Corrigé

1 Exemples

1. (a) Puisque le monôme $X_1^{d_1}X_2^{d_2}\dots X_n^{d_n}$ apparaît dans P (c'est-à-dire est affecté d'un coefficient non nul), il en est de même, par symétrie de P, de $X_1^{d_{\sigma(1)}}X_2^{d_{\sigma(2)}}\dots X_n^{d_{\sigma(n)}}$ pour tout $\sigma \in \mathcal{S}_n$. On a donc, puisque $\deg(P) = (d_1, d_2, \dots, d_n)$,

$$\forall \sigma \in \mathcal{S}_n,\ (d_{\sigma(1)}, d_{\sigma(2)}, \dots, d_{\sigma(n)}) \leq (d_1, d_2, \dots, d_n)$$

Supposons que l'on n'ait pas $d_1 \geq d_2 \geq \dots \geq d_n$, et considérons $r \in [\![1, n]\!]$ tel que $d_1 \geq d_2 \geq \dots \geq d_r$ et $d_r < d_{r+1}$. Pour la transposition $\tau = (r, r+1)$, on a $(d_1, d_2, \dots, d_n) < (d_{\tau(1)}, d_{\tau(2)}, \dots, d_{\tau(n)})$, ce qui contredit l'inégalité précédente. On a prouvé par l'absurde $d_1 \geq d_2 \geq \dots \geq d_n$.

   (b) Lorsque l'on développe le produit $\Sigma_1^{d_1-d_2}\Sigma_2^{d_2-d_3}\dots\Sigma_n^{d_n}$, l'exposant de X_1 dans chaque monôme vaut au plus $(d_1-d_2)+(d_2-d_3)+\dots+(d_{n-1}-d_n)+d_n = d_1$. Les monômes dont l'exposant de X_1 vaut d_1 sont obtenus en "choisissant" dans chaque facteur $\Sigma_k^{d_k-d_{k+1}}$ un terme contenant $X_1^{d_k-d_{k+1}}$ (donc, en particulier, en choisissant $X_1^{d_1-d_2}$ dans $\Sigma_1^{d_1-d_2}$). Parmi ceux-là, l'exposant de X_2 est donc au plus $(d_2-d_3)+(d_3-d_4)+\dots+(d_{n-1}-d_n)+d_n = d_2$ et ceux pour lesquels il vaut deux sont obtenus en choisissant, dans les facteurs $\Sigma_k^{d_k-d_{k+1}}$, $2 \leq k \leq n$, un terme contenant $(X_1X_2)^{d_k-d_{k+1}}$ (en particulier donc, en choisissant X_1X_2 dans Σ_2). Poursuivant ainsi, on voit que le terme de plus haut degré apparaissant dans $\Sigma_1^{d_1-d_2}\Sigma_2^{d_2-d_3}\dots\Sigma_n^{d_n}$ est obtenu en "choisissant" $X_1^{d_1-d_2}$ dans $\Sigma_1^{d_1-d_2}$, $(X_1X_2)^{d_2-d_3}$ dans $\Sigma_2^{d_2-d_3}$, …, $(X_1X_2\dots X_{n-1})^{d_{n-1}-d_n}$ dans $\Sigma_{n-1}^{d_{n-1}-d_n}$ et, bien sûr, $(X_1X_2\dots X_n)^{d_n}$ dans $\Sigma_n^{d_n}$. Il vaut $X_1^{d_1}X_2^{d_2}\dots X_n^{d_n}$.

   (c) L'ensemble $\{(e_1, e_2, \dots, e_n) \in \mathbb{N}^n;\ (e_1, e_2, \dots, e_n) \leq \deg(P)\}$ n'est pas fini en général : si $d_1 > 1$, il contient tous les $(d_1 - 1, e_2, \dots, e_n)$ $(e_i \in \mathbb{N})$. Par contre, l'ensemble $\{(e_1, e_2, \dots, e_n) \in \mathbb{N}^n;\ (e_1, e_2, \dots, e_n) \leq \deg(P)$ et $\exists Q \in K[X_1, X_2, \dots, X_n],\ Q$ symétrique, $\deg(Q) = (e_1, e_2, \dots, e_n)\}$ est fini car si $(e_1, e_2, \dots, e_n)$ lui appartient, alors $d_1 \geq e_1 \geq e_2 \geq \dots \geq e_n$.

   (d) Supposons par l'absurde l'existence d'un P un polynôme symétrique ne pouvant s'exprimer comme polynôme en les Σ_k. Soit $(d_1, d_2, \dots, d_n) = \deg(P)$ et a le coefficient de $X_1^{d_1}X_2^{d_2}\dots X_n^{d_n}$ dans P. Alors $P_1 = P - a\Sigma_1^{d_1-d_2}\Sigma_2^{d_2-d_3}\dots\Sigma_n^{d_n}$ est symétrique et de degré strictement inférieur à $\deg(P)$. Le polynôme P_1 ne peut pas s'exprimer comme polynôme en les Σ_k (sinon P le pourrait aussi). En réitérant cette construction, la suite des degrés successifs constitue suite strictement décroissante de n-uplets dont l'existence contredit la finitude de l'ensemble invoqué dans la question 1c.

   (e) Avec la notation suggérée dans l'énoncé, on a $P = \sum X_1^3X_2$. La démonstration

précédente invite à évaluer :

$$\begin{aligned}\Sigma_1^2\Sigma_2 &= (\sum X_1)^2(\sum X_1X_2)\\ &= (\sum X_1^2 + 2\sum X_1X_2)(\sum X_1X_2)\\ &= \sum X_1^3X_2 + \sum X_1^2X_2X_3 + 2\Sigma_2^2\\ &= \sum X_1^3X_2 + \Sigma_1\Sigma_3 + 2\Sigma_2^2\end{aligned}$$

D'où $P = \Sigma_1^2\Sigma_2 - \Sigma_1\Sigma_3 - 2\Sigma_2^2$.

2. Notons τ la transposition (b, c). La permutation circulaire $\sigma = (a, b, c)$ laisse invariante l'expression $(a + j^2b + jc)^3$. Comme $\mathcal{S}\{a, b, c\} = \{\mathrm{id}, \sigma, \sigma^2, \tau, \tau\sigma, \tau\sigma^2\}$, on obtient en permutant les lettres a, b, c de toutes les manières possibles seulement deux expressions : $u = (a + j^2b + jc)^3$ et $u' = (a + jb + j^2c)^3$.

   Comme τ échange les expressions qui fournissent u et u', celles qui donnent $u + u'$ et uu' sont, elles, invariantes par toutes permutations. D'après la première question, elles peuvent s'écrire comme des polynômes à coefficients dans $\mathbb{Q}(j)$ en $p = \Sigma_2(a, b, c)$ et $q = \Sigma_3(a, b, c)$. Ce sont donc des éléments de $\mathbb{Q}(j)(p, q) \subset K(j)$. Ainsi, u et u' sont racines d'une équation du second degré à coefficients dans $K(j)$ qu'on sait résoudre par radicaux (on ne sait pas quelle racine est u ou u' mais cela n'a pas d'importance : les échanger revient à échanger deux des racines a, b, c). En extrayant des racines cubiques de u et u', on obtient, à une multiplication par j ou j^2 près, $v = a + jb + j^2c$ et $v' = a + j^2b + jc$. Comme $a + b + c = 0$, il ne reste plus qu'à résoudre un système linéaire 3×3 (inversible car de Van der Mond).

   Pour lever l'ambiguïté (due aux multiplications par j ou j^2), on peut noter que $vv' = (a^2 + b^2 + c^2) + j(ac + ba + cb) + j^2(ab + bc + ca) = -3q$. Un choix pour v implique donc un choix pour v'. Il reste trois possibilités pour le choix de u qui sont toutes les trois valides puisqu'elles correspondent simplement à une "renumérotation cyclique" des racines (l'échange v, v' correspondant à une "renumérotation par transposition").

3. L'expression est invariante par les huit permutations appartenant à l'ensemble $St = \{\mathrm{id}, (1, 2), (3, 4), (1, 2)(3, 4), (1, 3)(2, 4), (1, 4)(2, 3), (1, 3, 2, 4)$ et $(1, 4, 2, 3)\}$.

   Les transpositions $\tau = (x_1, x_3)$ et $\tau' = (1, 4)$, elles, la transforment en $v = x_1x_3 + x_2x_4$ et $w = x_1x_4 + x_2x_3$.

   Comme $\mathcal{S}_4 = St \cup \tau St \cup \tau' St$, les seules expressions obtenues sont effectivement u, v, w. Ces expressions sont permutées lorsqu'on permute les x_i. Donc $u+v+w$, $uv+vw+wu$ et uvw sont des expressions symétriques des x_i et peuvent s'écrire comme polynômes en $p = \Sigma_2(x_1, x_2, x_3, x_4)$, $q = \Sigma_3(x_1, x_2, x_3, x_4)$ et $r = \Sigma_4(x_1, x_2, x_3, x_4)$. Ce sont donc des éléments de $K(p, q, r)$ et u, v et w sont racines d'une équation de degré 3 à coefficients dans $K(p, q, r)$, que l'on sait résoudre par radicaux. On en déduit tous les x_ix_j $(i \neq j)$ puisque, par exemple, x_1x_2 et x_3x_4 sont racines du polynôme $Z^2 - uZ + r$. On en déduit finalement $x_1^2 = \frac{x_1x_2x_1x_3}{x_2x_3}$ puis x_1.

4. On a $u+v=\sum_{k=1}^{6}\xi^k=-1$ et $uv=(\xi^4+\xi^6+1)+(\xi^5+1+\xi)+(1+\xi^2+\xi^3)=2$. Donc u et v sont racines du polynôme U^2+U+2. Par ailleurs en combinant les deux relations $u=\xi+\xi^2+\xi^4$ et $v=\xi^3+\xi^5+\xi^6$, on voit que ξ vérifie : $\xi^3+v\xi^2-u\xi+v=0$. C'est une équation de degré 3 que l'on peut résoudre par radicaux en n'utilisant que des radicaux de degré 2 et 3. Donc il existe une expression radicale de ξ n'utilisant que des radicaux de degré 2 et 3.

2 Premières propriétés

1. On munit L de la loi additive du corps L et de la loi externe $.: K\times L\to L$, restriction à $K\times L$ de la loi produit du corps L. Les axiomes de la structure d'espace vectoriel sont immédiats à vérifier.

2. Soient $(e_i)_{1\leq i\leq n}$ une base du K-espace vectoriel L et $(f_j)_{1\leq j\leq m}$ une base du L-espace vectoriel M. On vérifie sans mal que $(e_if_j)_{i,j}$ est une base du K-espace vectoriel M.

3. On a bien entendu $K[a]\subset K(a)$. Pour vérifier l'égalité, il suffit d'établir que $K[a]$ est un corps. Or si $P\in K[X]$ est tel que $P(a)\neq 0$, alors $P\wedge\pi_{a,K}=1$ (car $\pi_{a,K}$ est irréductible) et il existe, par Bezout, $U,V\in K[X]$ tels que $UP+V\pi_{a,K}=1$. Il vient $U(a)P(a)=1$ d'où $P(a)^{-1}\in K[a]$.

   Notons qu'il est aussi possible d'utiliser le lemme prouvé dans la question suivante.

   On voit par ailleurs aisément que $1,a,a^2,\ldots,a^{d-1}$ (où $d=\deg(\pi_{a,K})$ est une base de $K[a]$. Donc $[K(a):K]=d$.

4. (a) Les deux applications proposées sont linéaires et de noyau restreint à $\{0\}$ (car a n'est pas un diviseur de zéro). L'algèbre A étant de dimension finie, ce sont des isomorphismes (d'espaces vectoriels). En particulier elles sont surjectives et il existe $b,c\in A$ tels que $ab=ca=1_A$. Il vient $b=(ca)b=c(ab)=c$: a est inversible.

   (b) Il est évident que LM contient l'ensemble N des éléments de la forme indiquée. Pour prouver l'égalité, il suffit de prouver que N est un corps. Or N est de manière évidente une K-algèbre unitaire intègre de dimension finie (car si $(e_i)_{1\leq i\leq s}$ et $(f_j)_{1\leq j\leq t}$ sont des K-bases de de L et M, alors $(e_if_j)_{i,j}$ est une famille génératrice de N) donc, d'après la question précédente, un corps.

3 K-morphismes de L dans $\mathbb{C}$

1. Comme $\deg(P')=\deg(P)-1$ et parce que P est irréductible, on a $P\wedge P'=1$. Donc les racines de P dans $\mathbb{C}$ sont simples.

2. On a, pour tout $P\in K[X]$ et $x\in L$, $\sigma(P(x))=P^\sigma(\sigma(x))=P(\sigma(x))$. En substituant à P le polynôme $\pi_{x,K}$ (lorsque x est algébrique), il vient $\pi_{x,K}(\sigma(x))=0$.

3. (a) On a $\sigma(P(a)) = 0$ donc, puisque σ fixe chaque élément de K, $P(\sigma(a)) = 0$, d'où $\sigma(a) \in \{a_1, a_2, \ldots, a_p\}$.

   (b) Si Q et $R \in K[X]$ sont tels que $Q(a) = R(a)$, alors $\pi_{a,K}$ divise $Q - R$ et, par conséquent, $Q(a_k) = R(a_k)$. On peut donc, de manière cohérente, définir une application $\sigma : K(a) \to \mathbb{C}$ en posant $\sigma(Q(a)) = Q(a_k)$. C'est un K-morphisme de corps puisque $\sigma(x) = x$ pour tout $x \in K$ et, pour tous Q et $R \in K[X]$, $\sigma(Q(a)R(a)) = \sigma((QR)(a))) = (QR)(a_k) = Q(a_k)R(a_k) = \sigma(Q(a))\sigma(R(a))$ et, de même, $\sigma(Q(a) + R(a)) = \sigma(Q(a)) + \sigma(R(a))$.

   On peut aussi, de manière plus savante, considérer les morphismes d'anneaux

$$\phi : \begin{array}{ccc} K[X] & \to & K(a) \\ P & \mapsto & P(a) \end{array} \qquad \text{et} \qquad \psi_k : \begin{array}{ccc} K[X] & \to & \mathbb{C} \\ P & \mapsto & P(a_k) \end{array}$$

   Ils passent au quotient modulo l'idéal $(\pi_{a,K})$ et ϕ induit un isomorphisme $\tilde{\phi}$ de $\frac{K[X]}{(\pi_{a,K})}$ dans $K(a)$, ψ_k un morphisme $\tilde{\psi}_k$ de $\frac{K[X]}{(\pi_{a,K})}$ dans $\mathbb{C}$: l'application $\tilde{\psi}_k \circ \tilde{\phi}^{-1}$ convient.

   (c) Le polynôme P^η est un polynôme à coefficients dans $\eta(K)$, irréductible sur ce corps. Il admet donc p racines distinctes b_1, $b_2, \ldots,$ b_n. Un prolongement σ de η vérifie $\sigma(P(a)) = 0$ donc $P^\eta(\sigma(a)) = 0$, d'où $\sigma(a) \in \{b_1, b_2, \ldots, b_n\}$. Si $\sigma(a) = b_k$, il vient, pour tout $Q \in K[X]$, $\sigma(Q(a)) = Q^\eta(b_k)$. On vérifie comme ci-dessus que cette relation définit effectivement un morphisme σ (si $Q(a) = R(a)$ alors $\pi_{a,K}$ divise $Q - R$ donc $\pi^\eta_{a,K} = \pi_{b_k,\eta(K)}$ divise $Q^\eta - R^\eta$, d'où $Q^\eta(b_k) = R^\eta(b_k)$).

4. Il existe $b_1, b_2, \ldots, b_p \in L$ tels que $L = K(b_1, b_2, \ldots, b_p) = K(b_1)(b_2)\ldots(b_p)$. Soit d_k le degré de b_k sur $K(b_1, \ldots, b_{k-1})$. Alors il y a, d'après ce qui précède, d_1 K-morphismes de $K(b_1)$ dans $\mathbb{C}$. Chacun peut se prolonger de d_2 manières en un K-morphisme de $K(b_1)(b_2)$ dans $\mathbb{C}$ et, par une récurrence évidente, on voit qu'il existe $d_1 d_2 \ldots d_p = [L : K]$ K-morphismes de L dans $\mathbb{C}$.

5. C'est immédiat en adaptant très légèrement la construction qui vient d'être faite.

6. On a $|\operatorname{Mor}_K(M, \mathbb{C})| = [M : K] = [M : L][L : K] = |\operatorname{Mor}_L(M, \mathbb{C})||\operatorname{Mor}_K(L, \mathbb{C})|$.

7. Supposons le contraire, et considérons p minimal tel qu'existent $\sigma_1, \sigma_2, \ldots, \sigma_p \in \operatorname{Mor}_K(L, \mathbb{C})$, deux à deux distincts, et $\lambda_1, \ldots, \lambda_p \in K$ non tous nuls (donc tous non nuls par minimalité de p) tels que

$$\lambda_1\, \sigma_1 + \lambda_2\, \sigma_2 + \ldots + \lambda_p\, \sigma_p = 0$$

   Alors on a aussi, pour tout $y \in L$,

$$\lambda_1\sigma_1(y)\, \sigma_1 + \lambda_2\sigma_2(y)\, \sigma_2 + \ldots + \lambda_p\sigma_p(y)\, \sigma_p = 0$$

   Pour le voir, il suffit d'appliquer la première relation à xy, où $x \in L$ et d'utiliser le fait que les σ_i sont des morphismes.

   On en déduit, par une combinaison linéaire :

$$\lambda_1(\sigma_1(y) - \sigma_p(y))\, \sigma_1 + \lambda_2(\sigma_2(y) - \sigma_p(y))\, \sigma_2 + \ldots + \lambda_{p-1}(\sigma_{p-1}(y) - \sigma_p(y))\, \sigma_{p-1} = 0$$

Comme $\sigma_{p-1} \neq \sigma_p$, on peut choisir y tel que $\sigma_{p-1}(y) - \sigma_p(y) \neq 0$. La relation obtenue contredit la minimalité de p.

4 Théorème de l'élément primitif

1. Montrons par récurrence sur $p \in \mathbb{N}^*$ que E ne peut pas s'écrire comme réunion de p sous-espaces vectoriels stricts. C'est évident pour $p = 1$. Supposons $p > 1$ et l'énoncé vrai pour une valeur strictement inférieure. Soient $F_1, \ldots, F_p$ des sous-espaces vectoriels stricts. Alors il existe $a \in E \setminus F_1$ et $b \in E \setminus (F_2 \cup \ldots \cup F_p)$. La droite affine D passant par a et b n'est contenue ni dans aucun des F_i. Donc $\mathrm{Card}(D \cap F_i) \leq 1$ et $\mathrm{Card}\,(D \cap (\bigcup_{i=1}^p F_i)) \leq p$. Or D étant infinie (car K est infini), on ne peut avoir $\bigcup_{i=1}^p F_i = E$.

2. On a les d'équivalences :

$$\xi \text{ primitif} \iff K(\xi) = L \iff [L : K(\xi)] = 1 \iff |\mathrm{Mor}_{K(\xi)}(L, \mathbb{C})| = 1$$

Comme $\mathrm{Mor}_{K(\xi)}(L, \mathbb{C}) = \{\sigma \in \mathrm{Mor}_K(L, \mathbb{C});\ \sigma(\xi) = \xi\}$, la conclusion suit.

3. L'ensemble des éléments non primitifs est, d'après la question **2.** (et en notant abusivement id l'injection canonique de L dans $\mathbb{C}$),

$$\bigcup_{\sigma \in \mathrm{Mor}_K(L,\mathbb{C}) \setminus \{\mathrm{id}\}} \{x \in L;\ \sigma(x) = x\}$$

Il s'agit d'une réunion finie de sous-K-espaces vectoriels stricts de L. Comme K est infini, la question **1.** montre qu'elle est strictement incluse dans L. Il existe donc des éléments primitifs.

5 Groupe de Galois d'un polynôme

1. $(i) \implies (ii)$: il suffit d'appliquer (i) à $F - G$.
$(ii) \implies (iii)$ Il suffit d'appliquer (ii) en prenant pour G la fraction rationnelle constante égale à $F(a, b, \ldots, z)$.
$(iii) \implies (i)$ Immédiat.

Il est immédiat aussi que id satisfait (i). Convenons de noter, dans cette question uniquement, pour $\sigma \in \mathcal{S}\{a, b, \ldots, z\}$ et $F \in K(A, B, \ldots, Z)$, $F^\sigma = F(\tilde{\sigma}(A), \tilde{\sigma}(B), \ldots, \tilde{\sigma}(Z))$, où $\tilde{\sigma}$ est la permutation de $A, B, \ldots, Z$ correspondante à σ. Supposons que σ et σ' satisfont (i). Alors $F(\sigma \circ \sigma'(a), \sigma \circ \sigma'(b), \ldots, \sigma \circ \sigma'(z)) = F^\sigma(\sigma'(a), \sigma'(b), \ldots, \sigma'(z))$. Comme σ' vérifie (i) et $F^\sigma \in K[A, B, \ldots, Z]$, on a $F(\sigma \circ \sigma'(a), \sigma \circ \sigma'(b), \ldots, \sigma \circ \sigma'(z)) = F^\sigma(a, b, \ldots, z) = F(\sigma(a), \sigma(b), \ldots, \sigma(z)) = F(a, b, \ldots, z)$, d'où l'on déduit que $\sigma \circ \sigma'$ vérifie (i).

De même, $F(\sigma^{-1}(a), \sigma^{-1}(b), \ldots, \sigma^{-1}(z)) = F^{\sigma^{-1}}(a, b, \ldots, z)$
$= F^{\sigma^{-1}}(\sigma(a), \sigma(b), \ldots, \sigma(z)) = F(a, b, \ldots, z)$, donc σ^{-1} vérifie (i).

On a ainsi montré que $\mathrm{Gal}_K(P)$ est un sous-groupe de $\mathcal{S}\{a; b; \ldots, z\}$.

2. Soient σ une permutation galoisienne des racines. Tout élément $z \in L$ peut s'écrire sous la forme $z = F(a, b, \ldots, z)$, où $F \in K(A, B, \ldots, Z)$. Bien sûr, F n'est pas unique, mais l'énoncé (ii) montre que la quantité $F(\sigma(a), \sigma(b), \ldots, \sigma(z))$ est indépendante du choix de F. On peut donc définir un prolongement $\sigma : L \to L$ de σ (que de manière abusive on note encore σ) en posant $\sigma(F(a, b, \ldots, z)) = F(\sigma(a), \sigma(b), \ldots, \sigma(z))$. Cette nouvelle application est un morphisme de corps puisque $\sigma(1) = 1$,

$$\begin{aligned}\sigma(F(a,b,\ldots,z)G(a,b,\ldots,z)) &= \sigma((FG)(a,b,\ldots,z)) \\ &= (FG)(\sigma(a),\sigma(b),\ldots,\sigma(z)) \\ &= F(\sigma(a),\sigma(b),\ldots,\sigma(z))G(\sigma(a),\sigma(b),\ldots,\sigma(z))\end{aligned}$$

et de la même façon,
$\sigma(F(a, b, \ldots, z)G(a, b, \ldots, z)) = F(\sigma(a), \sigma(b), \ldots, \sigma(z)) + G(\sigma(a), \sigma(b), \ldots, \sigma(z))$. L'énoncé (iii) montre ensuite que σ est un K-morphisme. Enfin, comme L est de dimension finie sur K (et que σ est injective comme tout morphisme de corps), σ est bien un automorphisme de L.

Réciproquement, si $\sigma : L \to L$ est un K-morphisme (donc un K-automorphisme), on a pour toute racine x de P, $P(\sigma(x)) = \sigma(P(x)) = 0$. Donc $\sigma(x)$ est une racine de P. Comme σ est une application injective, σ induit une permutation des racines $a, b, \ldots, z$ de P. Enfin, si $F(a, b, \ldots, z) = 0$ alors $F(\sigma(a), \sigma(b), \ldots, \sigma(z)) = \sigma(F(a, b, \ldots, z)) = 0$: la permutation induite est bien galoisienne.

3. Tout $x \in L$ peut s'écrire $x = Q(a, b, \ldots, z)$, où $Q \in K[A, B, \ldots, Z]$. Pour $\sigma \in \mathrm{Mor}_K(L, \mathbb{C})$, on a $\sigma(x) = \sigma(Q(a, b, \ldots, z) = Q(\sigma(a), \sigma(b), \ldots, \sigma(z))$. Or, comme ci-dessus, σ induit une permutation des racines de P. Donc $\sigma(x) \in L$. Ainsi σ est à valeurs dans $\mathbb{C}$ et, d'après **3.4.**, $|\operatorname{Gal}_K(P)| = n$.

4. On sait qu'il existe $R \in K[X]$ tel que $x = R(x)$. Soit $Q \in K_{n-1}[X]$ le reste dans la division euclidienne de R par $\pi_{\xi,K}$ (qui est de degré n). On a bien $\deg(Q) \leq n - 1$ et $x = Q(\xi)$. Pour tout $\sigma \in \operatorname{Gal}_K(P)$ (qu'on a identifié à $\operatorname{Gal}_K(L)$), on a $x = \sigma(x) = \sigma(Q(\xi)) = Q(\sigma(\xi))$. Comme $\sigma(\xi)$ parcourt l'ensemble des conjugués de ξ quand σ parcourt $\operatorname{Gal}_k(P)$, on a $x = Q(\xi')$ pour tout conjugué ξ' de ξ. Le polynôme $Q - x \in L_{n-1}[X]$, qui admet ainsi (au moins) n racines distinctes dans $\mathbb{C}$ est donc nul et l'on a, puisque les coefficients de Q sont dans K, $x \in K$.

   On en déduit immédiatement l'équivalence

$$\operatorname{Gal}_K(P) = \{\mathrm{id}\} \quad \Longleftrightarrow \quad L = K \quad \Longleftrightarrow \quad P \text{ scindé}$$

5. Si a est une racine de P, l'ensemble des racines de P est $\{a\xi^k,\ k \in [\![0, n-1]\!]\}$, où ξ est une racine primitive n-ième de l'unité. Pour tout $\sigma \in \operatorname{Gal}_K(P)$, il existe donc $j \in [\![0, n-1]\!]$ tel que $\sigma(a) = a\xi^j$, et σ est entièrement déterminé par la donnée de j puisque, dans la mesure où $\xi \in K$, on a $\sigma(\xi) = \xi$ donc $\sigma(a\xi^k) = \sigma(a)\sigma(\xi)^k = a\xi^{k+j}$.

L'application

$$\begin{array}{rccc} \phi & : & \mathrm{Gal}_K(P) & \to & \frac{\mathbb{Z}}{n\mathbb{Z}} \\ & & \sigma & \mapsto & [j]_n \end{array}$$

est un morphisme de groupe (car si $\sigma(a) = a\xi^j$ et $\sigma'(a) = a\xi^{j'}$ alors $\sigma' \circ \sigma(a) = a\xi^{j+j'}$) injectif (car si $j \equiv 0\ [n]$ alors $\sigma(a) = a\xi^j = a$). Donc $\mathrm{Gal}_K(P)$ est isomorphe à un sous-groupe de $\frac{\mathbb{Z}}{n\mathbb{Z}}$ et, par conséquent, est un groupe cyclique.

6. (a) Si tel n'était pas le cas, on aurait la relation $\sum_{k=0}^{n-1} \xi^{-k}\sigma^k = 0$, contredisant la liberté sur K de la famille $(\mathrm{id}, \sigma, \sigma^2, \ldots, \sigma^{n-1})$ (lemme de Dedekind).

   (b) On a $\sigma(a) = \sum_{k=0}^{n-1} \xi^{-k}\sigma^{k+1}(\theta) = \xi \sum_{k=0}^{n-1} \xi^{-(k+1)}\sigma^{k+1}(\theta) = \xi a$.

   On en déduit $\sigma(a^k) = \xi^k a^k$ pour tout $k \in [\![0, n-1]\!]$. On peut interpréter cette relation en disant que a^k est un vecteur propre pour la valeur propre ξ^k de l'application σ vue comme endomorphisme du K-espace vectoriel L. Donc $(1, a, \ldots, a^{n-1})$ est K-libre.

   Par ailleurs, $\sigma(a^n) = a^n$. Comme σ est un générateur de $\mathrm{Gal}_K(L)$, a^n est un point fixe de tous les éléments de $\mathrm{Gal}_K(L)$ et, par **4**, $a^n \in K$ (rappelons que toute extension galoisienne est le corps de décomposition d'un polynôme; ce qui a été fait en **4** s'applique donc).

   (c) Posons $\alpha = a^n$. Comme $\alpha \in K$ et parce que $(1, a, \ldots, a^{n-1})$ est K-libre, $\pi_{a,K} = X^n - a$. On a donc $[K(a) : K] = n = |\mathrm{Gal}_K(L)| = [L : K]$ (car l'extension $K \subset L$ est galoisienne) d'où, puisque $K(a) \subset L$, $L = K(a) = K(a, a\xi, \ldots, a\xi^{n-1})$ (car $\mathbb{U}_n \subset K$) : L est bien le corps de décomposition de $X^n - \alpha$.

7. Le corps $K(\xi)$ est le corps de décomposition sur K de $X^n - 1$. C'est donc une extension galoisienne de K et tout $\sigma \in \mathrm{Gal}_K(K(\xi))$ est déterminé par l'image de ξ, qui est un conjugué de ξ donc de la forme $\sigma(\xi) = \xi^j$. Si σ et σ' sont deux éléments de $\mathrm{Gal}_K(K(\xi))$ et qu'on pose $\sigma(\xi) = \xi^j$, $\sigma'(\xi) = \xi^{j'}$, alors $\sigma \circ \sigma'(\xi) = \sigma(\xi^{j'}) = \xi^{jj'} = \sigma' \circ \sigma(\xi)$ d'où $\sigma \circ \sigma' = \sigma' \circ \sigma$.

8. (a) Tout L-morphisme de M dans $\mathbb{C}$ est aussi un K-morphisme, donc est à valeurs dans M (car $K \subset M$ est galoisienne). Donc $L \subset M$ est galoisienne.

   De plus, $\mathrm{Gal}_L(M) \subset \mathrm{Gal}_K(M)$ de manière évidente.

   (b) Il est clair que si $\phi \in \mathrm{Gal}_L(M)$, alors $\sigma\phi\sigma^{-1} \in \mathrm{Gal}_{\sigma(L)}(M)$. Donc $\sigma\,\mathrm{Gal}_L(M)\sigma^{-1} \subset \mathrm{Gal}_{\sigma(L)}(M)$. De même, puisque $L = \sigma^{-1}(\sigma(L))$, $\sigma^{-1}\,\mathrm{Gal}_{\sigma(L)}(M)\sigma \subset \mathrm{Gal}_L(M)$ et l'égalité suit.

   (c) L'extension $K \subset L$ est galoisienne si et seulement si L est stable par tout élément de $\mathrm{Mor}_K(L, \mathbb{C})$. Or tout K-morphisme de L dans $\mathbb{C}$ peut s'étendre en un K-morphisme de M dans $\mathbb{C}$ d'après **3.5.** donc, en fait, en un élément de $\mathrm{Gal}_K(M)$ puisque $K \subset M$ est galoisienne. Donc $(i) \iff (ii)$.

   Supposons maintenant (ii). Alors $\sigma(L) = L$ (ces deux K-espaces vectoriels ont même dimension) et $\sigma\,\mathrm{Gal}_L(M)\sigma^{-1} = \mathrm{Gal}_{\sigma(L)}(M) = \mathrm{Gal}_L(M)$, d'où (iii).

Supposons maintenant (iii). Alors $\mathrm{Gal}_{\sigma(L)}(M) = \sigma\,\mathrm{Gal}_L(M)\sigma^{-1} \supset \mathrm{Gal}_L(M)$. Donc les éléments de $\sigma(L)$ sont fixés par tous les L-morphismes de M ce qui, par **4.**, montre $\sigma(L) \subset L$.

On a ainsi prouvé l'équivalence des trois énoncés. Considérons, dans l'hypothèse où ils sont vrais, l'application $\mathrm{Gal}_K(M) \to \mathrm{Gal}_K(L)$ qui à un morphisme associe l'application induite sur L (correctement définie grâce à (ii)). C'est un morphisme, surjectif par **3.5.** et parce que $K \subset M$ est galoisienne. Son noyau est $\{\sigma \in \mathrm{Gal}_K(M);\ \forall x \in L, \sigma(x) = x\} = \mathrm{Gal}_L(M)$. Donc elle induit un isomorphisme de $\frac{\mathrm{Gal}_K(M)}{\mathrm{Gal}_L(M)}$ sur $\mathrm{Gal}_K(L)$.

6 Augmentation du corps de base

1. Soit $\sigma \in \mathrm{Mor}_L(LM, \mathbb{C})$. Tout élément z de LM peut s'écrire $z = \sum_{i=1}^p x_i y_i$, où $x_i \in L$, $y_i \in M$ et l'on a $\sigma(z) = \sum_{i=1}^p \sigma(x_i) y_i$. Or $\sigma(x_i) \in L$ puisque σ fixe K et que $K \subset L$ est galoisienne. Donc $\sigma(z) \in LM$: on a prouvé que $M \subset LM$ est galoisienne.

   De manière alternative, on peut dire que, $K \subset L$ étant galoisienne, L est le corps de décomposition d'un polynôme $P \in K[X]$ et que LM est le corps de décomposition de P vu comme polynôme de $M[X]$, donc que $M \subset LM$ est galoisienne.

2. Soit $\sigma \in \mathrm{Gal}_M(LM)$. Comme σ fixe K et que $K \subset L$ est galoisienne, on a $\sigma(L) \subset L$ et σ induit un K-morphisme ϕ de L, c'est-à-dire un élément de $\mathrm{Gal}_K(L)$. L'application qui a σ associe ϕ est évidemment un morphisme de groupe. Si $\phi = \mathrm{id}_L$, alors σ fixe chaque élément de L. Comme σ fixe chaque élément de M, σ fixe chaque élément de $L \cup M$ donc de LM. L'application $\sigma \mapsto \phi$ est donc un morphisme injectif. Son image est clairement contenue dans $\mathrm{Gal}_{L\cap M}(L)$.

   Soit maintenant $\phi \in \mathrm{Gal}_{L\cap M}(L)$. Soit a un élément primitif de l'extension $L\cap M \subset M$: $M = (L \cap M)(a)$ (il en existe puisque cette extension est évidemment de degré fini). On sait par **3.5** que ϕ peut se prolonger en un $L \cap M$-morphisme de $\sigma : L(a) \to \mathbb{C}$ vérifiant $\sigma(a) = a$ (et donc $\forall x \in M,\ \sigma(x) = x$). Or $L \cup M \subset L(a) \subset LM$, d'où $L(a) = LM$. On a ainsi $\sigma \in \mathrm{Mor}_M(LM, \mathbb{C})$ et, puisque $M \subset LM$ est galoisienne, $\sigma \in \mathrm{Gal}_M(LM)$.

   On a prouvé que l'application $\sigma \mapsto \phi$ est un isomorphisme de $\mathrm{Gal}_M(LM)$ dans $\mathrm{Gal}_{L\cap M}(L)$.

3. (a) Comme $K \subset L$ et $K \subset M$ sont galoisiennes, tous les K-conjugués d'un élément de $L \cap M$ sont dans L dans M, donc dans $L \cap M$. L'extension $K \subset L \cap M$ est donc galoisienne. Par **5.8c.**, appliqué à la suite d'extension $K \subset L \cap M \subset L$, on a $\mathrm{Gal}_K(L \cap M) \simeq \frac{\mathrm{Gal}_K(L)}{\mathrm{Gal}_{L\cap M}(L)}$.

   (b) Les rôles de L et M sont ici symétriques. On a donc, modulo les identifications faites dans l'énoncé,

$$\frac{\mathrm{Gal}_K(L)}{\mathrm{Gal}_M(LM)} \simeq \mathrm{Gal}_K(L \cap M) \simeq \frac{\mathrm{Gal}_K(M)}{\mathrm{Gal}_L(LM)}$$

7 Le groupe d'une équation résoluble est résoluble

1. Soit $L = K(a, b, \ldots, z)$ le corps de décomposition de P et $M = K(\xi)$. Ces deux extensions sont galoisiennes (la seconde parce que ξ est primitive) et l'on a $LM = L(\xi)$. De plus, $\mathrm{Gal}_K(L) = \mathrm{Gal}_K(P)$, $\mathrm{Gal}_{K(\xi)}(L(\xi)) = \mathrm{Gal}_{K(\xi)}(P)$ (l'égalité est un peu abusive mais l'inclusion de $\mathrm{Gal}_{K(\xi)}(P)$ dans $\mathrm{Gal}_K(P)$ correspond bien à l'injection de $\mathrm{Gal}_{K(\xi)}(L(\xi))$ dans $\mathrm{Gal}_K(L)$).

   Par la question précédente, on a donc $\mathrm{Gal}_{K(\xi)}(P) \lhd \mathrm{Gal}_K(P)$, $\mathrm{Gal}_L(L(\xi)) \lhd \mathrm{Gal}_K(K(\xi))$, et $\frac{\mathrm{Gal}_K(P)}{\mathrm{Gal}_{K(\xi)}(P)} = \frac{\mathrm{Gal}_K(L)}{\mathrm{Gal}_{K(\xi)}(L(\xi))} \simeq \frac{\mathrm{Gal}_K(K(\xi))}{\mathrm{Gal}_L(L(\xi))}$. Comme $\mathrm{Gal}_K(K(\xi))$ est abélien par **5.7.**, le groupe $\frac{\mathrm{Gal}_K(P)}{\mathrm{Gal}_{K(\xi)}(P)}$ est abélien.

2. L'extension $K \subset K(r)$ est galoisienne puisque, $\mathbb{U}_q$ étant contenu dans K, $K(r)$ est le corps de décomposition sur K de $X^q - r^q \in K[X]$. Comme ci-dessus, on a l'isomorphisme : $\frac{\mathrm{Gal}_K(P)}{\mathrm{Gal}_{K(r)}(P)} = \frac{\mathrm{Gal}_K(L)}{\mathrm{Gal}_{K(r)}(L(r))} \simeq \frac{\mathrm{Gal}_K(K(r))}{\mathrm{Gal}_L(L(r))}$

   Comme $\mathrm{Gal}_K(K(r))$ est cyclique par **5.5.**, il en est de même de $\frac{\mathrm{Gal}_K(P)}{\mathrm{Gal}_{K(\xi)}(P)}$.

3. On suppose P résoluble par radicaux, c'est-à-dire qu'il existe une suite de complexes $r_1, r_2, \ldots, r_q$ tels que $r_1^{n_1} \in K$ pour un certain $n_1 \in \mathbb{N}^*$, $r_2^{n_2} \in K(r_1)$ pour un certain $n_2 \in \mathbb{N}^*$, $\ldots$, $r_q^{n_q} \in K(r_1, r_2, \ldots, r_{q-1})$ pour un certain $n_q \in \mathbb{N}^*$ et tels que les racines de P appartiennent à $K(r_1, r_2, \ldots, r_q)$. Comme $K(r_1, r_2, \ldots, r_{q-1})$ ne contient pas nécessairement $\mathbb{U}_{n_q}$, on ne peut appliquer directement la question précédente.

   Notons ξ_k une racine primitive n_k-ième de l'unité et considérons les extensions de corps
   $$K \subset K(\xi_1) \subset K(\xi_1, r_1) \subset K(\xi_1, \xi_2, r_1) \subset K(\xi_1, \xi_2, r_1, r_2) \subset \ldots$$
   $$\subset K(\xi_1, \xi_2, \ldots, \xi_q, r_1, r_2, \ldots, r_q)$$

   Les groupes de galois successifs de P forment une suite décroissante et le dernier est réduit au neutre puisue P est scindé sur $K(\xi_1, \ldots, \xi_q, r_1, \ldots, r_q)$:

   $$\mathrm{Gal}_K(P) \supset \mathrm{Gal}_{K(\xi_1)}(P) \supset \mathrm{Gal}_{K(\xi_1, r_1)}(P) \supset \ldots \supset \mathrm{Gal}_{K(\xi_1 \ldots, \xi_q, r_1, \ldots, r_q)}(P) = \{\mathrm{id}\}$$

   Par **1.** et **2.**, chaque groupe est distingué dans le précédent et les quotients successifs sont abéliens. On a montré que $\mathrm{Gal}_K(P)$ est un groupe résoluble.

8 Une équation dont le groupe est résoluble est résoluble par radicaux

1. Soient $\pi : G \to \frac{G}{H}$ la surjection canonique et J un sous-groupe strict maximal de $\frac{G}{H}$. Posons $H' = \pi^{-1}(J)$. C'est un sous-groupe distingué de G car, $\frac{G}{H}$ étant abélien, J est un sous-groupe distingué de $\frac{G}{H}$. De plus, l'application canonique $G \to \frac{G/H}{J}$ (qui a $x \in G$ associe la classe modulo J de la classe modulo H de x) est surjective de noyau H'. Elle induit donc un isomorphisme de $\frac{G}{H'}$ sur $\frac{G/H}{J}$. Or, par maximalité de J, $\frac{G/H}{J}$ ne contient aucun sous-groupe non trivial. C'est donc un groupe cyclique (d'ordre égal à 1 ou premier).

2. Soit G un groupe résoluble et H un sous-groupe de G. Il existe par hypothèse une suite

$$\{e\} = G_0 \subset G_1 \subset \ldots \subset G_{m-1} \subset G_m = G$$

de sous-groupes de G vérifiant, pour tout $i \in [\![1, m]\!]$: $G_{i-1} \lhd G_i$ et $\frac{G_i}{G_{i-1}}$ abélien.

Considérons la suite

$$\{e\} = G_0 \cap H \subset G_1 \cap H \subset \ldots \subset G_{m-1} \cap H \subset G_m \cap H = H$$

de sous-groupes de H.

On a, pour tout $g \in G_i \cap H$, $g(G_{i-1} \cap H)g^{-1} \subset G_i$ car $G_{i-1} \lhd G_i$, et $g(G_{i-1} \cap H)g^{-1} \subset H$ de manière évidente. Donc $G_{i-1} \cap H \lhd G_i \cap H$.

De plus, l'application $G_i \cap H \to \frac{G_i}{G_{i-1}}$ (qui a x associe sa classe modulo G_{i-1} a pour noyau $G_{i-1} \cap H$. Elle induit donc une injection de $\frac{G_i \cap H}{G_{i-1} \cap H}$ dans $\frac{G_i}{G_{i-1}}$, ce qui montre que $\frac{G_i \cap H}{G_{i-1} \cap H}$ est abélien.

On a prouvé que H est résoluble.

3. (a) C'est évident, puisque P est dans ce cas un polynôme scindé sur K.

   (b) Si $\mathrm{Gal}_{K(\xi)}(P)) \subsetneq \mathrm{Gal}_K(P)$ alors, puisque $\mathrm{Gal}_{K(\xi)}(P))$ est résoluble par **2.** et par l'hypothèse de récurrence, P est résoluble par radicaux sur $K(\xi)$. Comme ξ est radical d'un élément de K, P est résoluble par radicaux sur K.

   Supposons maintenant $\mathbb{U}_q \subset K$. On a admis $\mathrm{Gal}_{L^H}(L) = H$. Donc $\mathrm{Gal}_{L^H}(L)$ est un sous-groupe distingué de $\mathrm{Gal}_K(L)$ et l'extension $K \subset L^H$ est galoisienne de groupe de Galois isomorphe à $\frac{\mathrm{Gal}_K(L)}{H}$ qui est cyclique par hypothèse, disons d'ordre q. D'après **5.6.**, il existe $r \in L^H$ tel que $r^q \in K$ et $L^H = K(r)$. Il vient $\mathrm{Gal}_{K(r)}(P) = \mathrm{Gal}_{L^H}(L) = H$ qui est résoluble en tant que sous-groupe d'un groupe résoluble. Donc P est résoluble sur $K(r)$ par l'hypothèse de récurrence, donc résoluble sur K.

   Au final, P est résoluble sur K car en commençant par adjoindre ξ à K, soit le groupe de galois est effectivement réduit et l'on est dans le premier cas, soit il ne l'est pas et on peut, en substituant $K(\xi)$ à K, utiliser le second.

9 Un exemple d'équation non résoluble par radicaux

10 Points constructibles à la règle et au compas

11 La correspondance de Galois