

*Durée : 1h30. Justifiez toutes vos réponses. Documents, calculatrices et téléphones portables sont interdits. Le barème est donné à titre indicatif et est susceptible d'être modifié.*

Si  $A$  et  $B$  sont deux

**Exercice 1 (4 points)**

- 1) On considère l'anneau  $A = \mathbb{F}_7[x]/(x^3 + x + 1)$ . La classe du polynôme  $x + 3$  est-elle inversible dans  $A$ ? Si oui, calculer son inverse.
- 2) Résoudre dans  $\mathbb{F}_7[x]$  le système de congruences :

$$\begin{cases} P \equiv x^2 + 1 \pmod{x^3 + x + 1} \\ P \equiv 3 \pmod{x + 3}. \end{cases}$$

**Exercice 2 (5 points)**

On considère les deux courbes planes  $\mathcal{C}_1, \mathcal{C}_2 \subset \mathbb{R}^2$  définies par  $f_1(x, y) = 0$  (resp.  $f_2(x, y) = 0$ ) où

$$\begin{cases} f_1(x, y) = x^2 - y^2 \\ f_2(x, y) = x^3 - 3y^2(y + 3) \end{cases}$$

- 1) Rappeler l'énoncé du théorème d'élimination.
- 2) On note  $R(y)$  le polynôme  $\text{Res}_x(f_1, f_2)$ . Montrer que si  $(x_0, y_0) \in \mathbb{R}^2$  est un point de  $\mathcal{C}_1 \cap \mathcal{C}_2$ , alors  $R(y_0) = 0$ .
- 3) Calculer  $R(y)$ .
- 4) Résoudre l'équation  $R(y) = 0$ ,  $y \in \mathbb{R}$ .
- 5) En déduire  $\mathcal{C}_1 \cap \mathcal{C}_2$ .

**Exercice 3 (4 points)**

Soient  $K$  un corps et  $P \in K[X]$  un polynôme non nul à coefficients dans  $K$ . On note  $n$  son degré,  $a$  son coefficient dominant et  $\alpha_1, \dots, \alpha_n$  ses racines (éventuellement, les racines ne sont pas dans  $K$  mais dans un corps plus grand). On peut donc écrire

$$P = a \prod_{i=1}^n (X - \alpha_i).$$

On notera qu'il peut y avoir des répétitions dans les  $\alpha_i$ .

- 1) Pour un indice  $i$  fixé, calculer  $P'(\alpha_i)$ .
- 2) En déduire la formule

$$\text{Res}(P, P') = (-1)^{\frac{n(n-1)}{2}} a^{2n-1} \prod_{i < j} (\alpha_i - \alpha_j)^2.$$

- 3) Retrouver avec cette formule le fait que le discriminant d'un polynôme  $P$  est nul si et seulement si  $P$  a une racine multiple.

**Exercice 4 (7 points)**

Soit  $K$  un corps. et  $Q$  un polynôme à coefficients dans  $K$ .

1) Pour  $P \in K[X]$  non nul, montrer que la  $K$ -algèbre  $A_P := K[X]/(P)$  est de dimension finie sur  $K$ . Préciser la dimension et expliciter une base.

2) Soient  $P$  et  $Q$  deux polynômes non nuls à coefficients dans  $K$ . Montrer que la multiplication par  $Q$  définit une application  $K$ -linéaire de  $A_P$  dans  $A_P$ . On notera  $\mu_Q$  cette application.

**Définition :** Si  $P$  et  $Q$  sont deux polynômes non nuls à coefficients dans  $K$ , de degrés respectifs  $\alpha$  et  $\beta$ , et de coefficients dominants  $p_\alpha$  et  $q_\beta$ , on pose

$$T(P, Q) = p_\alpha^\beta \det(\mu_Q).$$

Les questions ci-dessous sont indépendantes les unes des autres.

3) Si  $P$  et  $Q$  ne sont pas premiers entre eux, montrer que  $T(P, Q) = 0$ .

4) Si  $P$  et  $Q$  sont premiers entre eux, montrer que  $T(P, Q)$  est non nul. (On pourra utiliser une relation de Bezout, et montrer que  $\mu_Q$  est inversible.)

5) Si  $Q = Q_1P + R$  est la division euclidienne de  $Q$  par  $P$ , montrer que  $T(P, Q) = p_\alpha^{\beta - \deg R} T(P, R)$ .

6) Le but de cette question est de montrer que le résultant de  $P$  et  $Q$  est égal à  $T(P, Q)$ . On considère les applications linéaires suivantes :

$$\varphi: \begin{cases} K_{\beta-1}[X] \times K_{\alpha-1}[X] & \longrightarrow K_{\alpha+\beta-1}[X] \\ (U, V) & \longmapsto PU + VQ \end{cases}$$

$$Div: \begin{cases} K_{\alpha+\beta-1}[X] & \longrightarrow K_{\beta-1}[X] \times K_{\alpha-1}[X] \\ F & \longmapsto (A, B) \end{cases}$$

où  $F = AP + B$  est la division euclidienne de  $F$  par  $P$ .

a) Montrer que  $Div \circ \varphi(U, 0) = (U, 0)$  pour tout  $U \in K_{\beta-1}[X]$ .

b) Si  $V \in K_{\alpha-1}[X]$ , que vaut la deuxième composante de  $Div \circ \varphi(0, V)$  ?

c) Pour  $K_l[X]$ , on choisit la base  $(X^l, \dots, X, 1)$  (pour  $l \in \{\alpha - 1, \beta - 1, \alpha + \beta - 1\}$ ). Montrer que dans ces bases, le déterminant de  $Div \circ \varphi$  est égal à  $\det(\mu_Q)$ .

d) Montrer que dans ces bases, le déterminant de  $Div$  vaut  $p_\alpha^{-\beta}$ .

e) Que vaut le déterminant de  $\varphi$  (toujours dans ces bases) ?

f) Conclure.