

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 cherchiez-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

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

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 $1 \leq i \leq \deg f_\alpha$ et $1 \leq j \leq \deg f_\beta$. 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 le 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 $i|z_1 z_2|$. 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 $|\alpha - \frac{p}{q}| > \frac{A}{q^n}$.

- Montrer que $|f(\frac{p}{q})| \geq \frac{1}{q^n}$.
- Montrer qu'il existe $M > 0$ tel que $|f(\frac{p}{q})| < M \cdot |\alpha - \frac{p}{q}|$ pour $\frac{p}{q}$ dans un voisinage de α , et conclure.
- 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 ≥ 1 , on en déduit $|f(\frac{p}{q})| \geq \frac{1}{q^n}$.

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 $\alpha = \lim_{n \rightarrow \infty} \frac{p_n}{q_n}$ avec $|\alpha - \frac{p_n}{q_n}| \leq \frac{1}{(q_n)^n}$ et $q_n \geq 2$ pour tout n . Alors, pour $m \geq n$, on obtient $|\alpha - \frac{p_m}{q_m}| \leq \frac{1}{(q_m)^{m-n}} \frac{1}{(q_n)^n} \leq \frac{1}{2^{m-n}} \frac{1}{(q_n)^n}$. On voit donc que α ne peut être algébrique de degré $n \geq 1$ d'après le théorème de Liouville, et ceci étant valable pour tout n , α est transcendant ou rationnel. Pour un exemple de telle suite, on peut prendre $\frac{p_n}{q_n} = \sum_{k=0}^n 10^{-k!}$. La limite α est un réel non rationnel (car son développement décimal ne devient pas périodique à partir d'un certain rang) donc il est transcendant.

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

- Montrer que K n'est pas de type fini en tant que k -algèbre.
- Soit $F \in K \setminus k$. On écrit $F = \frac{P(X)}{Q(X)}$, avec $P, Q \in k[X]$ premiers entre eux.
 - Montrer que X est algébrique sur $k(F)$ (on pourra considérer $R(T) := P(T) - FQ(T) \in k(F)[T]$).
 - En déduire que F est transcendant sur k .
 - Montrer que $[K : k(F)] = \max(\deg(P), \deg(Q))$ (on pourra montrer que $R(T)$ est irréductible dans $k[F][T]$).
- Soit $\phi : \text{GL}_2(k) \rightarrow \text{Aut}_k(K)$ 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 $\text{Ker}(\phi) = k^\times$.

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

- 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, $[k(X) : k(F)] \leq \deg(R) = \max(\deg(P), \deg(Q))$.
 - 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.
 - On a déjà l'inégalité $[k(X) : k(F)] \leq \deg(R) = \max(\deg(P), \deg(Q))$. 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, $\text{pgcd}(P, Q) = 1$, donc R est primitif en tant que polynôme de $k[T][F]$, donc R est irréductible dans $k[T][F]$ donc aussi dans $k(F)[T]$. D'où le résultat.

- c) Soit $\varphi \in \text{Aut}_k(K)$, 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 $\frac{aX+b}{cX+d}$. Écrivons $F = \frac{P}{Q}$ 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 $\text{GL}_2(k)$.

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

- Montrer que $K = K_{z_1, z_2, z_3} := \mathbb{C}(X)[T]/(X^3 - f(T))$ est un corps de degré de transcendance 1 sur $\mathbb{C}$. Calculer $[K : \mathbb{C}(X)]$ et $[K : \mathbb{C}(T)]$.
- Si $z_1 = z_2$, montrer que K est transcendant pur engendré par $\frac{X}{T-z_1}$.
- Supposons les z_i distincts deux à deux. Montrer qu'il existe $\lambda \in \mathbb{C} \setminus \{0, 1\}$ tel que $K_{z_1, z_2, z_3} \simeq K_{0, 1, \lambda}$.
- 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 $K := \mathbb{F}_p(X, Y)$.

- Montrer que $K^p := \{x^p, x \in K\}$ est un sous corps de K et que $[K : K^p] = p^2$.
- 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 , et on a $K^p = \mathbb{F}_p(X^p, Y^p)$. Introduisons l'extension intermédiaire $K' := \mathbb{F}_p(X^p, Y)$. Il suffit de montrer que $[K' : K^p] = [K : K'] = p$. L'extension K'/K^p est de la forme $k(Y)/k(Y^p)$ en posant $k = \mathbb{F}_p(X^p)$. Il est clair que $k[Y]$ est un $k[Y^p]$ -module libre de base $\{1, \dots, Y^{p-1}\}$. Cette famille est donc $k(Y^p)$ -libre dans $k(Y)$. Elle est aussi $k(Y^p)$ -génératrice puisque $\forall P, Q \in k[Y]$, on a $\frac{P}{Q} = \frac{1}{Q^p} \cdot PQ^{p-1}$ et $Q^p \in k(Y^p)$. On voit donc que $[K' : K^p] = p$ et, de même, on montre $[K : K'] = p$.

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

2 Autour du Nullstellensatz

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

- Vérifier qu'on obtient ainsi un morphisme de k -algèbres de $k[X_1, \dots, X_n]$ dans la k -algèbre des fonctions de k^n dans k .
- Montrer que ce morphisme est injectif si et seulement si k est infini.

Solution. a) est immédiat. b) Lorsque k est fini et $n = 1$, le polynôme $\prod_{\alpha \in k} (X - \alpha)$ induit la fonction nulle. Supposons k infini et prouvons l'injectivité par récurrence sur n . Si $n = 1$, on sait que pour tout $\alpha \in k$, si $f(\alpha) = 0$ alors $(X - \alpha)$ divise f , ce qui montre que f a un nombre fini de racines, borné par son degré. Il s'ensuit que pour k infini, un polynôme à une indéterminée qui induit la fonction nulle doit être nul. Supposons maintenant le résultat acquis au rang $n - 1$, et soit $f \in k[X_1, \dots, X_n]$ induisant la fonction nulle sur k^n . On peut écrire $f = \sum_i f_i(X_1, \dots, X_{n-1})X_n^i$ pour des polynômes $f_i \in k[X_1, \dots, X_{n-1}]$ uniquement déterminés. Fixons alors $\alpha_1, \dots, \alpha_{n-1}$. La fonction associée au polynôme $\sum_i f_i(\alpha_1, \dots, \alpha_{n-1})X_n^i$ en une indéterminée X_n est nulle, par hypothèse, donc ce polynôme est nul, i.e. $f_i(\alpha_1, \dots, \alpha_{n-1}) = 0$ pour tout i . Par hypothèse de récurrence, il s'ensuit que $f_i = 0$ pour tout i , et finalement que $f = 0$.

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

- Montrer que $\mathcal{O}(V) \simeq \mathbb{C}[X_1, \dots, X_n]/\sqrt{I}$.
- Soit $V' \subset \mathbb{C}^n$ un autre ensemble algébrique. On dit qu'une application $V \rightarrow V'$ est polynômiale si elle est restriction d'une application $\mathbb{C}^n \rightarrow \mathbb{C}^n$ polynômiale. Montrer que $\{\text{App. Pol. } V \rightarrow V'\} \simeq \text{Hom}_{\mathbb{C}\text{-alg}}(\mathcal{O}(V'), \mathcal{O}(V))$.

3 Quelques polynômes irréductibles

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

- Montrer que $X^n - 1 = \prod_{d|n} \Phi_d$. En déduire que $\Phi_n \in \mathbb{Z}[X]$.
- Soit ζ une racine primitive n 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 $f|g| \Phi_n$ et $f|g(X^p)$.
- 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.
- 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 $\mathbb{Z}[X]$.

- 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 $f|g| \Phi_n$. Enfin, ζ est racine de $g(X^p)$ qui est dans $\mathbb{Q}[X]$, donc $f|g(X^p)$.

- 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 Φ_n 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 a $h|\bar{g}^p$ 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 $\bar{\mathbb{F}}_p$ 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 $\mathbb{F}_p$.

- 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 $P = X^p - X - a \in \mathbb{F}_p[X]$.

- Si $a = 0$, donner la décomposition en facteur irréductible de P . On suppose dorénavant $a \neq 0$.
- Montrer que $P(X + 1) = P(X)$.
- Soit Q un facteur irréductible de P . Montrer que $Q(X + 1)$ est aussi un facteur irréductible de P .
- 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).
- Montrer que si $R \in \mathbb{F}_p[X]$ est de degré $\leq p - 1$ et $R(X + 1) = R(X)$, alors R est un polynôme constant.
- En déduire que P est irréductible.
- 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 $X^p - X = \prod_{a \in \mathbb{F}_p} (X - a)$.

- clair
- $P(X) = Q(X)R(X) \Rightarrow P(X) = P(X + 1) = Q(X + 1)R(X + 1)$ donc $Q(X + 1)$ divise P . Par ailleurs $Q(X + 1)$ est irréductible.
- 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 $\deg(R) \geq p$.
- f) découle de d) et e).

4 Polynômes symétriques

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

- a) Notons $\Sigma_1, \dots, \Sigma_n \in A$ 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 $\mathbb{Z}[Y_1, \dots, Y_n] \rightarrow A^{\mathfrak{S}_n}$ 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 $(\Lambda, \preceq)$ est un monoïde commutatif ordonné tel que $\forall \lambda \in \Lambda, \{\mu \preceq \lambda\}$ 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 $\mu_1, \dots, \mu_n$. Montrer que B est un anneau de polynômes en les $e_{\mu_1}, \dots, e_{\mu_n}$.

- c) Soit $\Lambda := \{\nu \in \mathbb{N}^n, \nu_1 \geq \dots \geq \nu_n\}$. 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 $\mu_j = (1, \dots, 1, 0, \dots, 0)$ avec j termes 1 et $n-j$ termes 0.

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

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

i) Montrer que $\preceq$ est une relation d'ordre sur $\mathbb{N}^n$ compatible à l'addition et t.q. $\forall \lambda \in \Lambda, \{\mu \in \Lambda, \mu \preceq \lambda\}$ 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 $\Delta_n \in \mathbb{Z}[Y_1, \dots, Y_n]$ tel que $\prod_{i < j} (X_i - X_j)^2 = \Delta_n(\Sigma_1, \dots, \Sigma_n)$.

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

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

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 $\varphi : \mathbb{Z}[Y_1, \dots, Y_n] \rightarrow B$ qui envoie Y_i sur e_{μ_i} est un isomorphisme. Pour $\lambda = n_1 \mu_1 + \dots + n_n \mu_n$, 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 $a_{\lambda_1} f_{\lambda_1} + \dots + a_{\lambda_r} f_{\lambda_r} = 0$ 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 (*)

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

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. $\nu \prec \nu' \Rightarrow (\forall \mu \in \mathbb{N}^n, (\mu + \nu) \prec (\mu + \nu'))$). Si maintenant $\lambda, \mu \in \Lambda$ et $\mu \prec \lambda$, alors $\mu_1 \leq \lambda_1$ et, comme $\mu_i \leq \mu_1$ pour $i \geq 1$, 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 $i = 1, \dots, r$, 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 $X^3 - 2$.

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 $[K : \mathbb{Q}(\sqrt{2})] \mid 2$. 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 $\sigma \in \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, 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 $\sigma \in \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}(\sqrt{2}))$ tel que $\sigma(\sqrt{3}) = -\sqrt{3}$. De même il existe $\sigma' \in \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}(\sqrt{3}))$ 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 $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ 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 .

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

Solution. a) Notons $c := \beta - \alpha$. Pour toute racine α' de f , il existe d'après le cours un automorphisme $\sigma \in \text{Aut}_{k\text{-alg}}(\bar{k})$ qui envoie α sur α' . On en déduit que $\alpha' + c = \sigma(\alpha + c) = \sigma(\beta)$ est une racine de f . En d'autres termes, l'ensemble des racines de f est stable par addition de c , ce qui n'est possible que s'il existe $n \in \mathbb{N}$ tel que $nc = 0$, puisque c'est un ensemble fini.

b) Notons $c := \beta\alpha^{-1}$. Pour toute racine α' de f , il existe d'après le cours un automorphisme $\sigma \in \text{Aut}_{k\text{-alg}}(\bar{k})$ qui envoie α sur α' . On en déduit que $\alpha'c = \sigma(\alpha c) = \sigma(\beta)$ est une racine de f . En d'autres termes, l'ensemble des racines de f est stable par multiplication par c , ce qui n'est possible que s'il existe $n \in \mathbb{N}$ tel que $c^n = 1$, puisque c'est un ensemble fini.

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.

- Montrer que f inséparable $\Leftrightarrow f' = 0$.
- Supposons f inséparable.
 - Montrer que k est de caractéristique $p > 0$.
 - Montrer qu'il existe un unique polynôme irréductible *séparable* $g \in k[X]$ et un unique entier r tel que $f(X) = g(X^{p^r})$.
 - Montrer que les coefficients de f ne sont pas tous dans l'image du Frobenius φ_k .

Solution. a) On sait que f est inséparable si et seulement si le pgcd de f et f' n'est pas inversible. Puisque f est irréductible, cela équivaut à ce que ce pgcd soit (f) , et donc à ce que f divise f' . Comme $\deg f' < \deg f$, ceci équivaut encore à $f' = 0$.

- D'après a), on a $f' = 0$. Puisque f est non constant, cela n'est pas possible en caractéristique nulle.
 - Écrivons $f = \sum_i a_i X^i$. L'égalité $f' = 0$ implique $i a_i = 0$ pour tout i . On a donc $a_i \neq 0 \Rightarrow p \mid i$. On peut donc écrire f sous la forme $f = f_1(X^p)$ avec $f_1 = \sum_i a_{ip} X^i$. Soit alors r le plus grand entier tel qu'on peut écrire f sous la forme $f = f_r(X^{p^r})$ (l'ensemble des tels entiers est clairement borné, et non vide comme on vient de le voir). Explicitement, on a $r = \min\{v_p(i), a_i \neq 0\}$. De plus, f_r est irréductible puisque toute factorisation non triviale $f_r = PQ$ en induit une factorisation non triviale $f = P(X^r)Q(X^r)$. Enfin, f_r est séparable, sinon on pourrait l'écrire $f_r = f_{r+1}(X^p)$ et on aurait $f = f_{r+1}(X^{p^{r+1}})$, contredisant la maximalité de r .
 - Notons que les éléments de k qui apparaissent comme coefficients de f sont les mêmes que ceux qui apparaissent comme coefficients de $g = f_r$ ou encore de chaque f_i , $i \leq r$. En particulier, si a_i est de la forme $a_i = b_i^p$ pour tout i , alors $f = f_1(X^p) = (\sum_i b_{ip} X^i)^p$, ce qui contredit l'irréductibilité de f .

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*.

Solution. L'équivalence entre a) et b) est dans le cours. L'exercice précédent montre l'implication c) $\Rightarrow$ a). Supposons donc a) et montrons que φ_k est surjectif. Pour cela, il suffit de montrer que pour tout $\alpha \in k$, le polynôme $X^p - \alpha$ a une racine dans k (nécessairement unique). Or l'hypothèse a) nous dit que $X^p - \alpha$ n'est pas irréductible. On peut donc l'écrire $X^p - \alpha = fg$ dans $k[X]$ avec $\deg f, \deg g > 0$. Soit $\bar{k}$ une clôture algébrique de k et β une racine de $X^p - \alpha$ dans $\bar{k}$. On a donc $X^p - \alpha = (X - \beta)^p$ dans $\bar{k}[X]$. Il s'ensuit qu'il existe $0 < r < p$ tel que $f = (X - \beta)^r$ dans $\bar{k}[X]$. En particulier, le coefficient de X^{r-1} dans f est $-r\beta$. Ce coefficient est dans k puisque $f \in k[X]$. Comme $r \neq 0$, on en déduit $\beta \in k$ comme voulu.

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.

Solution. a) est dans le cours. Pour b), soit $\alpha \in K$ et f_α son polynôme minimal sur K_{sep} . D'après l'exercice 16, on peut écrire $f_\alpha = g(X^{p^r})$ avec g irréductible séparable. Il s'ensuit que α^{p^r} est une racine de g , donc est un élément séparable sur K_{sep} . D'après le cours, il est aussi séparable sur k , donc il appartient à K_{sep} . Il s'ensuit que $g = X - \alpha^{p^r}$, donc $f = X^{p^r} - \alpha^{p^r}$ et α est purement inséparable.

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. Soit k un corps de caractéristique $p > 0$.

- a) Soit $f := X^p - X + a \in k[X]$. On note K_f un corps de décomposition, G_f son groupe de Galois, et α une racine de f dans K_f .
 - i) Montrer que l'ensemble des racines de f dans K_f est de la forme $\{\alpha + b, b \in \mathbb{F}_p\}$ et en conclure que $K_f = k(\alpha)$.
 - ii) Montrer que l'application $\sigma \mapsto \sigma(\alpha) - \alpha$ définit un morphisme de groupe injectif de G_f dans $(\mathbb{F}_p, +)$. En conclure que f est soit scindé, soit irréductible, auquel cas G_f est cyclique d'ordre p .
- b) Soit $f := X^{p^r} - X + a \in k[X]$. On suppose que k contient $\mathbb{F}_{p^r}$. Construire un morphisme injectif de G_f dans $(\mathbb{F}_{p^r}, +)$. En conclure que, si f est irréductible, alors $G_f \simeq (\mathbb{Z}/p\mathbb{Z})^r$.

Solution. a) i) Si $k \in \mathbb{F}_p$, on a $(\alpha + k)^p - (\alpha + b) + a = (\alpha^p - \alpha + a) + (b^p - b) = 0$. Donc les $\alpha + b$ sont des racines. Il y en a p , donc on a toutes les racines. Par définition K_f est engendré par les $\alpha + b$, donc aussi simplement par α .

ii) L'application est bien définie par la question précédente. Notons $b_\sigma := \sigma(\alpha) - \alpha$. On a $b_{\sigma\sigma'} = \sigma\sigma'(\alpha) - \alpha = \sigma(\alpha + b_{\sigma'}) - \alpha = \sigma(\alpha) + b_{\sigma'} - \alpha = b_\sigma + b_{\sigma'}$. On a donc bien défini un morphisme de groupe. Celui-ci est injectif car α engendre K_f . Ainsi G_f est un sous-groupe de $\mathbb{F}_p$, donc $G_f = \{1\}$, auquel cas f est scindé, ou $G_f = \mathbb{F}_p$, auquel cas G_f agit transitivement (cycliquement) sur les racines de f dans K_f , donc f est irréductible.

- b) On vérifie que l'ensemble des racines de f dans K_f est de la forme $\alpha + \mathbb{F}_{p^r}$ et on définit le morphisme exactement comme ci-dessus.

Exercice 22. Montrer que les extensions suivantes de $\mathbb{Q}$ sont Galoisiennes et calculer leur groupe de Galois : $\mathbb{Q}(\sqrt[4]{2})$, $\mathbb{Q}(\sqrt{2}, \sqrt{3})$, $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$.

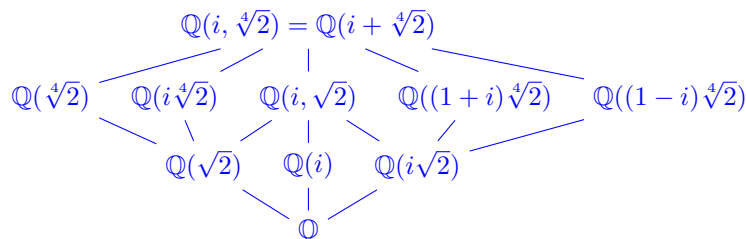
Exercice 23. Soit $f = X^4 - 2 \in \mathbb{Q}[X]$ et K le corps de décomposition de f . Décrire le groupe de Galois $G = \text{Gal}(K/\mathbb{Q})$ de f et toutes les extensions intermédiaires K' telles que $\mathbb{Q} \subset K' \subset K$.

Solution. Le polynôme f est irréductible d'après le critère d'Eisenstein. L'ensemble des racines de f dans $\mathbb{C}$ est $\Omega := \{\zeta \sqrt[4]{2}, \zeta \in \mu_4\}$. Donc $\mathbb{Q}(\sqrt[4]{2})$ est un corps de rupture de degré $[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = 4$ et le corps de décomposition est $K := \mathbb{Q}(\Omega) = \mathbb{Q}(\sqrt[4]{2}, i)$. Comme $i \notin \mathbb{Q}(\sqrt[4]{2})$ mais est racine de $X^2 + 1$ qui est de degré 2, $[K : \mathbb{Q}(\sqrt[4]{2})] = 2$ et donc, par multiplicativité, $[K : \mathbb{Q}] = 8$.

En numérotant l'ensemble Ω des racines de f (par exemple dans l'ordre $\sqrt[4]{2}, i\sqrt[4]{2}, -\sqrt[4]{2}, -i\sqrt[4]{2}$), on obtient un plongement $G_f \hookrightarrow \mathfrak{S}_4$. Puisque $|G_f|$ est d'ordre 8, c'est un 2-Sylow de $\mathfrak{S}_4$. On sait qu'un tel 2-Sylow est de la forme $\mathbb{Z}/4\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$. Ici, le facteur $\mathbb{Z}/4\mathbb{Z}$ est engendré par le 4-cycle $(1, 2, 3, 4)$ qui est le générateur de $\text{Gal}(K/\mathbb{Q}(i))$ correspondant à i via l'isomorphisme $\text{Gal}(K/\mathbb{Q}(i)) \xrightarrow{\sim} \mu_4$, $\sigma \mapsto \frac{\sigma(\sqrt[4]{2})}{\sqrt[4]{2}}$. De plus, on peut prendre pour générateur de $\mathbb{Z}/2\mathbb{Z}$ la transposition $(2, 4)$, qui correspond à la conjugaison complexe.

En regardant Ω comme un carré dans $\mathbb{C}$, on remarque que (1234) et (24) définissent des isométries du carré, et donc G_f est le groupe D_4 des isométries du carré.

Les extensions intermédiaires de $K/\mathbb{Q}$ correspondent aux sous-groupes H de D_4 . Les sous-groupes non triviaux du groupe diédral sont les suivants : d'ordre 2, il y a le groupe engendré par la rotation $(1\ 3)(2\ 4)$ d'angle π (alors $K^H = \mathbb{Q}(i, \sqrt{2})$), les deux groupes engendrés par les symétries $(1\ 3)$ (alors $K^H = \mathbb{Q}(i\sqrt[4]{2})$), $(2\ 4)$ (alors $K^H = \mathbb{Q}(\sqrt[4]{2})$), $(1\ 2)(3\ 4)$ (alors $K^H = \mathbb{Q}((1+i)\sqrt[4]{2})$) et $(14)(23)$ (alors $K^H = \mathbb{Q}((1-i)\sqrt[4]{2})$); d'ordre 4 il y a le groupe N engendré par (1234) ($K^N = \mathbb{Q}(i)$), et les deux sous-groupes $\{id, (1\ 3)(2\ 4), (1\ 3), (2\ 4)\}$ (alors $K^H = \mathbb{Q}(\sqrt{2})$) et $\{id, (1\ 3)(2\ 4), (1\ 2)(3\ 4), (14)(23)\}$ (alors $K^H = \mathbb{Q}(i\sqrt{2})$).



Exercice 24. Soient $f = X^4 + aX^2 + b \in \mathbb{Q}[X]$ un polynôme irréductible, K le corps de décomposition de f et $G = \text{Gal}(K/\mathbb{Q})$. On note $\pm\alpha, \pm\beta$ les racines de f .

- Montrer que G est isomorphe à un sous-groupe du groupe diédral D_4 d'ordre 8.
- Montrer que $G \simeq \mathbb{Z}/4\mathbb{Z}$ si et seulement si $(\alpha/\beta - \beta/\alpha) \in \mathbb{Q}$.
- Montrer que $G \simeq (\mathbb{Z}/2\mathbb{Z})^2$ si et seulement si $\alpha\beta \in \mathbb{Q}$ ou $\alpha^2 - \beta^2 \in \mathbb{Q}$.
- Montrer que sinon G est isomorphe à D_4 .
- Déterminer le groupe de Galois de $X^4 - 4X^2 - 1$.

Solution. a) Il y a plusieurs manières de voir ça.

Première manière : on sait que $G \subset \mathfrak{S}_4$ (après numérotation des racines), et que les 2-Sylow de $\mathfrak{S}_4$ sont isomorphes à D_4 . Il suffit donc de voir que K est une 2-extension. Or, $K = \mathbb{Q}(\sqrt{A}, \sqrt{B})$ où A, B sont les deux racines de $X^2 + aX + b$.

Deuxième manière : si $\sigma \in G$, on doit avoir $\sigma(-\alpha) = -\sigma(\alpha)$ et $\sigma(-\beta) = -\sigma(\beta)$. Si on dispose les racines aux sommets d'un carré de façon à ce que α et $-\alpha$ soient deux sommets opposés, alors les permutations des racines vérifiant les deux propriétés ci-dessus sont exactement les isométries du carré. Donc $G \subset D_4$.

- On rappelle que D_4 a trois sous-groupes d'ordre 4 dont un seul, celui engendré par la rotation $r = (\alpha\ \beta\ -\alpha\ -\beta)$, est monogène (cf. exercice 3).

On a $r(\alpha/\beta - \beta/\alpha) = \alpha/\beta - \beta/\alpha$, donc $\alpha/\beta - \beta/\alpha \in L^{\langle r \rangle}$. Donc si $G = \langle r \rangle$, alors $\alpha/\beta - \beta/\alpha \in L^G = \mathbb{Q}$. Réciproquement, si $s \notin \langle r \rangle$, alors $s(\alpha/\beta - \beta/\alpha) = -(\alpha/\beta - \beta/\alpha)$. Donc si $\alpha/\beta - \beta/\alpha \in \mathbb{Q}$, on en déduit que $G \subset \langle r \rangle$, et donc $G = \langle r \rangle$ puisque $4 \mid \#G$ puisque f est irréductible.

- c) On a deux sous-groupes de D_4 isomorphes à $(\mathbb{Z}/2\mathbb{Z})^2$, à savoir $H_1 := \{id, (1\ 3)(2\ 4), (1\ 3), (2\ 4)\}$ et $H_2 := \{id, (1\ 3)(2\ 4), (1\ 2)(3\ 4), (14)(23)\}$.
On a $\sigma(\alpha\beta) = \alpha\beta$ si $\sigma \in H_2$ et $= -\alpha\beta$ si $\sigma \notin H_2$. Donc si $G = H_2$, $\alpha\beta \in L^G = \mathbb{Q}$ et réciproquement si $\alpha\beta \in \mathbb{Q}$, $G \subset H_2$ et donc $G = H_2$ par le même argument de cardinalité qu'à la question précédente.
On a $\sigma(\alpha^2 - \beta^2) = \alpha^2 - \beta^2$ si $\sigma \in H_1$ et $= -(\alpha^2 - \beta^2)$ si $\sigma \notin H_1$. Donc si $G = H_1$, $\alpha^2 - \beta^2 \in L^G = \mathbb{Q}$ et réciproquement si $\alpha^2 - \beta^2 \in \mathbb{Q}$, $G \subset H_1$ et donc $G = H_1$ par le même argument de cardinalité qu'à la question précédente (en fait, le cas $G = H_1$ est impossible car H_1 n'agit pas transitivement sur les racines, et ceci contredit l'irréductibilité de f).
- d) Comme $4 \nmid \#G$ par irréductibilité de f , si $\#G \neq 4$, alors $G = D_4$.
- e) On a $\alpha = \sqrt{2 + \sqrt{5}}$ et $\beta = \sqrt{2 - \sqrt{5}}$. On en déduit $\alpha^2 - \beta^2 = 2\sqrt{5} \notin \mathbb{Q}$, $\alpha\beta = \sqrt{-1} \notin \mathbb{Q}$ et $(\alpha^2 - \beta^2)/\alpha\beta = \sqrt{-5} \notin \mathbb{Q}$. Donc $G = D_4$.

Exercice 25. 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 $\text{Gal}(K_f/\mathbb{Q}(\mu_n))$ est distingué, de quotient $G_f/\text{Gal}(K_f/\mathbb{Q}(\mu_n)) \xrightarrow{\sim} \text{Gal}(\mathbb{Q}(\mu_n)/\mathbb{Q}) = (\mathbb{Z}/n\mathbb{Z})^\times$. De plus, on sait d'après le cours que $\text{Gal}(K_f/\mathbb{Q}(\mu_n)) \simeq \mu_m$ 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 $\sigma \mapsto (\zeta_\sigma, a_\sigma)$ définit un morphisme de groupes $G_f \rightarrow \mu_n \rtimes (\mathbb{Z}/n\mathbb{Z})^\times$. 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 $K_f = \mathbb{Q}(\sqrt[6]{a})(\mu_6)$, la surjection du a) admet une rétraction, donnée par l'inverse du caractère cyclotomique $\chi_{n, \mathbb{Q}(\sqrt[6]{a})}^{-1} : (\mathbb{Z}/n\mathbb{Z})^\times \xrightarrow{\sim} \text{Gal}(K_f/\mathbb{Q}(\sqrt[6]{a})) \hookrightarrow G_f$.
- e) Notons d'abord que $(\mathbb{Z}/6\mathbb{Z})^\times = \{\pm 1\}$, 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 le sous-groupe $\text{Gal}(K_f/\mathbb{Q}(\sqrt[3]{-3}))$ de G_f n'est pas distingué, G_f n'est pas abélien et 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 $G_f = \text{Gal}(K_f/\mathbb{Q}(\beta)) \rtimes \text{Gal}(K_f/\mathbb{Q}(\alpha))$ 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 $\text{Gal}(K_f/\mathbb{Q}(\beta)) \xrightarrow{\sim} \mu_3$ et on note σ le générateur qui correspond à j (i.e qui envoie α sur $j\alpha$). Calculons $\psi(\sigma) = (\zeta_\sigma, a_\sigma)$ 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, $\text{Gal}(K_f/\mathbb{Q}(\alpha)) \xrightarrow{\sim} \{\pm 1\}$ 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 26. 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 $K_1 K_2$ le sous-corps de L engendré par K_1 et K_2 .

- Montrer que $[K_1 K_2 : k] \leq [K_1 : k][K_2 : k]$, et qu'en cas d'égalité, $k = K_1 \cap K_2$.
- On suppose dorénavant K_1/k galoisienne. Montrer que $K_1 K_2/K_2$ est galoisienne et construire un isomorphisme $\text{Gal}(K_1 K_2/K_2) \xrightarrow{\sim} \text{Gal}(K_1/K_1 \cap K_2)$.
- Montrer que $[K_1 K_2 : k] = [K_1 : k][K_2 : k]/[K_1 \cap K_2 : k]$.
- On suppose dorénavant que K_2/k est également galoisienne. Montrer que $K_1 K_2$ et $K_1 \cap K_2$ sont des extensions galoisiennes de k .
- Construire un morphisme injectif $\phi : \text{Gal}(K_1 K_2/k) \rightarrow \text{Gal}(K_1/k) \times \text{Gal}(K_2/k)$
- Montrer que l'image de ϕ est $\{(g_1, g_2) \in \text{Gal}(K_1/k) \times \text{Gal}(K_2/k), \pi_1(g_1) = \pi_2(g_2)\}$, où $\pi_i : \text{Gal}(K_i/k) \rightarrow \text{Gal}(K_1 \cap K_2/k)$ est la surjection canonique.
- Soit $\mathbb{Q}^{\text{ab}}$ l'ensemble des nombres algébriques x contenus dans une extension galoisienne L de $\mathbb{Q}$ telle que $\text{Gal}(L/\mathbb{Q})$ soit commutatif. Montrer que $\mathbb{Q}^{\text{ab}}$ est un corps. Est-ce une extension finie de $\mathbb{Q}$?

Solution. a) Considérons l'application $K_1 \times K_2 \rightarrow K_1 K_2, (x, y) \mapsto xy$. Elle est $K_1 \cap K_2$ -bilinéaire donc, par propriété universelle du produit tensoriel, on en déduit une application $K_1 \otimes_{K_1 \cap K_2} K_2 \rightarrow K_1 K_2$ telle que $x \otimes y \mapsto xy$. Celle-ci est même un morphisme de $K_1 \cap K_2$ -algèbres et est surjective, par définition de $K_1 K_2$. En prenant les dimensions sur $K_1 \cap K_2$, on voit donc que $[K_1 K_2 : K_1 \cap K_2] \leq [K_1 : K_1 \cap K_2][K_2 : K_1 \cap K_2]$. En multipliant par $[K_1 \cap K_2 : k]^2$, on en déduit $[K_1 K_2 : k] \leq [K_1 : k][K_2 : k]$. En cas d'égalité, on a en particulier $[K_1 \cap K_2 : k] = 1$.

- Puisque K_1 est galoisienne et donc normale, tout $\sigma \in \text{Gal}(K_1 K_2/K_2)$ stabilise K_1 , d'où une application "restriction à K_1 " $\sigma \mapsto \sigma|_{K_1}$, $\text{Gal}(K_1 K_2/K_2) \xrightarrow{\sim} \text{Gal}(K_1/K_1 \cap K_2)$. C'est clairement un morphisme de groupe. Comme tout élément du noyau est l'identité sur K_2 et K_1 , donc aussi sur $K_1 K_2$, ce morphisme est injectif. Soit H son image. Les H -invariants dans K_1 sont alors donnés par $(K_1)^H = (K_1)^{\text{Gal}(K_1 K_2/K_2)} = K_1 \cap (K_1 K_2)^{\text{Gal}(K_1 K_2/K_2)} = K_1 \cap K_2$. On a donc $H = \text{Gal}(K_1/K_1 \cap K_2)$ et le morphisme ci-dessus est aussi surjectif.
- découle facilement de b)
- Plongeons L dans une clôture algébrique $\bar{k}$ de k . Puisque K_1/k et K_2/k sont normales, K_1 et K_2 sont stables par tout automorphisme de $\bar{k}$. Il en est donc de même pour $K_1 \cap K_2$ et $K_1 K_2$, et les extensions $K_1 K_2/k$ et $(K_1 \cap K_2)/k$ sont aussi normales. Elles sont aussi séparables par le cours.
- Il suffit de poser $\phi(\sigma) = (\sigma|_{K_1}, \sigma|_{K_2})$. Le morphisme obtenu est injectif car si σ est l'identité sur K_1 et K_2 , il est l'identité sur le corps engendré par K_1 et K_2 .
- L'image de ϕ est clairement contenue dans le sous-groupe de l'énoncé. On sait que $|\text{Gal}(K_1 K_2/k)| = [K_1 : k][K_2 : k][K_1 \cap K_2 : k]^{-1}$ donc il suffit de montrer que le groupe de l'énoncé a le même cardinal. Notons $G_i := \text{Gal}(K_i/k)$, $H := \text{Gal}(K_1 \cap K_2/k)$ et $G_1 \times_H G_2 \subset G_1 \times G_2$ le sous-groupe de l'énoncé. Les surjections canoniques π_i induisent un morphisme surjectif $G_1 \times G_2 \rightarrow H \times H$, qui se restreint en un morphisme surjectif $\pi : G_1 \times_H G_2 \rightarrow H$ (où H est plongé diagonalement dans $H \times H$). Le noyau de ce morphisme est $\text{Ker } \pi = \text{Ker } \pi_1 \times \text{Ker } \pi_2 = \text{Gal}(K_1/K_1 \cap K_2) \times \text{Gal}(K_2/K_1 \cap K_2)$. On a donc $(G_1 \times_H G_2)/\text{Ker } \pi \simeq H$, d'où l'égalité $|G_1 \times_H G_2| = [K_1 : K_1 \cap K_2][K_2 : K_1 \cap K_2][K_1 \cap K_2 : k]$. On conclut en utilisant $[K_i : K_1 \cap K_2] = [K_i : k][K_1 \cap K_2 : k]^{-1}$.

Exercice 27. Soit $f \in k[X]$ de la forme $f = X^n + aX + b$. Montrer que

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

Solution. Écrivons $f = (X - \alpha_1) \cdots (X - \alpha_n)$ dans $\bar{k}[X]$, où $\bar{k}$ est une clôture algébrique de k . On va utiliser la formule $\text{disc}(f) = (-1)^{n(n-1)/2} \prod_{i=1}^n f'(\alpha_i)$. On a $f' = nX^{n-1} + a$. Compte tenu de $f(\alpha_i) = 0$, on a donc

$$\alpha_i f'(\alpha_i) = n(-a\alpha_i - b) + a\alpha_i = (1-n)a\alpha_i - bn.$$

En faisant le produit, il vient

$$(-1)^n b \prod_{i=1}^n f'(\alpha_i) = \prod_{i=1}^n ((1-n)a\alpha_i - bn).$$

Les $\beta_i := (1-n)a\alpha_i - bn$ sont les racines du polynôme $g(Y) := f(\frac{Y+bn}{(1-n)a})$. On a donc

$$\begin{aligned} \prod_{i=1}^n ((1-n)a\alpha_i - bn) &= (-1)^n \frac{\text{terme constant de } g}{\text{terme dominant de } g} = (-1)^n \frac{(\frac{bn}{(1-n)a})^n + a\frac{bn}{(1-n)a} + b}{(\frac{1}{(1-n)a})^n} \\ &= (-1)^n b (b^{n-1}n^n + (1-n)^{n-1}a^n). \end{aligned}$$

Lorsque $b \neq 0$, on en déduit la formule annoncée en simplifiant par $(-1)^nb$. Si $b = 0$, on a une factorisation $f = X(X^{n-1} + a)$. Supposons que $\alpha_1 = 0$. On a alors $f'(\alpha_1) = a$ et, pour $i > 1$ on a $\alpha_i^{n-1} = -a$ donc $f'(\alpha_i) = (1-n)a$. Il s'ensuit que $\prod_{i=1}^n f'(\alpha_i) = (1-n)^{n-1}a^n$ comme voulu.

Exercice 28. Soit $f = X^5 + 20X - 16 \in \mathbb{Q}[X]$.

- Montrer que f est irréductible et que G_f contient un 5-cycle.
- En réduisant modulo 7, montrer que G_f contient un 3-cycle.
- Montrer que la conjugaison complexe induit un élément non-trivial de G_f . En conclure que $|G_f|$ est divisible par 30.
- Montrer que G_f est contenu dans $\mathfrak{A}_5$.
- Après avoir montré que tout sous-groupe d'indice 2 d'un groupe fini est distingué, en conclure que $G_f = \mathfrak{A}_5$.

Solution. a) Il suffit de montrer que la réduction $\bar{f}$ de f modulo 3 est irréductible. Pour cela, comme $\bar{f}$ est de degré 5, il suffit de montrer que $\bar{f}$ n'a pas de facteur de degré 1 ou 2, i.e. n'a pas de racine dans $\mathbb{F}_3$ ni dans $\mathbb{F}_9$. Or $\bar{f} = X^5 - X - 1$ n'a manifestement pas de racine dans $\mathbb{F}_3$. Pour voir qu'il n'en a pas dans $\mathbb{F}_9$, il faut montrer que $\bar{f}$ est premier avec $X^9 - X$. Vu la décomposition $X^9 - X = X(X^4 - 1)(X^4 + 1)$, il suffit de montrer que $\bar{f}$ est premier avec $X^4 - 1$ et $X^4 + 1$ respectivement. Or, $\bar{f} \equiv -1 \pmod{X^4 - 1}$ et $\bar{f} \equiv X - 1 \pmod{X^4 + 1}$.

Donc, f est bien irréductible, et il s'ensuit que $5 = \deg f$ divise $|G_f|$. Comme les seuls éléments de $\mathfrak{S}_5$ d'ordre 5 sont les 5-cycles, on en déduit que G_f contient un 5-cycle.

- Modulo 7, on a $\bar{f} = X^5 - X - 2$. On constate que 2 et 3 sont racines de $\bar{f}$, et sont les seules racines dans $\mathbb{F}_7$. On a donc une factorisation $\bar{f} = (X - 2)(X - 3)g$ avec $\deg g = 3$. Soit en calculant g , soit en vérifiant que $\bar{f}$ est séparable (et donc en calculant que $(\bar{f}, \bar{f}') = 1$), on voit que g n'a pas de racine dans $\mathbb{F}_7$, donc est irréductible dans $\mathbb{F}_7[X]$. Par le théorème de spécialisation du cours, on en déduit que G_f contient une permutation de type $(1, 1, 3)$, i.e. un 3-cycle.
- Comme $f' = 5X^4 + 20$, la fonction réelle $x \mapsto f(x)$ est strictement croissante et n'a donc qu'un seul zéro. Donc f n'a qu'une racine réelle, et ses racines complexes viennent par paires conjuguées. La conjugaison complexe induit donc un élément non trivial de G_f , et il s'ensuit que $2 \mid |G_f|$. Avec a) et b), on en déduit que $30 = 2 \cdot 3 \cdot 5$ divise $|G_f|$.
- Appliquons la formule de l'exercice précédent pour le discriminant. On trouve $\text{disc}(f) = 20^5 \times 4^4 + 5^5 \times 16^4 = 5^5 \times (2^{18} + 2^{16}) = 5^5 \times (4 + 1) \times 2^{16} = 5^6 \times 2^{16}$ qui est un carré dans $\mathbb{Q}$. Par un théorème du cours, on sait alors que G_f est contenu dans $\mathfrak{A}_5$ (quel que soit le plongement $G_f \hookrightarrow \mathfrak{S}_5$ considéré).
- Soit $H < G$ un sous-groupe d'indice 2. Pour tout $x \in G \setminus H$, on a $Hx = G \setminus H = xH$, donc $xHx^{-1} = H$. On en déduit que H est distingué dans G , et le quotient G/H est $\mathbb{Z}/2\mathbb{Z}$ et est en particulier abélien. Or, on sait que $\mathfrak{A}_5 = [\mathfrak{A}_5, \mathfrak{A}_5]$, i.e. $\mathfrak{A}_5$ n'a pas de quotient abélien non trivial. On en conclut que $G_f = \mathfrak{A}_5$.

Exercice 29. Soit f le polynôme $X^4 + 8X + 12 \in \mathbb{Q}[X]$ et soit K_f le corps de décomposition de f dans $\overline{\mathbb{Q}}$.

- Montrer que f est irréductible sur $\mathbb{Q}$.
- Montrer que $G_f = \text{Gal}(K_f/\mathbb{Q})$ est isomorphe à $\mathfrak{A}_4$.
- Montrer qu'il n'existe pas d'extension quadratique de $\mathbb{Q}$ contenue dans K_f .

Solution. a) Si on regarde modulo 5, le polynôme réduit $\bar{f}$ est séparable (calcul) et possède une seule racine dans $\mathbb{F}_5$, à savoir -1 . Le type de décomposition de $\bar{f}$ est donc $(3, 1)$ (un facteur de degré 3 irréductible fois un facteur de degré 1). Par ailleurs, la fonction $x \in \mathbb{R} \mapsto f(x)$ ne s'annule pas sur $\mathbb{R}$ (son minimum est atteint en $\sqrt[3]{-2}$ et est positif), donc le type de décomposition de f dans $\mathbb{R}[X]$ est $(2, 2)$ (produit de deux facteurs irréductibles de degré 2). Soit alors g un facteur irréductible de f dans $\mathbb{Q}[X]$. Le type de décomposition dans $\mathbb{R}[X]$ implique que g a degré 2 ou 4, et celui dans $\mathbb{F}_5[X]$ implique que g a degré 1, 3 ou 4. Donc g a degré 4 et f est irréductible.

Exercice 30. Le but est d'exhiber une extension Galoisienne de $\mathbb{Q}$ de groupe $H_8 = \{\pm 1, \pm i, \pm j, \pm k\}$.

- Soit $a := (2 + \sqrt{2})(3 + \sqrt{6})$. Montrer que $\mathbb{Q}(a) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, et que pour tout $\sigma \in \text{Gal}(\mathbb{Q}(a)/\mathbb{Q})$, on a $\sigma(a)/a \in (\mathbb{Q}(a)^\times)^2$. Montrer aussi que a n'est pas un carré dans $\mathbb{Q}(a)$.
- Soit d une racine carrée de a dans $\overline{\mathbb{Q}}$. Montrer que $\mathbb{Q}(d)$ est Galoisienne sur $\mathbb{Q}$, et que $\text{Gal}(\mathbb{Q}(d)/\mathbb{Q}(a))$ est central dans $\text{Gal}(\mathbb{Q}(d)/\mathbb{Q})$.
- Montrer que $\text{Gal}(\mathbb{Q}(d)/\mathbb{Q})$ est isomorphe à H_8 .

Exercice 31 (Galois inverse pour les groupes symétriques). Soit n un entier non nul. Une *partition* de n est une suite finie *décroissante* $n_1 \geq n_2 \geq \dots \geq n_r$ d'entiers non nuls, dont la somme $\sum_{i=1}^r n_i$ vaut n (le nombre de parts r n'est pas fixé).

À une permutation $\sigma \in \mathfrak{S}_n$, on associe la partition de n formée par les longueurs $\ell(c_i)$ dans une décomposition $\sigma = \prod_{i=1}^r c_i$ de σ en produit de cycles à supports disjoints de longueurs décroissantes.

À un polynôme $f \in k[X]$, on associe la partition de n formée par les degrés $\deg f_i$ dans une décomposition $f = \prod_{i=1}^r f_i$ de f en produit de diviseurs irréductibles de degrés décroissants.

- Montrer que deux permutations sont conjuguées dans $\mathfrak{S}_n$ si, et seulement si, leur partitions associées sont égales.
- Soit p premier. Montrer qu'il existe des éléments irréductibles de tout degré dans $\mathbb{F}_p[X]$, et en déduire que toute partition de n est associée à au moins un polynôme $f \in \mathbb{F}_p[X]$ unitaire de degré n .
- Montrer que si p est assez grand en fonction de n , toute partition de n est associée à au moins un polynôme $f \in \mathbb{F}_p[X]$ unitaire *séparable* de degré n .
- Soient $C_1, \dots, C_m \subset \mathfrak{S}_n$ des classes de conjugaison d'éléments de $\mathfrak{S}_n$. Montrer qu'il existe $f \in \mathbb{Z}[X]$ unitaire irréductible de degré n tel que, pour toute numérotation des racines de f , on ait $G_f \cap C_i \neq \emptyset$ pour tout $i = 1, \dots, m$.
- Lorsque n est premier, en déduire l'existence de $f \in \mathbb{Z}[X]$ tel que $G_f = \mathfrak{S}_n$. Essayer de généraliser à n quelconque.

Solution. a) Classique, cf cours sur les groupes finis.

- Soit α un élément primitif de l'extension $\mathbb{F}_{p^d}/\mathbb{F}_p$. Son polynôme minimal f_α a degré $d = [\mathbb{F}_{p^d} : \mathbb{F}_p]$ (rappelons que $\mathbb{F}_{p^d}$ a été défini comme un corps de décomposition de $X^{p^d} - X$, donc cet argument n'est pas circulaire). Si $(n_1 \geq \dots \geq n_r)$ est une partition de n , on peut donc choisir f_i irréductible de degré n_i , et le produit $f = \prod_i f_i$ a pour partition associée la partition de départ.
- Dans la situation précédente, il faut pouvoir choisir les f_i 2 à 2 distincts, pour que f soit séparable. Par exemple, si $n_1 = n_2 = \dots = n_k$, il faut pouvoir choisir k polynômes irréductibles de degré n_1 *distincts*. Il suffira donc de trouver p tel que pour tout $d \leq n$, le nombre $I(d, p)$ de polynômes irréductibles unitaires de degré d dans $\mathbb{F}_p[X]$ soit supérieur à n/d . Par le raisonnement de la question b), on voit que $I(d, p)$ est le nombre d'orbites d'éléments primitifs de $\mathbb{F}_{p^d}$ sous l'action de Galois (ie Frobenius). Soit $P(d, p)$ le nombre d'éléments primitifs de $\mathbb{F}_{p^d}$; comme un élément primitif a d conjugués, on a donc $I(d, p) = P(d, p)/d$, et il suffit de trouver une condition pour que $P(d, p) \geq n$. Les éléments primitifs de $\mathbb{F}_{p^d}$ sont ceux qui n'appartiennent à aucun sous-corps $\mathbb{F}_{p^s}$ pour $s|d$. En majorant grossièrement, on a donc $P(d, p) \geq p^d - \sum_{k=0}^{d-1} p^k = p^d - \frac{p^d - 1}{p - 1} = \frac{p^{d+1} - 2p^d + 1}{p - 1} \geq p^d - 2p^{d-1}$. En particulier $p \geq n$ suffit.
- D'après la question précédente on peut trouver des premiers distincts $p_1, \dots, p_m$ et, pour chaque $i = 1, \dots, m$, un polynôme unitaire séparable $\bar{f}_i \in \mathbb{F}_{p_i}[X]$ de partition associée C_i . On peut aussi choisir un autre premier p_0 et un polynôme unitaire irréductible $\bar{f}_0$ de degré n dans $\mathbb{F}_{p_0}[X]$. Par le théorème des restes Chinois, il existe un polynôme unitaire $f \in \mathbb{Z}[X]$ de degré n tel que pour tout $i = 0, \dots, m$, on a $f \pmod{p_i} = \bar{f}_i$ dans $\mathbb{F}_{p_i}[X]$. Alors le théorème de spécialisation s'applique et nous dit que, pour chaque i , les substitutions de Frobenius en p_i appartiennent à $G_f \cap C_i$.
- Lorsque n est premier, on sait que $\mathfrak{S}_n$ est engendré par un n -cycle et une transposition quelconques. Il suffit donc d'appliquer la question précédente avec $C_1 = (n)$ et $C_2 = (2, 1, \dots, 1)$. En général, $\mathfrak{S}_n$ est engendré par un n -cycle, un $(n-1)$ -cycle et une transposition quelconques, et il suffit donc d'appliquer la question précédente à $C_1 = (n)$, $C_2 = (n-1, 1)$ et $C_3 = (2, 1, \dots, 1)$. Pour le voir, en supposant que le cycle est $c_n = (1, 2, \dots, n)$ (quitte à renuméroter), il suffit de générer la transposition $(1, 2)$. En conjuguant la transposition donnée par une puissance convenable de c_n , on obtient une transposition de la forme $(1, i)$. De même, en conjuguant le $(n-1)$ -cycle donné par une puissance convenable de c_n , on obtient un cycle c_{n-1} dont l'unique point fixe est 1. Mais alors, en conjuguant $(1, i)$ par une puissance convenable de c_{n-1} , on obtient la transposition $(1, 2)$ comme voulu.

Exercice 32. On veut montrer que le corps $\mathbb{C}(X)$ peut être plongé dans $\mathbb{C}$. Pour cela, notons $\Theta \subset \mathbb{C}$ une base de transcendance de $\mathbb{C}$ sur $\mathbb{Q}$.

- a) Expliquer pourquoi $\mathbb{C}$ est une clôture algébrique de $\mathbb{Q}(\Theta)$.
- b) Soit k un corps au plus dénombrable.
 - i) Montrer qu'une clôture algébrique de k est au plus dénombrable.
 - ii) Montrer que $k(X)$ est au plus dénombrable.
- c) i) Montrer que le degré de transcendance de $\mathbb{C}$ sur $\mathbb{Q}$ est infini.
 ii) En déduire que Θ est en bijection avec $\Theta \sqcup \{X\}$, puis construire un isomorphisme de corps $\mathbb{Q}(\Theta) \xrightarrow{\sim} \mathbb{Q}(\Theta)(X)$.
- d) Montrer que $\mathbb{C}(X)$ est isomorphe à un sous-corps de $\mathbb{C}$.
- e) Est-ce que $\overline{\mathbb{Q}}(X)$ est isomorphe à un sous-corps de $\overline{\mathbb{Q}}$?