M1-MF Exercices Algèbre - Corps et Théorie de Galois
Novembre 2020

Exercice 1. *Soit K un corps. Soit $\sigma : K \to K$ un automorphisme de K. Soit L un K-espace vectoriel.*

1. *Montrer que $(L, +)$, muni de la loi externe $(\alpha, x) \mapsto \sigma(\alpha).x$ est aussi un K-espace vectoriel, que l'on notera L'.*
2. *Montrer que si L est de dimension finie d, alors L' est aussi de dimension d.*
3. *En déduire que si K est un corps parfait de caractéristique $p > 0$, toute extension finie de K est un corps parfait.*
4. *Le résultat de 3. reste-t-il vrai pour une extension algébrique (pas forcément finie) ?*

Solution.

1. *Posons $\alpha \bullet x = \sigma(\alpha).x$. Comme σ est un morphisme de corps, on vérifie alors immédiatement les quatre axiomes requis :*
   $1 \bullet x = x$ *pour tout* $x \in L$.
   $\alpha \bullet (\beta \bullet x) = (\alpha\beta) \bullet x$ *pour tous* $\alpha, \beta \in K$ *et tout* $x \in L$.
   $\alpha \bullet (x + y) = \alpha \bullet x + \alpha \bullet y$ *pour tout* $\alpha \in K$ *et tous* $x, y \in L$.
   $(\alpha + \beta) \bullet x = \alpha \bullet x + \beta \bullet x$ *pour tous* $\alpha, \beta \in K$ *et tout* $x \in L$.
2. *Soit $(e_1, ..., e_d)$ une base du K-ev L, montrons que c'est aussi une base de L'. Si $\lambda_1, ..., \lambda_d$ dans K vérifient*
$$\sum_{i=1}^{d} \lambda_i \bullet e_i = 0,$$
   alors
$$\sum_{i=1}^{d} \sigma(\lambda_i).e_i = 0$$
   d'où $\sigma(\lambda_i) = 0$ pour tout i, puis $\lambda_i = 0$ puisque σ est injectif. Ainsi $(e_1, ..., e_d)$ est libre dans L'. Si maintenant $x \in L'$, on écrit $x = \sum_{i=1}^{d} \mu_i.e_i$ dans L avec $\mu_i \in K$, d'où $x = \sum_{i=1}^{d} \sigma^{-1}(\mu_i) \bullet e_i$ dans L', ce qui montre que la famille $(e_1, ..., e_d)$ est également génératrice dans L'.
3. *Par hypothèse, le morphisme de corps σ défini par $\sigma(x) = x^p$ est un automorphisme de K. Soit L une extension finie de K, qu'on peut voir comme un K-ev, notons L' le K-ev défini comme en a). Alors l'application $u : x \mapsto x^p$ est un morphisme du K-ev L dans le K-ev L' : en effet $u(x+y) = u(x)+u(y)$ résulte de ce qu'on est en caractéristique p ; si $\alpha \in K$ et $x \in L$, on a*
$$u(\alpha.x) = \alpha^p x^p = \sigma(\alpha).u(x) = \alpha \bullet x.$$
   Comme il est immédiat que $\ker u = 0$, u est injective et elle est donc bijective car $\dim L = \dim L'$ est finie. Ceci signifie exactement que $x \mapsto x^p$ est bijective de L dans L, et donc que L est parfait.
4. *Mais oui ! Si F est une extension algébrique de K et si $x \in F$, alors $L := K[x]$ est une extension finie de K puisque x est algébrique sur K. Appliquant alors c) à L, on obtient qu'il existe $y \in L \subset F$ tel que $y^p = x$. Ainsi, F est parfait.*

   Une autre méthode (vue en cours) consiste à observer qu'un corps K est parfait si et seulement si toute extension finie de K est séparable, propriété qui se conserve quand on fait une extension finie (ou algébrique) de K.

Exercice 2. *Soit L/K une extension de corps. Soit M le sous-corps de L constitué des éléments algébriques sur K. On suppose que tout polynôme irréductible de $K[X]$ est scindé sur L.*

1. *Montrer que tout polynôme de $K[X]$ est scindé sur M.*

2. *Soit F une extension finie de M. Montrer que tout $x \in F$ est algébrique sur K.*
3. *En déduire que M est un corps algébriquement clos.*

Solution.

1. *Il suffit de montrer que si $P \in K[X]$ est irréductible, alors il est scindé sur M. Or par hypothèse P est scindé sur L, et par ailleurs toute racine α de P dans L est par définition algébrique sur K, donc $\alpha \in M$; d'ù le résultat.*
2. *Si $x \in F$, alors x est algébrique sur M, donc il annule un polynôme unitaire de $M[X]$. Si $a_0, ..., a_r$ sont les coefficients de ce polynôme, alors x est algébrique sur $K(a_0, ..., a_r)$, qui est de dimension finie sur K puisque tous les a_i (qui sont dans M) sont algébriques sur K. En particulier $K(a_0, ..., a_r)[x]$ est de dimension finie sur $K(a_0, ..., a_r)$ et aussi sur K (par multiplicativité des degrés), ce qui implique que $K[x]$ est de dimension finie sur K. Finalement, x est algébrique sur K.*
3. *Avec les notations de b), x annule un polynôme irréductible π de $K[X]$ (son polynôme minimal sur K), et π est scindé sur M d'après a). Finalement $x \in M$, ce qui montre que la seule extension finie de M est M, et donc que M est algébriquement clos (sinon il y aurait un polynôme irréductible Q de degré au moins 2 dans $M[X]$, et $M[X]/(Q)$ serait une extension finie de M de degré ≥ 2).*

Exercice 3. *Soit K un corps. On note $\mathcal{I}$ l'ensemble des polynômes irréductibles unitaires de $K[X]$. On forme l'anneau de polynômes $A := K[(T_{P,i})_{P\in\mathcal{I}, 1\leq i\leq \deg P}]$ et pour tout $P \in \mathcal{I}$, on écrit dans $A[X]$:*

$$P - \prod_{i=1}^{\deg P} (X - T_{P,i}) = \sum_{j=0}^{\deg P - 1} a_{P,j} X^j,$$

où les $a_{P,j}$ sont dans A. On suppose par l'absurde que l'idéal I de A engendré par les $a_{P,j}$ est A et on va montrer qu'on aboutit à une contradiction.

1. *Montrer qu'il existe une partie finie $\mathcal{I}_1$ de $\mathcal{I}$ tels que l'idéal engendré par les $a_{P,j}$ avec $P \in \mathcal{I}_1$ soit égal à A.*
2. *Soit $Q = (\prod_{P\in\mathcal{I}_1} P) \in K[X]$ et soit L un corps de décomposition de Q sur K. Pour $P \in \mathcal{I}_1$, on pose*

$$P = \prod_{i=1}^{\deg P} (X - \alpha_{P,i}), \quad \alpha_{P,i} \in L.$$

Soit $A_1 \subset A$ l'anneau $K[(T_{P,i})_{P\in\mathcal{I}_1, 1\leq i\leq \deg P}]$. Montrer qu'il existe un morphisme de K-algèbres φ de A_1 dans L qui envoie chaque $T_{P,i}$ sur $\alpha_{P,i}$ pour tout $P \in \mathcal{I}_1$ et tout i avec $1 \leq i \leq \deg P$.

3. *Montrer que le morphisme $\tilde{\varphi} : A_1[X] \to L[X]$ induit par φ envoie $P - \prod_{i=1}^{\deg P}(X - T_{P,i})$ sur 0 (pour tout $P \in \mathcal{I}_1$), et aboutir à une contradiction.*

Soit maintenant J un idéal maximal de K contenant I (qui existe d'après ce qui précède), on note Ω le corps A/J, qui est une extension de K.

4. *Montrer que tout polynôme irréductible de K est scindé sur Ω.*
5. *En utilisant l'exercice 2., montrer que K admet une clôture algébrique (théorème de Steinitz).*
6. *Montrer que si F et F' sont deux clôtures algébriques de K, elles sont isomorphes (on appliquera le lemme de Zorn aux K-morphismes de E dans F', où E est une extension intermédiaire entre K et F).*

Solution.

1. *Comme l'idéal engendré par tous les $a_{P,j}$ est A, on peut écrire 1 comme combinaison linéaire Ãă coefficients dans A d'un nombre fini de ces $a_{P,j}$, correspondant Ãă des P dans une partie finie $\mathcal{I}_1$ de $\mathcal{I}$. L'idéal engendré par les $a_{P,j}$ pour $P \in \mathcal{I}_1$ (et toujours $0 \leq j < \deg P$) contient alors 1, donc est égal Ãă A.*
2. *Malgré les notations effrayantes, il s'agit tout simplement de la propriété universelle d'un anneau de polynômes !*

3. *Comme $P \in K[X]$, on a $\tilde{\varphi}(P) = P$. Par ailleurs*

$$\tilde{\varphi}(\prod_{i=1}^{\deg P}(X - T_{P,i})) = \prod_{i=1}^{\deg P}(X - \alpha_{P,i}) = P.$$

Ainsi, $\tilde{\varphi}$ envoie $P - \prod_{i=1}^{\deg P}(X - T_{P,i})$ sur 0. Par définition des $a_{P,j}$, cela donne $\varphi(a_{P,j}) = 0$ pour tout $P \in \mathcal{I}_1$ (et tout $j \in [0, \deg P[$). Comme ces $a_{P,j}$ engendrent l'idéal A de A, on obtient $\varphi(A) = 0$, ce qui n'est pas possible puisque $\varphi(1) = 1$.

4. *Si P est un polynôme irréductible de K (qu'on peut supposer unitaire), alors comme dans A/J l'image de tous les $a_{P,j}$ est nulle (puisque J contient I), on obtient*

$$P = \prod_{i=1}^{\deg P}(X - u_i),$$

ù u_i est l'image de $T_{P,i}$ dans $\Omega = A/J$. Ceci montre que P est scindé sur Ω.

5. *On vient de trouver une extension Ω de K telle que tout polynôme irréductible de $K[X]$ soit scindé sur Ω. D'après l'exercice 2., l'ensemble $\overline{K}$ des éléments de Ω algébriques sur K est un corps algébriquement clos, et comme c'est une extension algébrique de K, c'est une clôture algébrique de K.*

6. *On considère l'ensemble S des paires (E, i),où $K \subset E \subset F$ et $i : E \to F'$ est un morphisme de corps. On ordonne S par $(E_1, i_1) \leq (E_2, i_2)$ si $E_1 \subset E_2$ et i_2 prolonge i_1. Il est alors immédiat que toute famille non vide totalement ordonnée de S admet un majorant (si (E_j, i_j) est une telle famille, on prend pour majorant (E, i)où E est la réunion des E_j et i le morphisme qui coïncide avec i_j sur chaque E_j). D'après le lemme de Zorn, S possède donc un élément maximal (E_0, i_0). Montrons que $E_0 = F$. Si on avait un $x \in F \setminus E_0$, alors le polynôme minimal de x (qui est algébrique sur K) aurait une racine x' dans F' (qui est algébriquement clos et contient K), ce qui permettrait de prolonger i_0 en un K-morphisme de corps de $E_0[x]$ dans F' en envoyant x sur x', ce qui contredit la maximalité. On obtient donc finalement un morphisme de corps $i_0 : F \to F'$. Mais alors, comme tout élément de F' est algébrique sur K, donc sur F, le fait que F soit algébriquement clos implique que i_0 est un isomorphisme.*

Exercice 4. *Soit K un corps. Soient K_1, K_2 deux extensions de K (c'est-àă-dire que ce sont des corps qui sont en même temps des K-algèbres). On dit que K_1 et K_2 sont linéairement disjointes sur K si la K-algèbre $K_1 \otimes_K K_2$ est un anneau intègre.*

1. *On suppose que $K_1 \simeq K[X]/(P)$, où P est un polynôme irréductible sur K. Donner une condition nécessaire et suffisante sur P pour que K_1 et K_2 soient linéairement disjointes.*
2. *Les extensions $\mathbb{Q}(i)$ et $\mathbb{Q}(\sqrt{2})$ sont-elles linéairement disjointes sur $\mathbb{Q}$? Même question pour $\mathbb{Q}(\sqrt[3]{2})$ et $\mathbb{Q}(j\sqrt[3]{2})$.*

Solution.

1. *Comme on l'a vu en cours, $K[X]/(P) \otimes_K K_2$ est isomorphe àă $K_2[X]/(P)$. La condition est donc que P (qui est irréductible dans K puisque K_1 est un corps) reste irréductible dans K_2.*
2. *D'après a), $\mathbb{Q}(i)$ et $\mathbb{Q}(\sqrt{2})$ sont linéairement disjointes sur $\mathbb{Q}$, en prenant $P = X^2+1$, qui est bien irréductible sur $\mathbb{Q}(\sqrt{2})$. Ce n'est pas le cas de $\mathbb{Q}(\sqrt[3]{2})$ et $\mathbb{Q}(j\sqrt[3]{2})$, le polynôme $X^3 - 2$ n'étant pas irréductible dans $\mathbb{Q}(j\sqrt[3]{2})$ (il a une racine dans ce corps).*

Exercice 5. *Soit K un corps infini. Soit L un surcorps de K, on suppose qu'il n'existe qu'un nombre finis de corps M avec $K \subset M \subset L$. On veut montrer qu'il existe $a \in L$ tel que $L = K(a)$.*

1. *Montrer que l'extension L/K est finie.*
2. *On suppose que $L = K(\alpha_1, \alpha_2)$ avec $\alpha_1, \alpha_2 \in K$. En considérant les corps $K(\alpha_1 + \beta\alpha_2)$ avec $\alpha \in K$, montrer que l'un de ces corps est égal à L.*
3. *En déduire le résultat annoncé.*

4. *Soit réciproquement $L = K(\alpha)$ une extension de K engendrée par un élément α. Soit M une extension intermédiaire entre K et L. On note P le polynôme minimal de α sur K et P_M son polynôme minimal sur M. Montrer que P_M divise P dans $L[T]$ et que l'application $M \mapsto P_M$ est injective.*
5. *En déduire qu'il n'y a qu'un nombre fini de telles extensions intermédiaires M.*
6. *Montrer que $\mathbb{F}_p(X,Y)$ admet une extension finie qui n'est pas engendrée par un élément (autrement dit le théorème de l'élément primitif tombe en défaut sur ce corps imparfait).*

Solution.

1. *Comme tous les éléments de L sont supposés algébriques sur K, on a $K(a_1,...,a_r)$ de dimension finie sur K pour tous $a_1,...,a_r$ de L. Si L est de dimension infinie sur K, cela permet de construire une suite infinie strictement croissante*
$$K(a_1) \subset K(a_1,a_2), \subset K(a_1,a_2,...,a_n) \subset ...$$
de corps intermédiaires entre K et L, ce qui contredit l'hypothèse.
2. *Comme K est infini et le nombre d'extensions intermédiaires est fini, il existe $\beta \neq \beta'$ dans K tels que $K(\alpha_1+\beta\alpha_2) = K(\alpha_1+\beta'\alpha_2)$. Posons $M = K(\alpha_1+\beta\alpha_2)$, alors*
$$(\alpha_1+\beta'\alpha_2) - (\alpha_1+\beta\alpha_2) \in M$$
d'ù $\alpha_2 \in M$ (vu que $(\beta-\beta') \in K^*$) et
$$\alpha_1 = \alpha_1+\beta\alpha_2-\beta\alpha_2 \in M$$
. On en déduit que $M = L$.
3. *Comme L est de dimension finie sur K, on peut trouver $\alpha_1,...,\alpha_n$ dans L tels que $L = K(\alpha_1,...,\alpha_n)$. Le b) donne alors par récurrence sur n que L s'écrit $K(\alpha)$ avec $\alpha \in L$.*
4. *Comme $P \in M[X]$ et $P(\alpha) = 0$, on obtient par définition du polynôme minimal que P_M divise P dans $M[T]$, donc aussi dans $L[T]$. Soient maintenant M et N des extensions intermédiaires telles que $P_M = P_N$. Supposons d'abord que $N \subset M$, alors comme $L = M[\alpha]$ et P_M est le polynôme minimal de α sur M, on a $\deg P_M = [L:M]$ et de même pour N, ce qui implique $[L:M] = [L:N]$, puis $[M:K] = [L:K]$ par multiplicativité des degrés. D'où $M = N$ dans ce cas puisque $N \subset M$ et ces deux K-espaces vectoriels ont même dimension. On se ramène au cas où $N \subset M$ en considérant $N' = N \cap M$, qui vérifie encore l'hypothèse que $P_{N'} = P_M$, puisque $P_M \in N'[X]$ annule α et est le minimal de α sur M, donc a fortiori sur N'.*
5. *C'est une conséquence de d), vu que P n'a qu'un nombre fini de diviseurs unitaires dans $L[T]$ (décomposer P en produit de facteurs irréductibles unitaires).*
6. *Posons $K = \mathbb{F}_p(X,Y)$ et prenons pour L le corps de décomposition du polynôme $(T^p-X)(T^p-Y)$ sur K. Ainsi $L = K(a,b)$ avec $a^p = X$ et $b^p = Y$. On constate alors que pour tout $m \in \mathbb{N}$, l'extension $M_m := K(a+X^m b)$ est intermédiaire entre K et L. Or, pour $m < n$, les extensions M_m et M_n sont distinctes, sinon M_m contiendrait $(X^n-X^m)b$, donc aussi b puisque $(X^n-X^m) \in K^*$. Alors M_m contiendrait aussi $a = a+X^m b - X^m b$, et on aurait finalement $M_m = L$. Mais ceci n'est pas possible car $a+X^m b$ annule le polynôme $Q = T^p - (X+YX^{mp})$ qui est de degré p, donc $M_m = K(a+X^m b)$ est de degré au plus p sur K, tandis que L est de degré p^2 sur K. Finalement, il y a une infinité d'extensions intermédiaires entre K et L, et on conclut avec 5.*

Exercice 6. *Montrer que le polynôme X^4+1 est irréductible sur $\mathbb{Q}$. Soit L un corps de rupture pour ce polynôme ; comment X^4+1 se factorise-t-il sur L ?*

Solution. *Les racines de $P = X^4+1$ sont $z_1 = e^{i\frac{\pi}{4}}$, $z_2 = e^{i\frac{-\pi}{4}} = \overline{z_1}$, $z_3 = e^{i\frac{3\pi}{4}}$, $z_4 = e^{i\frac{-3\pi}{4}} = \overline{z_3}$; elle ne sont pas dans $\mathbb{Q}$, donc P n'a pas de facteur de degré 1. Un corps de rupture de P est $\mathbb{Q}(\omega)$ où $\omega = e^{i\frac{\pi}{4}}$; comme les autres racines de P sont ω^3, ω^5 et ω^7 qui appartiennent évidement à $\mathbb{Q}(\omega)$, P se décompose sur le corps de rupture $\mathbb{Q}(\omega)$ qui est alors aussi son corps de décomposition. On a $P = (X-\omega)(X-\omega^3)(X-\omega^5)(X-\omega^7)$ dans $\mathbb{Q}(\omega)$.*

Exercice 7. *Soit p un nombre premier, et soit $K = \mathbb{F}_p(T)$, où T est un élément transcendant sur $\mathbb{F}_p$. Montrer que $X^p - T$ est irréductible sur K. Soit L un corps de rupture de ce polynôme ; comment le polynôme se factorise-t-il sur L ?*

Solution. *Le polynôme $P = X^p - T$ est irréductible dans $\mathbb{F}_p(T)[X]$ car $T \in \mathbb{F}_p(T) - \mathbb{F}_p(T)^p$.*
En effet, supposons que $Q \in \mathbb{F}_p(T)[X]$ soit un facteur irréductible de P. Si x est une racine de $P = X^p - T$ dans un corps de rupture L, on a $x^p = T$ donc $P(X) = X^p - x^p = (X - x)^p$ dans $L[X]$; donc forcément $Q = (X - x)^i$ avec $1 \leq i \leq p$. comme $x \notin K$, on a que $i \geq 2$ et donc Q n'est pas séparable, ce qui implique que $Q \in K[X^p]$ (en calculant la dérivé de Q on a que les seuls coefficients non nuls de Q sont les puissances de p), donc le degré de Q est un multiple de p et donc $i = p$. On a donc bien $P = Q$ et P est irréductible.
Sur $L[X]$, $P = (X - x)^p$.

Exercice 8.
1. *Montrer que pour tous nombres rationels a et b, $\mathbb{Q}(\sqrt{a}, \sqrt{b}) = \mathbb{Q}(\sqrt{a} + \sqrt{b})$.*
2. *A-t-on que $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}) = \mathbb{Q}(\sqrt{2} + \sqrt{3} + \sqrt{5})$?*
3. *Calculer le degré de $\sqrt{2} + \sqrt[3]{3}$.*

Solution.

1. *Les deux réels $\sqrt{a}$ et $\sqrt{b}$ sont algébriques sur $\mathbb{Q}$ car elles annulent les polynômes $X^2 - a$ et $X^2 - b$ respectivement. Comme $\sqrt{a} + \sqrt{b} \in \mathbb{Q}(\sqrt{a}, \sqrt{b})$ on a $\mathbb{Q}(\sqrt{a} + \sqrt{b}) \subset \mathbb{Q}(\sqrt{a} + \sqrt{b})$. Calculons le degré de l'extension $\mathbb{Q}(\sqrt{a}, \sqrt{b})/\mathbb{Q}$. On doit distinguer trois cas :*
   (a) *Si a et b sont des carrés dans $\mathbb{Q}^*$ alors $\mathbb{Q}(\sqrt{a}) = \mathbb{Q}(\sqrt{b}) = \mathbb{Q}(\sqrt{a}, \sqrt{b}) = \mathbb{Q}(\sqrt{a}, \sqrt{b}) = \mathbb{Q}$.*
   (b) *Si a n'est pas un carré dans $\mathbb{Q}^*$ mais b est un carré dans $\mathbb{Q}^*$, alors $[\mathbb{Q}(\sqrt{a}, \mathbb{Q}] = 2$ et $\sqrt{a} + \sqrt{b} \in \mathbb{Q}(\sqrt{a}) = \mathbb{Q}(\sqrt{b})(\sqrt{a})$, donc $\mathbb{Q}(\sqrt{a} + \sqrt{b})$ est une sous-extension de $\mathbb{Q}(\sqrt{a})$ qui n'est pas de degré 1 car $\sqrt{a} \notin \mathbb{Q}$, donc elle est de degré 2 et $\mathbb{Q}(\sqrt{a}, \sqrt{b}) = \mathbb{Q}(\sqrt{a} + \sqrt{b})$. C'est pareil si on inverse les rôles de a et b.*
   (c) *Supposons que ni a ni b soient des carrés dans $\mathbb{Q}$ de sorte que $[\mathbb{Q}(\sqrt{a}, \mathbb{Q}] = [\mathbb{Q}(\sqrt{b}), \mathbb{Q}] = 2$. Regardons l'extension $\mathbb{Q}(\sqrt{b})(\sqrt{a})$ de $\mathbb{Q}(\sqrt{b})$. Le polynôme $X^2 - a$ est irréductible sur $\mathbb{Q}(\sqrt{b})$ si et seulement si a n'est pas un carré dans $\mathbb{Q}(\sqrt{b})$. Or,*

$$\begin{aligned} a \in (\mathbb{Q}^*)^2 &\iff \exists p, q \in Q \,|\, (p + q\sqrt{b})^2 = a \\ &\iff \exists p, q \in Q \,|\, p^2 + 2pq\sqrt{b} + q^2 b = a \\ &\iff \exists p, q \in Q \,|\, p^2 + q^2 = a \; et \; 2pq = 0 \\ &\iff \exists p \in \mathbb{Q} \,|\, p^2 = a \; ou \; \exists q \in \mathbb{Q}, q^2 = \frac{a}{b} \end{aligned}$$

   On a alors que $\frac{a}{b}$ est un carré si est seulement si $\mathbb{Q}$, $[\mathbb{Q}(\sqrt{b})(\sqrt{a}) : \mathbb{Q}(\sqrt{b})] = 1$ et $[\mathbb{Q}(\sqrt{b}, \sqrt{a}) : \mathbb{Q}] = 2$. Dans ce cas, soit $\lambda \in \mathbb{Q}$ tel que $a = \lambda^2 b$. Alors $\sqrt{a} + \sqrt{b} = (1 + \frac{1}{\lambda})\sqrt{a}$ et $\sqrt{a} = \frac{1}{1 + \frac{1}{\lambda}}$ donc $\mathbb{Q}(\sqrt{a} + \sqrt{b}) = \mathbb{Q}(\sqrt{a}) = \mathbb{Q}(\sqrt{a}, \sqrt{b})$.
   Supposons maintenant que ni a ni b ni $\frac{a}{b}$ sont des carrés dans $\mathbb{Q}$. Alors a n'est pas un carré dans $\mathbb{Q}(\sqrt{b})$, $\mathbb{Q}(\sqrt{a}) \neq \mathbb{Q}(\sqrt{b})$ et donc $X^2 - a$ est irréductible sur $\mathbb{Q}(\sqrt{b})[X]$, donc $[\mathbb{Q}(\sqrt{b}, \sqrt{a}) : \mathbb{Q}(\sqrt{b})] = 2$ et $\{1, \sqrt{a}\}$ est une $\mathbb{Q}(\sqrt{b})$-base de $\mathbb{Q}(\sqrt{a}, \sqrt{b})$. De même, si $\frac{a}{b}$ n'est pas un carré dans $\mathbb{Q}$, $\frac{b}{a}$ non plus, donc $[\mathbb{Q}(\sqrt{a}, \sqrt{b}) : \mathbb{Q}(\sqrt{a})] = 2$ et $\{1, \sqrt{b}\}$ est une $\mathbb{Q}(\sqrt{a})$-base de $\mathbb{Q}(\sqrt{a}, \sqrt{b})$. Par le Théorème de la base télescopique on a $[Q(\sqrt{b}, \sqrt{a}) : \mathbb{Q}] = 4$ et $\{1, \sqrt{a}, \sqrt{b}, \sqrt{ab}\}$ est une $\mathbb{Q}$-base de $\mathbb{Q}(\sqrt{a}, \sqrt{b})$.

   Comme $\sqrt{a} + \sqrt{b} \in \mathbb{Q}(\sqrt{a}, \sqrt{b})$, $\sqrt{a} + \sqrt{b}$ est algébrique sur $\mathbb{Q}$ de degré divisant 4. En regardant les coordonnées de 1, $\sqrt{a} + \sqrt{b}$ et $(\sqrt{a} + \sqrt{b})^2$ dans la base $\{1, \sqrt{a}, \sqrt{b}, \sqrt{ab}\}$, on voit que $\{2, \sqrt{a} + \sqrt{b}, (\sqrt{a} + \sqrt{b})^2\}$ est une famille $\mathbb{Q}$-libre et donc le degré de $\sqrt{a} + \sqrt{b}$ est strictement plus grand que 2 ; c'est donc 4 et donc $\mathbb{Q}(\sqrt{a} + \sqrt{b}) = \mathbb{Q}(\sqrt{a}, \sqrt{b})$.
   En calculant $(\sqrt{a} + \sqrt{b})^2$ on trouve que $\sqrt{a} + \sqrt{b}$ est racine de $P(X) = X^4 - 2(a + b)X^2 + (a - b)^2$ qui est alors son polynôme minimal.

2. *On a* $\alpha = \sqrt{2}+\sqrt{3}+\sqrt{5} \in \mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5})$ *et l'extension* $\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5})$ *est galoisienne de degré* 8 *(c'est un corps de décomposition de* $(X^2-2)(X^2-3)(X^2-5)$ *sur* $\mathbb{Q}$*) et son groupe de Galois est isomorphe à* $(\mathbb{Z}/2\mathbb{Z})^3$*. En regardant l'action du groupe de Galois sur les générateurs de l'extension (*$\sqrt{2}$*,* $\sqrt{3}$*,* $\sqrt{5}$*) on voit que* α *admet bien* 8 *conjugués distincts donc* $[\mathbb{Q}(\alpha):\mathbb{Q}] = 8$ *et* $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5})$*.*

3. *Première méthode : posons* $\alpha = \sqrt{2}+\sqrt[3]{3}$*. Le polynôme minimal de* α *sur* $\mathbb{Q}$ *est* X^3-3*. On peut voir* X^3-3 *comme polynôme sur* $\mathbb{Z}[\sqrt{2}]$ *et par Einsentien il y est irréductible, c'est donc le polynôme minimal de* $\sqrt[3]{3}$ *sur* $\mathbb{Q}(\sqrt{2})$*. Ceci implique que* $P(X) = (X-\sqrt{2})^3-3$ *est encore irréductible sur* $\mathbb{Z}[\sqrt{2}]$ *et c'est le polynôme minimal de* $\alpha = \sqrt{2}+\sqrt[3]{3}$ *sur* $\mathbb{Z}[\sqrt{2}]$*. On a alors les inclusions* $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\alpha) \subset \mathbb{Q}(\sqrt{2})(\sqrt[3]{3}) = \mathbb{Q}(\sqrt{2},\sqrt[3]{3})$ *et les degrés :* $[\mathbb{Q}(\alpha):\mathbb{Q}] = [\mathbb{Q}(\alpha):\mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}):\mathbb{Q}] = 3\times 2 = 6$*.*
Deuxième méthode : on a $\mathbb{Q}(\alpha) \subset \mathbb{Q}(\sqrt{2},\sqrt[3]{3})$*. Montrons l'inclusion inverse en montrant que* $a = \sqrt{2}$ *et* $b = \sqrt[3]{3}$ *sont des fonctions rationnelles sur* α*. On a* $(\alpha-a)^3 = (\sqrt{2}+\sqrt[3]{3}-\sqrt{2})^3 = 3$ *donc* $\alpha^3-3a\alpha^2+12\alpha-2a = 3$ *donc* $a = \frac{3-c^3-12c}{(-3c^2-2)}$ *et* $a \in \mathbb{Q}(\alpha)$*. De plus,* $a+b = \alpha$ *donc* $b = \alpha - c$ *et donc* $b \in \mathbb{Q}(\alpha)$*. Ceci montre aussi que le degré de* $\mathbb{Q}(\alpha)$ *est égal à* 6*.*

Exercice 9. *On considère l'extension* $\mathbb{Q}(i,\sqrt[4]{2})$ *de* $\mathbb{Q}$*.*

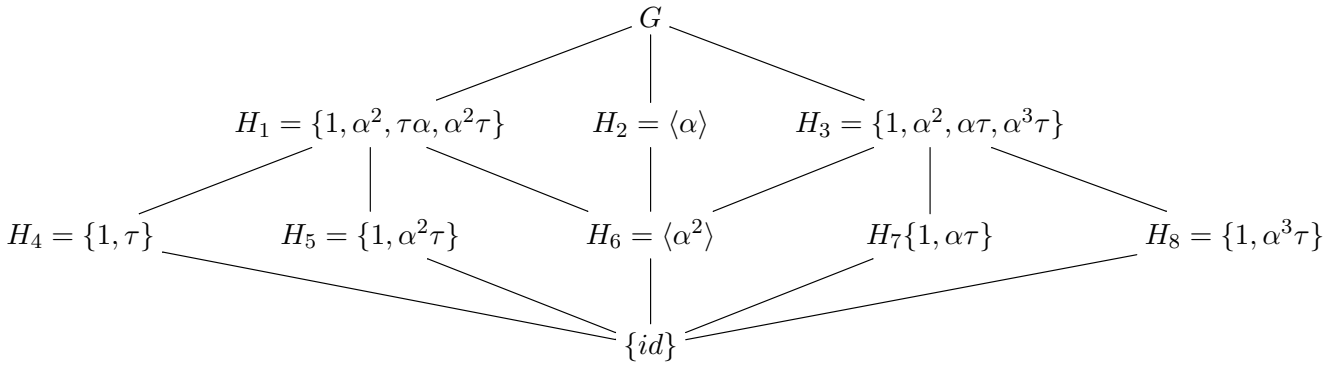
1. *Montrer que le groupe de Galois de cette extension est égal au produit semi-direct* $\langle\alpha\rangle \rtimes \{1,\tau\}$*, où* τ *est la conjugaison complexe et où* $\alpha(\sqrt[4]{2}) = i\sqrt[4]{2}$ *et* $\alpha(i) = i$*.*
2. *Montrer que cette extension est galoisienne.*
3. *Donner le treillis des sous-groupes de* $Gal(\mathbb{Q}(i,\sqrt[4]{2})/\mathbb{Q})$*.*
4. *Donner le treillis des extensions de* $\mathbb{Q}$ *contenues dans* $\mathbb{Q}(i,\sqrt[4]{2})$*.*

Solution. *Soit* $P = X^4-2$ *vu comme polynôme dans* $\mathbb{Q}[X]$ *et soit* K *un corps de décomposition de* P*.* P *est irréductible sur* $\mathbb{Q}$ *par Eisenstein et* $w = \sqrt[4]{2}$ *est une racine positive réelle de* P*. Les zéros de* P *dans* $\mathbb{C}$ *sont :* w*,*$-w$*,*iw *et* $-iw$*. Comme* $\frac{iw}{w} = i$ *on a* $i \in K$*. Comme* $\mathbb{Q}(w,i)$ *contient tous les zéros de* P *on a que* $K = \mathbb{Q}(w,i)$ *et comme* P *est séparable, on a que* K *est bien galoisienne. Calculons le degré de* K *comme extension de* $\mathbb{Q}$*. Soit* $E = \mathbb{Q}(w)$*. Comme* P *est irréductible sur* $\mathbb{Q}$*,* $[\mathbb{Q}(w):\mathbb{Q}] = 4$ *et* $\{1,w,w^2,w^3\}$ *est une* $\mathbb{Q}$*-base de* E*. Le polynôme minimal de* i *sur* E *est* X^2+1 *car* $E \subset \mathbb{R}$ *et* $\{1,i\}$ *est une* $\mathbb{Q}(w)$*-base de* $\mathbb{Q}(w,i)$*. On a alors que* $[K:E] = 2$ *et donc par le Théorème de la base télescopique* $[K:\mathbb{Q}] = 8$*. Une base de* K *sur* $\mathbb{Q}$ *est* $\{1,w,w^2,w^3,i,iw,iw^2,iw^3\}$*. Comme* K *est galoisienne : le groupe de Galois de* $K/\mathbb{Q}$ *est un groupe d'ordre* 8*. Notons* G *ce groupe de Galois. Tout élément* σ *de* G *est complètement déterminé par son action sur les éléments de la base* $\{1,w,w^2,w^3,i,iw,iw^2,iw^3\}$ *et donc ses valeurs sont déterminées par* $\sigma(w)$ *et* $\sigma(i)$ *car* σ *est un automorphisme. Le polynôme minimal de* i *sur* $\mathbb{Q}(w)$ *étant* X^2+1*, on a que* σ *doit envoyer* i *sur* i *ou sur* $-i$*. Posons* $\alpha(w) = iw$ *et* $\tau(i) = -i$ *(*τ *est un élément de* G *d'ordre* 2*). On peut donc écrire le tableau suivant qui donne l'action des éléments de* G *sur* w *et* i *:*

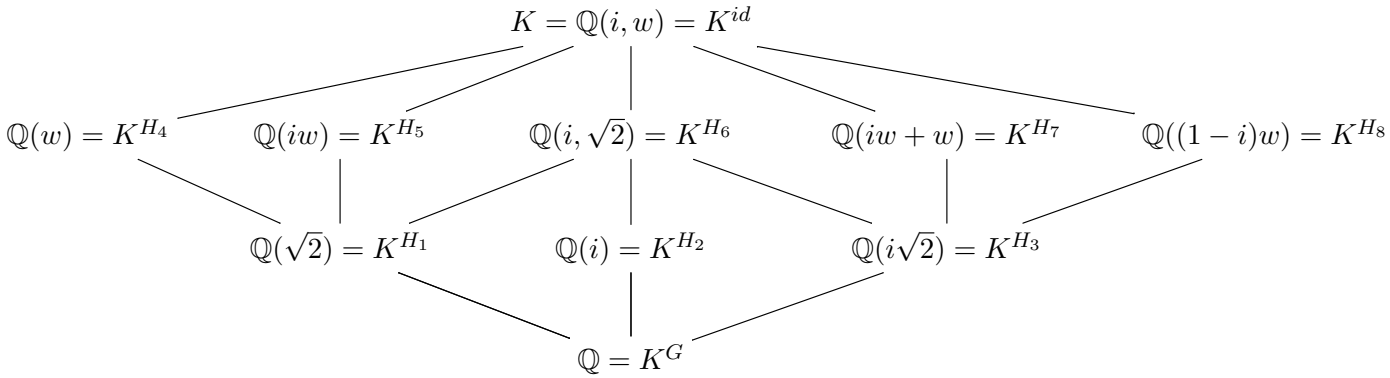
σ	id	α	α^2	α^3	τ	$\alpha\tau$	$\alpha^2\tau$	$\alpha^3\tau$
$\sigma(w)$	w	iw	-w	-iw	w	iw	-w	-iw
$\sigma(i)$	i	i	i	i	$-i$	$-i$	$-i$	$-i$

Pour identifier G*, on voit d'abord qu'il n'est pas abélien : par exemple* $\tau\alpha(w) = \tau(iw) = -iw$ *alors que* $\alpha\tau(w) = \alpha(w) = iw$*. De même, on voit facilement que* α *est d'ordre* 4 *et que* τ *est d'ordre* 2 *(*τ *est la conjugaison complexe) et que la relation suivante est vérifiée :* $\alpha\tau = \tau\alpha^3$*. On a donc que* $G = \langle\alpha\rangle \rtimes \{\tau\} = \{\alpha,\tau \mid \alpha^4 = 1, \tau^2 = 1, \alpha\tau = \tau\alpha^3\}$*. On aurait pu aussi remarquer que l'extension* $\mathbb{Q}(i,w)/\mathbb{Q}$ *est de Kummer :* $\mathbb{Q}(i)$ *contient les racines* 4*-ièmes de l'unité et* w *est racine de* X^4-2*. Comme de plus* $\mathbb{Q}(i)$ *ne contient aucune racine* 2*-ième de* 2*, cette extension est galoisienne et son groupe de Galois, que l'on note* $G(\mathbb{Q}(i,w)/\mathbb{Q})$ *est cyclique d'ordre* 4 *et il est engendré par l'automorphisme* α *de* $\mathbb{Q}(i,w)$ *qui laisse fixe les éléments de* $\mathbb{Q}(i)$ *et qui vérifie* $\alpha(w) = w$*. C'est un sous-groupe distingué de* G *car* $\mathbb{Q}(i)/\mathbb{Q}$ *est galoisienne (donc c'est une extension finie normale). Par ailleurs, si on considère le groupe engendré par* τ*, on a* $\langle\alpha\rangle\cap\tau = \{id\}$*,* $\langle\alpha\rangle.\langle\tau\rangle = G$ *et comme* $\langle\alpha\rangle$ *est distingué dans* G*, on a que* $G \simeq \langle\alpha\rangle \rtimes \langle\tau\rangle$*.*

Le treillis des sous-groupes de G s'écrit alors :



Par correspondance de Galois le treillis des sous-extensions de $\mathbb{Q}(i, w)$ est :



Pour trouver le treillis des sous-extensions on doit trouver les sous-corps de K suivants : $K^{H_i} = \{x \in K \mid \sigma(x) = x, \forall \sigma \in H_i\}$ pour tout $i = 1, 2, 3, 4, 5, 6, 7, 8$. Pour simplifier les notations posons $r_0 = id$, $r_1 = \alpha$, $r_2 = \alpha^2$, $r_3 = \alpha^3$, $u_1 = \tau$, $d_1 = \alpha\tau$, $u_2 = \alpha^2\tau$, $d_2 = \alpha^3\tau$ les éléments de G.

- *K^{H_2} (ce sont les éléments fixes par $\langle\alpha\rangle$ est une extension de degré 2 car H_2 est un sous-groupe d'ordre 4 et donc d'indice 2 (il est distingué dans G. Comme $\alpha^n(i) = i$ pour $n = 0, 1, 2, 3$ on conclut que $K^{H_2} = \mathbb{Q}(i)$.*
- *Comme H_4 est un groupe d'indice 4, K^{H_4} est une extension de degré 4 sur $\mathbb{Q}$. Comme $\tau(w) = w$ alors $\mathbb{Q}(w)$ est fixée par τ et id et que $[\mathbb{Q}(w) : \mathbb{Q}] = 4$, le Théorème de Galois dit que c'est la seule, donc $K^{H_4} = \mathbb{Q}(w)$.*
- *On sait que K^{H_7} est un extension de degré 4 sur $\mathbb{Q}$ car $H_7 = \{id, \alpha\tau\}$ est un groupe d'ordre 2. Si on calcule l'action de $\alpha\tau$ sur les éléments de $\{1, w, w^2, w^3, i, iw, iw^2, iw^3\}$ qui est une $\mathbb{Q}$-base de K on a $\{1, iw, -w^2, -iw^3, -i, , w, iw^2, -w\}$ et on voit que les éléments w et iw sont permutés par $\alpha\tau$. Ceci implique que $\alpha\tau(w+iw) = iw+w$ ie. $w+iw$ est stable par $\alpha\tau$ et donc $\mathbb{Q}(w+iw) \subset K^{H_7}$. Mais $[Q(w+iw) : \mathbb{Q}] = 4$: en effet, on aimerait trouver le polynôme minimal S de $\gamma = w + iw$ pour avoir le degré de cette extension. Pour tout conjugué γ' de γ sur $\mathbb{Q}$ il existe un élément $\sigma \in G$ tel que $\sigma(\gamma) = \gamma'$, donc pour trouver les racines de S on calcule $\sigma(\gamma)$, pour tout $\sigma \in G$; il suffit de calculer $\sigma(\gamma)$ pour σ dans un ensemble de représentants du quotient $G/H_7 = \{\overline{r_0}, \overline{r_1}, \overline{r_2}, \overline{r_3}\}$. On trouve alors que les conjugués de γ sont : γ, $-w + iw$, $iw - w$, $-w - iw$ et $-iw + w$ et donc que $S = X^4 + 8$.*

Exercice 10 (Calcul de groupes de Galois)**.** *Déterminer le groupe de Galois de chacune des extensions de corps ou chacun des polynômes suivants.*

1. *$\mathbb{Q}(\sqrt{2}, \sqrt{3})$ sur $\mathbb{Q}$.*
2. *$X^3 - 10$ sur $\mathbb{Q}$, puis sur $\mathbb{Q}(\sqrt{2})$.*

3. $X^3 - X - 1$ *sur* $\mathbb{Q}$.
4. $X^n - t$ *sur* $\mathbb{C}(t)$, *puis sur* $\mathbb{R}(t)$ *(où* t *est transcendant sur* $\mathbb{C}$*).*
5. $X^5 - pqX + p$ *sur* $\mathbb{Q}$, *où* p *est un nombre premier et* $q \geq 2$ *est un entier.*

Remarque *: le livre* Algebra *de Serge Lang contient des dizaines d'exercices de ce type.*

Solution.

1. $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ *est un extension galoisienne sur* $\mathbb{Q}$ *de degré* 4 *sur* $\mathbb{Q}$ *(c'est le corps de décomposition de* $(X^2 - 2)(X^2 - 3)$*) et* $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ *est une* $\mathbb{Q}$*-base de* K*. Le groupe de Galois* G *de* K *est le groupe* $\{\iota = id, \sigma_1, \sigma_2, \sigma_3\}$*, où* $\sigma_1 : a + b\sqrt{2} \in \mathbb{Q}(\sqrt{3})(\sqrt{2}) \mapsto a - b\sqrt{2} \in \mathbb{Q}(\sqrt{3})(\sqrt{2})$*,* $\sigma_2 : a + b\sqrt{3} \in \mathbb{Q}(\sqrt{2})(\sqrt{3}) \mapsto a - b\sqrt{3} \in \mathbb{Q}(\sqrt{2})(\sqrt{3})$ *et* $\sigma_3 = \sigma_1 \circ \sigma_2$*. On écrivant la table de groupe de* G*, on a*

$\circ$	ι	σ_1	σ_2	σ_3
ι	ι	σ_1	σ_2	σ_3
σ_1	σ_1	ι	σ_3	σ_2
σ_2	σ_2	σ_3	ι	σ_1
σ_3	σ_3	σ_2	σ_1	ι

   Et on voit que G *est isomorphe à* $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$*.*
2. $P = X^3 - 10 = (X - \sqrt[3]{10})(X - \xi\sqrt[3]{10})(X - \xi^2\sqrt[3]{10})$ *où* ξ *est une racine* 3*-ième de l'unité non triviale. Le corps de décomposition de* P *est* $\mathbb{Q}(\sqrt[3]{10}, \xi)$*. L'extension* $\mathbb{Q}(\xi)/\mathbb{Q}$ *est cyclotomique donc galoisienne de degré* ξ *(le polynôme minimal de* ξ *est* $X^2 + X + 1$*) et le groupe de Galois de* $\mathbb{Q}(\xi)/\mathbb{Q}$ *est* $\{1, \tau\}$ *où* τ *est la conjugaison. L'extension* $\mathbb{Q}(\xi)(\sqrt[3]{10})/\mathbb{Q}(\xi)$ *est de Kummer de degré* 3*, son groupe de Galois est* $\{1, \alpha, \alpha^2\}$ *où* $\alpha(\sqrt[3]{10}) = \xi\sqrt[3]{10}$*. On conclut alors que le groupe de Galois de* P *sur* $\mathbb{Q}$ *est* $\{1, \alpha, \alpha^2, \tau, \tau\alpha, \tau\alpha^2\}$ *qui est isomorphe à* $\mathcal{S}_3$*. Pour calculer le groupe de Galois sur* $\mathbb{Q}(\sqrt{2})$ *on considère la tour d'extensions* $\mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{2}\xi) \to \mathbb{Q}(\sqrt{2}, \xi, \sqrt[3]{10})$ *et le même raisonnement permet de dire que le groupe de Galois sur* $\mathbb{Q}(\sqrt{2})$ *est aussi* $\{1, \alpha, \alpha^2, \tau, \tau\alpha, \tau\alpha^2\}$*.*
3. $X^3 - X + 1$ *est irréductible sur* $\mathbb{Q}$ *et n'a qu'une seule racine réelle sont groupe de Galois* G *est alors isomorphe à* $\mathcal{S}_3$*. En effet, la conjugaison complexe* $\tau : i \mapsto -i$ *est un élément de non trivial de* G *d'ordre* 2*. Comme le degré de* P *est égal à* 3*, si* $\alpha \in K$ *est une racine de* P *(où on note* K *un corps de décomposition de* P*), l'extension* $\mathbb{Q}(\alpha)$ *est de degré* 3*, or* $[K : \mathbb{Q}] = [K = [K : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}]$ *donc* 3 *divise* $[K : \mathbb{Q}]$ *qui est l'ordre de* G*. Par le lemme de Cauchy, il existe un élément* $\sigma \in G$ *d'ordre* 3*. En considérant le morphisme de groupes qui a* τ *l'envoie sur une transposition quelconque de* $\mathcal{S}_3$ *et* σ *sur un* 3*-cycle, on a que* G *est bien isomorphe à* $\mathcal{S}_3$ *car ce dernier est engendré par une transposition et un* 3*-cycle.*
4. $\mathbb{C}(t)$ *contient les racines* n*-ièmes de l'unité donc un* K *est un corps de décomposition de* $X^n - t$ *est une extension de Kummer. On prend* $K = \mathbb{C}(t)(t^{1/n})$ *et le groupe de Galois de* K *est* $\{1, \alpha, \ldots, \alpha^{n-1}\}$ *où* $\alpha(t^{1/n}) = \xi t^{1/n}$ *où* ξ *est une racine* n*-ième de l'unité primitive. Sur* $\mathbb{R}(t)$ *on prend le même corps de décomposition et le groupe de Galois est le groupe de Galois de* K *sur* $\mathbb{C}(t)$ *produit semi-direct* $\{1, \tau\}$*, où* τ *est la conjugaison complexe.*
5. $P = X^5 - pqX + q$ *est irréductible sur* $\mathbb{Q}$ *par Eisenstein ; notons* K *un corps de décomposition de* P *et* $r_1, r_2, r_3, r_4, r_5 \in K$ *les racines de* P *(elles sont toutes distinctes car* $\mathbb{Q}$ *est parfait). Le groupe de Galois* G *de* P *est isomorphe à un sous-groupe de* $\mathcal{S}_5$*. En considérant* $\mathbb{Q}(r_i)$ *pour* $r_i \in K$ *une des racines de* P*, on voit que* 5 *divise l'ordre de* G*, il existe donc un élément de* G *qui est envoyé sur un* 5*-cycle dans* $\mathcal{S}_5$*. En calculant la dérivée de* P *on voit que* P' *a deux racines réelles :* $\pm\sqrt[4]{\frac{pq}{5}}$*, donc* P *a au plus* 3 *racines réelles (si elle en avait* 5*, sa dérivée s'annulerait* 4 *fois sur* $\mathbb{R}$ *et non* 2*). Comme* $P(X)$ *tend vers* $-\infty$ *quand* X *tend vers* $-\infty$*,* $P(-1) > 0$ *et* $P(1) < 0$ *on a que* P *a au moins de racines réelles ce qui implique qu'il en a exactement* 3*. Il a donc* 2 *racines complexes et* $\tau : i \mapsto -i$*, la conjugaison complexe, est un automorphisme de* G*. Le groupe* G *a alors un élément d'ordre* 2 *et un élément d'ordre* 5*, il est donc isomorphe à* $\mathcal{S}_5$*.*

Exercice 11. *Soit* K *un corps de caractéristique différente de* 2*, et soit* $P \in K[X]$ *un polynôme séparable. Soit* L *un corps de décomposition de* P *sur* K*, et soient* $r_1, \ldots, r_n$ *les racines de* P *dans* L*. On rappelle que le discriminant de* P *est un élément de* K *qui peut être défini par*

$$\Delta = \prod_{i<j} (r_i - r_j)^2.$$

1. *Soit* $d = \prod_{i<j}(r_i - r_j) \in L$. *Montrer que l'extension* $K(d)/K$ *est galoisienne de degré* 1 *ou* 2.
2. *On voit* $Gal(L/K)$ *comme un sous-groupe de* $\mathfrak{S}_n$ *agissant par permutation des racines de* P. *Montrer qu'un élément* σ *de* $Gal(L/K)$ *fixe* d *si, et seulement si,* $\sigma \in Gal(L/K) \cap \mathfrak{A}_n$.
3. *En déduire que* $K(d)$ *est l'extension de* K *correspondant au sous-groupe* $Gal(L/K) \cap \mathfrak{A}_n$ *de* $Gal(L/K)$.

Solution.

1. $\delta \in K$, *et* $X^2 - \Delta \in K[X]$ *a pour racines* d *et* $-d$ *dans* L, *donc l'extension* $K(d)$ *de* K *est donc un corps de décomposition de* $X^2 - \Delta$ *sur* K *et c'est une sous-extension de* L ($d \neq -d$ *car la caractéristique de* K *est différente de* 2). *Le polynôme minimal de* d *sur* K *divise alors* $X^2 - \Delta$ *et donc* $[K(d) : K] = 1$ *ou* 2.
2. $\sigma(d) = \prod_{i<j}(r_{\sigma(i)} - r_{\sigma_j}) = sign(\sigma).d$. *Donc* $\sigma(d) = d$ *si et seulement si* $sign(\sigma) = 1$ *ce qui est équivalent à* $\sigma \in Gal(L/K) \cap \mathfrak{A}_n$.
3. *Par définition de la correspondance de Galois, l'équivalence du 2. donne le résultat.*

Exercice 12. *Soit* $P \in \mathbb{R}[X]$ *un polynôme de degré* 3 *et de discriminant* Δ. *Montrer que*

1. P *a des racines multiples si* $\Delta = 0$;
2. P *a trois racines réelles distinctes si* $\Delta > 0$; *et*
3. P *a deux racines complexes conjuguées et une racine réelle si* $\Delta < 0$.

Solution. *Soient* $r_1, r_2, r_3 \in \mathbb{C}$ *les racines de* P. *Alors* $\Delta = (r_1 - r_2)^2(r_1 - r_3)^2(r_2 - r_3)^2$.

1. $\Delta = 0$ *si et seulement si il existe* $i, j \in \{1, 2, 3\}$ *tels que* $r_i = r_j$, *c'est-à-dire si* P *a une racine multiple.*
2. *Si les trois racines* $r_1, r_2, r_3 \in \mathbb{R}$ *sont distinctes alors* Δ *est le carrée d'un nombre réel non nul donc* $\Delta > 0$
3. *Si* $r_1 = a + bi$, $r_2 = a - bi$, *avec* $a, b \in \mathbb{R}$, $b \neq 0$ *et* $r_3 \neq 0$, *alors* $\Delta = -4b^2((a - r_3)^2 + b^2) < 0$.

Exercice 13. *Soient* t *un élément transcendant sur* $\mathbb{C}$, *et* $K = \mathbb{C}(t)[u]/(u^2 + t^2 - 1)$.

1. *Montrer que* K *est un corps, que l'on notera* $\mathbb{C}(t, u)$.
2. *Montrer que l'extension* $\mathbb{C}(t, u)$ *de* $\mathbb{C}(t^n, u^n)$ *est galoisienne, et calculer son groupe de Galois.*
3. *Montrer que l'élément* $u_n = \frac{1}{2}((t + iu)^n + (t - iu)^n)$ *est dans* $\mathbb{C}(t^n, u^n)$, *pour tout entier strictement positif* n.
4. *Utiliser les questions précédentes pour montrer que* $\cos(nx)$ *s'exprime comme fonction rationnelle de* $\cos^n(x)$ *et* $\sin^n(x)$.

Solution.

1. *Le polynôme* $P(u) = u^2 + t^2 - 1$ *est irréductible dans* $\mathbb{C}(t)[u]$ *car* $t^2 - 1$ *n'est pas un carré dans* $\mathbb{C}(t)$. *Donc l'idéal engendré par* P *dans* $\mathbb{C}(t)[u]$ *est maximal et donc* K *est un corps.*
2. *L'extension est galoisienne car* $\mathbb{C}(t, u)$ *est un corps de décomposition de* $(X^n - t^n)(X^n - u^n) \in \mathbb{C}(t^n, u^n)[X]$. *Calculons son groupe de Galois que nous notons* G. *Tout élément* σ *de* G *fixe* $\mathbb{C}(t^n, u^n)$ *donc* $\sigma(t^n) = t^n$ *et* $\sigma(u^n) = u^n$. *Ceci implique qu'il existe deux racines* n*-ièmes de l'unité* ξ *et* μ *telles que* $\sigma(t) = \xi t$ *et* $\sigma(u) = \mu u$. *Or* $t^2 + u^2 = 1$ *donc* $\sigma(1) = (\sigma(t))^2 + (\sigma(u))^2 = \xi^2 t^2 + \mu^2 - \mu^2 t^2 = 1$ *(car* σ *est un automorphisme de* $\mathbb{C}(t, u)$. *On a alors*
$$(\xi^2 - \mu^2)t^2 + \mu^2 = 1;$$
comme t *est transcendant sur* $\mathbb{C}$, *ceci implique que* $\xi^2 = \mu^2$ *et* $\mu^2 = 1$. *Comme* ξ *et* μ *sont des racines* n*-ièmes de l'unité, on distingue deux cas :*
   - *si* n *est impair alors* $\xi^2 = \mu = 1$ *implique* $\xi = 1$ *et* $\mu = 1$, *donc* $\sigma(t) = t$ *et* $\sigma(\mu) = \mu$ *donc* $\sigma = id$. *Dans ce cas* $G = \{1\}$ *et* $\mathbb{C}(t, u) = \mathbb{C}(t^n, u^n)$.
   - *si* n *est pair alors* $\xi^2 = \mu = 1$ *implique* $\xi = \pm 1$ *et* $\mu = \pm 1$. *Donc on a quatre choix possibles pour l'action de* σ *et donc l'ordre de* G *est inférieur ou égal à* 4. *De plus, on a la tour d'extension suivante :*
   $$\mathbb{C}(t^n, u^n) \to \mathbb{C}(t^2, u^2) = \mathbb{C}(t^2) \to \mathbb{C}(t) \to \mathbb{C}(t, u)$$
   car $u^2 = 1 - t^2$; *on a aussi* $[\mathbb{C}(t, u) : \mathbb{C}(t)] = 2$ *car* $\mathbb{C}(t, u) = \mathbb{C}(t)(u)$ *et* $u^2 + (1 - t^2) = 0$ *et le polynôme minimal de* u *dans* $\mathbb{C}(t)$ *est* $X^2 + (1 - t^2)$. *Donc,*
   $$[\mathbb{C}(t, u) : \mathbb{C}(t^n, u^n)] = [\mathbb{C}(t, u) : \mathbb{C}(t)][\mathbb{C}(t) : \mathbb{C}(t^2)][\mathbb{C}(t^2, u^2) : \mathbb{C}(t^n, u^n)] \geq 4$$
   donc l'ordre de G *est égal à* 4 *et* $G = \{1, \alpha, \beta, \alpha\beta\}$ *où* $\alpha(t) = -t$, $\alpha(u) = u$, $\beta(t) = t$ *et* $\beta(u) = -u$.

3. $[\mathbb{C}(t,u) : \mathbb{C}(t^n,u^n)]$ *est égal à* 1 *ou* 4 *en fonction de la parité de* n. *Si* n *est impair, ce degré est égal à* 1 *donc* $u_n \in \mathbb{C}(t^n,u^n)$ *car il appartient à* $\mathbb{C}(t,u)$. *Si* n *est pair, montrons que* $\sigma(u_n) = u_n$ *pour tout* $\sigma \in G$. *Il suffit de montrer qu'il est fixé par* α *et* β. *Or,* $\alpha(u_n) = \frac{1}{2}((-t+iu)^n + (-t-iu)^n) = u_n$ *et* $\beta(u_n) = \frac{1}{2}((t-iu)^n + (t+iu)^n) = u_n$.
4. *On pose* $t = \cos(x)$ *et* $u = \sin(x)$. *Alors* $\cos(x)$ *est bien transcendant sur* $\mathbb{C}$ *(il suffit de voir que* $1, \cos(x), \cos^2(x), \ldots$ *sont linéairement indépendants sur* $\mathbb{C}$*). Dans ce cas, on a* $\mathbb{C}(\cos(x),\sin(x)) \simeq \mathbb{C}(X,Y)/(X^2+Y^2-1)$ *et on applique la première partie de l'exercice :* $u_n = \frac{1}{2}((\cos(x)+i\sin(x))^n + (\cos(x)-i\sin(x))^n) = \cos(xn)$ *et d'après 3.* $\cos(nx) \in \mathbb{C}(\sin^n(x),\cos^n(x))$. *D'où* $\cos(nx)$ *s'exprime comme fonction rationnelle de* $\sin^n(x)$ *et* $\cos^n(x)$.

Exercice 14. *Soit* K *un corps de caractéristique* $p \neq 0$, *et soit* a *un élément de* K *qui ne peut pas s'écrire comme* $b^p - b$, *avec* $b \in K$. *Trouver le groupe de Galois du polynôme* $X^p - X - a$.

Solution. *Soit* L *un corps de décomposition de* $P = X^p - X - a$ *et soit* α *une racine de* P *dans* L. *Donc* $\alpha^p - \alpha = a$ *donc* $\alpha \in L\backslash K$. *Comme* K *est de caractéristique* p, *on a que* $(1+\alpha)$ *est aussi une racine de* P *et donc les racines de* P *sont* $\alpha, \alpha+1, \alpha+2, \ldots, \alpha+p-1$ *(il y en a* p*). Ceci implique que* P *est séparable,* L/K *est donc un extension galoisienne et* $L = K(\alpha, \alpha+1, \alpha+2, \ldots, \alpha+p-1) = K(\alpha)$. *Donc* $[L:K] \leq p$. *Si* σ *est un élément non trivial du groupe de Galois de* L *sur* K, *alors* $\sigma(\alpha) = \alpha + k$, *avec* $k \in \mathbb{F}_p\backslash\{0\}$. η *est donc d'ordre* p *et le groupe de Galois est engendré par* η *; il est donc isomorphe à* $\mathbb{Z}/p\mathbb{Z}$.

Exercice 15. *On rapeplle que le* n*-ième polynôme cyclotomique sur* $\mathbb{C}$ *est défini par*

$$\Phi_n(X) = \prod_{\zeta} (X - \zeta),$$

où le produit est pris sur toutes les racines n*-ièmes primitives de l'unité* ζ. *On rappelle que* $X^n - 1 = \prod_{d|n} \Phi_d(X)$ *et que* $\Phi_n(X)$ *est un polynôme irréductible.*

Un anneau à division est un anneau (non nécessairement commutatif) dont tous les éléments non nuls admettent un inverse. On se propose de montrer que tout anneau à division fini est commutatif. Soit A *un anneau à division fini et soit* $Z(A)$ *son centre (c'est un corps). Soit* n *la dimension de* A *sur* $Z(A)$, *et soit* q *l'ordre de* $Z(A)$.

1. *En utilisant l'équation des classes, montrer que*

$$q^n - 1 = q - 1 + \sum \frac{q^n - 1}{q^d - 1},$$

où la somme est prise sur les représentants d'éléments non dans $Z(A)^*$, *et* d *est la dimension du centralisateur de cet élément sur* $Z(A)$.

2. *Montrer qu'alors* $\Phi_n(q)$ *divise* $q - 1$.
3. *Montrer que si* $n > 1$, *alors* $\Phi_n(q) > q - 1$ *(indice : utiliser la décomposition de* $\Phi_n(X)$ *en facteurs linéaires dans* $\mathbb{C}[X]$*).*
4. *Conclure que* $A = Z(A)$ *et que* A *est un corps.*

Solution.

1. $A^\times$ *est un groupe multiplicatif qui agit sur lui même par conjugaison. l'équation aux classes s'écrit alors :* $|A^\times| = |Z(A^\times)| + \sum_{orbites\ de\ taille\ \geq 2} |orbites|$ *ce qui est équivalent à* $q^n - 1 = q - 1 + \sum_{d|n,\, d\neq n} \frac{q^n-1}{q^d-1}$
2. $\Phi_n(X)$ *divise* $X^n - 1$ *et aussi* $\frac{X^n-1}{X^d-1}$ *pour tout* d *diviseur de* n, $d \neq n$. *Donc* $\Phi_n(q)$ *divise* $q^n - 1$ *et* $\Phi_n(q)$ *divise* $\sum_{d|n,\, d\neq n} \frac{q^n-1}{q^d-1}$ *donc* $\Phi_n(q)$ *divise* $q - 1$.
3. *Dans* $\mathbb{C}[X]$, $\Phi_n(X) = \prod_{\xi\ racine\ n\text{-}ième\ de\ l'unité\ primitive} (X - \xi)$ *donc* $\Phi_n(q) = \prod(q-\xi) = \prod |q-\xi| \geq \prod ||q| - |\xi|| = \prod |q-1| > q - 1$.
4. *Si* $n > 1$, *on a que* $\Phi_n(q)$ *divise* $q - 1$ *et* $\Phi_n(q) > q - 1$ *ce qui n'est pas possible donc* $n = 1$. *Dans ce cas* $Z(A) = A$ *et* A *est alors un corps commutatif.*