, la chaîne $\mathfrak{p}_{m-1} \supsetneq \cdots \supsetneq \mathfrak{p}_0$ correspond alors (par b)) à une chaîne d'idéaux premiers de $S_x^{-1}A$. On a donc bien $m-1 \leq n-1$ par (ii).

d) Soit n un entier ≥ 0. En déduire que les propriétés suivantes sont équivalentes :

(i) $\dim(A) \leq n$;

(ii) *pour tous $x_0, \ldots, x_n \in A$, il existe $a_0, \ldots, a_n \in A$ et $m_0, \ldots, m_n \in \mathbf{N}$ tels que*

$$x_0^{m_0}(x_1^{m_1}(\cdots(x_{n-2}^{m_{n-2}}(x_{n-1}^{m_{n-1}}(x_n^{m_n}(1+a_nx_n)+a_{n-1}x_{n-1})+a_{n-2}x_{n-2})+\cdots)+a_1x_1)+a_0x_0) = 0.$$

Procédons par récurrence sur n. Pour $n = 0$, c'est la question c) : les anneaux de dimension < 0 sont les anneaux nuls et $S_x^{-1}A = 0$ si et seulement si $0 \in S_x$.

Supposons $n > 0$. Toujours par c), (i) est équivalente à ce que toutes les localisations $S_x^{-1}A$ sont de dimension $\leq n-1$, donc par hypothèse de récurrence, puisqu'on peut toujours écrire des éléments de $S_x^{-1}A$ avec le même dénominateur, à ce que pour tout $t \in S_x$ et tous $x_0, \dots, x_{n-1} \in A$, il existe $b_0, \dots, b_{n-1} \in S_x^{-1}A$ et $m_0, \dots, m_{m-1} \in \mathbf{N}$ tels que

$$\Big(\frac{x_0}{t}\Big)^{m_0}\Big(\Big(\frac{x_1}{t}\Big)^{m_1}\Big(\cdots\Big(\Big(\frac{x_{n-2}}{t}\Big)^{m_{n-2}}\Big(\Big(\frac{x_{n-1}}{t}\Big)^{m_{n-1}}\Big(1+\frac{b_{n-1}x_{n-1}}{t}\Big)+\frac{b_{n-2}x_{n-2}}{t}\Big)+\cdots\Big)+\frac{b_1x_1}{t}\Big)+\frac{b_0x_0}{t}\Big)=0$$

dans $S_x^{-1}A$. Ceci est encore équivalent à

$$x_0^{m_0}(x_1^{m_1}(\cdots(x_{n-2}^{m_{n-2}}(x_{n-1}^{m_{n-1}}(t+b'_{n-1}x_{n-1})+b'_{n-2}x_{n-2})+\cdots)+b'_1x_1)+b'_0x_0)=0$$

dans $S_x^{-1}A$, où $b'_j = b_j t^{m_{n-1}+\cdots+m_{j+1}}$. On voit donc que (i) est équivalent à ce que pour tout $x \in A$, tout $t \in S_x$ et tous $x_0, \dots, x_{n-1} \in A$, il existe $b_0, \dots, b_{n-1} \in S_x^{-1}A$ et $m_0, \dots, m_{m-1} \in \mathbf{N}$ tels que

$$x_0^{m_0}(x_1^{m_1}(\cdots(x_{n-2}^{m_{n-2}}(x_{n-1}^{m_{n-1}}(t+b_{n-1}x_{n-1})+b_{n-2}x_{n-2})+\cdots)+b_1x_1)+b_0x_0)=0 \tag{1}$$

dans $S_x^{-1}A$. Écrivant $b_i = a_i/s$, avec $a_0, \dots, a_{n-1} \in A$ et $s \in S_x$, on arrive à

$$x_0^{m_0}(x_1^{m_1}(\cdots(x_{n-2}^{m_{n-2}}(x_{n-1}^{m_{n-1}}(st+a_{n-1}x_{n-1})+a_{n-2}x_{n-2})+\cdots)+a_1x_1)+a_0x_0)=0$$

dans $S_x^{-1}A$, c'est-à-dire à ce que (i) est équivalent à ce que pour tout $x \in A$, tout $t \in S_x$ et tous $x_0, \dots, x_{n-1} \in A$, il existe $s, u \in S_x$, $a_0, \dots, a_{n-1} \in A$ et $m_0, \dots, m_{m-1} \in \mathbf{N}$ tels que

$$x_0^{m_0}(x_1^{m_1}(\cdots(x_{n-2}^{m_{n-2}}(x_{n-1}^{m_{n-1}}(stu+a_{n-1}ux_{n-1})+a_{n-2}ux_{n-2})+\cdots)+a_1ux_1)+a_0ux_0)=0$$

dans A. Ceci entraîne (ii).

Inversement, on peut énoncer (ii) ainsi : pour tout $x \in A$, tous $x_0, \dots, x_{n-1} \in A$, il existe $s \in S_x$, $a_0, \dots, a_{n-1} \in A$ et $m_0, \dots, m_{n-1} \in \mathbf{N}$ tels que

$$x_0^{m_0}(x_1^{m_1}(\cdots(x_{n-2}^{m_{n-2}}(x_{n-1}^{m_{n-1}}(s+a_{n-1}x_{n-1})+a_{n-2}x_{n-2})+\cdots)+a_1x_1)+a_0x_0)=0$$

dans A, donc dans $S_x^{-1}A$. En multipliant par t/s (t quelconque dans S_x), on obtient une forme de (1), ce qui prouve (i).

e) On suppose que A est une K-algèbre et que toute famille $(x_0, \dots, x_n)$ d'éléments de A est algébriquement dépendante sur K. Montrer que l'on a $\dim(A) \leq n$.

Soient $x_0, \dots, x_n \in A$. Il existe une relation polynomiale $P(x_0, \dots, x_n) = 0$, avec $P \in K[X_1, \dots, X_n]$ non nul. Ordonnons les monômes non nuls de P selon l'ordre lexicographique ; on peut donc écrire P sous la forme

$$tX_0^{m_0}\cdots X_n^{m_n} + X_0^{m_0}\cdots X_n^{m_n+1}P_n + X_0^{m_0}\cdots X_{n-1}^{m_{n-1}+1}P_{n-1} + \cdots + X_0^{m_0}X_1^{m_1+1}P_1 + X_0^{m_0+1}P_0,$$

avec $t \in K^*$ et $P_i \in K[X_i, \dots, X_n]$. C'est exactement une relation du type d)(ii), avec $a_i = \frac{1}{t}P_i(x_i, \dots, x_n)$.

f) En déduire $\dim(K[X_1, \dots, X_n]) = n$.

L'inégalité $\dim(K[X_1, \dots, X_n]) \geq n$ résulte de l'existence de la chaîne d'idéaux premiers

$$(X_1, \dots, X_n) \supsetneq \cdots \supsetneq (X_1) \supsetneq (0).$$

D'autre part, la prop. III.12.2.a) du cours dit qu'une famille d'éléments algébriquement indépendants de $K[X_1, \dots, X_n]$ a au plus n éléments. On a donc $\dim(K[X_1, \dots, X_n]) \leq n$ par e).

Problème 2. *Soit $P(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in \mathbf{Z}[X]$ un polynôme unitaire à coefficients entiers. Notons $z_1, \dots, z_n$ ses racines complexes (éventuellement confondues) et $K := \mathbf{Q}(z_1, \dots, z_n) \subset \mathbf{C}$ le corps de décomposition de P et posons $G := \mathrm{Gal}(K/\mathbf{Q})$. Soit A le sous-anneau $\mathbf{Z}[z_1, \dots, z_n]$ de K.*

a) Montrer que l'action du groupe G sur K laisse A stable.

Cela résulte du fait que G agit trivialement sur $\mathbf{Z}$ et permute les z_i.

b) Pour tout a dans A, on pose $N(a) = \prod_{g\in G} g(a)$. Montrer $N(a) \in \mathbf{Z}$.

Les z_i sont entiers sur $\mathbf{Z}$, donc A est une extension entière de $\mathbf{Z}$ par le cours. De plus, comme l'action de G sur K laisse A stable, $N(a)$ est entier sur $\mathbf{Z}$ par le cours. Il est d'autre part invariant sous l'action de G, donc il est dans $K^G = \mathbf{Q}$ (par la théorie de Galois, puisque l'extension $\mathbf{Q} \subset K$ est normale (c'est un corps de décomposition) et séparable (on est en caractéristique 0)). On a vu en cours que tout rationnel entier sur $\mathbf{Z}$ est dans $\mathbf{Z}$, donc $N(a) \in \mathbf{Z}$.

c) Soit p un nombre premier. En déduire que l'idéal pA de A est distinct de A.

Si $A = pA$, on peut écrire $1 = pa$, avec $a \in A$. On applique N et on obtient

$$1 = N(1) = N(pa) = \prod_{g\in G} g(pa) = \prod_{g\in G} pg(a) = p^{\mathrm{Card}(G)}N(a),$$

ce qui est absurde puisque $N(a) \in \mathbf{Z}$. On a donc $A \neq pA$.

d) Soit $\mathfrak{m}$ un idéal maximal de A contenant pA. Montrer que $k := A/\mathfrak{m}$ est un corps de décomposition pour le polynôme $\bar{P}(X) = X^n + \bar{a}_{n-1}X^{n-1} + \cdots + \bar{a}_0 \in \mathbf{F}_p[X]$, où $\bar{a}_i$ désigne la classe de l'entier a_i dans $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$.

Le morphisme canonique $\mathbf{Z} \to A \to A/pA \to k$ se factorise par $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$, donc k est une extension de $\mathbf{F}_p$. L'anneau k est engendré par les classes de $z_1, \ldots, z_n$ et on a $\bar{P}(X) = \prod_{i=1}^n (X - \bar{z}_i)$, donc k est un corps de décomposition pour $\bar{P}$.

On pose $D_\mathfrak{m} := \{g \in G \mid g(\mathfrak{m}) = \mathfrak{m}\}$. Lorsque g décrit $G - D_\mathfrak{m}$, les $g(\mathfrak{m})$ décrivent un ensemble fini $\{\mathfrak{m}_1, \ldots, \mathfrak{m}_r\}$, peut-être vide, d'idéaux maximaux de A distincts deux à deux et distincts de $\mathfrak{m}$.

e) Montrer que $D_\mathfrak{m}$ est un sous-groupe de G.

C'est clair.

f) Pour tout $i \in \{1, \ldots, r\}$, montrer que l'on a $\mathfrak{m} + \mathfrak{m}_i = A$.

Comme $\mathfrak{m}_i \not\subset \mathfrak{m}$ (sinon, étant tous les deux maximaux, ils seraient égaux), l'idéal $\mathfrak{m} + \mathfrak{m}_i$ contient strictement l'idéal maximal $\mathfrak{m}$: il est donc égal à A.

g) Montrer $\mathfrak{m} + \mathfrak{m}_1 \cdots \mathfrak{m}_r = A$.

Par d), on peut écrire $1 = a_i + m_i$, avec $a_i \in \mathfrak{m}$ et $m_i \in \mathfrak{m}_i$. On a alors $1 = \prod_{i=1}^r (a_i + m_i) = m + m_1 \cdots m_r$, où m est une somme de produits dans lesquels au moins un des a_i apparaît. On a donc $m \in \mathfrak{m}$.

h) Montrer qu'il existe $x \in A$ dont la classe $\bar{x}$ dans k engendre l'extension $\mathbf{F}_p \subset k$.

C'est un conséquence du théorème de l'élément primitif (l'extension $\mathbf{F}_p \subset k$ est séparable puisque $\mathbf{F}_p$ est parfait).

i) Montrer qu'il existe $z \in A$ tel que $\bar{z} = \bar{x}$ et $g(z) \in \mathfrak{m}$ pour tout $g \in G - D_\mathfrak{m}$.

Écrivons comme plus haut $1 = m + m'$, avec $m \in \mathfrak{m}$ et $m' \in \mathfrak{m}_1 \cdots \mathfrak{m}_r$ et posons $z = xm'$. On a alors $\bar{z} = \bar{x}$. Si $g \in G - D_\mathfrak{m}$, on a $g^{-1}(\mathfrak{m}) = \mathfrak{m}_i$ pour un certain i, et $g(z) = g(x)g(m')$, avec $g(m') \in g(\mathfrak{m}_1 \cdots \mathfrak{m}_r) \subset g(\mathfrak{m}_i) = \mathfrak{m}$, donc $g(z) \in \mathfrak{m}$.

j) Montrer que le polynôme $\mu(X) := \prod_{g\in G}(X - g(z))$ est à coefficients dans $\mathbf{Z}$.

Ce polynôme est invariant par l'action de G. Ses coefficients sont donc fixes sous cette action, donc dans $\mathbf{Q}$. Ils sont d'autre part dans A donc entiers sur $\mathbf{Z}$. Comme $\mathbf{Z}$ est intégralement clos, ils sont dans $\mathbf{Z}$.

Tout $g \in D_\mathfrak{m}$ laisse stable A et $\mathfrak{m}$, donc définit un élément de $\bar{G}$ que l'on note $\bar{g}$.

k) Si $\sigma \in \bar{G}$, déduire de j) qu'il existe $g \in D_\mathfrak{m}$ tel que $\sigma(\bar{x}) = \bar{g}(\bar{x})$, puis que le morphisme $D_\mathfrak{m} \to \bar{G}$, $g \mapsto \bar{g}$ est surjectif.

Notons $\bar{\mu}$ l'image de μ dans $\mathbf{F}_p[X]$. Puisque $g(z) \in \mathfrak{m}$ pour tout $g \in G - D_\mathfrak{m}$, on a

$$\bar{\mu}(X) := \prod_{g\in G} (X - \bar{g}(\bar{z})) = \prod_{g\in D_\mathfrak{m}} (X - \bar{g}(\bar{x})) \prod_{g\notin D_\mathfrak{m}} X.$$

Le polynôme $\mu(X)_\mathfrak{m} := \prod_{g\in D_\mathfrak{m}}(X - \bar{g}(\bar{x}))$ est donc aussi à coefficients dans $\mathbf{F}_p$. Comme $\bar{x}$ en est une racine, $\sigma(\bar{x})$ aussi ; c'est donc l'un des $\bar{g}(\bar{x})$, pour un $g \in D_\mathfrak{m}$. Puisque $k = \mathbf{F}_p(\bar{x})$, l'automorphisme $\bar{g}$ est égal à σ.

l) Si le polynôme $\bar{P}$ est séparable, montrer que ψ est un isomorphisme.

Si $\bar{z}_1, \ldots, \bar{z}_n$ sont distincts, $z_1, \ldots, z_n$ aussi. Si $\bar{g}$ est l'identité, il est l'identité comme permutation de $\bar{z}_1, \ldots, \bar{z}_n$, donc comme permutation de $z_1, \ldots, z_n$. C'est donc l'identité : ψ est injective.

m) Quelle est la nature du groupe $\bar{G}$?

C'est un groupe cyclique d'ordre n (où $\mathrm{Card}(k) = p^n$) engendré par l'automorphisme de Frobenius (prop. I.8.1 du cours).