1. Soient A un anneau commutatif et B une A-algèbre (non nécessairement commutative). On note ε l'image de X dans $A[X]/(X^2)$ et $A[\varepsilon] = A[X]/(X^2)$.

(a) Montrer que $B \otimes_A A[\varepsilon]$ est un B-module libre de base $1 \otimes 1$, $1 \otimes \varepsilon$. On note $B[\varepsilon] = B \otimes_A A[\varepsilon]$.

(b) Soit C une A-algèbre. Montrer que les morphismes de A-algèbres $B \to C[\varepsilon]$ sont en bijection avec les couples (f, D), où $f\colon B \to C$ est un morphisme de A-algèbres et $D\colon B \to C$ est une *f-dérivation*, c'est-à-dire une application A-linéaire qui vérifie

$$D(xy) = D(x)f(y) + f(x)D(y)$$

pour tous x, y dans B.

(c) Une *dérivation de B* est une id_B-dérivation. Montrer que les dérivations de l'algèbre tensorielle $T(M)$ sur un A-module M sont en bijection canonique avec les morphismes de A-modules de M dans $T(M)$.

(d) Supposons que B est une A-algèbre commutative. Montrer que l'ensemble des dérivations de B admet une structure naturelle de B-module. Montrer que si B est l'algèbre symétrique sur un A-module libre de rang fini n, ce module est libre de rang n.

Corrigé. (a) Il suffit de prouver que $A[\varepsilon]$ est libre de base $1, \varepsilon$, ce qui est clair. On peut donc écrire tout élément de $B[\varepsilon]$ sous la forme $x_0 + x_1\varepsilon$ avec $x_0, x_1 \in B$ uniquement déterminés.

(b) Soit $F\colon B \to C[\varepsilon]$ un morphisme de A-algèbres. D'après ce qu'on vient de prouver, on peut écrire de façon unique $F(x) = f(x) + D(x)\,\varepsilon$ pour tout $x \in B$, où f et D sont deux fonctions $B \to C$ dont il reste à examiner les propriétés. Manifestement f et D sont A-linéaires. Comme f peut se décrire comme la composée de F par le morphisme $C[\varepsilon] \to C$ envoyant ε sur 0, on voit que f est un morphisme d'algèbres. Quant à D, en écrivant $F(xy) = F(x)\,F(y)$, soit $f(xy) + D(xy)\,\varepsilon = f(x)\,f(y) + [D(x)\,f(y) + f(x)\,D(y)]\,\varepsilon$ pour tous x, y et en identifiant les termes, on voit qu'il vérifie l'identité demandée. Notons que $D(1) = 0$ en découle. Réciproquement, si f et D sont A-linéaires et vérifient ces propriétés, la fonction A-linéaire F définie par $F(x) = f(x) + D(x)\,\varepsilon$ vérifie bien $F(1) = 1$ et $F(xy) = F(x)\,F(y)$, donc F est un morphisme de A-algèbres.

(c) Si $D\colon T(M) \to T(M)$ est une dérivation, sa restriction à M (vu comme les tenseurs de degré 1 dans $T(M)$) définit une application A-linéaire $\gamma\colon M \to T(M)$, et d'après la définition des dérivations on a $D(x_1 \otimes \cdots \otimes x_m) = \sum_{j=1}^{m} x_1 \otimes \cdots \otimes \gamma(x_j) \otimes \cdots \otimes x_m$. Réciproquement, supposons que $\gamma\colon M \to T(M)$ soit une application A-linéaire quelconque, et définissons D sur $T^m(M) = M^{\otimes m}$ par cette formule : ceci a bien un sens car l'expression $\sum_{j=1}^{m} x_1 \otimes \cdots \otimes \gamma(x_j) \otimes \cdots \otimes x_m$ est multilinéaire ; on en déduit $D\colon T(M) \to T(M)$ application A-linéaire. Reste à prouver qu'on a $D(xy) = D(x)\,y + x\,D(y)$: or il suffit de le vérifier sur les tenseurs purs, et si $x = x_1 \otimes \cdots \otimes x_m$ et $y = y_1 \otimes \cdots \otimes y_n$, les deux membres de cette égalité sont bien égaux à $\sum_{j=1}^{m} x_1 \otimes \cdots \otimes \gamma(x_j) \otimes \cdots \otimes x_m \otimes y_1 \otimes \cdots \otimes y_n + \sum_{j=1}^{n} x_1 \otimes \cdots \otimes x_m \otimes y_1 \otimes \cdots \otimes \gamma(y_j) \otimes \cdots \otimes y_n$ et on a prouvé ce qu'on souhaitait.

On pouvait aussi utiliser le fait que les morphismes d'algèbres $T(M) \to T(M)[\varepsilon]$ sont naturellement en bijection avec les morphismes de A-modules $M \to T(M)[\varepsilon]$, or les premiers sont en bijection avec les couples formés d'un morphisme d'algèbre $f\colon T(M) \to T(M)$ et une f-dérivation $T(M) \to T(M)$ et les seconds sont en bijection avec les couples de deux morphismes de A-modules $M \to T(M)$, et on vérifie facilement que sur la première composante des couples il s'agit de la bijection qu'on attend.

(d) Si $D\colon B \to B$ est une dérivation et $b \in B$, avec B commutative, on a pour tous $x, y \in B$ que $b\,D(xy) = by\,D(x) + bx\,D(y)$, c'est-à-dire que $x \mapsto b\,D(x)$ est encore une dérivation. On peut donc voir les dérivations comme un sous-B-module des applications A-linéaires $B \to B$.

Si $B = S(M)$ est l'algèbre symétrique d'un A-module M, on va montrer de nouveau que les dérivations $B \to B$ sont en bijection canonique avec les applications A-linéaires $M \to B$. Si $D\colon B \to B$ est une dérivation, sa restriction à M (vu comme les tenseurs de degré 1 dans B) définit une application A-linéaire $\gamma\colon M \to B$, et d'après la définition des dérivations on a $D(x_1 \cdots x_m) = \sum_{j=1}^m \gamma(x_j)\, x_1 \cdots \widehat{x_j} \cdots x_m$. Réciproquement, supposons que $\gamma\colon M \to B$ soit une application A-linéaire quelconque, et définissons D sur $S^m(M)$ par cette formule : ceci a bien un sens car l'expression $\sum_{j=1}^m \gamma(x_j)\, x_1 \cdots \widehat{x_j} \cdots x_m$ est multilinéaire symétrique ; on en déduit $D\colon B \to B$ application A-linéaire. La même preuve que dans le cas tensoriel montre qu'il s'agit bien d'une dérivation. Et on constate immédiatement cette bijection $\gamma \mapsto D$ n'est pas seulement A-linéaire mais bien B-linéaire. On pouvait aussi, de nouveau, utiliser le fait que les morphismes d'algèbres $S(M) \to S(M)[\varepsilon]$ (cette fois puisque $S(M)[\varepsilon]$ est commutative !) sont naturellement en bijection avec les morphismes de A-modules $M \to S(M)[\varepsilon]$.

Notamment, si $M = A^n$ est libre de rang n, on vient de voir que le B-module des dérivations $B \to B$ s'identifiait avec le B-module des applications A-linéaires $A^n \to B$: or il s'agit du B-module libre B^n. ✓

2. Déterminer le groupe de Galois des équations suivantes :
(a) $t^4 + 4t^3 + 2t^2 + 3t - 5$ sur $\mathbb{Q}$;
(b) $t^3 - 3\lambda t - \lambda - \lambda^2 = 0$ sur $\mathbb{C}(\lambda)$, où λ est une indéterminée ;
(c) $t^6 - 3t^2 + 1 = 0$ sur $\mathbb{Q}$;
(d) $t^6 - 4t^2 - 1 = 0$ sur $\mathbb{Q}$.

Corrigé. (a) Modulo 2, ce polynôme, $t^4 + t + 1$, est irréductible sur $\mathbb{F}_2$, puisqu'il n'a pas de racine dans $\mathbb{F}_4$. On en déduit que $t^4 + 4t^3 + 2t^2 + 3t - 5$ est irréductible sur $\mathbb{Q}$, et que son groupe de Galois contient un 4-cycle. Modulo 3, il se factorise comme $(t + 1)\,(t^3 + 2t + 1)$ (où le second facteur est irréductible) : le groupe de Galois contient donc aussi un 3-cycle. Or un 4-cycle et un 3-cycle engendrent $\mathfrak{S}_4$ (quitte à renuméroter, on peut supposer que le 4-cycle est $(1\ 2\ 3\ 4)$ et que l'élément fixé par le 3-cycle est 4, et quitte à remplacer le 3-cycle par son carré on peut supposer que c'est $(1\ 2\ 3)$, et c'est alors une vérification facile). Bref, le groupe de Galois recherché est $\mathfrak{S}_4$. On pouvait aussi trouver une transposition dans la réduction modulo 5 ($t\,(t-1)\,(t^2+2)$) ou utiliser la conjugaison complexe.

(b) L'équation $t^3 - 3\lambda t - \lambda - \lambda^2 = 0$ n'a pas de racine dans $\mathbb{C}(\lambda)$: en effet, en notant v la valuation en $\lambda = 0$ d'un élément de $\mathbb{C}(\lambda)$ (c'est-à-dire l'ordre du zéro en 0 s'il y en a un, ou l'opposé de l'ordre du pôle en 0 s'il y en a un, avec la convention $v(0) = \infty$), si $f \in \mathbb{C}(\lambda)$, d'une part $v(f) \geq 1$ entraîne $v(f^3 - 3\lambda f - \lambda - \lambda^2) = 1$, et d'autre part $v(f) \leq 0$ entraîne $v(f^3 - 3\lambda f - \lambda - \lambda^2) = 3v(f) \leq 0$, donc dans les deux cas $f^3 - 3\lambda f - \lambda - \lambda^2$ ne s'annule pas (son ordre d'annulation en 0 est même au plus 1). Donc $t^3 - 3\lambda t - \lambda - \lambda^2$ est irréductible dans $\mathbb{C}(\lambda)[t]$. Mais le discriminant est $-27\,\lambda^2\,(\lambda - 1)^2$, qui est un carré dans $\mathbb{C}(\lambda)$. Donc le groupe de Galois est $\mathbb{Z}/3\mathbb{Z}$.

(c) Appelons $\vartheta_1, \vartheta_2, \vartheta_3$ les trois racines, toutes trois réelles, de l'équation $u^3 - 3u + 1 = 0$ vérifiée par t^2, avec, mettons, $\vartheta_1 < \vartheta_2 < \vartheta_3$ (on a d'ailleurs $\vartheta_1 = 2\cos\frac{2\pi}{9}$, $\vartheta_2 = 2\cos\frac{4\pi}{9}$ et $\vartheta_3 = 2\cos\frac{8\pi}{9}$, mais on n'utilisera pas ce fait). Comme le discriminant de l'équation cubique $u^3 - 3u + 1 = 0$ est $81 = 9^2$ et qu'elle est manifestement irréductible, son groupe de Galois $\mathrm{Gal}(\mathbb{Q}(\vartheta_i)/\mathbb{Q})$ est $\mathbb{Z}/3\mathbb{Z}$ (il faut y penser comme un quotient du groupe de Galois de $t^6 - 3t^2 + 1$). Appelons maintenant ξ_1, ξ_2, ξ_3 des racines carrées de $\vartheta_1, \vartheta_2, \vartheta_3$ respectivement : les six racines de $t^6 - 3t^2 + 1$ sont $\pm\xi_1, \pm\xi_2, \pm\xi_3$. Puisque $\vartheta_1 < 0 < \vartheta_2 < \vartheta_3$, la conjugaison complexe réalise un élément τ du groupe de Galois qui échange ξ_1 et $-\xi_1$ et laisse ξ_2 et ξ_3 fixes. Mais comme il existe nécessairement un élément σ du groupe de Galois qui envoie ϑ_1 sur ϑ_2 (donc ξ_1 sur $\pm\xi_1$), on voit que $\sigma\tau\sigma^{-1}$ échange ξ_2 et $-\xi_2$ en laissant ξ_1 et ξ_3 fixes, et, de

même, on peut trouver un élément qui échange ξ_3 et $-\xi_3$ en laissant ξ_1 et ξ_2 fixes. Ainsi, on a trouvé huit éléments réalisant n'importe quelle combinaison de signes $\xi_i \mapsto (\pm)_i\xi_i$. Or il s'agit là précisément du fixateur des ϑ_i (puisque tout élément fixant les ϑ_i doit opérer par une telle combinaison de signes) : c'est-à-dire que $\mathrm{Gal}(\mathbb{Q}(\xi_i)/\mathbb{Q}(\vartheta_i)) \cong (\mathbb{Z}/2\mathbb{Z})^3$. Enfin, le générateur $\sigma\colon \vartheta_1 \mapsto \vartheta_2 \mapsto \vartheta_3 \mapsto \vartheta_1$ de $\mathrm{Gal}(\mathbb{Q}(\vartheta_i)/\mathbb{Q}) \cong \mathbb{Z}/3\mathbb{Z}$ se relève en un $\tilde\sigma\colon \xi_1 \mapsto \xi_2 \mapsto \xi_3 \mapsto \xi_1$ (on a vu qu'on pouvait choisir arbitrairement les signes, donc on peut les prendre tous $+$), et on a prouvé que $\mathrm{Gal}(\mathbb{Q}(\xi_i)/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^3 \rtimes \mathbb{Z}/3\mathbb{Z}$, où $\mathbb{Z}/3\mathbb{Z}$ opère sur $(\mathbb{Z}/2\mathbb{Z})^3$ par permutation cyclique des indices. (On peut aussi voir ce groupe comme l'ensemble des permutations de $\{1, 1', 2, 2', 3, 3'\}$ qui préservent la partition $\{\{1, 1'\}, \{2, 2'\}, \{3, 3'\}\}$ en opérant cycliquement sur ces trois classes. Abstraitement il est isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathfrak{A}_4$ mais ce n'est pas bien intéressant.)

(d) Appelons $\vartheta_1, \vartheta_2, \vartheta_3$ les trois racines, toutes trois réelles, de l'équation $u^3 - 4u - 1 = 0$ vérifiée par t^2, avec, mettons, $\vartheta_1 < \vartheta_2 < \vartheta_3$. Comme le discriminant de l'équation cubique $u^3 - 4u - 1 = 0$ est 229 et qu'elle est manifestement irréductible, son groupe de Galois $\mathrm{Gal}(\mathbb{Q}(\vartheta_i)/\mathbb{Q})$ est $\mathfrak{S}_3$ (il faut y penser comme un quotient du groupe de Galois de $t^6 - 4t^2 - 1$). Appelons maintenant ξ_1, ξ_2, ξ_3 des racines carrées de $\vartheta_1, \vartheta_2, \vartheta_3$ respectivement : les six racines de $t^6 - 4t^2 - 1$ sont $\pm\xi_1, \pm\xi_2, \pm\xi_3$. Puisque $\vartheta_1 < \vartheta_2 < 0 < \vartheta_3$, la conjugaison complexe réalise un élément τ du groupe de Galois qui échange ξ_1 et $-\xi_1$ et ξ_2 et $-\xi_2$ tandis qu'il laisse ξ_3 fixe. Mais pour les mêmes raisons que dans le (c), on peut alors réaliser n'importe quel nombre *pair* de changements de signes sur les ξ_i, i.e., on a trouvé quatre éléments du groupe de Galois réalisant n'importe quelle combinaison de signe $\xi_i \mapsto (\pm)_i\xi_i$ où (zéro ou) deux des $(\pm)_i$ valent $-$. Comme par ailleurs $\vartheta_1\vartheta_2\vartheta_3 = 1$ (d'après le coefficient constant), on voit que $\xi_1\xi_2\xi_3$ vaut 1 ou -1 (selon les choix qu'on a faits des ξ_i) et doit en tout cas rester *fixe* par l'action du groupe de Galois : il n'y a donc aucun élément du groupe de Galois qui réalise un nombre impair de changements de signes sur les ξ_i. C'est-à-dire que $\mathrm{Gal}(\mathbb{Q}(\xi_i)/\mathbb{Q}(\vartheta_i)) \cong (\mathbb{Z}/2\mathbb{Z})^2$. Enfin, tout élément $\sigma \in \mathrm{Gal}(\mathbb{Q}(\vartheta_i)/\mathbb{Q}) \cong \mathfrak{S}_3$ se relève en une permutation des ξ_i à des changements de signe près, et ces changements de signe sont en nombre pair (toujours car $\xi_1\xi_2\xi_3$ est fixe par Galois), ce qui nous permet de prendre uniquement des $+$ d'après ce qu'on a déjà vu. On a ainsi prouvé que $\mathrm{Gal}(\mathbb{Q}(\xi_i)/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^2 \rtimes \mathfrak{S}_3$, où $\mathfrak{S}_3$ opère sur les trois éléments non nuls de $(\mathbb{Z}/2\mathbb{Z})^2$. (On peut aussi voir ce groupe comme l'ensemble des permutations de $\{1, 1', 2, 2', 3, 3'\}$ qui préservent la partition $\{\{1, 1'\}, \{2, 2'\}, \{3, 3'\}\}$ et envoient un nombre pair d'éléments de $\{1, 2, 3\}$ dans $\{1', 2', 3'\}$. Abstraitement il est isomorphe à $\mathfrak{S}_4$ mais ce n'est pas bien intéressant.) ✓

3. (a) Déterminer l'entier positif minimal n tel que le corps de décomposition L du polynôme $X^n - 1$ sur $\mathbb{Q}$ contient une sous-extension E de degré 3. Montrer que cette sous-extension est unique.

(b) Montrer que E est galoisienne et exhiber un polynôme irréductible unitaire à coefficients entiers dont c'est le corps de décomposition.

Corrigé. (a) Le groupe de Galois de $L = \mathbb{Q}(\zeta_n)$ sur $\mathbb{Q}$ est $(\mathbb{Z}/n\mathbb{Z})^\times$, d'ordre $\varphi(n)$ où φ est la fonction indicatrice d'Euler. Cet ordre est multiple de 3 en premier pour $n = 7$. On a alors $(\mathbb{Z}/7\mathbb{Z})^\times \cong (\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$. Or $(\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$ contient un unique sous-groupe H d'indice 3, c'est-à-dire d'ordre 2 : le corps fixe de ce sous-groupe est l'unique extension d'ordre 3 de $\mathbb{Q}$ contenue dans L.

(b) Comme le groupe de Galois de L sur $\mathbb{Q}$ est abélien, tout sous-groupe est distingué, c'est-à-dire que toute sous-extension de L est galoisienne, et notamment E l'est.

En posant $\zeta_7 = e^{2i\pi/7}$, l'élément non-trivial de H, c'est-à-dire l'unique élément non trivial de $\mathrm{Gal}(L/\mathbb{Q})$, est donné par $\zeta_7 \mapsto \zeta_7^{-1}$, ou, si on veut, par la conjugaison complexe. On a alors

un élément de E donné par $\zeta_7 + \zeta_7^{-1} = 2\cos\frac{2\pi}{7}$, et comme cet élément a bien deux autres conjugués distincts par le groupe de Galois, $\zeta_7^2 + \zeta_7^{-2} = 2\cos\frac{4\pi}{7}$ et $\zeta_7^3 + \zeta_7^{-3} = 2\cos\frac{6\pi}{7}$, il est de degré 3 donc engendre E. Son polynôme minimal sur $\mathbb{Q}$ est $(t - (\zeta_7 + \zeta_7^{-1}))(t - (\zeta_7^2 + \zeta_7^{-2}))(t - (\zeta_7^3 + \zeta_7^{-3}))$ soit, en développant et en simplifiant, $t^3 + t^2 - 2t - 1$ (et E en est corps de rupture ou corps de décomposition sur $\mathbb{Q}$). ✓

4. Soient K un corps et L une extension finie normale de K. Montrer qu'il existe une sous-extension E de L telle que L est galoisienne sur E et les éléments de E n'appartenant pas à K sont tous inséparables sur K.

Corrigé. Il n'y a rien à prouver en caractéristique 0 (on prend $E = K$) : on pourra se placer en caractéristique $p > 0$.

Soit G le groupe des automorphismes de L laissant K fixe, et soit $E = L^G$ le corps des éléments de L fixes par G.

Premièrement, L est galoisienne sur E d'après le lemme d'Artin. Rappelons le raisonnement dans ce cas : on sait déjà qu'elle est normale, et il s'agit donc de prouver qu'elle est séparable. Mais si x est un élément de L, l'orbite de x sous G est finie (puisque tout élément de cette orbite est racine du polynôme minimal de x sur K) ; si $x = x_1, \ldots, x_n$ sont tous les différents éléments de cette orbite, $\prod(t - x_i)$ est un polynôme dont x est racine, qui a ses coefficients dans E (ils sont stables par G) et qui est séparable. Donc x est bien séparable sur E.

Maintenant, si x et x' sont deux éléments de L ayant même polynôme minimal sur K, il existe un automorphisme de L envoyant x sur x' (en effet, l'isomorphisme entre $k(x)$ et $k(x')$ se prolonge en un automorphisme de L). Mais ceci prouve que le polynôme minimal d'un élément de E ne peut avoir qu'une seule racine distincte. *A fortiori*, tout élément de E qui n'appartient pas à K est inséparable sur K : son polynôme minimal est de la forme $t^{p^n} - a = 0$ (où $a = x^{p^n}$, avec n le plus petit entier naturel tel que ceci soit dans K).

En fait, on a prouvé que E était l'ensemble des x de L tels que x^{p^n} appartienne à K pour un certain n (on vient de voir qu'il existe un tel n lorsque $x \in E$, et, réciproquement, si x^{p^n} appartient à K alors x doit être laissé fixe par tout automorphisme de L). ✓