Université Paris Diderot
Master de Mathématiques

Algèbre
Année 2018-19
L. Merel, J.-F. Mestre

Corrigé du CONTRÔLE du 4 décembre 2018

Considérons les nombres réels positifs suivants : $\sqrt{2}$, $\sqrt[3]{2}$, $t = \sqrt[3]{2+\sqrt{2}}$ et $s = \sqrt[3]{2-\sqrt{2}}$. Considérons la racine cubique primitive de l'unité j dans $\mathbf{C}$.

I

1. Montrer que $Q(T) = T^6 - 4T^3 + 2 \in \mathbf{Q}[T]$ est le polynôme minimal de t sur $\mathbf{Q}$.
Ce polynôme annule t et est irréductible par le critère d'Eisenstein (en le premier 2).
2. Déterminer les conjugués de t dans $\mathbf{C}$.
Les nombres t, s, jt, js, j^2t, j^2s sont racines de Q.
3. Montrer que le corps de décomposition de Q dans $\mathbf{C}$ est $\mathbf{Q}(j,t,s)$.
Comme les racines de Q sont distinctes, ce corps est $\mathbf{Q}(t,s,jt,js,j^2t,j^2) = \mathbf{Q}(j,t,s)$.
4. Quel est le degré de l'extension $\mathbf{Q}(t)|\mathbf{Q}$? Cette extension est-elle galoisienne ?
On a $[\mathbf{Q}(t) : \mathbf{Q}] = 6$, car $d^0(Q) = 6$. L'extension n'est pas normale car $jt \notin \mathbf{Q}(t)$.
5. Quel est le degré de l'extension $\mathbf{Q}(j,t)|\mathbf{Q}$?
Comme $[\mathbf{Q}(j) : \mathbf{Q}] = 2$, et $j \notin \mathbf{R}$, on a $[\mathbf{Q}(j,t) : \mathbf{Q}(t)] = 2$. On a donc $[\mathbf{Q}(j,t) : \mathbf{Q}] = 12$.
6. Montrer que $\mathbf{Q}(j,t,s) = \mathbf{Q}(\sqrt[3]{2}, j, t)$.
On a $ts = \sqrt[3]{2}$, ce qui entraîne immédiatement l'égalité.
7. En déduire que $\mathbf{Q}(j,t,s)|\mathbf{Q}$ est de degré ≤ 36.
Comme $\sqrt[3]{2}$ est de degré 3 sur $\mathbf{Q}$, le corps $\mathbf{Q}(j,t,s) = \mathbf{Q}(\sqrt[3]{2}, j, t)$ est une extension de degré ≤ 3 de $\mathbf{Q}(j,t)$. Ainsi $\mathbf{Q}(j,t,s)|\mathbf{Q}$ est de degré $\leq 3 \times 12 = 36$.

II

8. Soit x une racine de $R(X) = (X^3-4)^3 - 54X^3 \in \mathbf{Q}[X]$. Montrer que $R(s+t) = 0$.
C'est un calcul direct.
9. Montrer que $z = (x^2 - 4/x)/3$ et $y = (x^3-4)/3$ vérifient $z^3 - 2 = 0$ et $y^3 - 6y - 8 = 0$.
Calcul direct.
10. Calculer les discriminants des polynômes $Z^3 - 2$ et $Y^3 - 6Y - 8$.
Le discriminant de $X^3 + aX + b$ est $-27b^2 - 4a^3$. On trouve $-108 = -3.6^2$ et $-864 = -6.12^2$.
11. Montrer que les corps de décompositions des polynômes $Z^3 - 2$ et $Y^3 - 6Y - 8$ contiennent des corps quadratiques distincts. En déduire que $\mathbf{Q}(y) \neq \mathbf{Q}(z)$.
Ces corps contiennent les corps quadratiques $\mathbf{Q}(\sqrt{-108}) = \mathbf{Q}(\sqrt{-3}) = \mathbf{Q}((1+\sqrt{-3})/2) = \mathbf{Q}(j)$ et $\mathbf{Q}(\sqrt{-864}) = \mathbf{Q}(\sqrt{-6})$. Si ces corps étaient égaux, il contiendraient tout deux $\sqrt{-6}/\sqrt{-3} = \sqrt{2}$ et seraient donc égaux à $\mathbf{Q}(\sqrt{2})$, ce qui est absurde puisque ce dernier corps est contenu dans $\mathbf{R}$ et ne peut donc contenir $\sqrt{-3}$. Si les corps $\mathbf{Q}(y)$ et $\mathbf{Q}(z)$ étaient égaux, ils auraient mêmes corps de décomposition dans $\mathbf{C}$, ce qui est absurde.
12. En déduire que $\mathbf{Q}(x)$ n'est pas de degré 3.
Si ce corps était de degré 3, il coïnciderait avec ses sous-corps $\mathbf{Q}(y)$ et $\mathbf{Q}(z)$, car ces derniers sont eux aussi cubiques. Ainsi, on aurait $\mathbf{Q}(y) = \mathbf{Q}(z)$.

13. Montrer que les facteurs irréductibles de R sont de degré 3, 6 ou 9.
Le corps $\mathbf{Q}(x)$ contient une racine cubique de 2. Ainsi 3 divise $[\mathbf{Q}(x) : \mathbf{Q}]$. Ainsi un corps de rupture de tout facteur irréductible de R est une extension de degré divisible par 3. Comme R est de degré 9 ses facteurs irréductibles sont de degrés ≤ 9.
14. En déduire que R est irréductible sur $\mathbf{Q}$ et le degré de l'extension $\mathbf{Q}(x)|\mathbf{Q}$.
Comme R n'admet pas de facteur irréductible de degré 3, il ne peut admettre de facteur irréductible de degré 6. Il est donc irréductible. Ainsi l'extension $\mathbf{Q}(x)|\mathbf{Q}$ est de degré 9.
15. En déduire que $\mathbf{Q}(j, t, s)|\mathbf{Q}$ est de degré 36. On suppose désormais que $x = s + t$.
Comme $\mathbf{Q}(j, t, s)$ contient $\mathbf{Q}(s+t)$ et $\mathbf{Q}(j, \sqrt{2})$, qui sont des extensions de $\mathbf{Q}$ de degré 9 et 4 respectivement, $[\mathbf{Q}(j, t, s) : \mathbf{Q}]$ est multiple de 9 et 4 et est donc multiple de 36. Comme $[\mathbf{Q}(j, t, s) : \mathbf{Q}] \leq 36$, on a $[\mathbf{Q}(j, t, s) : \mathbf{Q}] = 36$.

III

16. Placer les corps $\mathbf{Q}(j, t, s)$, $\mathbf{Q}(j, \sqrt{2})$, $\mathbf{Q}(\sqrt{-6}, y)$, $\mathbf{Q}(j, z)$, $\mathbf{Q}(x)$, $\mathbf{Q}(y)$, $\mathbf{Q}(z)$, $\mathbf{Q}(j)$, $\mathbf{Q}(\sqrt{2})$, $\mathbf{Q}(\sqrt{-6})$, $\mathbf{Q}$ dans un diagramme, où on indiquera les degrés des extensions.
17. Quel est l'ordre du groupe de Galois G du polynôme Q ?
Comme le corps de décomposition de Q est de degré 36, cet ordre est 36.
18. Montrer que G n'est pas abélien.
Si G était abélien, tous ses sous-groupes seraient distingués et toutes les extensions intermédiaires seraient galoisiennes. Mais ce n'est pas le cas de l'extension $\mathbf{Q}(t)|\mathbf{Q}$.
19. Les groupes $\mathcal{S}_6$ (groupe symétrique) et G admettent-ils un élément d'ordre 9 ?
Le groupe $\mathcal{S}_6$ ne contient pas de cycles à supports disjoints dont le ppcm des ordres est 9, car il ne contient pas de cycle d'ordre 9. Comme G est le groupe de Galois d'un polynôme de degré 6, il s'identifie à un sous-groupe de $\mathcal{S}_6$, qui est dénué d'élément d'ordre 9.
20. Montrer que G admet un unique sous-groupe H d'ordre 9.
Un sous-groupe d'ordre 9 est un 3-sous-groupe de Sylow de G. Il en existe donc. Deux tels sous-groupes sont conjugués dans G. Si l'un d'entre eux est distingué dans G, c'est le seul sous-groupe d'ordre 9. Or H est distingué si et seulement si le corps $\mathbf{Q}(j, t, s)^H$ des invariants sous H est une extension Galoisienne de $\mathbf{Q}$. Il suffit donc de montrer qu'il existe une extension galoisienne L de degré 4 de $\mathbf{Q}$ contenue dans $\mathbf{Q}(j, t, s)$. Le groupe $\mathrm{Gal}(\mathbf{Q}(j, t, s)/L))$ est alors un groupe d'ordre 9 distingué dans G. Or on a montré que l'extension $L = \mathbf{Q}(j, \sqrt{2})$ est contenue dans $\mathbf{Q}(j, t, s)$. L'extension $L|\mathbf{Q}$ est galoisienne (car biquadratique) de degré 4.
21. Quel est le corps formé par les invariants sous H ?
Par la théorie de Galois c'est une extension de $\mathbf{Q}$ de degré $|G/H| = 4$. Or, on a vu que $\mathbf{Q}(j, \sqrt{2})$ est la seule extension de degré 4 de $\mathbf{Q}$ contenue dans $\mathbf{Q}(j, t, s)$.

Remarque : Le groupe G s'identifie à un sous-groupe de $\mathcal{S}_6$ de la façon suivante. Le groupe H est d'ordre 9 sans élément d'ordre 9. Il est donc isomorphe au produit deux groupes cycliques d'ordre 3. Ainsi l'image de H dans $\mathcal{S}_6$ est engendrée par deux 3-cycles de supports S_1 et S_2 disjoints. Notons K le sous-groupe de $\mathcal{S}_6$ formé par les éléments qui laissent stables ou échangent S_1 et S_2. Il est d'ordre 72. Il possède un sous-groupe d'indice 2 formé par les permutations paires qui laissent stables S_1 et S_2 et les permutations impaires qui échangent S_1 et S_2. C'est l'image de G dans $\mathcal{S}_6$.