TD

1 Nombres algébriques et transcendants

Exercice 1. Trouver le polynôme minimal de $\sqrt{2}+\sqrt{3}$ dans $\mathbb{Q}[X]$. Plus généralement, soient α, β deux nombres algébriques. Comment chercheriez-vous un polynôme annulateur de $\alpha+\beta$ ou $\alpha\beta$, connaissant des polynômes annulateurs f_α et f_β de α et β respectivement ? (indication : penser à Cayley-Hamilton).

Exercice 2. Identifions $\mathbb{C}$ au plan euclidien $\mathbb{R}^2$. On dit qu'un complexe z est "constructible" si le point sous-jacent de $\mathbb{R}^2$ est "constructible à la règle et au compas" à partir des seuls points 0 de coordonnées $(0,0)$ et 1 de coordonnées $(1,0)$. Montrer que l'ensemble des complexes constructibles est un sous-corps de $\mathbb{C}$ algébrique sur $\mathbb{Q}$.

Exercice 3 (Théorème de Liouville)**.** Le théorème de Liouville montre que les nombres réels algébriques non rationnels sont "mal approximables" par des rationnels, et fournit ainsi une manière simple de construire des nombres transcendants. Soit $\alpha \in \mathbb{R}$ algébrique annulé par un polynôme $f \in \mathbb{Z}[X]$ irréductible de degré $n = \deg(f) > 1$. On veut montrer qu'il existe une constante $A > 0$ telle que pour tout rationnel $\frac{p}{q}$, on a $|\alpha - \frac{p}{q}| > \frac{A}{q^n}$.

a) Montrer que $|f(\frac{p}{q})| \geqslant \frac{1}{q^n}$.

b) Montrer qu'il existe $M > 0$ tel que $|f(\frac{p}{q})| < M.|\alpha - \frac{p}{q}|$ pour $\frac{p}{q}$ dans un voisinage de α, et conclure.

c) Construire des nombres transcendants.

Exercice 4. Soit k un corps et $K = k(X)$.

a) Montrer que K n'est pas de type fini en tant que k-algèbre.

b) Soit $F \in K \backslash k$. On écrit $F = \frac{P(X)}{Q(X)}$, avec $P, Q \in k[X]$ premiers entre eux.

   i) Montrer que X est algébrique sur $k(F)$ (on pourra considérer $R(T) := P(T) - FQ(T) \in k(F)[T]$).

   ii) En déduire que F est transcendant sur k.

   iii) Montrer que $[K : k(F)] = \max(\deg(P), \deg(Q))$ (on pourra montrer que $R(T)$ est irréductible dans $k[F][T]$).

c) Soit $\phi : \mathrm{GL}_2(k) \to \mathrm{Aut}_k(K)$ le morphisme de groupe défini par

$$\phi\begin{pmatrix} a & b \\ c & d \end{pmatrix}(R) = R\left(\frac{aX+b}{cX+d}\right).$$

Montrer que ϕ est surjectif, et que $\mathrm{Ker}(\phi) = k^\times$.

Exercice 5. Soit $f \in \mathbb{C}[T]$ unitaire de degré 3, de racines $z_1, z_2, z_3 \in \mathbb{C}$.

a) Montrer que $K = K_{z_1,z_2,z_3} := \mathbb{C}(X)[T]/(X^2 - f(T))$ est un corps de degré de transcendance 1 sur $\mathbb{C}$. Calculer $[K : \mathbb{C}(X)]$ et $[K : \mathbb{C}(T)]$.

b) Si $z_1 = z_2$, montrer que K est transcendant pur engendré par $\frac{X}{T-z_1}$.

c) Supposons les z_i distincts deux à deux. Montrer qu'il existe $\lambda \in \mathbb{C} \setminus \{0,1\}$ tel que $K_{z_1,z_2,z_3} \simeq K_{0,1,\lambda}$.

d) Montrer que $K_{0,1,\lambda}$ n'est pas transcendant pur, si $\lambda \neq 0, 1$.

Exercice 6. Soit p un nombre premier, et notons $K := \mathbb{F}_p(X,Y)$.

a) Montrer que $K^p := \{x^p, x \in K\}$ est un sous corps de K et que $[K : K^p] = p^2$.

b) Montrer que pour tout $x \in K$, le degré du polynôme minimal de x sur K^p est inférieur à p. En déduire que l'extension $K^p \subset K$ n'est pas monogène.

2 Autour du Nullstellensatz

Exercice 7. Polynômes vs fonctions polynomiales. Soit k un corps. Pour tout entier n on peut associer à un polynôme $f \in k[X_1, \cdots, X_n]$ une fonction $k^n \longrightarrow k$, $(x_1, \cdots, x_n) \mapsto f(x_1, \cdots, x_n)$.

a) Vérifier qu'on obtient ainsi un morphisme de k-algèbres de $k[X_1, \cdots, X_n]$ dans la k-algèbre des fonctions de k^n dans k.

b) Montrer que ce morphisme est injectif si et seulement si k est infini.

Exercice 8. Soient $f_1, \cdots f_m \in \mathbb{C}[X_1, \cdots, X_n]$. On suppose que le lieu $V = V_{f_1, \cdots, f_m} \subset \mathbb{C}^n$ des zéros de ces polynômes est non vide. On dit qu'une fonction $V \longrightarrow \mathbb{C}$ est *polynômiale* si c'est la restriction à V d'une fonction polynômiale sur $\mathbb{C}^n$ (donc donnée par évaluation d'un polynôme $g \in \mathbb{C}[X_1, \cdots, X_n]$). Notons $\mathcal{O}(V)$ la $\mathbb{C}$-algèbre des fonctions polynômiales sur V.

a) Montrer que $\mathcal{O}(V) \simeq \mathbb{C}[X_1, \cdots, X_n]/\sqrt{I}$.

b) Soit $V' \subset \mathbb{C}^{n'}$ un autre ensemble algébrique. On dit qu'une application $V \longrightarrow V'$ est polynômiale si elle est restriction d'une application $\mathbb{C}^n \longrightarrow \mathbb{C}^{n'}$ polynômiale. Montrer que $\{\text{App. Pol. } V \longrightarrow V'\} \simeq \mathrm{Hom}_{\mathbb{C}-\mathrm{alg}}(\mathcal{O}(V'), \mathcal{O}(V))$.

3 Quelques polynômes irréductibles

Exercice 9. Soit $n \in \mathbb{N}^*$. Soit $\Phi_n = \prod_{k \in (\mathbb{Z}/n\mathbb{Z})^\times} (X - e^{2i\pi k/n}) \in \mathbb{C}[X]$.

a) Montrer que $X^n - 1 = \prod_{d|n} \Phi_d$. En déduire que $\Phi_n \in \mathbb{Z}[X]$.

b) Soit ζ une racine primitive n^{e}de 1 et p un nombre premier premier à n. Soit f et g les polynômes minimaux unitaire sur $\mathbb{Q}$ de ζ et $\zeta' = \zeta^p$. On suppose $f \neq g$. Montrer que $fg|\Phi_n$ et $f|g(X^p)$.

c) Montrer que l'image de Φ_n dans $\mathbb{F}_p[X]$ a un facteur irréductible ayant multiplicité au moins deux, et en déduire une contradiction.

d) En déduire que Φ_n est un polynôme irréductible dans $\mathbb{Q}[X]$.

Exercice 10. Soit p un nombre premier et $a \in \mathbb{F}_p$. Soit $P = X^p - X - a \in \mathbb{F}_p[X]$.

a) Si $a = 0$, donner la décomposition en facteur irréductible de P. On suppose dorénavant $a \neq 0$.

b) Montrer que $P(X + 1) = P(X)$.

c) Soit Q un facteur irréductible de P. Montrer que $Q(X + 1)$ est aussi un facteur irréductible de P.

d) Montrer que $Q(X + 1) = Q(X)$ (on pourra considérer une action de $\mathbb{Z}/p\mathbb{Z}$ sur l'ensemble des facteurs irréductibles de P).

e) Montrer que si $R \in \mathbb{F}_p[X]$ est de degré $\leqslant p - 1$ et $R(X + 1) = R(X)$, alors R est un polynôme constant.

f) En déduire que P est irréductible.

g) Soit $b \in \mathbb{Z}$ premier à p. Montrer que $X^p - X - b$ est un polynôme irréductible de $\mathbb{Q}[X]$.

4 Polynômes symétriques

Exercice 11. On fait agir le groupe symétrique $\mathfrak{S}_n$ sur l'anneau $A = \mathbb{Z}[X_1, \cdots, X_n]$ par permutation des indéterminées en posant $\sigma(X_i) := X_{\sigma^{-1}(i)}$ pour tout $\sigma \in \mathfrak{S}_n$.

a) Notons $\Sigma_1, \cdots, \Sigma_n \in A$ les éléments déterminés par l'égalité suivante dans $A[T]$:

$$(T - X_1)(T - X_2) \cdots (T - X_n) = T^n - \Sigma_1 T^{n-1} + \Sigma_2 T^{n-2} + \cdots + (-1)^n \Sigma_n$$

Pour chaque i, calculer Σ_i et montrer qu'il est "symétrique", i.e. invariant par l'action de $\mathfrak{S}_n$.

On veut montrer que l'anneau $A^{\mathfrak{S}_n}$ des polynômes symétriques est un anneau de polynômes en les Σ_i, au sens où l'unique morphisme d'anneaux $\mathbb{Z}[Y_1, \cdots, Y_n] \longrightarrow A^{\mathfrak{S}_n}$ qui envoie Y_i sur Σ_i est un isomorphisme d'anneaux.

b) Soit B un anneau muni d'une $\mathbb{Z}$-base $(e_\lambda)_{\lambda \in \Lambda}$, où $(\Lambda, \preccurlyeq)$ est un monoïde commutatif ordonné tel que $\forall \lambda \in \Lambda, \{\mu \preccurlyeq \lambda\}$ est fini, et telle que pour tous $\lambda, \lambda' \in \Lambda$ on a

$$e_\lambda e_{\lambda'} \in e_{\lambda+\lambda'} + \sum_{\mu \prec \lambda+\lambda'} \mathbb{Z} e_\mu.$$

Supposons de plus que Λ est librement engendré par n éléments $\mu_1, \cdots, \mu_n$. Montrer que B est un anneau de polynômes en les $e_{\mu_1}, \cdots, e_{\mu_n}$.

c) Soit $\Lambda := \{\nu \in \mathbb{N}^n, \nu_1 \geqslant \cdots \geqslant \nu_n\}$. Pour $\lambda \in \Lambda$, on pose $S^\lambda := \sum_{\nu \in o(\lambda)} X^\nu$ où $X^\nu := X_1^{\nu_1} \cdots X_n^{\nu_n}$ et $o(\lambda)$ désigne la $\mathfrak{S}_n$-orbite de λ dans $\mathbb{N}^n$.

   i) Calculer S^{μ_j} pour $\mu_j = (1, \cdots, 1, 0, \cdots 0)$ avec j termes 1 et $n-j$ termes 0.

   ii) Montrer que les S^λ, $\lambda \in \Lambda$, forment une base de $A^{\mathfrak{S}_n}$.

d) Pour $\nu \in \mathbb{N}^n$, posons $|\nu| = \sum_i \nu_i$ et écrivons $\nu \preccurlyeq \nu'$ si $(|\nu|, \nu_1, \cdots, \nu_n) \leqslant (|\nu'|, \nu'_1, \cdots, \nu'_n)$ pour l'ordre lexicographique.

   i) Montrer que $\preccurlyeq$ est une relation d'ordre sur $\mathbb{N}^n$ compatible à l'addition et t.q. $\forall \lambda \in \Lambda, \{\mu \in \Lambda, \mu \preccurlyeq \lambda\}$ est fini.

   ii) Montrer que pour $\lambda, \lambda' \in \Lambda$, on a $S^\lambda S^{\lambda'} \in S^{\lambda+\lambda'} + \sum_{\mu \prec \lambda+\lambda'} \mathbb{Z}.S^\mu$.

e) Conclure.

f) Application : discriminant.

   i) Montrer qu'il existe un unique polynôme $\Delta_n \in \mathbb{Z}[Y_1, \cdots, Y_n]$ tel que $\prod_{i<j}(X_i - X_j)^2 = \Delta_n(\Sigma_1, \cdots, \Sigma_n)$.

   ii) Calculer Δ_2. Montrer que Δ_3 est de la forme $\Sigma_1^2\Sigma_2^2 - 4\Sigma_2^3 + 27\Sigma_3^2 + a\Sigma_1^3\Sigma_3 + b\Sigma_1\Sigma_2\Sigma_3$.

   iii) Soit k un corps et $f = X^n + a_1X^{n-1} + \cdots + a_nX^0$. Montrer que f est séparable si et seulement si $\Delta_n(-a_1, a_2, \cdots, (-1)^n a_n) \neq 0$.

   iv) Soit $f \in \mathbb{Z}[X]$ unitaire. Montrer que l'ensemble des nombres premiers p tel que $\bar{f} \in \mathbb{F}_p[X]$ est non séparable est fini.

5 Extensions normales

Exercice 12. Montrer qu'une extension $k \subset K$ de degré 2 est toujours normale. Est-ce vrai pour une extension de degré 3 ?

Exercice 13. On considère l'extension $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ de $k = \mathbb{Q}$.

a) Montrer qu'elle est normale de degré 4.

b) Soit $\alpha := \sqrt{2} + \sqrt{3}$. Calculer les conjugués de α dans K. Montrer que $K = \mathbb{Q}(\alpha)$.

Exercice 14. Soit k de caractéristique nulle, $f \in k[X]$ irréductible, et $\alpha, \beta \in \bar{k}$ deux racines distinctes de f dans une clôture algébrique de k.

a) Montrer que $\alpha - \beta \notin k$.

b) Montrer que si $\alpha\beta^{-1} \in k$ alors c'est une racine de l'unité.

6 Inséparabilité

Exercice 15. Soient k un corps , $F = X^3 - 3X - 1 \in k[X]$ et α une racine de F dans une clôture algébrique de k. Montrer que $k(\alpha)$ est une extension séparable de K.

Exercice 16. Soit k un corps et $f \in k[X]$ irréductible.

a) Montrer que f séparable $\Leftrightarrow f' = 0$.

b) Supposons f inséparable.

   i) Montrer que k est de caractéristique $p > 0$.

   ii) Montrer qu'il existe un unique polynôme irréductible *séparable* $g \in k[X]$ et un unique entier r tel que $f(X) = g(X^{p^r})$.

   iii) Montrer que les coefficients de k ne sont pas tous dans l'image du Frobenius φ_k.

Exercice 17. Soit k un corps de caractéristique $p > 0$. Montrer que les assertions suivantes sont équivalentes :

a) tout $f \in k[X]$ irréductible est séparable.

b) toute extension $k \subset K$ est séparable.

c) L'endomorphisme de Frobenius φ_k est surjectif (et donc bijectif).

Sous ces conditions, on dit que k est un corps *parfait.*

Exercice 18. Soit $k \subset K$ une extension algébrique de corps de caractéristique $p > 0$. On dit qu'un élément $\alpha \in K$ est *purement inséparable* sur k si son polynôme minimal est de la forme $X^{p^r} - x$ pour un $x \in k$.

a) Montrer que l'ensemble K_{sep} des éléments de K *séparables* sur k est une sous-extension $k \subset K_{\text{sep}} \subset K$.

b) Montrer que l'extension $K_{\text{sep}} \subset K$ est purement inséparable, au sens où tous ses éléments le sont.

Exercice 19. Un corps k est dit séparablement clos si tout polynôme irréductible séparable de $k[X]$ est scindé. On appelle clôture séparable (absolue) d'un corps k toute extension algébrique séparable et séparablement close de k. Montrer que tout corps k admet une clôture séparable, que celle-ci est unique à isomorphisme près, et que toute extension séparable s'y plonge.

Exercice 20. Soient K un corps de caractéristique un nombre premier p et L une extension finie de K de degré non divisible par p. Montrer que L est séparable sur K.

7 Extensions Galoisiennes

Exercice 21. Montrer que les extensions suivantes de $\mathbb{Q}$ sont Galoisiennes et calculer leur groupe de Galois : $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{2}, \sqrt{3})$, $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$.

Exercice 22. Soit $f = X^4 - 2 \in \mathbb{Q}[X]$ et K le corps de décomposition de f. Décrire le groupe de Galois $G = \mathrm{Gal}(K/\mathbb{Q})$ de f et toutes les extensions intermédiaires K' telles que $\mathbb{Q} \subset K' \subset K$.

Exercice 23. Soient $f = X^4 + aX^2 + b \in \mathbb{Q}[X]$ un polynôme irréductible, K le corps de décomposition de f et $G = \mathrm{Gal}(K/\mathbb{Q})$. On note $\pm\alpha, \pm\beta$ les racines de f.

a) Montrer que G est isomorphe à un sous-groupe du groupe diédral D_4 d'ordre 8.

b) Montrer que $G \simeq \mathbb{Z}/4\mathbb{Z}$ si et seulement si $(\alpha/\beta - \beta/\alpha) \in \mathbb{Q}$.

c) Montrer que $G \simeq (\mathbb{Z}/2\mathbb{Z})^2$ si et seulement si $\alpha\beta \in \mathbb{Q}$ ou $\alpha^2 - \beta^2 \in \mathbb{Q}$.

d) Montrer que sinon G est isomorphe à D_4.

e) Déterminer le groupe de Galois de $X^4 - 4X^2 - 1$.

Exercice 24. Soit $f = X^n - a \in \mathbb{Q}[X]$. Notons $K_f \subset \overline{\mathbb{Q}}$ son sous-corps de décomposition et G_f son groupe de Galois.

a) Montrer qu'il existe un morphisme surjectif $G_f \twoheadrightarrow (\mathbb{Z}/n\mathbb{Z})^\times$ dont le noyau est un groupe cyclique μ_m pour $m|n$.

b) Construire un morphisme injectif $\psi : G_f \hookrightarrow \mu_n \rtimes (\mathbb{Z}/n\mathbb{Z})^\times$.

c) Montrer que ψ est un isomorphisme si et seulement si $X^n - a$ est irréductible dans $\mathbb{Q}(\mu_n)[X]$. Montrer que c'est le cas en particulier si $X^n - a$ est irréductible dans $\mathbb{Q}[X]$ et $(n, \varphi(n)) = 1$.

d) Si $\Phi_n(X)$ est irréductible dans $\mathbb{Q}(\sqrt[n]{a})[X]$, montrer que $\psi(G_f)$ est de la forme $\mu_m \rtimes (\mathbb{Z}/n\mathbb{Z})^\times$.

e) Considérons le cas $n = 6$ et $a = -3$. Montrer que $\psi(G_f)$ est le sous-groupe de $\mu_6 \rtimes (\mathbb{Z}/6\mathbb{Z})^\times$ engendré par $(j, 1)$ et $(-1, -1)$. En particulier, $G_f \simeq \mathfrak{S}_3$ mais n'est pas un "sous-produit semi-direct" de $\mu_6 \rtimes (\mathbb{Z}/6\mathbb{Z})^\times$.

Exercice 25. Soit k un corps et L une extension de k. Soient K_1 et K_2 deux sous-corps de L contenant k de dimensions finies sur k. On note K_1K_2 le sous-corps de K engendré par K_1 et K_2.

a) Montrer que $[K_1K_2 : k] \leqslant [K_1 : k][K_2 : k]$, et qu'en cas d'égalité, $k = K_1 \cap K_2$.

b) On suppose dorénavant K_1/k galoisienne. Montrer que K_1K_2/K_2 est galoisienne et construire un isomorphisme $\mathrm{Gal}(K_1K_2/K_2) \xrightarrow{\sim} \mathrm{Gal}(K_1/K_1 \cap K_2)$.

c) Montrer que $[K_1K_2 : k] = [K_1 : k][K_2 : k]/[K_1 \cap K_2 : k]$.

d) On suppose dorénavant que K_2/k est également galoisienne. Montrer que K_1K_2 et $K_1 \cap K_2$ sont des extensions galoisiennes de k.

e) Construire un morphisme injectif $\phi : \mathrm{Gal}(K_1K_2/k) \to \mathrm{Gal}(K_1/k) \times \mathrm{Gal}(K_2/k)$

f) Montrer que l'image de ϕ est $\{(g_1, g_2) \in \mathrm{Gal}(K_1/k) \times \mathrm{Gal}(K_2/k), \pi_1(g_1) = \pi_2(g_2)\}$, où ! $\pi_i : \mathrm{Gal}(K_i/k) \to \mathrm{Gal}(K_1 \cap K_2/k)$ est la surjection canonique.

g) Soit $\mathbb{Q}^{\text{ab}}$ l'ensemble des nombres algébriques x contenus dans une extension galoisienne L de $\mathbb{Q}$ telle $\mathrm{Gal}(L/\mathbb{Q})$ soit commutatif. Montrer que $\mathbb{Q}^{\text{ab}}$ est un corps. Est-ce une extension finie de $\mathbb{Q}$?

Exercice 26. Soit $f \in k[X]$ de la forme $f = X^n + aX + b$. Montrer que

$$\mathrm{disc}(f) = (-1)^{n(n-1)/2} \left((1-n)^{n-1}a^n + n^n b^{n-1}\right).$$

Exercice 27. Soit $f = X^5 + 20X - 16 \in \mathbb{Q}[X]$.

a) Montrer que f est irréductible et que G_f contient un 5-cycle.

b) En réduisant modulo 7, montrer que G_f contient un 3-cycle.

c) Montrer que la conjugaison complexe induit un élément non-trivial de G_f. En conclure que $|G_f|$ est divisible par 30.

d) Montrer que G_f est contenu dans $\mathfrak{A}_5$.

e) Après avoir montré que tout sous-groupe d'indice 2 d'un groupe fini est distingué, en conclure que $G_f = \mathfrak{A}_5$.

Exercice 28. Soit f le polynôme $X^4 + 8X + 12 \in \mathbb{Q}[X]$ et soit K_f le corps de décomposition de f dans $\overline{\mathbb{Q}}$.

a) Montrer que f est irréductible sur $\mathbb{Q}$.

b) Montrer que $G_f = \mathrm{Gal}(K_f/\mathbb{Q})$ est isomorphe à $\mathfrak{A}_4$.

c) Montrer qu'il n'existe pas d'extension quadratique de $\mathbb{Q}$ contenue dans K_f.

Exercice 29. Le but est d'exhiber une extension Galoisienne de $\mathbb{Q}$ de groupe $H_8 = \{\pm 1, \pm i, \pm j, \pm k\}$.

a) Soit $a := (2 + \sqrt{2})(3 + \sqrt{6})$. Montrer que $\mathbb{Q}(a) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, et que pour tout $\sigma \in \mathrm{Gal}(\mathbb{Q}(a)/\mathbb{Q})$, on a $\sigma(a)/a \in (\mathbb{Q}(a)^\times)^2$. Montrer aussi que a n'est pas un carré dans $\mathbb{Q}(a)$.

b) Soit d une racine carrée de a dans $\overline{\mathbb{Q}}$. Montrer que $\mathbb{Q}(d)$ est Galoisienne sur $\mathbb{Q}$, et que $\mathrm{Gal}(\mathbb{Q}(d)/\mathbb{Q}(a))$ est central dans $\mathrm{Gal}(\mathbb{Q}(d)/\mathbb{Q})$.

c) Montrer que $\mathrm{Gal}(\mathbb{Q}(d)/\mathbb{Q})$ est isomorphe à H_8.