Université Louis Pasteur Département de Mathématiques

Master de mathématiques 1ère année

Algèbre M1S2

Corrigé de l'examen du 13 septembre 2007

Exercice 1.

(a) L'extension $K \subset L$ est de degré $|\mathrm{S}_n| = n!$ d'après le théorème 3.8 du cours et galoisienne d'après le corollaire 3.9.

(b) Les polynôme symétriques élémentaires sont invariants par les permutations des variables et appartiennent donc à $K = L^{\mathrm{S}_n}$. Cela implique que $K' = k(\sigma_1, \ldots, \sigma_n) \subset L$.

(c) On a $\Lambda(T) = \prod_{i=1}^{n}(T - X_i)$ donc Λ est décomposé sur L. Si Λ est décomposé sur un sous-corps $L' \subset L$, alors ses racines $X_1, \ldots, X_n$ appartiennent à L' donc $L = k(X_1, \ldots, X_n) \subset L'$ et par conséquent $L' = L$.

On a vu en TD qu'un corps de décomposition L de Λ sur K' est de degré divisant $(\deg \Lambda)! = n!$ donc $[L : K'] \leq n!$.

(d) On a $[L : K'] = [L : K][K : K']$ où $(n!)[K : K'] = [L : K'] \leq n!$ donc $[K : K'] = 1$, autrement dit $K = K'$.

Exercice 2.

Montrons d'abord que P est irréductible (même si ce n'est pas demandé).

Il est clair que $X^6 + X^3 + 8 = (X^2 + X + 2)^3$ dans $\mathbb{F}_3[X]$. Pour montrer que c'est la factorisation de $X^6 + X^3 + 8$ sur $\mathbb{F}_3$, il suffit de montrer que $X^2 + X + 2$ est irréductible dans $\mathbb{F}_3[X]$. Une vérification triviale montre que $X^2 + X + 2$ n'a pas de racine dans $\mathbb{F}_3$ et comme ce polynôme est de degré 2, cela implique qu'il est irréductible.

De même, on a évidement $X^6 + X^3 + 8 = (X^3 - 2)(X^3 - 4)$ dans $\mathbb{F}_7[X]$. On vérifie encore sans difficulté que les polynômes $X^3 - 2$ et $X^3 - 4$ n'ont pas de racine dans $\mathbb{F}_7$ et, étant de degré 3 chacun, sont donc irréductibles sur $\mathbb{F}_7$. On a trouvé la factorisation de $X^6 + X^3 + 8$ sur $\mathbb{F}_7$.

Supposons que P est réductible sur $\mathbb{Q}$. Alors P est également réductible sur $\mathbb{Z}$ donc on peut écrire $P = Q_1 Q_2$ où $1 < \deg(Q_1), \deg(Q_2) < 6$. On peut supposer Q_1 et Q_2 unitaires. En prenant les classes dans $\mathbb{F}_7[X]$ on trouve que $\deg Q_i = \deg \bar{Q}_i$ et $\bar{P} = \bar{Q}_1 \bar{Q}_2$ dont il résulte que $Q_1 = X^3 - 2$ et $Q_2 = X^3 - 4$ (ou réciproquement). En tout cas, si P est réductible, alors ses facteurs irréductibles dans $\mathbb{Z}[X]$ sont de degré

3. En prenant la réduction modulo 3 de la factorisation $P = Q_1Q_2$, on constate que, dans $\mathbb{F}_3[X]$, le produit $\bar{Q}_1\bar{Q}_2$ et le produit de trois polynôme irréductibles de degré 2. Cela est impossible, car un des facteurs doit alors diviser $\bar{Q}_1$ et le quotient est un facteur de $\bar{P}$ de degré 1, mais $\bar{P}$ ne possède pas de tel facteur.

Comme l'hypothèse que P soit réductible sur $\mathbb{Q}$ mène à une contradiction on a montré que P est irréductible.

(a) Évidemment

$$P(\alpha) = P(j\alpha) = P(j^2\alpha) = ((-1 + i\sqrt{31})/2)^2 + (-1 + i\sqrt{31})/2 + 8 = 0$$

et aussi

$$P(\beta) = P(j\beta) = P(j^2\beta) = 2^6\alpha^{-6} + 2^3\alpha^{-3} + 2^3 = 8\alpha^{-6}(8 + \alpha^3 + \alpha^6) = 0$$

donc $\alpha, j\alpha, j^2\alpha, \beta, j\beta, j^2\beta \in N$ sont des racines de P. Comme

$$\alpha^3 = (j\alpha)^3 = (j^2\alpha)^3 = (-1 + i\sqrt{31})/2 \neq (-1 - i\sqrt{31})/2 = \beta^3 = (j\beta)^3 = (j^2\beta)^3$$

les 6 racines de P trouvées ainsi sont distinctes et P étant de degré 6 il est décomposé dans $N[X]$.

Si $N' \subset N$ est un sous-corps tel que P est décomposé sur N', alors $\alpha, j\alpha \in N'$ donc $j \in N'$ ce qui implique que $N = \mathbb{Q}(j, \alpha) \subset N'$ d'où finalement $N = N'$. Cela montre que N est un corps de décomposition de P sur $\mathbb{Q}$. La caractéristique est nulle donc il résulte du théorème 3.14 du cours que N est une extension galoisienne de $\mathbb{Q}$. Le corollaire 3.15 implique que N/K est également galoisienne.

(b) On a $\mathbb{Q}(j) = \mathbb{Q}(i\sqrt{3})$ et $\mathbb{Q}(\alpha^3) = \mathbb{Q}(i\sqrt{31})$. Comme il n'existe pas d'éléments $a, b \in \mathbb{Q}$ tels que $(a + bi\sqrt{3})^2 = -31$, on a $i\sqrt{31} \notin \mathbb{Q}(i\sqrt{3})$ donc

$$[\mathbb{Q}(j, \alpha^3) : \mathbb{Q}] = [\mathbb{Q}(i\sqrt{3}, i\sqrt{31}) : \mathbb{Q}] = [\mathbb{Q}(i\sqrt{3}, i\sqrt{31}) : \mathbb{Q}(i\sqrt{3})][\mathbb{Q}(i\sqrt{3}) : \mathbb{Q}] = 4.$$

L'inclusion $\mathbb{Q}(j, \alpha^3) \subset N$ implique que $[N : \mathbb{Q}]$ est divisible par 4.

Comme P est irréductible sur $\mathbb{Q}$, on a $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 6$ et il comme $\mathbb{Q}(\alpha) \subset N$ s'ensuit que $[N : \mathbb{Q}]$ est divisible par 6. Étant divisible par 4 et par 6, le degré $[N : \mathbb{Q}]$ est même divisible par 12.

D'autre part, α est une racine de $P \in \mathbb{Q}(j)[X]$ donc $[N : K] \leq 6$ et la suite des inclusions $\mathbb{Q} \subset K \subset N$ montre que $[N : \mathbb{Q}] = [N : K][K : \mathbb{Q}] = 2[N : K] \leq 12$. On sait déjà que $[N : \mathbb{Q}]$ est divisible par 12 donc on a $[N : \mathbb{Q}] = 12$ et par conséquent $[N : K] = 6$.

(c) Comme $[N : K] = 6 = \deg(P)$ et $P(\alpha) = 0$, le polynôme P est le polynôme minimal de α sur K. L'extension N/K est galoisienne donc l'action de $H = \mathrm{Gal}(N/K)$ sur les racines de P est transitive. Le fait que $j\alpha$ et β sont des racines de P implique qu'il existe $\rho, \sigma \in H$ tels que $\rho(\alpha) = j\alpha$ et $\sigma(\alpha) = \beta$.

On a $\sigma^2(\alpha) = \sigma(\beta) = \sigma(2\alpha^{-1}) = 2\sigma(\alpha)^{-1} = 2\beta^{-1} = 2(2\alpha^{-1})^{-1} = \alpha$.

(d) Notons que $N = K(\alpha)$ donc un automorphisme $h \in H$ de N est déterminé par $h(\alpha)$. En particulier $\sigma^2 = \mathrm{id}_N$ car $\sigma^2(\alpha) = \alpha$ tandis que $\sigma \neq \mathrm{id}_N$ car $\sigma(\alpha) = \beta \neq \alpha$. Concernant ρ, on a $\rho^2(\alpha) = j^2\alpha \neq \alpha$ donc $\rho^2 \neq \mathrm{id}_N$, mais $\rho^3(\alpha) = \alpha$ donc $\rho^3 = \mathrm{id}_N$. On a montré que σ et ρ sont d'ordre 2 et 3 respectivement. Il résulte que $H' = \langle\rho\rangle$ est un sous-groupe de H d'ordre 3 et que $\sigma \notin H'$. Cela implique que $H' \subset H$ et $\sigma H' \subset H$ sont disjoints et comme $|H'| = |\sigma H'| = 3$ on a $H = H' \cup \sigma H'$, ce qui montre que $H = \langle\rho, \sigma\rangle$.

On a $\rho\sigma(\alpha) = \rho(\beta) = \rho(2\alpha^{-1}) = j^2\beta$ et $\sigma\rho(\alpha) = \sigma(j\alpha) = j\sigma(\alpha) = j\beta$ donc $\rho\sigma \neq \sigma\rho$. Le groupe H est donc non-commutatif d'ordre 6 et il résulte que $H \cong \mathrm{S}_3$.

Exercice 3.

(a) On a $N = \mathbb{Q}(j, \alpha)$ donc il suffit de montrer que $\bar{j} \in N$ et $\bar{\alpha} \in N$. Pour $\bar{j} = j^2$ c'est évident. Comme $P \in \mathbb{Q}[X]$ on a $P(\bar{\alpha}) = \overline{P(\alpha)} = 0$ et comme N est le corps de décomposition de P dans $\mathbb{C}$ cela implique que $\bar{\alpha} \in N$.

Comme la conjugaison complexe est un automorphisme de $\mathbb{C}$ d'ordre 2 et τ est sa restriction à N on a $\tau^2 = \mathrm{id}_N$. Comme $\tau(j) \neq j$ on a $\tau \neq \mathrm{id}_N$ donc τ est d'ordre 2.

(b) On a $|\alpha|^3 = |\alpha^3| = |(-1+i\sqrt{31})/2| = \sqrt{8}$ donc $|\alpha| = \sqrt{2}$ et par conséquent $\alpha\bar{\alpha} = 2$. Il s'ensuit que $\tau(\alpha) = \bar{\alpha} = 2\alpha^{-1} = \beta$.

On a

$$\rho\tau(\alpha) = \rho(\beta) = j^2\beta \quad \text{et} \quad \tau\rho(\alpha) = \tau(j\alpha) = j^2\beta$$

resp.

$$\rho\tau(j) = \rho(j^2) = j^2 \quad \text{et} \quad \tau\rho(j) = \tau(j) = j^2$$

donc le fait que $N = \mathbb{Q}(j, \alpha)$ implique que $\rho\tau = \rho\tau$. De même

$$\sigma\tau(\alpha) = \sigma(\beta) = \alpha \quad \text{et} \quad \tau\sigma(\alpha) = \tau(\beta) = \alpha$$

resp.

$$\sigma\tau(j) = \sigma(j^2) = j^2 \quad \text{et} \quad \tau\sigma(j) = \tau(j) = j^2$$

donc $\sigma\tau = \tau\sigma$.

(c) Le groupe H est engendré par σ et ρ donc la partie précédente implique que $\tau h = h\tau$ pour tout $h \in H$. L'identité commute avec tout les éléments de G donc

$sh = hs$ pour tous $s \in \{\mathrm{id}, \tau\}$ et $h \in H$. Pour $(s,h),(s',h') \in \{\mathrm{id},\tau\} \times H$ on a alors $f((s,h)(s',h')) = f(ss',hh') = ss'hh' = shs'h' = f((s,h))f((s',h'))$. Cela prouve que f est un morphisme de groupes.

Supposons que $f((s,h)) = \mathrm{id}_N$. Alors $sh(j) = j$ et comme $h(j) = j$ cela implique que $s = \mathrm{id}_N$. Mais cela implique que $\mathrm{id}_N = sh = h$ donc $(s,h) = (\mathrm{id}, \mathrm{id})$ et on a montré que f est injectif. Comme $N/\mathbb{Q}$ est une extension galoisienne de degré $[N : K][K : \mathbb{Q}] = 12$, le groupe G est d'ordre 12, le même ordre que celui de $\{\mathrm{id}, \tau\} \times H$. Le morphisme injectif f est donc également surjectif.

(d) L'intersection $M = N \cap \mathbb{R}$ est l'ensemble des éléments de N qui sont invariants pour la conjugaison complexe et comme τ est la restriction à N de la conjugaison complexe, M est l'ensemble des éléments de N qui sont invariants par τ. Cela montre que $M = N^{\{\mathrm{id},\tau\}}$.

Sous la correspondance de Galois, M correspond à $\{\mathrm{id}, \tau\} \subset G$. On vient de montrer que $G \cong \{\mathrm{id}, \tau\} \times H$ donc $\{\mathrm{id}, \tau\}$ est un sous-groupe distingué de G, ce qui implique que $M/\mathbb{Q}$ est une extension galoisienne. En outre $\mathrm{Gal}(M/\mathbb{Q}) \cong G/\{\mathrm{id}, \tau\} \cong H \cong \mathrm{S}_3$.

(e) Il y a une bijection entre l'ensemble des sous-corps de M et l'ensemble des sous-groupes de S_3. Un sous-corps $M' \subset M$ avec $[M' : \mathbb{Q}] = d'$ correspond à un sous-groupe de S_3 d'ordre $6/d'$. Le groupe S_3 a un sous-groupe d'ordre 1, trois sous-groupes d'ordre 2, un sous-groupe d'ordre 3 et un sous-groupe d'ordre 6. Tous ces sous-groupes sont distingués sauf ceux d'ordre 2.

Le corps M contient donc un sous-corps M' avec $[M' : \mathbb{Q}] = 1$ (c'est $\mathbb{Q}$), un sous-corps M' avec $[M' : \mathbb{Q}] = 2$, trois sous-corps M' avec $[M' : \mathbb{Q}] = 3$ et un sous-corps M' avec $[M' : \mathbb{Q}] = 6$ (c'est M). Un sous-corps $M' \subset M$ est une extension galoisienne de $\mathbb{Q}$ si et seulement si le sous-groupe correspondant de S_3 est distingué donc tous les sous-corps ci-dessus sont des extensions galoisiennes de $\mathbb{Q}$ sauf les extensions de degré 3.