Université Louis Pasteur Département de Mathématiques

Master de mathématiques 1ère année

Algèbre M1S2

Corrigé de l'examen du 14 juin 2006

Exercice 1.

(a) L'énoncé est faux. Comme contre-exemple on peut prendre $\alpha = \sqrt[4]{2} \in \mathbb{R} \subset \mathbb{C}$ et $P(X) = X^4 - 2$. Le critère d'Eisenstein montre que P est irréductible dans $\mathbb{Q}[X]$, donc $[K : \mathbb{Q}] = 4$. Comme P n'a que deux racines réelles (à savoir $\pm\sqrt[4]{2} \in K$) et comme $K \subset \mathbb{R}$, l'ensemble des racines de P dans K est $X = \{\pm\sqrt[4]{2}\}$ et d'après le cours on a alors un morphisme injectif $\mathrm{Gal}(K/\mathbb{Q}) \to \mathrm{Bij}(X)$. Cela donne $|\mathrm{Gal}(K/\mathbb{Q})| \leq 2 < 4 = [K : \mathbb{Q}]$ donc l'extension $K/\mathbb{Q}$ n'est pas galoisienne.

(b) L'énoncé est faux. Pour obtenir un contre-exemple soient

$$\alpha = e^{\pi i/4} = \frac{\sqrt{2}}{2}(1+i) \in \mathbb{C}$$

et $P(X) = X^4 + 1$. Clairement $P(\alpha) = 0$ donc $[K : \mathbb{Q}] \leq 4$. D'autre part, on a $\sqrt{2} = \alpha + \alpha^{-1}$ donc $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset K$ et

$$[K : \mathbb{Q}] = [K : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2[K : \mathbb{Q}(\sqrt{2})].$$

Comme $\mathbb{Q}(\sqrt{2}) \subset \mathbb{R}$ mais $K \not\subset \mathbb{R}$ on a $[K : \mathbb{Q}(\sqrt{2})] \geq 2$ ce qui montre qu'en effet $[K : \mathbb{Q}] = 4$ et que P est irréductible dans $\mathbb{Q}[X]$. Les racines de P sont $\alpha, \alpha^3, \alpha^5, \alpha^7 \in K$, donc P est décomposé à racines simples sur K et Ky est un corps de décomposition de P sur $\mathbb{Q}$. Il s'ensuit que $K/\mathbb{Q}$ est galoisienne. Un autre contre-exmple peut être obtenu en prenant $\alpha = e^{2\pi i/4}$, voir le cours ou la question 3(f).

(c) L'énoncé est vrai. Si P est décomposé sur K alors K est un corps de décomposition de P sur $\mathbb{Q}$. Comme P est irréductible et comme on est en caractéristique 0, on a $\mathrm{pgcd}(P, \partial_X P) = 1$ donc le théorème 4.14 implique que $K/\mathbb{Q}$ est galoisienne.

(d) L'énoncé est vrai. Pour le prouver, il suffit de montrer que si $K/\mathbb{Q}$ est galoisienne, alors P est décomposé sur K. Mais d'après le théorème 4.12, comme $\alpha \in K$ est une racine de P et comme $K/\mathbb{Q}$ est galoisienne, le polynôme minimal de α sur $\mathbb{Q}$ est décomposé sur K. Comme P est ce polynôme minimal, il est décomposé sur K.

Exercice 2.

(a) Le groupe multiplicatif $\mathbb{F}_5^\times$ est cyclique d'ordre 4. L'ordre de 2 dans $\mathbb{F}_5^\times$ divise 4 et comme $2^2 \neq 1$ dans $\mathbb{F}^5$, cet ordre ne divise pas 2. Cela implique que 2 est d'ordre 4 dans $\mathbb{F}_5^\times$, c'est donc un générateur de ce groupe.

Si $X^2 - 2$ est réductible dans $\mathbb{F}_5[X]$, ce polynôme a une racine x dans $\mathbb{F}_5$. L'ordre de x dans $\mathbb{F}_5^\times$ divise 4, donc l'ordre de $2 = x^2$ divise alors 2, ce qui contredit le fait que 2 engendre $\mathbb{F}_5^\times$. Cette contradiction implique que $X^2 - 2$ est irréductible dans $\mathbb{F}_5[X]$.

(b) Comme $X^2 - 2$ est irréductible, $K = \mathbb{F}_5[X]/(X^2 - 2)$ est un corps et comme $X^2 - 2$ est de degré 2, c'est une extension de $\mathbb{F}_5$ de degré 2. Cela implique que K est un corps d'ordre $5^2 = 25$.

Dans K, on a $\alpha^8 = 2^4 = 1$ donc l'ordre de α divise 8. D'autre part, l'ordre de α ne divise pas 4 car $\alpha^4 = 2^2 \neq 1$. Cela montre que α est d'ordre 8 dans $K^\times$.

(c) Les éléments d'ordre 3 dans $K^\times$ sont les éléments $x \in K^\times$ avec $x^3 = 1$ mais $x \neq 1$, c'est à dire les racines de $X^3 - 1 = (X - 1)(X^2 + X + 1)$ qui ne sont pas racine de $X - 1$, ce sont les racines de $X^2 + X + 1$.

Pour trouver ces racines, il faut résoudre $a, b \in \mathbb{F}_5$ dans l'équation

$$0 = (a + b\alpha)^2 + (a + b\alpha) + 1 = (a^2 + 2b^2 + a + 1) + (2ab + b)\alpha$$

qui est équivalent au système $a^2 + 2b^2 + a + 1 = 0$ et $2ab + b = 0$. Comme $\mathbb{F}_5^\times$ ne contient pas d'éléments d'ordre 3, le polynôme $X^2 + X + 1$ ne possède pas de racine dans $\mathbb{F}_5$ donc $b \neq 0$. Cela implique que $2a + 1 = 0$, d'où $a = 2$ et la première équation donne alors que $b = \pm 2$. Les racines de $X^2 + X + 1$ sont donc $2 \pm 2\alpha$.

(d) Noter que $|K^\times| = 24$, on cherche donc un élément d'ordre 24 dans ce groupe. Comme α est d'ordre 8 et $2 + 2\alpha$ d'ordre 3 et comme 3 et 8 sont premiers entre eux, $\beta = 2\alpha + 2\alpha^2 = 4 + 2\alpha$ est d'ordre 24 et c'est un générateur de $K^\times$.

On a $\beta^2 = 16+16\alpha+4\alpha^2 = 4+\alpha$ donc $\beta^2+2\beta+3 = 0$. Comme $K = \mathbb{F}_5(\beta)$, on sait que β est de degré 2 sur $\mathbb{F}_5$ et il s'ensuit que X^2+2X+3 est son polynôme minimal.

Exercice 3.

(a) Notons $g = f^2$, alors $g^2 = \mathrm{id}$ car f est d'ordre 4. L'endomorphisme g vérifie la relation $g^2 - 1 = 0$. Comme le polynôme X^2-1 est scindé sur K et à racines ± 1 simples, cela implique que g est diagonalisable sur K et que les valeurs propres sont parmi ± 1. Si 1 est la seule valeur propre de g, alors $f^2 = \mathrm{id}$ ce qui contredit le fait que f est d'ordre 4. Cela montre que -1 est une valeur propre de g. Si $\alpha \in L$, $\alpha \neq 0$, est un vecteur propre associé, alors $f^2(\alpha) = g(\alpha) = -\alpha$.

(b) Le stabilistateur de α dans $\mathrm{Gal}(L/K)$ est un sous-groupe

$$H \subset \mathrm{Gal}(L/K) = \{\mathrm{id}, f, f^2, f^3\}.$$

Les sous-groupes de $\mathrm{Gal}(L/K)$ sont $\{\mathrm{id}\}$, $\{\mathrm{id}, f^2\}$ et $\mathrm{Gal}(L/K)$. Comme on a $f^2(\alpha) \neq \alpha$ il s'ensuit que $f^2 \notin H$ ce qui donne $H = \{\mathrm{id}\}$.

(c) On a

$$\mathrm{Gal}(L/K(\alpha)) = \{g \in \mathrm{Gal}(L/K) \mid g(\alpha) = \alpha\} = \{\mathrm{id}\},$$

où la dernière égalité résulte de la question précédente. Cela implique que $\mathrm{Gal}(L/K(\alpha)) = \mathrm{Gal}(L/L)$ et comme la correspondance de Galois est une bijection on en déduit que $L = K(\alpha)$.

(d) D'après le théorème 4.12, le polynôme minimal de α sur K est scindé sur L à racines simples et l'ensemble des racines est l'orbite de α sous l'action de $\mathrm{Gal}(L/K)$. Notons que $f^3(\alpha) = f(f^2(\alpha)) = -f(\alpha)$. Le polynôme minimal de α sur K est

$$\begin{aligned}(X-\alpha)(X-f(\alpha))(X-f^2(\alpha))(X-f^3(\alpha)) = \\ (X-\alpha)(X+\alpha)(X-f(\alpha))(X+f(\alpha)) = (X^2-\alpha^2)(X^2-f(\alpha)^2) = \\ X^4-(\alpha^2+f(\alpha)^2)X^2+\alpha^2 f(\alpha)^2.\end{aligned}$$

(e) On vient de montrer que $B = (\alpha f(\alpha))^2$. Si $b \in K$ tel que $b^2 = B$ alors $b = \pm\alpha f(\alpha)$ donc $\alpha f(\alpha) \in K$ et cet élément est invariant par f. Mais $f(\alpha f(\alpha)) = f(\alpha)f^2(\alpha) = -\alpha f(\alpha)$ ce qui est une contradiction donc B n'est pas un carré dans K.

Comme les racines de T^2+AT+B sont α^2 et $f(\alpha)^2$, on a $D=(\alpha^2-f(\alpha)^2)^2$. Il s'ensuit que si D est un carré dans K alors $\alpha^2-f(\alpha)^2 \in K$, ce qui contredit le fait que $f(\alpha^2-f(\alpha)^2)=-(\alpha^2-f(\alpha)^2)$.

Les calculs précédents montrent que

$$DB^{-1}=\left(\alpha^2-f(\alpha)^2)(\alpha f(\alpha))^{-1}\right)^2$$

et comme

$$f\left((\alpha^2-f(\alpha)^2)(\alpha f(\alpha))^{-1}\right)=(\alpha^2-f(\alpha)^2)(\alpha f(\alpha))^{-1}$$

on a $(\alpha^2-f(\alpha)^2)(\alpha f(\alpha))^{-1}$ est invariant par f et appartient docn à K.

(f) On a vu dans le chapitre 4 (exemple 5) que $[\mathbb{Q}(\omega):\mathbb{Q}]=4$ et que $\mathbb{Q}(\omega)/\mathbb{Q}$ est une extension galoisienne avec $\mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q}) \cong (\mathbb{Z}/5\mathbb{Z})^\times$. Ce dernier groupe est cyclique d'ordre 4 engendré par $\bar{2}$. Soit $f \in \mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q})$ l'élément correspondant à $\bar{2}$ dans cet isomorphisme, alors f est caractérisé par le fait que $f(\omega)=\omega^2$. D'après ce qui précède, il existe $\alpha \in \mathbb{Q}(\omega)$ avec $f^2(\alpha)=-\alpha$ et cet élément possède les propriétés souhaitées. Il reste à trouver un tel α.

Comme $f^2(\omega)=\omega^4$, on a $f^2(\omega^4)=\omega$ et on peut prendre $\alpha=\omega-\omega^4$. (Pour trouver α on peut aussi écrire la matrice de f^2 dans la $\mathbb{Q}$-base $\{1,\omega,\omega^2,\omega^3\}$ de $\mathbb{Q}(\omega)$ et chercher un vecteur propre pour la valeur propre -1.) On a $f(\alpha)=\omega^2-\omega^3=\beta$ et le polynôme minimal de α sur $\mathbb{Q}$ est alors

$$X^4-(\alpha^2+\beta^2)X^2+\alpha^2\beta^2=X^4+5X^2+5.$$