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

Exercice 1 : Questions de cours (6 points)

1. Donnez la définition d'un élément séparable dans une extension de corps.
2. Donnez sans démonstration un exemple d'une extension de corps qui n'est pas normale :
   (a) en caractéristique 0,
   (b) en caractéristique différente de 0.
3. Énoncez le théorème de correspondance de Galois pour une extension finie galoisienne.

Corrigé. 1. [1 pt] Pour une extension E/K, on dit que $x \in E$ est *séparable sur* K si son polynôme minimal sur K n'a aucune racine double dans un corps de décomposition (ou une clôture algébrique).

2.(a) [1 pt] L'extension E/K avec $K = \mathbb{Q}$ et $E = \mathbb{Q}(\sqrt[3]{2})$ convient.

2.(b) [2 pts] On s'inspire de l'exemple précédent en cherchant un corps K qui ne contient pas toutes les racines troisièmes de l'unité, et un élément $t \in K$ qui n'est pas un cube. On peut prendre $K = \mathbb{F}_2(t)$ et $E = K[X]/(X^3 - t)$. En effet, le polynôme $X^3 - 1$ des racines cubiques de l'unité est séparable donc il a trois racines dans $\overline{\mathbb{F}}_2$ mais sa seule racine dans $\mathbb{F}_2$ est 1.

3. [2 pts] Soit E/K une extension finie galoisienne et $G = \mathrm{Gal}(E/K)$ son groupe de Galois. Pour toute sous-extension $L \subset E$ notons $f(L) = \mathrm{Gal}(E/L)$ et pour tout sous-groupe $H \subset G$ notons $g(H) = E^H$. Alors f et g réalisent des bijections inverses l'une de l'autre, strictement décroissantes, entre l'ensemble des sous-extensions de E/K et l'ensemble des sous-groupes de G. De plus L/K est galoisienne si et seulement si $\mathrm{Gal}(E/L)$ est distingué.

Exercice 2 : Sous-corps de $\mathbb{Q}(i + \sqrt{2})$ (6 points)

1. Montrez que $E = \mathbb{Q}(i + \sqrt{2})$ est une extension galoisienne de degré 4 de $\mathbb{Q}$.
2. Montrez que le groupe de Galois $\mathrm{Gal}(E/\mathbb{Q})$ est isomorphe à $(\mathbb{Z}/2\mathbb{Z})^2$.
3. Donnez la liste des sous-groupes de $(\mathbb{Z}/2\mathbb{Z})^2$.
4. Donnez la liste des sous-extensions de $E/\mathbb{Q}$.

Corrigé. 1. [1 pt] Posons $\alpha = i + \sqrt{2}$. On a $\alpha^2 = 1 + 2i\sqrt{2}$. On voit que $2i\alpha = -2 + 2i\sqrt{2}$ donc

$$2i\sqrt{2} = \alpha^2 - 1 = 2i\alpha + 2.$$

De la dernière égalité, on déduit que $i = (\alpha^2 - 3)/(2\alpha) \in \mathbb{Q}(\alpha)$ puis $\sqrt{2} = \alpha - i \in \mathbb{Q}(\alpha)$. Ceci démontre que l'inclusion $\mathbb{Q}(\alpha) \subset \mathbb{Q}(i, \sqrt{2})$ est une égalité, donc $E = \mathbb{Q}(i, \sqrt{2})$. Ainsi E est le corps de décomposition du polynôme $P = (X^2 + 1)(X^2 - 2)$. L'extension $E/\mathbb{Q}$ est donc finie, normale, et séparable (comme toute extension en caractéristique 0) donc galoisienne.
[1 pt] Il ne reste qu'à calculer $[E : \mathbb{Q}]$. D'abord, nous avons $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$. Par ailleurs $X^2 + 1$ est sans racine dans $\mathbb{Q}(\sqrt{2})$ puisque ce corps est inclus dans $\mathbb{R}$, donc c'est le polynôme minimal de i sur $\mathbb{Q}(\sqrt{2})$. On en déduit que $[E : \mathbb{Q}(\sqrt{2})] = 2$ et par le théorème de la base téléscopique $[E : \mathbb{Q}] = [E : \mathbb{Q}(\sqrt{2})]\,[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 4$.

2. [1 pt] L'extension $E/\mathbb{Q}(\sqrt{2})$ est monogène, engendrée par i de polynôme minimal X^2+1. Il y a donc un $\mathbb{Q}(\sqrt{2})$-automorphisme $\sigma : E \to E$ bien défini par la prescription $\sigma(i) = -i$. L'extension $E/\mathbb{Q}(i)$

est monogène, engendrée par $\sqrt{2}$ de polynôme minimal X^2-2. Il y a donc un $\mathbb{Q}(i)$-automorphisme $\tau : E \to E$ bien défini par la prescription $\tau(\sqrt{2}) = -\sqrt{2}$. On obtient ainsi deux $\mathbb{Q}$-automorphismes $\sigma, \tau : E \to E$.
1 pt Ces $\mathbb{Q}$-automorphismes vérifient $\sigma^2 = \tau^2 = \mathrm{id}$. Par ailleurs $\varphi = \sigma\tau = \tau\sigma$ est l'automorphisme tel que $\varphi(i) = -i$ et $\varphi(\sqrt{2}) = -\sqrt{2}$. Le groupe $\mathrm{Gal}(E/\mathbb{Q})$ est d'ordre égal au degré $[E : \mathbb{Q}]$ qui vaut 4, engendré par les involutions qui commutent σ et τ, donc il est isomorphe à $(\mathbb{Z}/2\mathbb{Z})^2$.

3. 1 pt Parmi les sous-groupes de $G = (\mathbb{Z}/2\mathbb{Z})^2$ figurent G et le sous-groupe trivial. Les autres sous-groupes sont d'ordre 2 par le théorème de Lagrange, et ils sont engendrés par des éléments autres que le neutre, à savoir $g_1 = (0,1)$, $g_2 = (1,0)$ et $g_3 = (1,1)$. Ces éléments engendrent trois sous-groupes distincts $H_i = \langle g_i \rangle$ isomorphes à $\mathbb{Z}/2\mathbb{Z}$. Il y a au total 5 sous-groupes.

4. 1 pt Exprimés avec les générateurs de $\mathrm{Gal}(E/\mathbb{Q})$, les trois sous-groupes d'ordre 2 sont $H_1 = \langle\sigma\rangle$, $H_2 = \langle\tau\rangle$ et $H_3 = \langle\sigma\tau\rangle = \langle\varphi\rangle$. D'après la correspondance de Galois, l'extension $E/\mathbb{Q}$ possède 5 sous-extensions qui sont E, $\mathbb{Q}$, et $E^{H_1} = E^\sigma = \mathbb{Q}(\sqrt{2})$, $E^{H_2} = E^\tau = \mathbb{Q}(i)$ et $E^{H_3} = E^\varphi = \mathbb{Q}(i\sqrt{2})$. (Pour la dernière, il est clair que $i\sqrt{2}$ est fixé par φ, donc $\mathbb{Q}(i\sqrt{2}) \subset E^{H_3}$, et comme $[E : E^{H_3}] = |\mathrm{Gal}(E/E^{H_3}) = |H_3| = 2$ d'après le théorème d'Artin, finalement $\mathbb{Q}(i\sqrt{2}) = E^{H_3}$.)

Exercice 3 : Réalisations de $\mathbb{F}_{16}$ (6 points)

Soit $\mathbb{F}_2$ le corps à deux éléments. On considère les polynômes $P(X) = X^4 + X + 1$ et $Q(X) = X^4 + X^3 + X^2 + X + 1$ et on note $K = \mathbb{F}_2[X]/(P)$ et $L = \mathbb{F}_2[X]/(Q)$.

1. Prouvez que P et Q sont irréductibles sur $\mathbb{F}_2$.
2. Montrez que K et L sont des corps finis dont vous préciserez le cardinal. Sont-ils isomorphes ?
3. Soient α l'image de X dans K, et β l'image de X dans L. Montrez que α engendre le groupe cyclique K^*, mais que β n'engendre pas le groupe cyclique L^*.
4. Montrez que $\gamma := \beta + 1$ engendre le groupe cyclique L^*.
5. Donnez un isomorphisme explicite $K \simeq L$.

Corrigé. 1. 1 pt En préliminaire notons qu'un polynôme irréductible de degré 2 sur $\mathbb{F}_2$ a pour coefficient dominant 1, pour terme constant 1 (sinon 0 serait racine), et le coefficient de X est forcément 1 (car $X^2 + 1 = (X+1)^2$). Le seul tel polynôme est donc $X^2 + X + 1$.
1 pt On a $P(0) = P(1) = 1$ donc P est sans racine, donc sans facteur de degré 1 ou 3. S'il était produit de facteurs irréductibles de degré 2 ce serait $(X^2 + X + 1)^2 = X^4 + X^2 + 1$ ce qui n'est pas le cas. Donc P est irréductible. Exactement les mêmes arguments montrent que Q est irréductible.

2. 1 pt L'anneau K est quotient de l'anneau de polynômes $\mathbb{F}_2[X]$ par l'idéal engendré par un polynôme irréductible, c'est donc un corps. Le théorème de division euclidienne montre que K est un $\mathbb{F}_2$-espace vectoriel de dimension 4 (le degré du polynôme), c'est donc un corps fini. Le théorème d'existence et unicité montre que K est isomorphe à un corps de décomposition de $X^4 - X$ sur $\mathbb{F}_2$. Les mêmes arguments s'appliquent pour L, donc $K \simeq L$.

3. 1 pt Le cardinal de K^* est 15 donc les ordres de ses éléments sont 1, 3, 5 ou 15. Par définition de α, on a $\alpha^4 = \alpha + 1$ donc $\alpha^5 = \alpha^2 + \alpha$. Comme l'écriture d'un élément sur la base $(1, \alpha, \alpha^2, \alpha^3)$ est unique, on constate que $\alpha \neq 1$, $\alpha^3 \neq 1$, $\alpha^5 \neq 1$. Ainsi α est d'ordre 15, donc il engendre K^*. En revanche, de $\beta^4 = \beta^3 + \beta^2 + \beta + 1$ on déduit que $\beta^5 = \beta^4 + \beta^3 + \beta^2 + \beta = 1$ donc β n'engendre par L^*.

4. 1 pt On calcule $\gamma^2 = \beta^2 + 1$, $\gamma^3 = \beta^3 + \beta^2 + \beta + 1$, $\gamma^4 = \beta^4 + 1 = \beta^3 + \beta^2 + \beta$, $\gamma^5 = \beta^3 + \beta^2 + 1$. En regardant les écritures uniques sur la base $(1, \beta, \ldots, \beta^3)$ on voit que $\gamma \neq 1$, $\gamma^3 \neq 1$, $\gamma^5 \neq 1$ donc γ est un générateur de L^*.

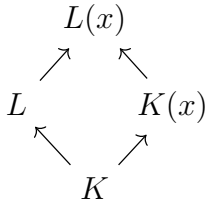
5. [1 pt] En chemin, on a vu que $\gamma^4 = \gamma^3 + 1$. Ceci signifie que $\gamma^4 + \gamma^3 + 1 = 0$ donc en multipliant par γ^{-1}, on trouve que l'élément $\delta := \gamma^{-1}$ vérifie $\delta^4 + \delta + 1 = 0$. En d'autres termes δ est racine de P. On en déduit l'existence d'un morphisme $f : K \to L$ tel que $f(\alpha) = \delta$. C'est un isomorphisme par raison de cardinal.

Exercice 4 : Permanence de l'irréductibilité après extension radicielle (6 points)

Soit L/K une extension de corps de caractéristique $p > 0$ qui est finie et *radicielle*. On note $P \in K[X]$ un polynôme irréductible et *séparable*. On souhaite montrer que P reste irréductible dans $L[X]$.

On note x une racine de P dans une clôture algébrique de L.

1. Démontrez que le degré séparable $[L : K]_s$ vaut 1.
2. Démontrez que $L(x)/K(x)$ est radicielle.
3. Démontrez que $L(x)/L$ est séparable.
4. En considérant le diagramme d'extensions ci-contre, déduisez-en que $[L(x) : L] = [K(x) : K]$.
5. Concluez que P est irréductible dans $L[X]$.



Corrigé. 1. [1 pt] Fixons une clôture algébrique $\overline{K}$ de K, c'est aussi une clôture algébrique de L et on voit L comme un de ses sous-corps. Soient $x_1, \dots, x_n \in L$ des générateurs de l'extension. Pour chaque i soit P_i le polynôme minimal de x_i sur K. Par définition d'une extension radicielle il existe $d \geqslant 1$ et $a \in K$ tels que $(x_i)^{p^d} = a$, donc P_i divise $X^{p^d} - a = (X - x_i)^{p^d}$ dont la seule racine dans $\overline{K}$ est x_i. Le degré séparable $[L : K]_s$ est le nombre K-morphismes $f : L \to \overline{K}$. Or pour chaque i l'image $f(x_i)$ est une racine de P_i, donc $f(x_i) = x_i$. Ainsi f est l'identité. Finalement $[L : K]_s = 1$.

2. [1 pt] Notons $n = \deg(P)$. On sait que $L(x)$ est un K-espace vectoriel de base $\{1, x, \dots, x^{n-1}\}$. Soit $u = u_0 + u_1 x + \cdots + u_{n-1}x^{n-1}$ un élément de $L(x)$, avec $u_i \in L$. Comme L/K est radicielle, pour chaque i il existe $d_i \geqslant 1$ tel que $(u_i)^{p^{d_i}} \in K$. Notons d le maximum des d_i. Alors $(u_i)^{p^d} \in K$ pour tout i donc $u^{p^d} = \sum (u_i)^{p^d} x^{ip^d} \in K(x)$. Ceci montre que $L(x)/K(x)$ est radicielle.

3. [1 pt] Comme $P(x) = 0$ dans K, on a aussi $P(x) = 0$ dans L. Il s'ensuit que le polynôme minimal $P_{x,L}$ de x dans L divise P. Comme P est séparable, alors son facteur $P_{x,L}$ est également séparable. Alors l'extension $L(x)/L$ est engendrée par un élément séparable, donc elle est séparable.

4. [2 pts] Calculons $[L(x) : K]_s$ avec le théorème de la base téléscopique séparable. D'une part :

$$[L(x) : K]_s = [L(x) : K(x)]_s \, [K(x) : K]_s = [K(x) : K]_s = [K(x) : K]$$

puisque $L(x)/K(x)$ est radicielle (on utilise ici les questions 2 et 1) et $K(x)/K$ est séparable (puisqu'engendrée par un élément séparable). D'autre part :

$$[L(x) : K]_s = [L(x) : L]_s \, [L : K]_s = [L(x) : L]$$

puisque $L(x)/L$ est séparable (question 3) et L/K est radicielle (question 1). Finalement :

$$[L(x) : L] = [L(x) : K]_s = [K(x) : K].$$

5. [1 pt] Notons $Q \in L[X]$ le polynôme minimal de x sur L. On a $Q \mid P$. Par ailleurs, d'après la question précédente nous avons $\deg(Q) = [L(x) : L] = [K(x) : K] = \deg(P)$. Comme P et Q sont unitaires, il s'ensuit que $Q = P$. Comme Q est irréductible dans $L[X]$, alors P l'est aussi.