Ecole Normale Supérieure FIMFA 2017–2018

Algèbre II

Examen du 17 janvier 2018. Durée 3h00.
Seul document autorisé : le poly du cours. Smartphones éteints.

Exercice 1. Soit $A := \mathbb{Q}[T]$ et $K := \mathbb{Q}(T)$. Pour un entier $n > 1$, considérons le polynôme

$$f = X^n - TX - T \in A[X].$$

Si $t \in \mathbb{Q}$ on note $f_t = X^n - tX - t \in \mathbb{Q}[X]$ le polynôme f spécialisé en $T = t$.

i. Montrer que f est irréductible et séparable dans $K[X]$. On notera K_f un corps de décomposition de f sur K et $G_f := \mathrm{Gal}(K_f/K)$.

Le critère d'Eisenstein appliqué avec l'élément irréductible T de l'anneau principal A assure que f est irréductible dans $K[T]$. Il est donc séparable puisqu'on est en caractéristique 0.

ii. Montrer que $f_{\frac{1}{2}}$ est le produit d'un polynôme irréductible de degré $n-1$ de $\mathbb{Q}[X]$ et d'un facteur de degré 1. En déduire qu'il existe une racine de f dans K_f dont le stabilisateur dans G_f agit transitivement sur les autres racines, puis en déduire que G_f agit *doublement* transitivement sur les racines de f dans K_f.

Un calcul montre que $f_{\frac{1}{2}} = (X-1)g$ avec $g = (X^{n-1} + X^{n-2} + \cdots + X + \frac{1}{2})$. Le polynôme $2Y^{n-1}g(\frac{1}{Y})$ est Eisenstein en 2 donc irréductible, et il s'ensuit que g l'est aussi. Le polynôme $f_{\frac{1}{2}}$ est donc séparable et son groupe de Galois coïncide avec celui de g, donc agit transitivement sur les racines de g. Par le théorème de spécialisation, il existe une bijection $\alpha \mapsto \tilde{\alpha}$ entre racines de $f_{\frac{1}{2}}$ dans $\overline{\mathbb{Q}}$ et racines de f dans K_f ainsi qu'un plongement $\iota : G_{f_{\frac{1}{2}}} \hookrightarrow G_f$ compatible avec les actions respectives sur les racines. Le groupe $\iota(G_f)$ stabilise donc la racine $\tilde{1}$ de f et permute transitivement les autres racines de f. A fortiori, le stabilisateur de $\tilde{1}$ dans G_f permute les autres racines de f. Puisque G_f agit transitivement sur les racines de f, le stabilisateur de n'importe quelle racine agit transitivement sur les autres racines. Soient maintenant (α, β) et (α', β') deux couples de racines distinctes. Il existe $\sigma \in G_f$ tel que $\sigma(\alpha) = \alpha'$ et $\sigma' \in G_f$ tel que $\sigma'(\alpha') = \alpha'$ et $\sigma'(\sigma(\beta) = \beta'$. Alors $\sigma'\sigma$ envoie α sur α' et β sur β'.

iii. Si $t \neq 0$, montrer que $\mathrm{pgcd}(f_t, f_t')$ divise $X - \frac{n}{1-n}$. En déduire que f_t est séparable sauf lorsque $t = t_0 := \frac{n^n}{(1-n)^{n-1}}$, auquel cas f_{t_0} est de la forme $(X - \frac{n}{1-n})^2 g_{t_0}$ avec g_{t_0} séparable et $g_{t_0}(\frac{n}{1-n}) \neq 0$.

On voit que $\mathrm{pgcd}(f_t, f_t')$ divise $nf_t' - Xf_t = t(1-n)(X - \frac{n}{1-n})$. La seule racine multiple possible est donc $\frac{n}{1-n}$ et elle est au plus double. On calcule que c'est effectivement une racine si et seulement si $t = t_0$.

TSVP

iv. Montrer que $\mathrm{disc}(f) = (-1)^{n(n-1)/2}T^{n-1}(n-1)^{n-1}(t_0 - T)$. *On pourra utiliser la formule (en la justifiant)* $\mathrm{disc}(f) = (-1)^{n(n-1)/2}\det(f'(M_f))$ *où* M_f *est la matrice compagnon de* f.

On a dans le cours la formule $\mathrm{disc}(f) = (-1)^{n(n(-1)/2}\prod_{i=1}^n f'(\alpha_i)$ où les α_i sont les racines de f dans K_f. Ce sont aussi les valeurs propres de la matrice compagnon M_f, donc a bien la formule $\mathrm{disc}(f) = (-1)^{n(n-1)/2}\det(f'(M_f))$ (si on diagonalise M_f alors $f'(M_f)$ est aussi diagonalisée dans la même base et ses v.p. sont les $f'(\alpha_i)$). On a $f' = nX^{n-1} - T$. On calcule que M_f^{n-1} est la matrice

$$\begin{bmatrix} 0 & T & 0 & \cdots & \cdots & 0 \\ \vdots & T & T & 0 & \cdots & 0 \\ \vdots & 0 & T & T & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \cdots & \cdots & 0 & T & T \\ 1 & 0 & \cdots & \cdots & 0 & T \end{bmatrix} \text{ donc } f'(M_f) = \begin{bmatrix} -T & nT & 0 & \cdots & \cdots & 0 \\ 0 & (n-1)T & nT & 0 & \cdots & 0 \\ \vdots & 0 & (n-1)T & nT & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \cdots & \cdots & 0 & (n-1)T & nT \\ n & 0 & \cdots & \cdots & 0 & (n-1)T \end{bmatrix} \text{ et il}$$

reste à courageusement calculer le déterminant en développant selon la première colonne.

v. Soit A_f la sous-A-algèbre de K_f engendrée par les racines de f et $\overline{A}_f := A_f/(T-t_0)A_f$.

(a) Montrer que $\overline{A}_f$ est une $\mathbb{Q}$-algèbre de dimension $|G_f| = [K_f : K]$.

C'est dans le cours. On montre d'abord que A_f est un A-module de type fini. Comme il est sans torsion et A principal, il est libre. Comme il engendre K_f comme K-ev, il est de rang $[K_f : K]$. Réduire modulo $(T - t_0)$ revient à tensoriser par $\mathbb{Q} = A/(T - t_0)A$ et préserve donc le rang.

(b) Montrer que A_f contient une racine carrée δ de $\mathrm{disc}(f)$ et que l'image $\bar{\delta}$ de δ dans $\overline{A}_f$ est un nilpotent d'ordre 2 *non nul*.

Si on numérote les racines, alors $\delta := \prod_{i<j}(\alpha_i - \alpha_j) \in A_f$ est une racine carrée de $\mathrm{disc}(f)$. Puisque $(T - t_0)|\mathrm{disc}(f) = \delta^2$, on a en effet $\bar{\delta}^2 = 0$. Supposons que $\bar{\delta} = 0$. Alors il existe $\beta \in A_f$ tel que $\delta = (T - t_0)\beta$ et donc $\mathrm{disc}(f) = (T - t_0)^2\beta^2$. Donc $\beta^2 \in K \cap A_f$. Mais A_f est fini donc entier sur A et A est principal donc intégralement clos, donc $\beta^2 \in A$. On obtient que $(T - t_0)^2|\mathrm{disc}(f)$ dans A, ce qui n'est pas le cas.

(c) Soit $\mathfrak{m}$ un idéal maximal de $\overline{A}_f$. Montrer qu'il existe deux racines α, β de f dans A_f telles que :

- $\bar{\alpha} = \bar{\beta} = \frac{n}{1-n}$ dans $\overline{A}_f/\mathfrak{m}$
- $\{\text{racines de } f \text{ dans } A_f\} \setminus \{\alpha, \beta\} \xrightarrow{\sim} \{\text{racines de } g_{t_0} \text{ dans } \overline{A}_f/\mathfrak{m}\}$ via $\gamma \mapsto \bar{\gamma}$.

En déduire que $\overline{A}_f/\mathfrak{m}$ est un corps de décomposition de g_{t_0} sur $\mathbb{Q}$.

$\overline{A}_f/\mathfrak{m}[X]$ est un anneau factoriel (car principal) dans lequel on a d'une part une factorisation $f_{t_0} = (X - \frac{n}{1-n})^2 g_0$ par la question iii), et d'autre part une factorisation $f_{t_0} = \prod_{i=1}^n (X - \bar{\alpha}_i)$ où les α_i sont les racines de f dans K_f et les $\bar{\alpha}_i$ désignent leurs images dans $\overline{A}_f/\mathfrak{m}$. L'unicité des factorisations implique qu'il existe $\alpha = \alpha_i$ et $\beta = \alpha_j$ telles que $\bar{\alpha} = \bar{\beta} = \frac{n}{1-n}$ et que les autres racines $\bar{\alpha}_k$ sont les racines de g_{t_0}. Comme celui-ci est séparable, l'application de réduction est bien bijective. *On remarquera ici que les deux factorisations de* f *sont valables dans* $\overline{A}_f[X]$*, mais qu'il n'est pas possible dans déduire une identification des "racines" car l'anneau* $\overline{A}_f[X]$ *n'est pas factoriel (ni même intègre ou réduit). De fait, les racines* α, β *dépendent du choix de* $\mathfrak{m}$.).

TSVP

(d) Expliquer pourquoi l'action de G_f sur A_f induit une action sur $\overline{A}_f$ par automorphismes de $\mathbb{Q}$-algèbres. Soit $G_{f,\mathfrak{m}} := \{\sigma \in G_f, \sigma(\mathfrak{m}) = \mathfrak{m}\}$ le stabilisateur de $\mathfrak{m}$ dans G_f. Expliquer pourquoi l'action de $G_{f,\mathfrak{m}}$ sur $\overline{A}_f$ induit une action sur $\overline{A}_f/\mathfrak{m}$ donnée par un morphisme de groupes $G_{f,\mathfrak{m}} \xrightarrow{\rho_{\mathfrak{m}}} \mathrm{Gal}((\overline{A}_f/\mathfrak{m})/\mathbb{Q})$.

le fait que les actions "passent au quotient" découle dans chaque cas de la propriété universelle des quotients

(e) Expliquer pourquoi G_f agit sur $\mathrm{Max}(\overline{A}_f)$. Soit $\mathcal{O}_{\mathfrak{m}} \subset \mathrm{Max}(\overline{A}_f)$ l'orbite de $\mathfrak{m}$ sous G_f. Montrer que le morphisme produit $\overline{A}_f \longrightarrow \prod_{\mathfrak{n}\in\mathcal{O}_{\mathfrak{m}}} \overline{A}_f/\mathfrak{n}$ est surjectif, *mais pas injectif*. En déduire l'inégalité stricte $|G_{f,\mathfrak{m}}| > [\overline{A}_f/\mathfrak{m} : \mathbb{Q}] = |G_{g_0}|$, et donc aussi que le morphisme $\rho_{\mathfrak{m}}$ n'est pas injectif.

La surjectivité découle du lemme Chinois. Pour le défaut d'injectivité, on remarque que $\overline{A}_f$ n'est pas réduite (puisque $\bar{\delta}$ est un nilpotent non trivial) alors que le produit de droite est un produit de corps, donc est réduit. En comparant les dimensions et en utilisant le fait que $\dim_{\mathbb{Q}}(\overline{A}_f/\mathfrak{n})$ est indépendant de $\mathfrak{n} \in \mathcal{O}_{\mathfrak{m}}$ (c'est la dimension d'un corps de décomposition de g_{t_0}), on obtient $|G_f| > |G_f/G_{f,\mathfrak{m}}||G_{g_{t_0}}|$.

(f) Montrer qu'un élément $\sigma \neq \mathrm{id}$ du noyau de $\rho_{\mathfrak{m}}$ est nécessairement la transposition (α, β).

D'après la question c) et la définition de $\rho_{\mathfrak{m}}$, l'élément σ fixe toutes les racines de f autres que α et β. Etant non trivial, il échange α et β.

vi. Montrer que $G_f \simeq \mathfrak{S}_n$. *Remarque : joint au théorème de spécialisation de Hilbert, ceci permet de voir que $\mathfrak{S}_n$ est groupe de Galois sur $\mathbb{Q}$ pour tout n.*

G_f contient une transposition $\sigma = (\alpha, \beta)$. Il est doublement transitif donc si α', β' sont deux autres racines disctinctes, il existe τ envoyant α sur α' et β sur β'. Mais alors $\tau\sigma\tau^{-1}$ est la transposition (α', β'). Donc G_f contient toutes les transpositions, et c'est bien $\mathfrak{S}_n$.

Exercice 2. Soit $A \subset B$ une extension d'anneaux entière (tout $b \in B$ est entier sur A).

i. Montrer que si A et B sont intègres, A est un corps si et seulement si B est un corps.

Si A est un corps, tout $b \in B$ engendre une A-algèbre de dimension finie intègre, donc est un corps, donc b est inversible s'il est non nul, et B est bien un corps. Si B est un corps, alors soit $a \neq 0$ dans A. Son inverse a^{-1} dans B est entier sur A donc il existe un entier n et des éléments $a_1, \cdots a_{n-1}$ de A tels que $a^{-n} = \sum_{i=0}^{n-1} a_i a^{-i}$. Donc $a^{-1} = \sum_{i=0}^{n-1} a_i a^{n-1-i} \in A$.

ii. Montrer que si $\mathfrak{q} \in \mathrm{Spec}(B)$, alors $\mathfrak{q} \in \mathrm{Max}(B) \Leftrightarrow \mathfrak{q} \cap A \in \mathrm{Max}(A)$.

Par passage au quotient, on obtient un morphisme injectif d'anneaux intègres $A/(\mathfrak{q}\cap A) \hookrightarrow B/\mathfrak{q}$. On vérifie immédiatement qu'il est encore entier (en relevant les éléments) et on peut donc appliquer la question i).

iii. ("*lying over*") Soit $\mathfrak{p} \in \mathrm{Spec}(A)$. On veut montrer qu'il existe $\mathfrak{q} \in \mathrm{Spec}(B)$ tel que $\mathfrak{q} \cap A = \mathfrak{p}$. Posons $A_{\mathfrak{p}} = S^{-1}A$ et $B_{\mathfrak{p}} = S^{-1}B$ avec $S = A \setminus \mathfrak{p}$.

TSVP

(a) Montrer que le morphisme canonique $A_\mathfrak{p} \longrightarrow B_\mathfrak{p}$ déduit de l'inclusion $A \subset B$ fait de $B_\mathfrak{p}$ une extension entière de $A_\mathfrak{p}$.

Montrons que le morphisme est injectif. Si $\frac{a}{s} \in S^{-1}A$ devient nul dans $S^{-1}B$, il existe $t \in S$ tel que $ta = 0$ dans B. Mais $ta \in A \subset B$ est alors nul et $\frac{a}{s}$ est nul dans $S^{-}A$ aussi. Montrons que cette inclusion est entière. Soit $\frac{b}{s} \in B_\mathfrak{p}$. Soient n et a_i tels que $0 = b^n + a_1 b^{n-1} + \cdots + a_n$. Alors $(\frac{b}{s})^n + \frac{a_1}{s}(\frac{b}{s})^{n-1} + \cdots \frac{a_n}{s^n} = 0$ donc $\frac{b}{s}$ est entier sur $S^{-1}A$.

(b) Soit $\mathfrak{q} \in \mathrm{Spec}(B)$ l'image réciproque d'un idéal maximal de $B_\mathfrak{p}$. Montrer que $\mathfrak{q} \cap A = \mathfrak{p}$.

Soit $\mathfrak{m} \in \mathrm{Max}(B_\mathfrak{p})$. D'après ii, $\mathfrak{m} \cap A_\mathfrak{p} \in \mathrm{Max}(A_\mathfrak{p})$ donc $\mathfrak{m} \cap A_\mathfrak{p} = \mathfrak{p}A_\mathfrak{p}$ (puisque $A_\mathfrak{p}$ a pour seul idéal maximal $\mathfrak{p}A_\mathfrak{p}$.) On a des diagrammes commutatif

$$\begin{array}{ccc} A & \longrightarrow & A_\mathfrak{p} \\ \downarrow & & \downarrow \\ B & \longrightarrow & B_\mathfrak{p} \end{array} \quad \text{et} \quad \begin{array}{ccc} \mathrm{Spec}(A) & \longleftarrow & \mathrm{Spec}(A_\mathfrak{p}) \\ \uparrow & & \uparrow \\ \mathrm{Spec}(B) & \longleftarrow & \mathrm{Spec}(B_\mathfrak{p}) \end{array}$$

(le second obtenu en appliquant Spec au premier) qui montrent que l'image réciproque $\mathfrak{q}$ de $\mathfrak{m}$ dans B s'envoie sur celle de $\mathfrak{p}A_\mathfrak{p}$ dans A qui n'est autre que $\mathfrak{p}$.

iv. ("*going up*") Soient $\mathfrak{p}, \mathfrak{p}' \in \mathrm{Spec}(A)$ tels que $\mathfrak{p} \subset \mathfrak{p}'$ et $\mathfrak{q} \in \mathrm{Spec}(B)$ tel que $\mathfrak{q} \cap A = \mathfrak{p}$. Montrer qu'il existe $\mathfrak{q}' \in \mathrm{Spec}(B)$ tel que $\mathfrak{q} \subset \mathfrak{q}'$ et $\mathfrak{q}' \cap A = \mathfrak{p}'$.

On a déjà vu qu'on a par passage au quotient un morphisme injectif et entier $A/\mathfrak{p} \longrightarrow B/\mathfrak{q}$. L'image $\mathfrak{p}'/\mathfrak{p}$ de $\mathfrak{p}'$ dans $A/\mathfrak{p}$ est un idéal premier auquel on peut appliquer iii) pour obtenir un idéal premier $\bar{\mathfrak{q}}'$ de $B/\mathfrak{q}$ dont la trace sur $A/\mathfrak{p}$ est $\mathfrak{p}'/\mathfrak{p}$. Il suffit alors de prendre l'image réciproque $\mathfrak{q}'$ de $\bar{\mathfrak{q}}'$ dans B.

v. ("*incomparability*") Nous voulons maintenant montrer que pour $\mathfrak{q}, \mathfrak{q}' \in \mathrm{Spec}(B)$ tels que $\mathfrak{q} \subset \mathfrak{q}'$, on a $(\mathfrak{q} \cap A = \mathfrak{q}' \cap A) \Rightarrow (\mathfrak{q} = \mathfrak{q}')$.

(a) Se ramener au cas où $\mathfrak{q} = 0$, et A,B intègres.

On a déjà vu qu'on a par passage au quotient un morphisme injectif et entier d'anneaux intègres $A/(\mathfrak{q} \cap A) \longrightarrow B/\mathfrak{q}$. L'énoncé est clairement équivalent à montrer que tout idéal premier $\mathfrak{q}'/\mathfrak{q}$ de $B/\mathfrak{q}$ de trace nulle sur $A/(\mathfrak{q} \cap A)$ est nul.

(b) Montrer dans ce cas que si $\mathfrak{q}' \cap A = 0$, alors $B_{\mathfrak{q}'}$ est une $\mathrm{Frac}(A)$-algèbre intègre entière, et en conclure que $\mathfrak{q}' = 0$.

Puisque B est intègre, $B_{\mathfrak{q}'}$ est aussi intègre, contenue dans $\mathrm{Frac}(B)$, et contient le localisé $A_{\mathfrak{q}' \cap A} = \mathrm{Frac}(A)$. Le corps $\mathrm{Frac}(B)$ est algébrique sur $\mathrm{Frac}(A)$, donc toute sous $\mathrm{Frac}(A)$-algèbre de $\mathrm{Frac}(B)$ est un corps, en particulier $B_{\mathfrak{q}'}$. On a donc $B_{\mathfrak{q}'} = \mathrm{Frac}(B)$ et donc $\mathfrak{q}' = 0$.

vi. (*dimension de Krull*) On appelle dimension d'un anneau A la longueur n maximale d'une chaîne $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n$ d'idéaux premiers de A. Montrer que si B est entier sur A alors $\dim(B) = \dim(A)$.

découle facilement de iv et v

TSVP

Remarque : joint au lemme de normalisation de Noether, ce résultat permet de montrer que la dimension de Krull d'une k-algèbre intègre est le degré de transcendance sur k de son corps des fractions.

Question bonus : le prouver !