Université Paris 7-Denis Diderot
M1 mathématiques

Algèbre
Année 2006-07
F. Conduché - L. Merel

Correction de l'EXAMEN du 10 janvier 2007

I

1. Les polynômes X^4+1, X^4-1 et X^4-3X^2+2 ont respectivement 0, 2 et 4 racines réelles.
2. Rappelons que les éléments d'une extension de $\mathbf{F}_p$ qui sont dans un corps à q éléments sont les racines du polynôme $X^q - X \in \mathbf{F}_p[X]$. Si α est dans un corps à q éléments, on a $\alpha^q - \alpha = 0$ et $\tilde{P}$ et $X^q - X$ ont une racine commune. Réciproquement, si $\tilde{P}$ et $X^q - X$ ont un facteur commun, une racine de P est racine de $X^q - X$ et est donc dans un corps à q éléments.
3. On a $\tilde{P} = (X^2 + aX + b)^2$ dans $\mathbf{F}_2[X]$. Le polynôme $\tilde{P}$ n'est donc jamais irréductible sur $\mathbf{F}_2$.

Étudions maintenant la réductibilité sur $\mathbf{F}_3$. Si $\tilde{P}$ est réductible il admet un facteur irréductible de degré 1 ou 2, *i.e.* un facteur parmi X, $X+1$, $X-1$, X^2+1, X^2-X-1 et X^2+X-1. Cela revient respectivement à $b \equiv 0 \pmod 3$, $a+b+1 \equiv 0 \pmod 3$, $a+b+1 \equiv 0 \pmod 3$, $1-a+b \equiv 0 \pmod 3$, $(a,b) \equiv (0,1) \pmod 3$, $(a,b) \equiv (0,1) \pmod 3$. L'une au moins de ces congruences est satisfaite sauf si $b \equiv -1 \pmod 3$ et $a \not\equiv 0 \pmod 3$. C'est donc seulement dans ces derniers cas que $\tilde{P}$ est irréductible.

4. Par exemple $P = X^4 - 5$, qui est irréductible par le critère d'Eisenstein et qui n'a que deux racines réelles.
5. Utilisons la formule suivante pour le discriminant Δ d'un polynôme unitaire P de degré n : $\Delta = (-1)^{n(n-1)/2} R(P,P') = (-1)^{n(n-1)/2} n^n \prod_i P(x_i)$, où x_i parcourt les racine de P' et où $R(P,P')$ désigne le résultant de P et P'. Dans le cas qui nous intéresse, on a $P' = 4X^3 + 2aX$, qui a pour racines 0 et les deux racines de $X^2 + a/2$. On a donc $\Delta = 4^4 b(a^2/4 - a^2/2 + b)^2 = 16b(a^2-4b)^2$. Le polynôme P a des racines multiples si et seulement si $b = 0$ ou $a^2 - 4b = 0$.

II

1. Le nombre α^2 est une racine du polynôme $Y^2 + aY + b$, dont le corps de décomposition K est $\mathbf{Q}$ ou quadratique sur $\mathbf{Q}$. Le corps $\mathbf{Q}(\alpha) = K(\alpha)$ est le corps de décomposition de $X^2 - \alpha^2$, c'est donc K ou une extension quadratique de K. Examinons les extensions successives $\mathbf{Q}(\alpha)|\mathbf{Q}$ et $\mathbf{Q}(\alpha,\beta)|\mathbf{Q}(\alpha)$ qui sont de degrés 1 ou 2. Le degré de l'extension $\mathbf{Q}(\alpha,\beta)|\mathbf{Q}$ est le produit de ces degrés, c'est donc 1, 2 ou 4.
2. Les racines de P sont, comptées avec multiplicité, α, $-\alpha$, β et $-\beta$. On a $-\alpha, -\beta \in \mathbf{Q}(\alpha,\beta)$. C'est pourquoi $\mathbf{Q}(\alpha,\beta)$ contient toutes les racines de P et est donc un corps de décomposition de P. On a $P = (X-\alpha)(X+\alpha)(X-\beta)(X+\beta)$, et donc $\alpha^2 + \beta^2 = a$. Le nombre $\beta \in \mathbf{Q}(\sqrt{a-\alpha^2})$ est donc dans une extension quadratique de $\mathbf{Q}(\alpha)$.
3. Les extensions $\mathbf{Q}(\alpha)|\mathbf{Q}$ et $\mathbf{Q}(\alpha,\beta)|\mathbf{Q}(\alpha)$ sont de degrés divisant 4 et 2 respectivement. L'extension $\mathbf{Q}(\alpha,\beta)|\mathbf{Q}$ est donc de degré divisant 8.
4. Toute extension de $\mathbf{Q}$ contenue dans L est de degré divisant $[L : \mathbf{Q}]$ et donc divisant 8. Ce degré ne peut donc être 3.
5. Le polynôme $X^4 - 5$ est irréductible sur $\mathbf{Q}$. Soit α l'une de ses racines réelles. Le corps $\mathbf{Q}(\alpha)$ est donc une extension de degé 4 de $\mathbf{Q}$ contenue dans $\mathbf{R}$. Soit β l'une des racines non réelles de P. On a $\beta \notin \mathbf{Q}(\alpha)$. Donc l'extension $\mathbf{Q}(\alpha,\beta)|\mathbf{Q}(\alpha)$ n'est pas de degré 1. Elle est de degré 2 car β est dans une extension quadratique de $\mathbf{Q}(\alpha)$ d'après la question 2. Le degré de l'extension $\mathbf{Q}(\alpha,\beta)|\mathbf{Q}$ est donc $2 \times 4 = 8$.
6. L'extension $L|\mathbf{Q}$ est séparable (on est en caractéristique 0) et normale (L est un corps de décomposition).

III

1. Le groupe G opère sur les racines de P dans L, qui, comptées avec multiplicités, sont au nombre de 4. On a donc un homomorphisme de groupe $G \to \mathcal{S}_4$. Comme aucun élément de G distinct de l'identité n'opère trivialement sur ces racines (sinon cet élément serait l'identité sur L), cet homomorphisme est injectif et définit donc un isomorphisme de groupes de G vers un sous-groupe de $\mathcal{S}_4$.

2. Le groupe G est d'ordre égal au degré de l'extension $L|\mathbf{Q}$. C'est donc un diviseur de 8 (d'après la question II.3) et donc une puissance de 2.
3. Le groupe $\mathcal{S}_4$ est d'ordre $4! = 24 = 8 \times 3$. Ses 2-sous-groupes de Sylow sont donc d'ordre 8. On peut choisir G_2 ainsi : $G_2 = \{\mathrm{id}, (13), (24), (13)(24), (1234), (4321), (12)(34), (14)(23)\}$ (cela revient à considérer les quatre sommets d'un carré et à ne retenir que les permutations qui sont des isométries du carré). Ce n'est pas un groupe abélien puisque les 4-cycles et les transpositions ne commutent pas. Tout 2-sous-groupe de Sylow de $\mathcal{S}_4$ est conjugué de G_2 et n'est donc pas abélien.

Remarque : Le groupe G_2 est diédral à 8 éléments. Il est engendré par $\sigma = (1234)$ d'ordre 4 et $\tau = (24)$ d'ordre 2 et on a $\tau\sigma = \sigma^{-1}\tau$.
4. Lorsque $P = X^4 - 5$, l'extension $L|\mathbf{Q}$ est de degré 8. Le groupe G est alors d'ordre 8. C'est donc un 2-sous-groupe de Sylow de $\mathcal{S}_4$. Il est donc conjugué de, et donc isomorphe à, G_2.
5. Si G est cyclique 8, c'est un 2-sous-groupe de Sylow de $\mathcal{S}_4$. Il n'est donc pas abélien. Ce ne peut pas être alors un groupe cyclique ou le produit de groupes cycliques.

Si $P = X^4 + 1$, le polynôme P est le 8-ème polynôme cyclotomique, qui est irréductible sur $\mathbf{Q}$. Le groupe G est isomorphe à $(\mathbf{Z}/8\mathbf{Z})^*$ qui est produit de deux groupes cycliques d'ordre 2. On aurait pu aussi prendre comme exemple $P = (X^2 - 2)(X^2 - 3)$, auquel cas $L = \mathbf{Q}(\sqrt{2}, \sqrt{3})$ et G est encore produit de deux groupes cycliques d'ordre 2.

(Remarque : si $P = X^4 + 4X^2 + 2$, le polynôme P est irréductible sur $\mathbf{Q}$ par le critère d'Eisenstein pour le nombre premier 2. On peut montrer que le groupe G est alors cyclique d'ordre 4.)
6. Le groupe G_2 donné ci-dessus possède un groupe d'ordre 8 (G_2 lui-même), trois sous-groupes d'ordre 4 (le groupe cyclique engendré par (1234), le groupe engendré par (13) et (24) et le groupe engendré par (12)(34) et (14)(23))), cinq sous-groupes d'ordre 2 (les groupes engendrés par (13), (24), (12)(34), (13)(24), (14)(23) respectivement) et un groupe d'ordre 1 (le groupe trivial).
7. Ces corps correspondent aux sous-groupes de G_2 d'indices 1, 2, 4 et 8 respectivement. C'est-à-dire aux sous-groupes d'ordre 8, 4, 2 et 1 respectivement. Il y en a 1, 3, 5 et 1 respectivement d'après la question 6.
8. On note α la racine quatrième de 5 dans $\mathbf{R}$ qui est > 0. On pose $\beta = i\alpha$. Pour voir le lien avec G_2 vu comme groupe de permutations posons $\alpha_1 = \alpha$, $\alpha_2 = i\alpha = \beta$, $\alpha_3 = -\alpha$ et $\alpha_4 = -i\alpha = -\beta$.

Considérons les éléments σ et τ de G associé à (1234) et (24) respectivement (voir la remarque de la question 3.). Ce sont des générateurs du groupe G. Déterminons comment ils agissent sur les générateurs α et $i = \beta/\alpha$ de $L = \mathbf{Q}(\alpha, \beta) = \mathbf{Q}(\alpha, \beta/\alpha) = \mathbf{Q}(\alpha, i)$. On a $\sigma(\alpha) = \sigma(\alpha_1) = \alpha_2 = i\alpha$, $\sigma(i) = \sigma(\alpha_2/\alpha_1) = \alpha_3/\alpha_2 = -\alpha/(i\alpha) = i$, $\tau(\alpha) = \tau(\alpha_1) = \alpha_1 = \alpha$ et $\tau(i) = \tau(\alpha_2/\alpha_1) = \alpha_4/\alpha_1 = -i\alpha/\alpha = -i$

Pour déterminer les sous-corps de L, considérons les corps des invariants sous les divers sous-groupes de G.

Le corps de degré 1 est $\mathbf{Q}$ (corps des invariants sous G). Les corps de degré 2 sont les corps suivants : $\mathbf{Q}(\sqrt{5})$ (corps des invariants sous le groupe engendré par τ et σ^2), $\mathbf{Q}(\sqrt{-1})$ (corps des invariants sous le groupe engendré par σ) et $\mathbf{Q}(\sqrt{-5})$ (corps des invariants sous le groupe engendré par $\tau\sigma$ et σ^2). Les corps de degré 4 sont les suivants : $\mathbf{Q}(\sqrt{5}, \sqrt{-1})$ (corps des invariants sous le groupe engendré par σ^2), $\mathbf{Q}(\alpha)$ (corps des invariants sous le groupe engendré par τ), $\mathbf{Q}(\beta)$ (corps des invariants sous le groupe engendré par $\sigma^2\tau$), $\mathbf{Q}(\alpha + \beta)$ (corps des invariants sous le groupe engendré par $\sigma\tau$)et $\mathbf{Q}(\alpha - \beta)$ (corps des invariants sous le groupe engendré par $\sigma^{-1}\tau$). Le corps de degré 8 est L (corps des invariants sous le groupe trivial).