

Corrigé du contrôle classant 2016

Ce corrigé constitue un ensemble d'indications pour résoudre les exercices.

Il ne s'agit en aucun cas d'un modèle de rédaction pour le contrôle classant.

Exercice 1.

- 1) Cours.
- 2) Elle est donnée par la conjugaison complexe.
- 3) Une racine de P irréductible engendre une extension d'ordre p . Donc p divise le degré du corps de décomposition de P , et donc l'ordre du groupe de Galois.
- 4) D'après la question 5 S contient un élément d'ordre p . p étant premier, la factorisation en produit de cycle implique que S contient un produit de p -cycles qui sont les éléments de S_p d'ordre p , donc S contient un p -cycle.
- 5) Pour $p = 5$, on a $\overline{P}(X) = X^5 - X - 2$. Pour $x \in \mathbf{F}_5$, on a $P(x) = -2 \neq 0$. Pour $x \in \mathbf{F}_{25}$, on a $x^{25} = x$, alors

$$x = (x^5)^5 = (x + 2)^5 = x^5 + 2^5 = x + 4,$$

contradiction.

6) On en déduit que la réduction de $P(X)$ dans $\mathbf{F}_5[X]$ est irréductible. Le lemme de Gauss implique alors que $P(X)$ est irréductible dans $\mathbf{Q}[X]$.

7) Il suffit de montrer que P a exactement 3 racines réelles. On l'obtient avec une étude de fonction car P' a deux racines réelles $\pm(5/6)^{1/4}$. On note alors que $P(-(5/6)^{1/4}) > 0$ et $P((5/6)^{1/4}) < 0$

Exercice 2.

- 1) On obtient
$$(X^2 + 3)(X^3 - 3X + 1).$$
- 2) Non car le polynôme n'est pas irréductible.
- 3) Les deux facteurs sont clairement résolubles (degrés 2 et 3), donc P l'est aussi.

4) Le degré est 6 ou 12, selon que G est isomorphe au sous-groupe de S_5 engendré par $(1, 2)$ et $(3, 4, 5)$ ou au sous-groupe de S_5 engendré par $(1, 2)$ et $\text{Bij}(3, 4, 5)$. Le groupe n'est commutatif que dans le premier cas.

5) On note que les racines de $X^3 - 3X + 1$ sont réelles. La base télescopique donne donc $[K : \mathbf{Q}] = 2[K' : \mathbf{Q}]$ où K' est le corps de décomposition de $X^3 - 3X + 1$. Son discriminant étant $4 \times 27 - 27 = 9^2$, son groupe de Galois est A_3 . Donc le degré est 6 et le groupe de Galois est commutatif.

Exercice 3.

1) Le groupe de Galois de l'extension cyclotomique est $(\mathbf{Z}/7\mathbf{Z})^*$ qui est cyclique car 7 est premier.

2) Elle est contenue dans $\mathbf{Q}[e^{2i\pi/7}]$ qui est clairement résoluble.

3) C'est une sous-extension de $\mathbf{Q}[e^{2i\pi/7}]/\mathbf{Q}$ qui a pour degré 6. Comme l'extension est réelle, le degré est 3 ou 1. On vérifie alors que $\cos(\frac{2\pi}{7})$ n'est pas dans \mathbf{Q} . Sinon, $\sin(\frac{2\pi}{7})$ serait de degré au plus 2, contradiction avec le degré 6 ci-dessus. La réponse est 3.

4) On aurait un i tel que $[k_{i+1} : k_i[x_i]]$ est divisible par 3. Donc on aurait au moins 3 conjugués de x_i réels (on rappelle que l'extension $\mathbf{Q}[e^{2i\pi/7}]/\mathbf{Q}$ est galoisienne), mais seuls x_i et $-x_i$ sont des conjugués réels de x_i .

5) Le corps de décomposition K est une extension galoisienne de k contenue dans \mathbf{R} et $[K : k]$ est divisible par 3 (par exemple K contient $k[x]$ pour x racine de P). On conclut comme ci-dessus.

6) Il suffit de regarder les conjugués de x_1, x_2, x_3 et de $e^{2i\pi/3}$.

7) Calcul direct pour les transpositions.

8) On considère

$$Q(X) = (X - y_1)(X - y_2) \in K'[X].$$

D'après la question précédente il est invariant pour l'action du groupe de Galois le $K'/k[e^{2i\pi/3}]$, donc ses coefficients sont dans $k[e^{2i\pi/3}]$.

9) On a l'invariance par conjugaison complexe car $\overline{x_2} = x_3$.

10) Comme $k[e^{2i\pi/3}] = k \oplus ke^{2i\pi/3}$, un élément réel de $k[e^{2i\pi/3}]$ est dans k .

11) On remarque d'abord que $x_1 + x_2 + x_3$ est dans k car c'est un coefficient de P . Comme de plus

$$3x_1 = (x_1 + x_2 + x_3) + y'_1 + y'_2,$$

avec $y'_1 = x_1 + e^{2i\pi/3}x_2 + e^{-2i\pi/3}x_3$ et $y'_2 = x_1 + e^{-2i\pi/3}x_2 + e^{2i\pi/3}x_3$ réels, il suffit de montrer le résultat pour $k[y'_1, y'_2]$. Notons $\Delta \in k$ le discriminant

de Q . On considère alors :

$$k \subset k[\sqrt{\Delta}] \subset k[\sqrt{\Delta}, y'_1] \subset k[\sqrt{\Delta}, y'_1, y'_2].$$

12) Il suffit de remplacer k_i par le sous-corps engendré par k_i et L .

13) D'après l'exercice 1, le groupe de Galois $\text{Gal}(K/k)$ contient un sous-groupe d'ordre p , puis on applique la correspondance de Galois.

14) Considérons une extension

$$k \subset k_1 \subset \cdots \subset k_r = k_{r-1}[x_{r-1}]$$

comme dans l'énoncé avec r minimal et les n_i premiers, ce qui est toujours possible quitte à ajouter des étages intermédiaires. En particulier on a $K \subset k_r$ et $k_{r-1} \subsetneq K$. L'extension k_r/k_{r-1} tant de degré premier n_{r-1} , l'extension Kk_{r-1} est soit égale k_{r-1} soit à k_r . Comme $K \neq k_{r-1}$, on a $Kk_{r-1} = k_r$. Comme K est une extension galoisienne de k , Kk_{r-1} est une extension galoisienne de k_{r-1} . Ainsi k_r est une extension galoisienne de k_{r-1} . On en conclut que tous les conjugués de x_{r-1} appartiennent à k_r . Comme k_r est réelle, les seules racines de l'unité appartenant à k_r sont 1 et -1 , ce qui force $n_{r-1} = 2$. Par ailleurs, l'injection du groupe $\text{Gal}(Kk_{r-1}/k_{r-1})$ dans $\text{Gal}(K/K \cap k_{r-1})$ montre que

$$[k_r : k_{r-1}] | [K : K \cap k_{r-1}] | [K : k],$$

on en déduit le résultat puisque $[K : k]$ est premier.

En utilisant les questions précédentes on obtient que tous les $[k_{i+1} : k_i]$ sont des puissances de 2 (si ce n'est pas le cas, 14 puis 13 donnent une contradiction). Le théorème de la base télescopique permet de conclure.