Université Louis Pasteur Département de Mathématiques

Master de mathématiques 1ère année

Algèbre M1S2

Corrigé de l'examen du 4 juin 2007

Exercice 1.

(a) et (b) Les énoncés sont vrais. On montrera l'énoncé (b) qui implique (a). Soit $P \in K[X]$ un polynôme irréductible possédant une racine $\alpha \in L$. Pour $a \in K^\times$ le coefficient dominant de P, on a $P = aP_\alpha$ où P_α est le polynôme minimal de α sur K. Il suffit de montrer que P_α est décomposé sur L et cela résulte du théorème 3.12 du cours.

(c) L'énoncé est vrai. Supposons que K est de caractéristique 0 et que tout polynôme irréductible $P \in K[X]$ qui possède une racine dans L est décomposé sur L. Soient $\alpha_1, \ldots, \alpha_n \in L$ tels que $L = K(\alpha_1, \ldots, \alpha_n)$. Pour chaque i, notons P_i le polynôme minimal de α_i sur K. L'hypothèse implique que chaque P_i est décomposé sur L. Comme K est de caractéristique 0 et P_i est irréductible sur K, on a $\mathrm{pgcd}(P_i, \partial_X P_i) = 1$, donc les racines de P_i dans L sont simples. Supposons que P_i et P_j ont une racine commune $\beta \in L$. Alors P_i est le polynôme minimal de β sur K et il en est de même pour P_j et il résulte que $P_i = P_j$. Cela implique que si $P_i \neq P_j$, alors P_i et P_j n'ont aucune racine commune dans L.

Soit P le produit des P_i *distincts*. Alors P est décomposé sur L à racines simples. Comme $L = K(\alpha_1, \ldots, \alpha_n)$, c'est un corps de décomposition de P sur K. D'après le théorème 3.14 du cours, L/K est une extension galoisienne.

Exercice 2.

(a) On a vu dans la proposition 4.6 du cours que L est un corps de décomposition de $P(X) = X^9 - 1$ sur $\mathbb{Q}$ et comme $\mathrm{pgcd}(P, \partial_X P) = 1$ cela implique que L/K est une extension galoisienne. L'ensemble $\mu_9 \subset L^\times \subset \mathbb{C}^\times$ des racines de P est un sous-groupe (multiplicatif), isomorphe au groupe additif $\mathbb{Z}/9\mathbb{Z}$ donc $\mathrm{Gal}(L/\mathbb{Q})$ s'identifie à un sous-groupe de

$$\mathrm{Aut}_{\text{groupes}}(\mu_9) \cong \mathrm{Aut}_{\text{groupes}}(\mathbb{Z}/9\mathbb{Z}) \cong (\mathbb{Z}/9\mathbb{Z})^\times.$$

(b) Notons $c\colon \mathbb{C} \to \mathbb{C}$ la conjugaison complexe. Comme $c(\omega) = e^{-2i\pi/9} = \omega^{-1} \in L$, la conjugaison complexe c est un automorphisme $\mathbb{Q}$-linéaire de $\mathbb{C}$ envoyant L dans L. Le degré $[L : \mathbb{Q}]$ étant fini, c se restreint à un $\mathbb{Q}$-*automorphisme* de L, autrement dit $c_{|L} \in \mathrm{Gal}(L/\mathbb{Q})$. D'une part $c_{|L} \neq \mathrm{id}_L$ car $c(\omega) \neq \omega$ et d'autre part $c^2 = \mathrm{id}$ donc $(c_{|L})^2 = \mathrm{id}_L$ et $c_{|L}$ est d'ordre 2.

(c) Notons $j = e^{2i\pi/3} = \omega^3$. On a $\alpha^3 = (\omega + \omega^{-1})^3 = \omega^3 + 3\omega + 3\omega^{-1} + \omega^{-3} = j + j^{-1} + 3\alpha$ donc $\alpha^3 - 3\alpha + 1 = j + j^{-1} + 1 = 0$.

(d) Comme $L/\mathbb{Q}$ est un extension galoisienne, on a $[L : \mathbb{Q}] = |\mathrm{Gal}(L/\mathbb{Q})|$ et le dernier groupe est isomorphe à un sous-groupe de $(\mathbb{Z}/9\mathbb{Z})^\times$. Comme $|(\mathbb{Z}/9\mathbb{Z})^\times| = 6$, cela implique que $[L : \mathbb{Q}]$ divise 6. D'après la question (b), le groupe $\mathrm{Gal}(L/\mathbb{Q})$ contient un élément d'ordre 2, donc $[L : \mathbb{Q}]$ est divisible par 2. Les seules racines rationnelles possibles du polynôme

$X^3 - 3X + 1$ sont ± 1, donc ce polynôme de degré 3 n'a pas de racine dans $\mathbb{Q}$ et il s'ensuit que $X^3 - 3X + 1$ est irréductible sur $\mathbb{Q}$. On conclut que $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$ et comme $\mathbb{Q}(\alpha) \subset L$ il résulte que $[L : \mathbb{Q}]$ est divisible par 3.

En résumant, le degré $[L : \mathbb{Q}]$ divise 6 et il est divisible par 2 et par 3 donc $[L : \mathbb{Q}] = 6$. Comme $|\mathrm{Gal}(L/\mathbb{Q})| = |(\mathbb{Z}/9\mathbb{Z})^\times| = 6$ on a $\mathrm{Gal}(L/\mathbb{Q}) \cong (\mathbb{Z}/9\mathbb{Z})^\times$ d'après ce qui précède.

(e) La racine de l'unité ω est une racine du polynôme

$$\Phi_9(X) = \frac{X^9 - 1}{X^3 - 1} = X^6 + X^3 + 1.$$

Comme ω est de degré 6 sur $\mathbb{Q}$ il s'ensuit que Φ_9 est le polynôme minimal de ω sur $\mathbb{Q}$.

(f) Le groupe $(\mathbb{Z}/9\mathbb{Z})^\times$ est engendré par $\bar{2}$ donc cyclique d'ordre 6. Les sous-groupes sont 1, $\{\pm\bar{1}\}$, $\{\bar{1}, \bar{4}, \bar{7}\}$ et $(\mathbb{Z}/9\mathbb{Z})^\times$. Le corps L contient donc 4 sous-corps, de degrés 6, 3, 2 et 1 sur $\mathbb{Q}$. Il ne peut s'agir que de L, $\mathbb{Q}(\alpha)$, $\mathbb{Q}(j)$ et $\mathbb{Q}$ respectivement.

Le corps $\mathbb{Q}$ est contenu dans tous ces sous-corps, qui sont à leur tous contenus dans L. Ce sont les seules inclusions entre les corps en question.

(g) Le groupe de Galois $\mathrm{Gal}(L/\mathbb{Q}) \cong (\mathbb{Z}/9\mathbb{Z})^\times$ est commutatif donc tout sous-groupe est distingué. Cela implique que tous les corps intermédiaires sont galoisiennes sur $\mathbb{Q}$.

Exercice 3.

(a) Les hypothèses impliquent que $[L : K] = 6$. On a $\mathrm{Gal}(L/K) \cong \mathrm{S}_3$ et comme $\{(1), (1,2)\} \subset \mathrm{S}_3$ est un sous-groupe d'ordre 2, le groupe de Galois $\mathrm{Gal}(L/K)$ contient un sous-groupe d'ordre 2. L'extension $M \subset L$ de K correspondant vérifie $[L : M] = 2$ donc $[M : K] = 3$.

(b) Soit $M \subset L$ une extension de K avec $[M : K] = 3$. D'après la correspondance de Galois, M correspond à un sous-groupe de d'ordre 2 de $\mathrm{Gal}(L/K)$. Dans l'isomorphisme $\mathrm{Gal}(L/K) \cong \mathrm{S}_3$ ce sous-groupe correspond à un sous-groupe de la forme $\{\mathrm{id}, \tau\}$ pour $\tau \in \mathrm{S}_3$ une transposition. Comme $\{\mathrm{id}, \tau\} \subset \mathrm{S}_3$ n'est pas distingué, $\mathrm{Gal}(L/M) \subset \mathrm{Gal}(L/K)$ n'est pas distingué non plus, donc M/K n'est pas une extension galoisienne.

(c) Comme $K \neq K(\alpha) \subset M$, le degré $[K(\alpha) : K]$ divise 3 et est différent de 1. Il en résulte que $[K(\alpha) : K] = 3$, donc α est de degré 3 sur K, ainsi que son polynôme minimal P.

(d) L'extension L/K est galoisienne et $\alpha \in L$. D'après le théorème 3.12 du cours le polynôme minimal P de α sur K est décomposé sur L et à racines simples. Ce dernier fait implique que $\mathrm{pgcd}(P, \partial_X P) = 1$.

(e) On vient de voir que P est décomposé sur L. Supposons que $N \subset L$ est une extension de K sur laquelle P est décomposé. Alors $\alpha \in N$ donc $M \subset N \subset L$ et le fait que $[L : M] = 2$ donne $N = M$ ou $N = L$. Si $N = M$, alors M est un corps de décomposition de P sur K. Comme P vérifie $\mathrm{pgcd}(P, \partial_X P) = 1$, cela implique que M/K est une extension galoisienne, en contradiction avec la question (b). On a donc $N \neq M$ d'où $N = L$ et cela montre que L est un corps de décomposition de P sur K.

(f) Outre les hypothèses de l'exercice, on doit supposer que $\mathrm{car}(K) \neq 2$. Supposons que le discriminant de P soit un carré. Alors le degré d'un corps de décomposition de P sur K est égal à 3 d'après l'exercice 4.2. C'est une contradiction car $[L : K] = 6$, donc le discriminant de P n'est pas un carré.