Université Louis Pasteur
Département de Mathématiques

Master de mathématiques 1ère année

Algèbre M1S2

Corrigé de l'examen du 11 septembre 2006

Exercice 1.

(a) Par hypothèse, P est décomposé sur L. Comme $\mathrm{car}(K) \neq 2$, on a $\partial_X P \neq 0$ et comme P est irréductible, cela implique que $\mathrm{pgcd}(P, \partial_X P) = 1$. Il s'ensuit que les racines de P dans L sont simples donc le polynôme P a 4 racines distinctes dans L.

Soit $\alpha \in L$ une racine de P, alors

$$P(-\alpha) = (-\alpha)^4 + A(-\alpha)^2 + B = P(\alpha) = 0$$

et $-\alpha$ est aussi une racine de P. Les racines de P étant simples, $\alpha \neq -\alpha$ donc les polynômes $X - \alpha$ et $X + \alpha$ sont premiers entre eux. Comme $X - \alpha$ et $X + \alpha$ divisent P, le produit $(X - \alpha)(X + \alpha)$ divise P.

Il existe une racine $\beta \in L$ de P avec $\beta \neq \pm\alpha$ et l'argument ci-dessus implique que $(X - \beta)(X + \beta)$ divise P. On déduit sans difficulté de ce qui précède que les éléments $\pm\alpha, \pm\beta$ sont distincts. Les polynômes $(X - \alpha)(X + \alpha)$ et $(X - \beta)(X + \beta)$ sont premiers entre eux donc leur produit divise encore P. Le fait que P est unitaire de degré 4 donne que

$$P(X) = (X - \alpha)(X + \alpha)(X - \beta)(X + \beta).$$

(b) Notons que D est un carré dans un corps $M \supset K$ si et seulement si le polynôme $T^2 + AT + B$ est décomposé sur M. Si D est un carré dans K, cette remarque implique que $T^2 + AT + B$ est réductible sur K, disons $T^2 + AT + B = (T - c)(T - d)$, mais alors $P(X) = (X^2 - c)(X^2 - d)$ est aussi réductible sur K, contrairement à l'hypothèse.

Comme $X^2 - \alpha^2 \in K(\alpha)[X]$ divise P, le quotient $X^2 - \beta^2$ appartient aussi à $K(\alpha)$ et $P(X) = (X^2 - \alpha^2)(X^2 - \beta^2)$ dans $K(\alpha)[X]$. Il s'ensuit que

$$T^2 + AT + B = (T - \alpha^2)(T - \beta^2)$$

dans $K(\alpha)[T]$, donc ce polynôme est réductible sur $K(\alpha)$ et par conséquent D est un carré dans $K(\alpha)$.

(c) Il suffit de montrer que $\beta \in K(\alpha)$ car cela implique que P est déjà décomposé sur $K(\alpha) \subset L$ et donc que $K(\alpha) = L$. D'après la question précédente, D est un carré dans $K(\alpha)$ et la dernière hypothèse implique que DB^{-1} est un carré dans $K(\alpha)$. Il s'ensuit que $B = (\alpha\beta)^2$ est un carré dans $K(\alpha)$ et donc que $\alpha\beta \in K(\alpha)$, ce qui donne que $\beta \in K(\alpha)$.

(d) Un résultat du cours implique que L, en tant que corps de décomposition sur K d'un polynôme à racines simples, est une extension galoisienne de K. Comme P est irréductible sur K, le groupe de Galois $\mathrm{Gal}(L/K)$ opère transitivement sur les racines de P dans L, d'où l'existence de $f \in \mathrm{Gal}(L/K)$ tel que $f(\alpha) = \beta$.

(e) Notons que $D = (\alpha^2-\beta^2)^2$ donc que $\delta = \pm(\alpha^2-\beta^2)$. Il suffit alors de montrer que $f(\alpha^2 - \beta^2) = -(\alpha^2 - \beta^2)$. Or $f(\alpha^2 - \beta^2) = \beta^2 - f(\beta^2)$ donc il suffit de déterminer $f(\beta^2)$. Comme $f(\beta^2)$ est une racine du polynôme $T^2 + AT + B$ on a $f(\beta^2) = \alpha^2$ ou β^2, et comme $f(\alpha^2) = \beta^2$ et $\alpha^2 \neq \beta^2$ (car $D \neq 0$) on doit avoir $f(\beta^2) = \alpha^2$. Cela montre bien que $f(\alpha^2 - \beta^2) = -(\alpha^2 - \beta^2)$.

(f) On sait déjà que l'extension L/K est galoisienne et que $L = K(\alpha)$ donc $|\mathrm{Gal}(L/K)| = [L : K] = 4$. Il suffit maintenant de montrer que f est d'ordre 4 dans ce groupe. Pour cela, il suffit de voir que $f^2 \neq \mathrm{id}$. Comme

$$DB^{-1} = \left(\frac{\delta}{\alpha\beta}\right)^2$$

est un carré dans K, on a $\delta(\alpha\beta)^{-1} \in K$ donc cet élément est invariant pour l'action de f. Cela donne que $f(\beta) = -\alpha$ donc $f^2(\alpha) = f(\beta) = -\alpha$ et on a bien montré que $f^2 \neq \mathrm{id}$.

Exercice 2.

(a) L'énoncé est vrai, c'est un résultat du cours.

(b) L'énoncé est vrai. Notons $p = \mathrm{car}(K)$ et $|K| = p^e$. D'après le cours, il existe un corps fini L d'ordre p^{de}. Toujours d'après le cours, K s'identifie à un sous-corps de L. Dans la suite on utilise cette identification pour considérer L comme une extension de K, on a alors $[L : K] = d$. Soit α un générateur du groupe multiplicatif de L. Alors $L = K(\alpha)$ et le polynôme minimal de α sur K est irréductible sur K et de degré d.

(c) L'énoncé est faux. Pour avoir un contre exemple, on peut prendre $K = \mathbb{Q}$, $L = \mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{C}$ et $P = X^3 - 2$. Alors P est irréductible sur K et $X - \sqrt[3]{2}$ est un facteur irréductible de P sur L, de degré 1. Comme $L \subset \mathbb{R}$ et comme P n'est pas décomposé sur $\mathbb{R}$, le polynôme P n'est pas décomposé sur L. Les facteurs irréductibles de P sur L ne sont donc pas tous de degré 1.

(d) L'énoncé est vrai. Soit Q un facteur irréductible unitaire de P dans $L[X]$. Alors pour tout $f \in \mathrm{Gal}(L/K)$, le polynôme $f(Q) \in L[X]$ est du même degré que Q et il est encore irréductible sur K. Il suffit donc de montrer que les facteurs irréductibles unitaires de P dans $L[X]$ sont exactement les polynômes $f(Q)$ pour $f \in \mathrm{Gal}(L/K)$, autrement dit que l'ensemble de ces facteurs est l'orbite de Q pour l'action de $\mathrm{Gal}(L/K)$.

D'une part, si $f \in \mathrm{Gal}(L/K)$, alors $f(Q)$ divise $f(P) = P$, donc $f(Q)$ est bien un facteur irréductible de P. D'autre part, soit $Y \subset L[X]$ l'orbite de Q pour l'action de $\mathrm{Gal}(L/K)$. Alors $R = \prod_{F \in Y} F$ est invariant pour l'action de $\mathrm{Gal}(L/K)$ donc $R \in K[X]$. Comme les différents $F \in Y$ sont premiers entre eux, R divise P et comme P est irréductible, on a $P = aR$ avec $a \in K$, $a \neq 0$. Cela montre que les éléments de Y sont exactement les facteurs irréductibles de P sur L.

Exercice 3.

(a) On a $\partial_X(X^4 - 11) = 4X^3$ donc $X^4 - 11$ et $\partial_X(X^4 - 11)$ sont premier entre eux, les racines de $X^4 - 11$ dans L sont simples et $L/\mathbb{Q}$ est une extension galoisienne. Les racines complexes de $X^4 - 11$ sont $\pm\sqrt[4]{11}$ et $\pm i\sqrt[4]{11}$ donc $L = \mathbb{Q}(i, \sqrt[4]{11})$ et il y a une suite d'extensions $\mathbb{Q} \subset \mathbb{Q}(\sqrt[4]{11}) \subset L$.

Comme $\mathbb{Q}(\sqrt[4]{11}) \subset \mathbb{R}$ on a $i \notin \mathbb{Q}(\sqrt[4]{11})$ et comme $i^2 = -1$, on conclut que i est de degré 2 sur $\mathbb{Q}(\sqrt[4]{11})$, d'où $[L : \mathbb{Q}(\sqrt[4]{11})] = 2$. Le critère d'Eisenstein implique que $X^4 - 11$ est irréductible sur $\mathbb{Q}$, donc $[\mathbb{Q}(\sqrt[4]{11}) : \mathbb{Q}] = 4$ et cela donne

$$[L : \mathbb{Q}] = [L : \mathbb{Q}(\sqrt[4]{11})] \cdot [\mathbb{Q}(\sqrt[4]{11}) : \mathbb{Q}] = 2 \cdot 4 = 8.$$

(b) On vient de voir que $L = \mathbb{Q}(i, \sqrt[4]{11})$ et comme $\bar{i} = -i \in L$ et $\overline{\sqrt[4]{11}} = \sqrt[4]{11} \in L$, le corps $L \subset \mathbb{C}$ est stable par la conjugaison complexe.

(c) Comme $L/\mathbb{Q}$ est une extension galoisienne et $\mathbb{Q}(i) \subset L$, l'extension $L/\mathbb{Q}(i)$ est également galoisienne donc $H = \mathrm{Gal}(L/\mathbb{Q}(i))$ est d'ordre $[L : \mathbb{Q}(i)] = 4$. D'après le cours, le groupe H est cyclique car $\mathbb{Q}(i)$ contient les racines 4èmes de l'unité et L est obtenu par adjonction à $\mathbb{Q}(i)$ d'une racine de $X^4 - 11$.

Il reste à montrer que $\mathrm{Gal}(L/\mathbb{Q}) = H \cup cH$. Clairement, $H \cup cH \subset \mathrm{Gal}(L/\mathbb{Q})$. La conjugaison complexe c opère non trivialement sur $\mathbb{Q}(i)$, donc $c \notin H$ et cela implique que H et cH sont disjoints. Cela donne

$$|H \cup cH| = 4 + 4 = 8 = |\mathrm{Gal}(L/\mathbb{Q})|$$

et on conclut que $\mathrm{Gal}(L/\mathbb{Q}) = H \cup cH$.

(d) La correspondance de Galois implique que le nombre de sous-corps $M \subset L$ de degré 4 sur $\mathbb{Q}$ est égal au nombre de sous-groupes de $\mathrm{Gal}(L/\mathbb{Q})$ d'ordre 2. Ce nombre est encore égal au nombre d'éléments d'ordre 2 de $\mathrm{Gal}(L/\mathbb{Q})$. Soit f un élément de $\mathrm{Gal}(L/\mathbb{Q}(i))$ avec $f(\sqrt[4]{11}) = i\sqrt[4]{11}$. Un tel élément existe parce que $X^4 - 11$ est irréductible sur $\mathbb{Q}(i)$. On a $f^2(\sqrt[4]{11}) = -\sqrt[4]{11}$ donc f est un générateur de $\mathrm{Gal}(L/\mathbb{Q}(i))$. D'après la question précédente on a $\mathrm{Gal}(L/K) = \{\mathrm{id}, f, f^2, f^3, c, cf, cf^2, cf^3\}$. Déterminons les ordre des éléments de ce groupe.

Évidemment, id est d'ordre 1, c et f^2 sont d'ordre 2 tandis que f et f^3 sont d'ordre 4. Il reste à trouver les ordres de cf, cf^2 et cf^3. Or $cf(i) = c(i) = -i$ et $cf(\sqrt[4]{11}) = c(i\sqrt[4]{11}) = -i\sqrt[4]{11}$ donc $(cf)^2(i) = i$ et

$$(cf)^2(\sqrt[4]{11}) = cf(-i)cf(\sqrt[4]{11}) = \sqrt[4]{11}.$$

On conclut que cf est d'ordre 2. De la même manière on montre que cf^2 et cf^3 sont d'ordre 2. Le nombre d'éléments d'ordre 2 de $\mathrm{Gal}(L/\mathbb{Q})$ ainsi que le nombre de sous-corps $M \subset L$ de degré 4 sur $\mathbb{Q}$ est donc égal à 5.