Résolution par radicaux

Daniel PERRIN

Ce texte reprend le thème d'un TER (Travail d'Étude et de Recherche de master) posé à Orsay en 2006. Je me suis appuyé sur la rédaction de Gwendoline Deveaux, que je remercie ici.

Dans ce TER, on utilise un peu de théorie de Galois. Les rudiments en sont rappelés dans l'annexe 1.

Table des matières

1 Introduction historique

Sur ce thème, on pourra consulter [1] et [2].

Jusqu’au XIX-ième siècle, la résolution des équations algébriques, c’est-à-dire des équations polynomiales $a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 = 0$, est pratiquement synonyme d’algèbre. Sans doute la résolution des équations de degré 1 est-elle connue depuis la nuit des temps, même s’il faut attendre les mathématiciens arabes pour la formuler en termes d’équations et de manipulations (le mot *al-jabr* désigne d’ailleurs le passage d’un membre à l’autre d’une équation). Les Babyloniens savent, sur des exemples, résoudre des équations du second degré et des équations bicarrées. C’est aussi le cas des Grecs, avec des méthodes géométriques, et des Arabes. Ces derniers détiennent en substance la formule avec la racine carrée du discriminant. Le plus important progrès ensuite a lieu au début du XVI-ième siècle avec la résolution, par les algébristes italiens (Scipion del Ferro, Tartaglia, Cardan) de l'équation du troisième degré par les formules dites maintenant de Cardan, par exemple pour l'équation $x^3 + ax = b$:

$$x = \sqrt[3]{\frac{b}{2} + \sqrt{\left(\frac{b}{2}\right)^2 + \left(\frac{a}{3}\right)^3}} + \sqrt[3]{\frac{b}{2} - \sqrt{\left(\frac{b}{2}\right)^2 + \left(\frac{a}{3}\right)^3}}.$$

Cette expression, qui fait intervenir des racines carrées et cubiques est l'objectif de ce qu'on appelle une **résolution par radicaux** de l'équation proposée, sujet qui constitue l'objet essentiel de ce texte.

Dans la foulée de ces travaux, Ferrari, un élève de Cardan parvient à résoudre en 1545 les équations de degré 4 en les ramenant à des équations de degrés 2 et 3. C'est aussi en étudiant le cas "irréductible" de l'équation de degré 3 que Bombelli invente les imaginaires. Dès lors, les mathématiciens (notamment Leibniz) tentent de passer aux degrés plus grands, sans succès. Deux autres thèmes sont à signaler : le lien entre coefficients et racines, reconnu par Viète et le fait qu'un polynôme de degré n admette n racines (éventuellement multiples, éventuellement imaginaires) annoncé par Girard, démontré par D'alembert (avec une preuve incomplète) et définitivement établi par Gauss.

En 1770, deux mémoires, l'un de Lagrange et l'autre de Van der Monde reprennent le cas des équations de degré ≤ 4, en expliquant [1] le succès des méthodes des italiens et cette analyse conduit à penser que les mêmes méthodes ne peuvent fonctionner en degré plus grand. C'est Abel qui montre en 1826 que l'équation générale de degré 5 ne peut être résolue par radicaux après des tentatives incomplètes de Ruffini (1799) et de Cauchy (1815). Mais c'est à Galois que revient le mérite d'achever ce travail en introduisant le groupe (de permutation des racines) qui porte son nom et qui permet de donner un critère pour qu'une équation soit résoluble par radicaux.

Le but de ce texte est de montrer le théorème de Galois qui fait le lien entre équations résolubles et groupes résolubles, de donner quelques exemples d'équations résolubles ou non résolubles et de prouver que l'équation générique de degré $n \geq 5$ n'est pas résoluble par radicaux.

1. Lagrange parle de la *métaphysique de la résolution des équations du troisième et du quatrième degré.*

2 Groupes résolubles

2.1 Les définitions

La notion de groupe résoluble – qui, comme son nom l'indique, est liée à la résolution des équations – généralise celle de groupe abélien. En vérité, il y a deux généralisations possibles de la notion de groupe abélien, l'une, fondée sur le centre, est celle de groupe nilpotent, l'autre, sur les commutateurs, celle de groupe résoluble. Rappelons une définition :

2.1 Définition. *Soit G un groupe. Le* **commutateur** *de $x, y \in G$ est l'élément $[x, y] = xyx^{-1}y^{-1}$.*

Bien entendu, x et y commutent si et seulement si $[x, y] = 1$ et G est commutatif si et seulement si tous ses commutateurs sont triviaux. La notion suivante est celle de groupe dérivé :

2.2 Définition. *Soit G un groupe. Le* **groupe dérivé** *de G est le sous-groupe $D(G)$ de G engendré par les commutateurs de G. On définit par récurrence la suite des groupes dérivés par la formule $D^n(G) = D(D^{n-1}(G))$.*

2.3 *Remarques.* 1) L'opération D est croissante : si l'on a $H \subset G$ on a $D(H) \subset D(G)$.

2) Pour obtenir un exemple où le mot "engendré" est essentiel, le lecteur résoudra l'exercice suivant.

2.4 *Exercice.* On considère le groupe $G = SL(2, \mathbf{R})$.

1) Montrer qu'on a $D(G) = G$, donc que $-\mathrm{Id}$ est un produit de commutateurs (consulter [7] au besoin).

2) Montrer que $-\mathrm{Id}$ n'est pas un commutateur dans G. Pour cela, on suppose qu'on a $-\mathrm{Id} = MNM^{-1}N^{-1}$ avec $M, N \in G$ et on résout les questions suivantes.

a) Montrer que N est conjugué de $-N$ dans G, en déduire qu'on a $\mathrm{Tr}\, N = 0$, puis $N^2 + \mathrm{Id} = 0$ et que N est conjugué dans $GL(2, \mathbf{R})$ de $B = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$.

b) Montrer qu'on peut supposer $N = B$.

c) Montrer que si M vérifie $-B = MBM^{-1}$ on a $\det M < 0$ et conclure.

La proposition suivante est évidente :

2.5 Proposition. *Le groupe dérivé de G est un sous-groupe distingué dans G et même caractéristique (i.e. invariant par tout automorphisme). Le quotient $G/D(G)$ est le plus grand quotient abélien de G (i.e. si N est un sous-groupe distingué de G et si G/N est abélien, on a $D(G) \subset N$). Le groupe G est abélien si et seulement $D(G)$ est réduit à l'élément neutre.*

On peut maintenant définir la notion de groupe résoluble.

2.6 Proposition-Définition. *Soit G un groupe. Les conditions suivantes sont équivalentes :*

1) Il existe $n \in \mathbf{N}$ tel que $D^n(G) = \{1\}$.

2) Il existe une suite de sous-groupes $G_0 = \{1\} \subset G_1 \subset \cdots \subset G_n = G$ tels que chaque G_i est distingué dans G et que chaque quotient G_{i+1}/G_i pour $i = 0, \ldots, n-1$ est abélien.

3) Comme 2) mais en supposant seulement que G_i est distingué dans G_{i+1}.

On dit que G est **résoluble** *s'il vérifie les propriétés ci-dessus.*

Démonstration. On montre 1) $\Longrightarrow$ 2) en posant $G_i = D^{n-i}(G)$ et 2) $\Longrightarrow$ 3) est trivial. Pour 3) $\Longrightarrow$ 1) on montre par récurrence descendante sur i qu'on a $D^{n-i}(G) \subset G_i$. Pour le pas de récurrence, on a $D^{n-i}(G) \subset G_i$, donc $D^{n-(i-1)}(G) \subset D(G_i)$ par la croissance de D, puis $D(G_i) \subset G_{i-1}$ par 2.5.

2.2 Exemples

2.7 Proposition. *1) Pour $n \geq 2$ on a $D(\mathfrak{S}_n) = \mathfrak{A}_n$.*

2) Pour $n \geq 5$ on a $D(\mathfrak{A}_n) = \mathfrak{A}_n$.

3) Le groupe $\mathfrak{S}_2$ est abélien, les groupes $\mathfrak{S}_3$ et $\mathfrak{S}_4$ sont résolubles. Les groupes $\mathfrak{S}_n$ et $\mathfrak{A}_n$ ne sont pas résolubles pour $n \geq 5$.

Démonstration. Voir [7] Ch. 1 §8.

2.3 Propriétés

2.8 Proposition. *1) Si G est résoluble, tout sous-groupe et tout quotient de G est résoluble.*

2) Si N et H sont résolubles et si G est extension de N par H (i.e. il existe un sous-groupe distingué de G isomorphe à N dont le quotient est isomorphe à H), alors G est résoluble.

Démonstration. 1) Supposons G résoluble et soit H un sous-groupe de G. Comme on a $D^k(H) \subset D^k(G)$ il est clair que H est résoluble. Soit N un sous-groupe distingué de G et $p : G \to G/N$ la projection. On vérifie qu'on a $D(G/N) = p(D(G))$ (car on a $p(ghg^{-1}h^{-1}) = p(g)p(h)p(g)^{-1}p(h)^{-1}$) et, plus généralement $D^k(G/N) = p(D^k(G))$, ce qui montre que le quotient est résoluble.

2) Si $H = G/N$ est résoluble, il admet une suite de sous-groupe distingués $H_i \subset H$ à quotients H_{i+1}/H_i abéliens. Si p est la projection de G sur H, les

$\widehat{H_i} := p^{-1}(H_i)$ sont distingués dans G avec des quotients $\widehat{H_{i+1}}/\widehat{H_i} \simeq H_{i+1}/H_i$ abéliens et, comme N est résoluble, on complète cette suite avec des N_i distingués dans N à quotients abéliens, ce qui montre que G est résoluble [2].

2.9 Proposition. *Un groupe simple et résoluble est isomorphe à* $\mathbf{Z}/p\mathbf{Z}$ *pour* p *premier.*

Démonstration. Rappelons qu'un groupe G est simple s'il n'est pas réduit à $\{1\}$ et si ses seuls sous-groupes distingués sont lui-même et $\{1\}$. Si G est simple on a donc $D(G) = G$ ou $D(G) = \{1\}$. Dans le premier cas, on a $D^n(G) = G$ et G n'est pas résoluble. Dans le second il est abélien, donc a des sous-groupes distingués de tout cardinal diviseur de $|G|$ et, comme il est simple, ce cardinal est donc premier.

2.10 *Remarque.* Il résulte de ce qui précède que, dans la caractérisation 2) de 2.6, on peut supposer que les quotients sont non seulement abéliens, mais cycliques d'ordre premier. En revanche on ne peut pas imposer cette condition dans la caractérisation 3) comme en témoigne l'exemple de $\mathfrak{A}_4$ dont l'unique sous-groupe distingué est le groupe $\mathbf{V}_4$ de Klein formé des doubles transpositions τ_i, groupe dont les seuls sous-groupes (distingués) sont engendrés par les τ_i qui ne sont pas distingués dans $\mathfrak{A}_4$.

3 Extensions radicales, extensions résolubles

3.1 Notations

Les rudiments de théorie des corps utilisés ici (corps de rupture et de décomposition, etc.) peuvent être trouvés dans [7] ou [9].

Tous les corps considérés dans ce texte sont supposés commutatifs et, sauf mention expresse du contraire, de caractéristique 0.

Une extension de corps est simplement une inclusion $K \subset L$. On parle parfois de l'extension L/K. Toutes les extensions sont supposées finies (i.e. L est un K-espace vectoriel de dimension finie).

Une tour est une suite de telles inclusions $K_0 \subset K_1 \subset \cdots \subset K_n$.

Le corps de décomposition d'un polynôme $P \in K[X]$ sur K est noté $D_K(P)$. C'est un corps engendré par les racines de P, il est unique à isomorphisme près.

2. On notera qu'ici c'est la caractérisation 3) qui donne le résultat car les sous-groupes distingués dans N ne le sont pas nécessairement dans G.

3.2 Les définitions principales

Dans ce paragraphe, on formalise la définition de la résolution par radicaux.

3.1 Définition. *Une extension $K \subset L$ est dite* **radicale** *s'il existe une tour*[3] *: $K = K_0 \subset K_1 \subset \cdots \subset K_n = L$ avec, pour tout $i = 1, \ldots, n$, $K_i = K_{i-1}(\alpha_i)$ où α_i vérifie $\alpha_i^{n_i} = a_i \in K_{i-1}$, avec $n_i \in \mathbf{N}^*$.*

3.2 *Remarque.* À chaque pas le nombre rajouté $\alpha_i = \sqrt[n_i]{a_i}$ est bien un radical et la présence de plusieurs extensions dans la tour signifie que les éléments de L s'obtiennent à partir de K par adjonction successives de radicaux. On obtient ainsi par exemple des éléments du type suivant :

$$\sqrt[3]{11}\,\sqrt[5]{\frac{7-\sqrt[6]{3}}{\sqrt[3]{2}}} + \sqrt[7]{23+\sqrt[3]{7}}.$$

3.3 Définition. *Une extension $K \subset L$ est dite* **résoluble** *(sous-entendu par radicaux), s'il existe une extension M de L telle que $K \subset M$ soit radicale.*

3.4 Définition. *Soit $P \in K[X]$ un polynôme. On dit que l'équation $P(x) = 0$ est* **résoluble par radicaux** *si l'extension $K \subset D_K(P)$ est résoluble.*

3.5 *Remarques.* 1) Une équation est résoluble par radicaux si toutes ses racines s'écrivent à l'aide de radicaux comme on l'a vu en 3.2. On pourrait imaginer une définition plus faible où l'on impose seulement qu'une des racines soit de cette forme. Pour P irréductible, on verra que ces deux définitions reviennent au même, voir 3.9.

2) La différence entre extensions résolubles et radicales est un peu plus subtile. On la comprendra mieux en regardant l'exemple des équations de degré 3 où la différence tient à la présence ou non de racines cubiques de l'unité, voir 5.7.

3) En caractéristique p, la bonne notion fait intervenir non seulement les équations radicales $x^n - a = 0$, mais aussi les équations de la forme $x^p - x - a = 0$, voir [4] Ch. VIII, §6.

3.3 Quelques propriétés

3.3.1 Deux premiers résultats

3.6 Proposition. *Soient $K \subset L \subset M$ des extensions.*

1) Si M/K est radicale, M/L l'est aussi.

2) Si L/K et M/L sont radicales, M/K l'est aussi.

3. Que l'on pourra dire radicale.

Démonstration. 1) Si les radicaux α_i engendrent la tour sur K ils l'engendrent *a fortiori* sur L.

2) Il suffit d'empiler les tours de L/K et M/L.

3.7 *Remarque.* En revanche, si M/K est radicale, L/K ne l'est pas nécessairement, voir 5.8.

3.8 Proposition. *Soit L/K une extension radicale et M une clôture normale de L sur K (voir 9.5). Alors l'extension M/K est radicale.*

Démonstration. Rappelons[4] que si $L = K(x_1, \dots, x_m)$, si on appelle P_i le polynôme minimal de x_i sur K et si on pose $P = P_1 \cdots P_m$, une clôture normale est un corps de décomposition $M = D_K(P)$.

La démonstration se fait par récurrence sur le nombre n d'étages d'une tour radicale de L/K. Pour $n = 0$ on a $K = L = M$ et le résultat est évident. Supposons donc le résultat établi pour $n - 1 \geq 0$ et passons à n. On a une tour $K = K_0 \subset K_1 \subset \cdots \subset K_{n-1} \subset K_n = L$ avec $K_i = K_{i-1}(\alpha_i)$ où α_i vérifie $\alpha_i^{n_i} = a_i \in K_{i-1}$. En particulier $L = K_{n-1}(\alpha)$ avec $\alpha^r = a \in K_{n-1}$. La clôture normale L_{n-1} de K_{n-1} est de la forme $D_K(Q)$ et, par l'hypothèse de récurrence, elle est radicale sur K. Comme M/K est normale, L_{n-1} s'injecte dans M.

Soit P le polynôme minimal[5] de α sur K. On a alors $M = D_K(PQ)$ et, si $\alpha = \alpha_1, \dots, \alpha_s$ sont les racines de P dans M, on a $M = L_{n-1}(\alpha_1, \dots, \alpha_s)$. Comme le groupe de Galois $G := \mathrm{Gal}(M/K)$ opère transitivement sur les α_i (voir 9.14), il existe $g_i \in G$ tel que $g_i(\alpha) = \alpha_i$. On a donc $\alpha_i^r = g_i(\alpha)^r = g_i(\alpha^r) = g_i(a)$ et comme a est dans L_{n-1} et que L_{n-1}/K est normale, le conjugué $g_i(a)$ est dans L_{n-1}. On voit que les α_i sont des radicaux d'éléments de L_{n-1}, de sorte que l'extension $L_{n-1} \subset M$ est radicale et donc aussi M/K en vertu de 3.6.

3.9 *Remarque.* Ce résultat permet de répondre à la question soulevée en 3.5.1 : si l'une des racines α d'un polynôme **irréductible** P s'exprime sous forme radicale, alors la propriété vaut pour toutes. En effet, l'hypothèse signifie que $K(\alpha)$ est inclus dans une extension L radicale, dont la clôture normale M est aussi radicale. Mais, comme M/K est normale, elle contient les autres racines de P, qui sont donc aussi radicales.

4. Attention, cette démonstration n'est pas complètement évidente et est assez emblématique des difficultés de la théorie de Galois pour les débutants.

5. Attention, il faut prendre le polynôme minimal sur K sous peine de perdre des conjugués.

3.3.2 Quelques résultats auxiliaires

La problématique de ce paragraphe est la suivante. On suppose qu'on a deux extensions $K \subset L$ et $K \subset M$ et il s'agit de construire un corps N qui coiffe les deux, c'est-à-dire tel que l'on ait $L \subset N$ et $M \subset N$. Attention, tel quel, ce n'est pas toujours possible. Par exemple, si on prend $k = \mathbf{R}$ et si L et M sont les sous-corps $\mathbf{R}(i)$ et $\mathbf{R}(j)$ du corps des quaternions $\mathbf{H}$, il n'existe pas de surcorps commutatif N qui les contienne tous les deux (sinon, l'équation $x^2 + 1 = 0$ aurait au moins quatre racines $\pm i, \pm j$ dans N). Il faut donc être plus précis et utiliser un homomorphisme de corps (nécessairement injectif, on parle de plongement). Le lemme est alors le suivant :

3.10 Lemme. *Soient $K \subset L$ et $K \subset M$ deux extensions. Il existe un corps N contenant M et un plongement $j : L \to N$ qui est l'identité sur K.*

Démonstration. Puisqu'on a supposé que les corps sont de caractéristique zéro, on peut supposer $L = K(x)$ par le théorème de l'élément primitif, voir 9.10. Soit P le polynôme minimal de x sur K et posons $N = D_M(P)$. C'est un corps contenant M et, comme il contient toutes les racines de P, il contient un corps de rupture de P sur K, qui est isomorphe à L par un K-isomorphisme (voir [7], Ch. III, 1.28).

L'intervention d'un plongement est innocente du point de vue de la radicalité, comme le montre le lemme suivant :

3.11 Lemme. *Soit $K \subset L$ une extension radicale et $j : L \to L'$ un K-isomorphisme. Alors $K \subset L'$ est radicale.*

Démonstration. Il suffit de transporter la tour par l'isomorphisme j.

3.12 Corollaire. *Soient $K \subset L$ et $K \subset M$ deux extensions avec L, M contenus dans N. On suppose que M/K est radicale et on note LM le sous-corps de N engendré par L et M. Alors l'extension $L \subset LM$ est radicale.*

Démonstration. On a la tour radicale $K \subset K(\alpha_1) \subset \cdots \subset K(\alpha_1, \ldots, \alpha_n) = M$ et elle donne la tour radicale $L \subset L(\alpha_1) \subset \cdots \subset L(\alpha_1, \ldots, \alpha_n) = LM$.

Nous aurons besoin du résultat suivant (utilisé par Abel dans son mémoire) :

3.13 Lemme. *Soit $K \subset M$ une extension radicale avec $K \neq M$. Il existe une tour $K = K_0 \subset K_1 \subset \cdots \subset K_r = M$ telle que, pour chaque $i = 1, \ldots, n$, K_i soit de la forme $K_i = K_{i-1}(\alpha_i)$ avec $\alpha_i^{p_i} = a_i$, $a_i \in K_{i-1}$ et p_i* **premier**.

Démonstration. On se ramène au cas où $M = K(\alpha)$ avec $\alpha^n = a$, $a \in K$ et n entier, $n > 1$. Si n n'est pas premier, on prend un facteur premier p de n, on considère $\beta = \alpha^{n/p}$ et on a $\beta^p = a$. On a donc décomposé l'extension en $K \subset K(\beta) \subset K(\alpha)$ et on conclut en raisonnant par récurrence sur n (puisque $\alpha^{n/p} = \beta$).

3.3.3 La troisième proposition

3.14 Proposition. *On considère des extensions $K \subset L \subset M$. Alors M/K est résoluble si et seulement si L/K et M/L sont résolubles.*

Démonstration. Si M/K est résoluble, M est plongée dans une extension radicale N de K. Il en résulte aussitôt que L/K est résoluble et, comme N/L est radicale par 3.6, M/L est aussi résoluble.

Inversement, si les deux étages sont résolubles, on peut plonger L dans L' avec L'/K radicale et M dans M' avec M'/L radicale. On applique alors 3.10 à $L \subset M'$ et $L \subset L'$: il existe N' avec $M' \subset N'$ et un plongement $j : L' \to N'$, d'image L'', qui est l'identité sur L. On applique ensuite 3.12 avec $L \subset L''$ et $L \subset M'$, tous contenus dans N', qui montre que $L''M'$ est radicale sur L''. Mais, par 3.11, L'' est radicale sur K, donc $L''M'$ aussi par transitivité. Comme M est contenue dans $L''M'$, elle est donc résoluble.

4 Le théorème de Galois

4.1 L'énoncé du théorème

L'énoncé du théorème met en parallèle les deux acceptions de résoluble :

4.1 Théorème. (Galois) *Soit $K \subset L$ une extension galoisienne. Alors l'extension est résoluble si et seulement si son groupe de Galois l'est.*

4.2 Un exemple

Le théorème de Galois permet de donner des exemples d'équations non résolubles par radicaux.

4.2 Proposition. *L'équation $x^5 - 6x + 3 = 0$ n'est pas résoluble par radicaux sur $\mathbf{Q}$.*

Démonstration. Le critère d'Eisenstein assure que F est irréductible sur $\mathbf{Q}$. Pour voir que l'équation n'est pas résoluble, il suffit de montrer que le groupe de Galois de cette équation est $\mathfrak{S}_5$, dont on a vu en 2.7 qu'il est non résoluble. Comme l'étude de la fonction $x \mapsto x^5 - 6x + 3$ montre que le polynôme F a exactement trois racines réelles, cela résulte du lemme suivant :

4.3 Lemme. *Soit p un nombre premier ≥ 3, $F \in \mathbf{Q}[X]$ un polynôme irréductible de degré p. On suppose que F admet, dans $\mathbf{C}$, $p-2$ racines réelles et 2 racines imaginaires conjuguées. Alors on a* $\mathrm{Gal}(F) \simeq \mathfrak{S}_p$.

Démonstration. (du lemme) On considère la conjugaison complexe τ. C'est un automorphisme de corps, qui fixe $\mathbf{Q}$ et laisse invariant le corps $D_{\mathbf{Q}}(F)$. De plus, comme F admet $p-2$ racines réelles (invariantes par τ) et deux imaginaires conjuguées (échangées par τ), τ, vue comme permutation des racines, est une transposition. Par ailleurs, comme le polynôme F est irréductible, le groupe $\mathrm{Gal}(F)$ est transitif sur les racines de F (voir 9.14). Son cardinal est donc multiple de p, donc il contient un élément d'ordre p, qui, comme p est premier, est nécessairement un p-cycle. Mais on sait qu'un p-cycle et une transposition engendrent $\mathfrak{S}_p$ et on a le résultat.

4.4 *Remarques.* 1) L'exemple ci-dessus fournit des exemples d'équations de tout degré $n \geq 5$ non résolubles par radicaux au sens où toutes leurs racines ne sont pas radicales. Il suffit en effet de prendre $x^{n-5}(x^5 - 6x + 3) = 0$. Bien entendu, c'est une tricherie honteuse ...

2) Plus sérieusement, on peut montrer que le groupe de Galois de l'équation $x^n - x - 1 = 0$ est toujours égal à $\mathfrak{S}_n$, mais c'est beaucoup plus difficile, voir [8] pour l'irréductibilité du polynôme et [5] pour le calcul du groupe de Galois. Pour un exemple plus accessible (de degré premier), le lecteur traitera le très bel exercice suivant (emprunté à [3] §3.6 Exercice 7).

4.5 *Exercice.* Soit p un nombre premier. Le but de l'exercice est de construire un polynôme $P \in \mathbf{Q}[X]$, irréductible de degré p et de groupe de Galois $\mathfrak{S}_p$, de sorte que l'équation $P(x) = 0$ n'est pas résoluble par radicaux pour $p \geq 5$.

1) Traiter les cas $p = 2, 3$. On suppose désormais $p \geq 5$.

2) On considère le polynôme (de degré p) :

$$Q(X) = (X^2 + m)(X - 2)(X - 4) \cdots (X - 2(p - 2))$$

où m est un entier pair positif.

a) Montrer que les nombres $Q(1)$, $Q(3)$, $Q(5)$, ..., $Q(2p-3)$ sont tous plus grands que 2 en valeur absolue et de signes alternés.

b) On pose $P(X) = Q(X) - 2$. Montrer que $P(X)$ admet au moins $p-2$ racines réelles.

c) On rappelle que, si le polynôme $X^n + a_1X^{n-1} + a_2X^{n-2} + \cdots + a_n$ admet les racines $x_1, \ldots, x_n$, on a $\sum_{i=1}^n x_i^2 = a_1^2 - 2a_2$. En déduire que la somme des carrés des racines est la même pour P et Q et qu'elle est négative si m est assez grand.

d) Montrer que P admet exactement deux racines complexes conjuguées.

e) Montrer que P est irréductible (utiliser le critère d'Eisenstein) et conclure avec 4.3.

4.3 La preuve du théorème, le sens direct

4.3.1 Trois exemples

Le sens direct du théorème va résulter de l'étude de trois exemples.

4.6 Proposition. *Soit n un entier ≥ 1 et soit $K \subset L = K(\zeta)$ où ζ désigne une racine primitive n-ième de l'unité. L'extension $K \subset L$ est galoisienne et son groupe de Galois s'injecte dans $(\mathbf{Z}/n\mathbf{Z})^*$, donc est abélien.*

Démonstration. Comme ζ est une racine primitive n-ième de l'unité, L est le corps de décomposition du polynôme $X^n - 1$, de sorte que l'extension L/K est galoisienne (elle est séparable car on est en caractéristique 0). Soit $\sigma \in \mathrm{Gal}(L/K)$, alors $\sigma(\zeta)$ est une racine n-ième primitive de 1, de sorte qu'elle s'écrit $\sigma(\zeta) = \zeta^{i(\sigma)}$ avec $i(\sigma) \in \mathbf{Z}/n\mathbf{Z}$, premier à n, donc $i(\sigma) \in (\mathbf{Z}/n\mathbf{Z})^*$. De plus, si τ est un autre élément du groupe de Galois, correspondant à $i(\tau) \in (\mathbf{Z}/n\mathbf{Z})^*$, on a $\tau \circ \sigma(\zeta) = (\zeta^{i(\sigma)})^{i(\tau)} = \zeta^{i(\sigma)i(\tau)}$ et l'application $\sigma \mapsto i(\sigma)$ est donc un homomorphisme de $\mathrm{Gal}(L/K)$ dans $(\mathbf{Z}/n\mathbf{Z})^*$. Comme ζ est une racine primitive, cet homomorphisme est injectif et on a le résultat annoncé.

4.7 *Remarque.* Si le corps de base est $\mathbf{Q}$, le polynôme cyclotomique Φ_n est irréductible de degré $\varphi(n)$ (voir [7]) et le groupe de Galois est exactement $(\mathbf{Z}/n\mathbf{Z})^*$.

4.8 Proposition. *Soit $K \subset L = K(\alpha)$ avec $\alpha^n = a \in K$. On suppose que K contient une racine primitive n-ième de l'unité. L'extension $K \subset L$ est galoisienne et son groupe de Galois s'injecte dans $\mathbf{Z}/n\mathbf{Z}$ (donc est cyclique).*

Démonstration. Les racines du polynôme $X^n - a$ sont de la forme $\xi\alpha$ où ξ est une racine n-ième de l'unité. La présence d'une racine n-ième primitive de 1 (notée ζ) dans K assure que les racines de $X^n - a$ sont toutes dans L, donc que l'extension est galoisienne. Soit σ un élément de $\mathrm{Gal}(L/K)$. On a $\sigma(\alpha)^n = \sigma(a) = a$, ce qui impose $\sigma(\alpha) = \zeta^{i(\sigma)}\alpha$ avec $i(\sigma) \in \mathbf{Z}/n\mathbf{Z}$. De plus, si τ est un autre élément du groupe de Galois, on a $\tau \circ \sigma(\alpha) = \tau(\zeta^{i(\sigma)}\alpha) = \zeta^{i(\sigma)}\tau(\alpha) = \zeta^{i(\sigma)}\zeta^{i(\tau)}\alpha$ donc $i(\tau\sigma) = i(\tau) + i(\sigma)$. On a donc un homomorphisme de $\mathrm{Gal}(L/K)$ dans le groupe additif $\mathbf{Z}/n\mathbf{Z}$, évidemment injectif, d'où le résultat.

4.9 Proposition. *Soit K un corps, $a \in K^*$, $n \in \mathbf{N}^*$ et posons $L = D_K(X^n - a)$. L'extension $K \subset L$ est galoisienne et contient le sous-corps $K(\zeta)$ où ζ est une racine primitive n-ième de l'unité. Le groupe de Galois de L sur K est extension d'un groupe abélien par un groupe cyclique et il est donc résoluble.*

Démonstration. Il est clair que l'extension est galoisienne. Les racines du polynôme $X^n - a$ sont distinctes et si α, β sont deux telles racines, leur rapport est une racine n-ième de 1, de sorte que L contient le corps $M := K(\zeta)$ engendré par les racines n-ièmes de l'unité. Comme M/K est galoisienne, on a une suite exacte (voir 9.12) :

$$0 \to \mathrm{Gal}(L/M) \to \mathrm{Gal}(L/K) \to \mathrm{Gal}(M/K) \to 0$$

et on conclut par 4.6, 4.8 et 2.8.

4.10 *Exercice.* Soit $a \in \mathbf{Q}$ un rationnel et n un entier positif. On suppose que le polynôme $X^n - a$ est irréductible sur $\mathbf{Q}$.

1) Montrer que la condition est réalisée si a est de la forme $p_1 \cdots p_r$ avec des p_i premiers distincts (utiliser le critère d'Eisenstein).

2) Montrer que le groupe de Galois $\mathrm{Gal}_{\mathbf{Q}}(X^n - a)$ est le produit semi-direct $(\mathbf{Z}/n\mathbf{Z}) \rtimes (\mathbf{Z}/n\mathbf{Z})^*$.

4.11 *Exercice.* Soit K un corps de caractéristique différente de 2 et 3 et soit $P(X) = X^4 + q \in K[X]$.

1) Montrer que P est réductible dans deux cas exactement :

- Si $-q$ est un carré de K.
- Si $4q = a^4$ avec $a \in K$.

On donnera les décompositions de P dans les deux cas.

2) On suppose P irréductible sur K. Montrer que le groupe de Galois G de P sur K est le groupe diédral $\mathbf{D}_4$, sauf dans deux cas :

- Si K contient une racine quatrième primitive i de 1 auquel cas on a $G \simeq \mathbf{Z}/4\mathbf{Z}$.
- Si q est un carré de K auquel cas on a $G \simeq \mathbf{V}_4$ (groupe de Klein).

(Si i est dans K on utilisera 4.9, sinon, on étudiera la conservation de l'irréductibilité de P en passant de K à $K(i)$.)

4.3.2 Le sens direct

On peut maintenant prouver le sens direct de 4.1 : si l'extension est résoluble, le groupe de Galois l'est aussi.

1) On peut supposer que L/K est radicale (et galoisienne). En effet, comme L/K est résoluble on peut la plonger dans une extension radicale M/K et, en vertu de 3.8, on peut supposer M/K galoisienne. Si le théorème vaut dans ce cas, le groupe $\mathrm{Gal}(M/K)$ est résoluble, donc aussi son quotient $\mathrm{Gal}(L/K)$.

2) On prouve le théorème dans le cas radical en raisonnant par récurrence sur le degré n de l'extension, le cas $n = 1$ étant trivial. Par définition, il existe

une extension $K \subset K_1$ ($K_1 \neq K$) où K_1 est engendré par un radical α tel que $\alpha^r = a$ avec $a \in K$. On considère la clôture normale N de K_1 sur K. Rappelons que si P est le polynôme minimal de α sur K, c'est l'extension $D_K(P)$. C'est une extension galoisienne, radicale en vertu de 3.8. Comme M/K est normale, on peut supposer que N est contenue dans M. Il y a deux cas :

a) Si N est strictement contenue dans M, les deux extensions N/K et M/N sont radicales et galoisiennes, de degré $< n$, donc, par l'hypothèse de récurrence, leurs groupes de Galois sont résolubles. Mais alors, $\mathrm{Gal}(M/K)$ qui en est extension, l'est aussi.

b) Si N est égale à M, comme α est racine de $X^r - a$, son polynôme minimal P divise $X^r - a$, de sorte que $N = M$ est contenue dans $N' := D_K(X^r - a)$. Mais le groupe de Galois de N'/K est résoluble en vertu de 4.9, donc aussi $\mathrm{Gal}(M/K)$ qui en est un quotient.

4.4 Le sens réciproque

Soit $K \subset L$ une extension galoisienne. On suppose que le groupe $G := \mathrm{Gal}(L/K)$ est résoluble et il s'agit de montrer que l'extension est résoluble. On raisonne par récurrence sur $|G|$, le cas $|G| = 1$ étant trivial.

1) Par dévissage on se ramène au cas où G est résoluble et simple, c'est-à-dire cyclique d'ordre p premier en vertu de 2.9. En effet, si G n'est pas simple, il admet un sous-groupe distingué H non trivial qui correspond, par la théorie de Galois (cf. 9.12) à une extension galoisienne intermédiaire non triviale $K \subset M \subset L$ avec $H = \mathrm{Gal}(L/M)$ et $G/H = \mathrm{Gal}(M/K)$. Comme ces groupes sont résolubles en vertu de 2.8, l'hypothèse de récurrence assure que les extensions M/K et L/M le sont et on conclut par 3.6.

2) Comme tout groupe d'ordre p premier est isomorphe à $\mathbf{Z}/p\mathbf{Z}$, il reste donc à prouver :

4.12 Lemme. *Soit $K \subset L$ une extension galoisienne de groupe de Galois $\mathbf{Z}/p\mathbf{Z}$. Alors L/K est résoluble.*

3) On commence par prouver le cas particulier suivant :

4.13 Lemme. *Soit $K \subset L$ une extension galoisienne de groupe $\mathbf{Z}/p\mathbf{Z}$. On suppose que K contient une racine p-ième primitive ζ de 1. Alors $L = K(\alpha)$, avec $\alpha^p = a \in K$.*

Admettons un instant ce lemme et prouvons 4.12. Posons $M = D_L(X^p - 1)$. On a $M = L(\zeta)$ où ζ est une racine primitive p-ième de l'unité. On note que M/K est encore normale [6]. En effet, comme L/K est normale on a $L = D_K(P)$, avec $P \in K[X]$ et il s'ensuit que M est le corps de décomposition de $(X^p - 1)P$ qui est encore à coefficients dans K. Il suffit alors de prouver que M/K est radicale. Mais on a $K \subset K(\zeta) \subset M$ et comme $K(\zeta)/K$ est radicale, il suffit de voir que $M/K(\zeta)$ l'est. On a deux morphismes de groupes, une inclusion $i : \mathrm{Gal}(M/K(\zeta)) \to \mathrm{Gal}(M/K)$ et une projection (la restriction) $p : \mathrm{Gal}(M/K) \to \mathrm{Gal}(L/K)$ et le composé $p \circ i$ est injectif car si $\sigma \in \mathrm{Gal}(M/K(\zeta))$ est l'identité sur L, comme il l'est aussi sur $K(\zeta)$, il l'est sur $M = L(\zeta)$. Le groupe de Galois de M sur $K(\zeta)$ s'injecte donc dans $\mathbf{Z}/p\mathbf{Z}$ donc, comme p est premier, c'est $\{1\}$ ou $\mathbf{Z}/p\mathbf{Z}$. Dans le premier cas on a $M = K(\zeta)$ et M/K est radicale, dans le second, on conclut par le lemme 4.13.

4) Il reste à prouver 4.13. Il y a de nombreuses méthodes ! On note τ un générateur de G. On a donc $\tau^p = \mathrm{Id}$. Il suffit de trouver $\alpha \in L$, $\alpha \notin K$, tel que $\tau(\alpha) = \zeta\alpha$. En effet, on a alors $\tau(\alpha)^p = \tau(\alpha^p) = \zeta^p \alpha^p = \alpha^p$ et $a := \alpha^p$ est invariant par G, donc dans K (voir 9.13). Comme α n'est pas dans K il engendre L (car le degré de $K(\alpha)$ divise p, donc est égal à p) et on a gagné.

a) Une première méthode consiste à prendre α de la forme :

$$\alpha = R(x, \zeta) := x + \zeta\tau(x) + \zeta^2\tau^2(x) + \cdots + \zeta^{p-1}\tau^{p-1}(x)$$

($R(x, \zeta)$ est ce qu'on appelle une résolvante de Lagrange [7]). On a $\tau(\alpha) = \tau(x) + \zeta\tau^2(x) + \cdots + \zeta^{p-1}x = \alpha/\zeta = \xi\alpha$ (en posant $\xi = \zeta^{-1}$) et on a gagné, pourvu que α ne soit pas dans K. Si α est dans K il est invariant par τ et on a $\alpha = \xi\alpha$ donc $\alpha = 0$. Le tout est donc de trouver un $x \in L$ et une racine primitive de l'unité tels que $R(x, \zeta)$ soit non nul.

a1) Une méthode élémentaire pour faire cela consiste à prendre y tel que $L = K(y)$. On pose alors $\beta = y + \tau(y) + \cdots + \tau^{p-1}(y)$, qui est invariant par τ, donc dans K, puis $x = y - \frac{\beta}{p}\cdot$ On a encore $L = K(x)$ avec cette fois $x + \tau(x) + \cdots + \tau^{p-1}(x) = 0$. Je dis qu'il existe une racine primitive de 1 telle que $R(\xi, x) \neq 0$. Sinon, le système de p équations linéaires à p inconnues :

$$x + \tau(x) + \cdots + \tau^{p-1}(x) = 0$$

$$x + \zeta\tau(x) + \cdots + \zeta^{p-1}\tau^{p-1}(x) = 0$$

$$x + \zeta^2\tau(x) + \cdots + \zeta^{2(p-1)}\tau^{p-1}(x) = 0$$

$$\cdots$$

$$x + \zeta^{p-1}\tau(x) + \cdots + \zeta^{(p-1)^2}\tau^{p-1}(x) = 0$$

6. Attention, la notion d'extension normale n'est pas transitive.
7. Voilà le premier protagoniste de notre histoire.

admet la solution non nulle $x, \tau(x), \dots, \tau^{p-1}(x)$. Mais cela implique que son déterminant est nul. Or, ce déterminant est le déterminant de Van der Monde[8] associé à $1, \zeta, \dots, \zeta^{p-1}$ qui est non nul !

a2) Pour trouver x on peut aussi invoquer le lemme d'indépendance des automorphismes d'Artin :

4.14 Lemme. *Soit L un corps, $\tau_1, \dots, \tau_n$ des automorphismes distincts de L. Alors les τ_i sont indépendants sur L, i.e. si l'on a $\lambda_1\tau_1 + \cdots + \lambda_n\tau_n = 0$ avec des $\lambda_i \in L$, on a $\lambda_i = 0$ pour tout i.*

Démonstration. (du lemme) On suppose qu'on a une relation non triviale et on la suppose de longueur $n \geq 2$ minimale, de sorte que les λ_i sont tous non nuls. On a donc, pour tout $x \in L$, $\sum_{i=1}^n \lambda_i\tau_i(x) = 0$ et, pour tout $y \in L$, en multipliant par $\tau_1(y)$, $\sum_{i=1}^n \lambda_i\tau_i(x)\tau_1(y) = 0$. Mais, on a aussi $\sum_{i=1}^n \lambda_i\tau_i(xy) = 0$ et, en soustrayant, on a pour tous $x, y \in L$:

$$0 = \lambda_2\tau_2(x)(\tau_1(y) - \tau_2(y)) + \cdots + \lambda_n\tau_n(x)(\tau_1(y) - \tau_n(y)).$$

Mais, comme τ_n et τ_1 sont distincts, il existe y tel que $\tau_1(y) - \tau_n(y) \neq 0$ et la relation précédente, qui vaut pour tout x, donne une relation linéaire entre $\tau_2, \dots, \tau_n$ donc plus courte que la relation initiale, ce qui est absurde.

On peut alors trouver une résolvante de Lagrange non nulle. En effet, comme les τ^i sont distincts, on a $\mathrm{Id} + \zeta\tau + \cdots + \zeta^{p-1}\tau^{p-1} \neq 0$, donc il existe x avec $R(x, \zeta) \neq 0$.

2) La dernière méthode[9] est de penser en termes de valeurs propres. En effet, il suffit de montrer que τ, vu comme K-endomorphisme de L, admet une valeur propre ζ racine p-ième primitive de 1 car un vecteur propre α pour ζ sera non nul donc un générateur de L. Mais on a $\tau^p = \mathrm{Id}$ de sorte que le polynôme minimal de τ divise $X^p - 1$, donc n'a que des racines simples. Il en résulte que τ est diagonalisable et, comme il n'est pas l'identité, il a une valeur propre $\neq 1$!

4.15 *Remarque.* Comme on le verra dans le cas de l'équation de degré 3, l'intérêt de la résolvante de Lagrange est de fournir **explicitement** un radical qui engendre L/K.

4.16 *Exercice.* Retrouver la résolvante de Lagrange comme un vecteur propre de τ en utilisant une base de L/K de la forme $x, \tau(x), \dots, \tau^{p-1}(x)$.

8. Voilà le second !
9. Qui m'a été soufflée par Claire Voisin quand elle était élève à l'ENSJF.

5 Exemple 1 : l'équation de degré 3

5.1 Le cadre

Soit K un corps et $P(X) = X^3 + aX^2 + bX + c$ un polynôme unitaire de degré 3 à coefficients dans K. On se propose d'étudier, voire de calculer, l'extension $L = D_K(P)$. La première remarque est bien classique :

5.1 Proposition. *On suppose que K n'est pas de caractéristique* 3. *Il existe $p, q \in K$ tels que L soit le corps de décomposition du polynôme $Y^3 + pY + q$.*

Démonstration. On sait que $-a$ est la somme des racines de P. Pour l'annuler, on effectue le changement de variable $Y = X + \frac{a}{3}$ et on a $P(X) = P(Y - \frac{a}{3}) = Y^3 + pY + q$ avec $p = b - \frac{a^3}{3}$ et $q = \frac{2a^3}{27} - \frac{ab}{3} + c$.

5.2 *Exercice.* Le but de cet exercice est d'exhiber, en caractéristique 3, un polynôme de degré 3 dont le corps de décomposition n'est pas celui d'un polynôme $Y^3 + pY + q$.

1) Soient K un corps de caractéristique 3, $Q(Y) = Y^3 + pY + q$ avec $p, q \in K$ et $L = D_K(Q)$. Soient u, v, w les racines de Q dans L. Montrer qu'on a la formule $-vw - wu - uv = (u - v)^2$ et en déduire que le discriminant $\Delta(Q) = -p^3$ est un carré de K.

2) Soit $K = \mathbf{F}_3(T)$ le corps des fractions rationnelles en l'indéterminée T. On considère le polynôme $P(X) = X^3 + X^2 - T$ à coefficients dans K.

a) Montrer que P est irréductible sur K (on montrera que sinon il aurait une racine dans $\mathbf{F}_3[T]$).

b) Montrer que le discriminant de P est égal à T (utiliser 10.7 avec P').

c) Montrer que l'extension $L = D_K(P)$ n'est pas le corps de décomposition d'un polynôme du type $Y^3 + pX + q$.

5.3 *Remarque.* En caractéristique 0 tout polynôme est séparable. Si la caractéristique p de K est positive mais distincte de 2 et 3 tout polynôme de degré 3 est séparable (et donc L/K est séparable, voir 9.7). En effet, ses facteurs irréductibles sont de degrés $1, 2$ ou 3 donc ne sont pas des polynômes en X^p, donc sont séparables en vertu de 9.8.

Dans ce qui suit on suppose K de caractéristique différente de 2 **et** 3**.** On peut alors supposer P de la forme $X^3 + pX + q$ et on le suppose[10] **irréductible**. L'extension L/K est galoisienne et on note G son groupe de Galois. Si les racines de P dans L sont notées x_1, x_2, x_3, on a $L = K(x_1, x_2, x_3)$ et G s'identifie à un sous-groupe du groupe $\mathfrak{S}_3$ des permutations des x_i. Les

10. Si ce n'est pas le cas, on se ramène à une équation de degré ≤ 2.

coefficients du polynôme se calculent à partir des racines : $0 = x_1 + x_2 + x_3$, $p = x_2x_3 + x_3x_1 + x_1x_2$ et $q = -x_1x_2x_3$.

On sait, voir 10.8, que le discriminant de P est alors $\Delta = -4p^3 - 27q^2$ et on a la proposition suivante :

5.4 Proposition. *1) Si Δ n'est pas un carré de K, on a $[L : K] = 6$ et $G \simeq \mathfrak{S}_3$.*

2) Si Δ est un carré de K, on a $[L : K] = 3$ et $G \simeq \mathfrak{A}_3$.

Démonstration. Comme le polynôme est irréductible, G est transitif sur les racines en vertu de 9.15, donc de cardinal multiple de 3. On conclut avec 10.4 qui montre que G est contenu dans $\mathfrak{A}_3$ si et seulement si Δ est un carré.

5.2 La résolvante de Lagrange

Comme le groupe G est un sous-groupe de $\mathfrak{S}_3$, il est résoluble, donc aussi l'extension L/K et nous allons chercher à voir si cette extension est radicale et, sinon, à plonger L dans une telle extension. Soit N le sous-groupe de G isomorphe à $\mathfrak{A}_3$ (égal à G si le discriminant est un carré). Ce groupe est cyclique d'ordre 3 engendré par un élément g qui correspond sur les x_i à la permutation circulaire $(1, 2, 3)$. Le corps fixe de N est l'extension $M := K(\sqrt{\Delta})$, de degré ≤ 2 et L est de degré 3 sur M. L'extension L/K sera radicale si l'on a $L = M(y)$ avec y radical de degré 3, donc vérifiant $y^3 = a$, $a \in M$. Si tel est le cas, y n'est pas dans M, donc il est de degré 3 sur M et le polynôme $Y^3 - a$ est son polynôme minimal. Comme L/M est galoisienne, elle contient les autres racines de ce polynôme qui sont jy et j^2y où j est une racine cubique de l'unité. Cela implique que j est dans L et même dans M car de degré ≤ 2 sur M. On voit que l'extension n'est radicale qu'en présence de racines cubiques de l'unité. C'est le moment d'appliquer le principe de Jeanne d'Arc[11] et d'adjoindre éventuellement à K une telle racine de l'unité, si elle n'y est déjà.

On suppose désormais que K contient les racines cubiques primitives de l'unité j et j^2.

On notera que cela n'altère pas l'irréductibilité de P (car il est de degré 3) mais que cela peut changer le groupe de Galois de $\mathfrak{S}_3$ en $\mathfrak{A}_3$ si Δ est égal à -3, discriminant de $K(j)$, modulo un carré.

Cela étant posé, on cherche alors $y \in M$ tel que $y^3 \in M$. Comme M est le corps fixe de N, qui est engendré par g, on doit avoir $g(y^3) = g(y)^3 = y^3$ et $g(y) \neq y$, donc $g(y) = jy$ ou j^2y. On cherche y sous la forme $y =$

11. Répondant à la question de ses juges : – *Jeanne, êtes-vous en état de grâce ? – Si je n'y suis, Dieu veuille m'y mettre, si j'y suis, Dieu veuille m'y tenir.*

$\lambda x_1 + \mu x_2 + \nu x_3$. Comme g correspond au cycle $(1, 2, 3)$, la relation $g(y) = \lambda x_2 + \mu x_3 + \nu x_1 = j^2 y$ impose $\lambda = \mu j^2$, $\mu = \nu j^2$ et $\nu = \lambda j^2$, soit $\mu = j\lambda$ et $\nu = j\mu$ donc, par exemple, $y = x_1 + jx_2 + j^2 x_3$. C'est cet élément que l'on appelle la **résolvante de Lagrange**[12]. Comme on a $g(y) = j^2 y$, donc $g(y^3) = y^3$, y^3 est bien dans M.

5.3 le calcul des racines

En fait, il y a une autre possibilité pour la résolvante qui est l'élément $z = x_1 + j^2 x_2 + jx_3$ obtenu à partir de y par la transposition $\tau = (3, 2)$. De la même manière on a $g(z) = jz$, donc $g(z^3) = z^3$ et $z^3 \in M$. Comme g et τ engendrent le groupe de Galois, $y^3 + z^3$ et $y^3 z^3$ sont invariants par G donc sont dans K (on les calculera explicitement dans un instant).

Notons déjà que y ou z n'est pas dans M (donc engendre L). En effet, si y est dans M on a à la fois $g(y) = y = j^2 y$ et cela impose $y = 0$ et de même pour z. Mais x_1, x_2, x_3 sont solutions du système suivant :

$$\begin{cases} x_1 + x_2 + x_3 = 0 \\ x_1 + jx_2 + j^2 x_3 = y \\ x_1 + j^2 x_2 + jx_3 = z \end{cases}$$

dont le déterminant est un Van der Monde non nul et, si y et z sont nuls, cela implique que les x_i sont tous nuls, ce qui est absurde. On voit que y et z ne sont pas tous deux nuls, donc que l'un d'eux engendre L, et on calcule les racines à partir de y, z en résolvant le système ci-dessus : $x_1 = (y + z)/3$, $x_2 = (j^2 y + jz)/3$ et $x_3 = (jy + j^2 z)/3$.

Il reste à calculer y et z. On note d'abord qu'on a $yz \in K$. En effet, cet élément est invariant par τ (qui échange y et z) et aussi par g : $g(yz) = g(y)g(z) = j^2 yjz = yz$. En fait, yz est un polynôme symétrique en les x_i, qui se calcule à partir des fonctions symétriques élémentaires, donc des coefficients du polynôme. En effet, on a :

$$yz = (x_1 + jx_2 + j^2 x_3)(x_1 + j^2 x_2 + jx_3) = x_1^2 + x_2^2 + x_3^2 - x_2 x_3 - x_3 x_1 - x_1 x_2$$

$$= (x_1 + x_2 + x_3)^2 - 3(x_2 x_3 + x_3 x_1 + x_1 x_2) = -3p.$$

On en déduit $y^3 z^3 = -27p^3$, puis on calcule $y^3 + z^3$ comme suit. On a $y + z = 3x_1$, d'où $(y + z)^3 = 27x_1^3 = y^3 + z^3 + 3yz(y + z)$, donc $y^3 + z^3 = 27x_1^3 + 27px_1$. Mais comme x_1 est solution de l'équation initiale, on obtient $y^3 + z^3 = -27q$.

12. On comparera avec celle apparue dans la preuve de 4.13

On peut alors calculer y^3 et z^3 comme racines de l'équation du second degré $X^2+27qX-27p^3$. Le discriminant D de cette équation est égal à -27Δ et on obtient :

$$y^3 = \frac{-27q + 3\sqrt{-3\Delta}}{2} \quad \text{et} \quad z^3 = \frac{-27q - 3\sqrt{-3\Delta}}{2}.$$

et on en déduit les x_i par les formules ci-dessus, par exemple :

$$x_1 = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{p^3}{27} + \frac{q^2}{4}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{p^3}{27} + \frac{q^2}{4}}}.$$

Attention, les racines cubiques y et z ne doivent pas être choisies n'importe comment car elles doivent vérifier $yz = -3p$. Une fois ce choix effectué, on a aussi $3x_2 = j^2y + jz$ et $3x_3 = jy + j^2z$. Ces formules (dites de Cardan) constituent la résolution par radicaux de l'équation du troisième degré.

5.4 Que faisait Cardan ?

Partant de l'équation $x^3+px+q = 0$, l'astuce de Cardan consiste à écrire x sous la forme $x = u+v$ puis à calculer $x^3+px+q = u^3+v^3+(3uv+p)(u+v)+q$ et à imposer la condition supplémentaire $3uv + p = 0$. L'équation se ramène alors à $u^3 + v^3 = -q$ et, avec $uv = -\frac{p}{3}$ donc $u^3v^3 = -\frac{p^3}{27}$ on calcule u^3 et v^3 en résolvant l'équation du second degré $Y^2 + qY - \frac{p^3}{27}$ et on en déduit u, v par extraction de racines cubiques (en n'oubliant pas la condition sur uv) et enfin $x = u + v$. On voit que le calcul est exactement le même que celui effectué ci-dessus avec $y = 3u$ et $z = 3v$.

5.5 Retrouver le calcul du discriminant

Les formules donnant y, z en fonction des x_i donnent, par différence, $y - z = (j - j^2)(x_2 - x_3)$, $y - jz = (1 - j)(x_1 - x_2)$ et $y - j^2z = (1 - j^2)(x_1 - x_3)$. Rappelons que le discriminant est donné par $\Delta = \delta^2$ avec $\delta = (x_1 - x_2)(x_1 - x_3)(x_2 - x_3)$. On en déduit aussitôt $y^3 - z^3 = (y - z)(y - jz)(y - j^2z) = 3(j - j^2)\delta$, puis $-27\Delta = (y^3 - z^3)^2$. Mais on a $(y^3 - z^3)^2 = (y^3 + z^3)^2 - 4y^3z^3 = 27^2q^2 + 4 \times 27p^3$ et on retrouve bien $\Delta = -4p^3 - 27q^2$.

5.6 Le cas "irréductible" de l'équation de degré 3

La méthode de Cardan s'applique sans difficulté lorsque le discriminant $D = -27\Delta$ de l'équation du second degré $X^2 + 27qX - 27p^3 = 0$ est positif. Ce cas se produit lorsque l'équation du troisième degré a une unique racine réelle en vertu du lemme suivant :

5.5 Lemme. *L'équation $x^3 + px + q = 0$ admet une unique racine réelle si et seulement si on a $4p^3 + 27q^2 > 0$.*

Démonstration. C'est un exercice facile en étudiant la fonction $f(x) = x^3 + px + q$.

Lorsque D est négatif (c'est-à-dire lorsque Δ est positif), on tombe sur une équation du second degré sans racine réelle [13]. On peut cependant faire le calcul de Cardan avec les complexes, et c'est d'ailleurs pour faire ce calcul qu'ils ont été inventés par Bombelli vers 1572. En fait, Bombelli introduit une sorte de signe supplémentaire à côté des signes plus (*piu*) et moins (*meno*), signe qu'il appelle *piu di meno* (plus de moins) et qui correspond en langage moderne à $i = \sqrt{-1}$. Il utilise aussi $-i$ appelé *meno di meno*. Je renvoie, pour de plus amples précisions, à ma page web :

`https://www.math.u-psud.fr/~perrin/CAPES/algebre/Cardan10.pdf`

La question est de savoir si ce détour par les complexes est inévitable. La proposition suivante [14] montre que c'est bien le cas :

5.6 Proposition. *Soit K un corps contenu dans $\mathbf{R}$ et soit $P(X) = X^3 + pX+q \in K[X]$ un polynôme irréductible. On suppose $\Delta = -4p^3-27q^2$ positif (de sorte que P admet trois racines réelles). Alors il n'existe pas d'extension radicale M de K, contenant $L = D_K(P)$ et contenue dans $\mathbf{R}$.*

Démonstration. Supposons qu'une telle extension radicale existe. Si $L = D_K(P) = K(x_1, x_2, x_3)$ où les x_i sont les racines de P, on note d'abord que la racine du discriminant $\sqrt{\Delta}$ est dans L. En effet, c'est, au signe près, $\delta = (x_1 - x_2)(x_1 - x_3)(x_2 - x_3)$, voir l'annexe 2 ci-dessous.

On peut remplacer K par $K(\sqrt{\Delta})$. En effet, cela ne change pas le fait que P est irréductible, ni l'extension M, mais l'extension L est maintenant engendrée par l'une quelconque des racines de P. Comme M est radicale, on peut l'écrire sous la forme $K = K_0 \subset K_1 \subset \cdots \subset K_n = M$ où chaque extension $K_{i-1} \subset K_i$ est engendrée par un radical α_i qui vérifie $\alpha_i^{p_i} = a_i$ avec $a_i \in K_{i-1}$ et p_i premier (voir 3.13). Comme P est irréductible sur K et scindé sur M, il existe un indice i tel que P soit irréductible sur K_{i-1} et scindé [15] sur K_i. Quitte à remplacer K par K_{i-1} et M par K_i on est ainsi ramené au cas où $M = K(\alpha)$ avec $\alpha^p = a \in K$ et p premier.

On sait (voir [7] Ch. 3 §2-3, exercice 9) qu'alors, soit X^p-a est irréductible sur K, soit il admet une racine dans K. Mais, dans ce dernier cas, comme

13. On parle traditionnellement de “cas irréductible” de l'équation de degré 3 dans cette situation.

14. La première version de la preuve de cette proposition comportait plusieurs imprécisions. Je remercie chaleureusement Marc Pichereau de me les avoir signalées.

15. Car le discriminant est un carré de K_{i-1}.

on est dans $\mathbf{R}$ il n'y a qu'une racine réelle qui est donc α (ou $-\alpha$ si $p=2$) et on a $K=L=M$ ce qui est exclu.

Le polynôme X^p-a étant maintenant irréductible, l'extension $K\subset M$ est de degré p premier. Mais on a vu que M contient $L=K(x_1,x_2,x_3)$ qui est de degré 3. Elle lui est donc égale, de sorte que l'on a $p=3$. Comme L est normale sur K, le polynôme $X^p-a=X^3-a$ est scindé dans L et il admet trois racines distinctes α, $j\alpha$ et $j^2\alpha$ où j et j^2 sont les racines cubiques primitives de l'unité. Mais alors j est dans L et c'est une contradiction.

5.7 Corollaire. *Soit $P(X)=X^3-3X+1\in\mathbf{Q}[X]$ et $L=D_{\mathbf{Q}}(P)$. Alors l'extension $\mathbf{Q}\subset L$ est résoluble mais non radicale.*

Démonstration. Le discriminant de P est $\Delta=-4\times(-3)^3-27\times(1)^2=81$. Comme c'est un carré de $\mathbf{Q}$, l'extension est de degré 3 avec un groupe de Galois $\mathfrak{A}_3\simeq\mathbf{Z}/3\mathbf{Z}$. Elle est donc galoisienne et résoluble. De plus, les trois racines de P sont réelles en vertu de 5.5 et on a donc $L\subset\mathbf{R}$. La conclusion vient alors de 5.6.

5.8 *Remarque.* Comme une extension résoluble se plonge dans une extension radicale, cet exemple montre aussi qu'une extension contenue dans une extension radicale ne l'est pas nécessairement, question soulevée en 3.7.

6 Exemple 2 : l'équation de degré 4

6.1 Le cadre

On désigne par K un corps de caractéristique différente de 2 et 3 et par P un polynôme de degré 4 à coefficients dans K : $P(X)=X^4+rX^3+sX^2+pX+q$. On suppose que P est irréductible sur K, on pose $L=D_K(P)$ et on note x_1,x_2,x_3,x_4 les racines de P dans L. L'extension L/K est galoisienne (elle est normale comme corps de décomposition et séparable car P l'est en vertu de 9.8) et on pose $G=\mathrm{Gal}(L/K)$. On sait que G s'identifie à un sous-groupe de $\mathfrak{S}_4$ vu comme groupe de permutations des x_i.

Le but de ce qui suit est de préciser le degré $[L:K]$, la structure de G et de calculer les racines x_i par radicaux en fonction des coefficients.

6.1 *Remarques.* 1) Comme la caractéristique est différente de 2, on peut trouver un polynôme $Q(Y)$ sans terme en X^3 tel que $D_K(Q)=L$. Il suffit pour cela de faire le changement de variable $Y=X+\frac{r}{4}$.

2) En revanche, on ne peut pas toujours trouver un polynôme de la forme X^4+pX+q qui définisse L. En effet, si K est le corps des rationnels, une équation de la forme $Q(x)=x^4+px+q=0$ admet au plus deux racines

réelles, de sorte que $D_{\mathbf{Q}}(Q)$ ne peut être égal à $D_{\mathbf{Q}}(P)$ si P a 4 racines réelles. C'est le cas du polynôme (irréductible par Eisenstein) $P(X) = X^4 - 4X^2 + 2$.

Nous porterons néanmoins une attention particulière aux polynômes de la forme $X^4 + pX + q$.

6.2 *Remarque.* On sait, voir 10.4, que le groupe de Galois de L/K est contenu dans le groupe alterné $\mathfrak{A}_4$ si et seulement si le discriminant $\Delta(P)$ est un carré de K. On sait aussi, voir 10.9, que, si P est de la forme $X^4 + pX + q$ le discriminant vaut $\Delta(P) = 4^4q^3 - 3^3p^4 = 256q^3 - 27p^4$. Le lecteur courageux calculera Δ lorsque s, voire r, est non nul.

6.3 *Remarque.* Comme P est irréductible, les corps de rupture $K(x_i)$ sont de degré 4 sur K. Il en résulte que le degré de L est multiple de 4 et divise 24, donc peut valoir *a priori* $4, 8, 12$ ou 24. Cet entier est aussi le cardinal de G. Comme G est un sous-groupe de $\mathfrak{S}_4$ il peut être *a priori* isomorphe au groupe cyclique $\mathbf{Z}/4\mathbf{Z}$, au groupe de Klein $\mathbf{V}_4 \simeq \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$, au groupe diédral $\mathbf{D}_4$ d'ordre 8, au groupe alterné $\mathfrak{A}_4$ ou au groupe symétrique tout entier $\mathfrak{S}_4$. Nous verrons que tous ces cas sont possibles.

6.2 La résolvante

On identifie G à un sous-groupe de $\mathfrak{S}_4$ et on pose $H = G \cap \mathfrak{A}_4$ et $N = G \cap \mathbf{V}_4$. Rappelons que $\mathbf{V}_4$ est le sous-groupe de $\mathfrak{A}_4$ formé de l'identité et des trois doubles transpositions $(12)(34)$, $(13)(24)$ et $(14)(23)$. On a la proposition suivante :

6.4 Proposition. *1) Le corps fixe de G est égal à K.*

2) Le corps fixe de H est égal à $K(\sqrt{\Delta})$.

3) On note σ le cycle (123). Le corps fixe M de N contient les éléments $u_1 = x_1x_2 + x_3x_4$, $u_2 = \sigma(u_1) = x_2x_3 + x_1x_4$ et $u_3 = \sigma(u_2) = x_1x_3 + x_2x_4$.

Démonstration. Le premier point résulte du théorème de Galois et le second des propriétés du discriminant. Pour le troisième, on note que tout $g \in N$ fixe les u_i, soit qu'il fixe x_ix_j et x_kx_l, soit qu'il les échange.

6.5 *Remarques.* 1) Attention *a priori* rien n'assure que les permutations $(12)(34)$, (123), etc. correspondent effectivement à des éléments de G.

2) La théorie de Galois appliquée à la suite de sous-groupes $\{\mathrm{Id}\} \subset N \subset H \subset G$ donne la suite de sous-corps en sens inverse : $K = L^G \subset K(\sqrt{\Delta}) = L^H \subset M = L^N \subset L$.

6.6 Proposition. *On définit le polynôme $R(X) = (X - u_1)(X - u_2)(X - u_3) := X^3 + aX^2 + bX + c$ (la* **résolvante** *de Lagrange). Il est à coefficients* *dans K, précisément, c'est un polynôme en les coefficients r, s, p, q de P. Dans le cas $P(X) = X^4 + pX + q$ on a $R(X) = X^3 - 4qX - p^2$.*

Démonstration. Le groupe $\mathfrak{S}_4$ est engendré par $\mathbf{V}_4$, σ et $\tau = (12)$. Les éléments de $\mathbf{V}_4$ fixent les u_i, σ les permute circulairement et τ fixe u_1 et échange u_2 et u_3. Tous ces éléments fixent donc les coefficients de R qui sont des fonctions symétriques des u_i. On en déduit que R est dans $K[X]$ en vertu de 6.4.1 et, comme ses coefficients sont des polynômes symétriques en les x_i, ce sont des polynômes en les fonctions symétriques élémentaires, c'est-à-dire les coefficients de P. Pour calculer a, b, c, on note qu'on a $-a = u_1 + u_2 + u_3$, $b = u_2u_3 + u_3u_1 + u_1u_2$ et $c = -u_1u_2u_3$. On voit que a (resp. b, resp. c) est un polynôme homogène de degré 2 (resp. 4, resp. 6) en les x_i. Par ailleurs, r, s, p, q sont homogènes de degrés $1, 2, 3, 4$ en les x_i, de sorte que si r et s sont nuls, on voit que a est nul (on vérifie aussitôt qu'on a $a = -s$), puis que b est égal à βq et $c = \gamma p^2$. Pour calculer β et γ on spécialise le polynôme $X^4 + pX + q$ d'abord en $X^4 - X$. Les racines x_i sont alors $0, 1, j, j^2$ et les u_i sont $1, j$ et j^2, d'où $c = -1 = \gamma$. On spécialise ensuite P en $X^4 - 1$ de racines $1, -1, i, -i$ qui donnent $u_i = 0, -2i$ et $2i$, d'où $b = 4 = -\beta$ et on a le résultat.

6.7 *Exercice.* Calculer la résolvante dans le cas général en utilisant les fonctions symétriques. (On trouve $a = -s$, $b = pr - 4q$ et $c = -p^2 - qr^2 + 4qs$.)

On suppose désormais que P est de la forme $X^4 + pX + q$.

6.3 Le calcul des racines

Comme les u_i sont racines d'une équation de degré 3, la méthode de Cardan permet de les calculer par radicaux à partir des coefficients p et q. On en déduit les x_i comme suit.

Comme le coefficient r de X^3 dans P est nul on a $x_3+x_4 = -(x_1+x_2)$. Par ailleurs, on a aussi $s = 0$, c'est-à-dire $x_1x_2+x_3x_4+x_1x_3+x_1x_4+x_2x_3+x_2x_4 = 0$ ou encore $u_1+(x_1+x_2)(x_3+x_4) = 0$. On en déduit $u_1 = (x_1+x_2)^2 = (x_3+x_4)^2$ et, de même, $u_2 = (x_1 + x_4)^2 = (x_2 + x_3)^2$ et $u_3 = (x_1 + x_3)^2 = (x_2 + x_4)^2$.

Cela permet de calculer les x_i en fonction des u_i. On choisit l'une des racines carrées de u_1 et on impose $\sqrt{u_1} = x_1 + x_2$, puis on choisit une racine de u_2 et on impose $\sqrt{u_2} = x_1 + x_4$. Attention, le troisième choix, qui donne $\sqrt{u_3} = x_1 + x_3$, n'est pas libre. En effet, on a la formule :

$$(x_1+x_2)(x_1+x_4)(x_1+x_3) = x_1^2(x_1+x_2+x_3+x_4)+x_2x_3x_4+x_1x_3x_4+x_1x_2x_4+x_1x_2x_3 = -p$$

et $x_1 + x_3$ est connu si $x_1 + x_2$ et $x_1 + x_4$ sont fixés. On en déduit la valeur de x_1 :

$$\sqrt{u_1} + \sqrt{u_2} + \sqrt{u_3} = 3x_1 + x_2 + x_3 + x_4 = 2x_1$$

puis celle des autres x_i :

$$2x_2 = \sqrt{u_1} - \sqrt{u_2} - \sqrt{u_3},\ 2x_3 = -\sqrt{u_1} - \sqrt{u_2} + \sqrt{u_3},\ 2x_4 = -\sqrt{u_1} + \sqrt{u_2} - \sqrt{u_3}.$$

6.8 *Remarque.* On vérifie aussitôt que, dans le cas X^4+pX+q, on a $\Delta(P) = \Delta(R)$ en appliquant les formules donnant le discriminant en fonction des coefficients. On peut aussi le voir à partir des formules $u_1 = (x_1+x_2)^2$, $u_2 = (x_1+x_4)^2$ et $u_3 = (x_1+x_3)^2$ en montrant que $\delta_3 = (u_1-u_2)(u_1-u_3)(u_2-u_3)$ est égal à $-\delta_4$ avec $\delta_4 = (x_1-x_2)(x_1-x_3)(x_1-x_4)(x_2-x_3)(x_2-x_4)(x_3-x_4)$.

6.4 Le calcul du groupe de Galois

6.4.1 Le cas $[L : K] \geq 12$

6.9 Théorème. *Le groupe G contient le groupe $\mathfrak{A}_4$ si et seulement si R est irréductible sur K. Précisément, on a $G = \mathfrak{S}_4$ (resp. $\mathfrak{A}_4$) si et seulement si R est irréductible sur K et si Δ n'est pas un carré de K (resp. est un carré).*

Démonstration. Si R est irréductible, L, qui contient $K(x_i)$ et $K(u_i)$ est de degré multiple de 4 et de 3, donc de 12 et on a le résultat. Inversement, si R est réductible, une de ses racines, disons u_1, est dans K et les autres sont de degrés ≤ 2, avec $u_1+u_2+u_3 = 0$, de sorte que $K(u_1, u_2, u_3)$ est de degré ≤ 2 et, par les formules ci-dessus, L est engendré par $\sqrt{u_2}$ et $\sqrt{u_3}$, donc est de degré ≤ 8 sur K et G ne contient pas $\mathfrak{A}_4$.

6.10 *Remarque.* Un autre argument est le suivant. Si G contient $\mathfrak{A}_4$ et si R est réductible, on a, disons, $u_1 \in K$, mais, comme la permutation paire $\sigma = (123)$ est dans G, on a $\sigma(u_1) = u_2 = u_1$ et $\sigma(u_2) = u_3 = u_1$ car G fixe K. On a donc $u_1 = u_2 = u_3$ et, avec $u_1+u_2+u_3 = 0$, on en déduit $u_1 = u_2 = u_3 = 0$, donc $p = q = 0$ et P n'est pas irréductible, ce qui est absurde.

6.11 *Exemples.* On a $\mathrm{Gal}_{\mathbf{Q}}(X^4+X+1) = \mathfrak{S}_4$ et $\mathrm{Gal}_{\mathbf{Q}}(X^4-8X+12) = \mathfrak{A}_4$. En effet, dans le premier cas on a $R(X) = X^3-4X-1$ et ce polynôme est irréductible sur $\mathbf{Q}$ (sinon il aurait une racine rationnelle, et même entière car $\mathbf{Z}$ est intégralement clos, voir [7], et elle diviserait 1) et $\Delta(P) = 229$ n'est pas un carré. Dans le second cas[16] on a $R(X) = X^3-48X-64$ qui est irréductible sur $\mathbf{Q}$ (réduire modulo 5) et $\Delta(P) = 2^{12} \times 3^4 = (2^6 \times 3^2)^2$.

16. Le lecteur vérifiera que $X^4-8X+12$ est irréductible sur $\mathbf{Q}$.

6.4.2 Le cas du groupe $\mathbf{V}_4$

Un corollaire du théorème précédent fournit le cas du groupe de Klein :

6.12 Corollaire. *On a les équivalences :* $\mathrm{Gal}(P) \simeq \mathbf{V}_4 \iff$ *R admet une racine dans K et Δ est un carré de K^* $\iff$ R est scindé dans K.*

Démonstration. Montrons déjà l'équivalence des deux dernières propriétés, c'est-à-dire le lemme suivant :

6.13 Lemme. *Soit $R(X) = X^3 + aX^2 + bX + c \in K[X]$. Les propriétés suivantes sont équivalentes :*
1) R est scindé dans K,
2) R admet une racine dans K et son discriminant est un carré.

Démonstration. Si R est scindé, ses trois racines u_1, u_2, u_3 sont dans K et on a $\Delta(R) = \delta^2$ avec $\delta = (u_1 - u_2)(u_1 - u_3)(u_2 - u_3) \in K$, de sorte que Δ est un carré. Inversement, supposons que u_1 est dans K ainsi que δ. Alors, $u_2 + u_3 = -a - u_1$ est dans K, ainsi que $u_2 u_3 = -c/u_1$ (si u_1 est nul on conclut avec $b = u_2 u_3$). Or, on a $\delta = [u_1^2 - (u_2 + u_3)u_1 + u_2 u_3](u_2 - u_3)$. Le crochet est dans K et, s'il est non nul, on en déduit $u_2 - u_3 \in K$ puis $u_2, u_3 \in K$. Si le crochet $(u_1 - u_2)(u_2 - u_3)$ est nul c'est que u_2 ou u_3 est égale à u_1 donc est dans K et donc aussi la troisième racine.

Revenons à 6.12. Supposons d'abord R scindé. Alors le groupe de Galois est contenu dans $\mathfrak{A}_4$, de cardinal multiple de 4 et n'est pas égal à $\mathfrak{A}_4$ en vertu de 6.9, c'est donc $\mathbf{V}_4$. Inversement, si le groupe est $\mathbf{V}_4$, il est contenu dans le groupe alterné, donc $\Delta(P) = \Delta(R)$ est un carré et R n'est pas irréductible, donc admet une racine et on a la conclusion.

6.14 *Exemple.* Le polynôme cyclotomique $P(X) = X^4 + 1$ a pour groupe de Galois $\mathbf{V}_4$. En effet, $R(X) = X^3 - 4X = X(X-2)(X+2)$ est scindé. On peut aussi montrer qu'on a $\mathrm{Gal}_{\mathbf{Q}}(X^4 + 1) \simeq (\mathbf{Z}/8\mathbf{Z})^* \simeq \mathbf{V}_4$, voir 4.6.

6.4.3 Les cas des groupes $\mathbf{D}_4$ et $\mathbf{Z}/4\mathbf{Z}$

Lorsque R est réductible et que $\Delta(P)$ n'est pas un carré, le groupe de Galois est égal au groupe diédral $\mathbf{D}_4$ ou au groupe cyclique $\mathbf{Z}/4\mathbf{Z}$. Le théorème suivant distingue ces deux cas :

6.15 Théorème. *On suppose $P(X) = X^4 + pX + q \in K[X]$ irréductible et on suppose que R est réductible et que $\Delta(P)$ n'est pas un carré de K. En vertu de 6.13 le polynôme R admet une unique racine u_1 dans K. On a les cas suivants :*

1) $\mathrm{Gal}_K(P) \simeq \mathbf{Z}/4\mathbf{Z}$ *dans deux cas :*
a) Si $u_1 = 0$ *et si* K *contient une racine primitive* 4*-ième de l'unité.*
b) Si $4qu_1 - 3p^2$ *est un carré non nul de* K*.*
2) Dans tous les autres cas, on a $\mathrm{Gal}_K(P) \simeq \mathbf{D}_4$*.*

Démonstration. Supposons d'abord que le groupe de Galois est $\mathbf{Z}/4\mathbf{Z}$, de sorte que $[L : K] = 4$. En vertu des résultats précédents la résolvante admet une unique racine dans K, disons u_1, et le discriminant de P n'est pas un carré. La résolvante s'écrit $R(X) = (X-u_1)Q(X)$ avec $Q(X) = (X-u_2)(X-u_3)$ irréductible sur K. Comme le groupe de Galois a un unique sous-groupe d'ordre 2, il y a une unique extension intermédiaire de degré 2 qui est donc tout à la fois $K(u_2) = K(u_3) = K(\sqrt{\Delta(P)}) = K(\sqrt{\Delta(Q)})$. On commence par un petit résultat sur les extensions quadratiques :

6.16 Lemme. *Soit* K *un corps,* $d \in K$*, non carré, et soit* $M = K(\sqrt{d})$*. Un élément* x *de* K*, qui n'est pas un carré de* K*, est un carré de* M *si et seulement si* dx *est dans* $(K^*)^2$*.*

Démonstration. Si x est un carré de M on a $x = (a+b\sqrt{d})^2 = a^2+db^2+2ab\sqrt{d}$ et comme x est dans K, a ou b est nul. Si b est nul, $x = a^2$ est un carré de K et c'est exclu, donc $a = 0$ et $x = db^2$, donc $dx = d^2b^2$.

Revenons au théorème. On élimine déjà le cas où u_1 est un carré [17] de K :

6.17 Lemme. *Si* u_1 *est un carré de* K*, on a* $u_1 = 0$*,* $p = 0$ *et le groupe* $G = \mathrm{Gal}_K(X^4+q)$ *est le groupe* $\mathbf{D}_4$*, sauf si* K *contient une racine quatrième primitive de* 1*.*

Démonstration. On a $u_1 = x_1x_2 + x_3x_4 = (x_1 + x_2)^2 = (x_3 + x_4)^2$. Le groupe G étant $\mathbf{Z}/4\mathbf{Z}$ est engendré par un cycle g d'ordre 4 qui fixe u_1, ce qui impose $g = (1324)$ (ou son inverse). En effet, on vérifie que (1234) et (1243) transforment respectivement u_1 en u_2 et u_3. Si u_1 est un carré de K, sa racine $x_1 + x_2$ est dans K donc fixe par g, or on a $g(x_1 + x_2) = x_3 + x_4$, et, comme $x_1 + x_2 + x_3 + x_4 = 0$ on en déduit $x_1 + x_2 = 0$, donc $u_1 = 0$, donc $p = 0$ puisque u_1 est racine de $X^3 - 4qX - p^2$. On a donc $P(X) = X^4 + q$ et la conclusion vient de 4.11.

Revenons encore au théorème. Comme u_1 n'est pas un carré de K, $\sqrt{u_1} = x_1 + x_2$ est dans L et de degré 2 sur K et u_1 est un carré de $K(\sqrt{\Delta(Q)})$. Le lemme 6.16 montre que $v := u_1\Delta(Q)$ est un carré de K^*. Il reste à calculer v. On a $\Delta(Q) = (u_2 - u_3)^2 = (u_2 + u_3)^2 - 4u_2u_3$. Or, on a $u_1 + u_2 + u_3 = 0$ donc $(u_2 + u_3)^2 = u_1^2$ et $v = u_1^3 - 4u_1u_2u_3 = u_1^3 - 4p^2$ et, comme u_1 est racine

17. Merci à Ahmed Abbès de m'avoir aidé à éclaircir ce cas, jadis ...

de R, on a $u_1^3 = 4qu_1 + p^2$, donc $v = 4qu_1 - 3p^2$ et on obtient la condition annoncée.

Il reste à prouver la réciproque. Si $v = u_1\Delta(Q)$ est un carré, on voit que $\sqrt{u_1}$ est dans $K(u_2)$. Alors, on a $L = K(u_2)(\sqrt{u_2})$, ce qui prouve que L est de degré 4 et donc de groupe $\mathbf{Z}/4\mathbf{Z}$. En effet, vu le calcul des racines de P, L est engendré par les trois racines des u_i, mais on a vu qu'elles sont liées par la formule $\sqrt{u_1}\sqrt{u_2}\sqrt{u_3} = \pm p$, donc la racine de u_2 engendre L.

6.18 *Exemples.* 1) On a $\mathrm{Gal}_{\mathbf{Q}}(X^4 - 2) \simeq \mathbf{D}_4$.

2) On a $\mathrm{Gal}_{\mathbf{Q}}(X^4-8X+14) \simeq \mathbf{Z}/4\mathbf{Z}$. En effet, on a $R(X) = X^3-56X-64$ qui a l'unique racine rationnelle $u_1 = 8$ et $4qu_1 - 3p^2 = 256 = 16^2$.

6.19 *Exercice.* Déterminer les groupes de Galois sur $\mathbf{Q}$ des polynômes suivants :

$$4X^4 + 24X + 7 \quad X^4 + 3X + 10 \quad 9X^4 + 12X + 7 \quad 117X^4 + 38X + 37$$

$$31X^4 + 32X + 16 \quad X^4 + X + 2 \quad 36X^4 + 24X + 13 \quad 3X^4 + X + 5$$

$$100X^4 - 40X + 21 \quad 4X^4 - 72X + 117 \quad 7X^4 + 8X + 4 \quad X^4 + 17X + 3$$

$$7X^4 + 16X + 16 \quad 109X^4 + 128X + 64 \quad 49X^4 - 252X + 387.$$

6.20 *Remarque.* Pour une vision géométrique de la résolution d'une équation de degré 4 en termes d'intersection de deux coniques, on pourra consulter :
`https://www.math.u-psud.fr/~perrin/CAPES/algebre/Ferrari.pdf`

7 Un problème sur les équations de degré 5

Le but de ce problème est de calculer le groupe de Galois d'un polynôme de la forme $X^5 + pX + q$ et de donner notamment un exemple où ce groupe est le groupe diédral $\mathbf{D}_5$. On pourra consulter [7] pour des précisions sur la théorie des groupes. En particulier, on n'oubliera pas que $\mathfrak{A}_5$ est simple.

7.1 Le groupe $\mathbf{D}_5$

On note $\mathbf{D}_5$ le groupe des isométries d'un pentagone régulier, dont les sommets seront notés $1, 2, 3, 4, 5$ (dans l'ordre naturel sur le cercle circonscrit), de sorte que $\mathbf{D}_5$ s'identifie à un sous-groupe du groupe symétrique $\mathfrak{S}_5$.

1) Vérifier que $\mathbf{D}_5$ est engendré par les éléments $\rho = (12345)$ et $\tau = (25)(34)$ et qu'il est inclus dans le groupe alterné $\mathfrak{A}_5$.

2) Déterminer les orbites de $\mathbf{D}_5$ dans son action naturelle sur les couples (i, j) d'éléments distincts de $\{1, 2, 3, 4, 5\}$ et les décrire en termes géométriques.

3) Montrer que les permutations :

$$\sigma_0 = \mathrm{Id},\ \sigma_1 = (123),\ \sigma_2 = (234),\ \sigma_3 = (345),\ \sigma_4 = (451),\ \text{et } \sigma_5 = (512)$$

forment un système de représentants de $\mathfrak{A}_5/\mathbf{D}_5$.

4) Montrer que les seuls sous-groupes de $\mathfrak{A}_5$ contenant $\mathbf{D}_5$ sont $\mathbf{D}_5$ et $\mathfrak{A}_5$.

5) On pose $\alpha = (2354)$. Montrer que α normalise $\mathbf{D}_5$ (c'est-à-dire qu'on a $\alpha\mathbf{D}_5\alpha^{-1} = \mathbf{D}_5$) et que $\mathfrak{S}_5$ est engendré par $\mathbf{D}_5$, σ_1 et α.

7.2 La résolvante

Soit K un corps de caractéristique zéro, soit $P(X) = X^5 + rX^4 + sX^3 + tX^2 + pX + q$ un polynôme de degré 5 à coefficients dans K et soit $L = D_K(P)$ un corps de décomposition de P sur K, engendré par les racines $x_1, \dots, x_5$. On pose $\delta = \prod_{1 \leq i < j \leq 5} (x_i - x_j)$ et on rappelle que $\Delta = \delta^2$ est le discriminant de P. On pose :

$$u = (x_1x_2 + x_2x_3 + x_3x_4 + x_4x_5 + x_5x_1) - (x_1x_3 + x_2x_4 + x_3x_5 + x_4x_1 + x_5x_2)$$

et on appelle résolvante de P le polynôme $R(X) = \prod_{i=0}^{5}(X - \sigma_i(u))$ où les σ_i sont définis en 7.1.3 ci-dessus. On note enfin :

$$R(X) = X^6 + aX^5 + bX^4 + cX^3 + dX^2 + eX + f.$$

A) On suppose que les x_i sont des indéterminées. Le groupe $\mathfrak{S}_5$ opère sur $K(x_1, \dots, x_5)$ par permutation des x_i et les coefficients de P sont, au signe près, les polynômes symétriques élémentaires en les x_i. Si F est un polynôme en les x_i on dit que F est **alterné** si l'on a :

$$\forall \sigma \in \mathfrak{S}_5, \quad F(x_{\sigma(1)}, \dots, x_{\sigma(5)}) = \epsilon(\sigma) F(x_1, \dots, x_5).$$

1) Montrer que F est alterné si et seulement s'il s'écrit $F = \delta G$ où G est un polynôme symétrique.

2) Vérifier que u est invariant sous l'action de $\mathbf{D}_5$ et calculer $\alpha(u)$. Montrer que les coefficients a, c, e (resp. b, d, f) de $R(X)$ sont des polynômes alternés (resp. symétriques) en les x_i (utiliser la permutation α).

3) En déduire, par un argument de degré, que l'on a $a = c = 0$ et $e = E\delta$ avec $E \in \mathbf{Z}$. Préciser les degrés des monômes[18] du type $p^i q^j$ dans b, d, f.

18. Pour le calcul explicite des coefficients de R en fonction de ceux de P, voir J. Buhler, *Icosahedral Galois representations*, Springer Lecture Notes 654, pp. 98-99.

B) On suppose $P(X) = X^5 + pX + q$.

1) Montrer que l'on a $a = c = 0$, $e = E\delta$, $b = Bp$, $d = Dp^2$, $f = Fp^3$ avec $B, D, E, F \in K$, indépendants de p, q.

2) Calculer[19] u et les $\sigma_i(u)$ dans le cas particulier $P(X) = X^5 - X$ et en déduire qu'on a, dans le cas général de $P(X) = X^5 + pX + q$:

$$R(X) = X^6 - 20pX^4 + 240p^2X^2 - 32\delta X + 320p^3.$$

7.3 Calcul du groupe de Galois

A) Les notations sont celles du début de 7.2. On pose $G = \mathrm{Gal}(L/K)$.

1) On suppose P irréductible sur K et R irréductible sur $K(\delta)$. Montrer qu'on a $G = \mathfrak{S}_5$ ou $G = \mathfrak{A}_5$.

2) Inversement, on suppose que G contient $\mathfrak{A}_5$.

a) Montrer que P est irréductible sur K et que δ est non nul.

¶ b) Montrer que les $\sigma_i(u)$ sont tous distincts. (On raisonnera par l'absurde en montrant que, sinon, u serait stable par $\mathfrak{A}_5$, donc serait dans $K(\delta)$, puis qu'il serait nul et on trouvera une contradiction avec $R(X)$.)

c) Montrer que R est irréductible sur $K(\delta)$ (utiliser 9.15).

B) On suppose $K \subset \mathbf{R}$ et $P(X) = X^5 + pX + q$.

1) Montrer que le discriminant de P est $5^5q^4 + 4^4p^5$ (voir 10.9).

2) Montrer que P a des racines non réelles et en déduire que $|G|$ est pair.

3) On suppose que $P(X)$ est irréductible sur K et que Δ est un carré de K. Montrer que G est égal à $\mathfrak{A}_5$ ou à $\mathbf{D}_5$ et que $G = \mathbf{D}_5$ si et seulement si R admet une racine dans K (on se souviendra que u est racine de R).

7.4 Un exemple d'équation résoluble

1) Montrer que le groupe de Galois de $P(X) := X^5 - 5X + 12$ sur $\mathbf{Q}$ est égal à $\mathbf{D}_5$ (qui est donc résoluble).

2) On se propose de calculer par radicaux les racines de cette équation. Pour cela on pose $\zeta = e^{2i\pi/5}$. C'est une racine primitive cinquième de l'unité et on rappelle les formules $\zeta + \zeta^{-1} = \dfrac{-1+\sqrt{5}}{2}$ et $\zeta^2 + \zeta^{-2} = \dfrac{-1-\sqrt{5}}{2}$.

On suppose que x_1 est l'unique racine réelle de P et que les racines x_2, x_5 (resp. x_3, x_4) sont complexes conjuguées. On pose :

$$y_1 = x_1 + \zeta x_2 + \zeta^2 x_3 + \zeta^{-2} x_4 + \zeta^{-1} x_5, \quad y_4 = x_1 + \zeta^{-1} x_2 + \zeta^{-2} x_3 + \zeta^2 x_4 + \zeta x_5,$$

19. Le calcul est facile mais fastidieux. On trouve $u = \sigma_1(u) = \sigma_2(u) = \sigma_5(u) = -2i$, $\sigma_3(u) = 2 + 4i$ et $\sigma_4(u) = -2 + 4i$ et on a $\delta = -16i$.

$y_2 = x_1 + \zeta^2 x_2 + \zeta^{-1} x_3 + \zeta x_4 + \zeta^{-2} x_5, \quad y_3 = x_1 + \zeta^{-2} x_2 + \zeta x_3 + \zeta^{-1} x_4 + \zeta^2 x_5.$

a) Montrer que les y_i sont réels et qu'on a les formules $y_1 y_4 = -5\sqrt{5}$ et $y_2 y_3 = 5\sqrt{5}$ puis (¶¶¶) $y_1^5 + y_4^5 = 6250 - 2500\sqrt{5}$ et $y_2^5 + y_3^5 = 6250 + 2500\sqrt{5}$. (Un logiciel de calcul formel est bien utile ici.)

b) En déduire que y_1^5 et y_4^5 (resp. y_2^5 et y_3^5) sont racines de l'équation $Y^2 + (6250 - 2500\sqrt{5})Y - 5^7\sqrt{5} = 0$ (resp. $Y^2 + (6250 + 2500\sqrt{5})Y + 5^7\sqrt{5} = 0$) et calculer ces nombres.

c) Montrer qu'on a $5x_1 = y_1 + y_2 + y_3 + y_4$, $5x_2 = \zeta^{-1} y_1 + \zeta^{-2} y_2 + \zeta^2 y_3 + \zeta y_4$ et les formules analogues avec x_3, x_4, x_5 et en déduire les valeurs des racines de $X^5 - 5X + 12 = 0$.

8 L'équation générale de degré n

Dans ce paragraphe on aborde le cas de l'équation générale de degré n. Attention, il y a deux mots que l'on doit distinguer soigneusement : le mot générique fait référence à l'usage d'indéterminées, qu'elles soient au niveau des coefficients ou des racines. Le mot générale, au contraire, concerne des coefficients numériques décrivant une partie suffisamment grande de K^n. Bien entendu, on se doute qu'il y a un lien entre les deux.

8.1 L'équation générique de degré n

8.1.1 L'équation à coefficients génériques

8.1 Définition. *Soit K un corps et soient $A_1, \dots, A_n$ des indéterminées. On appelle* **équation de degré n à coefficients génériques** *l'équation $T^n + A_1 T^{n-1} + \cdots + A_{n-1} T + A_n = 0$.*

Cette équation peut être vue à coefficients dans $\mathbf{Z}[A_1, \dots, A_n]$ voire dans $k[A_1, \dots, A_n]$ où k désigne un corps quelconque. L'intérêt de l'équation générique est qu'on peut la "spécialiser" en donnant aux A_i des valeurs $a_i \in k$, en espérant que les propriétés vont se conserver dans cette opération.

8.1.2 L'équation à racines génériques

8.2 Définition. *Soit k un corps et soient $X_1, \dots, X_n$ des indéterminées. On appelle* **équation de degré n à racines génériques** *l'équation, à coefficients dans $k[X_1, \dots, X_n]$, $(T - X_1) \cdots (T - X_n) = 0$.*

En fait, l'équation à racines génériques est aussi à coefficients génériques (et on parlera désormais d'équation générique dans l'un ou l'autre cas) en vertu de la proposition suivante :

8.3 Proposition. *Les coefficients de l'équation à racines génériques sont, au signe près, les polynômes symétriques élémentaires en les X_i :*

$$\Sigma_1 = X_1 + \cdots + X_n, \ldots, \Sigma_k = \sum_{1 \leq i_1 < \cdots < i_k \leq n} X_{i_1} \cdots X_{i_k}, \ldots, \Sigma_n = X_1 \cdots X_n.$$

Précisément, on a la formule :

$$P(T) := (T-X_1)\cdots(T-X_n) = T^n - \Sigma_1 T^{n-1} + \cdots + (-1)^k \Sigma_k T^{n-k} + \cdots + (-1)^n \Sigma_n.$$

Si k est un corps quelconque, le sous-anneau $k[\Sigma_1, \ldots, \Sigma_n]$ de $k[X_1, \ldots, X_n]$ est isomorphe à $k[A_1, \ldots, A_n]$ où les A_i sont des indéterminées.

Démonstration. Le calcul des coefficients est classique, voir par exemple [4] Ch. V §9. Pour la dernière assertion on considère l'homomorphisme Φ : $R := k[A_1, \ldots, A_n] \to S := k[\Sigma_1, \ldots, \Sigma_n]$ qui à A_i associe Σ_i. Il s'agit de montrer qu'il est injectif. On raisonne par l'absurde. Soit $F \in R$ un polynôme non nul et supposons qu'on a $F(\Sigma_1, \ldots, \Sigma_n) = 0$. On peut supposer k infini (quitte à le plonger, par exemple, dans $k(T)$). On sait alors (voir par exemple [6] Ch. I, 2.4) qu'il existe $(a_1, \ldots, a_n) \in k^n$ tels que $F(a_1, \ldots, a_n)$ soit non nul. On considère le polynôme $G(T) = T^n - a_1 T^{n-1} + \cdots + (-1)^n a_n$. Soit $k' := D_k(G)$ un corps de décomposition de ce polynôme et soient $x_1, \ldots, x_n$ ses racines dans k'. On a $G(T) = (T - x_1) \cdots (T - x_n)$ ce qui montre qu'on a $\Sigma_k(x_1, \ldots, x_n) = a_k$. Mais alors, on a $F(a_1, \ldots, a_n) = F(\Sigma_1, \ldots, \Sigma_n)(x_1, \ldots, x_n) = 0$ et c'est une contradiction.

8.1.3 L'extension générique

Il s'agit de l'extension des corps de fractions rationnelles $K := k(\Sigma_1, \ldots, \Sigma_n) \subset L := k(X_1, \ldots, X_n)$. On a le théorème suivant :

8.4 Théorème. *L'extension $K := k(\Sigma_1, \ldots, \Sigma_n) \subset L := k(X_1, \ldots, X_n)$ est finie, galoisienne, de degré $n!$, on a $L = D_K(P)$ où $P(T) = (T-X_1)\cdots(T-X_n) = T^n - \Sigma_1 T^{n-1} + \cdots + (-1)^k \Sigma_k T^{n-k} + \cdots + (-1)^n \Sigma_n$ est le polynôme générique de degré n à coefficients dans k. Le groupe de Galois de L/K est le groupe symétrique $\mathfrak{S}_n$. Pour $n \geq 5$, l'équation générique de degré n n'est pas résoluble par radicaux.*

Démonstration. Le polynôme générique est dans $K[T]$. Comme les X_i sont racines de P, l'extension est algébrique et comme elle engendrée par un nombre fini d'éléments elle est finie. On a $L = D_K(P)$, de sorte que L/K est normale et elle est galoisienne car les racines X_i sont distinctes. On sait qu'alors le groupe de Galois est inclus dans $\mathfrak{S}_n$ et, ici, il contient $\mathfrak{S}_n$, car les permutations des X_i définissent des automorphismes de L qui, comme les polynômes Σ_k sont symétriques, laissent K invariant.

Comme le groupe symétrique est non résoluble pour $n \geq 5$, l'équation générique n'est donc pas résoluble par radicaux.

8.2 L'équation générale de degré n

8.2.1 Le théorème d'irréductibilité de Hilbert

On étudie d'abord un cas particulier dont la problématique est la suivante. On considère un polynôme en deux lettres $f(T, X) \in k[T, X]$ et on suppose qu'il est irréductible dans $k[T, X]$. La question est de savoir s'il le reste lorsqu'on spécialise la variable T en un scalaire $t \in k$. Le résultat dépend fondamentalement du corps sur lequel on travaille. Par exemple, si $f(T, X) = X^2 - T$, irréductible sur n'importe quel corps, si k est le corps $\mathbf{C}$ il ne reste irréductible en X pour aucune valeur de $t \in \mathbf{C}$. En revanche, si l'on a $k = \mathbf{Q}$, il reste irréductible pourvu que t ne soit pas un carré de $\mathbf{Q}$. Dans le cas de $\mathbf{Q}$, le théorème de Hilbert montre qu'il existe une infinité de valeurs de t telles que $f(t, X)$ reste irréductible si $f(T, X)$ l'est. Précisément, ces valeurs sont celles du complémentaire d'un ensemble (appelé parfois "mince"), dont la définition est trop technique pour être donnée ici [20].

En fait, le théorème vaut avec un nombre fini de variables $T_1, \dots, T_n$:

8.5 Théorème. (Hilbert) *Soit $P(T_1, \dots, T_n; X) \in \mathbf{Q}[T_1, \dots, T_n; X]$ un polynôme irréductible. Il existe une infinité de n-uplets $(t_1, \dots, t_n) \in \mathbf{Q}^n$ tels que $f(t_1, \dots, t_n; X)$ soit irréductible dans $\mathbf{Q}[X]$.*

On renvoie à [3] pour une démonstration.

8.2.2 Et ses conséquences

Le théorème d'irréductibilité permet de prouver le résultat attendu sur l'équation générale de degré n :

8.6 Corollaire. *Il y a une infinité de n-uplets $(a_1, \dots, a_n) \in \mathbf{Q}^n$ tels que le groupe $\mathrm{Gal}_{\mathbf{Q}}(T^n - a_1 T^{n-1} + \cdots + (-1)^{n-1} a_{n-1} T + (-1)^n a_n)$ soit égal au groupe symétrique $\mathfrak{S}_n$ (et donc tels que l'équation correspondante ne soit pas résoluble par radicaux si $n \geq 5$).*

20. Une idée trop simple serait de prendre pour parties minces les sous-ensembles algébriques de $\mathbf{Q}^n$, voir [6]. Cette définition est insuffisante, par exemple pour $n = 1$ les parties minces seraient seulement les ensembles finis, or on souhaite, par exemple, que les carrés forment une partie mince.

Démonstration. On considère l'extension générique $K := \mathbf{Q}(\Sigma_1, \dots, \Sigma_n) \subset L := \mathbf{Q}(X_1, \dots, X_n)$. On a vu en 8.4 que $L = D_K(P)$ avec $P(X) = X^n - \Sigma_1 X^{n-1} + \cdots + (-1)^n \Sigma_n = (X - X_1) \cdots (X - X_n)$ de sorte que L/K est galoisienne de degré $n!$ et de groupe de Galois $\mathfrak{S}_n$.

On considère un polynôme $A(X_1, \dots, X_n) = \alpha_1 X_1 + \cdots + \alpha_n X_n$ avec des $\alpha_i \in \mathbf{Q}$, tous distincts. Alors A est un générateur de K sur L. En effet, ses conjugués s'obtiennent en permutant les X_i et comme les α_i sont distincts, les $n!$ permutés le sont aussi, de sorte que A est de degré $n!$.

Soit $F(\Sigma_1, \dots, \Sigma_n)(X)$ le polynôme minimal de A sur K. Il est irréductible et on peut supposer qu'il est dans $\mathbf{Q}[\Sigma_1, \dots, \Sigma_n]$. En vertu du théorème d'irréductibilité de Hilbert 8.5, il existe une infinité de n-uplets de rationnels $(a_1, \dots, a_n)$ tels que $F(a_1, \dots, a_n)[X]$ soit encore irréductible sur $\mathbf{Q}$. On considère alors le corps de décomposition M sur $\mathbf{Q}$ de $Q(X) = X^n - a_1 X^{n-1} + \cdots + (-1)^n a_n$ et on note $x_1, \dots, x_n$ les racines de Q dans M. L'extension $M/\mathbf{Q}$ est galoisienne et, comme Q est de degré n, son groupe de Galois est un sous-groupe de $\mathfrak{S}_n$ et le degré de l'extension est $\leq n!$.

Soit Φ l'homomorphisme de $\mathbf{Q}[X_1, \dots, X_n]$ dans M qui à X_i associe x_i. L'image de Σ_i par Φ est égale à a_i car a_i est le i-ième polynôme symétrique en les x_i. Soit $\alpha = \alpha_1 x_1 + \cdots + \alpha_n x_n$ l'image de A, c'est un élément de L. Comme A vérifie $F(\Sigma_1, \dots, \Sigma_n)(A) = 0$, on a, par application de Φ, $F(a_1, \dots, a_n)(\alpha) = 0$ et comme le polynôme $F(a_1, \dots, a_n)[X]$ est irréductible sur $\mathbf{Q}$, c'est le polynôme minimal de α, qui est donc de degré $n!$. Cela montre que L est de degré $\geq n!$, mais on a vu qu'il est $\leq n!$, c'est donc exactement $n!$ et le groupe de Galois de Q est égal à $\mathfrak{S}_n$.

On déduit aussi de 8.5 le corollaire suivant, fondamental dans l'étude du problème inverse [21] de Galois (étant donné un groupe fini G existe-t-il un polynôme P à coefficients rationnels tel que $\mathrm{Gal}(P)$ soit isomorphe à G) :

8.7 Corollaire. *Soit $P_T(X) = X^n + a_{n-1} X^{n-1} + \cdots + a_0$ un polynôme à coefficients dans $K = \mathbf{Q}(T_1, \dots, T_r)$. On suppose P_T irréductible sur K. Alors, il existe une infinité de r-uplets $(t_1, \dots, t_r) \in \mathbf{Q}^r$, tels que le polynôme $P_t(X)$ obtenu en remplaçant T_i par t_i soit irréductible sur $\mathbf{Q}$ et que $\mathrm{Gal}_{\mathbf{Q}}(P_t)$ soit égal à $\mathrm{Gal}_K(P_T)$.*

La démonstration consiste encore essentiellement à préserver l'irréductibilité du polynôme minimal d'un l'élément primitif.

9 Annexe 1 : un peu de théorie de Galois

Cette annexe vise à rappeler le b-a ba de la théorie de Galois qui est utile,

21. Toujours ouvert à l'heure actuelle.

dans ce sujet et dans d'autres. On utilise les notations et les résultats de [7], notamment pour ce qui concerne les corps de décomposition. La rédaction ci-dessous est parfois sommaire. Le lecteur qui souhaiterait en savoir plus ira consulter l'excellent livre de Ian Stewart [9].

9.1 Introduction

La problématique de la théorie de Galois est la suivante. On a une extension finie[22] de corps $K \subset L$ et on s'intéresse aux extensions intermédiaires $K \subset M \subset L$. Il y a plusieurs raisons pour cela :

• Quand on étudie les constructions à la règle et au compas, on doit déterminer s'il existe une "tour" d'extensions $K = K_0 \subset K_1 \subset \cdots \subset K_n = L$ dans laquelle chaque extension intermédiaire est de degré 2.

• Quand on étudie la résolution par radicaux on cherche aussi de telles tours, mais avec des extensions intermédiaires de la forme $K_{i+1} = K_i(\alpha)$ avec $\alpha^r = a$ pour $a \in K_i$ (donc où $\alpha = \sqrt[r]{a}$ est un radical).

L'idée de la théorie de Galois est d'établir un **dictionnaire** entre ces extensions intermédiaires et les sous-groupes d'un groupe fini associé à l'extension initiale et appelé groupe de Galois. Bien entendu, cela repose sur l'idée que la situation est plus simple du côté des groupes que du côté des corps, ce qui est effectivement le cas.

9.2 Le groupe de Galois

9.1 Définition. *Soit $K \subset L$ une extension. Le groupe de Galois de l'extension est le groupe des automorphismes de corps de L qui induisent l'identité sur K. On le note* $\mathrm{Gal}(L/K)$. *Si $L = D_K(P)$ on note aussi* $\mathrm{Gal}(L/K) = \mathrm{Gal}(P)$.

Rappelons qu'un automorphisme de corps est une bijection qui conserve addition et multiplication. L'idée intuitive qu'il faut avoir est la suivante :

9.2 Proposition. *Soit $K \subset L$ une extension et soit $\alpha \in L$ un élément algébrique sur K qui annule le polynôme $P \in K[X]$. Alors, si σ est un élément de* $\mathrm{Gal}(L/K)$*, il envoie α sur une (autre) racine du polynôme P.*

Démonstration. On écrit $P(\alpha) = \alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0$, avec $a_i \in K$ et on applique σ. Comme il fixe K et que c'est un automorphisme, on a $\sigma(P(\alpha)) = \sigma(\alpha)^n + a_{n-1}\,\sigma(\alpha)^{n-1} + \cdots + a_1\,\sigma(\alpha) + a_0 = P(\sigma(\alpha)) = 0$.

22. Cela signifie que L est un K-espace vectoriel de dimension finie. Cette dimension s'appelle le degré de l'extension et on la note $[L : K]$

On voit que les éléments du groupe de Galois permutent les racines de P. Cela pose aussitôt deux questions :

• Les racines de P sont-elles toutes dans L ? (Autrement dit, P est-il scindé dans L ?)

• Ces racines sont-elles toutes distinctes ?

Ces questions conduisent à poser les définitions suivantes :

9.3 Définition. *Soit $K \subset L$ une extension finie.*

1) On dit que l'extension est **normale** *si pour tout polynôme irréductible $P \in K[X]$, si P a une racine dans L il est scindé sur L.*

2) On dit que l'extension est **séparable** *si pour tout polynôme irréductible $P \in K[X]$ admettant une racine dans L, ses racines (dans un corps de décomposition) sont toutes distinctes.*

3) On dit que l'extension est **galoisienne** *si elle est à la fois normale et séparable.*

9.4 *Remarques.* 1) La condition de normalité est essentielle. L'exemple type d'une extension non normale est $\mathbf{Q} \subset \mathbf{Q}(\sqrt[3]{2})$. En effet, le polynôme $X^3 - 2$ a une racine dans cette extension (réelle) mais pas les deux autres qui sont $j\sqrt[3]{2}$ et $j^2\sqrt[3]{2}$.

2) Cette condition peut sembler difficile à vérifier si on veut le faire pour tout polynôme. Heureusement, on a un critère très simple : une extension est normale si et seulement si c'est le corps de décomposition $D_K(P)$ d'un polynôme $P \in K[X]$, voir [9]. Autrement dit, il suffit de vérifier la condition pour un seul polynôme. Cela montre que $\mathbf{Q} \subset \mathbf{Q}(\sqrt[3]{2}, j) = D_{\mathbf{Q}}(X^3 - 2)$ est normale.

3) La condition de séparabilité est plus délicate, mais elle est automatique en caractéristique zéro ou sur un corps fini, voir ci-dessous.

9.3 Clôture normale

9.5 Proposition-Définition. *Soit $K \subset L$ une extension finie. Il existe une extension finie $K \subset L \subset M$ telle que M/K soit normale et minimale pour cette propriété (i.e., si $K \subset L \subset N$ avec N/K normale, M est isomorphe à un sous-corps de N). Cette extension est unique à un K-isomorphisme près. On dit que M/K est une* **clôture normale** *de L/K.*

Démonstration. On écrit $L = K(\alpha_1, \ldots, \alpha_n)$, on appelle P_i le polynôme minimal de α_i sur K, on pose $P = P_1 \cdots P_n$. Alors il est clair que $M = D_K(P)$ convient et l'unicité résulte de celle du corps de décomposition.

9.4 Séparabilité

9.6 Définition. *Soit $P \in K[X]$ un polynôme de degré n. On dit que P est* **séparable** *si ses n racines, dans un corps de décomposition de P, sont toutes distinctes. Sinon, on dit que P est inséparable.*

L'intérêt de cette notion est dans la proposition suivante, que nous admettrons (voir [9]) :

9.7 Proposition. *Soit K un corps, $P \in K[X]$ un polynôme séparable et $L = D_K(P)$. L'extension L/K est séparable (donc galoisienne). Inversement, toute extension galoisienne est de la forme $L = D_K(P)$ avec P séparable.*

La proposition suivante précise les polynômes séparables :

9.8 Proposition. *Soit $P \in K[X]$ un polynôme, $P = P_1^{\alpha_1} \cdots P_r^{\alpha_r}$ sa décomposition en produit d'irréductibles sur K.*

1) Le polynôme P est séparable si et seulement si les P_i le sont et si les exposants α_i sont tous égaux à 1.

2) Si P est irréductible, il est inséparable si et seulement si son polynôme dérivé P' est le polynôme nul.

3) En caractéristique 0 tout polynôme irréductible est séparable.

4) En caractéristique p, un polynôme irréductible non séparable est de la forme $P(X) = Q(X^p)$. Sur un corps fini, tout polynôme irréductible est séparable.

Démonstration. Le point 1) est clair car deux polynômes irréductibles distincts n'ont pas les mêmes racines.

2) Dire que P n'est pas séparable c'est dire qu'il a une racine double α qui est alors racine de P'. Le *pgcd* de P et P', soit δ, est alors divisible par $X - \alpha$, donc de degré > 0. Mais, comme P est irréductible, on a $\delta = P$, donc P divise P', et cela implique $P' = 0$ pour une raison de degré.

3) On écrit $P(X) = a_n X^n + \cdots + a_0$ avec $n > 0$ et $a_n \neq 0$. On a $P'(X) = na_n X^{n-1} + \cdots$ et ce polynôme n'est pas nul.

4) Il est clair que seuls les polynômes en X^p peuvent être inséparables puisque leur dérivée doit être le polynôme nul. Supposons K fini. Considérons un polynôme en X^p, $P(X) = a_n X^{np} + \cdots + a_1 X^p + a_0$ avec $a_i \in K$. Sur K, l'homomorphisme de Frobenius $x \mapsto x^p$ est surjectif, de sorte qu'il existe b_i tel que $a_i = b_i^p$. Mais alors, si on pose $Q(X) = b_n X^n + \cdots + b_0$, on a $P = Q^p$ (Frobenius encore !), et cela contredit l'irréductibilité de P.

9.9 Corollaire. *Si $K = \mathbf{F}_q$ et $L = \mathbf{F}_{q^n}$ sont des corps finis, l'extension $K \subset L$ est galoisienne.*

Démonstration. En effet, on a $L = D_K(X^{q^n} - X)$, de sorte que l'extension est normale et, comme K est fini, elle est séparable.

9.5 Le théorème de l'élément primitif

Le principal intérêt de la séparabilité réside dans le résultat suivant :

9.10 Théorème. (Théorème de l'élément primitif) *Soit $K \subset L$ une extension séparable. Alors, elle est monogène, autrement dit il existe $\alpha \in L$ tel que $L = K(\alpha)$.*

Par exemple, on vérifie qu'on a $\mathbf{Q}(\sqrt[3]{2}, j) = \mathbf{Q}(\sqrt[3]{2} + j)$. C'est d'ailleurs l'idée de la preuve du théorème, voir [9].

9.6 Le théorème de Galois

9.6.1 La correspondance de Galois

Soit $K \subset L$ une extension et $G = \mathrm{Gal}(L/K)$ son groupe de Galois. Notons $\mathcal{K}$ l'ensemble des extensions intermédiaires $K \subset M \subset L$ et $\mathcal{G}$ l'ensemble des sous-groupes de G. On a deux applications $\Phi : \mathcal{K} \to \mathcal{G}$ et $\Psi : \mathcal{G} \to \mathcal{K}$ définies comme suit.

L'application Φ est la plus naturelle. Elle associe à M le groupe de Galois de l'extension **du haut** $H = \mathrm{Gal}(L/M)$. C'est bien un sous-groupe de G (parmi les automorphismes de L fixant K on se limite à ceux qui fixent M). **Attention** en revanche $\mathrm{Gal}(M/K)$ **n'est pas** un sous-groupe de G, voir plus loin. On note que H fixe M et cela nous conduit au point suivant.

L'application Ψ associe à un sous-groupe H de G son **corps fixe** $M = L^H$:

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

9.11 *Remarques.* 1) Les applications Φ et Ψ sont décroissantes relativement à l'inclusion.

2) Le théorème de Galois affirme que, dans le cas galoisien, les applications Φ et Ψ sont réciproques l'une de l'autre. Ce qu'on peut dire d'emblée c'est que si M est dans $\mathcal{K}$ et H dans $\mathcal{G}$ on a $M \subset \Psi \circ \Phi(M)$ et $\Phi \circ \Psi(H) \supset H$.

9.6.2 Le théorème

9.12 Théorème. (Galois) *Soit $K \subset L$ une extension finie galoisienne et G son groupe de Galois. On reprend les notations ci-dessus.*

1) Le groupe G est fini et son cardinal est égal au degré n de l'extension.

2) Les applications Φ et Ψ sont des bijections décroissantes réciproques l'une de l'autre.

3) Si $K \subset M \subset L$ est une extension intermédiaire, les propriétés suivantes sont équivalentes :

i) L'extension $K \subset M$ est normale.
ii) Le sous-groupe $\mathrm{Gal}(L/M)$ *est distingué dans* G*.*
iii) Pour tout $\sigma \in G$ on a $\sigma(M) = M$.
De plus, on a alors un isomorphisme : $\mathrm{Gal}(M/K) \simeq \mathrm{Gal}(L/K)/\mathrm{Gal}(L/M)$.

Démonstration. Comme L/K est séparable, le théorème de l'élément primitif permet de l'écrire $L = K(\alpha)$, avec α de degré n, de polynôme minimal P.

1) Comme l'extension est normale, ce polynôme a n racines (distinctes) dans L : $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_n$ et on a une application de G dans l'ensemble des racines qui associe à σ la racine $\sigma(\alpha)$. Comme α est de degré n elle engendre L, de sorte que l'application est injective. Elle est aussi surjective : si α_i est une racine de P, il existe $\sigma \in G$ tel que $\sigma(\alpha) = \alpha_i$. C'est une conséquence de l'unicité du corps de rupture, voir [7] ou 9.14 ci-dessous.

2) Remarquons d'abord que si M est une extension intermédiaire, l'extension $M \subset L$ est galoisienne. En effet, si on a $L = D_K(P)$, avec P séparable, on a aussi $L = D_M(P)$.

Montrons alors que la composée $\Phi \circ \Psi$ est l'identité de $\mathcal{G}$. Soit H un sous-groupe et $M = L^H$ son corps fixe. On a $L = M(\alpha)$. Je dis que α est algébrique sur M de degré $\leq |H|$. En effet, α est racine du polynôme $Q(X) = \prod_{\sigma \in H} X - \sigma(\alpha)$ et on voit que ce polynôme est invariant sous H (les éléments de H permutent ses facteurs). Cela montre qu'on a $[L : M] \leq |H|$. Considérons alors $H' = \mathrm{Gal}(L/M)$. On a vu ci-dessus qu'il contient H. Mais on a vu aussi en 1) qu'on a $[L : M] = |H'| \geq |H|$. On en déduit $H = H'$ comme annoncé.

Le fait que $\Psi \circ \Phi$ soit l'identité de $\mathcal{K}$ en résulte facilement.

3) On montre l'équivalence de *ii)* et *iii)*, qui est facile, puis celle de *i)* et *iii)*. Pour cela on utilise encore le théorème de l'élément primitif en écrivant $M = K(\beta)$ avec Q comme polynôme minimal. Supposons $K \subset M$ normale. Si on a $\sigma \in G$, comme $\sigma(\beta)$ est une racine de Q, elle est dans M et M est stable. Inversement, si M est stable, les racines de Q sont dans M qui est donc égal à $D_K(Q)$, donc normale.

Enfin, l'isomorphisme s'obtient en restreignant les éléments de G à M (qui est stable). Cela donne un homomorphisme de $\mathrm{Gal}(L/K)$ dans $\mathrm{Gal}(M/K)$, dont le noyau est $\mathrm{Gal}(L/M)$ par définition. On a donc une injection

$$\mathrm{Gal}(L/K)/\mathrm{Gal}(L/M) \subset \mathrm{Gal}(M/K)$$

et c'est une bijection car les cardinaux sont égaux (par le point 1 du théorème de Galois et celui de la base télescopique, voir [7]).

Une conséquence importante du théorème est la suivante :

9.13 Corollaire. *Soit $K \subset L$ une extension galoisienne de groupe G. Le corps fixe de L sous G est égal à K.*

Démonstration. En effet, on a $\Phi(K) = G$, donc $\Psi(G) = L^G = K$.

9.6.3 Conjugués

Le théorème de Galois permet de préciser 9.1 et d'introduire la notion de conjugué :

9.14 Proposition-Définition. *Soit $K \subset L$ une extension galoisienne finie, $G = \mathrm{Gal}(L/K)$. Soient $\alpha, \beta \in L$. Les propriétés suivantes sont équivalentes :*
1) Les nombres α et β ont même polynôme minimal sur K.
2) Il existe $\sigma \in G$ tel que $\sigma(\alpha) = \beta$.
On dit alors que α et β sont **conjugués** *sur K.*

Démonstration. Seule l'implication $1 \Longrightarrow 2$ mérite une preuve. L'unicité du corps de rupture (voir [7]) fournit un isomorphisme de $K[\alpha]$ sur $K[\beta]$. Celle du corps de décomposition (*loc. cit.*) permet de le prolonger en un automorphisme de $D_K(P) = M$. Enfin, la surjectivité de la restriction $\mathrm{Gal}(L/K) \to \mathrm{Gal}(M/K)$ vue en 9.12 permet de conclure.

9.15 Corollaire. *Soit $K \subset L$ une extension galoisienne de groupe de Galois G et soit $P \in K[X]$, scindé dans L. Le groupe G opère transitivement sur les racines de P si et seulement si P est irréductible sur K.*

10 Annexe 2 : Discriminant

10.1 Définition et propriété caractéristique

10.1 Notations. Dans toute cette annexe on désigne par K un corps de caractéristique différente de 2, par P un polynôme de degré $n > 0$ à coefficients dans K et par L son corps de décomposition $L = D_K(P)$. On suppose que le polynôme P est séparable c'est-à-dire qu'il admet n racines distinctes dans L, que l'on note $x_1, \dots, x_n$. L'extension L/K est alors galoisienne et on note G son groupe de Galois, qui s'injecte dans le groupe symétrique $\mathfrak{S}_n$ par la formule : $g(x_i) = x_{\sigma_g(i)}$ (voir 9.2).

10.2 Proposition-Définition. *On pose* $\delta = \prod_{1 \le i < j \le n} (x_i - x_j)$ *et* $\Delta = \delta^2 = \prod_{1 \le i < j \le n} (x_i - x_j)^2$. *Le nombre*[23] Δ *est appelé* **discriminant** *du polynôme P.*

23. On le note $\Delta(P)$ lorsqu'on veut préciser de quel polynôme il est le discriminant.

Les nombres δ et Δ sont des éléments de L^* et on a la formule

$$\Delta = (-1)^{n(n-1)/2} \prod_{i \neq j} (x_i - x_j).$$

Le signe $(-1)^{n(n-1)/2}$ est égal à 1 si $n \equiv 0, 1 \pmod 4$ et à -1 sinon.

Démonstration. Il suffit de compter les signes $-$, donc les couples (i, j) avec $i > j$, il y en a bien $n(n-1)/2$.

10.3 *Remarque.* Attention, certains auteurs prennent $\Delta = \prod_{i \neq j} (x_i - x_j)$ comme définition du discriminant, mais la proposition suivante montre que c'est mal adapté à la théorie de Galois.

10.4 Proposition. *Soit g un élément de G et σ_g la permutation associée.*
1) On a $g(\delta) = \epsilon(\sigma_g)\delta$, où $\epsilon(\sigma_g)$ désigne la signature de σ_g, et $g(\Delta) = \Delta$.
2) Le discriminant Δ est dans K^* (et pas seulement dans L^*).
3) On a les équivalences :

$$\delta \in K^* \iff \Delta \in K^{*2} \iff G \subset \mathfrak{A}_n.$$

Démonstration. La formule avec δ résulte du comptage du nombre d'inversions[24] de σ_g et celle avec Δ est évidente. Le point 2) en résulte car K est le corps fixe de G, voir 9.13. Enfin, le point 3) résulte lui aussi de 1) : si G est formé de permutations paires, les éléments de G fixent δ et inversement.

10.5 *Exemple.* Calculons le discriminant du polynôme du second degré $ax^2 + bx + c$. Ses racines sont x_1 et x_2 et on a $\Delta = (x_1 - x_2)^2 = (x_1 + x_2)^2 - 4x_1x_2 = \big(-\frac{b}{a}\big)^2 - 4\frac{c}{a} = \frac{b^2 - 4ac}{a^2}\cdot$

10.2 Calcul du discriminant

10.6 Notations. On reprend les notations précédentes mais on suppose de plus que P est unitaire :

$$P(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0.$$

On suppose que la caractéristique du corps ne divise pas n. On considère le polynôme dérivé $P'(x)$ et on note $y_1, \ldots, y_{n-1}$ ses racines. On a donc :

$$P'(X) = nX^{n-1} + (n-1)a_{n-1}X^{n-2} + \cdots + a_1 = n \prod_{j=1}^{n-1} (X - y_j).$$

24. Voire de la définition de la signature que l'on peut donner par cette formule, vue dans l'anneau de polynômes $K[x_1, \ldots, x_n]$.

10.7 Théorème. *Soit Δ le discriminant de P. On a les formules :*

$$\Delta = (-1)^{n(n-1)/2} \prod_{i=1}^{n} P'(x_i) = (-1)^{n(n-1)/2} \prod_{i,j} (x_i - y_j) = (-1)^{n(n-1)/2} n^n \prod_{j=1}^{n-1} P(y_j).$$

Démonstration. On part de la formule $P(X) = \prod_{i=1}^{n} (X - x_i)$ que l'on dérive :

$$P'(X) = \sum_{i=1}^{n} (X - x_1) \cdots (\widehat{X - x_i}) \cdots (X - x_n)$$

où le chapeau signifie que le terme correspondant est omis. On calcule alors $P'(x_i)$. Tous les termes de la somme sont nuls sauf celui où l'on a omis x_i et on a donc, pour i fixé, $P'(x_i) = \prod_{j, j \neq i} (x_i - x_j)$. On en déduit la valeur du produit $\prod_{i=1}^{n} P'(x_i) = \prod_{i,j,\, j \neq i} (x_i - x_j)$ et la première formule vient de 10.2. En utilisant l'expression de P' en fonction de ses racines, on a $P'(x_i) = n \prod_{j=1}^{n-1} (x_i - y_j)$ d'où $\prod_{i=1}^{n} P'(x_i) = n^n \prod_{i,j} (x_i - y_j)$ et la seconde formule. Mais on a aussi $P(y_j) = \prod_{i=1}^{n} (y_j - x_i)$ et donc $\prod_{j=1}^{n-1} P(y_j) = \prod_{i,j} (y_j - x_i)$. Par rapport à l'expression précédente, chaque terme $x_i - y_j$ est changé de signe, ce qui fait $n(n-1)$ changements. Comme ce nombre est pair, le signe est le même et on a bien la troisième formule.

Ces formules permettent de calculer le discriminant du polynôme du troisième degré :

10.8 Proposition. *Le discriminant de $P(X) = X^3 + pX + q$ est $\Delta = -4p^3 - 27q^2$.*

Démonstration. On calcule $P'(X) = 3X^2 + p$ dont les racines sont $y_j = \pm\sqrt{-\dfrac{p}{3}}$, $j = 1, 2$, et on vérifie que le produit $P(y_1)P(y_2)$ vaut $A = \dfrac{27q^2 + 4p^3}{27}$. On a alors $\Delta = -27A$ et le résultat.

10.9 *Exercice.* Montrer que le discriminant de $P(X) = X^n + pX + q$ est donné par la formule :

$$\Delta = (-1)^{n(n-1)/2} \big(n^n q^{n-1} + (-1)^{n-1} (n-1)^{n-1} p^n \big).$$

Références

[1] Bourbaki Nicolas, *Éléments d'histoire des mathématiques*, Hermann, 1969.

[2] Dahan-Dalmedico A., Peiffer J. *Une histoire des mathématiques*, Le Seuil, coll. Points, 1986.

[3] Hadlock C.-R., *Field theory and its classical problems*, The Carus Mathematical Monographs, 19, 1978.

[4] Lang Serge, *Algebra*, Addison-Wesley, 1965.

[5] Osada Hiroyuki, *The Galois Groups of the Polynomial* $X^n + aX^l + b$, Journal of Number Theory **25**, 230-238 (1987).

[6] Perrin Daniel, *Introduction à la géométrie algébrique*, Interéditions, 1995.

[7] Perrin Daniel, *Cours d'algèbre*, Ellipses, 1996.

[8] Selmer Ernst S., *On the irreducibility of certain trinomials*, Math. Scand. **4**, 287-302 (1956).

[9] Stewart Ian, *Galois theory*, Chapmann-Hall, 1973.