M1 d'Algèbre - Examen
Juin 2009

La clarté et la concision de l'argumentation de même que la qualité de la rédaction seront des éléments importants dans l'appréciation de la copie.

On notera $\mu_{x,k}$ pour le polynôme minimal d'un élément x algébrique sur un corps k.

Les exercices sont largement indépendants les uns des autres à l'exception des questions **o** et **t** de l'exercice 5 ainsi que de la question **e** de l'exercice 6 qui toutes trois font appel aux résultats de l'exercice 3.

Exercice 1 – Groupe symétrique et parties génératrices formées de transpositions.

Partie 1.

a) Montrer que les transpositions engendrent $\mathfrak{S}_n$.

b) Soit $\sigma \in \mathfrak{S}_n$. Déterminer l'entier n_σ minimal tel que σ s'écrive comme produit de n_σ transpositions (on pourra utiliser les matrices de permutation).

c) Quels sont les $\sigma \in \mathfrak{S}_n$ tels que n_σ soit maximal. Quel est cette valeur maximale de n_σ ?

Partie 2.

d) Montrer que les transpositions de la forme $\tau_i = (i, i+1)$ pour $1 \leq i \leq n-1$ engendrent $\mathfrak{S}_n$.

e) Soit $\sigma = (i, i+2)$ avec $1 \leq i \leq n-2$. Déterminer le nombre minimum de transpositions de la forme τ_i dont le produit est égal à σ.

f) Soient $k \in [\![1\,,\, n]\!]$ et $\sigma = (i, i+k)$ avec $1 \leq i \leq n-k$. Déterminer le nombre minimum de transpositions de la forme τ_i dont le produit est σ. Comparer avec le nombre d'inversions de σ.

g) Soit $\sigma \in \mathfrak{S}_n$. Déterminer, en fonction du nombre d'inversions de σ, le nombre minimal de transpositions de la forme τ_i dont le produit est σ. On note c_σ ce nombre.

h) Déterminer la valeur maximal de c_σ. Quels sont les σ pour lesquels c_σ est maximal ?

Partie 3.

i) Montrer que les transpositions de la forme $\tau'_i = (1, i)$ pour $2 \leq i \leq n$ engendrent $\mathfrak{S}_n$.

j) Soit $\sigma \in \mathfrak{S}_n$ un cycle de longueur ℓ. Déterminer le nombre minimum de transpositions de la forme τ'_i dont le produit est σ (on prendra garde au fait que 1 peut ne pas appartenir au support de σ).

k) Soit $\sigma \in \mathfrak{S}_n$. Déterminer le nombre minimum de transpositions de la forme τ'_i dont le produit est σ. On note c'_σ ce nombre.

l) Déterminer la valeur maximal de c'_σ. Quels sont les σ pour lesquels c'_σ est maximal ?

Exercice 2 – Théorie de Galois et nombre premier. Dans tout le problème, p désigne un nombre premier. On pose $k = \mathbb{Q}(\sqrt{p})$, $\theta = \sqrt{p + \sqrt{p}}$ et $\mathrm{K} = \mathbb{Q}(\theta)$.

Partie 1.

a) Montrer que k est inclus dans K.

b) Déterminer dans l'ordre logique que vous préférez

(i) $[\mathrm{K} : \mathbb{Q}]$;
(ii) $[k : \mathbb{Q}]$;
(iii) $[\mathrm{K} : k]$;
(iv) le polynôme minimal de θ sur $\mathbb{Q}$;
(v) le polynôme minimal de θ sur k ;
(vi) les conjugués de θ sur $\mathbb{Q}$;
(vii) les conjugués de θ sur k.

c) Determiner tous les $\mathbb{Q}$-plongements de K dans $\overline{\mathbb{Q}}$.

Partie 2. On suppose dans cette partie que $p = 1 + a^2$ avec $a \in \mathbb{Z}$.

d) Montrer que l'extension $(\mathrm{K} : \mathbb{Q})$ est galoisienne.

e) Déterminer $\mathrm{Gal}(\mathrm{K} : \mathbb{Q})$ (on pourra introduire $\theta' = \sqrt{p - \sqrt{p}}$ et calculer $\theta\theta'$).

f) En déduire les sous-extensions de $(\mathrm{K} : \mathbb{Q})$.

Partie 3. On suppose dans cette question que p n'est pas de la forme $p = 1 + a^2$ où $a \in \mathbb{Z}$.

g) Montrer que $p^2 - p$ n'est pas un carré dans k. En déduire que $(\theta\theta'^{-1})^2$ n'est pas un carré dans k, donc que $k(\theta) \neq k(\theta')$.

h) Montrer que l'extension $(\mathrm{K} : \mathbb{Q})$ n'est pas galoisienne. Déterminer $\mathrm{Gal}(\mathrm{K} : \mathbb{Q})$.

i) Soit L une clôture normale de K. Calculer $[\mathrm{L} : \mathbb{Q}]$.

j) Trouver $d \in \mathbb{Z}$ tel que $\mathrm{L} = \mathbb{Q}(\theta, \sqrt{d})$. Que vaut $\mathrm{Gal}(\mathrm{L} : \mathbb{Q})$?

Exercice 3 – Étude de l'irréductibilité des polynômes de la forme $\mathrm{X}^n - a$. Dans ce problème, on désigne par k un corps. Pour $n \in \mathbb{N}$, on note $k^{[n]} = \{x^n,\ x \in k\}$ l'ensemble des puissances n-èmes de k.

Soit $a \in k$. L'objectif est de donner une caractérisation de l'irréductibilité de $\mathrm{X}^n - a$. On commence par se ramener au cas où n est une puissance d'un nombre premier (questions **a** et **b**). Puis dans les questions **c** et **d**, on traite le cas où n est un nombre premier (et même un peu plus). La partie 2 étudie le cas où n est un puissance d'un nombre premier impair. Enfin, la partie 3 traite le cas des puissances de 2.

Partie 1 : Préliminaires.

a) Soient n et m deux entiers naturels premiers entre eux et $a \in k$. Montrer l'équivalence

(i) $\mathrm{X}^n - a$ et $\mathrm{X}^m - a$ sont irréductibles sur k

(ii) $\mathrm{X}^{nm} - a$ est irréductible sur k.

b) En déduire qu'il suffit d'étudier le cas où n est une puissance d'un nombre premier.

c) Soient p un nombre premier et k un corps de caractéristique p. Montrer que si $a \in k \setminus k^{[p]}$ alors pour tout $n \in \mathbb{N}$, $\mathrm{X}^{p^n} - a$ est irréductible sur k (on pourra considérer une factorisation de $\mathrm{X}^{p^n} - a = \mathrm{QR}$ et considérer le terme de degré $(m-1)p^r$ où $\deg \mathrm{Q} = mp^r$ avec $m \wedge p = 1$).

d) Soient k un corps, q un nombre premier avec $q \neq car\, k$ et $a \in k$. Montrer que $\mathrm{X}^q - a$ est irréductible si et seulement si $a \in k \setminus k^{[q]}$ (indication : on pourra considérer une factorisation de $\mathrm{X}^q - a = \mathrm{QR}$, le terme de plus bas degré de Q et une relation de Bézout entre $\deg \mathrm{Q}$ et q).

Partie 2 : Le cas où q est impair. Soient k un corps, q un nombre premier **impair** avec $q \neq car\, k$ et $a \in k$ tel que $\mathrm{X}^q - a$ est irréductible. On note L le corps de décomposition de $\mathrm{X}^q - a$ sur k ; $\alpha \in \mathrm{L}$ une racine de L et $\mathrm{K} = k(\alpha)$.

Dans un premier temps (questions **e** à **i**), on va montrer que $\alpha \notin \mathrm{K}^{[p]}$ puis (question **j**), on montre que $\mathrm{X}^{q^n} - a$ est irréductible.

e) Montrer que L contient q racines q-èmes de l'unité. En déduire que L contient une racine q-ème primitive de l'unité qu'on note ζ.

f) Montrer que L est une extension galoisienne de k. On note $\mathrm{G} = \mathrm{Gal}(\mathrm{L} : k)$.

g) Pour tout $i \in [\![0\,,\, q-1]\!]$, montrer qu'il existe $\tau_i \in \mathrm{G}$ tel que $\tau_i(\alpha) = \zeta^i \alpha$.

h) On raisonne par l'absurde. On suppose qu'il existe $\beta \in \mathrm{K}$ tel que $\beta^q = \alpha$. On note $\beta_i = \tau_i(\beta)$. Déterminer le degré du polynôme minimal $\mu_{\beta,k}$ de β sur k, puis déterminer $\mu_{\beta,k}$ en fonction des β_i.

i) En considérant le terme de plus bas degré de $\mu_{\beta,k}$, montrer que $\alpha \notin \mathrm{K}^{[p]}$.

j) En déduire que $\mathrm{X}^{q^n} - a$ est irréductible sur k pour $n \geqslant 1$.

Partie 3 : Le cas où q est pair. Soient k un corps de caractéristique différente de 2 et $a \in k$ tel que $\mathrm{X}^2 - a$ est irréductible sur k. On note L le corps de décomposition de $\mathrm{X}^2 - a$ sur k ; $\alpha \in \mathrm{L}$ une racine de L et $\mathrm{K} = k(\alpha)$.

k) Montrer que $\mathrm{K} = \mathrm{L}$.

l) Montrer l'équivalence entre les conditions suivantes

(i) $\alpha \in \mathrm{K}^{[2]}$;

(ii) $-\alpha \in \mathrm{K}^{[2]}$;

(iii) $-4a \in k^{[4]}$.

m) On suppose que $-4a \in k^{[4]}$. Donner une factorisation de $\mathrm{X}^4 - a$ dans $k[\mathrm{X}]$.

n) En déduire que, si $-4a \in k^{[4]}$ alors pour $n \geq 2$, le polynôme $\mathrm{X}^{2^n} - a \in k[\mathrm{X}]$ est réductible.

o) On suppose que $-4a \notin k^{[4]}$. Montrer que $\mathrm{X}^4 - a$ est irréductible sur k.

p) En déduire que, si $-4a \notin k^{[4]}$ alors $\mathrm{X}^{2^n} - a$ est irréductible sur k.

Exercice 4 – Trace dans les extensions de corps. Soit $(\mathrm{L} : k)$ une extension finie. Pour $x \in \mathrm{L}$ on considère l'application k-linéaire

$$\begin{array}{rccc} m_x & \mathrm{L} & \to & \mathrm{L} \\ & y & \mapsto & xy \end{array} .$$

La trace de cette application est notée $\mathrm{Tr}_{\mathrm{L}/k}(x) \in k$, et appelée la *trace de x*.

Soit $x \in \mathrm{L}$, de polynôme minimal $\mu_{x,k} = \mathrm{X}^d - a_1\mathrm{X}^{d-1} + \ldots + (-1)^d a_d \in k[\mathrm{X}]$ égal à $\prod_{i=1}^{n}(\mathrm{X} - x_i)$ (avec $x_1 = x$) dans un corps de décomposition.

a) Montrer que $\mathrm{Tr}_{k(x)/k}(x) = a_1$.

b) Montrer que le k-espace vectoriel L est somme directe de $[\mathrm{L} : k(x)]$ sous-espaces vectoriels tous stables par m_x de sorte que les endomorphismes induits par m_x sur ces sous-espaces admettent tous une matrice commune. En déduire que $\mathrm{Tr}_{\mathrm{L}/k}(x) = [\mathrm{L} : k(x)]\mathrm{Tr}_{k(x)/k}(x)$.

c) On suppose que l'extension $(\mathrm{L} : k)$ est séparable de degré n. Soient $\sigma_1, \ldots, \sigma_n : \mathrm{L} \to \Omega$ les n homomorphismes de corps au-dessus de k. Montrer que $\mathrm{Tr}_{\mathrm{L}/k}(x) = \sum_i \sigma_i(x)$. En déduire que $\mathrm{Tr}_{\mathrm{L}/k}(x) = \sum_{\sigma \in \mathrm{Gal}(\mathrm{L}:k)} \sigma(x)$ lorsque $(\mathrm{L} : k)$ est galoisienne.

Dans les trois questions suivantes on suppose que $(\mathrm{L} : k)$ n'est pas séparable. On note p la caractéristique de k et L_s le sous-corps de L engendré sur k par l'ensemble des éléments de L séparables sur k.

d) Justifier que L_s/k est séparable.

e) Montrer que p divise $[\mathrm{L} : \mathrm{L}_s]$ (on remarquera que $\mathrm{L}_s \subsetneq \mathrm{L}$).

f) Soit $x \in \mathrm{L}$. Montrer que $\mathrm{Tr}_{\mathrm{L}/k}(x) = 0$ (on pourra distinguer deux cas selon que $x \in \mathrm{L}_s$ ou $x \notin \mathrm{L}_s$).

g) Montrer que l'extension $(\mathrm{L} : k)$ est séparable si et seulement si la condition suivante est vérifiée

$$\forall x \in \mathrm{L}^* \quad \exists y \in \mathrm{L}^* \quad \mathrm{Tr}_{\mathrm{L}/k}(xy) \neq 0 \ .$$

Dans la suite on admettra le résultat suivant : *Si $(\mathrm{L} : k)$ est une extension galoisienne cyclique de groupe de Galois engendré par σ, alors $x \in \mathrm{L}$ est de trace nulle si et seulement si il existe $\alpha \in \mathrm{L}$ tel que $\sigma(\alpha) - \alpha = x$.*

Rappel. On rappelle brièvement deux résultats de théorie de groupes qui pourront être utiles. Si G est un groupe fini d'ordre $n = p^\ell m$ avec $m \wedge p = 1$ alors il existe un sous-groupe de G d'ordre p^ℓ. Si G est un groupe d'ordre p^ℓ alors G admet des sous-groupes d'ordre p^j pour tout $j \in [\![0 , \ell]\!]$.

Exercice 5 – Extension séparable à degré divisible par un nombre premier. Dans cet exercice, l'objectif est de démontrer la proposition suivante.

Proposition 1 Soient k un corps et q un nombre premier. Si q est impair (resp $q = 2$) et k admet une extension **séparable** dont le degré est divisible par q (resp. par 4) alors k admet une extension dont le degré est divisible par q^n pour tout $n \geqslant 1$ (resp. $n \geqslant 2$).

Partie 1 : un résultat préliminaire. Soit k un corps de caractéristique p et K une extension galoisienne cyclique de k de degré p^m avec $m \geq 1$. On note σ un générateur de $\mathrm{Gal}(\mathrm{K} : k)$.

a) Montrer qu'il existe $\beta \in \mathrm{K}$ tel que $\mathrm{Tr}_{\mathrm{K}/k}(\beta) = 1$.

b) Calculer $\mathrm{Tr}_{\mathrm{K}/k}(\beta^p)$. En déduire qu'il existe $\alpha \in \mathrm{K}$ tel que $\alpha - \sigma(\alpha) = \beta^p - \beta$.

c) Montrer que le polynôme $\mathrm{P} = \mathrm{X}^p - \mathrm{X} - \alpha \in \mathrm{K}[\mathrm{X}]$ n'a pas de racine dans K (si u est une racine on pourra montrer que $u - \sigma(u) - \beta \in \mathbb{F}_p$ et calculer sa trace).

d) En déduire que P est irréductible sur K (si u est une racine de P on pourra exprimer les autres racines de P en fonction de u).

e) Soit L le corps de décomposition P sur K. Calculer $[\mathrm{L} : \mathrm{K}]$ puis $[\mathrm{L} : k]$.

f) Montrer que L/k est une extension séparable.

g) Montrer qu'on peut prolonger σ en un automorphisme de L en posant $\sigma^*(\theta) = \theta + \beta$ (où θ est une racine de P dans L). Montrer que σ^* est un automorphisme d'ordre p^{m+1}.

h) En déduire que $(\mathrm{L} : k)$ est galoisienne cyclique de degré p^{m+1} et de groupe de Galois engendré par σ^*.

Partie 2 : Où on se ramène au cas d'une extension cyclique. Dans cette partie, on suppose que k est un corps et que k admet une extension séparable de degré divisible par q^m avec q premier et $m \in \mathbb{N}^*$.

i) Montrer que k admet une extension galoisienne K de degré divisible par q^m.

j) Montrer qu'il existe une extension L de k telle que $[\mathrm{K} : \mathrm{L}] = q^m$ et $(\mathrm{K} : \mathrm{L})$ galoisienne.

k) En déduire que dans la démonstration de la proposition 1 on peut supposer que k admet une extension galoisienne $(\mathrm{K} : k)$ de degré q (resp. de degré 4). Que peut-on alors dire de $(\mathrm{K} : k)$?

Partie 3 : Le cas q impair. Soit $(\mathrm{K} : k)$ une extension galoisienne de degré q.

l) On suppose que $q = car\, k$. Montrer que k admet une extension galoisienne de degré q^n pour tout $n \in \mathbb{N}$.

On suppose pour les questions **m** à **o** que $car\, k \neq q$ et on note ζ une racine q-ème primitive de l'unité dans la clôture algébrique de K.

m) Montrer que $(\mathrm{K}(\zeta) : k)$ et $(\mathrm{K}(\zeta) : k(\zeta))$ sont galoisiennes. Calculer $[\mathrm{K}(\zeta) : k(\zeta)]$.

n) Montrer qu'il existe $x \in \mathrm{K}(\zeta)$ et $a \in k(\zeta)$ tels que $x^q - a$ et $\mathrm{K}(\zeta) = k(\zeta)(x)$.

o) En utilisant les résultats de l'exercice 3, montrer que k admet une extension dont le degré est divisible par q^n.

Partie 4 : Le cas $q = 2$. Soit $(\mathrm{K} : k)$ une extension galoisienne de degré 4.

p) On suppose que $car\, k = 2$. Montrer que k admet une extension galoisienne de degré 2^n pour tout $n \geq 2$.

On suppose pour les questions **q** à **t** que $car\, k \neq 2$ et on note i une racine 4-ème primitive de l'unité dans la clôture algébrique de K.

q) Montrer que $\mathrm{K}(i)$ est une extension galoisienne de k et de $k(i)$.

r) Montrer que $[\mathrm{K}(i) : k(i)] \in \{2, 4\}$. En déduire qu'il existe $a \in k(i)$ et $\alpha \in \mathrm{K}(i) \setminus k(i)$ tels que $\alpha^2 = a$.

s) Montrer que $-4a \notin k(i)^{[4]}$.

t) En utilisant les résultats de l'exercice 3, montrer que k admet une extension dont le degré est divisible par 2^n pour tout $n \geq 2$.

Exercice 6 — Corps à extensions bornées. L'objectif de ce problème est de déterminer (au moins partiellement) les corps k tels que l'ensemble des degrés des extensions finies de k est borné. Si k est un tel corps, on dit que k est à *extensions finies bornées* ou encore que k vérifie la propriété $\mathscr{B}$.

a) Donner des exemples de corps à extensions finies bornées.

b) On suppose que k vérifie la propriété $\mathscr{B}$, montrer que toute extension algébrique de k est finie. En déduire que la clôture algébrique de k est une extension finie de k.

c) Réciproquement, montrer que si la clôture algébrique de k est une extension finie de k alors k vérifie la propriété $\mathscr{B}$.

d) Montrer que, même si k vérifie la propriété $\mathscr{B}$, alors k admet des extensions infinies.

e) À l'aide de la question **c** de l'exercice 3, montrer que si k vérifie la propriété $\mathscr{B}$ alors k est un corps parfait.

Dans la suite (questions **f** à **j**), on suppose que k est un corps vérifiant la propriété $\mathscr{B}$ tel que k n'est pas algébriquement clos et on considére $(\mathrm{K} : k)$ une extension algébrique de degré supérieur ou égal à 2.

f) Montrer que K est de degré 2 sur k et que K est algébriquement clos.

g) Montrer que -1 n'est pas un carré dans k et que $\mathrm{K} = k(i)$ où $i^2 = -1$.

h) Montrer qu'une somme de carrés d'éléments de k est encore un carré de k (on pourra commencer par montrer que $x^2 + y^2$ est un carré, en considérant un élément $u + iv \in k(i)$ tel que $(u + iv)^2 = x + iy$.

i) En déduire que k est de caractéristique nulle.

j) Quel sont les degrés des polynômes irréductibles sur k ?

Enfin, pour terminer, une dernière question.

k) Soit k un corps algébriquement clos. Que peut-on dire de l'ordre d'un élément d'ordre fini de $\mathrm{Aut}(k)$ (on pourra distinguer le cas de la caractéristique nulle de celui de la caractéristique non nulle) ?