Université Paris Diderot — Algèbre
Master de Mathématiques — Année 2017-18
L. Merel, J.-F. Mestre

CORRIGÉ DU CONTRÔLE du 8 décembre 2017

Soit $P(X) = X^4 + 4X^2 + 2 \in \mathbf{Q}[X]$. Soit K un corps de décomposition de P dans $\mathbf{C}$.

1. Montrer que P est irréductible sur $\mathbf{Q}$.

L'irréductibilité de P se voit en appliquant le critère d'Eisenstein pour le nombre premier 2.

2. Démontrer que l'ensemble des racines de P dans $\mathbf{C}$ est de la forme $S = \{\alpha, -\alpha, \beta, -\beta\}$, avec α, $\beta \notin \mathbf{R}$.

Le polynôme P est pair (*i.e.* on a $P(X) = P(-X)$), d'où le fait que les racines sont des paires d'opposés. Si $x \in \mathbf{R}$, on a $P(x) = x^4 + 4x^2 + 4 \geq 4 > 0$. C'est pourquoi P n'a pas de racine réelle.

3. Démontrer que $\alpha^2\beta^2 = 2$.

Le produit des racines de P est égal à son coefficient constant : 2. On a donc $\alpha^2\beta^2 = 2$.

4. Démontrer que $\sqrt{2} \in \mathbf{Q}(\alpha)$.

On a $(\alpha^2 + 2)^2 = 2$ et donc $\sqrt{2} = \pm(\alpha^2 + 2) \in \mathbf{Q}(\alpha)$.

5. Démontrer que $\beta \in \mathbf{Q}(\alpha)$.

On a $\alpha^2\beta^2 = 2$ et donc $\beta = \pm\sqrt{2}/\alpha \in \mathbf{Q}(\alpha)$.

6. Quel est le degré de l'extension $K|\mathbf{Q}$?

Comme P est irréductible et de degré 4, on a $[\mathbf{Q}(\alpha) : \mathbf{Q}] = 4$ et donc $[K : \mathbf{Q}] = 4$.

7. Montrer que l'extension $K|\mathbf{Q}$ est galoisienne.

L'extension $K|\mathbf{Q}$ est séparable (car la caractéristique est 0) et normale (car K est un corps de décomposition).

8. Quel est l'ordre de $G = \mathrm{Gal}(K/\mathbf{Q})$?

L'extension $K|\mathbf{Q}$ est de degré 4 si bien que le groupe de Galois de cette extension est d'ordre 4.

9. L'extension $K|\mathbf{Q}$ est-elle résoluble par radicaux ?

L'extension $K|\mathbf{Q}$ est résoluble par radicaux, car engendrée par des racines carrées successives. En effet considérons les extensions composées : $\mathbf{Q} \subset \mathbf{Q}(\sqrt{2}) \subset K$. L'extension $K|\mathbf{Q}(\sqrt{2})$ est engendrée par α et on a $\alpha^2 = -2 \pm \sqrt{2}$. (On pourrait procéder différemment en montrant que $K|\mathbf{Q}$ est résoluble. En effet G est d'ordre 4 et est donc abélien et donc résoluble. On sait que les extensions résolubles par radicaux coïncident avec les extensions résolubles.)

10. Montrer que l'application $G \to S$ qui à σ associe $\sigma(\alpha)$ est injective.

C'est le cas puisque le corps K est engendré par α sur $\mathbf{Q}$.

11. Démontrer que la conjugaison complexe induit un élément c de G d'ordre 2. Posons $H = \{1, c\}$.

La conjugaison complexe est d'ordre 1 ou 2 dans G. Comme $\alpha \notin \mathbf{R}$, on a $c(\alpha) \neq \alpha$ et donc c est distinct de l'identité et donc c est d'ordre 2.

12. Quel est le sous-corps $K^H = \{x \in K / h(x) = x\, (h \in H)\}$?

Les éléments de K fixés par H sont les éléments de K fixés par c, *i.e.* les nombres réels dans K. On a donc $\mathbf{Q}(\sqrt{2}) \subset K^H$. Par ailleurs H est d'ordre 2, l'extension $K^H|\mathbf{Q}$

est donc de degré $|G/H| = 2$. Les extensions $K^H|\mathbf{Q}$ et $\mathbf{Q}(\sqrt{2})|\mathbf{Q}$ ont même degré. On a donc $\mathbf{Q}(\sqrt{2}) = K^H$.

13. Soit $\sigma \in G$ distinct de l'identité et de c. Démontrer que $\sigma(\alpha\beta) = -\alpha\beta$.

Comme G est d'ordre 4, σ est d'ordre 2 ou 4. Remarquons que $c(\alpha) = -\alpha$ et $c(\beta) = -\beta$ et que $\mathrm{Gal}(K/\mathbf{Q}(\sqrt{2})) = \{1, c\}$. On a $\sigma(\alpha\beta)^2 = \sigma((\alpha\beta)^2) = \sigma(4) = 4 = (\alpha\beta)^2$ et donc $\sigma(\alpha\beta) = \pm\alpha\beta$. Si $\sigma(\alpha\beta) = \alpha\beta$, on a $\sigma(\sqrt{2}) = \sqrt{2}$ et donc $\sigma \in \mathrm{Gal}(K/K^H)$ ce qui entraîne $\sigma = 1$ ou $\sigma = c$.

14. En déduire que σ est d'ordre 4.

Si $\sigma(\alpha) = \alpha$, on a $\sigma = 1$. De même, si $\sigma(\beta) = \beta$, on a $\sigma = 1$. Si $\sigma(\alpha) = -\alpha$, on a $\sigma(\beta) = -\beta$ et donc $\sigma = c$, ce qui est absurde. On a donc $\sigma(\alpha) = \beta$ ou $\sigma(\alpha) = -\beta$. Dans le premier cas, on a $\sigma(\beta) = -\alpha$ et donc $\sigma^2(\alpha) = -\alpha$ et donc σ est d'ordre 4.

15. Démontrer que K admet un unique sous-corps de degré 2 sur $\mathbf{Q}$.

De tels sous-corps coïncident avec les sous-groupes d'indice 2 de G. Or G est cyclique d'ordre 4. Il possède donc un unique sous-groupe d'indice 2. C'est H. Le sous-corps correspondant est $K^H = \mathbf{Q}(\sqrt{2})$.

16. Donner la partie réelle et la partie imaginaire d'une racine ζ primitive 8-ème de l'unité dans $\mathbf{C}$.

On a $e^{2i\pi/8} = \sqrt{2}/2 + i\sqrt{2}/2$.

17. Montrer que $\sqrt{2}$ est contenu dans le 8-ème corps cyclotomique $\mathbf{Q}(\zeta)$.

On a $\sqrt{2} = e^{2i\pi/8} + 1/e^{2i\pi/8} \in \mathbf{Q}(e^{2i\pi/8})$.

18. Notons G_8 le groupe de Galois de l'extension $\mathbf{Q}(\zeta)|\mathbf{Q}$. Montrer qu'il est isomorphe au produit de deux groupes cycliques d'ordre 2.

Le groupe G_8 est isomorphe à $(\mathbf{Z}/8\mathbf{Z})^*$ qui est isomorphe au produit de deux sous-groupes d'ordre 2.

19. Montrer que K n'est pas $\mathbf{Q}(\zeta)$.

Si $K = \mathbf{Q}(e^{2i\pi/8})$, le groupe G (cyclique d'ordre 4) est isomorphe à G_8 (non cyclique), ce qui est absurde.

20. Montrer que K est contenu dans le 16-ème corps cyclotomique.

Il faut montrer que l'une des racines α de P est contenue dans le 16-ème corps cyclotomique L. On a $\cos(2\pi/16) = \sqrt{2+\sqrt{2}}/2 \in L$ et par ailleurs $i \in L$ et $\sqrt{2} \in L$. On a $\alpha = \pm\sqrt{(-2 \pm \sqrt{2})/2}$, on peut le choisir tel que $\alpha^2 = (-2-\sqrt{2})/2$. On a alors $\alpha = \pm i\cos(2\pi/16)\sqrt{2} \in L$ et donc $K \in L$.

Une autre méthode consiste à vérifier que $\theta - 1/\theta$ est racine de Q, où θ est une racine 16-ème de l'unité. En effet, on a $Q(\theta - 1/\theta) = (\theta - 1/\theta)^4 + 4(\theta - 1/\theta)^2 + 2 = \theta^4 + -4\theta^2 + 6 - 4\theta^{-2} + \theta^{-4} + 4\theta^2 - 8 + 4\theta^{-2} + 2 = \theta^4 + \theta^{-4}$. Or, puisque θ est une racine primitive 16-ème de l'unité, on a $\theta^8 = -1$ et donc $\theta^4 + \theta^{-4} = 0$.