Contrôle Continu (6/12/21)

Durée : 1h30
Documents, téléphones portables et appareils électroniques interdits
La redaction et la clarté de l'argumentation sera prise en compte dans la notation
*Les deux questions avec un * sont plus difficiles et sont en bonus*

Exercice 1 (Autour du cours) Soient A un anneau factoriel et $P = a_0 + a_1X + \cdots + a_nX^n \in A[X]$ un polynôme non constant. Montrer que les racines de P dans $\mathrm{Fr}(A)$ sont de la forme $\frac{p}{q}$ avec $p, q \in A$ premiers entre eux, p un diviseur de a_0 et q un diviseur de a_n.

Soit p/q une racine de P avec p et q premier entre eux. On a alors

$$0 = q^nP(0) = a_0q^n + a_1pq^{n-1} + \cdots a_{n-1}qp^{n-1} + a_np^n. \tag{1}$$

Ainsi p divise a_0q^n et par le lemme de Gauss, puisque p et q sont premier entre eux, p divise a_0. De même, en reprenant (1), q divise a_np^n et par le lemme de Gauss, puisque p et q sont premier entre eux, q divise a_n.

Exercice 2 (Racine de puissances premières entre elles)
Soient $a \in \mathbb{Q}$ et $m, n \in \mathbb{N}$ deux entiers premier entre eux.

1) Montrer, sans chercher à l'expliciter et en utilisant les propriétés du corps $\mathbb{C}$, qu'il existe $\alpha_{mn} \in \mathbb{C}$ tel que $(\alpha_{mn})^{mn} = a$ (i.e. α_{mn} est une racine mn-ième de a).

Comme $\mathbb{C}$ est algébriquement clos, le polynôme $X^{mn} - a \in \mathbb{C}[X]$ admet une racine dans $\mathbb{C}$.

2) Montrer que $\mathbb{Q}(\alpha_{mn})$ contient une racine de $X^m - a$ et une racine de $X^n - a$. On les dénotera respectivement α_m et α_n dans la suite.

Comme $\alpha_mn^{mn} = a$ on a que α_{mn}^m est une racine de $X^n - a$ et α_{mn}^n est une racine de $X^m - a$.

3) Montrer proprement les inégalités suivantes.

$$[\mathbb{Q}(\alpha_{mn}) : \mathbb{Q}] \leq mn, \tag{2}$$
$$[\mathbb{Q}(\alpha_m) : \mathbb{Q}] \leq m, \tag{3}$$
$$[\mathbb{Q}(\alpha_n) : \mathbb{Q}] \leq n, \tag{4}$$
$$[\mathbb{Q}(\alpha_{mn}) : \mathbb{Q}(\alpha_m)] \leq n, \text{ et,} \tag{5}$$
$$[\mathbb{Q}(\alpha_{mn}) : \mathbb{Q}(\alpha_n)] \leq m. \tag{6}$$

Soit $k \in \{m, n, mn\}$. $\mathbb{Q}(\alpha_k)$ est un corps de rupture sur $\mathbb{Q}$ d'un polynôme $P_k \in \mathbb{Q}[X]$ irreductible sur $\mathbb{Q}$ et diviseur de $X^k - a$ (plus précisément P_k est le polynôme minimal de α_k sur $\mathbb{Q}$). Ainsi, $[\mathbb{Q}(\alpha_k) : \mathbb{Q}]$ est le degré de P qui est inférieur ou égal au degré de $X^k - a$. Cela donne les inégalité (2), (3) et (4).

Pour les deux autres, il faut voir que α_mn est une racine du polynôme $X^n - \alpha_m$ et $X^m - \alpha_n$. Ainsi, $\mathbb{Q}(\alpha_{mn}) = (\mathbb{Q}(\alpha_m))(\alpha_{mn})$ est le corps de rupture d'un polynôme $Q_n \in \mathbb{Q}(\alpha_m)[X]$ irréductible sur $\mathbb{Q}(\alpha_m)$ et diviseur de $X^n - \alpha_m$ (plus précisément Q_n le polynôme minimal de α_{mn} sur $\mathbb{Q}(\alpha_m)$). Ainsi $QQ(\alpha_{mn}) : \mathbb{Q}(\alpha_m)]$ est le degré de Q_n qui est inférieur ou égal au degré de $X^n - \alpha_m$. D'où (5). Finalement on fait de même en intervertissant m et n pour (6).

4) On suppose ici que $X^m - a$ et $X^n - a$ sont irréductibles sur $\mathbb{Q}$.

a) Montrer que les inégalités (3) et (4) sont des égalités.

Soit $k \in \{m, n\}$. Comme $X^m - a$ est irréductible, c'est le polynôme minimal de α_k sur $\mathbb{Q}$ et cela implique que $\mathbb{Q}(\alpha_k)$ est une extension de degré m de $\mathbb{Q}$.

b) En déduire que m et n divisent $[\mathbb{Q}(\alpha_{mn}) : \mathbb{Q}]$.

Soit $k \in \{m, n\}$. Comme $\mathbb{Q}(\alpha_{mn}) : \mathbb{Q}] = [\mathbb{Q}(\alpha_{mn}) : \mathbb{Q}(\alpha_k)][\mathbb{Q}(\alpha_k) : \mathbb{Q}]$ et que $[\mathbb{Q}(\alpha_k) : \mathbb{Q}] = k$, on a k qui divise $[\mathbb{Q}(\alpha_{mn}) : \mathbb{Q}]$.

c) En déduire que (2) est une égalité.

Comme m et n divisent $[\mathbb{Q}(\alpha_{mn}) : \mathbb{Q}]$ et que m et n sont premier entre eux, mn divise $[\mathbb{Q}(\alpha_{mn}) : \mathbb{Q}]$. Cependant, comme $[\mathbb{Q}(\alpha_{mn}) : \mathbb{Q}] \leq mn$, on a forcément $[\mathbb{Q}(\alpha_{mn}) : \mathbb{Q}] = mn$.

d) En déduire que $X^{mn} - a$ est irréductible sur $\mathbb{Q}$.

Soit P_{mn} le polynôme minimal de α_{mn} sur $\mathbb{Q}$. Comme α_{mn} est une racine de $X^{mn} - a$, P_{mn} divise $X^{mn} - a$. De plus, le degré de P_{mn} est égal à $[\mathbb{Q}(\alpha_{mn}) : \mathbb{Q}]$ qui est mn par la question précédente. Ainsi, comme P_{mn} et $X^{mn} - a$ sont unitaire, ils sont égaux ce qui montre que $X^{mn} - a$ est irréductible sur $\mathbb{Q}$ comme polynôme minimal d'un élément algébrique sur $\mathbb{Q}$.

5) On suppose ici que $X^{mn} - a$ est irréductible sur $\mathbb{Q}$.

a) Montrer que (2) est une égalité.

Comme $X^{mn} - a$ est irréductible sur $\mathbb{Q}$, unitaire et qu'il annule α_{mn} c'est le polynôme minimal de α_{mn} sur $\mathbb{Q}$. Ainsi $\mathbb{Q}(\alpha_m n)$ est le corps de rupture de $X^{mn} - a$ sur $\mathbb{Q}$ et $[\mathbb{Q}(\alpha_{mn}) : \mathbb{Q}] = mn$.

b) En déduire que (3) et (4) sont des égalités.

Soit $k \in \{m, n\}$. Par multiplicativité des degrés, $mn\mathbb{Q}(\alpha_{mn}) : \mathbb{Q}] = [\mathbb{Q}(\alpha_{mn}) : \mathbb{Q}(\alpha_k)][\mathbb{Q}(\alpha_k) : \mathbb{Q}]$. Or, par (3) et (4), ou (5) ou (6), $[\mathbb{Q}(\alpha_{mn}) : \mathbb{Q}(\alpha_k)] \leq mn/k$ et $[\mathbb{Q}(\alpha_k) : \mathbb{Q}] \leq k$. On a donc forcément $[\mathbb{Q}(\alpha_{mn}) : \mathbb{Q}(\alpha_k)] = mn/k$ et $[\mathbb{Q}(\alpha_k) : \mathbb{Q}] = k$.

c) En déduire que $X^m - a$ et $X^n - a$ sont irréductibles sur $\mathbb{Q}$.

Soit $k \in \{m, n\}$. On a $[\mathbb{Q}(\alpha_k) : \mathbb{Q}] = k$ donc α_k est algébrique sur $\mathbb{Q}$ de degré k. Comme $X^k - a \in \mathbb{Q}[X]$ est unitaire, de degré k et annulateur de α_k c'est forcément le polynôme minimal de α_k sur $\mathbb{Q}$. Il est en particulier irréductible sur $\mathbb{Q}$.

6*) Étudier l'irréductibilité sur $\mathbb{Q}$ des polynômes $X^{15} + 4$ et $X^{14} - 8$.

Par ce qui précède, $X^{15} + 4$ est irréductible sur $\mathbb{Q}$ si est seulement su $X^5 + 4$ et $X^3 + 4$ est irréductibles sur $\mathbb{Q}$. Par l'exercice 1, si $X^3 + 4$ avait une racine dans $\mathbb{Q}$, elle serait parmi ± 1, ± 2 ou ± 4 mais aucun de ces nombres n'est racine de $X^3 + 4$. Comme ce dernier est de degré 3, il est alors irréductible. Enfin $X^5 + 4$ est irréductible sur $\mathbb{Q}$ si est seulement si $(X + 1)^5 + 1$ est irréductible sur $\mathbb{Q}$. Or $(X + 1)^5 + 1 = X^5 + 5X^4 + 10X^3 + 10X^2 + 5X + 5$ est irréductible sur $\mathbb{Z}$, donc sur $\mathbb{Q}$, par le critère d'Eisenstein avec $p = 5$. En conclusion, $X^{15} + 4$ est irréductible sur $\mathbb{Q}$.

De même, $X^{14} - 8$ est irréductible sur $\mathbb{Q}$ si et seulement si $X^7 - 8$ et $X^2 - 8$ sont irréductibles sur $\mathbb{Q}$. Le second est irréductible sur $\mathbb{Q}$ car il n'a pas de racine dans $\mathbb{Q}$. Pour le premier, il est irréductible car $(X + 1)^7 - 8$ est irréductible sur $\mathbb{Z}$, donc sur $\mathbb{Q}$, par critère d'Eisenstein avec $p = 7$.

Exercice 3 (Quelques éléments algébriques sur $\mathbb{Q}$)

Montrer que les éléments suivants sont algébriques sur $\mathbb{Q}$ et donner, en le justifiant, leurs polynômes minimaux sur $\mathbb{Q}$.

1) $\sqrt[4]{2}$.

$X^4 - 2 \in \mathbb{Q}[X]$ est un polynôme annulateur de $\sqrt[4]{2}$ donc $\sqrt[4]{2}$ est algébrique sur $\mathbb{Q}$ et son polynôme minimal divise $X^4 - 2$. Or ce dernier est irréductible sur $\mathbb{Z}$, donc sur $\mathbb{Q}$, par critère d'Eisenstein avec $p = 2$. Comme il est unitaire, c'est le polynôme minimal de $\sqrt[4]{2}$ sur $\mathbb{Q}$.

2) $\sqrt{2} - 2$.

$\sqrt{2}-2$ annule $(X+2)^2-2 = X^2+4X+2 \in \mathbb{Q}[X]$ et ce dernier est unitaire et irréductible car il n'a pas de racine dans $\mathbb{Q}$ (son discriminant est < 0). Donc $\sqrt{2}-2$ est algébrique sur $\mathbb{Q}$ et X^2+4X+2 est son polynôme minimal sur $\mathbb{Q}$.

3*) $(1+i)\sqrt{3}$.

On a $\left((1+i)\sqrt{3}\right)^2 = 6i$ donc $\left((1+i)\sqrt{3}\right)^4 = -36$. Ainsi $(1+i)\sqrt{3}$ annule $X^4+36 \in \mathbb{Q}[X]$ et $(1+i)\sqrt{3}$ est algébrique sur $\mathbb{Q}$. L'extension $\mathbb{Q}\left((1+i)\sqrt{3}\right)$ contient strictement $\mathbb{Q}(i)$, car $\sqrt{3} \notin \mathbb{Q}(i)$, qui est une extension de degré 2 sur $\mathbb{Q}$. Ainsi $[\mathbb{Q}\left((1+i)\sqrt{3}\right) : \mathbb{Q}(i)] \geq 2$ et donc $[\mathbb{Q}\left((1+i)\sqrt{3}\right) : \mathbb{Q}] = [\mathbb{Q}\left((1+i)\sqrt{3}\right) : \mathbb{Q}(i)][\mathbb{Q}(i) : \mathbb{Q}] \geq 2 \times 2 = 4$. D'où le polynôme minimal de $(1+i)\sqrt{3}$ est de degré au moins 4. En conclusion, comme X^4+36 est unitaire, c'est le polynôme minimal de $(1+i)\sqrt{3}$ sur $\mathbb{Q}$.

Exercice 4 (Morphismes de corps)

Déterminer, en le justifiant proprement, tous les morphismes de corps de $\mathbb{Q}[\sqrt{15}]$ vers $\mathbb{Q}[\sqrt{17}]$. *on pourra écrire l'image de $\sqrt{15}$ par un tel morphisme sous la forme $a+b\sqrt{17}$ avec $a, b \in \mathbb{Q}$.*

Soit $\varphi\colon \mathbb{Q}[\sqrt{15}] \to \mathbb{Q}[\sqrt{17}]$ un morphisme de corps. et soit $a, b \in \mathbb{Q}$ tel que $\varphi(\sqrt{15}) = a+b\sqrt{17}$. Comme φ est un morphisme d'anneaux, $0 = \varphi(0) = \varphi(\sqrt{15}^2-15) = \left(\varphi(\sqrt{15})\right)^2 - \varphi(15)$. Or comme $\varphi(1) = 1$ et que φ préserve la somme et produit, $\varphi|_{\mathbb{Q}} = \mathrm{id}_{\mathbb{Q}}$. Ainsi, $\varphi(15)$ est une racine de X^2-15. Donc $15 = (a+b\sqrt{17})^2 = (a^2+17b^2)+2b\sqrt{17}$. Comme 15 et a^2+17b^2 sont rationnel, il en est de même de $2b\sqrt{17}$. D'où $b = 0$ et $a^2 = 15$. Mais comme 15 n'est pas un carré dans $\mathbb{Q}$, a ne peux exister. Contradiction.

En conclusion, il n'existe aucun morphisme de corps de $\mathbb{Q}[\sqrt{15}]$ vers $\mathbb{Q}[\sqrt{17}]$.