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).

Solution. Dans le cas concret proposé, on peut calculer les puissances de $\gamma := \sqrt{2}+\sqrt{3}$ et chercher une relation de dépendance linéaire. On a $\gamma^2 = 5+2\sqrt{6}$ et $\gamma^4 = 49+20\sqrt{6}$ d'où $\gamma^4 - 10\gamma^2 + 1 = 0$. Pour voir que c'est le polynôme minimal f_γ, on peut utiliser le fait que $[\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}(\sqrt{3})][\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 4$, donc $\deg f_\gamma$ vaut 2 ou 4. Mais le polynôme minimal de γ sur $\mathbb{Q}(\sqrt{3})$ est $(X+\sqrt{3})^2 - 2$. Ce polynôme doit diviser f_γ et, puisqu'il n'est pas dans $\mathbb{Q}[X]$, le degré de f_γ est 4.
En général, il peut être délicat de trouver un polynôme annulateur de $\alpha+\beta$ par calculs un peu "au hasard". Voici une manière, pas toujours efficace mais implémentable, d'en trouver un. L'idée est que, pour une extension de corps finie $k \subset K$, on a un morphisme de k-algèbres

$$K \longrightarrow \mathrm{End}_{k-ev}(K),\ x \mapsto m_x$$

où $m_x : K \longrightarrow K, y \mapsto xy$ est l'endomorphisme k-linéaire de K donné par multiplication par x. Puisque c'est un morphisme de k-algèbres, on a en particulier $m_x = 0 \Leftrightarrow x = 0$, et $m_{f(x)} = f(m_x)$ pour tout polynôme $f \in k[X]$ (ici $f(m_x)$ est un endomorphisme obtenu en évaluant le polynôme f en l'endomorphisme m_x). En particulier, tout polynôme annulateur de m_x annule aussi x. Or, le théorème de Cayley-Hamilton nous dit qu'un endomorphisme est annulé par son polynôme caractéristique, que l'on peut calculer par un beau déterminant. Mais pour calculer, il faut bien-sûr choisir une base.
Par exemple, dans l'exemple où $k = \mathbb{Q}$ et $K = \mathbb{Q}(\sqrt{2},\sqrt{3})$, on peut prendre la base $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$. La matrice de la multiplication par $\sqrt{2}+\sqrt{3}$ est assez facile à calculer (celle de $m_{\sqrt{2}}$ est diagonale par blocs, chaque bloc étant la matrice compagnon de X^2-2, et celle de $m_{\sqrt{3}}$ est formées de blocs diagonaux $a_{ij}I_2$ où (a_{ij}) est la matrice compagnon de X^2-3). Si on calcule le polynôme caractéristique de cette matrice on retrouve $X^4 - 10X^2 + 1$.
Pour α, β généraux, il est encore vrai que $\mathbb{Q}(\alpha,\beta)$ est engendré $\mathbb{Q}$-linéairement par les $\alpha^i\beta^j$ avec $1 \leqslant i \leqslant \deg f_\alpha$ et $1 \leqslant j \leqslant \deg f_\beta$. Même si ce n'est pas toujours une base, on peut quand-même former la "matrice" de m_α (diagonale par blocs égaux à la matrice compagnon de f_α) et la "matrice" de m_β (formée de blocs carrés scalaires de taille $\deg f_\alpha$ (ie de la forme $a_{ij}I_{\deg f_\alpha}$) où (a_{ij}) est la matrice compagnon de f_β). Alors le polynôme caractéristique de la somme $m_\alpha + m_\beta$ est toujours un polynôme annulateur de $\alpha+\beta$.

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 $\mathbb{Q}$.

Solution. L'addition ne pose pas de problème : on complète le parallélogramme (2 coups de compas). Pour la multiplication, on a deux sous-problèmes : construire la somme de deux angles, et construire le produit de deux longueurs. Pour la somme de deux angles, il suffit de reporter un des angles en construisant un triangle semblable (3 coups de compas). Pour le produit des longueurs, on utilise de théorème de Thalès : sur la droite réelle, on a 1 et on peut reporter z_1 pour obtenir le point $|z_1|$, et sur la droite imaginaire, on peut reporter z_2 pour obtenir le point $i|z_2|$. Alors, la parallèle à la droite $(i|z_2| : 1)$ passant par $|z_1|$ coupe la droite imaginaire en $i|z_1z_2|$. On procède de même pour la construction de l'inverse.
Les complexes constructibles forment donc un corps, qui est visiblement stable par conjugaison complexe. Pour montrer qu'ils sont algébriques, on remarque qu'ils sont inductivement obtenus comme intersection de cercles/droites avec cercles/droites fabriqués avec des points précédemment construits. Or, l'équation du cercle de centre α et passant par β est $(z-\alpha)(\bar{z}-\bar{\alpha}) = |\alpha-\beta|^2$ tandis que celle de la droite (réelle) passant par γ et δ est $(\bar{\delta}-\bar{\gamma})z + (\gamma-\delta)\bar{z} = \gamma\bar{\delta} - \bar{\gamma}\delta$. En éliminant $\bar{z}$ pour calculer leur intersection, on voit que z est annulé

par un polynôme de degré 2 à coefficients dans $\mathbb{Q}(\alpha, \bar{\alpha}, \beta, \bar{\beta}, \gamma, \bar{\gamma}, \delta, \bar{\delta})$. Donc, si $\alpha, \beta, \gamma, \delta$ sont algébriques alors les points d'intersections aussi. De même pour l'intersection de deux cercles ou deux droites. En fait, on voit même de cette manière que les nombres constructibles sont de degré une puissance de 2.

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.

Solution. a) Puisque f est irréductible de degré > 1, il n'a pas de racine rationnelle, donc $f(\frac{p}{q}) \neq 0$. Comme les coefficients de f sont entiers, on a $q^n f(\frac{p}{q}) \in \mathbb{Z}$. Puisqu'un entier non nul a valeur absolue $\geqslant 1$, on en déduit $|f(\frac{p}{q})| \geqslant \frac{1}{q^n}$.

b) L'inégalité des accroissements finis nous fournit M, après avoir fixé un voisinage borné I de α. Avec (a), on obtient donc $|\alpha - \frac{p}{q}| > \frac{A}{q^n}$ pour tout $\frac{p}{q} \in I$, avec par exemple $A = \frac{1}{2M}$.

c) Les réels s'obtiennent en général comme limites de suites de Cauchy de rationnels. Supposons par exemple $\alpha = \lim_{n\to\infty} \frac{p_n}{q_n}$ avec $|\alpha - \frac{p_n}{q_n}| \leqslant \frac{1}{(q_n)^n}$ et $q_n \geqslant 2$ pour tout n. Alors, pour $m \geqslant n$, on obtient $|\alpha - \frac{p_m}{q_m}| \leqslant \frac{1}{(q_m)^{m-n}} \frac{1}{(q_m)^n} \leqslant \frac{1}{2^{m-n}} \frac{1}{(q_m)^n}$. On voit donc que α ne peut être algébrique de degré n d'après le théorème de Liouville, et ceci étant valable pour tout n, α est transcendant. Pour un exemple de telle suite, on peut prendre $\frac{p_n}{q_n} = \sum_{k=0}^{n} 10^{-k!}$.

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 $\mathrm{Ker}(\phi) = k^\times$.

Solution. a) C'est du cours. Soit $F_i = \frac{P_i}{Q_i}$, $i = 1, \cdots, n$ des fractions rationnelles. Alors pour toute $F \in k[F_1, \cdots, F_n]$, le dénominateur de F divise une puissance de $Q_1 \cdots Q_n$. En d'autres termes, on a $k[F_1, \cdots, F_n] \subset S^{-1}k[X]$ où S est la partie multiplicative engendrée par les Q_i. Mais alors, $Q := \prod_i Q_i + 1 \notin S$, donc $F := \frac{1}{Q} \notin k[F_1, \cdots, F_n]$. Il s'ensuit que K n'est pas de type fini en tant que k-algèbre.

b) i) Evaluons $R \in k(F)[T] \subset k(X)[T]$ en X : on a $R(X) = P(X) - F(X)Q(X) = 0$, donc R est un polynôme annulateur non nul de X dans $k(F)[T]$, donc X est algébrique sur $k(F)$. De plus, $[k(X) : k(F)] \leqslant deg(R) = max(deg(P), deg(Q))$.

ii) Si F est algébrique sur k, $[k(F) : k]$ est fini. Or $[k(X) : k(F)]$ est fini donc par transitivité des degrés, $[k(X) : k]$ est fini, ce qui est absurde.

iii) On a déjà l'inégalité $[k(X) : k(F)] \leqslant deg(R) = max(deg(P), deg(Q))$. Pour avoir l'égalité, il suffit de démontrer que $R \in k(F)[T]$ est le polynôme minimal de X, ou de manière équivalente, que R est irréductible dans $k(F)[T]$. Comme F est transcendant sur k, $k[F]$ est un anneau de polynômes à une variable (en l'occurrence F) sur k, c'est donc un anneau principal, et a fortiori factoriel. Il suffit alors de montrer que R est un élément irréductible de $k[F][T] = k[T][F]$. Or vu comme polynôme en F à coefficient dans $k[T]$, R est de degré 1 en F, donc est irréductible dans $k(T)[F]$. De plus, $pgcd(P, Q) = 1$, donc R est primitif en tant que pôlynôme de $k[T][F]$, donc R est irréductible dans $k[T][F]$ donc aussi dans $k(F)[T]$. D'où le résultat.

c) Soit $\varphi \in \mathrm{Aut}_k(K)$, et $F = \varphi(X)$. Alors si $R(X) = \frac{P(X)}{Q(X)}$, on a $\varphi(R) = R(F)$. Il suffit donc de montrer que F est de la forme $\frac{aX+b}{cX+d}$. Ecrivons $F = \frac{P}{Q}$ avec P et Q premiers entre eux. Comme $k(F)$ est l'image de φ, par bijectivité de φ, on doit avoir $k(F) = K$. D'après a)iii),on a donc $max(deg(P), deg(Q)) = 1$, donc P est de la forme $aX + b$ et Q de la forme $cX + d$. Comme F n'est pas une fraction rationnelle constante, (a, b) et (c, d) ne sont pas colinéaires, et la matrice de l'énoncé est bien dans $\mathrm{GL}_2(k)$.

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.

Solution. a) K^p est l'image de l'endomorphisme de Frobenius $x \mapsto x^p$, qui est un endomorphisme de $\mathbb{F}_p$-algèbres. Donc c'est un sous-corps de K. On a $K^p = \mathbb{F}_p(X^p, Y^p)$ et on voit que les X^iY^j avec $0 \leqslant i, j < p$ forment une base de K sur K^p. D'où $[K : K^p] = p^2$.

b) Le polynôme minimal $f_x(T)$ de x sur K^p divise $T^p - x^p$. L'extension de K^p engendrée par K est donc de degré $\leqslant p$.

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 $\mathbb{Q}[X]$.

Solution. a) Partons de $X^n-1=\prod_{k\in\mathbb{Z}/n\mathbb{Z}}(X-e^{2i\pi k/n})$ et regroupons les k selon leur pgcd avec n. Pour δ un diviseur de n, et en posant $d:=n/\delta$, on a $\prod_{k\in\mathbb{Z}/n\mathbb{Z},(k,n)=\delta}(X-e^{2i\pi k/n})=\prod_{k'\in(\mathbb{Z}/d\mathbb{Z})^\times}(X-e^{2i\pi k'/d})=\Phi_d(X)$. On en déduit la formule $X^n-1=\prod_{d|n}\Phi_d(X)$. On montre alors par récurrence forte sur n que $\Phi_n(X)\in\mathbb{Z}[X]$. Le cas $n=1$ est clair puisque $\Phi_1(X)=X-1$. Supposons que $\Phi_d(X)\in\mathbb{Z}[X]$ pour $d<n$. En particulier $\Phi_d(X)\in\mathbb{Q}[X]$, donc $\Phi_n(X)\in\mathbb{Q}(X)\cap\mathbb{C}[X]=\mathbb{Q}[X]$. Comme Φ_d est unitaire, son contenu vaut 1. Mais alors, la factorisation $X^n-1=\Phi_n(X)\cdot\prod_{d||n}\Phi_d(X)$ dans $\mathbb{Q}[X]$ montre que le contenu de Φ_n est 1. En particulier il est dans $\mathbb{Z}[X]$.

b) Puisque ζ est une racine *primitive*, on a $\Phi_n(\zeta)=0$ donc f divise Φ_n. De même, ζ^p est primitive car $(p,n)=1$, donc g divise Φ_n. Par ailleurs, f et g sont irréductibles et unitaires, donc s'ils sont distincts, ils sont premiers entre eux. Par le lemme d'Euclide (ou de Gauss ?), il s'ensuit que $fg|\Phi_n$. Enfin, ζ est racine de $g(X^p)$ qui est dans $\mathbb{Q}[X]$, donc $f|g(X^p)$.

c) Montrons d'abord que $f\in\mathbb{Z}[X]$. En effet, écrivons $\Phi_n=fh$ avec $h\in\mathbb{Q}[X]$. Puisque f est unitaire, h l'est aussi. Leurs contenus respectifs sont donc des inverses d'entiers, i.e. $c(f)=\frac{1}{a_f}$ et $c(h)=\frac{1}{a_h}$ avec $a_f,a_h\in\mathbb{N}^*$. Mais alors l'égalité $1=c(\Phi_n)=c(f)c(h)$ implique $c(f)=c(h)=1$ et donc $f\in\mathbb{Z}[X]$. De même on a $g\in\mathbb{Z}[X]$.
Notons maintenant $\bar\Phi_n$ l'image de f dans $\mathbb{F}_p[X]$. On a donc $\bar f\bar g|\bar\Phi_n$ et $\bar f|\bar g(X^p)=(\bar g)^p$. Soit alors $h\in\mathbb{F}_p[X]$ un facteur irréductible de $\bar f$. On $h|\bar g^p$ donc $h|\bar g$ par le lemme d'Euclide (ou de Gauss ?), et finalement $h^2|\bar f\bar g|\bar\Phi_n$. Cela implique que $\bar\Phi_n$ a une racine double dans une clôture algébrique $\overline{\mathbb{F}}_p$ de $\mathbb{F}_p$ et donc il en est de même pour X^n-1. Il s'ensuit que X^n-1 et son polynôme dérivé nX^{n-1} devraient avoir une racine commune, ce qui est absurde car $n\neq 0$ dans $\mathbb{F}_p$.

d) Soit f le polynôme minimal de $e^{\frac{2i\pi}{n}}$. On a montré que l'ensemble des racines de f est stable par l'application $\zeta\mapsto\zeta^p$, pour tout premier p premier à n. Il est donc stable par l'application $\zeta\mapsto\zeta^m$ pour tout k premier à n. En particulier, il contient tous les $e^{\frac{2ik\pi}{n}}$ pour $k\in(\mathbb{Z}/n\mathbb{Z})^\times$. Il s'ensuit que $f=\Phi_n$.

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 $\mathbb{Q}[X]$.

Solution. a) On a $X^p-X=\prod_{a\in\mathbb{F}_p}(X-a)$.

b) clair

c) $P(X)=Q(X)R(X)\Rightarrow P(X)=P(X+1)=Q(X+1)R(X+1)$ donc $Q(X+1)$ divise P. Par ailleurs $Q(X+1)$ est irréductible.

d) Considérons l'action de $\mathbb{Z}/p\mathbb{Z}$ sur $\mathbb{F}_p[X]$ donnée par $(a\cdot P)(X):=P(X+a)$. Ses orbites sont de cardinal 1 ou p. De plus, l'orbite d'un polynôme irréductible est formée de polynômes irréductibles deux à deux premiers entre eux (puisque distincts et de même terme dominant). Donc, si $Q(X)\neq Q(X+1)$, tous les $Q(X+a)$ sont distincts et divisent P. Comme $\deg P=p$, cela implique $\deg Q=1$, ce qui n'est pas possible puisque P n'a pas de racine dans $\mathbb{F}_p$.

e) Soit α une racine de R dans $\overline{\mathbb{F}}_p$. Si $R(X)=R(X+1)$ alors $\alpha+a$ est une racine de R pour tout $a\in\mathbb{F}_p$, donc R a au moins p racines distinctes et $\deg(R)\geqslant p$.

f) découle de d) et e).

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.

Solution. a) Le groupe $\mathfrak{S}_n$ agit sur $A[T]$ coefficient par coefficient. En particulier, $f \in A[T]$ est $\mathfrak{S}_n$-invariant si et seulement si ses coefficients le sont. Puisque $\sigma(T - X_i) = T - X_{\sigma^{-1}(i)}$, on voit que $(T - X_1)\cdots(T - X_n)$ est $\mathfrak{S}_n$-invariant, donc ses coefficients le sont, et ce sont les Σ_i à un signe près.

b) On doit montrer que le morphisme d'anneaux $\varphi : \mathbb{Z}[Y_1, \cdots, Y_n] \longrightarrow B$ qui envoie Y_i sur e_{μ_i} est un isomorphisme. Pour $\lambda = n_1\mu_1 + \cdots + n_n\mu_n$, posons $f_\lambda := e_{\mu_1}^{n_1} e_{\mu_2}^{n_2} \cdots e_{\mu_n}^{n_n}$. Il s'agit donc de montrer que la famille $(f_\lambda)_{\lambda\in\Lambda}$ est une $\mathbb{Z}$-base de B (la liberté est équivalente à l'injectivité de φ, et le caractère générateur est équivalent à la surjectivité de φ). Pour cela, le point clef est que l'hypothèse de l'énoncé implique :

$$(*) \quad f_\lambda \in e_\lambda + \sum_{\mu\prec\lambda} \mathbb{Z} e_\mu.$$

Montrons que la famille $(f_\lambda)_{\lambda\in\Lambda}$ est libre. Soit $a_{\lambda_1} f_{\lambda_1} + \cdots + a_{\lambda_r} f_{\lambda_r} = 0$ une combinaison linéaire nulle entre les f_λ. Quitte à renuméroter, on peut supposer que λ_1 est maximal parmi les λ_i. On déduit de $(*)$

$$a_{\lambda_1} e_{\lambda_1} \in \sum_{\mu\prec\lambda_1} \mathbb{Z} e_\mu + \sum_{i=2}^{r} \sum_{\mu\preccurlyeq\lambda_i} \mathbb{Z} e_\mu.$$

Comme λ_1 n'apparaît pas dans la somme de droite, l'indépendance linéaire des e_λ implique que $a_{\lambda_1} = 0$. De même on montre que tous les autres coefficients sont nuls et on en déduit que la famille $(f_\lambda)_{\lambda\in\Lambda}$ est libre.

Montrons maintenant que la famille $(f_\lambda)_{\lambda\in\Lambda}$ est génératrice. Pour cela on va montrer que

$$(**) \quad e_\lambda \in f_\lambda + \sum_{\mu\prec\lambda} \mathbb{Z} f_\mu$$

par récurrence forte sur l'entier $v(\lambda) := |\{\mu \prec \lambda\}|$. En effet, $(*)$ nous dit que $e_\lambda \in f_\lambda + \sum_{\mu\prec\lambda} \mathbb{Z}e_\mu$. Donc, si $v(\lambda) = 0$, on a $e_\lambda = f_\lambda$. Plus généralement, supposons $v(\lambda) > 0$ et $(**)$ connu pour les λ' tels que $v(\lambda') < v(\lambda)$. Comme $\mu \prec \lambda \Rightarrow v(\mu) < v(\lambda)$, on déduit $(**)$ de $(*)$ et de l'hypothèse de récurrence.

c) i) On trouve $S^{\mu_j} = \Sigma_j$.

ii) Le point clef est l'observation suivante : *toute $\mathfrak{S}_n$-orbite dans $\mathbb{N}^n$ admet un unique représentant dans Λ*. On notera λ_ν l'unique représentant dans Λ de l'orbite $\mathfrak{S}_n \cdot \nu$ de $\nu \in \mathbb{N}^n$. On a en particulier $\lambda_\nu = \lambda_{\nu'} \Leftrightarrow \nu' \in \mathfrak{S}_n \cdot \nu$.

Montrons maintenant que $(S^\lambda)_{\lambda\in\Lambda}$ est libre. Soit $\sum_\lambda a_\lambda S^\lambda = 0$ une relation de dépendance linéaire. Alors $\sum_\nu a_{\lambda_\nu} X^\nu = 0$ est une relation de dépendance linéaire entre les X^ν. Mais ceux-ci forment une base de A, donc $a_{\lambda_\nu} = 0$ pour tout ν.

Montrons finalement que $(S^\lambda)_{\lambda\in\Lambda}$ est génératrice. Un élément $f \in A^{\mathfrak{S}_n}$ est un élément $f = \sum_\nu a_\nu X^\nu$ tel que $a_\nu = a_{\sigma(\nu)}$ pour tout ν et tout $\sigma \in \mathfrak{S}_n$, et donc tel que $a_\nu = a_{\lambda_\nu}$ pour tout ν. On a donc aussi $f = \sum_\Lambda a_\lambda S^\lambda$.

d) i) On sait que c'est une relation d'ordre, et on vérifie immédiatement qu'elle est compatible à l'addition (i.e. $\nu \preccurlyeq \nu' \Rightarrow (\forall \mu \in \mathbb{N}^n, (\mu + \nu) \preccurlyeq (\mu + \nu'))$. Si maintenant $\lambda, \mu \in \Lambda$ et $\mu \prec \lambda$, alors $\mu_1 \leqslant \lambda_1$ et, comme $\mu_i \leqslant \mu_1$ pour $i \geqslant 1$, on voit qu'il n'y a qu'un nombre fini de tels μ. Remarquons que cette finitude n'est pas vraie si on remplace Λ par $\mathbb{N}^n$. En effet, pour $n = 2$ par exemple, on a $(0, n) \prec (1, 0)$ pour tout $n \in \mathbb{N}$.

ii) On a $S^\lambda S^{\lambda'} = \sum_{\lambda_\nu=\lambda, \lambda_{\nu'}=\lambda'} X^{\nu+\nu'}$. On sait que ce produit est de la forme $S^\lambda S^{\lambda'} = \sum_{\lambda''} c_{\lambda,\lambda';\lambda''} S^{\lambda''}$, et en identifiant les deux expressions, on constate que

$$c_{\lambda,\lambda';\lambda''} = |\{(\nu, \nu') \text{ t.q. } \lambda_\nu = \lambda, \lambda_{\nu'} = \lambda' \text{ et } \lambda'' = \nu + \nu'\}|\,.$$

Pour conclure, il nous suffit donc de montrer que pour tout couple $(\nu, \nu') \in \mathfrak{S}_n\lambda \times \mathfrak{S}_n\lambda'$, on a $\nu + \nu' \prec \lambda + \lambda'$ avec égalité si et seulement si $\nu = \lambda$ et $\nu' = \lambda'$.

Pour montrer cette dernière assertion, soit $r := \max\{i, \nu_i = \lambda_i \text{ et } \nu'_i = \lambda'_i$. Si $r = n$, alors $\lambda = \nu$ et $\lambda' = \nu'$. Sinon, alors $(\lambda + \lambda')_i = (\nu + \nu')_i$ pour $i = 1, \cdots, r$, mais $(\lambda + \lambda')_{r+1} > (\nu + \nu')_{r+1}$ d'où $\nu + \nu' \prec \lambda + \lambda'$.

iii) D'après c) et d), on peut appliquer la question b) à $B = A^{\mathfrak{S}_n}$ et $(e_\lambda)_{\lambda\in\Lambda} = (S^\lambda)_{\lambda\in\Lambda}$, après avoir remarqué que les μ_i de la question c) forment une base de Λ. On en déduit que $A^{\mathfrak{S}_n}$ est un anneau de polynômes en les S^{μ_i}, i.e. sur les Σ_i.

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 ?

Solution. Soit $\alpha \in K \setminus k$. On a $\deg(f_\alpha)|2$ et $\deg(f_\alpha) \neq 1$ donc $\deg(f_\alpha) = 2$. Écrivons $f_\alpha = X^2 + aX + b$. Les racines de f_α sont α et b/α donc f_α est scindé dans $K[X]$. Comme on a de plus $K = k(\alpha)$, on voit que K est un corps de décomposition du polynôme f_α. C'est donc une extension normale.
On a vu en cours que l'extension $\mathbb{Q}(\sqrt[3]{2})$ n'est pas normale car elle ne contient pas les autres racines $j\sqrt[3]{2}$ et $j^2\sqrt[3]{2}$ de $X^2 - 3$.

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 $K = \mathbb{Q}(\alpha)$.

Solution. a) On a $[K : \mathbb{Q}] = [K : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}]$. On sait que $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ et $[K : \mathbb{Q}(\sqrt{2})]|2$. Pour voir que $[K : \mathbb{Q}(\sqrt{2})] = 2$, il faut montrer que $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$. Or, en écrivant $(a + b\sqrt{2})^2 = 3$, on obtient $3 = a^2$ ou $3 = 2b^2$, ce qui n'est pas possible pour $a, b \in \mathbb{Q}$. Donc $[K : \mathbb{Q}] = 4$. Par ailleurs, K contient, et est engendré par, les racines du polynôme $(X^2 - 2)(X^2 - 3)$. C'est donc un corps de décomposition de ce polynôme.

b) Si $\sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, on a $\sigma(\sqrt{2}) = \pm\sqrt{2}$ et $\sigma(\sqrt{3}) = \pm\sqrt{3}$. Donc $\sigma(\alpha) \in \{\pm\sqrt{2} \pm \sqrt{3}\}$. Montrons que les 4 nombres $\pm\sqrt{2} \pm \sqrt{3}$ sont bien conjugués à α. Puisque $X^2 - 3$ est irréductible sur $\mathbb{Q}(\sqrt{2})$, il existe $\sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}(\sqrt{2}))$ tel que $\sigma(\sqrt{3}) = -\sqrt{3}$. De même il existe $\sigma' \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}(\sqrt{3}))$ tel que $\sigma(\sqrt{2}) = -\sqrt{2}$. On alors $\sigma(\alpha) = \sqrt{2} - \sqrt{3}$, $\sigma'(\alpha) = -\sqrt{2} + \sqrt{3}$ et $\sigma\sigma'(\alpha) = -\sqrt{2} - \sqrt{3}$. L'orbite de α sous $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ est donc bien $\{\pm\sqrt{2} \pm \sqrt{3}\}$. En particulier, α est de degré 4 égal à $[K : \mathbb{Q}$, donc $K = \mathbb{Q}(\alpha)$.

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 $k \subset K_{\mathrm{sep}} \subset K$.

b) Montrer que l'extension $K_{\mathrm{sep}} \subset K$ 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 : $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{2}, \sqrt{3})$, $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$.

Solution.

— On sait que $\mathbb{Q}(\sqrt{2})$ est de degré 2 sur $\mathbb{Q}$, donc est normale (cf exercice plus haut). Son groupe de Galois est d'ordre 2, donc isomorphe à $\mathbb{Z}/2\mathbb{Z}$.

— On a déjà vu que $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ est de degré 4 sur $\mathbb{Q}$ (il faut voir que 3 n'est pas un carré dans $\mathbb{Q}(\sqrt{2})$). Par ailleurs, c'est le corps de décomposition de $(X^2-2)(X^2-3)$ donc elle est Galoisienne et son groupe de Galois est d'ordre 4. Il contient les deux groupes de Galois $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}(\sqrt{2}))$ et $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}(\sqrt{2}))$ qui sont distincts et chacun d'ordre 2. Donc $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

— Montrons d'abord que $\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5})$ est de degré 8 sur $\mathbb{Q}$. Par la formule $[\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5}):\mathbb{Q}] = [\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5}):\mathbb{Q}(\sqrt{2},\sqrt{3})][\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}]$, il suffit de montrer que 5 n'est pas un carré dans $\mathbb{Q}(\sqrt{2},\sqrt{3})$. Ecrivons $5 = (\alpha+\beta\sqrt{3})^2 = (\alpha^2+3\beta^2)+2\alpha\beta\sqrt{3}$ avec $\alpha,\beta\in\mathbb{Q}(\sqrt{2})$. Comme $1,\sqrt{3}$ forment une $\mathbb{Q}(\sqrt{2})$-base de $\mathbb{Q}(\sqrt{2},\sqrt{3})$, on en tire $\alpha\beta=0$, donc $\alpha^2=5$ ou $3\beta^2=5$. On écrit alors α ou β sous la forme $a+b\sqrt{2}$ et on obtient de même que $a^2=5$ ou $2b^2=5$ ou $3a^2=5$ ou $6b^2=5$, ce qui est impossible. Par ailleurs $\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5})$ est le corps de décomposition de $(X^2-2)(X^2-3)(X^2-5)$ donc est Galoisien sur $\mathbb{Q}$. Tout élément de son groupe de Galois envoie $\sqrt{2}$ sur $\pm\sqrt{2}$ et idem pour $\sqrt{3}$ et $\sqrt{5}$, donc tout tel élément est d'ordre 2. Il s'ensuit que Gal $= (\mathbb{Z}/2\mathbb{Z})^3$.

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 $\mu_6\rtimes(\mathbb{Z}/6\mathbb{Z})^\times$.

Solution. a) Soit $\alpha=\sqrt[n]{a}$ une racine n-ème de a. Les autres racines de f sont de la forme $\alpha\zeta$ avec $\zeta\in\mu_n$, donc $\mu_n\subset K_f$. Le corps cyclotomique $\mathbb{Q}(\mu_n)$ est Galoisien sur $\mathbb{Q}$, donc le groupe $\mathrm{Gal}(K_f/\mathbb{Q}(\mu_n))$ est distingué, de quotient $G_f/\mathrm{Gal}(K_f/\mathbb{Q}(\mu_n))\xrightarrow{\sim}\mathrm{Gal}(\mathbb{Q}(\mu_n)/\mathbb{Q})=(\mathbb{Z}/n\mathbb{Z})^\times$. De plus, on sait d'après le cours que $\mathrm{Gal}(K_f/\mathbb{Q}(\mu_n))\simeq\mu_m$ pour un $m|n$.

b) Pour tout $\sigma\in G_f$, on pose $\zeta_\sigma := \frac{\sigma(\sqrt[n]{a})}{\sqrt[n]{a}}\in\mu_n$ et on note $a_\sigma\in(\mathbb{Z}/n\mathbb{Z})^\times$ l'unique élément tel que $\sigma(\zeta)=\zeta^{a_\sigma}$ pour tout $\zeta\in\mu_n(K_f)$. Alors l'application $\sigma\mapsto(\zeta_\sigma,a_\alpha)$ définit un morphisme de groupes $G_f\longrightarrow\mu_n\rtimes(\mathbb{Z}/n\mathbb{Z})^\times$. Pour le voir, il suffit de montrer que $a_{\sigma\sigma'}=a_\sigma a_{\sigma'}$, ce qui est facile, et que $\zeta_{\sigma\sigma'}=\zeta_\sigma(\zeta_{\sigma'})^{a_\sigma}$, ce qui provient du calcul $\frac{\sigma\sigma'(\sqrt[n]{a})}{\sqrt[n]{a}}=\frac{\sigma(\sqrt[n]{a})}{\sqrt[n]{a}}\frac{\sigma\sigma'(\sqrt[n]{a})}{\sigma(\sqrt[n]{a})}=\frac{\sigma(\sqrt[n]{a})}{\sqrt[n]{a}}\sigma\left(\frac{\sigma'(\sqrt[n]{a})}{\sqrt[n]{a}}\right)=\zeta_\sigma\sigma(\zeta_{\sigma'})$.
Ce morphisme est injectif car son noyau fixe $\sqrt[n]{a}$ et μ_n, qui engendrent K_f.

c) Notons d'abord que ψ est un isomorphisme si et seulement si $|G_f|=n\varphi(n)$. Ceci équivaut encore à $[K_f:\mathbb{Q}(\mu_n)]=n$. Comme $K_f=\mathbb{Q}(\mu_n)(\sqrt[n]{a})$, ceci équivaut à ce que X^n-a soit le polynôme minimal de $\sqrt[n]{a}$ sur $\mathbb{Q}(\mu_n)$.
Supposons maintenant X^n-a irréductible dans $\mathbb{Q}[X]$ et $(n,\varphi(n))=1$. On a alors $n|[K_f:\mathbb{Q}]$ puisque $[\mathbb{Q}(\sqrt[n]{a}):\mathbb{Q}]=n$ et on sait par ailleurs que $\varphi(n)|[K_f:\mathbb{Q}]$ puisque $\mathbb{Q}(\mu_n)\subset K_f$. Il s'ensuit que $n\varphi(n)|\,|G_f|$, et donc $|G_f|=n\varphi(n)$.

d) Dans ce cas, puisque $K_f=\mathbb{Q}(\sqrt[n]{a})(\mu_n)$, la surjection du a) admet une rétraction, donnée par l'inverse du caractère cyclotomique $\chi^{-1}_{n,\mathbb{Q}(\sqrt[n]{a})}:(\mathbb{Z}/n\mathbb{Z})^\times\xrightarrow{\sim}\mathrm{Gal}(K_f/\mathbb{Q}(\sqrt[n]{a}))\hookrightarrow G_f$.

e) Notons d'abord que $(\mathbb{Z}/6\mathbb{Z})^\times=\{\pm1\}$, donc $\mu_6\rtimes(\mathbb{Z}/6\mathbb{Z})^\times$ est de cardinal 12. Par ailleurs, le critère d'Eisenstein nous dit que $f=X^6+3$ est irréductible. Donc $[K_f:\mathbb{Q}]$ vaut 6 ou 12. Remarquons maintenant que $e^{\frac{2i\pi}{6}}=\frac{1+i\sqrt{3}}{2}\in\mathbb{Q}(\sqrt{-3})$. On a donc $\mu_6\subset\mathbb{Q}(\sqrt{-3})\subset\mathbb{Q}(\sqrt[6]{-3})$. En particulier, $K_f=\mathbb{Q}(\sqrt[6]{-3})$. On en déduit que G_f est d'ordre 6. Comme son sous-groupe $\mathrm{Gal}(K_f/\mathbb{Q}(\sqrt[3]{-3})$ n'est pas abélien, on a $G_f\simeq\mathfrak{S}_3\simeq\mathbb{Z}/3\mathbb{Z}\rtimes\mathbb{Z}/2\mathbb{Z}$. En fait, on peut préciser ces sous-groupes : on a par exemple $G_f=\mathrm{Gal}(K_f/\mathbb{Q}(\beta))\rtimes$

$\mathrm{Gal}(K_f/\mathbb{Q}(\alpha))$ où on a fixé la racine cubique réelle $\alpha = \sqrt[3]{-3}$ et une racine carrée $\beta = \sqrt{-3}$ de -3. Notons que $\beta\alpha^{-1}$ est une racine sixième de -3. Puisque $K_f = \mathbb{Q}(\beta)(\alpha)$, on a $\mathrm{Gal}(K_f/\mathbb{Q}(\beta)) \xrightarrow{\sim} \mu_3$ et on note σ le générateur qui correspond à j (i.e qui envoie α sur $j\alpha$). Calculons $\psi(\sigma) = (\zeta_\sigma, a_\alpha)$ avec la notation de b). Par définition on a $\zeta_\sigma = j$, et on a $a_\sigma = 1$ car σ fixe $\mu_6 \subset \mathbb{Q}(\beta)$. De l'autre côté, $\mathrm{Gal}(K_f/\mathbb{Q}(\alpha)) \xrightarrow{\sim} \{\pm 1\}$ avec pour générateur l'automorphisme induit par la conjugaison complexe. On a alors $\psi(\tau) = (\zeta_\tau, a_\tau)$ avec $\zeta_\tau = \frac{\tau(\beta\alpha^{-1})}{\beta\alpha^{-1}} = \frac{(-\beta)\alpha^{-1}}{\beta\alpha^{-1}} = -1$ et $a_\tau = -1$ puisque $\tau(j) = \bar{j} = j^{-1}$.

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 $\mathbb{Q}^{\mathrm{ab}}$ 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 $\mathbb{Q}^{\mathrm{ab}}$ 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.