# Contrôle Continu 7/12/22

*Durée : 2h*
*Documents, téléphones portables et appareils électroniques interdits*
*La rédaction et la clarté de l'argumentation sera prise en compte dans la notation*

---

**Exercice 1 (Autour du cours)**
Soit $G$ un groupe fini. Montrer que $G$ admet une représentation fidèle.

Soit $(V, \rho)$ la représentation régulière et soit $(e_g)_{g\in G}$ une base telle que $\rho(g)\cdot e_h = e_{gh}$ pour tout $g, h \in G$. Vérifions que c'est une représentation fidèle, i.e. $\mathrm{Ker}(\rho) = \{1\}$. Soit donc $g \in G$ tel que $\rho(g) = \mathrm{id}_V$. En particulier, $e_g = \rho(g)\cdot e_1 = e_1$ et donc $g = 1$.

**Exercice 2 (Un polynôme irréductible ?)**
Soit $n \geq 1$ un entier. Est-ce que le polynôme $X^{2n} - Y^n X^n + Y$ est irréductible dans $\mathbb{Q}[X, Y]$ ?

Dans l'anneau $\mathbb{Q}[Y][X]$, le polynôme vérifie les conditions du critère d'Eisenstein en travaillant avec l'irréductible $Y$ de $\mathbb{Q}[Y]$ qui est un anneau factoriel (car euclidien). Il est donc irréductible dans $\mathrm{Fr}(\mathbb{Q}[Y])[X] = \mathbb{Q}(Y)[X]$ mais comme il est unitaire, il est aussi irréductible dans $\mathbb{Q}[Y][X] \simeq \mathbb{Q}[X, Y]$.

**Exercice 3 (Un peu de corps fini)**
Soit $\mathbb{F}_2 = \{0, 1\}$ le corps à deux éléments.

1. Donner tous les polynômes irréductibles de degré 1, 2 et 3 sur $\mathbb{F}_2$.

   Les polynômes irréductible de degré $\leq 3$ sont les polynômes de degré $\leq 3$ sans racine (car sans racine et degré $\leq 3$ implique irréductible). Donc après énumération ce sont les polynômes $X, X+1, X^2+X+1, X^3+X+1$ et $X^3+X^2+1$.

2. Soit $K_1 = \mathbb{F}_2[X]/(X^3+X+1)$ et $K_2[X] = \mathbb{F}_2[X]/(X^3+X^2+1)$. On notera $\alpha$ la classe de $X$ dans $K_1$ et $\beta$ la classe de $X$ dans $K_2$.

   (a) Justifier que $K_1$ et $K_2$ sont des corps. $K_1$ et $K_2$ sont des corps comme quotient de $\mathbb{F}_2[X]$, qui est principal, par un polynôme irréductible (et donc l'idéal engendré par ce polynôme est maximal).

   (b) Sans donner un isomorphisme, justifier que $K_1$ et $K_2$ sont isomorphe. $K_1$ et $K_2$ sont deux corps de rupture de polynôme de degré 3. En particulier, se sont des espaces vectoriel sur $\mathbb{F}_2$ de dimension 3 et ainsi $|K_1| = |K_2| = 2^3 = 8$. Ainsi $K_1$ et $K_2$ sont isomorphe par unicité à isomorphisme près du corps à 8 éléments.

   (c) Donner un isomorphisme de $K_2$ vers $K_1$ (on pourra vérifier que $\alpha^6 = \alpha^2 + 1$). L'indication n'était pas forcément si aidante, en fait il fallait trouver une racine de $X^3+X^2+1$ sans $K_1$. On pouvait par exemple voir que $(\alpha+1)^3 = (\alpha+1)^2+1$ et donc que $\alpha+1$ était une racine de $X^3+X^2+1$ dans $K_1$ (on aurait aussi pu utiliser $\alpha^6 = \alpha^2+1$ ou $\alpha^2+\alpha+1$ qui sont les autres racines de $X^3+X^2+1$). Ainsi, comme $K_2$ est le corps de rupture de $X^3+X^2+1$ sur $\mathbb{F}_2$, par propriété universelle des corps de rupture, il existe un morphisme $\varphi\colon K_2 \to K_1$ tel que $\varphi(\beta) = \alpha$. $\varphi$ est injectif comme morphisme de corps et c'est un isomorphisme car $|K_1| = |K_2|$.

3. Calculer l'inverse de $\beta + 1$ dans $K_2$.

   Dans $\mathbb{F}_2[X]$ on a la relation de Bezout $X^2(X+1) + (X^3+X^2+1) = 1$ et donc, en passant au quotient, $\beta^2(\beta+1) = 1$. Ainsi $(\beta+1)^{-1} = \beta^2$.

**Exercice 4 (Corps de rupture d'indices premier entre eux)**
Soient $k$ un corps et $P, Q \in k[X]$ deux polynômes irréductibles de degrés respectifs $n$ et $m$ avec $n$ et $m$ premiers entre eux. Soit $K$ un corps de rupture de $P$ sur $k$. On souhaite montrer que $Q$ est irréductible sur $K$. Soit $R$ un facteur irréductible de $Q$ dans $K[X]$ et $L$ un corps de rupture de $R$ sur $K$.

1. Justifier que $n \mid [L : k]$.
   Par multiplicativité des degrés on a $[K : k] \mid [L : k]$. Comme $K$ est un corps de rupture de $P$ sur $k$ et que $P$ est de degré $n$, on a $n = [K : k] \mid [L : k]$.
2. Justifier que $m \mid [L : k]$.
   Comme $L$ est un corps de rupture de $Q$ sur $K$, il contient une racine de $Q$. Soit $\alpha \in L$ une racine de $Q$. On a alors que $k(\alpha)$ est une corps de rupture de $Q$ ($Q$ irréductible) inclus dans $L$. Comme $Q$ est de degré $m$ et par multiplicativité des degrés, on a $m = [k(\alpha) : k] \mid [L : k]$.
3. En déduire que $[L : k] = mn$.
   Par construction comme des corps de rupture, on a que $[K : k] = n$ et que $[L : K] = \deg(R) \leq \deg(Q) = m$. Donc par multiplicativité des degrés, $[L : k] = [L : K][K : k] = n \deg(R) \leq mn$. D'un autre coté, par les deux questions précédentes $n \mid [L : k]$ et $m \mid [L : k]$. Donc comme $m$ et $n$ sont premiers entre eux, $mn \mid [L : k]$. Donc $[L : k] = mn$.
4. Conclure.
   Par la question précédente, on a $n \deg(R) = nm$ donc $\deg(R) = m$ et $Q$ est associé à $R$. Comme ce dernier est irréductible, $Q$ aussi.

**Exercice 5 (Étude d'une extension)**
Soit $L = \mathbb{Q}(\sqrt{2}, i\sqrt{3})$ et $\alpha = \sqrt{2} + i\sqrt{3}$.

1. Montrer que $[L : \mathbb{Q}] = 4$ et donner, en le justifiant, une base de $L$ en tant que $\mathbb{Q}$-espace vectoriel.
   Par multiplicativité des degré, $[L : Q] = [L : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}), \mathbb{Q}]$. Comme $X^2 - 2$ est sans racine et de degré 2 sur $\mathbb{Q}$, il est irréductible et est le polynôme minimal de $\sqrt{2}$ sur $\mathbb{Q}$. Ainsi $[\mathbb{Q}(\sqrt{2}), \mathbb{Q}] = 2$. Ensuite, $X^2 + 3$, dont les racines sont complexe, n'a pas de racine dans $\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{R}$. Donc, comme il est de degré 2, il est irréductible sur $\mathbb{Q}(\sqrt{2})$ et c'est donc le polynôme minimal de $i\sqrt{3}$ sur $\mathbb{Q}(\sqrt{2})$. Ainsi, comme $L = \mathbb{Q}(\sqrt{2})(i\sqrt{3})$, $[L : \mathbb{Q}] = 2 \times 2 = 4$. Une $\mathbb{Q}$-base de $\mathbb{Q}(\sqrt{2})$ est $(1, \sqrt{2})$ et une $\mathbb{Q}(\sqrt{2})$-base de $L$ est $(1, i\sqrt{3}$ donc, par le théorème de la base télescopique, une $\mathbb{Q}$-base est $(1, \sqrt{2}, i\sqrt{3}, i\sqrt{6})$.
2. Montrer que $L = \mathbb{Q}(\alpha)$.
   Comme $\alpha \notin \mathbb{Q}$ (car ce n'est pas un réel par exemple), $[\mathbb{Q}(\alpha) : \mathbb{Q}] \geq 1$ et par multiplicativité des degré, c'est un diviseur de 4. Or $\alpha^2 = 2i\sqrt{6} - 1$ ne peux s'écrire comme combinaison $\mathbb{Q}$-linéaire de 1 et $\alpha$ car la famille $(1, \sqrt{2}, i\sqrt{3}, i\sqrt{6})$ est libre. Ainsi, $\alpha$ n'est la racine d'aucun polynôme de degré 2 à coefficient dans $\mathbb{Q}$. Donc $[\mathbb{Q}(\alpha) : \mathbb{Q}] > 2$. Ainsi $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$ et $L = \mathbb{Q}(\alpha)$.
3. Donner, en le justifiant, le polynôme minimal de $\alpha$ sur $\mathbb{Q}$.
   Comme $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$, on sait que le degré du polynôme minimal sur $\mathbb{Q}$ de $\alpha$ est de degré 4. Par calcul de $\alpha^2, \alpha^3$ et $\alpha^4$, on trouve que $X^4 + 2X^2 + 25$ et un polynôme annulateur de $\alpha$. Comme il est de degré 4 et unitaire c'est le polynôme minimal de $\alpha$ sur $\mathbb{Q}$.

**Exercice 6 (Étude des automorphismes d'une extension)**
Soit $L = \mathbb{Q}(\sqrt{2}, \sqrt[3]{2})$.

1. Montrer que $\mathbb{Q}(\sqrt[3]{2})$ n'admet pas d'automorphisme non trivial.
   Comme tout automorphisme de corps fixe 1, il fixe aussi tout les éléments de $\mathbb{Q}$. En particulier, si $\varphi$ est un automorphisme de $\mathbb{Q}(\sqrt[3]{2})$, il est totalement déterminé par l'image de $\sqrt[3]{2}$. Comme $\sqrt[3]{2}$ est une racine de $X^3 - 2$ et que ce polynôme est à coefficients dans $\mathbb{Q}$, qui est fixé par $\varphi$, $\varphi(\sqrt[3]{2})$ est aussi une racine de $X^3 - 2$. Ce dernier n'ayant qu'une seul racine réelle et comme $\mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{R}$, $\varphi(\sqrt[3]{2}) = \sqrt[3]{2}$ et $\varphi = \mathrm{id}$.
2. On souhaite donner tous les automorphismes de $L$.

(a) Donner toutes les racines de $X^3 - 2$ dans $L$.

Par la même remarque que précédemment, comme $X^3 - 2$ n'a que $\sqrt[3]{2}$ comme racine réelle et que $L \subseteq \mathbb{R}$, $X^3 - 2$ n'a que $\sqrt[3]{2}$ comme racine dans $L$.

(b) Donner tous les automorphismes de $L$ fixant $\mathbb{Q}(\sqrt[3]{2})$.

Soit $\varphi$ un automorphisme de $L$ fixant $\mathbb{Q}(\sqrt[3]{2})$. Comme précédemment, comme $\sqrt{2}$ et $-\sqrt{2}$ sont les racines de $X^2 - 2$ dans $L$, $\varphi(\sqrt{2}) = \pm\sqrt{2}$. Comme $L$ est un corps de rupture de $X^2 - 2$ sur $\mathbb{Q}(\sqrt[3]{2})$ (irréductible sur $\mathbb{Q}(\sqrt[3]{2})$ par l'exercice 4), par propriété universelle des corps de ruptures, il existe exactement deux automorphismes de $L$ fixant $\mathbb{Q}(\sqrt{2})$ : un qui envoie $\sqrt{2}$ sur $-\sqrt{2}$ et l'autre qui envoie $\sqrt{2}$ sur $\sqrt{2}$ (c'est à dire l'identité).

(c) Conclure.

Soit $\varphi$ un automorphisme de $L$. Comme $\varphi$ fixe 1, il fixe $\mathbb{Q}$. Ainsi, $\varphi\colon L \to L$ envoie $\sqrt[3]{2}$ sur une racine de $X^2 - 2$. Par la question (a), il n'y en a pas d'autre dans $L$ donc $\varphi$ est l'identité sur $\mathbb{Q}(\sqrt[3]{2})$. Ainsi, par la question précédente, on a exactement deux automorphismes : l'identité et l'automorphisme de $L$ fixant $\mathbb{Q}(\sqrt[3]{2})$ et envoyant $\sqrt{2}$ sur $-\sqrt{2}$.