Université Paris Diderot
M2ENS Groupes, anneaux, corps

Examen du 13 janvier 2019
9h15-12h15

Les notes du cours sont autorisées, tandis que les appareils électroniques sont interdits. Pour tout $(i,j) \in \{1,\dots,45\}^2$ *tel que* $i < j$*, l'énoncé de la question numéro* i*, même non justifié, peut être utilisé dans la réponse à la question numéro* j*.*

Dans cette épreuve, on fixe un corps k, une clôture algébrique Ω de k et un entier $n \in \mathbb{N}$ tel que $n \geqslant 1$. Soient $k[A_1,\dots,A_n]$ l'anneau des polynômes à n indéterminées $A_1,\dots,A_n$ et à coefficients dans k, et $K := k(A_1,\dots,A_n)$ le corps des fractions de l'anneau $k[A_1,\dots,A_n]$. Soit $K[T]$ l'anneau des polynômes à une indéterminée T. On considère le polynôme unitaire $P \in K[T]$ défini par

$$P(T) = T^n - A_1T^{n-1} + \cdots + (-1)^n A_n.$$

Soit L un corps de scindement (ou corps de décomposition) du polynôme P. Par le morphisme de corps canonique $K \to L$, on considère K comme un sous-corps de L. Similairement, on considère k comme un sous-corps de Ω.

Première partie

Le but de cette partie est de montrer que l'extension $K \subset L$ est galoisienne dont le groupe de Galois est isomorphe au groupe symétrique $\mathfrak{S}_n$ (c'est-à-dire le groupe des bijections de $\{1,\dots,n\}$ dans lui-même).

Soient $k[X_1,\dots,X_n]$ l'anneau des polynômes à n indéterminées $X_1,\dots,X_n$ et à coefficients dans k, et $L' := k(X_1,\dots,X_n)$ le corps des fractions de l'anneau $k[X_1,\dots,X_n]$. On considère le polynôme $Q \in L'[T]$ défini par

$$Q(T) := \prod_{i=1}^{n}(T - X_i) = (T - X_1)\cdots(T - X_n).$$

On écrit Q sous la forme

$$Q(T) = T^n - S_1T^{n-1} + \cdots + (-1)^n S_n,$$

où pour tout $i \in \{1, \ldots, n\}$,

$$S_i = \sum_{\substack{(j_1,\ldots,j_i)\in\{1,\ldots,n\}^i \\ j_1<\ldots<j_i}} X_{j_1} \cdots X_{j_i} \in k[X_1, \ldots, X_n].$$

Soit $K' := k(S_1, \ldots, S_n)$, qui est un sous-corps de $L' = k(X_1, \ldots, X_n)$.

1. Montrer que L' est le corps de scindement (ou corps de décomposition) du polynôme $Q \in K'[T]$.

2. En déduire que l'extension $K' \subset L'$ est galoisienne.

3. On désigne par $\mathfrak{S}_{\{X_1,\ldots,X_n\}}$ le groupe des bijections de $\{X_1, \ldots, X_n\}$ dans lui-même. Montrer que, pour tout $\varphi \in \mathrm{Gal}(L'/K')$, la restriction de φ à $\{X_1, \ldots, X_n\}$ est une bijection de $\{X_1, \ldots, X_n\}$ dans lui-même. En outre, l'application de $\mathrm{Gal}(L'/K')$ dans $\mathfrak{S}_{\{X_1,\ldots,X_n\}}$ qui envoie $\varphi \in \mathrm{Gal}(L'/K')$ sur $\varphi|_{\{X_1,\ldots,X_n\}}$ est un isomorphisme de groupes.

4. On rappelle que Ω désigne une clôture algébrique de k fixée au début de l'épreuve. Montrer que, pour tout $(\lambda_1, \ldots, \lambda_n) \in \Omega^n$, il existe $(x_1, \ldots, x_n) \in \Omega^n$ tel que

$$(\lambda_1, \ldots, \lambda_n) = (S_1(x_1, \ldots, x_n), \ldots, S_n(x_1, \ldots, x_n)).$$

Indication : on peut considérer les racines d'un polynôme unitaire de degré n dans $\Omega[T]$ bien choisi.

5. Soit R un élément non nul de $k[A_1, \ldots, A_n]$. Montrer qu'il existe au moins un $(\lambda_1, \ldots, \lambda_n) \in \Omega^n$ tel que $R(\lambda_1, \ldots, \lambda_n) \neq 0$. *Indication : On peut raisonner par récurrence sur n.*

6. En déduire que le morphisme d'anneaux

$$k[A_1, \ldots, A_n] \longrightarrow k[X_1, \ldots, X_n],$$

qui envoie tout polynôme $R \in k[A_1, \ldots, A_n]$ sur $R(S_1, \ldots, S_n) \in k[X_1, \ldots, X_n]$, est injectif.

7. Montrer que le morphisme d'anneaux dans la question précédente induit un isomorphisme de corps de K dans K'.

8. Montrer que le polynôme P est séparable. En déduire que l'extension $K \to L$ est galoisienne dont le groupe de Galois est isomorphe à $\mathfrak{S}_n$.

Deuxième partie

Dans cette partie, on suppose que $n \geqslant 2$. Pour tout $\sigma \in \mathfrak{S}_n$, soit

$$\mathrm{sgn}(\sigma) := \prod_{\substack{(i,j)\in\{1,\dots,n\}^2 \\ i<j}} (-1)^{\sigma(j)-\sigma(i)} \in \{1,-1\}.$$

9. Soit $\mathscr{P}_n$ l'ensemble des parties de cardinal 2 de $\{1,\dots,n\}$. Montrer que, pour tout $\sigma \in \mathfrak{S}_n$, on a

$$\mathrm{sgn}(\sigma) = \prod_{\{i,j\}\in\mathscr{P}_n} \frac{\sigma(j)-\sigma(i)}{j-i}.$$

10. En déduire que $\mathrm{sgn} : \mathfrak{S}_n \to \{1,-1\}$ est un morphisme de groupes, où on considère la loi multiplicative sur $\{1,-1\}$.

11. On désigne par $\delta_n \in L'$ l'élément défini par

$$\delta_n = \prod_{\substack{(i,j)\in\{1,\dots,n\}^2 \\ i<j}} (X_i - X_j).$$

Montrer que δ_n^2 appartient à K'.

12. Montrer qu'il existe un unique élément Δ_n de $k(A_1,\dots,A_n)$ tel que

$$\Delta_n(S_1,\dots,S_n) = \delta_n^2.$$

Déterminer Δ_2.

13. Pour tout $\sigma \in \mathfrak{S}_n$, soit φ_σ l'unique élément de $\mathrm{Gal}(L'/K')$ tel que $\varphi_\sigma(X_i) = X_{\sigma(i)}$ quel que soit $i \in \{1,\dots,n\}$. Montrer que, pour tout $\sigma \in \mathfrak{S}_n$, on a

$$\varphi_\sigma(\delta_n) = \mathrm{sgn}(\sigma)\delta_n.$$

Pour tout $\lambda = (\lambda_1,\dots,\lambda_n) \in k^n$, soit F_λ le polynôme

$$T^n - \lambda_1 T^{n-1} + \cdots + (-1)^n \lambda_n.$$

On choisit en outre un élément $(\alpha_1(\lambda),\dots,\alpha_n(\lambda)) \in \Omega^n$ tel que

$$F_\lambda(T) = \prod_{i=1}^{n} (T - \alpha_i(\lambda)).$$

Soit L_λ le corps $k(\alpha_1(\lambda),\dots,\alpha_n(\lambda))$.

14. Soit $\lambda = (\lambda_1, \ldots, \lambda_n) \in k^n$. Montrer que F_λ n'a que de racines simples dans Ω si et seulement si

$$\Delta_n(\lambda_1, \ldots, \lambda_n) \neq 0.$$

15. Soit $\lambda = (\lambda_1, \ldots, \lambda_n) \in k^n$ tel que $\Delta_n(\lambda_1, \ldots, \lambda_n) \neq 0$. Montrer que l'extension $k \subset L_\lambda$ est galoisienne.

Soit $\lambda = (\lambda_1, \ldots, \lambda_n) \in k^n$ tel que les racines $\alpha_1(\lambda), \ldots, \alpha_n(\lambda)$ soient distinctes. Pour tout élément $\phi \in \mathrm{Gal}(L_\lambda/k)$, soit τ_ϕ l'unique élément de $\mathfrak{S}_n$ tel que

$$\forall\, i \in \{1, \ldots, n\}, \quad \phi(\alpha_i(\lambda)) = \alpha_{\tau_\phi(i)}(\lambda).$$

Soit

$$\delta_n(\lambda) := \prod_{\substack{(i,j)\in\{1,\ldots,n\}^2 \\ i<j}} (\alpha_i(\lambda) - \alpha_j(\lambda)) \in L_\lambda.$$

16. Montrer que la correspondance $\phi \mapsto \tau_\phi$ définit un morphisme de groupes de $\mathrm{Gal}(L_\lambda/k)$ dans $\mathfrak{S}_n$.

17. Montrer que, pour tout $\phi \in \mathrm{Gal}(L_\lambda/k)$, la valeur de $\mathrm{sgn}(\tau_\phi)$ ne dépend pas du choix de l'ordre des $\alpha_1(\lambda), \ldots, \alpha_n(\lambda)$.

18. Montrer que, pour tout $\phi \in \mathrm{Gal}(L_\lambda/k)$, on a

$$\phi(\delta_n(\lambda)) = \mathrm{sgn}(\tau_\phi)\delta_n(\lambda).$$

19. On suppose que la caractéristique de k est différent de 2. Montrer que $\Delta_n(\lambda_1, \ldots, \lambda_n)$ appartient à l'image de l'application $k \to k$, $x \mapsto x^2$ si et seulement si $\mathrm{sgn}(\tau_\phi) = 1$ pour tout $\phi \in \mathrm{Gal}(L_\lambda/k)$.

Troisième partie

Le but de cette partie est d'étudier la résolubilité des groupes $\mathfrak{S}_n$. Pour tout entier $n \in \mathbb{N}$ tel que $n \geqslant 2$, soit $\mathfrak{A}_n$ le noyau du morphisme de groupes $\mathrm{sgn} : \mathfrak{S}_n \to \{1, -1\}$. Pour tout $(i, j) \in \{1, \ldots, n\}^2$ tel que $i \neq j$, on désigne par $(i\ j)$ la transposition dans $\mathfrak{S}_n$ qui échange i et j. On peut utiliser sans justification les faits que le groupe $\mathfrak{S}_n$ est engendré par les transpositions et que les transpositions sont toutes conjuguées (en d'autres termes, pour tous éléments i, j, k, l de $\{1, \ldots, n\}$ tels que $i \neq j$ et $k \neq l$, il existe $\sigma \in \mathfrak{S}_n$ tel que $(k\ l) = \sigma(i\ j)\sigma^{-1}$).

20. Soit $(i, j) \in \{1, \ldots, n\}^2$ tel que $i \neq j$. Montrer que $\mathrm{sgn}((i\ j)) = -1$.

21. Déterminer le cardinal de $\mathfrak{A}_3$. Montrer que $\mathfrak{A}_3$ est un groupe cyclique.

22. On suppose que $n = 4$. Soit G le sous-ensemble

$$\{\mathrm{Id}, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$$

de $\mathfrak{S}_4$.

(a) Montrer que G est un sous-groupe distingué de $\mathfrak{A}_4$.

(b) Montrer que G est isomorphe à $(\mathbb{Z}/2\mathbb{Z})^2$.

(c) Montrer que le groupe quotient $\mathfrak{A}_4/G$ est cyclique.

Dans le reste de cette partie, on suppose que $n \geqslant 5$. Soient V un groupe abélien et $g : \mathfrak{A}_n \to V$ un morphisme de groupes. Soit $\theta : \mathfrak{A}_n \to \mathfrak{A}_n$ l'application qui envoie $\sigma \in \mathfrak{A}_n$ sur $(1\ 2)\sigma(1\ 2)$.

23. Montrer que θ est un automorphisme de groupes.

24. Montrer que, pour tout $(\sigma, \tau) \in \mathfrak{A}_n^2$, on a

$$g(\tau\sigma\tau^{-1}) = g(\sigma).$$

25. Montrer que le groupe $\mathfrak{A}_n$ est engendré par les éléments de la forme $(i\ j)(k\ l)$, où i, j, k, l sont des éléments de $\{1, \ldots, n\}$ tels que $i \neq j$ et $k \neq l$.

26. Montrer que, pour tout $(i, j, k, l) \in \{1, \ldots, n\}^4$ tel que $i \neq j$ et $k \neq l$, il existe $(a, b) \in \{1, \ldots, n\}^2$ tel que $a \neq b$ et que

$$(i\ j)(k\ l) = (a\ b)(i\ j)(k\ l)(a\ b).$$

27. En déduire que $g \circ \theta = g$.

28. Soit $\widetilde{g} : \mathfrak{S}_n \to V$ l'application définie par

$$\widetilde{g}(\sigma) := \begin{cases} g(\sigma), & \sigma \in \mathfrak{A}_n \\ g(\sigma(1\ 2)), & \sigma \in \mathfrak{S}_n \setminus \mathfrak{A}_n. \end{cases}$$

Montrer que $\widetilde{g}$ est un morphisme de groupes.

29. Montrer que, pour tout $(i, j) \in \{1, \ldots, n\}^2$ tel que $i \neq j$, $\widetilde{g}((i\ j))$ est l'élément neutre de V. En déduire que g est le morphisme trivial.

Quatrième partie

Dans cette partie, on étudie la résolubilité par radicaux des équations polynomiales. On suppose que le corps k continent toutes les racines de l'unité dans Ω. En d'autres termes, pour tout $\zeta \in \Omega$, s'il existe un entier

$d \geqslant 1$ tel que $\zeta^d = 1$ (sous cette condition ζ est appelé une *racine $d^{ème}$ de l'unité*), alors $\zeta \in k$. On fixe un vecteur $\lambda = (\lambda_1, \ldots, \lambda_n) \in k^n$ tel que $\Delta_n(\lambda_1, \ldots, \lambda_n) \neq 0$. On peut utiliser sans justification le fait suivant (démontré dans le cours) : pour tout entier $d \geqslant 1$ qui n'est pas divisible par la caractéristique de k, l'ensemble

$$\mu_d(k) = \{\zeta \in k \,:\, \zeta^d = 1\}$$

est un sous-groupe cyclique d'ordre d du groupe multiplicaitve $k^\times$. On suppose que l'extension $k \subset L_\lambda$ admet des corps intermédiaires $F_0, \ldots, F_r$ qui vérifient les conditions suivantes :

(a) $k = F_0 \subset F_1 \subset \ldots \subset F_r = L_\lambda$,

(b) pour tout $i \in \{1, \ldots, r\}$, il existe $y_i \in F_i \setminus \{0\}$ et $m_i \in \mathbb{N}$ non divisible par la caractéristique de k, tels que $y_i^{m_i} \in F_{i-1}$ et $F_i = F_{i-1}(y_i)$.

30. Montrer que, pour tout $i \in \{1, \ldots, r\}$, l'extension $F_{i-1} \subset F_i$ est galoisienne et le groupe de Galois $\mathrm{Gal}(F_i/F_{i-1})$ est cyclique. *Indication : pour montrer le deuxième énoncé on peut étudier l'application de* $\mathrm{Gal}(F_i/F_{i-1})$ *dans* $F_i \setminus \{0\}$ *qui envoie* $\sigma \in \mathrm{Gal}(F_i/F_{i-1})$ *sur* $\sigma(y_i)/y_i$.

31. Montrer que le groupe de Galois $\mathrm{Gal}(L_\lambda/k)$ admet des sous-groupes

$$\mathrm{Gal}(L_\lambda/k) = H_0 \supset H_1 \supset \ldots \supset H_r = \{\mathrm{Id}\}$$

tels que, pour tout $i \in \{1, \ldots, r\}$, H_i soit un sous-groupe distingué de H_{i-1} et le groupe quotient H_{i-1}/H_i soit cyclique.

32. En déduire que $\mathrm{Gal}(L_\lambda/k)$ ne peut pas être $\mathfrak{S}_n$ dès que $n \geqslant 5$.

Soit $d \geqslant 2$ un entier qui n'est pas divisible par la caractéristique de k. Soit k' un sous-corps de Ω contenant k, qui est une extension galoisienne de k. On suppose que le groupe de Galois $\mathrm{Gal}(k'/k)$ est cyclique d'ordre d. Soit σ un générateur du groupe de Galois $\mathrm{Gal}(k'/k)$.

33. On considère k' comme un espace vectoriel de dimension finie sur k et σ comme un endomorphisme k-linéaire de k'.

(a) Montrer que l'endomorphisme σ est diagonalisable.

(b) Montrer que les valeurs propres de σ forment un sous-groupe de $\mu_d(k)$

(c) Montrer que toute racine $d^{\text{ème}}$ de l'unité est une valeur propre de σ.

(d) Montrer que tout sous-espace vectoriel propre de σ est de dimension 1 sur k.

34. Soit ζ un générateur du groupe cyclique $\mu_d(k)$. Soit α un élément non nul de k' tel que $\sigma(y) = \zeta y$.

(a) Montrer que l'orbite de y sous l'action du groupe de Galois $\mathrm{Gal}(k'/k)$ a exactement d éléments.

(b) En déduire que le polynôme minimal de y sur k est de degré d et que $k' = k(y)$.

(c) Montrer que $y^d \in k$. *Indication : On peut considérer le produit des éléments dans l'orbite de y sous l'action du groupe de Galois.*

On suppose que n n'est pas divisible par la caractéristique de k. Soit $a = (a_1, \ldots, a_n)$ un élément de k^n tel que $\Delta_n(a_1, \ldots, a_n) \neq 0$. On suppose que le groupe de Galois $\mathrm{Gal}(L_a/k)$ admet des sous-groupes $G_0, \ldots, G_r$ qui vérifient les conditions suivantes :

(a) $\mathrm{Gal}(L_a/k) = G_0 \supset G_1 \supset \ldots \supset G_r = \{\mathrm{Id}\}$,

(b) pour tout $i \in \{1, \ldots, r\}$, G_i est un sous-groupe distingué de G_{i-1}, et le groupe quotient G_{i-1}/G_i est cyclique, dont l'ordre est noté comme d_i.

35. En utilisant le théorème fondamental de la théorie de Galois, montrer qu'il existe des éléments $z_1, \ldots, z_r$ dans Ω tels que $L_a = k(z_1, \ldots, z_r)$ et que $z_i^{d_i} \in k(z_1, \ldots, z_{i-1})$ pour tout $i \in \{1, \ldots, r\}$, où par convention $k(z_1, \ldots, z_{i-1}) = k$ lorsque $i = 1$.

Cinquième partie

Le but de cette partie est de trouver des formules explicites pour résoudre les polynômes «génériques» de degré $\leqslant 3$ par la théorie de Galois. On suppose dans cette partie que la caractéristique du corps k ne divisible pas 6.

36. Montrer qu'il existe $R_n \in L \setminus K$ tel que $R_n^2 = \Delta_n$. *Indication : on peut utiliser l'extension $K' \subset L'$.*

37. On suppose que $n = 2$. Montrer que $L = K(R_2)$.

38. Exprimer les solutions de l'équation

$$T^2 - A_1 T + A_2$$

en fonction de A_1, A_2 et R_2.

Dans le reste de la partie, on suppose que $n = 3$. Soit ζ un générateur du groupe $\mu_3(k)$.

39. Montrer que l'extension $K(R_3) \subset L$ est galoisienne et que son groupe de Galois est isomorphe à $\mathbb{Z}/3\mathbb{Z}$.

On désigne par σ un générateur de $\mathrm{Gal}(L/K(R_3))$. On considère σ comme un endomorphisme $K(R_3)$-linéaire de L, vu comme un espace vectoriel de dimension 3 sur $K(R_3)$.

40. Montrer que l'ensemble de valeurs propres de σ est $\{1, \zeta, \zeta^2\}$.

On désigne par V_0, V_1 et V_2 les sous-espaces propres de L associés aux valeurs propres 1, ζ et ζ^2 respectivement. Soit x une racine du polynôme

$$T^3 - A_1T^2 + A_2T - A_3.$$

On écrit x sous la forme $u + v + w$, où $u \in V_0$, $v \in V_1$ et $w \in V_2$.

41. Montrer que 1 et x sont linéairement indépendant sur $K(R_3)$.

42. Montrer que $u = A_1/3$.

43. Montrer que $\{v^3, w^3, vw\} \subset K(R_3)$.

44. En déduire que

$$vw = \frac{A_1^2}{9} - \frac{A_2}{3}, \quad v^3 + w^3 = A_3 - \frac{4A_1^3}{27} + \frac{A_1A_2}{3}.$$

Indication : On peut écrire $x^3 - A_1x^2 + A_2x - A_3$ comme une combinaison linéaire de 1 et x à coefficients dans $K(R_3)$.

45. Expliciter les racines du polynôme $T^3 - A_1T^2 + A_2T - A_3$ sous forme de combinaison des additions, multiplications et radicaux des A_1, A_2 et A_3, et des éléments de k.

Fin de l'épreuve