THÉORIE DE GALOIS II - CORRIGÉ

Exercice 1 — 1. L'action du groupe $\mathrm{Gal}(\mathrm{K}(\mathscr{R})/\mathrm{K})$ sur $\mathrm{K}(\mathscr{R})$ stabilise l'ensemble $\mathscr{R}$ et définit donc un homomorphisme $\mathrm{Gal}(\mathrm{K}(\mathscr{R}/\mathrm{K}) \to \mathfrak{S}(\mathscr{R})$, qui est injectif car un élément de $\mathrm{Gal}(\mathrm{K}(\mathscr{R}/\mathrm{K})$ opèrant trivialement sur $\mathscr{R}$ est trivial.

2. L'élément $\mathrm{D} = (-1)^{\frac{n(n-1}{2}} \prod_{x\neq y\in\mathscr{R}}(x-y)$ de $\mathrm{K}(\mathscr{R})$ est invariant par toute permutation de $\mathscr{R}$, donc par $\mathrm{Gal}(\mathrm{K}(\mathscr{R}/\mathrm{K})$, et D appartient au corps K.

Ayant choisi un ordre total sur $\mathscr{R}$, on peut écrire D sous la forme

$$\mathrm{D} = \prod_{x<y}(x-y)^2$$

et cela montre que D est un carré dans K. Quelle que soit la permutation $\sigma \in \mathfrak{S}(\mathscr{R})$,

$$\sigma\left(\prod_{x<y}(x-y)\right) = \prod_{x<y}(\sigma(x)-\sigma(y)) = (-1)^r \prod_{x<y}(x-y)$$

où r est le nombre de couples $(x,y) \in \mathscr{R}^2$ tels que $x<y$ et $\sigma(x)>\sigma(y)$; lorsque le corps K est de caractéristique distincte de 2, $(-1)^r$ est la signature $\varepsilon(\sigma)$ de la permutation σ et nous en déduisons qu'une permutation de $\mathscr{R}$ fixe chacune des deux racines carrées de D dans $\mathrm{K}(\mathscr{R})$ si et seulement si elle est *paire*.

Vu ce que l'on vient de dire, le discriminant D est un carré dans K (de caractéristique distincte de 2) si et seulement si le groupe $\mathrm{Gal}(\mathrm{K}(\mathscr{R})/\mathrm{K})$ est contenu dans le groupe alterné $\mathfrak{A}(\mathscr{R})$.

3. Écrivant P sous la forme $a\prod_{x\in\mathscr{R}}(\mathrm{T}-x)$, $\mathrm{P}' = a\sum_{x\in\mathscr{R}}\prod_{y\neq x}(\mathrm{T}-y)$ et donc

$$\prod_{x\neq y}(x-y) = \prod_{x\in\mathscr{R}}\prod_{y\neq x}(x-y) = \prod_{x\in\mathscr{R}} a^{-1}\mathrm{P}'(x) = a^{-n}\prod_{x\in\mathscr{R}}\mathrm{P}'(x),$$

soit

$$a^n\mathrm{D} = (-1)^{\frac{n(n-1)}{2}}\prod_{x\in\mathscr{R}}\mathrm{P}'(x).$$

Si l'on pose d'autre part $\mathrm{P}' = a\prod_{\lambda\in\mathscr{R}'}(\mathrm{T}-\lambda)$,

$$\prod_{x\in\mathscr{R}}\mathrm{P}'(x) = a^n\prod_{x\in\mathscr{R}}\prod_{\lambda\in\mathscr{R}'}(x-\lambda) = (-1)^{n-1}a^n\prod_{\lambda\in\mathscr{R}'}\prod_{x\in\mathscr{R}}(\lambda-x) = (-1)^{\frac{n(n-1)}{2}}a^n\prod_{\lambda\in\mathscr{R}'}a^{-1}\mathrm{P}(\lambda) = (-1)^{\frac{n(n-1)}{2}}a\prod_{\lambda\in\mathscr{R}'}\mathrm{P}(\lambda),$$

c'est-à-dire

$$a^{n-1}\mathrm{D} = (-1)^{\frac{n(n-1)}{2}}\prod_{\lambda\in\mathscr{R}'}\mathrm{P}(\lambda).$$

Si l'on note x_1 et x_2 les deux racines de $\mathrm{T}^2+a\mathrm{T}+b$, $\mathrm{D} = (x_1-x_2)^2 = x_1^2+x_2^2-2x_1x_2 = (x_1+x_2)^2-4x_1x_2 = a^2-4b$.

Pour calculer le discriminant du polynôme $\mathrm{T}^3+p\mathrm{T}+q$, on peut utiliser la formule faisant intervenir les racines du polynômes dérivé :

$$\begin{aligned}\mathrm{D} &= -27\left(\sqrt{\frac{-p}{3}}^3 + p\sqrt{\frac{-p}{3}}+q\right)\left(\sqrt{-\frac{-p}{3}}^3 - p\sqrt{\frac{-p}{3}}+q\right) = -27\left(\frac{2p}{3}\sqrt{\frac{-p}{3}}+q\right)\left(-\frac{2p}{3}\sqrt{\frac{-p}{3}}+q\right)\\ &= -27\left(\frac{2p^3}{27}+q^2\right) = -4p^3-27q^2.\end{aligned}$$

Exercice 2 — 1. L'entier n étant premier à la caractéristique du corps K, les polynômes T^n-1 et $n\mathrm{T}^{n-1}$ sont premiers entre eux ; le polynôme T^n-1 est donc séparable sur K et son corps de décomposition $\mathrm{K}(\mu_n)$ (dans une clôture algébrique de K) est par conséquent une extension galoisienne de K.

2. Le groupe $\mathrm{Gal}(\mathrm{K}(\mu_n)/\mathrm{K})$ opère par permutation sur l'ensemble μ_n des racines n-èmes de l'unité dans $\mathrm{K}(\mu_n)$. Étant donnée une racine *primitive* $\zeta \in \mu_n$ — c'est-à-dire un générateur du groupe cyclique μ_n — $\sigma(\zeta)$ est encore une racine primitive pour tout automorphisme $\sigma \in \mathrm{Gal}(\mathrm{K}(\mu_n)/\mathrm{K})$ et il existe donc une application bien définie

$\chi_\zeta : \mathrm{Gal}(\mathrm{K}(\mu_n)/\mathrm{K}) \to (\mathbb{Z}/n\mathbb{Z})^\times$ telle que $\sigma(\zeta) = \zeta^{\chi_\zeta(\sigma)}$ pour tout $\sigma \in \mathrm{Gal}(\mathrm{K}(\mu_n)/\mathrm{K})$. Étant données deux racines primitives $\zeta, \xi \in \mu_n$, $\xi = \zeta^d$ avec $d \in (\mathbb{Z}/n\mathbb{Z})^\times$ donc

$$\xi^{\chi_\xi(\sigma)} = \sigma(\xi) = \sigma(\zeta^d) = \sigma(\zeta)^d = \zeta^{d\chi_\zeta(\sigma)}$$

et $\chi_\zeta(\sigma) = \chi_\xi(\sigma)$ pour tout élément σ de $\mathrm{Gal}(\mathrm{K}(\mu_n)/\mathrm{K})$. Nous obtenons ainsi l'existence d'une application

$$\chi : \mathrm{Gal}(\mathrm{K}(\mu_n)/\mathrm{K}) \to (\mathbb{Z}/n\mathbb{Z})^\times$$

telle que $\sigma(\zeta) = \zeta^{\chi(\sigma)}$ pour toute racine *primitive* $\zeta \in \mu_n$ et tout $\sigma \in \mathrm{Gal}(\mathrm{K}(\mu_n)/\mathrm{K})$. La dernière identité est bien entendue valable sans restriction sur la racine de l'unité : étant donnée une racine primitve $\zeta \in \mu_n$, tout élément de μ_n est de la forme ζ^d avec $d \in \mathbb{Z}$ et $\sigma(\zeta^d) = \sigma(\zeta)^d = \zeta^{d\chi(\sigma)} = (\zeta^d)^{\chi(\sigma)}$. Il est immédiat de vérifier que l'application χ est un homomorphisme de groupes : quelle que soit la racine primitive ζ,

$$\tau\sigma(\zeta) = \tau(\zeta^{\chi(\sigma)}) = \zeta^{\chi(\tau)\chi(\sigma)}$$

et donc $\chi(\tau\sigma) = \chi(\tau)\chi(\sigma)$. Enfin, l'injectivité de χ est claire puisque un élément de $\mathrm{Gal}(\mathrm{K}(\mu_n)/\mathrm{K})$ est uniquement déterminé par sa restriction à μ_n.

3. Soit μ_n' le sous-ensemble de μ_n formé des racines *primitives*. Quelle que soit la racine primitive $\zeta \in \mu_n'$, les conjugués de ζ dans $\mathrm{K}(\mu_n)$ sont les racines du polynômes minimal f_ζ de ζ sur K ; le polynôme

$$\Phi_n = \prod_{\zeta \in \mu_n'} (\mathrm{T} - \zeta) = \prod_{\mu_n'/\mathrm{Gal}(\mathrm{K}(\mu_n)/\mathrm{K})} f_\zeta$$

appartient par conséquent à $\mathrm{K}[\mathrm{T}]$.

L'homomorphisme χ est surjectif si et seulement si le groupe $\mathrm{Gal}(\mathrm{K}(\mu_n)/\mathrm{K})$ est d'ordre $\varphi(n)$; comme $\deg(\Phi_n) = \varphi(n)$, cela est le cas si et seulement si $\mathrm{Gal}(\mathrm{K}(\mu_n)/\mathrm{K})$ opère transitivement sur μ_n', ce qui équivaut à l'irréductibilité du polynôme Φ_n.

4. (i) De manière générale, tout polynôme unitaire $\mathrm{P} \in \mathbb{Q}[\mathrm{T}]$ dont les racines sont des entiers algébriques est à coefficients entiers : en effet, l'expression des coefficients de P comme fonctions symétriques élémentaires de ses racines montre que ceux-ci sont également des entiers algébriques, et ce sont donc des entiers puisque l'anneau $\mathbb{Z}$ est intégralement clos. Cette observation s'applique dans le cas que l'on considère puisque les racines de l'unité sont des entiers algébriques.

(ii) Par construction, le polynôme P divise $\mathrm{Q}(\mathrm{T}^p)$ dans $\mathbb{Q}[\mathrm{T}]$: $\mathrm{Q}(\mathrm{T}^p) = \mathrm{PR}$ avec $\mathrm{R} \in \mathbb{Q}[\mathrm{T}]$. En outre, le polynôme R est unitaire et ses racines, étant des racines de l'unité, sont des entiers algébriques ; on a donc $\mathrm{R} \in \mathbb{Z}[\mathrm{T}]$ et P divise ainsi $\mathrm{Q}(\mathrm{T}^p)$ dans $\mathbb{Z}[\mathrm{T}]$.

(iii) Comme $\mathrm{Q}(\mathrm{T}^p) = \mathrm{Q}(\mathrm{T})^p$ dans $\mathbb{F}_p[\mathrm{T}]$, la réduction modulo p de l'identité précédente montre que les polynômes P et Q ont une racine commune dans toute clôture algébrique de $\mathbb{F}_p$. Si P et Q étaient distincts, ces polynômes seraient deux facteurs irréductibles de Φ_n — car ζ et ζ^p sont toutes deux des racines primitives de l'unité — et Φ_n serait par suite divisible par le produit PQ dans $\mathbb{Z}[\mathrm{T}]$. En réduisant modulo p, il découlerait de ce que l'on vient de voir que le polynôme Φ_n aurait une racine double dans toute clôture algébrique de $\mathbb{F}_p$ et l'on aboutirait alors à une contradiction puisque, p et n étant premiers entre eux, le polynôme Φ_n est séparable sur $\mathbb{F}_p$ (c'est en effet un facteur du polynôme séparable $\mathrm{T}^n - 1$). Nous avons donc $\mathrm{P} = \mathrm{Q}$.

(iv) Nous venons de prouver que le polynôme minimal P de la racine primitive ζ s'annule en ζ^p pour tout nombre premier p ne divisant pas n. Comme ζ^p est encore une racine primitive, un raisonnement par récurrence évident permet d'en déduire que P s'annule en ζ^m pour tout entier non nul m premier à n ; P s'annule par conséquent en chaque racine primitive, ce qui implique $\mathrm{P} = \Phi_n$ et prouve que le polynôme Φ_n est irréductible sur $\mathbb{Q}$.

Exercice 3 — 1. Dire que le groupe $\mu_n(\mathrm{K})$ est d'ordre n revient à demander que le polynôme $\mathrm{T}^{-}1$ soit scindé à racines simples sur K, ce qui implique en particulier que l'entier n soit premier à la caractéristique de K.

Le polynôme $\mathrm{T}^n - a$ est scindé sur $\mathrm{K}(\alpha)$:

$$\mathrm{T}^n - a = \prod_{\zeta \in \mu_n(\mathrm{K})} (\mathrm{T} - \zeta\alpha)$$

et le corps $\mathrm{K}(\alpha)$, étant un corps de décomposition de $\mathrm{T}^n - a$, est une extension galoisienne de K.

L'application $\mathrm{Gal}(\mathrm{K}(\alpha)/\mathrm{K}) \to \mathrm{K}(\alpha)$, $\sigma \mapsto \frac{\sigma(\alpha)}{\alpha}$ est à valeurs dans le sous-groupe $\mu_n(\mathrm{K})$ de $\mathrm{K}^\times$. Étant donnés $\sigma,\ \tau \in \mathrm{Gal}(\mathrm{K}(\alpha)/\mathrm{K})$,

$$\frac{\tau\sigma(\alpha)}{\alpha} = \frac{\tau(\sigma(\alpha))}{\tau(\alpha)}\frac{\tau(\alpha)}{\alpha} = \tau\left(\frac{\sigma(\alpha)}{\alpha}\right)\frac{\tau(\alpha)}{\alpha} = \frac{\sigma(\alpha)}{\alpha}\frac{\tau(\alpha)}{\alpha}$$

car $\frac{\sigma(\alpha)}{\alpha} \in \mathrm{K}$; cette application est donc un homomorphisme de groupes. Il s'agit enfin manifestement d'une application injective.

Soit d le plus petit entier ≥ 1 tel que $\alpha^d = 1$. Le polynôme $\mathrm{T}^d - \alpha^d$ est irréductible sur K : en effet, le terme constant de tout facteur de degré $m \geq 1$ du polynôme

$$\mathrm{T}^d - \alpha^d = \prod_{\zeta \in \mu_d(\mathrm{K})} (\mathrm{T} - \zeta\alpha)$$

est de la forme $\left(\prod_{\zeta\in \mathrm{E}} \zeta\right)\alpha^m$ pour un certain sous-ensemble E de $\mu_d(\mathrm{K})$ de cardinal m et, pour que ce facteur soit à coefficients dans K, il est nécessaire que l'on ait $\alpha^m \in \mathrm{K}$, soit $m = d$. Le groupe de Galois $\mathrm{Gal}(\mathrm{K}(\alpha)/\mathrm{K})$ opère par conséquent transitivement sur les racines de $\mathrm{T}^d - \alpha^d$, ce qui équivaut à dire que son image dans $\mu_n(\mathrm{K})$ est le sous-groupe $\mu_d(\mathrm{K})$.

2. Soit L/K une extension galoisienne finie dont le groupe de Galois est cyclique et d'ordre n. Ayant fixé un générateur σ de G, on pose

$$(\zeta, \alpha) = \sum_{i=0}^{n-1} \zeta^{-i}\sigma^i(\alpha)$$

pour toute racine $\zeta \in \mu_n(\mathrm{K})$.

(i) Il est immédiat que

$$\sigma(\zeta,\alpha) = \sum_{i=0}^{n-1} \sigma(\zeta^{-i}\sigma^i(\alpha)) = \sum_{i=0}^{n-1} \zeta^{-i}\sigma^{i+1}(\alpha) = \zeta\sum_{i=1}^{n} \zeta^{-i}\sigma^i(\alpha),$$

soit $\sigma(\zeta,\alpha) = \zeta(\zeta,\alpha)$ puisque $\zeta^{-n}\sigma^n(\alpha) = \alpha$. On en déduit que $(\zeta,\alpha)^n$ est fixé par σ et donc appartient à K.

(ii) Cette question n'a pas lieu d'être !

(iii) En vertu du lemme de Dedekind, les n éléments $1, \sigma, \ldots, \sigma^{n-1}$ de $\mathrm{Gal}(\mathrm{L}/\mathrm{K})$ sont linéairement indépendants sur L. Par suite, quelle que soit la racine de l'unité $\zeta \in \mu_n(\mathrm{K})$, il existe un élément α de L tel que $(\zeta,\alpha) \neq 0$. Étant donné un élément primitif x de l'extension L/K, il est loisible de choisir α parmi les puissances x^k de x, $0 \leq x \leq n-1$ puisque celles-ci forment une base de L comme K-espace vectoriel.

Considérons finalement une racine primitive $\zeta \in \mu_n(\mathrm{K})$ ainsi qu'un élément α de L tel que $(\zeta,\alpha) \neq 0$. Puisque $\sigma(\zeta,\alpha) = \zeta(\zeta,\alpha)$, le groupe de Galois $\mathrm{Gal}(\mathrm{L}/\mathrm{K})$ opère transitivement sur les racines du polynôme

$$\mathrm{T}^n - (\zeta,\alpha)^n = \prod_{i=0}^{n-1} (\mathrm{T} - \zeta^i(\zeta,\alpha))$$

et ce dernier est donc irréductible. On en déduit que l'élément (ζ,α) de L est de degré $n = [\mathrm{L} : \mathrm{K}]$ sur K, c'est-à-dire $\mathrm{L} = \mathrm{K}((\zeta,\alpha))$.

Nous venons de prouver que, lorsque le groupe $\mu_n(\mathrm{K})$ est d'ordre n, les extensions galoisiennes L/K telles que le groupe $\mathrm{Gal}(\mathrm{L}/\mathrm{K})$ soit cyclique et d'ordre n sont exactement les extensions de la forme $\mathrm{K}(\alpha)/\mathrm{K}$ avec $\alpha^n \in \mathrm{K}^\times$ et $\alpha^d \notin \mathrm{K}$ pour tout diviseur strict d de n.

3. On se limite maintenant à supposer que l'entier n soit premier à la caractéristique du corps K, de sorte que le polynôme $\mathrm{T}^n - 1$ soit séparable, mais non nécessairement scindé, sur K. On considère de nouveau un élément a de $\mathrm{K}^\times$ et un corps de décomposition L du polynôme $\mathrm{T}^n - a$ au-dessus de K.

(i) Soit α une racine de $\mathrm{T}^n - a$ dans L. Le polynôme $\mathrm{T}^n - a$ étant scindé sur L, $\zeta\alpha \in \mathrm{L}$ et donc $\zeta \in \mathrm{L}$ pour toute racine n-ème de l'unité dans une clôture algébrique de L. Le polynôme $\mathrm{T}^n - 1$ est ainsi scindé sur L et ses racines engendrent une sous-extension K_1 de K dans L.

(ii) L'extension L/K_1 est galoisienne car l'extension L/K l'est tandis que l'extension K_1/K est galoisienne car K_1 est le corps de décomposition de $\mathrm{T}^n - 1$. En vertu de l'exercice 2, le groupe $\mathrm{Gal}(\mathrm{K}_1/\mathrm{K})$ est canoniquement isomorphe à un sous-groupe de $(\mathbb{Z}/n\mathbb{Z})^\times$ tandis que le choix d'une racine α de $\mathrm{T}^n - a$ dans L permet de définir un plongement du groupe $\mathrm{Gal}(\mathrm{L}/\mathrm{K}_1)$ dans $\mu_n(\mathrm{K}_1)$.

(iii) On dispose d'une suite exacte de groupes

$$1 \longrightarrow \mathrm{Gal}(\mathrm{L}/\mathrm{K}_1) \longrightarrow \mathrm{Gal}(\mathrm{L}/\mathrm{K}) \longrightarrow \mathrm{Gal}(\mathrm{K}_1/\mathrm{K}) \longrightarrow 1\ .$$

Si l'on fait opérer $\mathrm{Gal}(\mathrm{L}/\mathrm{K})$ sur lui-même par conjuguaison, on obtient un homomorphisme de $\mathrm{Gal}(\mathrm{L}/\mathrm{K})$ dans $\mathrm{Aut}(\mathrm{Gal}(\mathrm{L}/\mathrm{K}_1))$ qui se factorise à travers la projection de $\mathrm{Gal}(\mathrm{L}/\mathrm{K})$ sur $\mathrm{Gal}(\mathrm{K}_1/\mathrm{K})$ en vertu de la commutativité de $\mathrm{Gal}(\mathrm{L}/\mathrm{K}_1)$. Ce dernier groupe étant cyclique d'ordre d égal au degré des facteurs irréductibles de $\mathrm{T}^n - a$ sur K_1, nous obtenons finalement un homomorphisme canonique

$$u : \mathrm{Gal}(\mathrm{K}_1/\mathrm{K}) \to (\mathbb{Z}/d\mathbb{Z})^\times\ .$$

Le choix d'une racine α de $\mathrm{T}^n - a$ dans L permet de construire une *section* s_α de la surjection $\mathrm{Gal}(\mathrm{L}/\mathrm{K}) \to \mathrm{Gal}(\mathrm{K}_1/\mathrm{K})$ en associant à tout élément σ de $\mathrm{Gal}(\mathrm{K}_1/\mathrm{K})$ son unique prolongement à L fixant α ; cette racine α permet par ailleurs d'identifier $\mathrm{Gal}(\mathrm{L}/\mathrm{K}_1)$ à un sous-groupe $\mu_d(\mathrm{K}_1)$. Tout élément de $\mathrm{Gal}(\mathrm{L}/\mathrm{K})$ s'écrit de manière unique sous la forme $\tau s_\alpha(\sigma)$ avec $\tau \in \mathrm{Gal}(\mathrm{L}/\mathrm{K}_1)$ et $\sigma \in \mathrm{Gal}(\mathrm{K}_1/\mathrm{K})$ et, vu ce qui précède,

$$\begin{aligned}(\tau' s_\alpha(\sigma'))(\tau s_\alpha(\sigma)) &= \tau' s_\alpha(\sigma')\tau s_\alpha(\sigma')^{-1} s_\alpha(\sigma') s_\alpha(\sigma) \\ &= \tau' \tau^{u(\sigma)} s_\alpha(\sigma'\sigma).\end{aligned}$$

Le groupe $\mathrm{Gal}(\mathrm{L}/\mathrm{K})$ s'identifie donc à l'ensemble $\mathrm{Gal}(\mathrm{L}/\mathrm{K}_1) \times \mathrm{Gal}(\mathrm{K}_1/\mathrm{K})$ muni du produit « tordu » par l'automorphisme u :

$$(\tau', \sigma') * (\tau, \sigma) = (\tau' \tau^{u(\sigma')}, \sigma'\sigma)\ ;$$

c'est le *produit semi-direct* de $\mathrm{Gal}(\mathrm{K}_1/\mathrm{K})$ par $\mathrm{Gal}(\mathrm{L}/\mathrm{K}_1)$.

Exercice 4 — Une extension de corps L/K est dite *radicale élémentaire* si $\mathrm{L} = \mathrm{K}(\alpha)$ avec $\alpha^n \in \mathrm{K}$ pour un certain entier $n \geq 1$ et elle est dite *radicale* si elle l'aboutissement d'une tour d'extensions radicales élémentaires ; enfin, elle est dite *résoluble par radicaux* si elle est contenue dans une extension radicale de K. Cette dernière condition signifie précisément que tout élément de L peut s'exprimer en termes de radicaux itérés construits à partir d'éléments de K.

Supposons que le corps K soit de caractéristique nulle et fixons-en une clôture algébrique $\overline{\mathrm{K}}$.

(i) Soit $n \geq 1$ un entier et soit K_1 le corps de décomposition du polynôme $\mathrm{T}^n - 1$ dans $\overline{\mathrm{K}}$. Si l'extension composée LK'/K est résoluble par radicaux, l'extension L/K est bien évidemment résoluble par radicaux. Réciproquement, si L/K est une extension résoluble par radicaux et si L'/K est une extension radicale contenant L, l'extension composée $\mathrm{L}'\mathrm{K}'/\mathrm{K}$ est radicale puisqu'elle s'obtient à partir de L' par adjonction de racines de l'unité et, comme $\mathrm{LK}' \subset \mathrm{L}'\mathrm{K}'$, l'extension LK'/K est résoluble par radicaux. En conclusion, une extension L/K est résoluble par radicaux si et seulement si tel est le cas de l'extension composée LK'/K.

(ii) Quelle que soit l'extension galoisienne L/K, l'extension composée LK'/K est galoisienne et $\mathrm{Gal}(\mathrm{L}/\mathrm{K})$ est le quotient de $\mathrm{Gal}(\mathrm{LK}'/\mathrm{K})$ par le sous-groupe abélien et distingué $\mathrm{Gal}(\mathrm{K}'/\mathrm{K})$ tandis que le groupe $\mathrm{Gal}(\mathrm{LK}'/\mathrm{K}')$ s'identifie à un sous-groupe de $\mathrm{Gal}(\mathrm{L}/\mathrm{K})$. Il en découle que le groupe $\mathrm{Gal}(\mathrm{L}/\mathrm{K})$ est résoluble si et seulement si tel est le cas du groupe $\mathrm{Gal}(\mathrm{LK}'/\mathrm{K}')$.

(iii) Considérons finalement une extension galoisienne finie L de K dans $\overline{\mathrm{K}}$.

- Si l'extension L/K est résoluble par radicaux, considérons une extension radicale L' de K dans $\overline{\mathrm{K}}$ contenant L et désignons par K' le corps de décomposition du polynôme $\mathrm{T}^{[\mathrm{L}':\mathrm{K}]} - 1$ dans $\overline{\mathrm{K}}$. Vu ce que l'on a établi au cours de l'exercice 3, toute extension radicale élémentaire de K' est galoisienne de groupe de Galois cyclique et toute extension radicale est galoisienne, de groupe de Galois résoluble ; appliquant cela à l'extension $\mathrm{L}'\mathrm{K}'/\mathrm{K}'$, nous en déduisons que le groupe $\mathrm{Gal}(\mathrm{L}'\mathrm{K}'/\mathrm{K}')$ est résoluble. Ceci prouve que le groupe $\mathrm{Gal}(\mathrm{L}/\mathrm{K})$.
- Si réciproquement le groupe $\mathrm{Gal}(\mathrm{L}/\mathrm{K})$ est résoluble, désignons par K' le corps de décomposition du polynôme $\mathrm{T}^{|\mathrm{Gal}(\mathrm{L}/\mathrm{K})|} - 1$ dans $\overline{\mathrm{K}}$. En s'appuyant de nouveau sur l'exercice 3, la tour d'extensions de K' déduite d'une suite de composition de $\mathrm{Gal}(\mathrm{L}/\mathrm{K})$ à quotients cycliques est une tour d'extensions radicales élémentaires ; l'extension LK'/K' est donc radicale. Il en est alors de même de l'extension LK'/K, ce qui prouve que l'extension L/K est résoluble par radicaux.

Exercice 6 — Soit K un sous-corps de $\mathbb{R}$.

1. [...]

2. Soit L une extension galoisienne finie de K contenue dans $\mathbb{R}$. Étant donnés un élément a de K, un entier $n \geq 1$ et une racine α du polynôme $\mathrm{T}^n - a$ dans $\mathbb{R}$, tout K-automorphisme $\sigma \in \mathrm{Gal}(\mathrm{L}/\mathrm{K})$ envoie α sur une autre racine du

polynôme $T^n - a$ et donc

$$\sigma(\alpha) = \begin{cases} \alpha & \text{si } n \text{ est impair ;} \\ \pm\alpha & \text{si } n \text{ est pair.} \end{cases}$$

Dans tous les cas, $\sigma(\alpha) \in K(\alpha)$ et le sous-groupe H de $\mathrm{Gal}(L/K)$ fixant le corps $L \cap K(\alpha)$ est d'indice 1 ou 2, de sorte que $[L \cap K(\alpha) : K] \in \{1,2\}$.

Supposons que l'extension galoisienne L/K soit résoluble par radicaux *réels*, c'est-à-dire qu'il existe une tour d'extensions radicales élémentaires $K = K_0 \subset K_1 \subset \ldots \subset K_r \subset \mathbb{R}$ telle que $L \subset K_r$. D'après ce que l'on vient de dire, $[L \cap K_{i+1} : L \cap K_i] \in \{1,2\}$ pour tout $i \in \{0,\ldots,r-1\}$ et donc

$$[L : K] = \prod_{i=0}^{r-1} [L \cap K_{i+1} : L \cap K_i]$$

est une puissance de 2. Nous avons ainsi prouvé que, si l'extension galoisienne L/K est résoluble par radicaux réels, alors son degré est une puissance de 2. L'assertion réciproque est vraie : toute extension de degré 2 entre deux sous-corps de $\mathbb{R}$ est élémentairement radicale en vertu de l'exercice 3 et l'extension L/K est donc résoluble par radicaux réels si elle est résoluble par radicaux et si son degré est une puissance de 2.

Exercice 7 — 1. Soient x_1 et x_2 les deux racines du polynôme $T^2 + aT + b$ dans une clôture algébrique de K. Le groupe de Galois G du corps de décomposition L de ce polynôme est un sous-groupe du groupe symétrique $\mathfrak{S}(\{x_1,x_2\})$. Le groupe alterné $\mathfrak{A}(\{x_1,x_2\})$ étant trivial, il découle de l'exercice 1 que G est trivial si le discriminant $D = a^2 - 4b$ est un carré dans K et que $G = \{1,(x_1,x_2)\}$ sinon. Dans ce second cas, l'extension $L/K(\sqrt{D})$ est triviale et les deux racines $x_1,\ x_2$ s'expriment donc en fonction d'une racine carrée du discriminant.

2. Rappelons tout d'abord que tout polynôme cubique $S^3 + aS^2 + bS + c$ peut s'écrire sous la forme $P = T^3 + pT + q$: il suffit de faire le changement de variable $S = T - \frac{a}{3}$. Cette opération a pour vertu de simplifier l'expression du discriminant D du polynôme et de fournir la relation $x_1 + x_2 + x_3 = 0$ entre les trois racines $x_1,\ x_2$ et x_3 de P dans une clôture algébrique de K. On rappelle que $D = -4p^3 - 27q^2$.

Soit $L = K(x_1,x_2,x_3)$ le corps de décomposition du polynôme P et soit G son groupe de Galois, que l'on identifie à un sous-groupe du groupe symétrique $\mathfrak{S}(\{x_1,x_2,x_3\})$. En vertu de l'exercice 1, $G \cap \mathfrak{A}(\{x_1,x_2,x_3\})$ est sous-groupe de G fixant le corps $K(\sqrt{D})$ et, comme $\mathfrak{A}(\{x_1,x_2,x_3\})$ est un groupe cyclique d'ordre 3, les quatre cas de figure possibles sont les suivants :

- $G = \{1\}$;
- $G \simeq \mathbb{Z}/2\mathbb{Z}$ fixe l'une des racines de P et permute les deux autres ;
- $G = \mathfrak{A}(\{x_1,x_2,x_3\})$;
- $G = \mathfrak{S}(\{x_1,x_2,x_3\})$.

Le premier cas se produit si P est scindé sur K, le deuxième si P possède exactement une racine dans K, le troisième si P est irréductible sur K et si D est un carré dans K, le quatrième enfin si P est irréductible sur K et si D n'est pas un carré dans K.

Remarque : il convient d'observer que, dans le deuxième cas de figure, P *est scindé sur le corps* $K(\sqrt{D})$. *Cela peut également se voir en vérifiant que le discriminant du facteur irréductible quadratique de* P *est un carré dans* $K(\sqrt{D})$.

Nous supposons dans ce qui suit que le polynôme P est irréductible sur K ; l'extension $L/K(\sqrt{D})$ est alors cyclique de degré 3 et nous allons appliquer la théorie de Kummer exposée à l'exercice 3. Cela suppose de disposer des racines cubiques de l'unité dans le corps de base ; notant K' un corps de décomposition de $T^3 - 1$, nous allons travailler dans l'extension composée $L' = LK' = K(x_1,x_2,x_3,\rho)$, où ρ est une racine cubique primitive de 1. L'extension $L'/K'(\sqrt{D})$ est non triviale puisque $[L' : K]$ est un multiple de 3 tandis que $[K'(\sqrt{D}) : K]$ est une puissance de 2, donc $\mathrm{Gal}(L'/K'(\sqrt{D}))$ est le groupe cyclique $\mathfrak{A}(\{x_1,x_2,x_3\})$. Soit σ le 3-cycle (x_1,x_2,x_3) et considérons les trois résolvantes de Lagrange

$$(1,x_1) = x_1 + \sigma(x_1) + \sigma^2(x_1) = x_1 + x_2 + x_3 = 0,$$
$$(\rho,x_1) = x_1 + \rho^{-1}\sigma(x_1) + \rho^{-2}\sigma^2(x_1) = x_1 + \rho^2 x_2 + \rho x_3$$

et

$$(\rho^2,x_1) = x_1 + \rho x_2 + \rho^2 x_3.$$

Les trois racines x_1,x_2 et x_3 s'expriment en fonction des résolvantes :

$$x_1 = \frac{1}{3}\big((\rho,x_1) + (\rho^2,x_1)\big),\ \ x_2 = \frac{1}{3}\big(\rho(\rho,x_1) + \rho^2(\rho^2,x_1)\big)\ \text{ et }\ x_3 = \frac{1}{3}\big(\rho^2(\rho,x_1) + \rho(\rho^2,x_1)\big).$$

On a par ailleurs $\sigma(\rho,x_1)=\rho(\rho,x_1)$ et $\sigma(\rho^2,x_1)=\rho^2(\rho^2,x_1)$, donc $(\rho,x_1)^3$, $(\rho^2,x_1)^3\in \mathrm{K}'(\sqrt{\mathrm{D}})$; il reste par conséquent à calculer explicitement ces deux derniers cubes dans $\mathrm{K}'(\sqrt{\mathrm{D}})$ pour obtenir une expression des trois racines de P en termes de radicaux quadratiques et cubiques faisant intervenir les coefficients de P et le trois racines cubiques de l'unité.

On a :

$$\begin{aligned}(\rho,x_1)^3 &= (x_1+\rho^2x_2+\rho x_3)^3\\ &= x_1^3+x_2^3+x_3^3+6x_1x_2x_3+3(x_1^2x_3+x_2^2x_1+x_3^2x_2)\rho+3(x_1x_3^2+x_2x_1^2+x_3x_2^2)\rho^2\\ &= \mathrm{A}+3\mathrm{B}\rho+3C\rho^2\end{aligned}$$

où

$$\begin{aligned}\mathrm{A} &= (x_1+x_2+x_3)^3-3(\mathrm{B}+\mathrm{C})\\ &= -3(\mathrm{B}+\mathrm{C})\\ &= -3(x_1x_2(x_1+x_2)+x_2x_3(x_2+x_3)+x_1x_3(x_1x_3))\\ &= -3(-x_1x_2x_3-x_1x_2x_3-x_1x_2x_3)\\ &= 9x_1x_2x_3\\ &= -9q,\end{aligned}$$

$$\mathrm{B}+\mathrm{C}=3q$$

et

$$\mathrm{B}-\mathrm{C}=(x_1-x_2)(x_2-x_3)(x_1-x_3)$$

est une racine carrée de D que l'on note $\sqrt{\mathrm{D}}$; on en déduit finalement

$$(\rho,x_1)^3=-9q+\frac{3}{2}(3q+\sqrt{D})\rho+\frac{3}{2}(3q-\sqrt{\mathrm{D}})\rho^2=-\frac{27}{2}q+\frac{3}{2}\sqrt{D}\sqrt{-3}$$

où l'on a posé $\sqrt{-3}=\rho-\rho^2$ puisque $(\rho-\rho^2)^2=\rho^2+\rho-2=-3$.

Il suffit de permuter ρ et ρ^2 pour obtenir (ρ^2,x_1) à partir de (ρ,x_1) donc

$$(\rho^2,x_1)=-\frac{27}{2}q-\frac{3}{2}\sqrt{D}\sqrt{-3}.$$

Remarque : on peut observer que $(\rho,x_1)(\rho^2,x_1)$ est invariant par σ et appartient donc à $\mathrm{K}'(\sqrt{\mathrm{D}})$. Un calcul immédiat fournit en fait la relation $(\rho,x_1)(\rho^2,x_1)=-3p$, d'où l'on tire $(\rho,x_1)^3+(\rho^2,x_1)^3=-q$. Cela montre que $(\rho,x_1)^3$ et $(\rho^2,x_1)^3$ sont les deux racines du polynôme $\mathrm{T}^2+q\mathrm{T}-27p^3$.