École Polytechnique
Algèbre et théorie de Galois MAT 451

Corrigé du contrôle classant 2020

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) Pour $p = 3$, on a $\overline{P}(X) = X^5 - X^2 + 1$. Alors $\overline{P}(0) = \overline{P}(1) = 1$ et $\overline{P}(-1) = -1$, donc $\overline{P}$ n'a pas de racine dans $\mathbf{F}_3$. Puis pour $x \in \mathbf{F}_9 \setminus 0$, on a $x^8 = 1$, donc si $x^5 = x^2 - 1$ on a $1 = x^8 = x^5 - x^3 = x^2 - 1 - x^3$. Donc $x^3 = x^2 + 1$ et $x^5 = x^4 + x^2 = x^2 - 1$, et $x^4 = -1$, contradiction avec $x^8 = 1$.

2) On obtient que $\overline{P}(X)$ est irréductible dans $\mathbf{F}_3[X]$. Il aurait sinon un facteur irréductible de degré au plus 2 et donc une racine dans $\mathbf{F}_9$. On en déduit que P est irréductible dans $\mathbf{Z}[X]$, et le lemme de Gauss permet de conclure.

3) Comme P est irréductible, il est séparable et a 5 racines distinctes dans $\mathbf{C}$. L'action du groupe de Galois sur ces racines et fidèle et donne l'identification souhaitée.

4) On a $P'(X) = X(5X^3 - 2)$ qui a exactement deux racines réelles. L'étude de la fonction polynômiale réelle associée à P montre que P a au plus 3 racines réelles. Mais $P(0) = 1 > 0$ et $P(1) = -2$ donc le théorème des valeurs intermédiaires montre que P a exactement 3 racines réelles. Donc P a 2 racines complexes non réelles conjuguées et la conjugaison complexe est un élément du groupe de Galois correspondant à une transposition.

5) Le théorème de réduction modulo 3 s'applique.

6) Il suffit de montrer qu'un sous-groupe de S_5 contenant une transposition et un 5-cycle est S_5 (voir PC 1).

Exercice 2.

1) Comme $\xi^p = 1$, c'est une extension algébrique. De plus, ξ est une racine primitive $p$ème de 1, donc les conjugués de ξ sont des puissances de ξ.

2) Le polynôme minimal est le polynôme cyclotomique $X^{p-1} + X^{p-2} + \cdots + 1$ et l'extension est de degré $p-1$.

3) Il s'agit d'une extension cyclotomique, le groupe de Galois est commutatif (cours). De plus, il s'identifie au groupe des inversible $(\mathbf{Z}/p\mathbf{Z})^* \simeq \mathbf{Z}/(p-1)\mathbf{Z}$ cyclique car p est premier.

4) L'extension est algébrique et le groupe de Galois est commutatif. Il n'est pas toujours cyclique, par exemple $(\mathbf{Z}/8\mathbf{Z})^* \simeq (\mathbf{Z}/2\mathbf{Z})^2$ n'est pas cyclique.

5) Si x, y sont des carré alors xy et x^{-1} sont des carrés. Si x est un carré et y n'est pas un carré, alors xy n'est pas un carré (sinon $y = (xy)x^{-1}$ le serait aussi). Donc il suffit de montrer que si x, y ne sont pas des carrés, alors xy est un carré. On a l'automorphisme $x \mapsto x^2$ du groupe $\mathbf{F}_p^*$ de noyau $\{1, -1\}$ car $\mathbf{F}_p$ est un corps. L'image $((\mathbf{F}_p)^*)^2$ est donc un sous-groupe d'ordre $(p-1)/2$. Son complémentaire est ainsi $-((\mathbf{F}_p)^*)^2$. Mais $x, y \in -((\mathbf{F}_p)^*)^2$ implique $xy \in ((\mathbf{F}_p)^*)^2$.

6) τ est bien défini car $\exp\left(\frac{2i\pi a}{p}\right)$ ne dépend que de la classe de a modulo p.

7) L'élément g envoie ξ sur ξ^m pour un certain $1 \leq m < p$. Alors

$$g(\tau) = \sum_{a \in (\mathbf{F}_p)^*} \sum_{a \in \mathbf{F}_p^*} \left(\frac{a}{p}\right) \xi^{am} = \left(\frac{m}{p}\right) \tau.$$

8) Si $\tau = 0$, on aurait un polynôme annulateur de ξ de degré $p-1$ différent du polynôme minimal.

9) On a alors

$$x(\tau^2) = x(\tau)x(\tau) = \left(\frac{m}{p}\right)^2 \tau^2 = \tau^2.$$

Comme c'est vrai pour tout élément x du groupe de Galois, on a $\tau^2 \in \mathbf{Q}^*$.

10) On a vu qu'il existe m tel que $\left(\frac{m}{p}\right) = -1$. Pour x correspondant dans le groupe de Galois, on a $x(\tau) = -\tau \neq \tau$ car $\tau \neq 0$. Donc $\tau \notin \mathbf{Q}$.

Exercice 3.

1) Pour une permutation τ, on a

$$\prod_{\sigma \in \mathfrak{S}_d} \left(X - \sum_{i=1}^{d} Y_{\tau(i)} \xi_{\sigma(i)}\right)$$

qui vaut R par changement de variable $\sigma\tau^{-1}$ à la place de σ.

2) On note que $\mathfrak{S}_d$ est le groupe de Galois de l'extension de K engendrée par les Y_i comme dans le cours.

3) Les racines de h sont stables par l'action du groupe de Galois, elles sont donc contenues dans l'ensemble des $g(\sum_i Y_i\xi_i) = \sum_i Y_i g(\xi_i)$. Ces éléments sont de plus distincts car si $g(\xi_i) = g'(\xi_i)$ pour tout i, $g = g'$. Donc h est divisible par $\prod_{g\in G}\left(X - \sum_i Y_i g(\xi_i)\right)$ qui est à coefficients dans K, c'est donc h.

4) C'est le groupe de Galois de $K(Y_1, \cdots, Y_d)$ sur l'extension engendrée par les coefficients de h comme polynôme en X. Il suffit de montrer que les racines de h engendrent $K(Y_1, \cdots, Y_d)$ (alors on obtient le groupe de Galois de ce polynôme).