École Polytechnique
Algèbre et théorie de Galois MAT 451

Corrigé du contrôle classant 2021

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) On obtient $P(X) = (1+X)^8$.

2) Le corps de décomposition est $\mathbf{F}_2$.

3) Comme $3 \wedge 8 = 1$, on peut appliquer le résultat du cours et G est un sous-groupe $(\mathbf{Z}/8\mathbf{Z})^* \simeq (\mathbf{Z}/2\mathbf{Z})^2$.

4) On obtient $Q(X) = (X-1)(X+1)(1+X^2)(X^2+X-1)(X^2-X-1)$.

5)On voit que le corps de décomposition de Q n'est pas $\mathbf{F}_3$. Mais les racines d'un polynôme irréductible de degré 2 sont dans $\mathbf{F}_9$. C'est donc le corps de décomposition de Q.

Exercice 2.

1) Le polynôme minimal est X^6-2X^3-2, irréductible dans $\mathbf{Q}[X]$ d'après le critère d'Eisenstein. Le degré est donc 6.

2) On obtient $K = \mathbf{Q}[\alpha, j, \beta]$.

3) On a alors $[\mathbf{Q}[\alpha, j] : \mathbf{Q}] = [\mathbf{Q}[\alpha, j] : \mathbf{Q}[\alpha]][\mathbf{Q}[\alpha] : \mathbf{Q}] = 12$ et $12|[K : \mathbf{Q}] \leq 36$.

4) L'action sur les conjugués de α : $\{\alpha, j\alpha, j^2\alpha, \beta, j\beta, j^2\beta\}$ donne le plongement dans S_6. La sous-extension $\mathbf{Q}[\alpha]/\mathbf{Q}$ n'est pas galoisienne (α a des conjugués non réels), donc G n'est pas commutatif.

5) On a $\mathrm{Gal}(\mathbf{Q}[\sqrt{3}, j]/\mathbf{Q}) \simeq (\mathbf{Z}/2\mathbf{Z})^2$ quotient de G par $\mathrm{Gal}(K/\mathbf{Q}[\sqrt{3}, j])$.

6) La conjugaison complexe σ donne la double transposition $(j\alpha, j^2\alpha)(j\beta, j^2\beta)$. On a $\sigma(j) = j^2$ et $\sigma(\sqrt{3}) = \sqrt{3}$ ce qui caratérise son image dans $\mathrm{Gal}(\mathbf{Q}[\sqrt{3}, j]/\mathbf{Q})$.

7) On remarque $\alpha\beta = -2^{\frac{1}{3}}$ donc $K' \subset K$. C'est clairement une extension galoisienne de $\mathbf{Q}$. On a $[K' : \mathbf{Q}] = 2[\mathbf{Q}[\sqrt{3}, 2^{\frac{1}{3}}] : \mathbf{Q}]$. Comme $[\mathbf{Q}[\sqrt{3}] : \mathbf{Q}] = 2$ et $[\mathbf{Q}[2^{\frac{1}{3}}] : \mathbf{Q}] = 3$ on obtient $[K' : \mathbf{Q}] = 12$.

8) On considère la suite exacte de Galois pour la sous-extension galoisienne $\mathrm{Gal}(\mathbf{Q}[\sqrt{3}, j]/\mathbf{Q}$ comme dans la question 5.

9) Leur ordre divise 12. Comme le groupe n'est pas commutatif (il y a une sous-extension non galoisienne), l'ordre est 1, 2, 3, 4 ou 6. Il suffit donc de montrer qu'il n'y a pas d'élément d'ordre 4. Soit ϕ le morphisme de la suite exacte et g d'ordre 4. On a $\phi(g^2) = e$ donc $g^2 \in \mathrm{Ker}(\phi)$ et $g^2 \neq e$. Donc g^2 n'est pas d'ordre 2, contradiction.

10) Il faut trouver le nombre de sous-groupes d'ordre 6 et 3. Soit g d'ordre 3. Alors $g^2 \in \mathrm{Ker}(\phi)$ et $g^3 = e$, donc $g \in \mathrm{Ker}(\phi)$. Il y a donc deux éléments d'ordre 3 et $\mathrm{Ker}(\phi)$ est le seul sous-groupe d'ordre 3. Donc il y a un seul sous-corps de degré 4 (c'est $\mathbf{Q}[j, \sqrt{3}]$). Pour H un sous-groupe d'ordre 6, ϕ ne peut être injective sur H donc $\mathrm{Ker}(\phi) \subset H$. Donc $H = \phi^{-1}(\phi(H))$ est déterminé par $\phi(H)$ sous-groupe d'ordre 2. Il y a donc 3 possibilités, et 3 sous-corps de degré 2 ($\mathbf{Q}[\sqrt{3}]$, $\mathbf{Q}[i\sqrt{3}]$, $\mathbf{Q}[i]$).

11) Le groupe $\mathrm{Gal}(K/K')$ est d'ordre 1, 2 ou 3 donc commutatif. La suite exacte ci-dessous montre que $\mathrm{Gal}(K'/\mathbf{Q})$ est résoluble. On a ensuite

$$0 \to \mathrm{Gal}(K/K') \to G \to \mathrm{Gal}(K'/\mathbf{Q}) \to 0$$

donc G est résoluble.

12) L'extension $\mathbf{Q}[2^{\frac{1}{3}}]/\mathbf{Q}$ de degré 3 ne serait contenir une extension quadratique de $\mathbf{Q}$. On a $[K : \mathbf{Q}] = 2 \times [\mathbf{Q}[\alpha, 2^{\frac{1}{3}}] : \mathbf{Q}[2^{\frac{1}{3}}]] \times 3$ avec le deuxième facteur qui vaut 2, 3 ou 6. Comme $\sqrt{3} \in \mathbf{Q}[\alpha, 2^{\frac{1}{3}}]$, le degré ne peut pas être 3 d'après la question précédente. C'est donc 2 ou 6.

13) Supposons que $[\mathbf{Q}[\alpha, 2^{\frac{1}{3}}] : \mathbf{Q}[2^{\frac{1}{3}}]] = 2$. Alors $\alpha = a + b\sqrt{3}$ avec $a, b \in \mathbf{Q}[2^{\frac{1}{3}}]$. En prenant le cube, on obtient $1 = a^3 + 9ab^2 = 3a^2b + 3b^3$. Alors $b \neq 0$ et $0 = x^3 - 3x^2 + 9x - 3$ où $x = a/b \in \mathbf{Q}[2^{\frac{1}{3}}]$. Le degré est donc 36.

Exercice 3.

1) On peut supposer $j < k$ par exemple. Alors F_j divise $F_k - 2$. Donc $F_j \wedge F_k = F_j \wedge 2 = 1$.

2) Comme p_k divise F_k, p_k est impair et $2 \in (\mathbf{Z}/p_k\mathbf{Z})^*$. De plus, $2^{2^k} = -1[p_k]$ et $2^{2^{k+1}} = 1[p_k]$. L'ordre de 2 divise 2^{k+1} mais n'est pas égal à 2^k, c'est donc 2^{k+1}.

3) D'après le théorème de Lagrangen on a donc $2^{k+1} | (p_k - 1)$. Donc pour $t \leq k + 1$, $p_k = 1[2^t]$.

4) Pour $k \neq k'$, on a $p_k \neq p_{k'}$ d'après 1. Donc on obtient une infinité de nombre premiers $p_{t-1}, p_t, \cdots$.

5) On a $c = 2^{p^{t-1}}[p]$ et comme $p^{t-1} = 1[p-1]$, on a $c = 2[p]$.

6) On écrit

$$M = (c^{p-1} - 1) + (c^{p-2} - 1) + \cdots + (c - 1) + p.$$

Donc $M \wedge (c-1) = p \wedge (c-1)$ qui vaut 1 ou p comme p est premier. Mais $c - 1 = 1[p]$ n'est pas divisible par p, donc le pgcd vaut 1.

7) On a $a^{p^t} = 1[q]$ et donc l'ordre de a divise p^t. Si cet ordre divise p^{t-1}, on a $c = 1[q]$ et $q|c-1$, contradiction avec $M \wedge (c-1) = 1$. Donc l'ordre est p^t.

8) Comme ci-dessus, on en déduit que $q = 1[p^t]$. Mais q ne divise pas a et est donc distinct des q_i. On a donc une infinité de nombres premiers.

9) Il existe un nombre premier q tel que $q = 1[m]$ d'après les questions précédentes. Alors le groupe de Galois de la $q$ème extension cyclotomique est isomorphe à $\mathbf{Z}/(q-1)\mathbf{Z}$. Le quotient par le sous-groupe engendré par m est cyclique d'ordre m. Le théorème de la correspondance de Galois donne alors le résultat.

10) D'après le théorème chinois, on a

$$(\mathbf{Z}/n\mathbf{Z})^* \simeq (\mathbf{Z}/(p_1\mathbf{Z}))^* \times \cdots \times (\mathbf{Z}/(p_n\mathbf{Z}))^*.$$

11) D'après la première partie, on peut trouver des nombres premiers distincts p_i tels que pour chaque i, $p_i = 1[m_i]$. On conclut alors avec les questions précédents.

12) On a $5 = 13 = 1[4]$, on peut donc choisir $n = 65$.

13) C'est alors une conséquence directe du théorème chinois et de 11.