université de BORDEAUX Collège S & T	**Année universitaire 2019/2020** **Session 1 d'automne** **Parcours : 4TMF5** **Code UE : 4TMF502U** **Épreuve : Structures algébriques 2** **Date : 13/12/2019** **Heure : 14h30–17h30** Documents non autorisés. Épreuve de M. Qing LIU

Exercice 1 (Irréductibilité)

1. Rappeler une preuve de l'irréductibilité de $X^{p-1} + X^{p-2} + \cdots + X + 1$ dans $\mathbb{Z}[X]$ pour tout nombre premier p.
2. Montrer que $X^6 + X^3 + 1$ est irréductible dans $\mathbb{Z}[X]$ et dans $\mathbb{Q}[X]$.

Exercice 2 (Polynômes réels positifs) Un polynôme $P(X) \in \mathbb{R}[X]$ est dit *positif* si $P(x) \geq 0$ pour tout $x \in \mathbb{R}$.

1. Montrer que $P_1(X)^2 + P_2(X)^2$ est positif si $P_1(X), P_2(X) \in \mathbb{R}[X]$.
2. Nous allons maintenant montrer la réciproque. Soit $P(X) \in \mathbb{R}[X]$ non nul et positif. Soit

$$P(X) = c \prod_{1 \leq j \leq n} (X - x_j)^{r_j} \prod_{1 \leq k \leq m} (X^2 + a_k X + b_k)^{s_k}$$

sa décomposition en produit de puissances d'irréductibles de $\mathbb{R}[X]$, 2 à 2 non associés (et où c est le coefficient dominant de $P(X)$).

   (a) Montrer que $c \geq 0$ et que les r_j sont pairs.

   (b) Pour tout $k \leq m$, soit $X^2 + a_k X + b_k = (X - z_k)(X - t_k)$ la décomposition dans $\mathbb{C}[X]$. Montrer que $t_k = \bar{z}_k$ (conjuguaison complexe).

   (c) Soit $F(X) = \prod_{1 \leq k \leq m} (X - z_k)^{s_k} \in \mathbb{C}[X]$. En écrivant $F(X)$ sous la forme $F(X) = G_1(X) + iG_2(X)$ avec $G_1(X), G_2(X) \in \mathbb{R}[X]$, montrer que

$$\prod_{1 \leq k \leq m} (X^2 + a_k X + b_k)^{s_k} = G_1(X)^2 + G_2(X)^2.$$

   (d) Conclure.

Exercice 3 Soit $\alpha = 2\cos(2\pi/7) \in \mathbb{R}$. Nous allons déterminer son polynôme minimal $m(X)$ sur $\mathbb{Q}$.

1. Montrer que $\deg m(X) = 3$ (en utilisant le résultat du cours concernant $[\mathbb{Q}[\cos(2\pi/n)] : \mathbb{Q}]$, $n \geq 2$).
2. Soit $\zeta \in \mathbb{C}$ une racine primitive 7-ième de l'unité. Posons $\lambda_k = \zeta^k + \zeta^{-k}$ pour $k = 1, 2, 3$. Montrer que

$$\lambda_1^2 = \lambda_2 + 2, \quad \lambda_1^3 = \lambda_3 + 3\lambda_1.$$

3. Donner le polynôme minimal de ζ sur $\mathbb{Q}$ et montrer que $\lambda_1+\lambda_2+\lambda_3+1=0$.
4. En déduire que λ_1 est racine du polynôme $X^3+X^2-2X-1 \in \mathbb{Q}[X]$.
5. En prenant $\zeta = \exp(2i\pi/7)$, donner le polynôme minimal $m(X)$ de α sur $\mathbb{Q}$.
6. En prenant respectivement $\zeta = \exp(4i\pi/7)$ et $\zeta = \exp(6i\pi/7)$, montrer que $2\cos(4\pi/7)$ et $2\cos(6\pi/7)$ sont racines de X^3+X^2-2X-1.
7. Montrer que $\mathbb{Q}[\cos(2\pi/7)]$ est le corps de décomposition de $m(X) \in \mathbb{Q}[X]$.

Exercice 4 Soit $L = \mathbb{Q}[\sqrt[3]{2},\ \zeta_3]$ où $\zeta_3 = \exp(2i\pi/3) \in \mathbb{C}$.

1. Calculer les degrés $[\mathbb{Q}[\sqrt[3]{2}] : \mathbb{Q}]$ et $[\mathbb{Q}[\zeta_3] : \mathbb{Q}]$. En déduire que $[L : \mathbb{Q}] = 6$.
2. Quels sont les degrés possibles des sous-extensions de $L/\mathbb{Q}$?
3. Soit $K_0 = \mathbb{Q}[\zeta_3]$. Soit K_1 une sous-extension quadratique de L (i.e. $[K_1 : \mathbb{Q}] = 2$). Montrer que le compositum K_0K_1 est de degré 2. En déduire que $K_1 = K_0$.
4. Donner trois sous-extensions de degré 3 de L.

Exercice 5 On fixe un nombre premier p. Nous allons étudier le nombre $N(d)$ de polynômes $\in \mathbb{F}_p[X]$ unitaires irréductibles de degré d. On fixe une clôture algébrique $\bar{\mathbb{F}}_p$ de $\mathbb{F}_p$. Soit $n \geq 1$. Considérons l'application

$$\rho_n : \mathbb{F}_{p^n} \to \mathbb{F}_p[X], \quad x \mapsto \mathrm{Irr}(x, \mathbb{F}_p, X) \in \mathbb{F}_p[X].$$

1. Soit $d \geq 1$. Soit $\alpha \in \bar{\mathbb{F}}_p$ de degré d sur $\mathbb{F}_p$, de sorte que $[\mathbb{F}_p[\alpha] : \mathbb{F}_p] = d$. Montrer que $\alpha \in \mathbb{F}_{p^n}$ si et seulement si d divise n.
2. Soit $P(X) \in \mathbb{F}_p[X]$ irréductible unitaire de degré $d \geq 1$ divisant n. Montrer que $\rho_n^{-1}(P(X))$ est de cardinal d.
3. En déduire que $p^n = \sum_{d|n} dN(d)$.
4. Calculer les valeurs de $N(1), N(2)$.
5. Pour tout $d \geq 1$, montrer que $dN(d) \leq p^d$ et que $\sum_{1 \leq d < n; d|n} dN(d) \leq p^{(n/2)+1}$. En déduire que la suite $(nN(n))_{n\geq 1}$ est strictement croissante et que $nN(n) \geq p^{n/2-1}$ pour tout $n \geq 3$.