Problème : Résolubilité par radicaux d'une équation polynomiale (petite introduction à la théorie de Galois)

problème proposé par Romain Krust, Juillet 2007

*Ce problème suppose le lecteur familier avec les notions d'élément algébrique et de polynôme minimal d'un élément algébrique, avec l'algèbre linéaire (on utilise un peu de réduction dans la question **5.6b**), ainsi qu'avec les bases de la théorie des groupes (notions de sous-groupe distingué et groupe quotient en particulier, groupes cycliques). Il peut être intéressant d'avoir préalablement traité les problèmes 7 (au moins la partie I) et 8 (au moins les parties I et II) proposés par Jean-Etienne Rombaldi (à l'adresse http://perso.orange.fr/rombaldi/AgregInterne/EnoncesPbRevisionAgreg.pdf).*

Il s'agit d'une présentation de la théorie de Galois, motivée[1] *par le problème qui a été à la source des découvertes de Galois, le problème de la résolubilité par radicaux des équations polynomiales.*

Les définitions manquantes ou des compléments d'information pourront être trouvés dans [Del] pour la théorie des groupes et [Esc] pour la théorie des corps et la théorie de Galois. Les oeuvres de Galois [Gal] sont accessibles sur le site de la bibliothèque nationale de France. Il est très émouvant — surtout quand on songe au très jeune âge de l'auteur, mort à vingt ans — d'y lire, dans le mémoire "Sur les conditions de résolubilité des équations par radicaux", l'acte de naissance de la théorie des groupes, de la théorie des corps et, bien sûr, de la théorie de Galois. Enfin, pour tout savoir, on peut parcourir le magnifique ouvrage [Cox] de David A. Cox.

Tous les corps invoqués seront des sous-corps de $\mathbb{C}$.

1 Exemples

Dans cette partie, on donne quelques exemples de résolution par radicaux

1. *Dans cette question, on montre qu'un polynôme symétrique en plusieurs variables peut s'exprimer comme polynôme des polynômes symétriques élémentaires. Comme elle est un peu technique (et le problème assez long !), elle pourra éventuellement être admise.*

   Soit K un corps et X_1, $X_2, \ldots,$ X_n des indéterminées. Rappelons qu'on note $K[X_1, X_2, \ldots, X_n]$ la K-algèbre des polynômes en X_1, $X_2, \ldots,$ X_n. On appellera ici degré d'un monôme $X_1^{d_1} X_2^{d_2} \ldots X_n^{d_n}$ le n-uplet $(d_1, d_2, \ldots, d_n)$ et degré d'un polynôme $P \in K[X_1, X_2, \ldots, X_n]$ le degré du monôme de plus haut degré, pour l'ordre lexicographique, intervenant dans l'écriture de P.

[1] Dans les exposés "modernes", c'est-à-dire depuis Artin, on développe d'abord la théorie des corps et la correspondance de Galois. À l'issue de ces développements, le problème de la résolubilité par radicaux, regardé comme simple application, tombe comme un fruit mûr. La méthode, parfaitement justifiée tant sur le plan de la cohérence de l'exposé que du point de vue de l'importance relative des résultats, peut néanmoins sembler un peu aride à qui prend contact avec cette théorie.

On appelle polynômes symétriques élémentaires les polynômes :

$$\begin{aligned}
&\Sigma_1 = X_1 + X_2 + \ldots + X_n \\
&\Sigma_2 = X_1X_2 + X_1X_3 + \ldots + X_{n-1}X_n = \textstyle\sum_{1\leq i<j\leq n} X_iX_j \\
&\Sigma_3 = X_1X_2X_3 + X_1X_2X_4 + \ldots + X_{n-2}X_{n-1}X_n = \textstyle\sum_{1\leq i<j<k\leq n} X_iX_jX_k \\
&\quad \ldots \\
&\Sigma_n = X_1X_2\ldots X_n
\end{aligned}$$

Soit $P \in K[X_1, X_2, \ldots, X_n]$ un polynôme non nul et symétrique, c'est-à-dire vérifiant : $\forall \sigma \in \mathcal{S}_n,\ P(X_{\sigma(1)}, X_{\sigma(2)}, \ldots, X_{\sigma(n)}) = P(X_1, X_2, \ldots, X_n)$

On souhaite prouver l'existence d'un polynôme Q en n variables à coefficients dans K tel que

$$P(X_1, X_2, \ldots, X_n) = Q(\Sigma_1, \Sigma_2, \ldots, \Sigma_n)$$

Soit $(d_1, d_2, \ldots, d_n)$ le degré de P.

(a) Montrer $d_1 \geq d_2 \geq \ldots \geq d_n$.

(b) Montrer $\deg(\Sigma_1^{d_1-d_2}\Sigma_2^{d_2-d_3}\ldots\Sigma_n^{d_n}) = (d_1, d_2, \ldots, d_n)$.

(c) L'ensemble $\{(e_1, e_2, \ldots, e_n) \in \mathbb{N}^n;\ (e_1, e_2, \ldots, e_n) \leq \deg(P)\}$ est-il fini ? Montrer que l'ensemble $\{(e_1, e_2, \ldots, e_n) \in \mathbb{N}^n;\ (e_1, e_2, \ldots, e_n) \leq \deg(P)$ et $\exists Q \in K[X_1, X_2, \ldots, X_n], Q$ symétrique, $\deg(Q) = (e_1, e_2, \ldots, e_n)\}$ est fini.

(d) Conclure.

Noter que cette démonstration fournit un algorithme permettant de trouver un tel polynôme Q.

(e) Exprimer le polynôme $X_1^3(X_2+X_3)+X_2^3(X_3+X_1)+X_3^3(X_1+X_2) \in K[X_1, X_2, X_3]$ en fonction des Σ_i.

On pourra, pour tout monôme $X_1^{e_1}X_2^{e_2}X_3^{e_3}$, convenir de noter $\sum X_1^{e_1}X_2^{e_2}X_3^{e_3}$ le polynôme symétrique obtenu en permutant les X_i et en sommant les monômes obtenus, mais sans répéter deux monômes égaux. Par exemple $\sum X_1^2X_2 = X_1^2X_2 + X_1^2X_3 + X_2^2X_1 + X_2^2X_3 + X_3^2X_1 + X_3^2X_2$ mais $\sum X_1X_2 = X_1X_2 + X_2X_3 + X_3X_1 = \Sigma_2$.

2. *Dans cette question, on montre comment résoudre l'équation de degré 3.*
Soient K un sous-corps de $\mathbb{C}$, $p, q \in K$ et $P = X^3 + pX + q$ et a, b, c ses racines complexes.

On pose $u = (a + j^2b + jc)^3$. Montrer qu'en permutant les racines a, b, c dans l'expression de u, on n'obtient que deux valeurs, u et u', puis que u et u' sont racines d'une équation du second degré à coefficients dans K. En déduire une méthode de résolution par radicaux de l'équation $P(x) = 0$ (on se contentera d'expliquer pourquoi la résolution est possible, sans nécessairement mener les calculs à leur terme).

3. *Dans cette question, on montre comment résoudre l'équation de degré 4.*
Soient K un sous-corps de $\mathbb{C}$, $p, q \in K$ et $P = X^4 + pX^2 + qX + r$ et x_1, x_2, x_3, x_4 ses racines complexes.

On pose $u = x_1x_2 + x_3x_4$. Montrer qu'en permutant les racines x_1, x_2, x_3, x_4 dans l'expression de u, on n'obtient que trois valeurs u, v et w, puis que u, v et w sont les trois racines d'une équation de degré trois à coefficients dans K. En déduire une méthode de résolution par radicaux de l'équation $P(x) = 0$ (on se contentera d'expliquer pourquoi la résolution est possible, sans nécessairement mener les calculs à leur terme).

4. On considère le polynôme $X^6 + X^5 + X^4 + X^3 + X^2 + X + 1 \in \mathbb{Q}[X]$, dont les racines sont les ξ^k, où $k \in [\![1, 6]\!]$ et $\xi = e^{\frac{2i\pi}{7}}$.

   On pose $u = \xi + \xi^2 + \xi^4$ et $v = \xi^3 + \xi^5 + \xi^6$. Vérifier que u et v sont les deux racines d'une équation de degré deux à coefficients dans $\mathbb{Q}$. En déduire une équation de degré 3 à coefficient dans $\mathbb{Q}(u)$ dont ξ est racine et prouver qu'il existe une expression de ξ ne faisant appel, outre les rationnels et les opérations élémentaires, qu'aux symboles $\sqrt{}$ et $\sqrt[3]{}$ (et sans se soucier des problèmes d'ambiguïté).

Les méthodes de résolution des équations de degré 3 et 4 présentées ci-dessus font intervenir des quantités auxiliaires (parfois appelées résolvantes) invariantes par certaines permutations des racines et, de ce fait, racines d'une équation de degré inférieur. La possibilité d'une expression algébrique telle que $x_1x_2 + x_3x_4$ par exemple est liée à l'existence d'un morphisme de groupe non trivial de S_4 dans S_3 (à chaque permutation des x_i est associée une permutation de u, v, w). Le fait que S_5 ne contienne qu'un seul sous-groupe distingué non trivial, le groupe alterné A_5 qui est simple[2]*, permet d'entrevoir que ce type de méthode ne s'étendra pas à l'équation générale de degré 5. Néanmoins :*
- L'argument est trop faible pour prouver la non-existence de formules de résolution par radicaux.
- Il concerne l'équation "générale" [3]*, c'est-à-dire une équation pour laquelle les racines jouent des rôles parfaitement symétriques et sont indiscernables du point de vue du corps K (dans le sens où, lorsqu'une relation algébrique $F(x_1, x_2, \ldots, x_n) = 0$, $F \in K[X_1, X_2, \ldots, X_n]$, a lieu, elle a lieu aussi en permutant les x_i). Mais pour une équation particulière, il peut se produire une rupture de symétrie qui change la donne. Pour mieux percevoir cette idée, considérons quelques exemples.*

1. *Pour ce qui est des racines du polynômes $(X^2 - 2)(X^2 - 3) \in \mathbb{Q}[X]$, $\pm\sqrt{2}$ et $\pm\sqrt{3}$ sont parfaitement discernables du point de vue de $K = \mathbb{Q}$ (la symétrie est rompue) puisque les premières annulent le polynôme $X^2 - 2 \in \mathbb{Q}[X]$ tandis que les secondes annulent $X^2 - 3$ (alors que $\sqrt{2}$ et $-\sqrt{2}$ par exemple restent "indiscernables").*

2. *Si le polynôme P est scindé sur K, la symétrie entre racines est totalement rompue. Noter que lorsqu'on veut résoudre une équation par radicaux, on cherche justement,*

[2] Un groupe est dit simple quand il n'admet aucun sous groupe distingué non trivial.

[3] Pour formaliser convenablement cette notion, on peut travailler dans le corps $K(X_1, \ldots, X_n)$ et considérer le polynôme $P(X) = X^n - \Sigma_1 X^{n-1} + \ldots + (-1)^n \Sigma_n$, où les Σ_k sont les polynômes symétriques élémentaires et dont les racines sont les X_i, vu comme polynôme à coefficients dans le corps $K(\Sigma_1, \Sigma_2, \ldots, \Sigma_n)$ (qu'il ne s'agisse pas ici de sous-corps de $\mathbb{C}$ n'est pas un vrai problème, cette restriction pouvant en caractéristique nulle être levée sans grande difficulté).

en augmentant le corps de base en lui adjoignant des radicaux, à rendre P scindé, donc à rompre totalement la symétrie entre racines.

3. *Dans le cas du polynôme $X^6 + X^5 + X^4 + X^3 + X^2 + X + 1 \in \mathbb{Q}[X]$, la symétrie est "fortement" rompue dans la mesure où, dès que l'on choisit une racine, les autres arrivent en tant que puissance de celle-ci.*

   Comme on l'a vu, en posant $a = \xi + \xi^2 + \xi^4$ et $b = \xi^3 + \xi^5 + \xi^6$, a et b sont racines d'une équation de degré 2 à coefficients dans $\mathbb{C}$. L'expression formelle $x_1 + x_2 + x_4$ prend pourtant 20 valeurs différentes lorsque l'on substitue à x_1, x_2, x_4 leurs images par toutes les permutations des 6 variables $x_1, \ldots, x_6$ et rien ne prédisposait deux de ces valeurs à être les deux racines d'une équation du second degré à coefficients dans $\mathbb{Q}$ sauf, bien sûr, le fait qu'existent de nombreuses relations entre les racines[4], c'est-à-dire la très faible symétrie[5] de l'ensemble des racines.

Cette symétrie entre racines est "mesurée" par le groupe de Galois de l'équation. L'idée (confuse pour le moment) est donc que plus le groupe de symétrie est "grand", moins il y a de relations entre les racines et plus l'équation est "difficile" à résoudre. Le groupe de Galois sera défini précisément dans la partie 5. Pour l'exploiter au mieux, il convient de commencer par étudier les bases de la théorie des corps.

2 Premières propriétés

1. Soient L un corps et K un sous-corps de L (on dit aussi que L est une extension de K). Montrer que L est naturellement muni d'une structure de K espace vectoriel. On dira que l'extension est de degré fini lorsque L est dimension finie en tant que K-espace vectoriel. La dimension de L sur K est appelée degré de l'extension et notée $[L : K]$.

2. Soient $K \subset L$ et $L \subset M$ deux extensions de degré fini. Montrer que $K \subset M$ est de degré fini et que
$$[M : K] = [M : L][L : K]$$

3. Soit K un sous-corps de $\mathbb{C}$ est $a \in \mathbb{C}$. On suppose a algébrique sur K et on note $K(a)$ le sous-corps de $\mathbb{C}$ engendré par $\{a\} \cup K$ ainsi que $\pi_{a,K}$ le polynôme minimal de a sur K (rappelons que c'est un polynôme irréductible). Montrer que $K(a) = K[a]$, que $[K(a) : K] = \deg \pi_{a,K}$.

4. (a) Soient K un corps et A une K-algèbre unitaire de dimension finie sans diviseurs de zéros. Montrer que tout élément de A est inversible (en particulier, si A est unitaire, intègre[6], de dimension finie, alors A est un corps). On pourra considérer

[4] On peut "mesurer" l'ensemble des relations existant entre n complexes $x_1, x_2, \ldots, x_n$ à l'aide de l'idéal $I = \{F \in K[X_1, X_2, \ldots, X_n];\ F(x_1, x_2, \ldots, x_n) = 0\}$.

[5] La forte symétrie géométrique, qui traduit le grand nombre de relations existantes entre les racines, ne s'oppose pas, au contraire, à une faible symétrie du point de vue galoisien. Ces deux symétries sont en quelque sorte duales l'une de l'autre.

[6] Intègre = commutative et sans diviseur de zéro.

un élément $a \in A$ non nul et les applications

$$\begin{array}{ccc} A & \to & A \\ x & \mapsto & ax \end{array} \quad \text{et} \quad \begin{array}{ccc} A & \to & A \\ x & \mapsto & xa \end{array}$$

(b) Soient L et M deux extensions de degrés finis d'un sous-corps K de $\mathbb{C}$. Montrer que le sous-corps de $\mathbb{C}$ engendré par $L \cup M$, qu'on note LM, est l'ensemble des éléments de la forme $\sum_{i=1}^{p} x_i y_i$, où $p \in \mathbb{N}$, $x_i \in L$, $y_i \in M$.

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

Pour toute extension de degré fini $K \subset L$ de sous-corps de $\mathbb{C}$, on note $\mathrm{Mor}_K(L, \mathbb{C})$ l'ensemble des K-morphismes de L dans $\mathbb{C}$, c'est-à-dire des morphismes de corps $\sigma : L \to \mathbb{C}$ vérifiant :

$$\forall x \in K,\ \sigma(x) = x$$

(on rappelle qu'un morphisme de corps est toujours injectif).
Pour un tel morphisme σ et pour $P \in L[X]$, on note $P^\sigma \in \mathbb{C}[X]$ le polynôme dont les coefficients sont les images par σ des coefficients de P :

$$\text{Si } P = \sum_{k=0}^{s} a_k X^k \text{ alors } P^\sigma = \sum_{k=0}^{s} \sigma(a_k) X^k$$

On va prouver dans cette partie : $|\mathrm{Mor}_K(L, \mathbb{C})| = [L : K]$

1. Soient K un sous-corps de $\mathbb{C}$ et $P \in K[X]$ un polynôme irréductible. Montrer que les racines de P dans $\mathbb{C}$ sont simples (on dit que P est séparable).

2. Soient $K \subset L$ une extension finie et $\sigma \in \mathrm{Mor}_K(L, \mathbb{C})$. Montrer que, pour tout $x \in L$, $\sigma(x)$ est un K-conjugué de x.

3. Soient K un sous-corps de $\mathbb{C}$, $a \in \mathbb{C} \setminus K$ un élément algébrique sur K, et $L = K(a)$. Soient $a = a_1, a_2, \ldots, a_p$ les racines de $\pi_{a,K}$ dans $\mathbb{C}$ (les a_i sont appelés les conjugués de a).

   (a) Soit $\sigma \in \mathrm{Mor}_K(L, \mathbb{C})$. Montrer $\sigma(a) \in \{a_1, a_2, \ldots, a_p\}$.

   (b) Soit $k \in [\![1, p]\!]$. Prouver l'existence d'un unique $\sigma \in \mathrm{Mor}_K(L, \mathbb{C})$ tel que $\sigma(a) = a_k$.

   (c) Soit $\eta : K \to \mathbb{C}$ un morphisme de corps. Montrer, par un procédé similaire à celui qui vient d'être mis en oeuvre, que η peut se prolonger d'exactement p manières différentes à un morphisme de $K(a)$ dans $\mathbb{C}$.

4. Soit $K \subset L$ une extension de degré fini. Prouver $|\mathrm{Mor}_K(L, \mathbb{C})| = [L : K]$.

5. Montrer que pour toute extension finie $K \subset L$ et pour tout $a \in L$ et pour tout K-conjugué $b \in \mathbb{C}$ de a, il existe $\sigma \in \mathrm{Mor}_K(L, \mathbb{C})$ tel que $\sigma(a) = b$.

   Plus généralement, montrer que si $K \subset L \subset M$ sont des sous-corps de $\mathbb{C}$, chaque extension étant de degré fini, tout élément de $\mathrm{Mor}_K(L, \mathbb{C})$ se prolonge en un élément de $\mathrm{Mor}_K(M, \mathbb{C})$.

6. Soient $K \subset L \subset M$ des sous-corps de $\mathbb{C}$, chaque extension étant de degré fini. Prouver

$$|\operatorname{Mor}_K(M,\mathbb{C})| = |\operatorname{Mor}_L(M,\mathbb{C})||\operatorname{Mor}_K(L,\mathbb{C})|$$

7. Montrer que les éléments de $\operatorname{Mor}_K(L,\mathbb{C})$, en tant qu'éléments du K-espace vectoriel des applications de L dans $\mathbb{C}$, forment une famille libre (lemme de Dedekind).

4 Théorème de l'élément primitif

Soit $K \subset L$ une extension de sous-corps de $\mathbb{C}$. Un élément $\xi \in L$ est dit primitif si $L = K(\xi)$. Le théorème de l'élément primitif affirme, lorsque l'extension est de degré fini, l'existence d'un élément primitif.

1. On commence par établir un lemme d'algèbre linéaire. Soit E un espace vectoriel sur K : prouver que E ne peut pas s'écrire comme réunion d'un nombre fini de ses sous-espaces stricts. On pourra s'inspirer de l'idée suivante : Si E est réunion de p de sous-espaces vectoriels stricts F_i et que l'on considère une droite <u>affine</u> D de E non contenue dans l'un des F_i, alors $D \cap F_i$ est de cardinal au plus un, donc D est de cardinal au plus p.

2. Soit $\xi \in L$. Montrer que ξ est primitif si et seulement si le seul K-morphisme σ de L dans $\mathbb{C}$ vérifiant $\sigma(\xi) = \xi$ est l'injection canonique de L dans $\mathbb{C}$.

3. Conclure.

5 Groupe de Galois d'un polynôme

Dans cette partie, on définira le groupe de Galois d'un polynôme, le groupe de Galois d'une extension finie, et on établira un certain nombre de faits utiles dans la suite.

Soient K un sous-corps de $\mathbb{C}$ et $P \in K[X]$. On note $a, b, \ldots, z$ les racines complexes de P, que l'on suppose simples, et $L = K(a, b, \ldots, z)$ (L s'appelle le corps de décomposition de P relativement à K).
Soit $\sigma \in \mathcal{S}(a, b, \ldots, z)$ une permutation des racines de P. On dira que σ est galoisienne si elle vérifie l'une des propriétés équivalentes suivantes ($A, B, \ldots, Z$ sont des indéterminées):
(i) Pour toute $F \in K(A, B, \ldots, Z)$,

$$F(a, b, \ldots, z) = 0 \implies F(\sigma(a), \sigma(b), \ldots, \sigma(z)) = 0$$

(ii) Pour tout couple $F, G \in K(A, B, \ldots, Z)$,

$$F(a, b, \ldots, z) = G(a, b, \ldots, z) \implies F(\sigma(a), \sigma(b), \ldots, \sigma(z)) = G(\sigma(a), \sigma(b), \ldots, \sigma(z))$$

(iii) Pour toute $F \in K(A, B, \ldots, Z)$,

$$F(a, b, \ldots, z) \in K \implies F(\sigma(a), \sigma(b), \ldots, \sigma(z)) = F(a, b, \ldots, z)$$

On note $\operatorname{Gal}_K(P)$ l'ensemble des permutations galoisiennes.

1. Établir l'équivalence de ces trois énoncés et vérifier que $\mathrm{Gal}_K(P)$ forme un sous-groupe de $\mathcal{S}(\{a, b, \ldots, z\})$ (attention : sans être difficile, cette question mérite d'être soigneusement rédigée).

2. Montrer que si $\sigma \in \mathcal{S}(\{a, b, \ldots, z\})$ est une permutation galoisienne, alors σ se prolonge de manière unique en un K-automorphisme du corps L. Montrer réciproquement que tout K-automorphisme de L induit une permutation galoisienne des racines de P.

On note $\mathrm{Gal}_K(L)$ le groupe des K-automorphismes de L. C'est donc, d'après ce qui précède, un groupe canoniquement isomorphe à $\mathrm{Gal}_K(P)$. On les identifie et, si $\sigma \in \mathrm{Gal}_K(P)$, on notera encore σ son image dans $\mathrm{Gal}_K(L)$.
Dans la suite de cette partie, on pose $n = [L : K]$ et on note ξ un élément primitif de L.

3. Montrer que tout élément de $\mathrm{Mor}_K(L, \mathbb{C})$ est à valeurs dans L. En déduire

$$|\mathrm{Gal}_K(P)| = n$$

Pour toute extension de degré fini $K \subset M$ de sous-corps de $\mathbb{C}$, on note encore $\mathrm{Gal}_K(M)$ le groupe des K-automorphismes de M et on dit que l'extension est galoisienne si $|\mathrm{Gal}_K(M)| = [M : K]$. Cela signifie[7] *que tous les éléments de $\mathrm{Mor}_K(M, \mathbb{C})$ sont à valeurs dans M, ou encore (puisque les valeurs prises par les $\sigma(x)$, quand x est fixé dans L et σ parcourt $\mathrm{Mor}_K(L, \mathbb{C})$, sont les K-conjugués de x) que tous les K-conjugués des éléments de M sont dans M. On vient de voir que le corps de décomposition d'un polynôme $P \in K[X]$ est une extension galoisienne de K. La réciproque est vraie, car si $K \subset M$ est galoisienne et si ξ est un élément primitif de M, alors toutes les racines de $\pi_{\xi,K}$ sont dans M et M est le corps de décomposition de $\pi_{\xi,K}$. Noter que si $K \subset M$ est une extension galoisienne, alors pour tout corps L vérifiant $K \subset L \subset M$, l'extension $L \subset M$ est galoisienne.*

4. Soit $x \in L$ vérifiant : $\forall\, \sigma \in \mathrm{Gal}_K(P),\ \sigma(x) = x$.

   Montrer qu'il existe $Q \in K_{n-1}[X]$ tel que $x = Q(\xi)$. En considérant les $Q(\xi')$, où ξ' parcourt l'ensemble des conjugués de ξ, montrer que $\deg(Q) = 0$. En déduire

$$K = \{x \in L;\ \forall\, \sigma \in \mathrm{Gal}_K(P),\ \sigma(x) = x\}$$

   À quelle condition sur P a-t-on $\mathrm{Gal}_K(P) = \{\mathrm{id}\}$?

L'égalité $K = \{x \in L;\ \forall\, \sigma \in \mathrm{Gal}_K(P),\ \sigma(x) = x\}$ est fondamentale. Elle atteste que, pour montrer qu'un élément de L de la forme $Q(a, b, \ldots, z)$ appartient à K, il n'est pas nécessaire que Q soit symétrique. Il suffit que Q soit invariant par les permutations de $\mathrm{Gal}_K(P)$. Cela explique le succès de la méthode employée en ***I.4.****.*

5. On suppose maintenant $\mathbb{U}_n \subset K$ et $P = X^n - \alpha$ (où $\alpha \in K$). Montrer qu'il existe une injection de $\mathrm{Gal}_K(P)$ dans $\frac{\mathbb{Z}}{n\mathbb{Z}}$. En déduire que $\mathrm{Gal}_K(P)$ est cyclique.

[7] Ceci ne serait pas correct si on omettait l'hypothèse que M est un sous-corps de $\mathbb{C}$ (il faudrait prendre en compte d'éventuels problèmes de séparabilité).

6. Réciproquement, soit $K \subset L$ une extension galoisienne (de sous-corps de $\mathbb{C}$) telle que $\mathrm{Gal}_K(L)$ soit cyclique d'ordre $n \geq 2$ et $\mathbb{U}_n \subset K$. Soit σ un générateur de $\mathrm{Gal}_K(L)$ et $\theta \in L$. Posons (on note $\xi = e^{\frac{2i\pi}{n}}$)

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

   (a) Montrer que l'on peut choisir θ de telle sorte que $a \neq 0$ (on pourra utiliser le lemme de Dedekind).

   (b) Vérifier $\sigma(a) = \xi a$. En déduire que la famille $(1, a, \ldots, a^{n-1})$ est K-libre et que $a^n \in K$.

   (c) Conclure à l'existence de $\alpha \in K$ tel que L soit le corps de décomposition sur K de $X^n - \alpha$.

7. Soit K un sous-corps de $\mathbb{C}$ et ξ une racine $n^{\text{ième}}$ primitive de l'unité. Montrer que $\mathrm{Gal}_K(K(\xi))$ est un groupe abélien.

8. Soient $K \subset L \subset M$ des sous-corps de $\mathbb{C}$. On suppose l'extension $K \subset M$ galoisienne.

   (a) Montrer que l'extension $L \subset M$ est galoisienne et que $\mathrm{Gal}_L(M)$ est un sous-groupe de $\mathrm{Gal}_K(M)$.

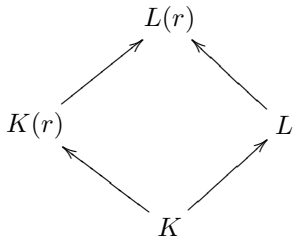
   (b) Pour tout $\sigma \in \mathrm{Gal}_K(M)$, $\sigma(L)$ est clairement un sous-corps de M. Prouver $\mathrm{Gal}_{\sigma(L)}(M) = \sigma \,\mathrm{Gal}_L(M) \sigma^{-1}$.

   (c) Montrer que sont équivalents les énoncés
   (i) L'extension $K \subset L$ est galoisienne
   (ii) $\forall \sigma \in \mathrm{Gal}_K(M),\ \sigma(L) \subset L$
   (iii) $\mathrm{Gal}_L(M) \lhd \mathrm{Gal}_K(M)$
   et que, lorsqu'ils sont vrais, $\mathrm{Gal}_K(L) \simeq \frac{\mathrm{Gal}_K(M)}{\mathrm{Gal}_L(M)}$.

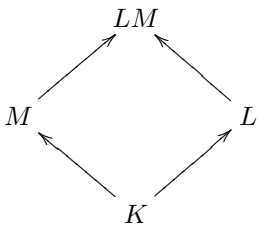
6 Augmentation du corps de base

Soit $P \in K[X]$. Dans la terminologie de Galois, "adjoindre une quantité r à l'équation" consiste à regarder P comme polynôme à coefficients dans $K(r)$.
Résoudre l'équation $P(x) = 0$ par radicaux consiste à trouver une succession 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 $K(r_1, r_2, \ldots, r_q)$.
Les groupes de Galois successifs $\mathrm{Gal}_K(P)$, $\mathrm{Gal}_{K(r_1)}(P), \ldots, \mathrm{Gal}_{K(r_1, r_2, \ldots, r_q)}(P)$ sont clairement décroissants et le fait que P soit scindé sur $K(r_1, r_2, \ldots, r_q)$ équivaut à $\mathrm{Gal}_{K(r_1, r_2, \ldots, r_q)}(P) = \{\mathrm{id}\}$. On cherche donc à adjoindre des radicaux successifs de manière à réduire le groupe de Galois au neutre.
Pour savoir si une telle réduction existe, il convient d'observer comment est réduit le groupe de Galois de P lorsqu'on adjoint un radical r à l'équation. Quatre corps entrent dans la danse : le corps de base K, le corps de décomposition $L = K(a, b, \ldots, z)$ de P sur K, $K(r)$,

et le corps de décomposition de P sur $K(r)$, à savoir $L(r) = K(r, a, b, \ldots, z)$, ce qui conduit au schéma :



Il est donc naturel d'étudier la situation plus générale :



où $K \subset L$ est une extension galoisienne (qu'on cherche à étudier), $K \subset M$ est une extension de degré fini (l'outil pour "réduire" l'extension $K \subset L$) et LM désigne, comme convenu, le plus petit corps de $\mathbb{C}$ contenant $L \cup M$. On adopte ces notations dans cette situation dans cette partie.

1. Montrer que l'extension $M \subset LM$ est galoisienne.

2. Montrer qu'il existe une injection naturelle de $\mathrm{Gal}_M(LM)$ dans $\mathrm{Gal}_K(L)$. Prouver que l'image de cette injection est $\mathrm{Gal}_{L\cap M}(L)$ (on pourra, pour prouver que l'image contient $\mathrm{Gal}_{L\cap M}(L)$, considérer un élément primitif de l'extension $L \cap M \subset M$).

Le résultat qu'on d'établir est connu sous le nom de théorème des irrationnalités naturelles. Cette appellation vient de l'idée suivante. En augmentant le corps de base K (de K à M), c'est-à-dire en lui adjoignant des "irrationnalités", on réduit le groupe de Galois de $\mathrm{Gal}_K(L)$ à $\mathrm{Gal}_M(LM)$. Le résultat précédent montre qu'on peut obtenir la même réduction en n'adjoignant que des quantité appartenant à L (des irrationnalités "naturelles") : il suffit d'augmenter K à $L \cap M$. Les irrationnalités non "naturelles" sont dites "accessoires". Notons cependant qu'une irrationnalité accessoire et radicale ne peut pas nécessairement être remplacée par une irrationnalité naturelle et elle-même radicale.

3. On suppose maintenant que l'extension $K \subset M$ est galoisienne.

   (a) Montrer que $K \subset L \cap M$ est galoisienne. En déduire $\mathrm{Gal}_{L\cap M} L \lhd \mathrm{Gal}_K(L)$ et

$$\frac{\mathrm{Gal}_K(L)}{\mathrm{Gal}_{L\cap M} L} \simeq \mathrm{Gal}_K(L \cap M)$$

(b) Montrer qu'en identifiant $\mathrm{Gal}_M(LM)$ avec $\mathrm{Gal}_{L\cap M}\, L$ et $\mathrm{Gal}_L(LM)$ avec $\mathrm{Gal}_{L\cap M}\, M$, on a l'isomorphisme[8]

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

7 Le groupe d'une équation résoluble par radicaux est résoluble

1. Soit $P \in K[X]$. Soit ξ une racine primitive de l'unité. Prouver $\mathrm{Gal}_{K(\xi)}(P) \lhd \mathrm{Gal}_K(P)$ et montrer que $\frac{\mathrm{Gal}_K(P)}{\mathrm{Gal}_{K(\xi)}(P)}$ est abélien.

2. Soit $P \in K[X]$. Soit $r \in \mathbb{C}$ tel que $r^q \in K$. On suppose $\mathbb{U}_q \subset K$. Prouver $\mathrm{Gal}_{K(r)}(P) \lhd \mathrm{Gal}_K(P)$ et montrer que $\frac{\mathrm{Gal}_K(P)}{\mathrm{Gal}_{K(r)}(P)}$ est cyclique.

3. Soit $P \in K[X]$. On suppose P résoluble par radicaux (dans le sens indiqué plus haut). Montrer qu'il existe une suite

$$\{e\} = G_0 \subset G_1 \subset \ldots \subset G_{m-1} \subset G_m = \mathrm{Gal}_K(P)$$

de sous-groupes de $\mathrm{Gal}_K(P)$ vérifiant, pour tout $i \in [\![1, m]\!]$: $G_{i-1} \lhd G_i$ et $\frac{G_i}{G_{i-1}}$ abélien. On dit d'un groupe (ici $\mathrm{Gal}_K(P)$) possédant cette propriété que c'est un groupe résoluble.

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

1. Soit G un groupe fini et H un sous-groupe distingué strict de G. On suppose $\frac{G}{H}$ abélien. Montrer qu'il existe un sous-groupe H' tel que $H \subset H' \subset G$, $H' \lhd G$ et $\frac{G}{H'}$ cyclique (on pourra considérer un sous-groupe strict maximal de $\frac{G}{H}$).

2. Montrer qu'un sous-groupe d'un groupe résoluble est résoluble.

Dans la prochaine question, on admet le fait suivant, qui sera prouvé ultérieurement : soit $K \subset L$ une extension galoisienne et H un sous-groupe de $\mathrm{Gal}_K(P)$. *On note*

$$L^H = \{x \in L;\ \forall\, \sigma \in H,\ \sigma(x) = x\}$$

Alors L^H est un sous-corps de L contenant K et l'on a $\mathrm{Gal}_{L^H}(L) = H$.

3. Soit $P \in K[X]$. On montre ici, par récurrence sur $|\mathrm{Gal}_K(P)|$, que si $\mathrm{Gal}_K(P)$ est résoluble alors P est résoluble par radicaux.

   (a) Vérifier que tel est bien le cas si $|\mathrm{Gal}_K(P)| = 1$.

[8] Ce petit lemme, qui à ma connaissance n'apparaît pas dans la littérature — même s'il est une conséquence immédiate des théorèmes usuels, correspondance de Galois et théorème des irrationnalités naturelles —, est directement inspiré de la lecture de [Gal].

Dans la suite de cette question, on suppose $|\operatorname{Gal}_K(P)| > 1$, et on fait l'hypothèse que tout polynôme dont le groupe de Galois est de cardinal strictement inférieur à $|\operatorname{Gal}_K(P)| = 1$ est résoluble par radicaux (et ceci quelque soit le corps de base).

(b) Soit $H \subsetneqq \operatorname{Gal}_K(P)$, $H \lhd \operatorname{Gal}_K(P)$ tel que $\frac{\operatorname{Gal}_K(P)}{H}$ soit cyclique. Soit q l'ordre de $\frac{\operatorname{Gal}_K(P)}{H}$ et $\xi = e^{\frac{2i\pi}{q}}$.

Montrer que si $\operatorname{Gal}_{K(\xi)}(P) \subsetneq \operatorname{Gal}_K(P)$, alors P est résoluble par radicaux.

Montrer que si $\mathbb{U}_q \subset K$, alors $\operatorname{Gal}_K(L^H)$ est cyclique d'ordre q. En déduire qu'il existe $r \in L$ tel que $r^q \in K$ et $\operatorname{Gal}_{K(r)}(P) = H$, puis que P est résoluble par radicaux. Conclure.

9 Un exemple d'équation non résoluble par radicaux

À compléter.

10 Points constructibles à la règle et au compas

À compléter.

11 La correspondance de Galois

À compléter.

References

[Cox] David A. Cox, *Galois Theory*, Wiley

[Del] Jean Delcourt, *Théorie des groupes*, Dunod

[Esc] Jean-Pierre Escofier *Théorie de Galois*, Dunod

[Gal] Evariste Galois *Oeuvres mathématiques*, Gabay (téléchargeables sur http://gallica.bnf.fr/)