

EXAMEN PARTIEL, MERCREDI 9 NOVEMBRE 2011, ÉLÉMENTS DE CORRECTION

A–

1. Pour $x \in \mathbb{F}_5$, on a $x^5 = x$, donc $P(x) = 1$.
2. Soit α une racine de P dans K .
 $P(\alpha + 1) = (\alpha + 1)^5 - (\alpha + 1) - 1 = (\alpha^5 + 1) - (\alpha + 1) - 1 = 0$.
3. Soit $F : K \rightarrow K$ le morphisme de Frobenius. Pour tout $k \geq 0$, $F^k(\alpha)$ est racine du polynôme minimal de α , P_α .
 On a $F^k(\alpha) = \alpha + k$, donc P_α a 5 racines : $P = P_\alpha$ est irréductible sur $\mathbb{F}_5$.
4. L'extension $(K : \mathbb{F}_5)$ est de degré 5. Son groupe de Galois est cyclique d'ordre 5, engendré par le morphisme de Frobenius.
5. Le groupe de Galois $\text{Gal}(K : \mathbb{F}_5)$ agit par translation sur les racines de P : $F^k(\beta) = \beta + k$.
6. Soit γ une racine de $Q = X^{25} - X - 1$ dans le corps de décomposition de Q sur $K : L$. Alors $\gamma + \gamma^5$ est racine de P , donc $\mathbb{F}_p(\gamma)$ contient K .

Le corps $\mathbb{F}_5(\gamma)$ contient toutes les racines de Q : les $\gamma + x$, avec $x \in K$. On a donc une tour d'extensions :

$$\mathbb{F}_5 \subset K = \mathbb{F}_5(\alpha) \subset L = \mathbb{F}_5(\gamma) .$$

Etudions les degrés :

$$[L : \mathbb{F}_5] \leq 25 , [K : \mathbb{F}_5] = 5 , \text{ donc } [L : K] \leq 5 .$$

Il en résulte que Q n'est pas irréductible sur K .

Le polynôme minimal de γ sur K a pour racines les $\gamma + k = F^{5k}(\gamma)$, il est de degré 5 (F note encore le morphisme de Frobenius). L'extension $(L : \mathbb{F}_5)$ est de degré 25 : Q est le polynôme minimal de γ sur $\mathbb{F}_5$, il est irréductible sur $\mathbb{F}_5$.

B–

Soit $\zeta = e^{\frac{i\pi}{10}}$.

Soit $F = \mathbb{Q}(\nu)$, avec $\nu = e^{\frac{i2\pi}{5}}$.

1. Le corps $F = \mathbb{Q}(\nu)$ est une extension cyclotomique. Son groupe de Galois $\text{Gal}(F : \mathbb{Q})$ est isomorphe au groupe multiplicatif $(\mathbb{Z}/5\mathbb{Z})^\times$. C'est un groupe cyclique d'ordre 4.
2. $\alpha = \nu + \nu^{-1} = 2 \cos \frac{2\pi}{5}$ est un nombre réel de F . L'extension $(F : \mathbb{Q}(\alpha))$ est quadratique. L'extension $(\mathbb{Q}(\alpha) : \mathbb{Q})$ l'est aussi, elle est donc galoisienne.
3. Les sous-corps de F correspondent aux sous-groupes de $\text{Gal}(F : \mathbb{Q}) \simeq \mathbb{Z}/4$. Ce sont $\mathbb{Q}$, $\mathbb{Q}(\alpha)$, et F .
4. Le groupe de Galois $\text{Gal}(L : \mathbb{Q})$ est isomorphe à $(\mathbb{Z}/20\mathbb{Z})^\times \simeq (\mathbb{Z}/4)^\times (\mathbb{Z}/5)^\times \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$.
5. On obtient 8 sous-groupes, les sous-corps correspondants sont :

$$\mathbb{Q} , \mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{5}) , \mathbb{Q}(i) , \mathbb{Q}(i\sqrt{5}) , F = \mathbb{Q}(\nu) , \mathbb{Q}(\alpha, i) = \mathbb{Q}(i\alpha) , \mathbb{Q}(\zeta^2 + \zeta^{-2}) , L .$$

C–

1. Il y a 3 polynômes unitaires de degré 2 irréductibles sur $\mathbb{F}_3$: $X^2 + 1$, $X^2 + X + 2$ et $X^2 + 2X + 1$. ($9 = n_1 + 2 \times n_2$).
2. Le polynôme $X^4 + X - 1 \in \mathbb{F}_3[X]$ n'a pas de racine et n'est divisible par aucun des trois polynômes irréductibles de degré 2 précédents : il est irréductible sur $\mathbb{F}_3$.
3. $P = X^4 + 4X - 1$ est unitaire et irréductible modulo 3 : il est irréductible sur $\mathbb{Z}$ donc sur $\mathbb{Q}$. Par contre : $Q = X^3 + 4X + 16 = (X + 2)(X^2 - 2X + 8)$ n'est pas irréductible.
4. Le corps de décomposition de Q est une extension quadratique : $\mathbb{Q}(i\sqrt{7})$. Le groupe $\text{Gal}(Q)$ est cyclique d'ordre 2.

5. (a) Les $\sigma_i(\theta_1, \theta_2, \theta_3)$, $1 \leq i \leq 3$, sont invariants sous l'action du groupe de Galois de P (permutation des racines de P), ils appartiennent donc au corps fixe : $\mathbb{Q}$. Pour calculer ces nombres, on va exprimer les polynômes symétriques correspondants dans les 4 variables X_i , notés T_1, T_2 , et T_3 , en fonction des polynômes symétriques élémentaires, qu'on va noter S_j pour distinguer de ceux en 3 variables, puis substituer les valeurs données par les coefficients de P : $S_1 = 0$, $S_2 = 0$, $S_3 = 4$, $S_4 = -1$.

$$T_1 = 2S_2, \quad T_2 = S_2^2 + S_3S_1 - 4S_4, \quad T_3 = S_1S_2S_3 - 2S_3^2 - S_1^2S_4.$$

Donc :

$$\sigma_1(\theta_1, \theta_2, \theta_3) = 0, \quad \sigma_2(\theta_1, \theta_2, \theta_3) = 4, \quad \sigma_3(\theta_1, \theta_2, \theta_3) = -16.$$

Ce qui veut dire que $\theta_1, \theta_2, \theta_3$ sont les racines de Q .

- (b) Le groupe $G = \text{Gal}(L : \mathbb{Q})$ est isomorphe à un sous-groupe de S_4 . Le groupe $\text{Gal}(L : K)$ est le sous-groupe de G formé des éléments qui agissent trivialement sur les θ_i ; c'est un sous-groupe d'indice 2 de G contenu dans le groupe des permutations des α_j qui agissent trivialement sur les θ_i . Les éléments de S_4 qui agissent trivialement sur les θ_i forment le sous-groupe de Klein $V = \{\text{id}, (12)(34), (12)(34), (12)(34)\}$ qui est un sous-groupe normal. Il reste à voir que $\text{Gal}(L : K)$ est égal à tout ce sous-groupe. Le corps L contient les racines carrées des $-\theta_i : \sqrt{2}$ et r avec $r^2 = -1 + i\sqrt{7}$. Le corps $\mathbb{Q}(\sqrt{2}, r)$ est une extension de $K = \mathbb{Q}(i\sqrt{7})$ de degré 4 car $-1 + i\sqrt{7}$ n'est pas un carré dans $\mathbb{Q}(\sqrt{2}, i\sqrt{7})$. On a donc $[L : K] = 4$, et $\text{Gal}(L : K)$ est le groupe de Klein V .
- (c) $\text{Gal}(K : \mathbb{Q})$ est cyclique d'ordre 2 ; $\text{Gal}(L : K)$ est isomorphe au sous-groupe normal à 4 élément de S_4 , le groupe de Klein V ; $\text{Gal}(L : \mathbb{Q})$ est isomorphe au groupe diédral D_8 .