Corps et théorie de Galois (HAX801X)

Contrôle terminal. Durée : 3h.

Toute affirmation doit être justifiée. La clarté et la précision de la rédaction auront une place importante dans la notation. Le barême est donné à titre indicatif.

Exercice 1 : Questions de cours (4 points)

Soit K un corps. Donnez la définition des concepts suivants :

1. un corps de rupture d'un polynôme $P \in K[X]$: [0,5 pt] c'est une extension L/K telle que P possède une racine x dans L, et L est engendré par x comme extension de K.
2. un corps de décomposition d'un polynôme $P \in K[X]$: [0,5 pt] c'est une extension L/K telle que P est scindé dans $L[X]$, et ses racines engendrent L comme extension de K.
3. une clôture algébrique de K : [1 pt] c'est une extension algébrique L/K telle que L est algébriquement clos (c'est-à-dire que tout polynôme à coefficients dans L est scindé dans $L[X]$).

Soient $E/L/K$ des extensions de corps, et $x \in E$. Démontrez que :

4. si x est séparable sur K, il l'est sur L : [1 pt] si x est séparable sur K, son polynôme minimal $P_{x,K}$ est séparable (scindé à racines simples dans une clôture algébrique $\overline{K}/K$). Comme le polynôme minimal $P_{x,L}$ divise $P_{x,K}$, il est également séparable, donc x est séparable sur L.
5. si x est radiciel sur K, il l'est sur L : [1 pt] si x est radiciel sur K, il existe un entier $n \geqslant 1$ tel que $x^{p^n} \in K$. Dans ce cas, on a $x^{p^n} \in L$ donc x est radiciel sur L.

Exercice 2 : Un multiple irréductible défini sur le corps de base (2 points)

Démontrer que si E/K est une extension finie et $P \in E[X]$ est irréductible sur E, il existe $Q \in K[X]$ irréductible sur K tel que P divise Q dans $E[X]$.

Corrigé. [1 pt] Soit E'/E un corps de rupture de P, engendré par une racine $x \in E'$. Soit $Q = P_{x,K}$ le polynôme minimal de x sur K ; comme tout polynôme minimal, Q est irréductible.
[1 pt] On sait de plus que P est à coefficients dans E, irréductible dans $E[X]$ et annule x, donc c'est le polynôme minimal de x sur E. Comme Q est à coefficients (dans K donc) dans E et annule x, on déduit que P divise Q.

Exercice 3 : Un polynôme irréductible (4 points)

On considère les deux nombres complexes $\alpha = \sqrt{2}$ et $\beta = \sqrt[3]{5}$, et on pose $\gamma = \alpha + \beta$.

1. Calculez les degrés de α et β sur $\mathbb{Q}$.
2. Trouvez un polynôme $P \in \mathbb{Q}[X]$ de degré 6 tel que $P(\gamma) = 0$.
3. Démontrez que $\mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\gamma)$.
4. Déduisez-en que P est irréductible.

Corrigé. 1. [0,5 pt] Le polynôme $X^2-2 \in \mathbb{Q}[X]$ annule α et est irréductible car de degré 2 et sans racine, donc c'est le polynôme minimal de α sur $\mathbb{Q}$. Ainsi $\deg(\alpha)=2$. Le polynôme $X^3-5 \in \mathbb{Q}[X]$ annule β et est irréductible d'après le critère d'Eisenstein appliqué avec le premier $p=5$, donc c'est le polynôme minimal de β sur $\mathbb{Q}$. Ainsi $\deg(\beta)=3$.

2. [1 pt] En utilisant le binôme de Newton et le fait que $\alpha^2=2$, on a $5=\beta^3=(\gamma-\alpha)^3=\gamma^3-3\alpha\gamma^2+6\gamma-2\alpha$. On en déduit que $\gamma^3+6\gamma-5=3\alpha\gamma^2+2\alpha=(3\gamma^2+2)\alpha$ puis $(\gamma^3+6\gamma-5)^2=2(3\gamma^2+2)^2$. Ainsi $P=X^6-6X^4-10X^3+12X^2-60X+17$ est de degré 6 et annule γ.

3. [0,5 pt] À la question précédente nous avons montré que $\gamma^3+6\gamma-5=(3\gamma^2+2)\alpha$ donc $\alpha=\frac{\gamma^3+6\gamma-5}{3\gamma^2+2}$. Ceci montre que $\alpha \in \mathbb{Q}(\gamma)$. On en déduit que $\beta=\gamma-\alpha \in \mathbb{Q}(\gamma)$. Ainsi l'inclusion $\mathbb{Q}(\gamma) \subset \mathbb{Q}(\alpha,\beta)$ est une égalité.

4. [1 pt] Soient n_α, n_β, n les degrés de $\mathbb{Q}(\alpha), \mathbb{Q}(\beta), \mathbb{Q}(\alpha,\beta)$ sur $\mathbb{Q}$. D'après la question 1 on a $n_\alpha=2$ et $n_\beta=3$. Le théorème de la base télescopique pour $\mathbb{Q}(\alpha,\beta)/\mathbb{Q}$ appliqué avec les deux extensions intermédiaires $\mathbb{Q}(\alpha)$ et $\mathbb{Q}(\beta)$ montre que n est divisible par 2 et 3, donc par 6.
[1 pt] Par ailleurs d'après les questions 2 et 3 on a $n=[\mathbb{Q}(\gamma):\mathbb{Q}]=\deg(\gamma) \leqslant \deg(P)=6$. En conséquence, $n=6$. Il en découle que le degré du polynôme minimal $P_{\gamma,\mathbb{Q}}$ est égal à 6, puis que $P=P_{\gamma,\mathbb{Q}}$. Comme tout polynôme minimal, P est alors irréductible.

Exercice 4 : Racines n-ièmes de l'unité dans $\overline{K}$ (3 points)

Soit K un corps et $p=\max(1,\mathrm{car}(K))$ son exposant caractéristique. Pour tout entier $n \geqslant 1$, on note μ_n le groupe des racines n-ièmes de l'unité dans une clôture algébrique de K.

1. Démontrez qu'il existe des entiers $s \geqslant 0$ et $m \geqslant 1$ tels que $n=p^s m$ et $\mathrm{pgcd}(p,m)=1$.
2. Ces entiers sont-ils uniques ?
3. Démontrez que $\mathrm{card}(\mu_n)=m$ et donnez la structure du groupe μ_n.

Corrigé. 1. [0,5 pt] Si $p=1$, les entiers $s=0$ et $m=n$ conviennent. Sinon, l'entier p est un nombre premier. Notons s son exposant dans la décomposition en facteurs premiers de n. On peut alors écrire $n=p^s m$ où l'entier m n'est pas divisible par p, i.e. $\mathrm{pgcd}(p,m)=1$.

2. [0,5 pt] Si $p=1$ l'égalité $n=p^s m=m$ montre que m est unique (il est égal à n), mais s peut prendre toute valeur entière donc il n'est pas unique. Sinon, l'égalité $n=p^s m$ avec $\mathrm{pgcd}(p,m)=1$ impose que s est égal à l'exposant de p dans la décomposition en facteurs premiers de n et que m est la partie première à p dans cette décomposition, donc (s,m) est unique.

3. [0,5 pt] Par définition le groupe μ_n est l'ensemble des racines de $P=X^n-1$ dans une clôture algébrique $\overline{K}$. Que l'on ait $p=1$ auquel cas c'est tautologique ou $p>1$ auquel cas c'est dû à l'existence du morphisme de Frobenius, on peut toujours écrire $P=X^{p^s m}-1=(X^m-1)^{p^s}$. Celui-ci a mêmes racines que $Q=X^m-1$, donc $\mu_n=\mu_m$.
[1 pt] Par ailleurs le dérivé de Q est $Q'=mX^{m-1}$ avec $m \neq 0$ dans K, donc Q' est de degré $m-1$ avec pour seule racine le nombre $x=0$. Comme 0 n'est pas racine de Q, on a $\mathrm{pgcd}(Q,Q')=1$ si bien que Q est séparable. Il en découle que $|\mu_n|=|\mu_m|=m$.
[0,5 pt] Enfin on sait que tout sous-groupe fini du groupe multiplicatif K^* est cyclique, donc μ_n est un groupe cyclique d'ordre m.

Exercice 5 : Une extension galoisienne (5 points)

Soit $\mathbb{F}_2$ le corps à 2 éléments.

1. Démontrez que l'anneau $\mathbb{F}_4=\mathbb{F}_2[X]/(X^2+X+1)$ est un corps à 4 éléments. Démontrez que la classe de X modulo X^2+X+1, notée j, est une racine primitive troisième de l'unité.

Soient $E = \mathbb{F}_4(t)$ le corps de fractions rationnelles en une indéterminée t et $\sigma, \tau : E \to E$ les automorphismes définis par :

$$\begin{cases} \sigma(a) = a^2 & \text{si } a \in \mathbb{F}_4 \\ \sigma(t) = t \end{cases} \qquad \begin{cases} \tau(a) = a & \text{si } a \in \mathbb{F}_4 \\ \tau(t) = jt. \end{cases}$$

2. Les automorphismes σ et τ commutent-ils ?
3. À quel groupe fini connu le groupe G engendré par σ et τ dans $\mathrm{Aut}(E)$ est-il isomorphe ?
4. Démontrez que le corps de points fixes $K = E^G$ est égal à $\mathbb{F}_2(t^3)$.
5. Combien l'extension E/K possède-t-elle de sous-extensions ?

Corrigé. 1. [0,5 pt] Le polynôme $P = X^2 + X + 1$ vérifie $P(0) = P(1) = 1$ donc est sans racine dans $\mathbb{F}_2$, de degré 2. C'est donc un élément irréductible de l'anneau principal $\mathbb{F}_2[X]$, et il engendre un idéal maximal. L'anneau quotient $\mathbb{F}_4 = \mathbb{F}_2[X]/(X^2 + X + 1)$ est donc un corps. Par division euclidienne, c'est aussi un $\mathbb{F}_2$-espace vectoriel de base $\{1, j\}$ donc son cardinal est $2^2 = 4$.
[0,5 pt] Dans $\mathbb{F}_4$, l'élément j est distinct de 1 et vérifie $j^3 - 1 = (j-1)(j^2 + j + 1) = 0$ donc c'est une racine primitive troisième de l'unité.
2. [0,5 pt] On a $(\sigma\tau)(t) = \sigma(jt) = j^2 t$ et $(\tau\sigma)(t) = \tau(t) = jt$. Comme $j \neq j^2$, on a $(\sigma\tau)(t) \neq (\tau\sigma)(t)$ donc σ et τ ne commutent pas.
3. [1 pt] L'automorphisme σ est d'ordre 2 et l'automorphisme τ est d'ordre 3. Montrons que $\sigma\tau = \tau^2\sigma$. On a déjà calculé $(\sigma\tau)(t) = \sigma(jt) = j^2 t$, et par ailleurs $(\tau^2\sigma)(t) = \tau^2(t) = j^2 t$. De plus, si $a \in \mathbb{F}_4$ on a $(\sigma\tau)(a) = \sigma(a) = a^2$ et $(\tau^2\sigma)(a) = \tau^2(a^2) = a^2$. En résumé $\sigma\tau$ et $\tau^2\sigma$ prennent la même valeur sur les éléments de $\mathbb{F}_4$ et sur t, donc ils sont égaux. Finalement le groupe G est engendré par un élément σ d'ordre 2 et un élément τ d'ordre 3 tels que $\sigma\tau\sigma^{-1} = \tau^2$, ce qui caractérise le groupe diédral $\mathbb{D}_3$.
4. [0,5 pt] Le théorème d'Artin implique que l'extension $E^G \subset E$ est galoisienne de degré $|G| = 6$.
[0,5 pt] Or l'extension $\mathbb{F}_2(u) \subset E$ est de degré 6 : en effet, si l'on pose $u = t^3$ pour alléger, elle est composée de l'extension $\mathbb{F}_2(u) \subset \mathbb{F}_2(t)$ de degré 3 (extension non triviale, engendrée par l'élément t racine de $P = X^3 - u \in \mathbb{F}_2(u)$) et l'extension $\mathbb{F}_2(t) \subset \mathbb{F}_4(t)$ de degré 2.
[0,5 pt] Par la base télescopique on a $[E^G : \mathbb{F}_2(u)] = [E : \mathbb{F}_2(u)]/[E : E^G] = 6/6 = 1$ donc $E^G = \mathbb{F}_2(u)$.
Remarque : un calcul direct des éléments de E fixes sous l'action du groupe G donne aussi le résultat.
5. [1 pt] Comme on l'a dit, le théorème d'Artin implique que E/K est galoisienne de groupe G. D'après la correspondance de Galois, le nombre de sous-extensions de E/K est égal au nombre de sous-groupes de G. Voici la liste des sous-groupes de G : le sous-groupe $\{1\}$ d'ordre 1, trois sous-groupes d'ordre 2 engendrés par les trois éléments d'ordre 2, un sous-groupe d'ordre 3 engendré par l'un des deux éléments d'ordre trois (ils engendrent le même sous-groupe), et un sous-groupe d'ordre 6 égal à G lui-même. Cela fait au total 6 sous-groupes, donc 6 sous-extensions.

Exercice 6 : Décomposition de Jordan-Chevalley (6 points)

Soient $\mathrm{M}_n(K)$ la K-algèbre des matrices carrées de taille $n \geqslant 1$ à coefficients dans K, et $A \in \mathrm{M}_n(K)$. On rappelle l'énoncé du théorème de décomposition de Jordan-Chevalley [(1)] :

> *Si le polynôme caractéristique χ_A est scindé sur K, il existe un unique couple de matrices $(S, N) \in \mathrm{M}_n(K)^2$ telles que $A = S + N$; S est diagonalisable ; N est nilpotente ; et $SN = NS$.*

Dans la suite, on suppose que K est *parfait* et on se propose de démontrer que, sans aucune hypothèse sur χ_A il existe une décomposition de Jordan-Chevalley $A = S + N$ avec pour seule modification que l'on demande que S soit diagonalisable sur une clôture algébrique de K.

(1). Appelée le plus souvent *décomposition de Dunford* dans l'enseignement français.

1. On note E/K le corps de décomposition de χ_A. Démontrez que l'extension E/K est galoisienne.
2. Soit σ un élément du groupe $G = \mathrm{Gal}(E/K)$. Pour toute matrice $M = (m_{i,j})$ dans $\mathrm{M}_n(E)$, on note $\sigma(M)$ la matrice de coefficients $\sigma(m_{i,j})$. Démontrez que l'application $\mathrm{M}_n(E) \to \mathrm{M}_n(E)$ qui à M associe $\sigma(M)$ est un automorphisme de K-algèbres.
3. Comme χ_A est scindé sur E, le théorème de Jordan-Chevalley fournit une écriture unique $A = S + N$ avec $S, N \in \mathrm{M}_n(E)$. Démontrez que pour tout $\sigma \in G$ on a $\sigma(S) = S$ et $\sigma(N) = N$.
4. Déduisez-en que $S \in \mathrm{M}_n(K)$ et $N \in \mathrm{M}_n(K)$.
5. On considère la matric de rotation $A = \left(\begin{smallmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{smallmatrix}\right)$, avec $\theta \in \mathbb{R}$. Calculez son polynôme caractéristique et sa décomposition de Jordan-Chevalley $A = S + N$ dans $\mathrm{M}_2(\mathbb{R})$.

Corrigé. 1. [0,5 pt] On sait d'après le cours qu'une extension qui est un corps de décomposition est la même chose qu'une extension finie normale ; donc E/K est normale. De plus, comme K est parfait toute extension E/K est séparable. Ainsi E/K est séparable et normale, donc galoisienne.

2. [1 pt] On vérifie les axiomes d'un morphisme de K-algèbres. Soient deux matrices $M = (m_{i,j})$, $N = (n_{i,j})$ et un scalaire $\lambda \in K$. Alors la combinaison linéaire $P = \lambda M + N$ a pour coefficients les $p_{i,j} = \lambda m_{i,j} + n_{i,j}$ et le produit $Q = MN$ a pour coefficients les $q_{i,j} = \sum_{k=1}^{n} m_{i,k} n_{k,j}$. Comme σ est un K-automorphisme de corps, on a $\sigma(p_{i,j}) = \lambda\sigma(m_{i,j}) + \sigma(n_{i,j})$ et $\sigma(q_{i,j}) = \sum_{k=1}^{n} \sigma(m_{i,k})\sigma(n_{k,j})$. Ceci établit que $\sigma(\lambda M + N) = \lambda\sigma(M) + \sigma(N)$ et $\sigma(MN) = \sigma(M)\sigma(N)$. Pour finir, $\sigma(\mathrm{I}_n) = \mathrm{I}_n$.
[0,5 pt] On conclut en notant que l'application $M \mapsto \sigma^{-1}(M)$ en est l'application réciproque, de sorte que σ est un automorphisme de K-algèbres.

3. [1 pt] Les quatre propriétés caractéristiques de la décomposition de Jordan-Chevalley se traduisent de manière complètement explicite en écrivant :

1. $A = S + N$,
2. il existe $D, P \in \mathrm{M}_n(E)$ avec D diagonale telles que $S = PDP^{-1}$,
3. il existe un entier $k \geqslant 1$ tel que $N^k = 0$,
4. $SN = NS$.

D'après la question précédente, en appliquant σ on obtient $\sigma(A) = \sigma(S) + \sigma(N)$, de plus $\sigma(S) = \sigma(P)\sigma(D)\sigma(P)^{-1}$ avec $\sigma(D)$ diagonale et $\sigma(P)$ inversible (puisque $\sigma(P^{-1})$ est son inverse), par ailleurs $\sigma(N)^k = 0$, et enfin $\sigma(S)\sigma(N) = \sigma(N)\sigma(S)$. En conclusion nous voyons que $\sigma(A) = \sigma(S) + \sigma(N)$ est la décomposition de Jordan-Chevalley de $\sigma(A)$.
[0,5 pt] Or A étant à coefficients dans K, on a $\sigma(A) = A$. Donc $S + N = A = \sigma(S) + \sigma(N)$ est la décomposition de Jordan-Chevalley de A. Par unicité de celle-ci, on obtient $\sigma(S) = S$ et $\sigma(N) = N$.

4. [1 pt] L'égalité $\sigma(S) = S$ se traduit par $\sigma(s_{i,j}) = s_{i,j}$ pour tous i, j. Comme ceci a lieu pour chaque $\sigma \in G$, en fixant i, j on a un coefficient $s_{i,j} \in E^G$. Or on sait que $E^G = K$ (dans le cours ceci découle du « théorème d'inégalité »). On en déduit que $s_{i,j} \in K$, donc $S \in \mathrm{M}_n(K)$. Le même raisonnement montre que $N \in \mathrm{M}_n(K)$.

5. [0,5 pt] Le polynôme caractéristique est $\chi_A(X) = X^2 - \mathrm{tr}(A)X + \det(A) = X^2 - 2\cos(\theta)X + 1$.
[1 pt] Son discriminant vaut $\Delta(\chi_A) = 4\cos^2(\theta) - 4 = -4(1 - \cos^2(\theta))$. Distinguons trois cas. Si $\theta \equiv 0 \mod (2\pi)$, on a $A = \mathrm{I}_2$ qui est diagonalisable dans $\mathbb{R}$. Si $\theta \equiv \pi \mod (2\pi)$, on a $A = -\mathrm{I}_2$ qui est diagonalisable dans $\mathbb{R}$. Si $\theta \not\equiv 0, \pi \mod (2\pi)$, on a $\Delta(\chi_A) < 0$ donc la matrice A possède deux valeurs propres complexes distinctes, et elle est diagonalisable dans $\mathbb{C}$. Dans tous les cas, la décomposition de Jordan-Chevalley de A dans $\mathbb{C}$ est fournie par $S = A$ et $N = 0$. Comme nous l'avons démontré avant, cette décomposition vit dans $\mathbb{R}$, c'est la décomposition de Jordan-Chevalley dans $\mathbb{R}$.