

Corps et théorie de Galois (HAX801X), CC1 (1h30) : corrigé

Exercice 1 : Questions de cours (4 points) Donnez, en fournissant des justifications *complètes* :

1. la définition d'une extension algébrique de corps : 1 pt c'est une extension de corps E/K telle que chaque élément $x \in E$ est racine d'un polynôme non nul $P \in K[X]$.
2. un polynôme de degré $n > 1$ dont le corps de rupture n'est pas égal au corps de décomposition : 1 pt prenons $K = \mathbb{Q}$ et $P(X) = X^3 - 2 \in K[X]$. L'extension $E = \mathbb{Q}(\alpha)$ engendrée par la racine réelle $\alpha := \sqrt[3]{2}$ de P est un corps de rupture, mais pas un corps de décomposition car les deux autres racines complexes $j\alpha$ et $j^2\alpha$ de P n'appartiennent pas à E puisqu'elles ne sont pas réelles.
3. un polynôme de degré $n > 1$ dont le corps de rupture est égal au corps de décomposition : 1 pt prenons $K = \mathbb{Q}$ et $P(X) = X^2 + 1 \in K[X]$. L'extension $E = \mathbb{Q}(i)$ engendrée par la racine i de P est un corps de rupture, et aussi un corps de décomposition puisque $P = (X + i)(X - i)$ est décomposé (ou scindé) dans $E[X]$.
4. une démonstration du fait que le cardinal d'un corps fini est une puissance d'un nombre premier : 1 pt si K est fini, sa caractéristique – le générateur positif du noyau du morphisme d'anneaux $f : \mathbb{Z} \rightarrow K$ tel que $f(n) = n1_K$ – ne peut être nulle. C'est donc un nombre premier $p > 0$. Alors f induit un morphisme $f' : \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} \rightarrow K$ qui fait de K un $\mathbb{F}_p$ -espace vectoriel, forcément de dimension n finie. Puisque $K \simeq (\mathbb{F}_p)^n$ comme espace vectoriel, on a $|K| = p^n$.

Exercice 2 : Divisibilité pour le degré du corps de décomposition (7 points)

Démontrez par récurrence sur l'entier $n \geq 1$ la propriété : « Si L est le corps de décomposition d'un polynôme P de degré n à coefficients dans un corps K , l'entier $[L : K]$ divise $n!$ ».

Dans la récurrence, on pourra traiter d'abord le cas P irréductible, puis le cas P réductible.

Corrigé. On rappelle que tous les corps de décomposition sont K -isomorphes.

1 pt Pour $n = 1$, le polynôme est scindé donc K est un corps de décomposition et $[L : K] = 1 \leq 1!$. Pour $n \geq 2$, démontrons que $[L : K]$ divise $n!$.

- 1 pt Si P est irréductible, soit $\alpha \in L$ une racine de P . Par irréductibilité, P est égal au polynôme minimal de α sur K et le sous-corps $K(\alpha) \subset L$ est de degré n sur K .
1 pt De plus, dans $K(\alpha)[X]$ on a une écriture $P = (X - \alpha)Q$ et le corps L est engendré par les racines du polynôme Q de degré $n - 1$ donc c'est un corps de décomposition de Q sur $K(\alpha)$.
1 pt Par l'hypothèse de récurrence, l'entier $[L : K(\alpha)]$ divise $(n - 1)!$. Du théorème de la base télescopique on en déduit que $[L : K] = [L : K(\alpha)][K(\alpha) : K] = n[L : K(\alpha)]$ divise $n!$.
- 1 pt Si P est réductible, écrivons $P = QR$ avec Q et R de degrés q, r tels que $0 < q, r < n$. Notons K' la sous-extension de L engendrée par les racines de Q ; c'est un corps de décomposition pour Q sur K .
1 pt Alors L est engendrée comme K' -extension par les racines de R , et bien sûr R est scindé dans $L[X]$. Il s'ensuit que L est un corps de décomposition pour R sur K' .
1 pt L'hypothèse de récurrence fournit $[K' : K] \mid q!$ et $[L : K'] \mid r!$. On en déduit que $[L : K] = [L : K'] \cdot [K' : K]$ divise $q!r!$. Enfin puisque $q!r!$ divise $n!$ (le quotient étant le coefficient binomial $\binom{n}{q}$), on conclut que $[L : K]$ divise $n!$.

Exercice 3 : Un corps de décomposition de degré 3 (11 points)

On considère les nombres complexes $\zeta = e^{2i\pi/7}$, $\alpha = \zeta + \zeta^{-1}$, $\beta = \zeta^2 + \zeta^{-2}$, $\gamma = \zeta^3 + \zeta^{-3}$ et le polynôme $\Phi_7(X) = X^6 + X^5 + X^4 + X^3 + X^2 + X + 1$ dans $\mathbb{Q}[X]$.

1. Démontrez que Φ_7 est irréductible sur $\mathbb{Q}$ si et seulement si $\Phi_7(X+1)$ est irréductible sur $\mathbb{Q}$.
2. Démontrez que Φ_7 est irréductible sur $\mathbb{Q}$. Quelles sont ses racines complexes ?
3. Démontrez qu'il existe un polynôme $P \in \mathbb{Q}[X]$ tel que $\Phi_7(X) = X^3P(X + \frac{1}{X})$.
4. Démontrez que P est irréductible sur $\mathbb{Q}$. Quelles sont ses racines complexes ?
5. Démontrez que β et γ appartiennent à $\mathbb{Q}(\alpha)$.
6. Dites quel est le corps de décomposition de P sur $\mathbb{Q}$ et donnez son degré.

Corrigé.

1. 1 pt Si Φ_7 est réductible (sur $\mathbb{Q}$), il existe $Q, R \in \mathbb{Q}[X]$ non constants tels que $\Phi_7 = QR$, donc $\Phi_7(X+1) = Q(X+1)R(X+1)$ avec $Q(X+1), R(X+1)$ non constants, donc $\Phi_7(X+1)$ est réductible. Réciproquement, si $\Phi_7(X+1)$ est réductible, il existe $F, G \in \mathbb{Q}[X]$ non constants tels que $\Phi_7(X+1) = FG$, donc $\Phi_7(X) = F(X-1)G(X-1)$ avec $F(X-1), G(X-1)$ non constants, donc $\Phi_7(X)$ est réductible. En passant aux contraposées, c'est exactement l'équivalence demandée.
2. 1 pt D'après la question précédente il suffit de démontrer que $\Phi_7(X+1)$ est irréductible. Or, on calcule $(X+1)^7 = X^7 + 7X^6 + 21X^5 + 35X^4 + 35X^3 + 21X^2 + 7X + 1$. Comme $\Phi_7(X) = (X^7 - 1)/(X - 1)$, on en déduit que $\Phi_7(X+1) = ((X+1)^7 - 1)/X = X^6 + 7X^5 + 21X^4 + 35X^3 + 35X^2 + 21X + 7$.
1 pt Les coefficients $a_0, \dots, a_5$ de ce polynôme sont tous divisibles par 7 et a_0 n'est pas divisible par 49, donc d'après le critère d'Eisenstein appliqué avec le premier $p = 7$ ce polynôme est irréductible. De la relation $(X-1)\Phi_7 = X^7 - 1$ découle que les racines complexes de Φ_7 sont les racines primitives 7^{èmes} de l'unité.

3. 1 pt Posons $Y = X + \frac{1}{X}$. La formule du binôme de Newton donne $Y^2 = X^2 + X^{-2} + 2$ et $Y^3 = X^3 + X^{-3} + 3Y$.

1 pt On calcule alors :

$$\begin{aligned}\Phi_7(X) &= X^3(X^3 + X^2 + X + 1 + X^{-1} + X^{-2} + X^{-3}) \\ &= X^3(Y^3 - 3Y + Y^2 - 2 + Y + 1) = X^3(Y^3 - Y^2 - 2Y - 1).\end{aligned}$$

Ceci montre que $\Phi_7(X) = X^3P(X + \frac{1}{X})$ avec $P(Y) = Y^3 - Y^2 - 2Y - 1$.

4. 1 pt Le coefficient constant et le coefficient dominant de P sont $a_0 = -1$ et $a_n = 1$. Par le critère pour les racines rationnelles, une éventuelle racine $a \in \mathbb{Q}$ sera de la forme $a = p/q$ avec $p \in \mathbb{Z} \setminus \{0\}$ et $q \in \mathbb{N} \setminus \{0\}$ premiers entre eux, avec les contraintes $p \mid a_0$ et $q \mid a_n$. Ceci implique que $q = 1$ et $p = \pm 1$. Or $P(1) = -3$ et $P(-1) = -1$ donc P ne possède aucune racine rationnelle. Comme il est de degré 3, il est automatiquement irréductible sur $\mathbb{Q}$.

1 pt Étudions maintenant ses racines complexes. Comme ζ, ζ^2, ζ^3 sont des racines de Φ_7 , la relation $\Phi_7(X) = X^3P(X + \frac{1}{X})$ évaluée sur ces trois valeurs montre que α, β, γ sont des racines de P .

1 pt Or ces trois nombres sont distincts car $\alpha = 2\cos(2\pi/7)$, $\beta = 2\cos(4\pi/7)$, $\gamma = 2\cos(6\pi/7)$ et les trois angles $2\pi/7, 4\pi/7, 6\pi/7$ sont distincts et dans l'intervalle $[0, \pi]$ sur lequel la fonction cosinus est injective. On a trouvé trois racines distinctes de P qui est de degré 3, donc ce sont toutes les racines de P .

5. 1 pt Le calcul déjà fait dans la question 3 montre que $\beta = \alpha^2 - 2$ et $\gamma = \alpha^3 - 3\alpha$. Ainsi β et γ appartiennent à $\mathbb{Q}(\alpha)$.

6. 1 pt D'après la question précédente, sur le corps $\mathbb{Q}(\alpha)$ on a $P(X) = (X - \alpha)(X - \alpha^2 + 2)(X - \alpha^3 + 3\alpha)$. Le polynôme P est donc scindé. Comme $\mathbb{Q}(\alpha)$ est engendré par α (donc aussi par les trois racines α, β, γ) on déduit que le corps de décomposition de P est $\mathbb{Q}(\alpha)$.

1 pt Comme P est irréductible, l'isomorphisme $\mathbb{Q}[X]/(P) \simeq \mathbb{Q}(\alpha)$ fournit le degré $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$.