Chapitre 5
Retour aux équations

Sommaire

1 Introduction **1**

2 La résolubilité des équations par radicaux **2**
2.1 La condition nécessaire 2
2.2 Les extensions cycliques de Kummer 4
2.3 Résolution des équations de degré 3 6
2.4 La condition suffisante 7
2.5 Une autre vue sur la condition suffisante 8

3 Variations sur le même thème **9**
3.1 Constructibilité à la règle et au compas (II) 9
3.2 Le casus irreducibilis 11
3.3 Les équations résolubles de degré premier 13

1 Introduction

On revient dans ce chapitre au point de départ, la théorie des équations algébriques. Le résultat essentiel est la caractérisation des équations résolubles par radicaux en termes de groupe de Galois.

On considère un corps $\mathbb{K}$ et une clôture algébrique Ω de $\mathbb{K}$. Sans nuire à la généralité, nous supposons, comme d'habitude, que toutes les extensions finies de $\mathbb{K}$ considérées sont contenues dans Ω.

Rappels

Si $\mathbb{L}$ est un sous-corps de Ω extension finie de $\mathbb{K}$, on dit que $\mathbb{L}/\mathbb{K}$ est *résoluble par radicaux* s'il existe $m \in \mathbb{N}^*$, $\alpha_1, \ldots, \alpha_m$ dans Ω, $n_1, \ldots, n_m$ dans $\mathbb{N}^*$ tels que :

$$(1) \qquad \mathbb{L} \subset \mathbb{K}(\alpha_1, \ldots, \alpha_m),$$

$$(2) \qquad \forall i \in \{1, \ldots, m\}, \quad a_i = {\alpha_i}^{n_i} \in \mathbb{K}(\alpha_1, \ldots, \alpha_{i-1})\ [1].$$

Deux propriétés sont immédiates.

- Toute extension de $\mathbb{K}$ contenue dans une extension résoluble par radicaux est résoluble par radicaux.

1. En convenant bien sûr que, pour $i = 1$, ceci signifie : $\alpha_1^{n_1} \in \mathbb{K}$.

- Une composée d'extension résolubles par radicaux est résoluble par radicaux.

D'autre part, l'équation algébrique $P(x) = 0$ à coefficients dans $\mathbb{K}$ est résoluble par radicaux si ses racines appartiennent à une extension de $\mathbb{K}$ résoluble par radicaux, c'est-à-dire si l'extension $D_{\mathbb{K}}P/\mathbb{K}$ est résoluble par radicaux.

Nous utiliserons largement les résultats du chapitre **4** : correspondance de Galois, théorème des « irrationalités naturelles », caractère galoisien d'une composée d'extensions galoisiennes, ainsi que les deux résultats suivants, qui sont les « briques de base » des extensions résolubles par radicaux et que nous énonçons à nouveau pour la commodité du lecteur [2].

Lemme 1. *Si $\mathbb{K}$ est de caractéristique nulle, si $X^n - 1$ est scindé sur $\mathbb{K}$ et si a est un élément de $\mathbb{K}$, alors l'extension $D_{\mathbb{K}}(X^n - a)/\mathbb{K}$ est cyclique de degré divisant n.*

Précisément, si α est une racine de $X^n - a$ dans Ω, l'application

$$\sigma \in Gal(D_{\mathbb{K}}(X^n - a)/\mathbb{K}) \longmapsto \frac{\sigma(\alpha)}{\alpha}$$

est un morphisme injectif de $Gal(D_{\mathbb{K}}(X^n - a)/\mathbb{K})$ dans le groupe $\mathbb{U}_n(\mathbb{K})$ des racines n-ièmes de 1 dans $\mathbb{K}$.

Lemme 2. *Si $\mathbb{K}$ est de caractéristique nulle, l'extension $D_{\mathbb{K}}(X^n - 1)/\mathbb{K}$ est abélienne.*

Précisément, si ε est une racine primitive n-ième de 1 dans Ω, et si σ est dans $Gal(D_{\mathbb{K}}(X^n - 1)/\mathbb{K})$, notons $k(\sigma)$ la classe modulo n de tout k tel que $\sigma(\varepsilon) = \varepsilon^k$. Alors

$$\sigma \longmapsto k(\sigma)$$

est un morphisme injectif de $Gal(D_{\mathbb{K}}(X^n - 1)/\mathbb{K})$ dans $\mathbb{Z}/n\mathbb{Z}^*$.

Dans la section **1**, on caractérise la résolubilité par radicaux en termes de groupe de Galois. La section **2** est consacrée à quelques compléments : équations de degré premier, constructibilité à la règle et au compas, casus irreducibilis.

2 La résolubilité des équations par radicaux

2.1 La condition nécessaire

Le coeur de ce paragraphe est le résultat suivant. Sa démonstration, qui conduit à considérer les groupes que l'on peut obtenir par extensions successives à partir des groupes abéliens, est à l'origine de la notion de groupe résoluble.

Théorème 1. *Soit $\mathbb{L}/\mathbb{K}$ une extension finie, résoluble par radicaux. Alors le groupe*

$$Gal(\mathit{Clnorm}_{\mathbb{K}}(\mathbb{L}/\mathbb{K})$$

est résoluble [3].

2. Le lemme 1 fait usage du caractère cyclique du groupe $\mathbb{U}_n(\mathbb{K})$ (chapitre 1, **3.1**, théorème 3).

3. Une conséquence est que, dès qu'une racine d'une équation algébrique est contenue dans une extension résoluble par radicaux, il en est de même de toutes les autres.

Preuve. On adopte les notations de l'introduction et on note $\mathbb{L}' = \mathrm{Clnorm}_{\mathbb{K}}\mathbb{L}$. La preuve est presque évidente dès lors que l'inclusion de $\mathbb{L}$ dans $\mathbb{K}(a_1, \ldots, a_m)$ est une égalité, $\mathbb{L}/\mathbb{K}$ est normale, et $\mathbb{K}$ contient assez de racines de 1. On va se ramener à ce cas.

Étape 1. Réduction au cas d'une extension normale, engendrée par radicaux successifs, dont le corps de base contient suffisamment de racines de l'unité. Posons

$$\mathbb{M} = \mathbb{K}(\alpha_1, \ldots, \alpha_m), \qquad \mathbb{M}' = \mathrm{Clnorm}_{\mathbb{K}}\mathbb{M}.$$

L'extension $\mathbb{M}/\mathbb{K}$ est résoluble par radicaux. Pour σ dans $\mathrm{Hom}_{\mathbb{K}}(\mathbb{M}, \Omega)$, on a :

$$\sigma(\mathbb{M}) = \mathbb{K}(\sigma(\alpha_1), \ldots, \sigma(\alpha_m)).$$

Il en résulte que l'extension $\mathbb{M}'/\mathbb{K}$, composée d'extension résoluble par radicaux, est résoluble par radicaux. Il existe donc r dans $\mathbb{N}^*$, $\beta_1, \ldots, \beta_r$ dans Ω, $n_1, \ldots, n_r$ dans $\mathbb{N}^*$ tels que :

- $\mathbb{M}' = \mathbb{K}(\beta_1, \ldots, \beta_r)$,
- pour i dans $\{2, \ldots, r-1\}$, $\beta_i^{n_i} \in \mathbb{K}(\beta_1, \ldots, \beta_{i-1})$.

Mais $\mathrm{Gal}(\mathbb{L}'/\mathbb{K})$ est un quotient de $\mathrm{Gal}(\mathbb{M}'/\mathbb{K})$. Il suffit donc de montrer que $\mathrm{Gal}(\mathbb{M}'/\mathbb{K})$ est résoluble.

Soient maintenant n le ppcm des n_i, ε une racine primitive n-ième de 1 dans Ω. Comme composée de deux extensions galoisiennes $\mathbb{M}'/\mathbb{K}$ et $\mathbb{K}(\varepsilon)/\mathbb{K}$, l'extension $\mathbb{M}'(\varepsilon)/\mathbb{K}$ est galoisienne. Le groupe $\mathrm{Gal}(\mathbb{M}'/\mathbb{K})$ est un quotient de $\mathrm{Gal}(\mathbb{M}'(\varepsilon)/\mathbb{K})$. Il suffit donc de montrer que $\mathrm{Gal}(\mathbb{M}'(\varepsilon)/\mathbb{K})$ est résoluble.

L'extension $\mathbb{K}(\varepsilon)/\mathbb{K}$ étant galoisienne, $\mathrm{Gal}(\mathbb{M}'(\varepsilon)/\mathbb{K}(\varepsilon))$ est un sous-groupe normal de $\mathrm{Gal}(\mathbb{M}'(\varepsilon)/\mathbb{K})$; d'autre part, le quotient

$$\mathrm{Gal}(\mathbb{M}'(\varepsilon)/\mathbb{K})/\mathrm{Gal}(\mathbb{M}'(\varepsilon)/\mathbb{K}(\varepsilon))$$

est cyclique car isomorphe à $\mathrm{Gal}(\mathbb{K}(\varepsilon)/\mathbb{K})$. On est ainsi ramené à montrer que le groupe Gal $(\mathbb{M}'(\varepsilon)/\mathbb{K}(\varepsilon))$ est résoluble.

Le diagramme ci-après permet de visualiser la démonstration.

$$\begin{array}{ccccc}
\mathbb{K} & \to & \mathbb{L} & \to & \mathbb{L}' \\
| & & \downarrow & & \downarrow \\
| & & \mathbb{M} & \to & \mathbb{M}' \\
\downarrow & & \downarrow & & \downarrow \\
\mathbb{K}(\varepsilon) & \to & \mathbb{M}(\varepsilon) & \to & \mathbb{M}'(\varepsilon)
\end{array}$$

Étape 2. Fin de la démonstration. Avec les notations de l'étape 1, posons :

$$\mathbb{K}_0 = \mathbb{K}(\varepsilon), \quad \mathbb{K}_1 = \mathbb{K}(\varepsilon, \beta_1), \quad \ldots \quad \mathbb{K}_r = \mathbb{K}(\varepsilon, \beta_1, \ldots, \beta_r) = \mathbb{M}'(\varepsilon).$$

Comme $\mathbb{K}_r/\mathbb{K}_0$ est galoisienne, les extensions $\mathbb{K}_r/\mathbb{K}_i$ pour $0 \leq i \leq r-1$ le sont aussi. Pour i dans $\{0, \ldots, r-1\}$, l'extension est abélienne. Une récurrence descendante évidente montre que, pour tout i de $\{1, \ldots, r\}$, le groupe $\mathrm{Gal}(\mathbb{K}_r/\mathbb{K}_i)$ est résoluble. L'application à $i = 0$ démontre le théorème.

Exemples

1. *L'équation générale de degré n*

   Puisque Gal $(\mathbb{K}_X/\mathbb{K}_\Sigma)$ est isomorphe à $\mathcal{S}_n$, non résoluble si $n \geq 5$, un corollaire du théorème est la « non-résolubilité par radicaux de l'équation générale de degré 5 ». Il mérite d'être énoncé.

   Proposition 1. *L'extension $\mathbb{K}_X/\mathbb{K}_\Sigma$ n'est pas résoluble par radicaux pour $n \geq 5$.*

   Lagrange est sans doute le premier mathématicien à avoir considéré ce résultat comme plausible. Ruffini en a publié plusieurs démonstrations réputées incomplètes, mais montrant en substance que l'équation générale de degré 5 ne peut être « ramenée » à des équations de degrés strictement plus petits. La première preuve considérée comme satisfaisante, basée sur les idées de Ruffini, est celle d'Abel ; la proposition est d'ailleurs souvent nommée « théorème d'Abel-Ruffini ».

2. *Une classe d'équations numériques non résolubles par radicaux*

   L'exemple 8 du chapitre 4 (**4.1**) fournit, à travers la proposition suivante, une classe d'équations numériques non résolubles par radicaux.

   Proposition 2. *Soient $\mathbb{K}$ un sous-corps de $\mathbb{R}$, p un nombre premier, et $P \in \mathbb{K}[X]$ irréductible sur $\mathbb{K}$ de degré p. Si P admet exactement deux racines non réelles, $Gal_{\mathbb{K}}P$ est isomorphe à $\mathcal{S}_p$. En particulier, si $p \geq 5$, l'équation $P(x) = 0$ n'est pas résoluble par radicaux.*

L'exercice ci-après montre qu'en caractéristique p, il existe des extensions à groupe résoluble qui ne sont pas de la forme décrite dans le théorème 1.

Exercice 1. ④ *Soient p un nombre premier, $\mathbb{K}$ un corps de caractéristique p. On dit que l'extension $\mathbb{L}/\mathbb{K}$ est résoluble par p-radicaux s'il existe r dans $\mathbb{N}^*$ et $\alpha_1, \ldots, \alpha_r$ dans Ω tels que :*

i) $\mathbb{L} \subset \mathbb{K}(\alpha_1, \ldots, \alpha_r)$,

ii) Pour $1 \leq i \leq r$, de deux choses l'une :

- soit il existe $n_i \in \mathbb{N}^*$ tel que $a_i = \alpha_i^{n_i} \in \mathbb{K}(\alpha_1, \ldots, \alpha_{i-1})$,

- soit $\alpha_i^p - \alpha_i \in \mathbb{K}(\alpha_1, \ldots, \alpha_{i-1})$.

Supposons $\mathbb{L}/\mathbb{K}$ séparable finie et résoluble par p-radicaux. Montrer que le groupe $Gal(Clnorm_{\mathbb{K}}\mathbb{L}/\mathbb{K})$ est résoluble.

2.2 Les extensions cycliques de Kummer

Comment démontrer la réciproque du théorème 1 ? Comme les groupes résolubles sont ceux que l'on peut obtenir par extensions successives à partir des groupes cycliques, il est naturel d'étudier en premier lieu les extensions cycliques. D'autre part, il n'est pas restrictif, lorsqu'on étudie la résolubilité par radicaux, de supposer que $\mathbb{K}$ contient les racines de 1. Le résultat essentiel de ce paragraphe est de montrer que, sous ces hypothèses, les extensions cycliques de $\mathbb{K}$ sont alors des corps de décomposition de binômes. Précisément, on dispose du résultat ci-après, qui donne une réciproque au lemme 1 [4].

4. Les extensions ainsi obtenues sont dites *de Kummer*. Nous verrons dans le paragraphe suivant que Lagrange avait, en substance, compris cette situation.

Théorème 2. *Soit n dans $\mathbb{N}^*$. On suppose que $|\mathbb{U}_n(\mathbb{K})| = n$.*[5] *Soit $\mathbb{L}/\mathbb{K}$ une extension finie. Les deux assertions suivantes sont équivalentes.*

i) Il existe $a \in \mathbb{K}$ tel que $X^n - a$ soit irréductible sur $\mathbb{K}$, et que l'on ait :

$$\mathbb{L} = D_{\mathbb{K}}(X^n - a).$$

ii) L'extension $\mathbb{L}/\mathbb{K}$ est cyclique de degré n.

Preuve. L'implication *i)* $\Rightarrow$ *ii)* a été vue dans le chapitre 4. Supposons *ii)* vérifié. Soit σ un générateur de $\mathrm{Gal}(\mathbb{L}/\mathbb{K})$.

Étape 1. Où l'on se ramène à trouver un élément α de $\mathbb{L}^*$ tel que $\sigma(\alpha)$ soit de la forme $\varepsilon\alpha$ avec ε racine n-ième primitive de 1.

Soit α un élément de $\mathbb{L}^*$ tel que $a = \alpha^n$ soit dans $\mathbb{K}$. Il existe alors ε dans $U_n(\mathbb{K})$ tel que $\sigma(\alpha) = \varepsilon\alpha$. L'ensemble des $\mathbb{K}$-conjugués de α est l'ensemble

$$\{\tau(\alpha)\ ;\ \tau \in <\sigma>\} = \{\mu\alpha\ ;\ \mu \in <\varepsilon>\}\,.$$

Dire que $\mathbb{K}(\alpha) = \mathbb{L}$, c'est dire que α est de degré n sur $\mathbb{K}$, donc que ε engendre le groupe $U_n(\mathbb{K})$.

Si ε est un générateur de $\mathbb{U}_n(\mathbb{K})$ et α un élément de $\mathbb{L}^*$ tel que

$$\sigma(\alpha) = \varepsilon\alpha,$$

alors $\alpha^n = a$ est fixe par $\mathrm{Gal}(\mathbb{L}/\mathbb{K})$ donc dans $\mathbb{K}$; d'autre part, l'argumentation précédente montre que $\mathbb{K}(\alpha) = \mathbb{L}$.

Étape 2. Existence de α.

Les morphismes $\mathrm{id}\ , \sigma, \ldots, \sigma^{n-1}$ sont $\mathbb{K}$-linéairement indépendants (indépendance des morphismes). De ceci et de l'égalité : $\sigma^n = \mathrm{id}$, on déduit que le polynôme minimal de σ (vu comme $\mathbb{K}$-endomorphisme de $\mathbb{L}$) est $X^n - 1$, donc que σ a pour spectre $U_n(\mathbb{K})$.

Formulation élémentaire de l'argument, choix « explicite » de α.

Soit

$$P = \frac{X^n - 1}{X - \varepsilon}.$$

On a $P = X^{n-1} + \varepsilon X^{n-2} + \cdots + \varepsilon^{n-1}$, d'où :

$$0 = \sigma^n - \mathrm{id}\ = (\sigma - \varepsilon\mathrm{id}\ ) \circ P(\sigma).$$

Tout élément non nul de $\mathrm{Im}\ P(\sigma)$ est un vecteur propre de σ associé à ε. Par indépendance des morphismes, on dispose de $x \in \mathbb{L}$ tel que $P(\sigma)(x) \neq 0$. On pose alors :

$$\alpha = P_\sigma(x).$$

On dit que α est une *résolvante de Lagrange de* $\mathbb{L}/\mathbb{K}$.

Exercice 2. ③ *Les notations sont celles du théorème précédent et de sa démonstration. Décrire les sous-extensions de $\mathbb{L}/\mathbb{K}$ au moyen de α.*

5. Rappelons (chapitre 1, proposition 6, **3.1**) que tel est le cas si et seulement si la caractéristique de $\mathbb{K}$ ne divise pas n et $\mathbb{K}$ contient les racines n-ièmes de 1 dans Ω.

Exercice 3. ④ *Les hypothèses sont celles du théorème 2, on note G le groupe $Gal(\mathbb{L}/\mathbb{K})$. On se propose de décrire les éléments x de $\mathbb{L}$ tels que $x^n \in \mathbb{K}$.*

a) Montrer, si $\chi \in Hom(G, \mu_n)$ et $x \in \mathbb{L}$, que la puissance n-ième de $\sum_{g\in G} \chi(g)g(x)$ est dans $\mathbb{K}$.

b) À l'aide du (cas cyclique du) théorème de la base normale, montrer qu'un élément y de $\mathbb{L}$ tel que $y^n \in K$ est de la forme $\sum_{g\in G} \chi(g)g(x)$ avec $x \in \mathbb{L}$.

Sur le modèle du théorème 2, on peut caractériser les extensions cycliques de degré p d'un corps de caractéristique p ; ce résultat est dû à Artin et Schreier.

Exercice 4. ⑤ *Soient p un nombre premier, $\mathbb{K}$ un corps de caractéristique p, $\mathbb{L}$ une extension galoisienne de degré p de $\mathbb{K}$. Montrer qu'il existe $a \in \mathbb{K}$ et $\alpha \in \mathbb{L}$ tels que :*

i) le polynôme $X^p - X - a$ est irréductible sur $\mathbb{K}$;

ii) l'élément α est racine de $X^p - X - a$;

iii) on a $\mathbb{L} = \mathbb{K}(\alpha)$.

2.3 Résolution des équations de degré 3

Illustrons la démonstration du théorème 2 en expliquant comment les résolvantes de Lagrange permettent de résoudre les équations de degré 3. On suppose ici que $\mathbb{K}$ est de caractéristique nulle, on considère un élément

$$P = X^3 + pX + q$$

de $\mathbb{K}[X]$, on note $\Delta(P) = -4p^3 - 27q^2$ le discriminant de P.

Cherchons à exprimer les racines x_1, x_2, x_3 de P dans Ω en fonction de p et q au moyen de radicaux. Conformément à la théorie générale, on adjoint à $\mathbb{K}$ les racines cubiques de l'unité ; on note j une racine cubique primitive de 1 :

$$j = -1/2 + \sqrt{-3}/2,$$

où $\sqrt{-3}$ est un élément de Ω de carré -3. Le calcul présenté après la démonstration du théorème 2 montre que $x_1 + jx_2 + j^2x_3$ et $x_1 + j^2x_2 + jx_3$ ont leur cube dans $K(\sqrt{\Delta(P)})$. Des calculs faciles fournissent :

$$(x_1 + jx_2 + j^2x_3)^3 = -\frac{27}{2}q + \frac{3}{2}\sqrt{-3}\sqrt{\Delta(P)},$$

$$(x_1 + j^2x_2 + jx_3)^3 = -\frac{27}{2}q - \frac{3}{2}\sqrt{-3}\sqrt{\Delta(P)}.$$

On obtient a priori trois valeurs pour chaque résolvante, donc neuf valeurs pour le couple en extrayant les racines cubiques. Mais il est facile de vérifier que

$$(x_1 + jx_2 + j^2x_3)(x_1 + j^2x_2 + jx_3) = -3p.$$

L'une des résolvantes impose l'autre, et le couple de résolvantes prend trois valeurs. Utilisant de plus $x_1 + x_2 + x_3 = 0$, il est aisé de déterminer x_1, x_2, x_3 en résolvant un système de Vandermonde. Ce système est particulièrement simple puique les coefficients sont des racines cubiques de 1 (exercice 7). On obtient ainsi les formules de Cardan.

Exercice 5. ① *Quelle hypothèse « optimale » faire sur la caractéristique de* $\mathbb{K}$ *pour faire fonctionner les calculs précédents ?*

Exercice 6. ① *Compléter les détails de ces calculs.*

Exercice 7. ② *Soient* $n \geq 2$ *un entier* ε *une racine primitive* n*-ième de* 1 *dans* $\mathbb{C}$, V *la matrice de Vandermonde* $\left(\varepsilon^{(i-1)(j-1)}\right)_{1\leq i,j\leq n}$. *Vérifier que l'inverse de* V *est* $\dfrac{{}^t\overline{V}}{n}$.

Exercice 8. ⑤ *On suppose* $n \geq 2$, $\mathbb{K}$ *de caractéristique nulle et* $X^n - 1$ *scindé sur* $\mathbb{K}$. *On se donne* n *indéterminées* $X_1, \ldots, X_n$, *on pose* $\mathbb{K}_X = \mathbb{K}(X_1, \ldots, X_n)$. *Le groupe* $\mathcal{S}_n$ *agit naturellement sur* $\{X_1, \ldots, X_n\}$. *On sait que le corps fixe est* $\mathbb{K}_\Sigma = \mathbb{K}(\Sigma_1, \ldots, \Sigma_n)$ *où les* Σ_i *sont les polynômes symétriques élémentaires. Montrer que, si* ε *est une racine primitive* n*-ième de* 1, *alors* $\displaystyle\sum_{j=1}^{n} \varepsilon^j X_j$ *est de degré* $(n-1)!$ *sur* $\mathbb{K}_\sigma$.

2.4 La condition suffisante

On complète ici, en supposant $\mathbb{K}$ de caractéristique nulle, la caractérisation des équations résolubles par radicaux.

Théorème 3. *Supposons* $\mathbb{K}$ *de caractéristique nulle, soit* $\mathbb{L}$ *une extension finie de* $\mathbb{K}$. *Les conditions suivantes sont équivalentes.*

i) L'extension $\mathbb{L}/\mathbb{K}$ *est résoluble par radicaux.*

ii) Le groupe $Gal(Clnorm_{\mathbb{K}}\mathbb{L}/\mathbb{K})$ *est résoluble.*

Preuve. i) $\Rightarrow$ *ii)* a été établi. Supposons donc *ii)*, notons

$$\mathbb{L}' = \mathrm{Clnorm}_{\mathbb{K}}\mathbb{L}, \qquad G = \mathrm{Gal}(\mathbb{L}'/\mathbb{K})$$

et montrons que $\mathbb{L}'/\mathbb{K}$ est résoluble par radicaux, ce qui prouvera *i)*. La résolubilité de G entraîne l'existence d'une chaîne de sous-groupes de G :

$$\{\mathrm{id}\,\} = G_r \subset G_{r-1} \subset \cdots \subset G_0 = G$$

tel que, pour $0 \leq i \leq r-1$, G_{i+1} soit normal dans G_i et le quotient G_i/G_{i+1} soit cyclique. [6]

Pour $0 \leq i \leq r-1$, posons $\mathbb{K}_i = \mathbb{L}'^{G_i}$, de sorte que

$$\mathbb{K} = \mathbb{K}_0 \subset \mathbb{K}_1 \subset \cdots \subset \mathbb{K}_r = \mathbb{L}',$$

et que chaque extension $\mathbb{K}_{i+1}/\mathbb{K}_i$ est galoisienne, de groupe de Galois isomorphe à G_i/G_{i+1}. Si $\mathbb{K}$ contenait suffisamment de racines de l'unité, on pourrait conclure à l'aide du théorème 2. Dans le cas général, on rajoute les racines de 1 manquantes. Précisément, soit $n_i = [\mathbb{K}_{i+1} : \mathbb{K}_i]$ pour $0 \leq i \leq r-1$. Notons

6. On peut même supposer ces quotients d'ordre premier, mais nous n'en aurons pas besoin.

n le ppcm de $n_0, \ldots, n_{r-1}$, et choisissons ε une racine primitive n-ième de 1 dans Ω. On a le diagramme :

$$\begin{array}{ccccccccc} \mathbb{K} = \mathbb{K}_0 & \to & \mathbb{K}_1 & \to & \mathbb{K}_2 & \to & \cdots & \to & \mathbb{K}_r = \mathbb{L}' \\ \downarrow & & \downarrow & & \downarrow & & & & \downarrow \\ \mathbb{K}_0(\varepsilon) & \to & \mathbb{K}_1(\varepsilon) & \to & \mathbb{K}_2(\varepsilon) & \to & \cdots & \to & \mathbb{L}'(\varepsilon) \end{array}$$

Pour i dans $\{0, \ldots, r-1\}$, le théorème des irrationalités naturelles (chapitre 4, proposition 7, **3.3**) dit que $\mathbb{K}_{i+1}(\varepsilon)/\mathbb{K}_i(\varepsilon)$ est galoisienne, de groupe de Galois H_i isomorphe à un sous-groupe de G_i/G_{i+1}, donc cyclique. Puisque $K_i(\varepsilon)$ contient les racine $|H_i|$-ièmes de l'unité, le théorème 2 montre que $K_{i+1}(\varepsilon) = \mathbb{K}_i(\varepsilon)(\alpha_i)$ où $a_i \in K_{i+1}(\varepsilon)$ est tel que : ${\alpha_i}^{|H_i|} \in \mathbb{K}_i(\varepsilon)$. En fin de compte :

$$\mathbb{L}' \subset \mathbb{L}'(\varepsilon) = \mathbb{K}(\varepsilon, \alpha_1, \ldots, \alpha_{r-1}).$$

Le théorème est démontré.

Exemple. *Si le groupe de Galois est un p-groupe.*

Soit p un nombre premier. Puisque tout p-groupe est résoluble, tout polynôme de $\mathbb{K}[X]$ dont le corps de décomposition a pour degré sur $\mathbb{K}$ une puissance de p est résoluble par radicaux.

L'exercice ci-après complète l'exercice 1 et caractérise les extensions résolubles en caractéristique p.

Exercice 9. ④ *Soient p un nombre premier, $\mathbb{K}$ un corps de caractéristique p. On dit que l'extension $\mathbb{L}/\mathbb{K}$ est résoluble par p-radicaux si et seulement si existent $r \in \mathbb{N}^*$, $a_1, \ldots, a_r$ dans $\mathbb{C}$ tels que :*

i) $\mathbb{L} \subset \mathbb{K}(a_1, \ldots, a_r)$,

ii) Pour $1 \leq i \leq r$, de deux choses l'une :

- soit il existe $n_i \in \mathbb{N}^*$ tel que $a_i^{n_i} \in \mathbb{K}(a_1, \ldots, a_{i-1})$,

- soit $a_i^p - a_i \in \mathbb{K}(a_1, \ldots, a_{i-1})$.

Supposons $\mathbb{L}/\mathbb{K}$ séparable finie. Montrer que $\mathbb{L}/\mathbb{K}$ est résoluble par p-radicaux si et seulement si $Gal(Clnorm_{\mathbb{K}}\mathbb{L}/\mathbb{K})$ est résoluble.

2.5 Une autre vue sur la condition suffisante

On peut simultanément généraliser et simplifier l'argument conduisant au théorème 3. Si $\mathbb{A}$ est une $\mathbb{K}$-algèbre et G un groupe d'automorphismes de $\mathbb{A}$, notons $\mathbb{A}^G$ la sous-algèbre de $\mathbb{A}$ constituée des éléments fixes sous l'action de G :

$$\mathbb{A}^G = \{x \in \mathbb{A} \; ; \; \forall g \in G, \qquad g(x) = x\}.$$

Lemme 3. *Soient $\mathbb{A}$ une $\mathbb{K}$-algèbre de dimension finie, G un groupe d'automorphismes de G. On suppose G abélien fini d'exposant n, $|\mathbb{U}_n(\mathbb{K})| = n$. Alors tout élément de $\mathbb{A}$ est somme de n éléments de*

$$\left\{x \in \mathbb{A}, \; x^n \in \mathbb{A}^G\right\}.$$

Preuve. Les éléments de G annulent $X^n - 1$, qui est simplement scindé sur $\mathbb{K}$ par hypothèse. Ils sont donc diagonalisables. Comme G est abélien, ils sont

codiagonalisables. Autrement dit, $\mathbb{A}$ est engendré vectoriellement par les vecteurs propres communs aux éléments de G. Mais si x est un tel vecteur propre commun, il existe, pour tout g de G, une racine n-ième de 1 notée ω_g telle que

$$\forall g \in G, \qquad g(x) = \omega_g \, x.$$

Ainsi

$$\forall g \in G, \qquad g(x^n) = g(x)^n = x^n \quad \text{puis} \quad x^n \in \mathbb{A}^G.$$

Il reste à établir une version résoluble de ce résultat. L'argument crucial est le lemme immédiat ci-après.

Lemme 4. *Soit X un ensemble, G un groupe agissant sur X, N un sous-groupe normal de G. Alors l'action de G sur X donne par passage au quotient une action de G/N sur X^N pour laquelle*

$$X^G = \left(X^N\right)^{G/N}.$$

On en déduit aussitôt le résultat suivant, qui contient la condition suffisante de résolubilité par radicaux.

Proposition 3. *Soient $\mathbb{A}$ une $\mathbb{K}$-algèbre, G un groupe résoluble fini d'automorphismes de $\mathbb{A}$, $(G_i)_{0\leq i\leq n}$ une suite de sous-groupes de G telle que :*

$$\{e\} = G_r \lhd G_{r-1} \lhd \cdots \lhd G_1 \lhd G_0 = G,$$

et que, pour tout i de $\{0, \ldots, r-1\}$, G_{i+1}/G_i soit abélien d'ordre n_i. Supposons que $\mathbb{K}$ contienne les racines de 1 dans Ω et que la caractéristique de $\mathbb{K}$ ne divise aucun des n_i. Alors, pour tout i de $\{1, \ldots, r\}$, tout élément de $\mathbb{A}^{G_{i-1}}$ s'écrit

$$\sum_{i=1}^{r} x_i, \qquad \textit{avec} \quad \forall i \in \{1, \ldots, n_i\}, \quad {x_i}^{n_i} \in \mathbb{A}^{G_i}.$$

Exercice 10. ⑤ *Donner une méthode de résolution de l'équation de degré 4 fondée sur les idées de ce paragraphe et/ou du précédent.*

3 Variations sur le même thème

Les notations sont les mêmes que celles de la section précédente. Mais les résultats proposés ici ont un caractère moins central.

3.1 Constructibilité à la règle et au compas (II)

Nous allons revenir sur les constructions à la règle et au compas, notamment dans le but d'expliquer le travail de Gauss sur les polygones réguliers.

La section **5** du chapitre 2 motive la définition suivante : l'extension finie $\mathbb{L}/\mathbb{K}$ est dite *constructible* s'il existe une chaîne de corps :

$$\mathbb{K} = \mathbb{K}_0 \subset \mathbb{K}_1 \subset \cdots \subset \mathbb{K}_n$$

telle que $\mathbb{L} \subset \mathbb{K}_n$ et $[\mathbb{K}_{i+1} : \mathbb{K}_i] = 2$ pour $1 \leq i \leq n-1$.

Les remarques relatives aux extensions résolubles par radicaux s'appliquent aux extensions constructibles : toute extension contenue dans une extension constructible est constructible, toute composée d'extensions constructibles est constructible Les extensions constructibles sont décrites par l'énoncé ci-après, dont la preuve est une variante (plus simple) de celle du théorème 3.

Théorème 4. *Soit $\mathbb{L}/\mathbb{K}$ une extension finie séparable. Alors $\mathbb{L}/\mathbb{K}$ est constructible si et seulement si $[Clnorm_{\mathbb{K}}\mathbb{L} : \mathbb{K}]$ est puissance de 2.*

Preuve. On pose : $\mathbb{L}' = \mathrm{Clnorm}_{\mathbb{K}}\mathbb{L}$.

Supposons d'abord $\mathbb{L}/\mathbb{K}$ constructible ; $\mathbb{L}'$ est engendré sur $\mathbb{K}$ par les $\sigma(\mathbb{L})$ pour σ dans $\mathrm{Hom}_{\mathbb{K}}(\mathbb{L}, \Omega)$. En choisissant des $\mathbb{K}_i$ comme dans la définition, on a

$$\forall \sigma \in \mathrm{Hom}_{\mathbb{K}}(\mathbb{L}, \Omega),\ \forall i \in \{0, \ldots, n-1\}, \qquad [\sigma(\mathbb{K}_{i+1}) : \sigma(\mathbb{K}_i)] = 2.$$

On en déduit que $\mathbb{L}'/\mathbb{K}$ est constructible, donc que $[\mathbb{L}' : \mathbb{K}]$ est puissance de 2.

Réciproquement, supposons $[\mathbb{L}' : \mathbb{K}] = 2^m$ avec $m \in \mathbb{N}^*$ et notons le groupe $G = \mathrm{Gal}\,(\mathbb{L}'/\mathbb{K})$. La théorie des p-groupes fournit une chaîne de sous-groupes de G :

$$G = G_0 \supset G_1 \supset \cdots \supset G_m = \{\mathrm{id}\ \}$$

telle que, pour tout i de $\{0, \ldots, m-1\}, G_{i+1}$ est d'indice 2 dans G_i. L'extension $\mathbb{L}'/\mathbb{K}$ étant galoisienne, on en déduit, en posant $\mathbb{K}_i = (\mathbb{L}')^{G_i}$, que l'on a :

$$\mathbb{K}_0 = K \subset \mathbb{K}_1 \subset \cdots \subset \mathbb{K}_m = \mathbb{L}',$$

et que chaque corps de cette chaîne est extension de degré 2 du précédent. Par suite $\mathbb{L}'/\mathbb{K}$ est constructible, et $\mathbb{L}/\mathbb{K}$ aussi.

Comme dans la section **5** du chapitre 2, soit $\mathcal{C}$ le plus petit sous-corps de $\mathbb{C}$ stable par racine carrée, c'est-à-dire la réunion des sous-corps $\mathbb{K}$ de $\mathbb{C}$ telle que l'extension $\mathbb{K}/\mathbb{Q}$ soit finie et constructible. Le théorème 4 permet de dépasser substantiellement le théorème de Wantzel (corollaire 7, chapitre 2).

Corollaire 1. *Un nombre complexe z appartient à $\mathbb{C}$ si et seulement s'il est algébrique et si $[D_{\mathbb{Q}}\Pi_{\mathbb{Q},z} : \mathbb{Q}]$ est une puissance de 2.*

Exercice 11. ③ *Soit z un nombre algébrique de degré 4. On suppose que $Gal_{\mathbb{Q}}\Pi_{\mathbb{Q},z}$ est isomorphe à $\mathcal{A}_4$. Montrer que z n'appartient pas à $\mathcal{C}$.*

Un cas particulier du théorème est la caractérisation des polygones réguliers constructibles découverte par Gauss.

Corollaire 2. *L'extension $\mathbb{Q}\left(e^{2i\pi/n}\right)/\mathbb{Q}$ est constructible si et seulement si $\varphi(n)$ est une puissance de 2.*

Le polygone régulier à 17 côtés est donc constructible à la règle et au compas. Plus généralement, appelons *nombre premier de Fermat* tout nombre premier de la forme : $2^q + 1$ avec $q \in \mathbb{N}^*$, condition qui implique que q est une puissance de 2, comme on le voit en notant que $2^a + 1$ divise $2^b + 1$ si a est impair et divise b. Alors $\varphi(n)$ est une puissance de 2 si et seulement si n est produit d'une puissance de 2 et de nombres premiers de Fermat deux à deux distincts.

Le travail de Gauss sur l'équation cyclotomique

Gauss a prouvé la partie difficile de ce résultat (c'est-à-dire la suffisance). Son travail préfigure la théorie de Galois. Il donne en effet, si p est un nombre premier, une base normale de chaque corps intermédiaire de l'extension cyclotomique $\mathbb{Q}(e^{2i\pi/p})/\mathbb{Q}$, et montre comment calculer $e^{2i\pi/p}$ à l'aide des racines carrées si p est de Fermat ; les calculs sont menés jusqu'au bout pour $p = 17$. Les exercices ci-après détaillent ces résultats.

Exercice 12. ⑤ *Soient p un nombre premier, $\omega = e^{2i\pi/p}$, f un diviseur de $p-1$, $e = (p-1)/f$, g un générateur du groupe cyclique $\left(\mathbb{Z}/p\mathbb{Z}^*, \times\right)$. L'isomorphisme naturel entre $\left(\mathbb{Z}/p\mathbb{Z}^*, \times\right)$ et Gal $(\mathbb{Q}(\omega)/\mathbb{Q})$ dit que ce dernier groupe est engendré par l'unique $\mathbb{Q}$-automorphisme de $\mathbb{Q}(\omega)$ expédiant ω sur ω^g. On note $\mathbb{K}$ le corps fixe sous σ^f, qui est de degré f sur $\mathbb{Q}$. Pour former une $\mathbb{Q}$-base de $\mathbb{K}$, Gauss introduit les f « périodes » :*

$$\alpha_{r,\,f} = \sum_{0\le j\le e-1} \omega^{g^{jf+r}} \quad \text{où} \quad 0 \le r \le f-1.$$

a) Vérifier que les $\alpha_{r,\,f}$ sont fixes par σ^f.

b) Vérifier que $(\alpha_{r,\,f})_{0\le r\le f-1}$ est $\mathbb{Q}$-libre.

c) Vérifier que les $\alpha_{r,\,f}$ sont $\mathbb{Q}$-conjugués ; la famille $(\alpha_{r,\,f})_{0\le r\le f-1}$ est donc une base normale de $\mathbb{K}$ sur $\mathbb{Q}$.

Exercice 13. ⑤ *Calculer* $\cos(2\pi/17)$ *en utilisant uniquement des racines carrées.*

Abel a établi un analogue du corollaire 2 pour la division de la lemniscate.

3.2 Le casus irreducibilis

Soit P un polynôme de degré 3 à coefficients réels, que l'on suppose sans nuire à la généralité sans terme en X^2 :

$$P = X^3 + pX + q.$$

Une étude de fonction montre que P est simplement scindé sur $\mathbb{R}$ si et seulement si son discriminant

$$\Delta(P) = -4p^3 - 27q^2$$

est strictement négatif. Dans ce cas, les formules de Cardan font intervenir, d'une manière qui peut sembler paradoxale, des radicaux complexes.

Ainsi, si $P = X^3 - 15X - 4$, $\Delta(P) = 13068$, les formules de Cardan conduisent à chercher les racines cubiques de $2 + 11i$ et $2 - 11i$. Or, 4 est racine évidente de P, les deux autres racines étant $-2 - \sqrt{3}$ et $-2 + \sqrt{3}$. Cet exemple a été proposé en exercice au début du chapitre 1.

On étudie ici ce phénomène, connu sous le nom de « casus irreducibilis », dont l'élucidation semble due à Hölder.

Soit $\mathbb{L}/\mathbb{K}$ une extension finie avec $\mathbb{L} \subset \mathbb{R}$. On dit que $\mathbb{L}/\mathbb{K}$ est *résoluble par radicaux réels* s'il existe un entier $r \ge 1$, r éléments $a_1, \ldots, a_n$ de $\mathbb{R}^{+*}$, r éléments $n_1, \ldots, n_r$ de $\mathbb{N}^*$ tels que :

- $\mathbb{L} \subset \mathbb{K}\left(a_1{}^{1/n_1}, \ldots, a_r{}^{1/n_r}\right)$,

- $a_1 \in \mathbb{K}, a_2 \in \mathbb{K}\left(a_1{}^{1/n_1}\right), \ldots, a_r \in \mathbb{K}\left(a_1{}^{1/n_1}, \ldots, a_{r-1}{}^{1/n_{r-1}}\right)$.

Quitte à intercaler des radicaux intermédiaires, on peut de plus supposer que les n_i sont premiers.

Le casus irreducibilis s'explique alors par le théorème suivant.

Théorème 5. *Soient $\mathbb{L}$ un sous-corps de $\mathbb{R}$, $\mathbb{K}$ un sous-corps de $\mathbb{L}$ tel que $\mathbb{L}/\mathbb{K}$ soit finie et galoisienne. Les conditions suivantes sont équivalentes :*

i) $\mathbb{L}/\mathbb{K}$ est résoluble par radicaux réels,

ii) $[\mathbb{L} : \mathbb{K}]$ est une puissance de 2,

iii) $\mathbb{L}/\mathbb{K}$ est constructible.

En d'autres termes, toute extension galoisienne résoluble par radicaux réels s'obtient à l'aide de racines carrées.

L'implication *iii)* $\Rightarrow$ *i)* est évidente, sachant que toute extension quadratique d'un corps $\mathbb{K}$ de caractéristique différente de 2 est de la forme $\mathbb{K}\left(\sqrt{a}\right)$ avec $a \in \mathbb{K}$. L'implication *ii)* $\Rightarrow$ *iii)* vient du théorème 4. Ainsi, seule *i)* $\Rightarrow$ *ii)* est à prouver. L'essentiel de la démonstration est contenu dans le lemme ci-après.

Lemme 5. *Soient $\mathbb{L}$ un sous-corps de $\mathbb{R}$, $\mathbb{K}$ un sous-corps de $\mathbb{L}$ tel que l'extension $\mathbb{L}/\mathbb{K}$ soit finie et galoisienne. Supposons $q = [\mathbb{L} : \mathbb{K}]$ premier impair. Si p est un nombre premier et a un élément de $\mathbb{K} \cap \mathbb{R}^{+*}$, l'extension $\mathbb{L}(a^{1/p})$ / $\mathbb{K}(a^{1/p})$ est galoisienne de degré q.*

Preuve. Le théorème des irrationalités naturelles fournit le caractère galoisien de l'extension $\mathbb{L}(a^{1/p})/\mathbb{K}(a^{1/p})$ et le fait que $[\mathbb{L}(a^{1/p}) : \mathbb{K}(a^{1/p})]$ divise $[\mathbb{L} : \mathbb{K}] = q$.

Il reste à écarter l'éventualité :

$$\mathbb{L}(a^{1/p}) = \mathbb{K}(a^{1/p}), \quad \text{i.e.} \quad \mathbb{L} \subset \mathbb{K}(a^{1/p}).$$

Mais on sait (proposition 1, **2.2**, chapitre 1) que $\left[\mathbb{K}(a^{1/p}) : \mathbb{K}\right]$ vaut p ou 1 selon que $a^{1/p}$ est ou non dans $\mathbb{K}$. L'inclusion de $\mathbb{L}$ dans $\mathbb{K}(a^{1/p})$ force alors $\mathbb{L} = \mathbb{K}(a^{1/p})$ et $q = p$. Toujours grâce à la proposition 1 du chapitre 1, les $\mathbb{K}$-conjugués de $a^{1/p} = a^{1/q}$ sont les $\varepsilon a^{1/p}$, où ε décrit $\mathbb{U}_q$. Puisque $q \geq 3$, l'un au moins de ces nombres n'est pas réel, ce qui contredit la normalité de $\mathbb{L}/\mathbb{K}$.

Appliquant plusieurs fois le lemme 1, on obtient un cas particulier crucial du théorème 5, qui contient le casus irreducibilis classique :

Proposition 4. *Soit $\mathbb{L}$ un sous-corps de $\mathbb{R}$, $\mathbb{K}$ un sous-corps de $\mathbb{L}$ tel que l'extension $\mathbb{L}/\mathbb{K}$ soit finie galoisienne de degré premier impair. Alors, $\mathbb{L}/\mathbb{K}$ n'est pas résoluble par radicaux réels.*

Preuve de l'implication i) $\Rightarrow$ ii) du théorème 5. Supposons que $[\mathbb{L} : \mathbb{K}]$ n'est pas une puissance de 2. Soit q un diviseur premier impair de $[\mathbb{L} : \mathbb{K}]$. La correspondance de Galois et l'existence d'un élément d'ordre q dans $\mathrm{Gal}(\mathbb{L}/\mathbb{K})$ fournissent un sous-corps $\mathbb{K}'$ de $\mathbb{L}$ contenant $\mathbb{K}$ tel que $[\mathbb{L} : \mathbb{K}'] = q$. Le lemme 4 entraîne que $\mathbb{L}/\mathbb{K}'$ n'est pas résoluble par radicaux réels. Il en est a fortiori de même de $\mathbb{L}/\mathbb{K}$.

Exercice 14. ③ *Soient $\mathbb{K}$ un sous-corps de $\mathbb{R}$, $P \in \mathbb{K}[X]$ irréductible scindé sur $\mathbb{R}$, et $x \in \mathbb{R}$ une racine de P. On suppose $\mathbb{K}(x)/\mathbb{K}$ résoluble par radicaux réels. Montrer que $D_{\mathbb{K}}P/\mathbb{K}$ est résoluble par radicaux réels et que le degré de P est une puissance de 2.*

3.3 Les équations résolubles de degré premier

Soit p un nombre premier. On se propose de caractériser les polynômes irréductibles de degré p résolubles par radicaux. Si P est un polynôme de $\mathbb{K}[X]$ irréductible séparable de degré p, l'action du groupe $\mathrm{Gal}_{\mathbb{K}}(P)$ sur l'ensemble des racines de P est transitive. L'étude des équations irréductibles résolubles de degré p se ramène ainsi à celle des sous-groupes transitifs résolubles de $\mathcal{S}_p$. Pour comprendre ces derniers objets, on pense à $\mathcal{S}_p$ comme à $\mathcal{S}(\mathbb{F}_p)$.

On note $\mathrm{Aff}_1(\mathbb{F}_p)$ le groupe affine de $\mathbb{F}_p$, constitué des :

$$\sigma_{a,b} \ : x \mapsto ax + b \ , \quad a \in \mathbb{F}_p^*, \quad b \in \mathbb{F}_p.$$

Le sous-groupe $T_1(\mathbb{F}_p)$ de $\mathrm{Aff}_1(\mathbb{F}_p)$ constitué des translations $\sigma_{1,b}$, $b \in \mathbb{F}_p$ est cyclique d'ordre p. L'application :

$$\sigma_{a,b} \in G \longmapsto a \in \mathbb{F}_p^*$$

est un morphisme surjectif de noyau $T_1(\mathbb{F}_p)$. La stabilité de la classe des groupes résolubles par extension entraîne que le groupe $\mathrm{Aff}_1(\mathbb{F}_p)$ est résoluble. Par ailleurs, T agit transitivement sur $\mathbb{F}_p$. Le théorème suivant, dû à Galois, donne alors la description attendue des groupes transitifs résolubles de $\mathcal{S}(\mathbb{F}_p)$.

Théorème 6. *Soit G un sous-groupe transitif et résoluble de $\mathcal{S}(\mathbb{F}_p)$. Alors G est conjugué dans $\mathcal{S}(\mathbb{F}_p)$ à un sous-groupe de $Aff_1(\mathbb{F}_p)$ contenant $T_1(\mathbb{F}_p)$.*

La démonstration de ce théorème repose sur deux résultats.

Proposition 5. *Soient X un ensemble de cardinal p, G un sous-groupe de $\mathcal{S}(X)$ agissant transitivement sur X, H un sous-groupe normal non nul de G. Alors H agit transitivement sur X.*

Preuve. Supposons que H n'agisse pas transitivement sur X. Puisque p est premier, il existe alors x dans X dont l'orbite sous l'action de H est de cardinal 1, c'est-à-dire dont le stabilisateur contient H. Or, comme l'action est transitive, les stabilisateurs de deux points de X sont conjugués dans G. Puisque H est distingué dans G, il s'ensuit que H fixe tout point de X : H est nul.

Proposition 6. *Si σ est un élément de $\mathcal{S}(\mathbb{F}_p)$ tel que :*

$$\sigma \circ \tau_{1,1} \circ \sigma^{-1} \in Aff_1(\mathbb{F}_p),$$

alors σ appartient à $Aff_1(\mathbb{F}_p)$.

Preuve. La permutation $\sigma \circ \tau_{1,1} \circ \sigma^{-1}$ appartient à $\mathrm{Aff}_1(\mathbb{F}_p)$ et n'a pas de point fixe : c'est donc une translation. On dispose donc de a dans $\mathbb{F}_p^*$ tel que :

$$\forall x \in \mathbb{F}_p, \qquad \sigma(x+1) \ = \ \sigma(x) + a.$$

Il s'ensuit aussitôt que :

$$\forall x \in \mathbb{F}_p, \qquad \sigma(x) \ = \ ax + \sigma(0).$$

Preuve du théorème 6. Soit $(G_j)_{0\leq j\leq r}$ une suite de sous-groupes de G croissante pour l'inclusion, telle que $G_0 = \{e\}$, $G_r = G$ et que, pour tout i de $\{0, \ldots, r-1\}$, G_i soit normal dans G_{i+1} et le quotient G_{i+1}/G_i soit cyclique de cardinal premier. En utilisant la proposition 5 et une récurrence descendante, on montre que, pour tout j de $\{1, \ldots, r\}$, l'action de G_j sur $\mathbb{F}_p$ est transitive. L'ordre de G_1 est premier et divisible par p (transitivité), donc égal à p. Quitte à conjuguer G dans $\mathcal{S}(\mathbb{F}_p)$, on suppose que G_1 est le sous-groupe engendré par la translation $\tau_{1,1}$. En raisonnant par récurrence sur j, on montre à l'aide de la proposition 6 que, pour tout j de $\{1, \ldots, r\}$, G_j est contenu dans $\mathrm{Aff}_1(\mathbb{F}_p)$, ce qui établit le théorème.

Galois a donné une importante généralisation de ce théorème dans le texte *Des équations primitives qui sont résolubles par radicaux*. Ce « fragment d'un second mémoire » introduit la notion de groupe de permutation primitif et relie les groupes primitifs résolubles aux groupes affines en dimension > 1 sur $\mathbb{F}_p$. C'est d'ailleurs afin d'étudier ces groupes que Galois a introduit, dans le mémoire *Sur la théorie des nombres*, les corps finis $\mathbb{F}_{p^m}$.

Exercice 15. ④ *Dénombrer les sous-groupes transitifs résolubles de $\mathcal{S}_p$.*

L'application du théorème 6 aux équations est le très joli énoncé suivant. [7]

Théorème 7. *Supposons $\mathbb{K}$ de caractéristique nulle. Soient P dans $\mathbb{K}[X]$ irréductible de degré p, $x_1, \ldots, x_p$ les racines de P dans Ω, i et j distincts dans $\{1, \ldots, p\}$. Les deux conditions suivantes sont équivalentes.*

i) Le groupe $Gal_{\mathbb{K}}P$ est résoluble.

ii) On a : $D_{\mathbb{K}}P = \mathbb{K}(x_i, x_j)$,

Preuve. La clef de la preuve est la conséquence suivante du théorème 6 : si G est un sous-groupe de $\mathcal{S}_p$ transitif et résoluble, si g est un élément de G fixant deux points, alors g est l'identité. En effet, une application affine de $\mathbb{F}_p$ dans lui-même ayant deux points fixes est l'identité.

Preuve de i) $\Rightarrow$ ii). Supposons le groupe $\mathrm{Gal}_{\mathbb{K}}P$ résoluble. Soient i et j deux éléments distincts de $\{1, \ldots, p\}$. Si l'élément σ de $\mathrm{Gal}_{\mathbb{K}}P$ fixe x_i et x_j, l'observation ci-dessus montre que $\sigma = \mathrm{id}$. Par correspondance de Galois, il en résulte $\mathrm{D}_{\mathbb{K}}P = \mathbb{K}(x_i, x_j)$.

Preuve de ii) $\Rightarrow$ i). Puisque x_i est de degré p sur $\mathbb{K}$ et x_j de degré $\leq p-1$ sur $\mathbb{K}(x_i)$, *ii)* entraîne :

$$(1) \qquad |\mathrm{Gal}_{\mathbb{K}}P| = [\mathrm{D}_{\mathbb{K}}P : \mathbb{K}] \leq p(p-1).$$

Par ailleurs, la transitivité de $\mathrm{Gal}_{\mathbb{K}}P$ entraîne que p divise $|\mathrm{Gal}_{\mathbb{K}}P|$. Grâce au « lemme de Cauchy », le groupe $\mathrm{Gal}_{\mathbb{K}}P$ contient donc un élément d'ordre p. Cet

7. La formulation de ce théorème ne fait intervenir que les équations. Mais il semble difficile d'établir le résultat sans recours à la théorie des groupes. Cette constatation explique peut-être que Galois ait regardé ce résultat comme le point culminant de son mémoire.

élément est nécessairement un p-cycle γ, conjugué dans $\mathcal{S}_p$ à $\gamma_{1,1}$. Remplaçant $\mathrm{Gal}_{\mathbb{K}}P$ par un de ses conjugués dans $\mathcal{S}(\mathbb{F}_p)$, on peut donc supposer

$$T_1(\mathbb{F}_p) \subset \mathrm{Gal}_{\mathbb{K}}P.$$

Mais l'inégalité (1) montre que $\mathrm{Gal}_{\mathbb{K}}P$ ne peut contenir qu'un sous-groupe cyclique d'ordre p, qui est donc nécessairement distingué. Il reste à appliquer la proposition 5 pour conclure.

L'exercice ci-après, dû à Kronecker, explicite une classe d'équations de degré p non résolubles par radicaux.

Exercice 16. ③ *a) Soient $\mathbb{K}$ un corps, $\mathbb{L}$ une extension de $\mathbb{K}$, P dans $\mathbb{K}[X]$ irréductible sur $\mathbb{K}$ de degré p et résoluble par radicaux sur $\mathbb{K}$, n le nombre de racines de P appartenant à $\mathbb{L}$. Montrer que $n \in \{0, 1, p\}$.*

b) Montrer que $X^p - 2pX - p$ n'est pas résoluble par radicaux sur $\mathbb{Q}$ si $p \geq 5$ est premier.