

Chapitre 4

Théorie de Galois

Sommaire

1	Groupe de Galois d'une extension finie	2
1.1	Définition et premières remarques	2
1.2	Extensions normales	4
1.3	Extensions galoisiennes : définition et premières propriétés	5
1.4	Exemples de groupes de Galois	7
1.5	Changement d'extension	9
2	Groupe de Galois d'un polynôme	11
2.1	Action du groupe de Galois sur les racines	11
2.2	L'équation générale de degré n	15
2.3	Signature des éléments du groupe de Galois	15
2.4	(*) Le théorème de réduction modulo p	18
3	La correspondance de Galois	21
3.1	Le lemme d'Artin et le premier volet de la correspondance	21
3.2	Applications et exemples	23
3.3	Le second volet de la correspondance	28
4	(*) Deux exemples de groupes de Galois sur \mathbb{Q}	30
4.1	Les groupes abéliens finis	31
4.2	Les groupes symétriques	32
5	(*) Appendice : le théorème de la base normale	33

Présentation du chapitre

On aborde dans ce chapitre la théorie de Galois proprement dite. On se fixe un corps \mathbb{K} et une clôture algébrique Ω de \mathbb{K} . Toutes les extensions algébriques de \mathbb{K} considérées ici seront supposées plongées dans Ω . Comme on l'a vu dans le chapitre **3**, cette hypothèse ne nuit pas à la généralité.

La section **1** est consacrée aux notions de groupe Galois d'une extension finie, d'extension normale et d'extension galoisienne. Le lecteur peut, s'il le désire, se placer d'emblée en caractéristique zéro et éviter ainsi les problèmes de séparabilité (au demeurant minces à ce stade). Dans la section **2**, on fait le lien avec le point de vue historique (groupe de Galois d'un polynôme). La section **3**, consacrée à la correspondance de Galois, est l'aboutissement du chapitre. La section **4** donne deux exemples simples du « problème de Galois inverse ». La section **5** est dévolue au théorème de la base normale, qui permet, entre autres, une formulation « effective » de la correspondance.

1 Groupe de Galois d'une extension finie

1.1 Définition et premières remarques

Si \mathbb{L}/\mathbb{K} est une extension de corps, l'ensemble des automorphismes de la \mathbb{K} -algèbre \mathbb{L} est un sous-groupe du groupe des bijections de \mathbb{L} sur lui-même. On l'appelle *groupe de Galois* de l'extension \mathbb{L}/\mathbb{K} et on le note $\text{Gal}(\mathbb{L}/\mathbb{K})$. Les éléments de $\text{Gal}(\mathbb{L}/\mathbb{K})$ sont donc les bijections de \mathbb{L} sur lui-même qui respectent les relations algébriques à coefficients dans \mathbb{K} .

Nous nous intéresserons principalement au cas où l'extension \mathbb{L}/\mathbb{K} est finie. Dans ce cas, puisque tout endomorphisme injectif d'un \mathbb{K} -espace vectoriel de dimension finie est bijectif, on a

$$\text{Gal}(\mathbb{L}/\mathbb{K}) = \text{Hom}_{\mathbb{K}}(\mathbb{L}, \mathbb{L}).$$

Le lemme 4 du chapitre 3 (section 4) montre que cette égalité subsiste si \mathbb{L}/\mathbb{K} est algébrique, en particulier si $\mathbb{L} = \Omega$. Signalons au passage que le groupe de Galois $\text{Gal}(\Omega/\mathbb{K})$ est appelé « groupe de Galois absolu »¹ de \mathbb{K} et que l'on est loin de comprendre $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, même si beaucoup de travail a été effectué en ce sens.

Le groupe de Galois d'une extension finie est un invariant plus subtil que le degré. Il n'est cependant véritablement utile que s'il est « aussi gros que possible ». Précisons. On a vu que

$$(1) \quad \text{Gal}(\mathbb{L}/\mathbb{K}) = \text{Hom}_{\mathbb{K}}(\mathbb{L}, \mathbb{L}) \subset \text{Hom}_{\mathbb{K}}(\mathbb{L}, \Omega).$$

Cette inclusion est une égalité si et seulement si \mathbb{L} est « stable par \mathbb{K} -conjugaison », ou *normale*. On sait d'autre part que

$$(2) \quad |\text{Hom}_{\mathbb{K}}(\mathbb{L}, \Omega)| \leq [\mathbb{L} : \mathbb{K}],$$

avec égalité si et seulement si \mathbb{L}/\mathbb{K} est séparable. Ainsi, \mathbb{L}/\mathbb{K} est normale et séparable si et seulement si (1) et (2) sont des égalités. Les extensions normales et séparables sont dites *galoisiennes*.

Exercice 1. ③ *Démontrer que, pour une extension algébrique \mathbb{L}/\mathbb{K} , on a*

$$\text{Gal}(\mathbb{L}/\mathbb{K}) = \text{Hom}_{\mathbb{K}}(\mathbb{L}, \mathbb{L}).$$

Un exemple de base

Soit x un élément de Ω . Notons $x_1 = x, \dots, x_m$ les \mathbb{K} -conjugés de x . La détermination de $\text{Hom}_{\mathbb{K}}(\mathbb{K}(x), \Omega)$ effectuée dans le chapitre 3 permet de décrire $\text{Gal}(\mathbb{K}(x)/\mathbb{K})$. Pour i dans $\{1, \dots, m\}$, soit σ_i l'unique élément de $\text{Hom}_{\mathbb{K}}(\mathbb{K}(x), \Omega)$ envoyant x sur x_i . Soit I l'ensemble des éléments i de $\{1, \dots, m\}$ tels que x_i appartienne à $\mathbb{K}(x)$. Alors σ_i appartient à $\text{Gal}(\mathbb{K}(x)/\mathbb{K})$ si et seulement si i appartient à I . Cet exemple illustre l'alinéa précédent : $\mathbb{K}(x)/\mathbb{K}$ est galoisienne si et seulement si x est séparable et $\mathbb{K}(x)$ stable par \mathbb{K} -conjugaison.

Donnons quelques illustrations.

- On a $\mathbb{C} = \mathbb{R}(i)$, les \mathbb{R} -conjugés de i sont $\pm i$: il s'ensuit que $\text{Gal}(\mathbb{C}/\mathbb{R})$ contient deux éléments, l'identité de \mathbb{C} et la conjugaison complexe.

- Puisque $\sqrt{2}$ admet pour conjugés $\pm\sqrt{2}$, $\text{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$ contient deux éléments, l'identité de $\mathbb{Q}(\sqrt{2})$ et l'application σ définie par

$$\forall (a, b) \in \mathbb{Q}^2, \quad \sigma(a + b\sqrt{2}) = a - b\sqrt{2}.$$

1. Puisque deux clôtures algébriques de \mathbb{K} sont isomorphes comme \mathbb{K} -algèbres, ce groupe ne dépend pas du choix de Ω .

Ces deux extensions sont galoisiennes.

- Si $n \geq 3$, les \mathbb{Q} -conjugués de $a = \sqrt[n]{2}$ sont les ωa pour ω dans U_n . On en déduit que $\text{Gal}(\mathbb{Q}(a)/\mathbb{Q})$ contient deux éléments si n est pair, un si n est impair. L'extension n'est pas galoisienne.

- Pour n dans \mathbb{N}^* , les \mathbb{Q} -conjugués de $\omega = e^{2i\pi/n}$ sont les ω^k pour k dans $\{1, \dots, n\}$ premier à n : ils appartiennent à $\mathbb{Q}(\omega)$, l'extension $\mathbb{Q}(\omega)/\mathbb{Q}$ est galoisienne de degré $\varphi(n)$.

Exercice 2. ① *Expliciter les éléments de $\text{Gal}(\mathbb{Q}(a)/\mathbb{Q})$ si $a = \sqrt[n]{2}$ et si $n \geq 4$ est pair.*

La correspondance de Galois : discussion préliminaire

Si \mathbb{F} est un corps et G un sous-groupe du groupe $\text{Aut}(\mathbb{F})$ des automorphismes de \mathbb{F} , on note \mathbb{F}^G le corps des points de \mathbb{F} fixes sous l'action de G :

$$\mathbb{F}^G = \{x \in \mathbb{F}; \forall \sigma \in G, \sigma(x) = x\}.$$

Le but principal de ce chapitre est la correspondance de Galois pour les extensions finies. Décrivons brièvement ce dont il s'agit. Soit \mathbb{L}/\mathbb{K} une extension finie. Notons $\mathcal{K}_{\mathbb{L}/\mathbb{K}}$ l'ensemble des sous-corps de \mathbb{L} contenant \mathbb{K} , $\mathcal{G}_{\mathbb{L}/\mathbb{K}}$ l'ensemble des sous-groupes de $\text{Gal}(\mathbb{L}/\mathbb{K})$. À l'élément \mathbb{K}' de $\mathcal{K}_{\mathbb{L}/\mathbb{K}}$, on associe le sous-groupe

$$\varphi(\mathbb{K}') = \text{Gal}(\mathbb{L}/\mathbb{K}')$$

de $\text{Gal}(\mathbb{L}/\mathbb{K})$. Inversement, à l'élément G de $\mathcal{G}_{\mathbb{L}/\mathbb{K}}$, on associe l'élément

$$\psi(G) = \mathbb{L}^G$$

de $\mathcal{K}_{\mathbb{L}/\mathbb{K}}$. On dispose donc de deux applications

$$\mathcal{K}_{\mathbb{L}/\mathbb{K}} \xrightarrow{\varphi} \mathcal{G}_{\mathbb{L}/\mathbb{K}}, \quad \mathcal{G}_{\mathbb{L}/\mathbb{K}} \xrightarrow{\psi} \mathcal{K}_{\mathbb{L}/\mathbb{K}}.$$

Deux inclusions sont immédiates :

$$\forall \mathbb{K}' \in \mathcal{K}_{\mathbb{L}/\mathbb{K}}, \quad \mathbb{K}' \subset \mathbb{L}^{\text{Gal}(\mathbb{L}/\mathbb{K}')} = \psi \circ \varphi(\mathbb{K}'),$$

$$\forall G \in \mathcal{G}_{\mathbb{L}/\mathbb{K}}, \quad G \subset \text{Gal}(\mathbb{L}/\mathbb{L}^G) = \varphi \circ \psi(G).$$

Supposons \mathbb{L}/\mathbb{K} galoisienne. La correspondance de Galois consiste en deux résultats.

- Les applications φ et ψ sont deux bijections réciproques.

- Si $\mathbb{K}' \in \mathcal{K}_{\mathbb{L}/\mathbb{K}}$, \mathbb{K}'/\mathbb{K} est galoisienne si et seulement si $\text{Gal}(\mathbb{L}/\mathbb{K}')$ est un sous-groupe normal de $\text{Gal}(\mathbb{L}/\mathbb{K})$; dans ce cas, le quotient

$$\text{Gal}(\mathbb{L}/\mathbb{K})/\text{Gal}(\mathbb{L}/\mathbb{K}')$$

est naturellement isomorphe à $\text{Gal}(\mathbb{K}'/\mathbb{K})$.

Ce résultat permet de traiter des problèmes de théorie des corps par des méthodes de théorie des groupes. Il peut être vu comme une « théorie géométrique des équations ». La caractérisation des équations résolubles par radicaux en est l'origine historique et l'application la plus célèbre.²

2. L'intérêt de la solution de Galois dépasse de loin celui du problème initial. Comme le disent les notes historiques de Bourbaki : « À la lumière des découvertes de Galois, on s'aperçoit que le problème de la résolution « par radicaux » n'est qu'un cas particulier, assez artificiel, de la classifications des irrationnelles. »

1.2 Extensions normales

Soit \mathbb{L} un sous-corps de Ω contenant \mathbb{K} . La discussion de l'introduction conduit à distinguer le cas où, pour tout x de \mathbb{L} , les \mathbb{K} -conjugués de x sont dans \mathbb{L} , i.e. celui où :

$$\text{Hom}_{\mathbb{K}}(\mathbb{L}, \Omega) = \text{Gal}(\mathbb{L}/\mathbb{K}).$$

L'extension \mathbb{L}/\mathbb{K} est dite *normale* si elle possède cette propriété.

Lemme 1. *Soient \mathbb{L}/\mathbb{K} et \mathbb{M}/\mathbb{L} deux extensions. Si \mathbb{M}/\mathbb{K} est normale, il en est de même de \mathbb{M}/\mathbb{L} .*

Preuve. Chaque \mathbb{L} -conjugué de $x \in \mathbb{M}$ en est aussi un \mathbb{K} -conjugué.

En revanche, \mathbb{L}/\mathbb{K} n'a aucune raison d'être normale. Pour le voir, il suffit de considérer :

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{Q}(j, \sqrt[3]{2}) \quad \text{avec } j = e^{2i\pi/3}.$$

La normalité de $\mathbb{Q}(j, \sqrt[3]{2})/\mathbb{Q}$ provient de l'égalité $\mathbb{Q}(j, \sqrt[3]{2}) = D_{\mathbb{Q}}(X^3 - 2)$ et de la caractérisation ci-après des extensions normales finies.

Théorème 1. *Soit \mathbb{L}/\mathbb{K} une extension finie. Les deux assertions suivantes sont équivalentes.*

(i) *L'extension \mathbb{L}/\mathbb{K} est normale.*

(ii) *Il existe P dans $\mathbb{K}[X]$ tel que $\mathbb{L} = D_{\mathbb{K}}P$.*

Preuve. (i) \Rightarrow (ii) Écrivons $\mathbb{L} = \mathbb{K}(x_1, x_2, \dots, x_m)$ où chaque x_i est algébrique sur \mathbb{K} . Puisque \mathbb{L}/\mathbb{K} est normale, les \mathbb{K} -conjugués de x_i sont dans \mathbb{L} , et donc $\mathbb{L} = D_{\mathbb{K}}P$ où $P = \prod_{\mathbb{K}, x_1} \times \dots \times \prod_{\mathbb{K}, x_m}$.

(ii) \Rightarrow (i) Supposons $\mathbb{L} = D_{\mathbb{K}}P$ avec $P \in \mathbb{K}[X]$. Notons y_1, y_2, \dots, y_ℓ les racines de P dans Ω , de sorte que $\mathbb{L} = \mathbb{K}(y_1, \dots, y_\ell)$. Si i est dans $\{1, \dots, \ell\}$ et σ dans $\text{Hom}_{\mathbb{K}}(\mathbb{L}, \Omega)$, $\sigma(y_i)$ est l'un des y_j , donc est dans \mathbb{L} . Ainsi, $\sigma(\mathbb{L}) \subset \mathbb{L}$ et $\sigma \in \text{Gal}(\mathbb{L}/\mathbb{K})$.

Exercice 3. ① *Soit \mathbb{L} une extension finie de \mathbb{K} contenue dans Ω . Montrer que \mathbb{L}/\mathbb{K} est normale si et seulement si le seul sous-corps de Ω isomorphe à \mathbb{L} comme \mathbb{K} -algèbre est \mathbb{L} .*

Exercice 4. ② *Soient \mathbb{L}_1 et \mathbb{L}_2 deux sous-corps de Ω . On suppose que \mathbb{L}_1/\mathbb{K} et \mathbb{L}_2/\mathbb{K} sont normales. Montrer qu'il en est de même de $\mathbb{L}_1\mathbb{L}_2/\mathbb{K}$.*

Exercice 5. ③ *Soit \mathbb{K} un sous-corps de \mathbb{C} , extension normale de \mathbb{Q} de degré impair. Montrer que $\mathbb{K} \subset \mathbb{R}$.*

Exercice 6. ③ *Déterminer les signatures possibles pour une extension normale de degré n de \mathbb{Q} .*

Exercice 7. ③ a) *Montrer que toute extension de degré 2 est normale.*

b) *Quels sont $n \in \mathbb{N}^*$ tels que toute extension de degré n de \mathbb{Q} soit normale ?*

Exercice 8. ③ *Indiquer deux extensions normales finies \mathbb{L}/\mathbb{K} et \mathbb{M}/\mathbb{L} telles que \mathbb{M}/\mathbb{K} ne soit pas normale.*

Exercice 9. ③ *L'extension $\mathbb{Q}(\sqrt{4 + \sqrt{5}})/\mathbb{Q}$ est-elle normale ?*

Exercice 10. ③ *Soit n dans \mathbb{N}^* . L'extension $\mathbb{Q}(\cos(2\pi/n))/\mathbb{Q}$ est-elle normale ?*

Remarque *Sans les morphismes ?*

Sans référence aux morphismes, le théorème dit que, si le polynôme Q de $\mathbb{K}[X]$ a une racine dans $D_{\mathbb{K}}P$, alors Q est scindé dans $D_{\mathbb{K}}P$. En voici une preuve directe. Gardant les notations ci-dessus, soit α une racine de Q dans $D_{\mathbb{K}}P$: α s'écrit $T(x_1, \dots, x_n)$ où $T \in \mathbb{K}[X_1, \dots, X_n]$. Or, le théorème de structure des polynômes symétriques entraîne que le polynôme

$$\prod_{\sigma \in \mathcal{S}_m} (X - T(x_{\sigma(1)}, \dots, x_{\sigma(m)}))$$

est dans $\mathbb{K}[X]$; ce polynôme annule α et a toutes ses racines dans $D_{\mathbb{K}}P$.

Exercice 11. ④ Soient $P \in \mathbb{K}[X]$ irréductible, \mathbb{L}/\mathbb{K} une extension normale finie, P_1 et P_2 deux facteurs irréductibles de P dans $\mathbb{L}[X]$. Montrer qu'il existe $\sigma \in \text{Gal}(\mathbb{L}/\mathbb{K})$ tel que $P_2 = \sigma.P_1$. En particulier, les facteurs irréductibles de P dans $\mathbb{L}[X]$ ont même degré. Donner un contre-exemple si \mathbb{L}/\mathbb{K} n'est pas normale.

Exercice 12. ④ Soit \mathbb{L}/\mathbb{K} une extension finie. En faisant agir $|\text{Gal}(\mathbb{L}/\mathbb{K})|$ sur $|\text{Hom}_{\mathbb{K}}(\mathbb{L}, \Omega)|$, montrer que $|\text{Gal}(\mathbb{L}/\mathbb{K})|$ divise $|\text{Hom}_{\mathbb{K}}(\mathbb{L}, \Omega)|$.

Exercice 13. ② Soient $p \in \mathcal{P}$, $x \in \Omega$ de degré p sur \mathbb{K} , séparable, $x_1 = x, x_2, \dots, x_p$ les \mathbb{K} -conjugués de x . Si $x_2 \in \mathbb{K}(x)$, montrer que $\mathbb{K}(x)/\mathbb{K}$ est normale. On pourra utiliser l'exercice précédent.

Clôture normale

Si \mathbb{L}/\mathbb{K} n'est pas normale, on définit la *clôture normale de L dans Ω* comme le plus petit sous-corps de Ω normal sur \mathbb{K} et contenant \mathbb{L} . On peut le voir soit comme l'intersection des sous-corps de Ω contenant \mathbb{L} et normaux sur \mathbb{K} , soit comme le sous-corps de Ω engendré par les $\sigma(\mathbb{L})$ pour σ dans $\text{Hom}_{\mathbb{K}}(\mathbb{L}, \Omega)$ ³.

Si \mathbb{L}/\mathbb{K} est finie, on peut expliciter $\text{Clnorm}_{\mathbb{K}}\mathbb{L}$ de la façon suivante. Écrivant $\mathbb{L} = \mathbb{K}(x_1, \dots, x_m)$ et notant $x_{i,1}, \dots, x_{i,n_i}$ les racines de $\Pi_{\mathbb{K}, x_i}$ dans Ω , on a :

$$\text{Clnorm}_{\mathbb{K}}\mathbb{L} = \mathbb{K}(x_{1,1}, \dots, x_{1,n_1}, \dots, x_{m,1}, \dots, x_{m,n_m}).$$

Exemple. La clôture normale de $\mathbb{Q}(2^{1/n})$ sur \mathbb{Q} est $\mathbb{Q}(2^{1/n}, e^{2i\pi/n})$.

Exercice 14. ③ Soit p un nombre premier supérieur ou égal à 3. Montrer que l'extension $\mathbb{Q}(\sqrt{p+\sqrt{p}})/\mathbb{Q}$ n'est pas normale et que

$$\text{Clnorm}_{\mathbb{Q}}\mathbb{Q}(\sqrt{p+\sqrt{p}}) = \mathbb{Q}(\sqrt{p+\sqrt{p}}, \sqrt{p-1}).$$

Déterminer le degré de ce nouveau corps sur \mathbb{Q} .

1.3 Extensions galoisiennes : définition et premières propriétés

L'extension \mathbb{L}/\mathbb{K} est dite *galoisienne* si elle est normale et séparable. Si \mathbb{K} est de caractéristique zéro ou, plus généralement, parfait, les extensions galoisiennes sont les extensions normales.

Le théorème ci-après rassemble les propriétés des extensions galoisiennes qui découlent aisément des résultats déjà obtenus.⁴

3. Grâce à la version générale du théorème de prolongement des morphismes, on peut remplacer $\text{Hom}_{\mathbb{K}}(\mathbb{L}, \Omega)$ par $\text{Gal}(\Omega/\mathbb{K})$ dans cette phrase.

4. Le lecteur est invité à démontrer les résultats plutôt que d'en lire les preuves.

Théorème 2. Soit \mathbb{L}/\mathbb{K} une extension finie.

1. L'extension \mathbb{L}/\mathbb{K} est galoisienne si et seulement si :

$$|\text{Gal}(\mathbb{L}/\mathbb{K})| = [\mathbb{L} : \mathbb{K}].$$

2. Soit \mathbb{K}' un sous-corps de \mathbb{L} contenant \mathbb{K} . Si \mathbb{L}/\mathbb{K} est galoisienne, il en est de même de \mathbb{L}/\mathbb{K}' . De plus, dans ce cas :

$$\text{Gal}(\mathbb{L}/\mathbb{K}') \subset \text{Gal}(\mathbb{L}/\mathbb{K}).$$

3. Si \mathbb{L}/\mathbb{K} est galoisienne, alors les éléments du corps de base \mathbb{K} sont « reconnus » par le groupe de Galois :

$$\mathbb{K} = \mathbb{L}^{\text{Gal}(\mathbb{L}/\mathbb{K})}.$$

4. Si \mathbb{L}/\mathbb{K} est séparable, $\text{Clnorm}_{\mathbb{K}}\mathbb{L}/\mathbb{K}$ est galoisienne.

5. Supposons \mathbb{L}/\mathbb{K} galoisienne. Soit $x \in \mathbb{L}$. Les \mathbb{K} -conjugués de x sont les $\sigma(x)$ où σ décrit $G = \text{Gal}(\mathbb{L}/\mathbb{K})$. Il en résulte que

$$\Pi_{\mathbb{K},x} = \prod_{y \in G.x} (X - y)$$

où $G.x$ est l'orbite de x sous l'action de G .

Preuve de 1. On a

$$|\text{Hom}_{\mathbb{K}}(\mathbb{L}, \Omega)| \leq [\mathbb{L} : \mathbb{K}],$$

avec égalité si et seulement si \mathbb{L}/\mathbb{K} est séparable. De plus

$$\text{Gal}(\mathbb{L}/\mathbb{K}) \subset \text{Hom}_{\mathbb{K}}(\mathbb{L}, \Omega),$$

avec égalité si et seulement si \mathbb{L}/\mathbb{K} est normale.

Preuve de 2. La séparabilité de \mathbb{L}/\mathbb{K}' , immédiate, est formellement démontrée dans la proposition 9 du paragraphe 2.4 du chapitre 2. Le caractère normal de \mathbb{L}/\mathbb{K}' , également immédiat, est le lemme 1 de 1.2.

Preuve de 3. Comme \mathbb{L}/\mathbb{K} est séparable, \mathbb{K} est l'ensemble des éléments de \mathbb{L} fixes par les éléments de $\text{Hom}_{\mathbb{K}}(\mathbb{L}, \Omega)$. Mais, comme \mathbb{L}/\mathbb{K} est normale, $\text{Hom}_{\mathbb{K}}(\mathbb{L}, \Omega) = \text{Gal}(\mathbb{L}/\mathbb{K})$.

Preuve de 4. Il suffit d'utiliser la description de la clôture normale vue à la fin de 1.2, la séparabilité des \mathbb{K} -conjugués d'un élément séparable et le fait qu'une extension engendrée par des éléments séparables est séparable (chapitre 3, paragraphe 4.1, corollaire 8).

Preuve de 5. Les \mathbb{K} -conjugués de x sont les images de x par les éléments de $\text{Hom}_{\mathbb{K}}(\mathbb{L}, \Omega)$, lequel n'est autre que $\text{Gal}(\mathbb{L}/\mathbb{K})$. D'autre part, x est séparable sur \mathbb{K} , donc $\Pi_{\mathbb{K},x}$ est simplement scindé sur \mathbb{K} . Le résultat s'ensuit.

Les points 2 et 3 donnent « un sens » de la correspondance de Galois : toute sous-extension d'une extension galoisienne est corps fixe du sous-groupe correspondant.

Exercice 15. ② Soit \mathbb{L}/\mathbb{K} une extension galoisienne finie. Montrer que x est un élément primitif de l'extension \mathbb{L}/\mathbb{K} si et seulement si le seul élément de $\text{Gal}(\mathbb{L}/\mathbb{K})$ fixant x est l'identité de \mathbb{L} .

Exercice 16. ② Soit \mathbb{L}/\mathbb{K} une extension finie. Montrer qu'il existe une extension galoisienne finie de \mathbb{K} contenant \mathbb{L} si et seulement si \mathbb{L}/\mathbb{K} est séparable.

Comment reconnaître les extensions galoisiennes finies ?

En caractéristique nulle, les extensions galoisiennes finies sont les corps de décomposition. Voici le cas général.

Théorème 3. *Supposons \mathbb{L}/\mathbb{K} finie. Les deux conditions suivantes sont équivalentes.*

(i) *L'extension \mathbb{L}/\mathbb{K} est galoisienne.*

(ii) *Il existe un élément P de $\mathbb{K}[X]$ séparable tel que $\mathbb{L} = D_{\mathbb{K}}P$.*

Preuve. (i) \Rightarrow (ii) Si \mathbb{L}/\mathbb{K} est galoisienne, elle est en particulier normale et il existe Q dans $\mathbb{K}[X]$ tel que $\mathbb{L} = D_{\mathbb{K}}Q$. Soient P_1, \dots, P_ℓ les facteurs irréductibles (distincts) de Q dans $\mathbb{K}[X]$.

Posons $P = \prod_{i=1}^{\ell} P_i$. Alors $\mathbb{L} = D_{\mathbb{K}}P$. Puisque \mathbb{L}/\mathbb{K} est séparable, chaque P_i , étant irréductible, est séparable ; il en va de même de P .

(ii) \Rightarrow (i) Supposons $\mathbb{L} = D_{\mathbb{K}}P$ où $P \in \mathbb{K}[X]$ est à racines simples dans Ω . L'extension \mathbb{L}/\mathbb{K} est normale comme corps de décomposition. De plus, notant u_1, \dots, u_m les racines de P , les u_i sont séparables sur \mathbb{K} et $\mathbb{L} = \mathbb{K}(u_1, \dots, u_m)$. Engendrée par des éléments séparables, \mathbb{L}/\mathbb{K} est séparable et donc galoisienne.

Exercice 17. ② *Montrer que les deux assertions du théorème précédent équivalent à l'existence de P dans $\mathbb{K}[X]$, irréductible sur \mathbb{K} et séparable, tel que $\mathbb{L} = D_{\mathbb{K}}P$.*

Exercice 18. ④ *Soient \mathbb{L}/\mathbb{K} une extension galoisienne finie de groupe G , $\mathcal{L}_{\mathbb{K}}(\mathbb{L})$ l'algèbre des endomorphismes du \mathbb{K} -espace vectoriel \mathbb{L} . Montrer que*

$$\mathcal{L}_{\mathbb{K}}(\mathbb{L}) = \bigoplus_{g \in G} \mathbb{L} g.$$

Terminons par des définitions. L'extension \mathbb{L}/\mathbb{K} est dite *abélienne* (resp. *cyclique*, resp. *résoluble*) si elle est galoisienne de groupe de Galois abélien (resp. cyclique, resp. résoluble).

1.4 Exemples de groupes de Galois

Il est en général difficile de calculer un groupe de Galois. On présente ici quelques exemples classiques et importants. Les deux premiers sont fondamentaux, les deux derniers peuvent être réservés à une seconde lecture. Le quatrième nécessite la connaissance des corps finis.

Extensions par une racine n -ième si $X^n - 1$ est scindé sur \mathbb{K}

Supposons \mathbb{K} de caractéristique nulle ou première à n , et $X^n - 1$ scindé sur \mathbb{K} . On sait depuis le paragraphe 3.1 du chapitre 1 que le groupe $\mathbb{U}_n(\mathbb{K})$ des racines n -ièmes de 1 dans \mathbb{K} est alors cyclique de cardinal n .

Proposition 1. *Soient a un élément de \mathbb{K} et $\alpha \in \Omega$ tel que $\alpha^n = a$. Alors l'extension $\mathbb{K}(\alpha)/\mathbb{K}$ est cyclique de degré divisant n ; elle est de degré n si et seulement si $X^n - a$ est irréductible sur \mathbb{K} .*

Preuve. Les racines de $X^n - a$ dans Ω sont les $\varepsilon\alpha$ avec ε dans $\mathbb{U}_n(\mathbb{K})$. Par suite :

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

L'extension $\mathbb{K}(\alpha)/\mathbb{K}$ est donc galoisienne, et les \mathbb{K} -conjugués de α sont de la forme $\varepsilon\alpha$ avec $\varepsilon \in \mathbb{U}_n(\mathbb{K})$. On dispose donc de :

$$\varphi : \begin{array}{ccc} \text{Gal}(\mathbb{K}(\alpha)/\mathbb{K}) & \longrightarrow & \mathbb{U}_n(\mathbb{K}) \\ \sigma & \longmapsto & \frac{\sigma(\alpha)}{\alpha} \end{array} .$$

On vérifie aisément que φ est un morphisme injectif, d'où le résultat.

Extensions cyclotomiques

Soient \mathbb{K} un corps de caractéristique nulle, n un entier ≥ 2 et ε une racine primitive n -ième de 1 dans Ω . Comme $\mathbb{K}(\varepsilon) = D_{\mathbb{K}}(X^n - 1)$, l'extension $\mathbb{K}(\varepsilon)/\mathbb{K}$ est galoisienne. Si σ appartient à $\text{Gal}(\mathbb{K}(\varepsilon)/\mathbb{K})$, $\sigma(\varepsilon)$ est racine du n -ième polynôme cyclotomique Φ_n (car ε est racine de Φ_n , et Φ_n est à coefficients dans \mathbb{Q} , donc dans \mathbb{K}); $\sigma(\varepsilon)$ est donc de la forme ε^j avec $j \wedge n = 1$. En associant à σ la classe de j modulo n , on définit un morphisme injectif de $\text{Gal}(\mathbb{K}(\varepsilon)/\mathbb{K})$ dans $\mathbb{Z}/n\mathbb{Z}^*$.

On déduit de cette argumentation le résultat suivant.

Proposition 2. *Sous les hypothèses précédentes, le groupe $\text{Gal}(\mathbb{K}(\varepsilon)/\mathbb{K})$ est isomorphe à un sous-groupe de $(\mathbb{Z}/n\mathbb{Z}^*, \times)$, donc abélien. Pour que $\text{Gal}(\mathbb{K}(\varepsilon)/\mathbb{K})$ soit isomorphe à $(\mathbb{Z}/n\mathbb{Z}^*, \times)$, il faut et il suffit que Φ_n soit irréductible sur \mathbb{K} .*

En particulier, $\text{Gal}(\mathbb{Q}(e^{2i\pi/n})/\mathbb{Q})$ est isomorphe à $(\mathbb{Z}/n\mathbb{Z}^*, \times)$.⁵

Extensions par une racine n -ième, cas général

Soient n un entier ≥ 2 , \mathbb{K} un corps de caractéristique nulle, a un élément de \mathbb{K}^* , P le polynôme $X^n - a$, ε une racine primitive n -ième de 1 dans Ω et $\alpha \in \Omega$ une racine de P , et $\mathbb{L} = D_{\mathbb{K}}P = \mathbb{K}(\varepsilon, \alpha)$. Les exemples 1 et 2 sont des cas particuliers de détermination de $\text{Gal}(\mathbb{L}/\mathbb{K})$; voyons le cas général.

Soit $\text{Aff}(\mathbb{Z}/n\mathbb{Z})$ le groupe des bijections affines de $\mathbb{Z}/n\mathbb{Z}$ sur lui-même, c'est-à-dire des :

$$\gamma_{a,b} : \begin{array}{ccc} \mathbb{Z}/n\mathbb{Z} & \longrightarrow & \mathbb{Z}/n\mathbb{Z} \\ x & \mapsto & ax + b \end{array} \quad \text{où} \quad a \in \mathbb{Z}/n\mathbb{Z}^* \text{ et } b \in \mathbb{Z}/n\mathbb{Z}.^6$$

Proposition 3. *Sous les hypothèses précédentes, $\text{Gal}(\mathbb{L}/\mathbb{K})$ est isomorphe à un sous-groupe de $\text{Aff}(\mathbb{Z}/n\mathbb{Z})$; il est isomorphe à $\text{Aff}(\mathbb{Z}/n\mathbb{Z})$ si et seulement si le n -ième polynôme cyclotomique Φ_n est irréductible sur \mathbb{K} et $X^n - a$ est irréductible sur $\mathbb{K}(\varepsilon)$.*

Preuve. Montrons d'abord que $\text{Gal}(\mathbb{L}/\mathbb{K})$ est isomorphe à un sous-groupe de $\text{Aff}(\mathbb{Z}/n\mathbb{Z})$.

Si σ appartient à $\text{Gal}(\mathbb{L}/\mathbb{K})$, $\sigma(\alpha)$ est de la forme $\varepsilon^i \alpha$, $i \in \mathbb{Z}/n\mathbb{Z}$, et $\sigma(\varepsilon)$ est de la forme ε^j avec $j \in \mathbb{Z}/n\mathbb{Z}^*$ (abus de langage évident). De plus, σ est déterminé par $\sigma(\alpha)$ et $\sigma(\varepsilon)$, donc par i et j . On a ainsi défini une application injective de $\text{Gal}(\mathbb{L}/\mathbb{K})$ dans l'ensemble produit $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}^*$.

Reste à voir que cette application est un morphisme de $\text{Gal}(\mathbb{L}/\mathbb{K})$ dans $\text{Aff}(\mathbb{Z}/n\mathbb{Z})$. Pour cela, soient σ dans $\text{Gal}(\mathbb{L}/\mathbb{K})$ et σ' l'élément de $\text{Gal}(\mathbb{L}/\mathbb{K})$ donné par

$$\sigma'(\alpha) = \varepsilon^{i'} \alpha, \quad i' \in \mathbb{Z}/n\mathbb{Z} \quad \sigma'(\varepsilon) = \varepsilon^{j'}, \quad j' \in \mathbb{Z}/n\mathbb{Z}^*.$$

Le calcul suivant complète la démonstration :

$$\begin{aligned} \sigma' \circ \sigma(\varepsilon) &= \sigma'(\varepsilon^j) = (\sigma'(\varepsilon))^j \\ \sigma' \circ \sigma(\alpha) &= \sigma'(\varepsilon^i \alpha) = (\sigma'(\varepsilon))^i \sigma'(\alpha) = \varepsilon^{ij'+i'} \alpha. \end{aligned}$$

5. Dans les applications de la proposition 2, il peut être utile de connaître la structure de $(\mathbb{Z}/n\mathbb{Z}^*)^*$. Gauss a élucidé cette structure. Donnons sans démonstration le résultat pour n puissance d'un nombre premier, cas auquel on peut se ramener via l'isomorphisme chinois. Soient donc p un nombre premier, r un élément de \mathbb{N}^* . Si $p \geq 3$, $(\mathbb{Z}/p^r\mathbb{Z})^*$ est cyclique de cardinal $\varphi(p^r) = p^{r-1}(p-1)$. Si $p = 2$, $(\mathbb{Z}/2^r\mathbb{Z})^*$ est cyclique pour r valant 1 ou 2; si $r \geq 3$, la classe de 3 est un élément d'ordre 2^{r-2} et le sous-groupe engendré par cette classe ne contient pas la classe de -1 , d'où l'on déduit aisément que $(\mathbb{Z}/2^r\mathbb{Z})^*$ est isomorphe au groupe $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{r-2}\mathbb{Z}$.

6. Le lecteur savant notera que le groupe $\text{Aff}(\mathbb{Z}/n\mathbb{Z})$ est produit semi-direct du sous-groupe normal $T(\mathbb{Z}/n\mathbb{Z}) = \{\gamma_{1,b}; b \in \mathbb{Z}/n\mathbb{Z}\}$ des translations par le sous-groupe $H(\mathbb{Z}/n\mathbb{Z}) = \{\gamma_{a,0}; a \in \mathbb{Z}/n\mathbb{Z}^*\}$ des homothéties; il est en particulier résoluble.

Pour la seconde assertion, on part des inclusions :

$$\mathbb{K} \subset \mathbb{K}(\varepsilon) \subset \mathbb{L}.$$

Le groupe $\text{Gal}(\mathbb{L}/\mathbb{K})$ soit isomorphe à $\text{Aff}(\mathbb{Z}/n\mathbb{Z})$, si et seulement si

$$[\mathbb{L} : \mathbb{K}] = n\varphi(n).$$

Or, on a l'inégalité

$$[\mathbb{K}(\varepsilon) : \mathbb{K}] \leq \varphi(n),$$

qui est une égalité si et seulement si Φ_n est irréductible sur \mathbb{K} , tandis que

$$[\mathbb{K}(\varepsilon, \alpha) : \mathbb{K}(\varepsilon)] \leq n$$

avec égalité si et seulement si $X^n - a$ est irréductible sur $\mathbb{K}(\varepsilon)$.

Corps finis

Soient p un nombre premier, q une puissance de p et n dans \mathbb{N}^* . On a :

$$\mathbb{F}_{q^n} = D_{\mathbb{F}_q}(X^{q^n} - X),$$

et $X^{q^n} - X$ est séparable. L'extension $\mathbb{F}_{q^n}/\mathbb{F}_q$ est donc galoisienne. Son groupe de Galois est donné par le résultat suivant.

Proposition 4. *Le groupe $\text{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$ est cyclique d'ordre n ; il est engendré par l'automorphisme de Frobenius :*

$$\text{Frob}_{\mathbb{F}_{q^n}/\mathbb{F}_q} : \begin{array}{ccc} \mathbb{F}_{q^n} & \rightarrow & \mathbb{F}_{q^n} \\ x & \mapsto & x^q \end{array}.$$

Preuve. Car $\text{Frob}_{\mathbb{F}_{q^n}/\mathbb{F}_q}$ est un élément d'ordre n de $\text{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$, lequel est de cardinal n .

Exercice 19. ③ *Soient p un nombre premier impair, δ un élément de \mathbb{F}_p qui n'est pas un carré, $\sqrt{\delta}$ une de ses racines carrées dans \mathbb{F}_{p^2} . Montrer*

$$\forall (a, b) \in \mathbb{F}_p^2, \quad (a + b\sqrt{\delta})^p = a - b\sqrt{\delta}.$$

Exercice 20. ④ *Soient \mathbb{K} un corps de caractéristique différente de 2, \mathbb{L}/\mathbb{K} une extension, u_1, \dots, u_m des éléments de \mathbb{K}^* ayant des racines carrées notées respectivement $\sqrt{u_1}, \dots, \sqrt{u_m}$ dans \mathbb{L} . On pose $\mathbb{K}^{*2} = \{x^2, x \in \mathbb{K}^*\}$. On suppose que $[\mathbb{K}(\sqrt{u_1}, \dots, \sqrt{u_m}) : \mathbb{K}] = 2^m$, c'est-à-dire (chapitre 2, 3.2, exercice 35) que :*

$$\forall (\alpha_1, \dots, \alpha_m) \in \mathbb{Z}^m, \quad u_1^{\alpha_1} \times \dots \times u_m^{\alpha_m} \in \mathbb{K}^{*2} \iff \forall i \in \{1, \dots, m\}, 2 \mid \alpha_i.$$

Montrer que $\text{Gal}(\mathbb{K}(\sqrt{u_1}, \dots, \sqrt{u_m})/\mathbb{K})$ est isomorphe à $(\mathbb{Z}/2\mathbb{Z})^m$.

1.5 Changement d'extension

Le théorème 2 de 1.3 assure que, si \mathbb{L}/\mathbb{K} est galoisienne et si \mathbb{K}' est un sous-corps de \mathbb{L} contenant \mathbb{K} , alors \mathbb{L}/\mathbb{K}' est galoisienne et $\text{Gal}(\mathbb{L}/\mathbb{K}')$ est un sous-groupe de $\text{Gal}(\mathbb{L}/\mathbb{K})$. Les énoncés de ce paragraphe décrivent comment se comporte le groupe de Galois dans deux autres situations.

Proposition 5. *Supposons \mathbb{L}/\mathbb{K} galoisienne finie, soit \mathbb{K}' un sous-corps de \mathbb{L} contenant \mathbb{K} et normal (donc galoisien) sur \mathbb{K} . Soit*

$$\begin{array}{ccc} \rho : \text{Gal}(\mathbb{L}/\mathbb{K}) & \rightarrow & \text{Gal}(\mathbb{K}'/\mathbb{K}) \\ \sigma & \mapsto & \sigma|_{\mathbb{K}'} \end{array}$$

le morphisme de restriction. Alors ρ est surjectif de noyau $\text{Gal}(\mathbb{L}/\mathbb{K}')$. En particulier, le quotient $\text{Gal}(\mathbb{L}/\mathbb{K})/\text{Gal}(\mathbb{L}/\mathbb{K}')$ est isomorphe à $\text{Gal}(\mathbb{K}'/\mathbb{K})$.

Preuve. Le caractère normal de l'extension \mathbb{K}'/\mathbb{K} justifie la définition de ρ . La surjectivité de ρ vient du caractère normal de \mathbb{L}/\mathbb{K} et de la possibilité de prolonger les morphismes.

La proposition suivante montre que, lorsqu'on adjoint aux deux corps d'une extension les mêmes éléments⁷, le groupe de la nouvelle extension est un sous-groupe de celui de l'extension initiale.

Proposition 6. *Supposons \mathbb{L}/\mathbb{K} galoisienne finie, soit \mathbb{F} un sous-corps de Ω . L'extension $\mathbb{L}\mathbb{F}/\mathbb{K}\mathbb{F}$ est galoisienne, son groupe est isomorphe à un sous-groupe de $\text{Gal}(\mathbb{L}/\mathbb{K})$. En particulier, $[\mathbb{L}\mathbb{F} : \mathbb{K}\mathbb{F}]$ divise $[\mathbb{L} : \mathbb{K}]$.*

Preuve. Écrivons $\mathbb{L} = \mathbb{D}_{\mathbb{K}}P$ avec $P \in \mathbb{K}[X]$ séparable. Alors $\mathbb{L}\mathbb{F} = \mathbb{D}_{\mathbb{K}\mathbb{F}}P$ et $\mathbb{L}\mathbb{F}/\mathbb{K}\mathbb{F}$ est galoisienne finie. De plus, le morphisme de restriction :

$$\begin{array}{ccc} \rho : \text{Gal}(\mathbb{L}\mathbb{F}/\mathbb{K}\mathbb{F}) & \rightarrow & \text{Gal}(\mathbb{L}/\mathbb{K}) \\ \sigma & \mapsto & \sigma|_{\mathbb{L}} \end{array}$$

est bien défini puisque \mathbb{L}/\mathbb{K} est normale. Ce morphisme est injectif ; en effet, si σ est dans $\text{Ker}(\rho)$, on a :

$$\sigma|_{\mathbb{L}} = \text{id}_{\mathbb{L}} \quad \text{et} \quad \sigma|_{\mathbb{F}} = \text{id}_{\mathbb{F}},$$

ce qui entraîne $\sigma = \text{id}_{\mathbb{L}\mathbb{F}}$.

Si l'extension \mathbb{L}/\mathbb{K} n'est pas galoisienne, on a seulement l'inégalité évidente

$$[\mathbb{L}\mathbb{F} : \mathbb{K}\mathbb{F}] \leq [\mathbb{L} : \mathbb{K}].$$

On en a un exemple avec : $\mathbb{K} = \mathbb{Q}$, $\mathbb{L} = \mathbb{Q}(\sqrt[3]{2})$ et $\mathbb{F} = \mathbb{Q}(j\sqrt[3]{2})$.

La dernière proposition renseigne sur le groupe d'une composée.

Proposition 7. *Soient \mathbb{L}_1 et \mathbb{L}_2 deux sous-corps de Ω , extensions galoisiennes finies de \mathbb{K} . L'extension $\mathbb{L}_1\mathbb{L}_2/\mathbb{K}$ est galoisienne, de groupe isomorphe à un sous-groupe de $\text{Gal}(\mathbb{L}_1/\mathbb{K}) \times \text{Gal}(\mathbb{L}_2/\mathbb{K})$.*

Preuve. La normalité (resp. séparabilité) de $\mathbb{L}_1\mathbb{L}_2/\mathbb{K}$ provient de celles de \mathbb{L}_1/\mathbb{K} et \mathbb{L}_2/\mathbb{K} . On considère alors :

$$\begin{array}{ccc} \rho : \text{Gal}(\mathbb{L}_1\mathbb{L}_2/\mathbb{K}) & \rightarrow & \text{Gal}(\mathbb{L}_1/\mathbb{K}) \times \text{Gal}(\mathbb{L}_2/\mathbb{K}) \\ \sigma & \mapsto & (\sigma|_{\mathbb{L}_1}, \sigma|_{\mathbb{L}_2}) \end{array}.$$

L'application ρ est un morphisme de groupes, injectif parce qu'un élément de $\text{Gal}(\mathbb{L}_1\mathbb{L}_2/\mathbb{K})$ est déterminé par ses restrictions à \mathbb{L}_1 et \mathbb{L}_2 .

Exercice 21. ③ *Que subsiste-t-il des propositions 6 et 7 si on supprime les hypothèses de finitude ?*

Exercice 22. ① *On reprend les notations de la proposition 7. Montrer que ρ est un isomorphisme si et seulement si les extensions \mathbb{L}_1/\mathbb{K} et \mathbb{L}_2/\mathbb{K} sont linéairement disjointes, i.e. si*

$$[\mathbb{L}_1\mathbb{L}_2 : \mathbb{K}] = [\mathbb{L}_1 : \mathbb{K}] [\mathbb{L}_2 : \mathbb{K}].$$

7. Classiquement nommés « irrationalités naturelles », car adjoints aux deux corps.

Exercice 23. ④ On reprend les notations de la proposition 7. On suppose que le corps \mathbb{K} est de caractéristique 0 et que $\mathbb{L}_1 \cap \mathbb{L}_2 = \mathbb{K}$. Soit x (resp. y) un élément primitif de \mathbb{L}_1/\mathbb{K} (resp. \mathbb{L}_2/\mathbb{K}). Montrer que $x + y$ est un élément primitif de $\mathbb{L}_1\mathbb{L}_2/\mathbb{K}$. On considèrera un élément σ de $\text{Gal}(\mathbb{L}_1\mathbb{L}_2/\mathbb{K})$ fixant $x + y$ et on montrera que

$$\sigma(x) - x = y - \sigma(y)$$

est dans \mathbb{K} , puis que σ est l'identité de $\mathbb{L}_1\mathbb{L}_2$.

Exercice 24. ④ On reprend les notations de la proposition 7. On suppose que $[\mathbb{L}_1 : \mathbb{K}]$ et $[\mathbb{L}_2 : \mathbb{K}]$ sont premiers entre eux. Soit x (resp. y) un élément primitif de \mathbb{L}_1/\mathbb{K} (resp. \mathbb{L}_2/\mathbb{K}). Montrer que xy est un élément primitif de $\mathbb{L}_1\mathbb{L}_2/\mathbb{K}$. On considèrera un élément σ de $\text{Gal}(\mathbb{L}_1\mathbb{L}_2/\mathbb{K})$ fixant xy et on montrera que σ est l'identité de $\mathbb{L}_1\mathbb{L}_2$.

2 Groupe de Galois d'un polynôme

On revient ici au point de vue de Lagrange et Galois. On fixe un polynôme non constant P de $\mathbb{K}[X]$, dont on note x_1, \dots, x_n les racines distinctes dans Ω . On définit le *groupe de Galois de P sur \mathbb{K}* , que l'on identifie à un groupe de permutations de l'ensemble $\mathcal{R} = \{x_i ; 1 \leq i \leq n\}$ des racines de P .

Le paragraphe 2.1 est essentiel. Les paragraphes 2.2 et 2.3 présentent des applications très classiques. Le paragraphe 2.4, de nature assez différente, peut être réservé à une seconde lecture : étant donné un polynôme unitaire P de $\mathbb{Z}[X]$ et un nombre premier p , on étudie le lien entre le groupe de Galois de P sur \mathbb{Q} et le groupe de Galois de la réduction de P modulo p sur \mathbb{F}_p .

2.1 Action du groupe de Galois sur les racines

On appelle *groupe de Galois de P sur \mathbb{K}* ou simplement *groupe de P sur \mathbb{K}* et on note $\text{Gal}_{\mathbb{K}}P$ le groupe $\text{Gal}(\mathbb{D}_{\mathbb{K}}P/\mathbb{K})$. La définition en termes d'extension est plus intrinsèque : un même sous-corps de Ω peut être corps de décomposition de nombreux polynômes de $\mathbb{K}[X]$.

L'intérêt du point de vue des polynômes est qu'il permet de faire agir $\text{Gal}_{\mathbb{K}}P$ sur \mathcal{R} . En effet, si $\sigma \in \text{Gal}_{\mathbb{K}}P$, $\sigma(x_i)$ est un des x_j . Comme σ est déterminé par son action sur \mathcal{R} , on obtient ainsi une action fidèle de $\text{Gal}_{\mathbb{K}}P$ sur \mathcal{R} , c'est-à-dire un morphisme injectif de $\text{Gal}_{\mathbb{K}}P$ dans \mathcal{R} . (C'est la première moitié du résultat ci-après.

Théorème 4. (i) L'action sur les racines de P identifie $\text{Gal}_{\mathbb{K}}P$ à un sous-groupe de $\mathcal{S}(\mathcal{R})$.

(ii) Soient $P = \prod_{i=1}^r P_i$ la factorisation de P en produit d'irréductibles de $\mathbb{K}[X]$. Pour $i \in \{1, \dots, r\}$, soit R_i l'ensemble des racines de P_i dans Ω . Chaque ensemble R_i est stable par $\text{Gal}_{\mathbb{K}}P$, et $\text{Gal}_{\mathbb{K}}P$ agit transitivement sur R_i .

En particulier, P est irréductible si et seulement si l'action de $\text{Gal}_{\mathbb{K}}P$ sur \mathcal{R} est transitive. Si tel est le cas, le degré de P divise $|\text{Gal}_{\mathbb{K}}P|$.

Preuve de (ii). La stabilité de R_i par $\text{Gal}_{\mathbb{K}}P$ est claire. Pour le second point, on prend x et y dans R_i . Puisque $\Pi_{\mathbb{K},x} = \Pi_{\mathbb{K},y} = P_i$, x et y sont \mathbb{K} -conjugués, et il existe σ dans $\text{Gal}_{\mathbb{K}}P$ tel que $\sigma(x) = y$. Pour terminer, on se rappelle que, dans une action d'un groupe fini G , le cardinal d'une orbite divise $|G|$.

Remarques et exemples

1. Comment se ramener au cas séparable ?

Dans le cas où le corps de base est parfait, donc en particulier si \mathbb{K} est de caractéristique nulle ou fini, on peut ramener le groupe de Galois d'un polynôme à celui d'un polynôme séparable de la manière suivante. Factorisons P dans $\mathbb{K}[X]$:

$$P = \prod_{i=1}^r P_i^{n_i}$$

où les P_i est sont des irréductibles de $\mathbb{K}[X]$ deux à deux non associés et les n_i des éléments de \mathbb{N}^* . On note alors que les P_i sont à racines simples et que le radical R de P , défini par $R = \prod_{i=1}^r P_i$ a même ensemble de racines dans Ω que P et est dans $\mathbb{K}[X]$ car $R = \frac{P}{P \wedge P'}$.

2. Le groupe de Galois vu comme un sous-groupe de \mathcal{S}_n

Pour i dans $\{1, \dots, n\}$ et σ dans $\text{Gal}_{\mathbb{K}}P$, notons $x_{\tilde{\sigma}(i)} = \sigma(x_i)$. Comme σ est injectif, $\tilde{\sigma}$ est dans \mathcal{S}_n et l'application qui à $\sigma \in \text{Gal}_{\mathbb{K}}P$ associe $\tilde{\sigma}$ est injective.

En général, on identifie σ et $\tilde{\sigma}$. La représentation de $\text{Gal}_{\mathbb{K}}P$ comme sous-groupe de \mathcal{S}_n (i.e., l'application $\sigma \mapsto \tilde{\sigma}$) dépend cependant de la numérotation des racines. Un changement de numérotation revenant à une conjugaison dans \mathcal{S}_n , l'image de $\text{Gal}_{\mathbb{K}}P$ dans \mathcal{S}_n n'est définie qu'à conjugaison près. Un sous-groupe H de \mathcal{S}_n étant fixé, on cherchera donc à savoir si $\text{Gal}_{\mathbb{K}}P$ est contenu dans un conjugué de H .⁸

3. Une reformulation

En tant que groupe de permutations, $\text{Gal}_{\mathbb{K}}P$ apparaît comme le sous-groupe formé des permutations qui préservent les relations algébriques entre les racines, c'est-à-dire des $\sigma \in \mathcal{S}_n$ telles que :

$$\forall Q \in \mathbb{K}[X_1, \dots, X_n], \quad Q(x_1, \dots, x_n) = 0 \Rightarrow Q(x_{\sigma(1)}, \dots, x_{\sigma(n)}) = 0.$$

Cette propriété signifie en effet que la permutation $x_i \mapsto x_{\sigma(i)}$ se prolonge en un élément de $\text{Gal}_{\mathbb{K}}P$.

4. Polynômes réciproques

Le groupe de Galois d'un polynôme en reflète les symétries. Illustrons ce point en examinant le cas d'un polynôme réciproque séparable P de degré $2n$, $n \in \mathbb{N}^*$. Les racines de P dans Ω se répartissent en n parties $\mathcal{R}_i = \{x_i, 1/x_i\}$, avec $1 \leq i \leq n$. Si σ est un élément de $\text{Gal}_{\mathbb{K}}P$, σ permute les \mathcal{R}_i . Notons $\mathcal{B} = \{\mathcal{R}_1, \dots, \mathcal{R}_n\}$. On a donc un morphisme de $\text{Gal}_{\mathbb{K}}P$ dans $\mathcal{S}(\mathcal{B})$, c'est-à-dire dans \mathcal{S}_n , dont le noyau est formé des éléments de $\text{Gal}_{\mathbb{K}}P$ qui stabilisent chaque \mathcal{R}_i . Le cardinal du noyau divise 2^n , donc l'ordre de $\text{Gal}_{\mathbb{K}}P$ divise $2^n n!$.⁹

5. Groupe d'un polynôme irréductible séparable de degré 3

Si P est de degré 3 sur \mathbb{K} , l'action sur les racines identifie $\text{Gal}_{\mathbb{K}}P$ à un sous-groupe de \mathcal{S}_3 ; si P est irréductible, ce groupe est isomorphe soit à \mathcal{A}_3 soit à \mathcal{S}_3 selon que $[D_{\mathbb{K}}P : \mathbb{K}]$ vaut 3 ou 6. Nous précisons la situation plus loin. Mais notons déjà que $\text{Gal}_{\mathbb{Q}}(X^3 - 2)$ n'est autre que \mathcal{S}_3 (par exemple puisque $D_{\mathbb{Q}}(X^3 - 2) = \mathbb{Q}(j, \sqrt[3]{2})$ est de degré 6 sur \mathbb{Q}).

6. Groupe de $X^4 - 2$ sur \mathbb{Q}

8. Cette ambiguïté disparaît si H est normal dans \mathcal{S}_n .

9. L'argument donne plus que ce renseignement numérique. Les notions d'action primitive, de blocs et de produit en couronne de groupes de permutations donnent un cadre général pour exprimer ce type de phénomène.

La proposition 3 montre que $\text{Gal}_{\mathbb{Q}}(X^4 - 2)$ est isomorphe à $\text{Aff}(\mathbb{Z}/4\mathbb{Z})$; redémontrons directement que ce groupe est isomorphe au groupe diédral \mathcal{D}_4 . Le corps $\mathbb{K} = \mathbb{Q}(i, \sqrt[4]{2})$ est un corps de décomposition de $X^4 - 2$ sur \mathbb{Q} . Puisque $\sqrt[4]{2}$ est de degré 4 sur \mathbb{Q} et i de degré 2 sur $\mathbb{Q}(\sqrt[4]{2})$, on a : $[K : \mathbb{Q}] = 8$. Soit $G = \text{Gal}(K/\mathbb{Q})$. La conjugaison complexe induit un élément τ d'ordre 2 de G . Puisque $\sqrt[4]{2}$ est de degré 4 sur $\mathbb{Q}(i)$, les $\mathbb{Q}(i)$ -conjugués de $\sqrt[4]{2}$ sont ses \mathbb{Q} -conjugués, d'où σ dans G fixant i et envoyant $\sqrt[4]{2}$ sur $i\sqrt[4]{2}$. Ainsi σ et τ sont deux éléments de G d'ordres respectifs 4 et 2; comme $\tau \notin \langle \sigma \rangle$, on a : $G = \langle \sigma, \tau \rangle$. En identifiant τ à la réflexion orthogonale d'axe Ox et σ à la rotation d'angle $\pi/2$, on obtient un isomorphisme de G sur le groupe \mathcal{D}_4 dans sa réalisation usuelle de groupe d'isométries planes.

7. *Groupe de $X^p - a$ sur \mathbb{Q}*

Soient p un nombre premier, a un rationnel qui n'est pas une puissance p -ième dans \mathbb{Q} . Il découle de la proposition 3 et de l'irréductibilité sur \mathbb{Q} des polynômes $X^p - a$ et Φ_p (premier exposé) que $\text{Gal}_{\mathbb{Q}}(X^p - a)$ est isomorphe à $\text{Aff}(\mathbb{F}_p)$.

8. *La conjugaison complexe comme permutation des racines*

Soient \mathbb{K} un sous-corps de \mathbb{R} , $P \in \mathbb{K}[X]$ un polynôme séparable de degré $n \geq 1$, \mathcal{R} l'ensemble des racines de P dans \mathbb{C} , $G = \text{Gal}_{\mathbb{K}}P$. Notons $2m$ le cardinal de $\mathcal{R} \cap (\mathbb{C} \setminus \mathbb{R})$. La conjugaison complexe est un élément de G . La permutation de \mathcal{R} qu'elle induit est le produit de m transpositions à supports disjoints.

9. *Polynômes irréductibles de degré premier*

Soient p un nombre premier, P un polynôme irréductible séparable de degré p de $\mathbb{K}[X]$. Puisque $|\text{Gal}_{\mathbb{K}}P|$ est divisible par p , le lemme de Cauchy montre que ce groupe contient un élément d'ordre p . Cet élément agit comme un p -cycle sur l'ensemble des racines. Cet argument est une première application non triviale de la théorie des groupes.

10. *Réalisation de \mathcal{S}_p comme groupe de Galois sur \mathbb{Q} pour p premier*

Soient \mathbb{K} un sous-corps de \mathbb{C} , p un nombre premier, P un irréductible de degré p de $\mathbb{K}[X]$ admettant $p - 2$ racines réelles et 2 racines irréelles conjuguées. Grâce à l'item précédent, le groupe $\text{Gal}_{\mathbb{K}}P$, vu comme groupe de permutations des racines, contient une transposition d'après la remarque 8, un p -cycle d'après la remarque 9. Le lemme suivant entraîne que $\text{Gal}_{\mathbb{K}}P$ est isomorphe à \mathcal{S}_p .

Lemme 2. *Soient p un nombre premier, G un sous-groupe de \mathcal{S}_p contenant une transposition τ et un p -cycle γ . Alors $G = \mathcal{S}_p$.*

Preuve. On peut supposer $\tau = (1, 2)$. Une puissance de c envoie 1 sur 2; remplaçant c par cette puissance et conjuguant G par une permutation fixant 1 et 2 convenable, on peut supposer aussi $\gamma = (1, 2, \dots, p)$. En conjuguant τ par les puissances de γ , on voit alors que les transpositions $(1, 2), (2, 3), \dots, (p - 1, p)$ sont dans G . Or ces transpositions forment un système générateur de \mathcal{S}_p , d'où le résultat.

Exemple. Soient q un nombre premier, $P_q = X^5 - q^2X - q$. Le critère d'Eisenstein montre que P_q est irréductible sur \mathbb{Q} . Une étude de fonctions laissée au lecteur montre que P_q admet exactement trois racines réelles. Il s'ensuit que $\text{Gal}_{\mathbb{Q}}P$ s'identifie à \mathcal{S}_5 .

Exercice 25. ② *Démontrer l'assertion du théorème selon laquelle n divise $|\text{Gal}_{\mathbb{K}}P|$ si P est irréductible à l'aide de la multiplicativité des degrés.*

Exercice 26. ② *Soit $P \in \mathbb{K}[X]$ un polynôme séparable. Soit Q un diviseur de P dans $\mathbb{K}[X]$. Vérifier que $|\text{Gal}_{\mathbb{K}}Q|$ est un quotient de $|\text{Gal}_{\mathbb{K}}P|$.*

Exercice 27. ② Retrouver que, si P est un polynôme séparable de degré n de $\mathbb{K}[X]$, alors $[D_{\mathbb{K}}(P) : \mathbb{K}]$ divise $n!$. Que se passe-t-il si P n'est pas séparable ?

Exercice 28. ② Soit $P = X^5 - 6X + 3$. Montrer, en appliquant l'exemple 8, que $\text{Gal}_{\mathbb{Q}}P$ est isomorphe à S_5 .

Exercice 29. ③ Soient $\alpha = \sqrt{5 + \sqrt{21}}$, $\beta = \sqrt{5 - \sqrt{21}}$.

a) Calculer $\alpha\beta$ et en déduire que l'extension $\mathbb{Q}(\alpha)/\mathbb{Q}$ est galoisienne. Quel est son degré ?

b) Montrer que le groupe de Galois de l'extension précédente est isomorphe à $\mathbb{Z}/2\mathbb{Z}^2$.

c) Déterminer les sous-corps de $\mathbb{Q}(\alpha)$ de degré 2 sur \mathbb{Q} . On écrira chacun de ces corps sous la forme $\mathbb{Q}(\sqrt{a})$ avec $a \in \mathbb{N}^*$. On pourra écrire α sous la forme $\sqrt{u} + \sqrt{v}$ avec u et v dans \mathbb{Q} .

Exercice 30. ⑤ On suppose que \mathbb{K} est de caractéristique différente de 2. Soit $P = X^4 + aX^2 + b$ un irréductible de $\mathbb{K}[X]$.

a) Montrer que $\text{Gal}_{\mathbb{K}}(P)$ s'identifie à un sous-groupe de \mathcal{D}_4 .

b) Montrer que $\text{Gal}_{\mathbb{K}}(P)$ est isomorphe à l'un des groupes \mathcal{D}_4 , $\mathbb{Z}/4\mathbb{Z}$ ou $(\mathbb{Z}/2\mathbb{Z})^2$.

c) Décrire $\text{Gal}_{\mathbb{K}}(P)$ par des conditions explicites sur (a, b) .

Exercice 31. ③ Soit P un polynôme réciproque séparable de degré $2n$ de $\mathbb{K}[X]$. Démontrer directement à partir de la définition de $D_{\mathbb{K}}P$ que $[D_{\mathbb{K}}P : \mathbb{K}]$ divise $n! 2^n$.

Exercice 32. ④ Soit $m \geq 2$ un entier. Supposons que la caractéristique de \mathbb{K} ne divise pas m . Soit P un élément de $\mathbb{K}[X^m]$, séparable sur \mathbb{K} . Que dire de $\text{Gal}_{\mathbb{K}}P$?

Exercice 33. ③ Si \mathbb{K} est un corps de caractéristique nulle, n un entier supérieur ou égal à 4 et $a \in \mathbb{K}^*$, montrer que $\text{Gal}_{\mathbb{K}}(X^n - a)$ s'identifie par l'action sur les racines à un sous-groupe strict de \mathcal{S}_n .

Exercice 34. ④ Construire, si p est premier, un polynôme de degré p de $\mathbb{Q}[X]$ dont le groupe de Galois est isomorphe à \mathcal{S}_p .

L'exercice ci-après propose la détermination du groupe de Galois d'un polynôme d'Artin-Schreier (chapitre 1, 2.2, exercice 24).

Exercice 35. ④ Soient p un nombre premier, \mathbb{K} un corps de caractéristique p et a un élément de \mathbb{K} tel que $X^p - X - a$ n'ait pas de racine dans \mathbb{K} . Montrer que $\text{Gal}_{\mathbb{K}}P$ est cyclique d'ordre p .

Exercice 36. ④ Le corps \mathbb{K} est de caractéristique $p > 0$. Soient $\mathbb{L} = \mathbb{K}(s, t)$ où s et t sont algébriquement indépendants sur \mathbb{K} , et

$$P = X^p - sX - t \in \mathbb{L}[X].$$

Montrer que P est irréductible sur \mathbb{L} et séparable, que $\text{Gal}_{\mathbb{L}}(P)$ est isomorphe au groupe $\text{Aff}(\mathbb{F}_p)$.

Exercice 37. ⑤ Soit P un irréductible de $\mathbb{Q}[X]$ de degré premier p . Soient x_0, \dots, x_{p-1} les racines de P dans \mathbb{C} . Quitte à renuméroter les x_i , on peut supposer que $\text{Gal}_{\mathbb{Q}}P$ contient un élément qui induit sur l'ensemble \mathcal{R} des racines de P le p -cycle $(x_0, x_1, \dots, x_{p-1})$. Soient $\lambda_0, \dots, \lambda_{p-1}$ des rationnels tels que

$$y = \sum_{i=0}^{p-1} \lambda_i x_i \in \mathbb{Q}.$$

Que peut-on dire des λ_i ? On pourra utiliser la matrice circulante C de première ligne $(\lambda_0, \dots, \lambda_{p-1})$.

2.2 L'équation générale de degré n

Soient X_1, \dots, X_n des indéterminées (c'est-à-dire des éléments algébriquement indépendants sur \mathbb{K}), $\mathbb{K}_X = \mathbb{K}(X_1, \dots, X_n)$ le corps des fractions rationnelles en les X_i . Le *polynôme général de degré n* relatif à \mathbb{K} est le polynôme en l'indéterminée T :

$$P = \prod_{i=1}^n (T - X_i).$$

Ce polynôme est à coefficients dans le corps $\mathbb{K}_\Sigma = \mathbb{K}(\Sigma_1, \dots, \Sigma_n)$ où $\Sigma_1, \dots, \Sigma_n$ sont les fonctions symétriques élémentaires. Il est séparable.

Grâce à l'indépendance algébrique de X_1, \dots, X_n , le groupe symétrique \mathcal{S}_n agit naturellement sur \mathbb{K}_X par permutation des X_i , i.e. par :

$$\forall (\sigma, F) \in \mathcal{S}_n \times \mathbb{K}_X, \quad \sigma.F(X_1, \dots, X_n) = F(X_{\sigma(1)}, \dots, X_{\sigma(n)}).$$

Le groupe \mathcal{S}_n se réalise ainsi comme sous-groupe de $\text{Aut}(\mathbb{K}_X)$ et même, puisque les Σ_i sont invariantes sous l'action précédente, de $\text{Gal}(\mathbb{K}_X/\mathbb{K}_\Sigma)$. Autrement dit, le groupe de Galois est aussi gros que possible, c'est-à-dire égal à \mathcal{S}_n .

Proposition 8. *Le groupe de Galois du polynôme général de degré n à coefficients dans \mathbb{K} sur le sous-corps engendré sur \mathbb{K} par les fonctions symétriques élémentaires est le groupe \mathcal{S}_n .*

Remarque Application aux polynômes symétriques

En utilisant la caractérisation du corps de base d'une extension galoisienne finie, on déduit du résultat précédent le « théorème des fractions symétriques » : les éléments F de \mathbb{K}_X tels que

$$\forall \sigma \in \mathcal{S}_n, \quad \sigma.F = F$$

sont les éléments de \mathbb{K}_Σ .

Des arguments simples d'intégralité permettent d'en tirer le théorème des polynômes symétriques. Voici comment. On veut établir :

$$\mathbb{K}[X_1, \dots, X_n] \cap \mathbb{K}(\Sigma_1, \dots, \Sigma_n) = \mathbb{K}[\Sigma_1, \dots, \Sigma_n].$$

Puisque $\mathbb{K}[X_1, \dots, X_n]$ est entier sur $\mathbb{K}[\Sigma_1, \dots, \Sigma_n]$, il suffit de montrer que $\mathbb{K}[\Sigma_1, \dots, \Sigma_n]$ est intégralement clos. Mais puisque $\Sigma_1, \dots, \Sigma_n$ sont algébriquement indépendants sur \mathbb{K} , les \mathbb{K} -algèbres $\mathbb{K}[X_1, \dots, X_n]$ et $\mathbb{K}[\Sigma_1, \dots, \Sigma_n]$ sont isomorphes.¹⁰

Cette démonstration, due à Artin, renverse le statut du théorème de structure des polynômes symétriques : au lieu d'être un prérequis à la théorie de Galois, il en devient une conséquence.

2.3 Signature des éléments du groupe de Galois

Soit $\Delta(P)$ le discriminant de P :

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

On sait depuis le chapitre 1 (4.3) que $\Delta(P) \in \mathbb{K}$. Nous allons retrouver et préciser ce point.

Notons $\sqrt{\Delta(P)}$ une racine carrée de $\Delta(P)$ dans $D_{\mathbb{K}}P$.¹¹ La définition de la signature par les inversions donne le :

10. En particulier, l'anneau $\mathbb{K}[\Sigma_1, \dots, \Sigma_n]$ est factoriel.

11. Abus de langage inoffensif pour la suite, puisque les deux racines carrées engendrent la même extension de \mathbb{K} .

Lemme 3. Si σ est un élément de $\text{Gal}_{\mathbb{K}}P$, on a :

$$\sigma\left(\sqrt{\Delta(P)}\right) = \varepsilon(\sigma)\sqrt{\Delta(P)}.$$

Ce calcul montre que $\Delta(P)$ est fixe par tout élément de $\text{Gal}_{\mathbb{K}}P$, donc appartient au corps \mathbb{K} , comme annoncé. Il permet également de déterminer si $\text{Gal}_{\mathbb{K}}P$ est constitué uniquement de permutations paires.

Proposition 9. *i) Le discriminant $\Delta(P)$ appartient à \mathbb{K} .*

ii) Si \mathbb{K} est de caractéristique différente de 2, $\text{Gal}_{\mathbb{K}}P$ est contenu dans \mathcal{A}_n si et seulement si $\Delta(P)$ est un carré dans \mathbb{K} .¹² Dans le cas contraire, $\mathbb{K}\left(\sqrt{\Delta(P)}\right)$ est une extension quadratique de \mathbb{K} contenue dans $D_{\mathbb{K}}P$.

Exemples

1. *Groupe de Galois d'un polynôme irréductible de degré 3, suite*

Reprenons l'exemple 5 de **2.1**. On a $[\mathbb{L} : \mathbb{K}] = 3$ si et seulement si $\Delta(P) = -4p^3 - 27q^2$ est un carré dans \mathbb{K} . Dans ce cas, $\text{Gal}_{\mathbb{K}}P$ est cyclique de cardinal 3 ; sinon $\text{Gal}_{\mathbb{K}}P$ est isomorphe à \mathcal{S}_3 .

On peut donner des résultats analogues pour les polynômes de degré 4,5,... Le treillis des sous-groupes de \mathcal{S}_n devient rapidement très complexe, ce qui limite ce genre d'énoncé à de petits degrés. La détermination du groupe de Galois d'un polynôme de degré 4, accessible au niveau de ce cours, demande déjà une analyse nettement plus délicate.

2. *Inclusion d'une extension quadratique de \mathbb{Q} dans un corps cyclotomique*

Si $\mathbb{K} = \mathbb{Q}$ et $P = X^n - 1$, on sait depuis le chapitre 1 (**4.3**) que

$$\Delta(P) = n^n (-1)^{(n-1)(n-2)/2}.$$

Conséquence arithmétique. Si n est impair, la classe de $\Delta(P)$ dans le quotient $\mathbb{Q}^*/(\mathbb{Q}^*)^2$ est celle de $n(-1)^{(n-1)/2}$. Puisque $\delta(P) \in \mathbb{Q}(e^{2i\pi/n})$, on en déduit que $n(-1)^{(n-1)/2}$ est un carré de $\mathbb{Q}(e^{2i\pi/n})$.

Soient maintenant $m \in \mathbb{Z}^*$, d le plus grand diviseur impair de m . On vient de voir que $\pm d$ est un carré de $\mathbb{Q}(e^{2i\pi/d})$. De plus, la classe de m dans $\mathbb{Q}^*/(\mathbb{Q}^*)^2$ est celle de l'un des quatre entiers $\pm d, \pm 2d$. Dans tous les cas, m est un carré dans $\mathbb{Q}(i, \sqrt{2}, e^{2i\pi/d})$. Or $\mathbb{Q}(e^{2i\pi/8}) = \mathbb{Q}(i, \sqrt{2})$. Il s'ensuit que m est un carré de $\mathbb{Q}(e^{2i\pi/(8d)})$. On en déduit que toute extension quadratique de \mathbb{Q} est contenue dans une extension cyclotomique.

Exercice 38. ② Soit $P = X^3 - X^2 - 2X + 1$. Vérifier que P est irréductible sur \mathbb{Q} . Si α, β, γ sont les racines de P dans \mathbb{C} , montrer l'égalité

$$\mathbb{Q}(\alpha) = \mathbb{Q}(\beta) = \mathbb{Q}(\gamma).$$

Exercice 39. ② Soit $P = X^3 - 4X + 2$. Déterminer $\text{Gal}_{\mathbb{Q}}P$, puis $\text{Gal}_{\mathbb{Q}(\sqrt{37})}P$.

Exercice 40. ② Montrer que toute extension multiquadratique de \mathbb{Q} est contenue dans une extension cyclotomique.

¹² Puisque \mathcal{A}_n est un sous-groupe normal de \mathcal{S}_n , ou, mieux, puisque l'on peut définir la signature d'une permutation d'un ensemble fini, cet énoncé n'est pas ambigu, cf note 8 de **4.1**.

Exercice 41. ② Supposons \mathbb{K} de caractéristique 2. Soient $P \in \mathbb{K}[X]$ non constant et séparable. On suppose $[D_{\mathbb{K}}P : \mathbb{K}]$ impair. Montrer que $\Delta(P)$ est un carré dans \mathbb{K} .

Exercice 42. ④ Supposons \mathbb{K} de caractéristique 2. Soient P un polynôme unitaire séparable de $\mathbb{K}[X]$. On écrit

$$P = \prod_{i=1}^n (X - x_i) \quad (x_1, \dots, x_n) \in \Omega^n.$$

On pose

$$a = \sum_{1 \leq i < j \leq n} \frac{x_i}{x_i + x_j} \quad b = \sum_{1 \leq i < j \leq n} \frac{x_i^2}{x_i + x_j}.$$

- Justifier les définitions de a et b . Montrer que b est dans \mathbb{K} , que $a^2 + a = b$.
- Montrer que $\sigma(b)$ vaut b ou $b+1$ selon que σ agit de façon paire ou impaire sur les racines.
- Montrer que $\text{Gal}_{\mathbb{K}}P$ est contenu dans \mathcal{A}_n si et seulement si b s'écrit $x^2 + x$ avec x dans \mathbb{K} .

Le cas des extensions cycliques

On peut préciser le théorème 4 pour les extensions cycliques.

Proposition 10. Soit P un polynôme séparable de $\mathbb{K}[X]$. Notons $P = \prod_{i=1}^r P_i$ la factorisation de P en irréductibles de $\mathbb{K}[X]$, \mathcal{R}_i l'ensemble des racines de P_i dans Ω , $n_i = |\mathcal{R}_i| = \deg P_i$ et supposons $\text{Gal}_{\mathbb{K}}P$ cyclique engendré par γ .

Alors, pour tout i , γ induit un n_i -cycle sur \mathcal{R}_i .

Preuve. D'après le théorème 4, γ stabilise \mathcal{R}_i et l'action de $\langle \gamma \rangle$ sur \mathcal{R}_i est transitive, ce qui implique bien que γ induit un n_i -cycle sur \mathcal{R}_i .

Voici comment se traduit cette proposition pour les corps finis.

Corollaire 1. Soient p un nombre premier $r \in \mathbb{N}^*$, $q = p^r$, P un polynôme séparable de $\mathbb{F}_q[X]$. Notons $P = \prod_{i=1}^r P_i$ la factorisation de P en irréductibles de $\mathbb{F}_q[X]$, \mathcal{R}_i l'ensemble des racines de P_i dans Ω , $n_i = |\mathcal{R}_i| = \deg P_i$, k un corps de décomposition de P sur \mathbb{F}_q , n le p.p.c.m. de n_1, \dots, n_r .

- le corps k est isomorphe à \mathbb{F}_{q^n} ;
- si σ est l'automorphisme de Frobenius de k/\mathbb{F}_q , alors, si $i \in \{1, \dots, r\}$, σ induit un n_i -cycle sur \mathcal{R}_i .

L'énoncé suivant permet de décider si $\text{Gal}_{\mathbb{K}}P$ est contenu dans \mathcal{A}_n ; la seconde partie est souvent nommée théorème de Stickelberger.

Proposition 11. Supposons \mathbb{K} de caractéristique différente de 2. Soit P dans $\mathbb{K}[X]$, séparable de degré n , produit de r polynômes irréductibles de $\mathbb{K}[X]$ et tel que $\text{Gal}_{\mathbb{K}}P$ soit cyclique.

- On a $\text{Gal}_{\mathbb{K}}P \subset \mathcal{A}_n$ si et seulement si $n \equiv r \pmod{2}$.
- Si \mathbb{K} n'est pas de caractéristique 2, $\Delta(P)$ est un carré dans \mathbb{K} si et seulement si $n \equiv r \pmod{2}$.

Preuve. Si γ est un générateur de $\text{Gal}_{\mathbb{K}}P$, la signature de γ est $(-1)^{n-r}$. On en déduit le premier point. Le second suit par application de la proposition 10.

Exercice 43. ③ On suppose q impair. Soit $P \in \mathbb{F}_q[X]$ de degré n impair. On suppose que le discriminant de P n'est pas un carré. Montrer que P est réductible.

2.4 (*) Le théorème de réduction modulo p

Dans ce paragraphe, plus délicat que les précédents, on montre comment obtenir des informations sur le groupe de Galois d'un polynôme unitaire de $\mathbb{Z}[X]$ par réduction modulo p . Les techniques utilisées relèvent de la théorie algébrique des nombres.

Soit donc $P \in \mathbb{Z}[X]$ un polynôme unitaire de degré n :

$$P = \prod_{i=1}^n (X - x_i) \quad (x_1, \dots, x_n) \in \mathbb{C}^n.$$

On fixe un nombre premier p . On note $x \mapsto \bar{x}$ la réduction modulo p de \mathbb{Z} sur \mathbb{F}_p . On note

$$\mathbb{A} = \mathbb{Z}[x_1, \dots, x_n] \quad \mathbb{K} = \mathbb{Q}(x_1, \dots, x_n) = D_{\mathbb{Q}}(P).$$

Puisque $(\mathbb{A}, +)$ est un \mathbb{Z} -module sans torsion de rang fini, c'est un \mathbb{Z} -module libre de rang fini ; le quotient $\mathbb{A}/p\mathbb{A}$ est donc fini de cardinal p^m , où m est le rang de \mathbb{A} ¹³. Les idéaux de \mathbb{A} contenant p s'identifient aux idéaux de $\mathbb{A}/p\mathbb{A}$. L'ensemble \mathcal{M}_p des idéaux maximaux de \mathbb{A} contenant p est donc fini et non vide.¹⁴ Notons au passage que, puisqu'un anneau intègre fini est un corps, \mathcal{M}_p est l'ensemble des idéaux premiers de \mathbb{A} contenant p , ou *idéaux premiers au-dessus de p* .

La première observation est la suivante.

Lemme 4. *Soit \mathfrak{p} un élément de \mathcal{M}_p . On a $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$. L'application*

$$x \in \mathbb{A} \mapsto \bar{x} \in \mathbb{A}/\mathfrak{p}$$

prolonge la réduction modulo p . L'anneau $k = \mathbb{A}/\mathfrak{p}$ est un corps de décomposition de \bar{P} sur \mathbb{F}_p .

Preuve. Le premier point provient du fait que $\mathfrak{p} \cap \mathbb{Z}$ est un idéal de \mathbb{Z} contenant p mais pas 1 (sans quoi \mathfrak{p} contiendrait 1 et serait égal à \mathbb{A}). Le second point s'en déduit immédiatement. De ce second point, on tire que

$$\bar{P} = \prod_{i=1}^n (X - \bar{x}_i),$$

d'où l'on tire que $k = \mathbb{F}_p[\bar{x}_1, \dots, \bar{x}_n]$ est un corps de décomposition de \bar{P} sur \mathbb{F}_p .

Soit maintenant $G = \text{Gal}_{\mathbb{Q}}P = \text{Gal}(\mathbb{K}/\mathbb{Q})$. Il est clair que tout élément de G induit un automorphisme de l'anneau \mathbb{A} . Inversement, tout automorphisme de l'anneau \mathbb{A} se prolonge en un élément de G . Nous pouvons donc voir G comme le groupe des automorphismes de l'anneau \mathbb{A} . Un élément de G fixe p et transforme un idéal maximal en un idéal maximal. Il s'ensuit que G agit sur \mathcal{M}_p . Si $\mathfrak{p} \in \mathcal{M}_p$, on note désormais $G_{\mathfrak{p}}$ le stabilisateur de \mathfrak{p} .

Lemme 5. *(i) L'action de G sur \mathcal{M}_p est transitive.*

(ii) Si \mathfrak{p} et \mathfrak{q} sont deux éléments de \mathcal{M}_p , les sous-groupes $G_{\mathfrak{p}}$ et $G_{\mathfrak{q}}$ sont conjugués dans G .

Preuve. Le point (ii) est conséquence de (i) et du fait que si deux éléments sont dans une même orbite pour une action de groupe, leurs stabilisateurs sont conjugués. Soient donc \mathfrak{p} et \mathfrak{q}

13. C'est-à-dire $m = [\mathbb{K} : \mathbb{Q}]$.

14. Le caractère non vide provient également du lemme de Zorn dès lors que l'on sait que $p\mathbb{A} \neq \mathbb{A}$. Or, les éléments de \mathbb{A} sont des entiers algébriques, contrairement à $\frac{1}{p}$, d'où $p\mathbb{A} \neq \mathbb{A}$.

deux éléments distincts de \mathcal{M}_p . Supposons qu'il n'existe pas de σ dans G tel que $\sigma(\mathfrak{p}) = \mathfrak{q}$. Le théorème chinois fournit $x \in \mathbb{A}$ tel que

$$x \in \mathfrak{p} \quad \text{et} \quad \forall \sigma \in G, \quad x \equiv 1 \pmod{[\sigma(\mathfrak{q})]}.$$

Considérons $a = \prod_{\sigma \in G} \sigma(x)$. Cet élément est fixe sous l'action de G , donc rationnel, et entier algébrique. Il appartient donc à \mathbb{Z} . Puisque $x \in \mathfrak{p}$, a est dans \mathfrak{p} et donc dans $\mathbb{Z} \cap \mathfrak{p} = p\mathbb{Z}$. C'est contradictoire avec le caractère premier des $\sigma(\mathfrak{q})$, $\sigma \in G$.

Fixons \mathfrak{p} dans \mathcal{M}_p . Alors $G_{\mathfrak{p}}$ agit naturellement sur k . Cette action se fait par automorphismes d'anneaux. Or, les automorphismes de k sont exactement les éléments de $\text{Gal}(k/\mathbb{F}_p)$. On définit donc ainsi une application

$$\sigma \in G_{\mathfrak{p}} \longmapsto \bar{\sigma} \in \text{Gal}(k/\mathbb{F}_p)$$

telle que

$$\forall \sigma \in G_{\mathcal{I}}, \quad \forall x \in \mathbb{A}, \quad \bar{\sigma}(\bar{x}) = \overline{\sigma(x)}.$$

Cette application est un morphisme, et on a le résultat suivant.

Théorème 5. *Avec les notations précédentes, le morphisme*

$$\sigma \in G_{\mathfrak{p}} \longmapsto \bar{\sigma} \in \text{Gal}(k/\mathbb{F}_p)$$

est surjectif. Si l'élément \bar{P} de $\mathbb{F}_p[X]$ est séparable, ce morphisme est injectif.^{15 16}

Preuve. Étape 1. Surjectivité. Soit $\alpha \in k^*$ un élément primitif de l'extension k/\mathbb{F}_p . Notons $\alpha = \alpha_1, \dots, \alpha_{\ell}$ les \mathbb{F}_p -conjugés de α . Un élément g de $\text{Gal}(k/\mathbb{F}_p)$ est déterminé par $g(\alpha)$, qui est un des α_i . Il suffit donc de démontrer l'assertion suivante

$$\forall i \in \{1, \dots, \ell\}, \quad \exists \sigma \in G_{\mathfrak{p}}, \quad \bar{\sigma}(\alpha) = \bar{\alpha}_i.$$

À cet effet, il suffit d'établir qu'il existe $a \in \mathbb{A}$ tel que $\bar{a} = \alpha$ et

$$\prod_{\sigma \in G_{\mathfrak{p}}} (X - \overline{\sigma(a)}) \in \mathbb{F}_p[X].$$

Pour a dans \mathbb{A} , on a

$$\prod_{\sigma \in G} (X - \sigma(a)) \in \mathbb{Z}[X].$$

Il suffit donc de montrer qu'existe $a \in \mathbb{A}$ tel que $\bar{a} = \alpha$ et que

$$\forall \sigma \in G \setminus G_{\mathfrak{p}}, \quad \sigma(a) \in \mathfrak{p}.$$

Or, deux éléments distincts de \mathcal{M}_p sont comaximaux. Grâce au théorème chinois, on dispose donc de a dans \mathbb{A} vérifiant

$$\bar{a} = \alpha \quad \text{et} \quad a \in \bigcap_{\mathfrak{q} \in \mathcal{M}_p \setminus \{\mathfrak{p}\}} \mathfrak{q}.$$

Si σ est dans G , σ agit sur \mathcal{M}_p . Si de plus σ n'est pas dans $G_{\mathfrak{p}}$, alors $\sigma^{-1}(\mathfrak{p}) \neq \mathfrak{p}$. Par suite

$$\forall \sigma \in G \setminus G_{\mathfrak{p}}, \quad \sigma(a) \in \mathfrak{p}.$$

15. Il est légitime d'espérer une formulation de cet énoncé en termes d'extension. La réponse vient de la théorie algébrique des nombres : on prends pour \mathbb{K} un corps de nombre extension galoisienne de \mathbb{Q} dans lequel le nombre premier p ne se ramifie pas.

16. La séparabilité de \bar{P} équivaut au fait que p ne divise pas $\Delta(P)$.

Étape 2. *Injectivité en cas de séparabilité.* Supposons \overline{P} séparable. Soit σ dans $G_{\mathfrak{p}}$ tel que,

$$\forall x \in \mathbb{A}, \quad \sigma(x) - x \in \mathfrak{p}.$$

On sait que

$$\overline{P} = \prod_{i=1}^n (X - \overline{x}_i),$$

et que les \overline{x}_i , $1 \leq i \leq n$, sont deux à deux distincts, i.e. que les x_i , $1 \leq i \leq n$, sont deux à deux distincts modulo \mathfrak{p} . Il en résulte que

$$\forall i \in \{1, \dots, n\}, \quad \sigma(x_i) = x_i,$$

donc que σ est l'identité de \mathbb{A} .

Exercice 44. ③ *Montre que, si \overline{P} n'est pas séparable, le morphisme du théorème 5 n'est pas injectif.*

Remarques

1. Automorphisme de Frobenius

On sait qu'une extension finie d'un corps fini est cyclique engendré par l'automorphisme de Frobenius (proposition 4, 1.4). On déduit du théorème 5 l'énoncé suivant.

Corollaire 2. *Adoptons les notations du théorème 5. Il existe alors un unique σ dans $G_{\mathfrak{p}}$ tel que*

$$\forall x \in \mathbb{A}, \quad \sigma(x) - x^p \in \mathfrak{p}.$$

Le morphisme σ est l'automorphisme de Frobenius de \mathfrak{p} . D'après la remarque précédente, les automorphismes de Frobenius associés aux idéaux premiers au-dessus de p forment une classe de conjugaison dans G . Si \mathbb{K}/\mathbb{Q} est abélienne, cette classe est réduite à un élément, l'automorphisme de Frobenius associé à p .

2. Irréductibilité des polynômes cyclotomiques

Soit $n \geq 2$ un entier. Nous allons retrouver l'irréductibilité de Φ_n sur \mathbb{Q} d'une manière plus naturelle à partir du corollaire 2. Reprenons les notations de la proposition 2 de 1.4, en supposant que $\mathbb{K} = \mathbb{Q}$. L'irréductibilité de Φ_n sur \mathbb{Q} équivaut à la surjectivité du morphisme j de $G = \text{Gal}(\mathbb{Q}(\varepsilon)/\mathbb{Q}) = D_{\mathbb{Q}}(X^n - 1)$ dans $\mathbb{Z}/n\mathbb{Z}^*$ qui, avec l'abus de langage évident, associe à $\sigma \in G$ l'unique $j(\sigma)$ tel que $\sigma(\varepsilon) = \varepsilon^{j(\sigma)}$. Il suffit donc d'établir que, pour tout nombre premier p ne divisant pas n , il existe $\sigma \in G$ tel que $\sigma(\varepsilon) = \varepsilon^p$.

Fixons donc un nombre premier p ne divisant pas n , de sorte que la réduction de $X^n - 1$ modulo p est séparable, \mathfrak{p} un idéal premier de $\mathbb{Z}[\varepsilon]$ au-dessus de p . Soit σ l'automorphisme de Frobenius associé à p :

$$\forall g \in G, \quad \sigma(g) - g^p \in \mathfrak{p}.$$

Montrons qu'en fait $\sigma(\varepsilon) = \varepsilon^p$. On a, en évaluant en ε^p la dérivée de $X^n - 1$,

$$n \varepsilon^{p(n-1)} = \prod_{k \in \{0, \dots, n-1\} \setminus \{p\}} (\varepsilon^p - \varepsilon^k).$$

Comme n n'est pas dans $p\mathbb{Z} = \mathfrak{p} \cap \mathbb{Z}$ et ε est inversible dans $\mathbb{Z}[\varepsilon]$, le membre de gauche de cette égalité n'est pas dans \mathfrak{p} . Comme \mathfrak{p} est premier, les $\varepsilon^p - \varepsilon^k$, $0 \leq k \leq n-1$, $k \neq p$ ne sont pas dans \mathfrak{p} . Il en résulte que le seul i de $\{1, \dots, n-1\}$ tel que $\varepsilon^p - \varepsilon^i$ soit dans \mathfrak{p} est $i = p$, d'où le résultat.

3. Généralisation

Soit $\mathcal{O}_{\mathbb{K}}$ l'anneau des entiers de \mathbb{K} . Le théorème, la remarque 1, le corollaire 2 subsistent en remplaçant $\mathbb{A} = \mathbb{Z}[x_1, \dots, x_n]$ par un sous-anneau de $\mathcal{O}_{\mathbb{K}}$ contenant $\mathbb{Z}[x_1, \dots, x_n]$. Les démonstrations s'appliquent verbatim. En théorie algébrique des nombres, on utilise le résultat pour $\mathcal{O}_{\mathbb{K}}$; la séparabilité de \bar{P} équivaut alors au fait que p se ramifie dans \mathbb{K} .

Du théorème 5 et de la proposition 10, on déduit l'énoncé suivant, dû à Dedekind.¹⁷ Le résultat est de même nature que celui de la remarque 8 de **2.1**, mais nettement plus profond.

Théorème 6. *Avec les notations précédentes, supposons \bar{P} séparable et notons $\bar{P} = \prod_{i=1}^m Q_i$, où, pour tout $i \in \{1, \dots, m\}$, Q_i est un polynôme irréductible unitaire de $\mathbb{F}_p[X]$ dont on note d_i le degré. Soit $\mathcal{R} = \{x_1, \dots, x_n\}$ l'ensemble des racines de P . Alors il existe :*

- des sous-ensembles \mathcal{R}_i , $1 \leq i \leq m$ de \mathcal{R} partitionnant \mathcal{R} tels que, pour tout $i \in \{1, \dots, m\}$, \mathcal{R}_i ait pour cardinal d_i ;
- un élément σ de $\text{Gal}_{\mathbb{Q}}P$ tel que, pour tout $i \in \{1, \dots, m\}$, σ stabilise \mathcal{R}_i et induise sur \mathcal{R}_i un cycle de longueur d_i .

3 La correspondance de Galois

3.1 Le lemme d'Artin et le premier volet de la correspondance

Ce paragraphe est consacré à la démonstration du théorème ci-après, qui est le premier volet de la correspondance de Galois.¹⁸

Théorème 7. *Soit \mathbb{L}/\mathbb{K} une extension galoisienne finie. Les deux applications :*

$$\begin{array}{ccc} \varphi : \mathcal{G}_{\mathbb{L}/\mathbb{K}} & \rightarrow & \mathcal{K}_{\mathbb{L}/\mathbb{K}} \\ G & \mapsto & \mathbb{L}^G \end{array} \quad \text{et} \quad \begin{array}{ccc} \psi : \mathcal{K}_{\mathbb{L}/\mathbb{K}} & \rightarrow & \mathcal{G}_{\mathbb{L}/\mathbb{K}} \\ \mathbb{K}' & \mapsto & \text{Gal}(\mathbb{L}/\mathbb{K}') \end{array}$$

sont deux bijections réciproques décroissantes pour l'inclusion. On a de plus :

$$\forall G \in \mathcal{G}_{\mathbb{L}/\mathbb{K}}, \quad [\mathbb{L} : \mathbb{L}^G] = |G|.$$

Il s'agit de montrer que les applications $\psi \circ \varphi$ et $\varphi \circ \psi$ sont les identités respectives de $\mathcal{K}_{\mathbb{L}/\mathbb{K}}$ et $\mathcal{G}_{\mathbb{L}/\mathbb{K}}$. Si \mathbb{K}' est un élément de $\mathcal{K}_{\mathbb{L}/\mathbb{K}}$, l'extension \mathbb{L}/\mathbb{K}' est galoisienne finie. La caractérisation du corps de base d'une telle extension fournit

$$\varphi \circ \psi(\mathbb{K}') = \mathbb{K}'.$$

La relation manquante

$$\forall G \in \mathcal{G}_{\mathbb{L}/\mathbb{K}}, \quad \psi \circ \varphi(G) = G$$

et la dernière assertion du théorème sont des conséquences immédiates de l'énoncé ci-après, souvent nommé « lemme d'Artin », qui montre notamment que les extensions obtenues « en descendant » sont toujours galoisiennes.

Théorème 8. *Si \mathbb{F} est un corps et G un groupe fini d'automorphismes de \mathbb{F} , \mathbb{F}/\mathbb{F}^G est galoisienne de groupe G .*

^{17.} Dont il existe une preuve assez différente, fondée sur un argument de « spécialisation du groupe de Galois » remontant à Kronecker.

^{18.} Les notations sont celles utilisées dans l'introduction, page 2.

La première démonstration du lemme d'Artin, très courte, repose sur le théorème de l'élément primitif.

*Première preuve du théorème 8, valable si \mathbb{F}/\mathbb{F}^G est séparable.*¹⁹ Puisque $G \subset \text{Gal}(\mathbb{F}/\mathbb{F}^G)$, il suffit d'établir que l'extension \mathbb{F}/\mathbb{F}^G est finie de degré majoré par $|G|$ pour conclure. point essentiel est le suivant : si $x \in \mathbb{F}$ et si $G.x$ désigne l'orbite de x sous G , le polynôme

$$P = \prod_{y \in G.x} (X - y)$$

annule x et est à coefficients dans \mathbb{F}^G . Il s'ensuit que tout x de \mathbb{F} est séparable sur \mathbb{F}^G et de degré majoré par $|G.x|$ donc par $|G|$. La conclusion provient du théorème de l'élément primitif.

Artin souhaitait éviter le théorème de l'élément primitif²⁰. Il a donné une autre preuve du théorème 8, qui ne présuppose pas la séparabilité. Nous donnons une variante de son argument, fondée sur le théorème d'indépendance de Dedekind et le lemme d'algèbre linéaire suivant.

Lemme 6. *Soient E un ensemble, \mathbb{F} un corps, g_1, \dots, g_n des fonctions de E dans \mathbb{F} formant un système \mathbb{F} -libre. Alors il existe $(x_1, \dots, x_n) \in E^n$ tel que la matrice $(g_i(x_j))_{1 \leq i, j \leq n}$ soit inversible.*

Preuve. Soit

$$\begin{aligned} \tilde{g} : E &\rightarrow \mathbb{F}^n \\ x &\mapsto (g_1(x), \dots, g_n(x)) \end{aligned}$$

Puisque (g_1, \dots, g_n) est libre, $\tilde{g}(E)$ n'est contenu dans aucun hyperplan de \mathbb{F}^n : il contient donc une base de \mathbb{F}^n .²¹

Exercice 45. ③ *Démontrer le lemme précédent par récurrence en utilisant les déterminants.*

Seconde preuve du théorème 8. On a : $G \subset \text{Gal}(\mathbb{F}/\mathbb{F}^G)$ et il suffit donc d'établir que $[\mathbb{F} : \mathbb{F}^G] = |G|$. Posons $G = \{g_1, \dots, g_n\}$. Le théorème d'indépendance des morphismes et le lemme précédent fournissent $(x_1, \dots, x_n) \in \mathbb{F}^n$ tel que la matrice $(g_i(x_j))_{1 \leq i, j \leq n}$ soit inversible. Vérifions que (x_1, \dots, x_n) est une base de \mathbb{F} sur \mathbb{F}^G . Pour que tel soit le cas, il faut et il suffit que tout x de \mathbb{F} s'écrive de façon unique : $x = \sum_{i=1}^n a_i x_i$ où les a_i sont dans \mathbb{F}^G . Il revient au même de dire que le système :

$$(S_x) \begin{cases} g_1(x) = a_1 g_1(x_1) + \dots + a_n g_1(x_n) \\ \vdots \\ g_n(x) = a_1 g_n(x_1) + \dots + a_n g_n(x_n) \end{cases}$$

admet, pour tout x dans \mathbb{F} , une unique solution dans $(\mathbb{F}^G)^n$. Or, $x \in \mathbb{F}$ étant fixé, (S_x) est de Cramer et admet donc une unique solution $(a_1, \dots, a_n) \in \mathbb{F}^n$. De plus, si $g \in G$, la multiplication à gauche par g est une permutation de G , d'où il résulte que $(g(a_1), \dots, g(a_n))$ est également solution de (S_x) . Par unicité, les a_i sont fixes par l'action de G : c'est dire qu'ils appartiennent à \mathbb{F}^G .

La formulation d'Artin de la correspondance de Galois

Artin a fait du théorème 8 le coeur de la théorie de Galois, allant jusqu'à définir les extensions galoisiennes comme celles de la forme \mathbb{F}/\mathbb{F}^G où G est un groupe d'automorphismes du corps \mathbb{F} . Le

19. Ce qui suffit pour le théorème 7.

20. Raison de cette aversion : le caractère peu intrinsèque de la description d'une extension finie par un élément primitif, déjà mentionné dans la section 2.3 du chapitre 2.

21. Une équation d'un éventuel hyperplan contenant $\tilde{g}(E)$ donne une relation de liaison entre les g_i .

théorème 8 donne en fait une forme de la correspondance un peu plus générale que le théorème 7. Soient \mathbb{F} un corps, $\mathcal{G}_{\mathbb{F}}$ l'ensemble des sous-groupes finis de $\text{Aut}(\mathbb{F})$, $\mathcal{K}_{\mathbb{F}}$ l'ensemble des sous-corps \mathbb{K} de \mathbb{F} tels que \mathbb{F}/\mathbb{K} soit une extension galoisienne finie, φ et ψ les applications définies par :

$$\forall G \in \mathcal{G}_{\mathbb{F}}, \quad \varphi(G) = \mathbb{F}^G \quad \text{et} \quad \forall \mathbb{K} \in \mathcal{K}_{\mathbb{F}}, \quad \psi(\mathbb{K}) = \text{Gal}(\mathbb{F}/\mathbb{K}).$$

Grâce au théorème 8, φ arrive dans $\mathcal{K}_{\mathbb{F}}$ et $\psi \circ \varphi = \text{id}_{\mathcal{G}_{\mathbb{F}}}$. Si maintenant \mathbb{K} est dans $\mathcal{K}_{\mathbb{F}}$, la caractérisation du corps de base d'une extension galoisienne montre que $\psi(K)$ est dans $\mathcal{G}_{\mathbb{F}}$ et que $\varphi \circ \psi(\mathbb{K}) = \mathbb{K}$; ainsi $\varphi \circ \psi = \text{id}_{\mathcal{K}_{\mathbb{F}}}$. On a établi le résultat suivant.

Théorème 9. *Les applications φ et ψ sont deux bijections réciproques entre $\mathcal{G}_{\mathbb{F}}$ et $\mathcal{K}_{\mathbb{F}}$, décroissantes pour l'inclusion. On a de plus :*

$$\forall G \in \mathcal{G}_{\mathbb{F}}, \quad [\mathbb{F} : \mathbb{F}^G] = |G|.$$

Exercice 46. ② *Si \mathbb{L}/\mathbb{K} est finie, vérifier que \mathbb{L}/\mathbb{K} est galoisienne si et seulement s'il existe un groupe G d'automorphismes de \mathbb{L} tel que $\mathbb{K} = \mathbb{L}^G$.*

Exercice 47. ③ *Avec les notations ci-dessus, déduire la relation $\varphi \circ \psi = \text{id}_{\mathcal{K}_{\mathbb{F}}}$ du lemme d'Artin et de la majoration du cardinal d'un groupe de Galois par le degré de l'extension.*

3.2 Applications et exemples

Ce paragraphe est consacré à des illustrations de la correspondance de Galois, ainsi qu'à des applications du lemme d'Artin à la détermination de corps fixes par des groupes finis d'automorphismes. En première lecture, on pourra sans dommage se limiter aux illustrations 1 à 4.

Illustrations de la correspondance de Galois

Ces illustrations se partagent entre résultats généraux et applications aux corps de nombres. Pour les résultats généraux, l'injectivité de l'application φ , elle-même conséquence du théorème d'Artin, est souvent l'argument central.

1. Sous-corps correspondant au sous-groupe des permutations paires

Le résultat suivant, conséquence de l'injectivité de l'application φ , précise la proposition 9 (2.3) par l'identification du corps fixe par le sous-groupe des permutations paires.

Proposition 12. *Soient \mathbb{K} un corps de caractéristique différente de 2, $P \in \mathbb{K}[X]$ un polynôme séparable, \mathcal{R} l'ensemble des racines de P dans Ω . Alors :*

$$D_{\mathbb{K}}P(\text{Gal}_{\mathbb{K}}P \cap \mathcal{A}(\mathcal{R})) = \mathbb{K} \left(\sqrt{\Delta(P)} \right).$$

2. Corps de décomposition d'un polynôme de degré 3

Soient P dans $\mathbb{K}[X]$ irréductible séparable de degré 3 et $\mathbb{L} = D_{\mathbb{K}}P$.

Si $[\mathbb{L} : \mathbb{K}] = 3$, les sous-corps de \mathbb{L} contenant \mathbb{K} sont \mathbb{L} et \mathbb{K} (multiplicativité des degrés).

Si $[\mathbb{L} : \mathbb{K}] = 6$, $\text{Gal}_{\mathbb{K}}P$ est isomorphe à \mathcal{S}_3 (2.1). Il y a donc quatre sous-corps strictement intermédiaires entre \mathbb{L} et \mathbb{K} : trois de degré 3 et un de degré 2 sur \mathbb{K} . Ils correspondent respectivement aux trois sous-groupes engendrés par une transposition, et à \mathcal{A}_3 . Le sous-corps correspondant à \mathcal{A}_3 est explicité dans la proposition 12. Les autres sont $\mathbb{K}(\alpha)$, $\mathbb{K}(\beta)$ et $\mathbb{K}(\gamma)$ où α , β , γ sont les racines de P dans $D_{\mathbb{K}}P$.

Ainsi, les sous-corps de $\mathbb{Q}(j, \sqrt[3]{2})$ sont $\mathbb{Q}(j)$, $\mathbb{Q}(\sqrt[3]{2})$, $\mathbb{Q}(j\sqrt[3]{2})$ et $\mathbb{Q}(j^2\sqrt[3]{2})$.

3. *Sous-extensions de $\mathbb{Q}(e^{i\pi/4})/\mathbb{Q}$*

Posons $\mathbb{K} = \mathbb{Q}(e^{i\pi/4})$. D'après la proposition 1, \mathbb{K}/\mathbb{Q} est galoisienne de groupe $((\mathbb{Z}/8\mathbb{Z})^*, \times)$. Ce groupe admet trois sous-groupes non triviaux, à savoir les groupes cycliques de cardinal 2 engendrés par les classes de $\bar{3}$, $\bar{5}$ et $\bar{7}$. Il y a donc exactement trois sous-corps de \mathbb{K} de degré 2 sur \mathbb{Q} . On les devine aisément : $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(i)$, $\mathbb{Q}(i\sqrt{2})$.

Voyons comment les déterminer systématiquement. Soient $\varepsilon = e^{i\pi/n}$ et σ l'élément de $\text{Gal}(\mathbb{K}/\mathbb{Q})$ vérifiant $\sigma(\varepsilon) = \varepsilon^3$. Cherchons le corps fixe de σ en prenant (a_0, a_1, a_2, a_3) dans \mathbb{Q}^4 et en cherchant si $x = a_0 + a_1\varepsilon + a_2\varepsilon^2 + a_3\varepsilon^3$ vérifie $\sigma(x) = x$. On a $\sigma(x) = a_0 + a_1\varepsilon^3 + a_2\varepsilon^2 + a_3\varepsilon$, d'où :

$$x \in \mathbb{K}^{\langle \sigma \rangle} \Leftrightarrow a_2 = 0, a_1 = a_3 \Leftrightarrow x \in \mathbb{Q} + \mathbb{Q}(\varepsilon + \varepsilon^3) \Leftrightarrow x \in \mathbb{Q}(i\sqrt{2}).$$

Les autres cas sont analogues.

4. *Sous-extension quadratique d'une extension cyclotomique*

Soient p un nombre premier ≥ 3 , r dans \mathbb{N}^* et $\mathbb{K} = \mathbb{Q}(e^{2i\pi/p^r})$. L'extension \mathbb{K}/\mathbb{Q} est galoisienne de groupe de Galois cyclique d'ordre $(p-1)p^{r-1}$. Il s'ensuit que, pour tout diviseur d de $(p-1)p^{r-1}$, il existe un unique sous-corps de degré d sur \mathbb{Q} . Pour $d = 2$, l'exemple 2 du paragraphe 2.3 entraîne que la seule sous-extension quadratique de \mathbb{K}/\mathbb{Q} est $\mathbb{Q}(\sqrt{p^*})$ où on pose $p^* = (-1)^{\frac{p-1}{2}}$.

5. (*) *Corps finis*

On sait que l'extension $\mathbb{F}_{q^n}/\mathbb{F}_q$ est cyclique de degré n de groupe G engendré par l'endomorphisme de Frobenius F_q . Les sous-groupes de G sont les $\langle F_q^d \rangle$ pour $d|n$. Or, les points fixes de F_q^d sont les éléments de \mathbb{F}_{q^d} . On retrouve le fait que les sous-corps de \mathbb{F}_{q^n} contenant \mathbb{F}_q sont les \mathbb{F}_{q^d} pour d divisant n .

6. (*) *Théorème de Lagrange sur les fractions rationnelles*

Reprenons les notations de 2.2, en particulier

$$\mathbb{K}_X = K(X_1, \dots, X_n), \quad \mathbb{K}_\Sigma = \mathbb{K}(\Sigma_1, \dots, \Sigma_n).$$

Associons à un élément F de \mathbb{K}_X le sous-groupe G_F de \mathcal{S}_n formé des σ telles que :

$$F(X_{\sigma(1)}, \dots, X_{\sigma(n)}) = F(X_1, \dots, X_n).$$

Autrement dit, G_F est le groupe de Galois de $\mathbb{K}_X/\mathbb{K}_\Sigma(F)$ représenté comme groupe des racines du polynôme générique. Lagrange a établi que, pour F_1 et F_2 dans \mathbb{K}_X , on a :

$$G_{F_1} \subset G_{F_2} \iff F_2 \in \mathbb{K}_\Sigma(F_1).$$

Cette équivalence est immédiate à l'aide de l'interprétation susmentionnée de G_{F_1} et G_{F_2} comme groupes de Galois et de la correspondance.²²

22. Voici une preuve plus élémentaire, proche de l'argument de Lagrange. On part de la fraction :

$$\Psi(T) = \sum_{\sigma \in \mathcal{S}_n/G_{F_1}} \frac{\sigma.F_2}{T - \sigma.F_1}.$$

de $\mathbb{K}_X(T)$. L'hypothèse $G_{F_1} \subset G_{F_2}$ signifie que

$$\sigma^{-1}\sigma' \in G_{F_1} \implies \sigma.F_2 = \sigma'.F_2.$$

Cette implication justifie la définition de Ψ . Elle entraîne également que Ψ est invariante sous l'action de \mathcal{S}_n , donc appartient à $\mathbb{K}_\Sigma(T)$. Le résidu de Ψ relatif au pôle F_1 appartient donc à $\mathbb{K}_\Sigma(F_1)$; or ce résidu n'est autre que F_2 .

7. *Intersections de sous-groupes versus extensions composées*

Soient \mathbb{L}/\mathbb{K} une extension galoisienne finie, G_1, \dots, G_r des éléments de $\mathcal{G}_{\mathbb{L}/\mathbb{K}}$. Le sous-groupe $G_1 \cap G_2 \cap \dots \cap G_r$ est dans $\mathcal{G}_{\mathbb{L}/\mathbb{K}}$, et $\varphi(G_1 \cap \dots \cap G_r)$ est le sous-corps $\mathbb{L}^{G_1} \dots \mathbb{L}^{G_r}$ de \mathbb{L} engendré par les \mathbb{L}^{G_i} pour $1 \leq i \leq r$. En effet, l'image de $\mathbb{L}^{G_1} \dots \mathbb{L}^{G_r}$ par ψ est

$$\text{Gal}(\mathbb{L}/\mathbb{L}^{G_1} \dots \mathbb{L}^{G_r}) = \bigcap_{i=1}^r \text{Gal}(\mathbb{L}/\mathbb{L}^{G_i}) = \bigcap_{i=1}^r G_i.$$

En particulier, $\mathbb{L}^{G_1} \dots \mathbb{L}^{G_r} = \mathbb{L}$ si et seulement si :

$$\bigcap_{i=1}^r G_i = \{\text{id}_{\mathbb{L}}\}.$$

8. *Irrationalités naturelles*

Reprenons les notations de la proposition 6 (**1.5**). Il est clair que le sous-corps $\mathbb{L}^{\text{Im}(\rho)}$ de \mathbb{L} n'est autre que $\mathbb{K}\mathbb{F} \cap \mathbb{L}$. Par correspondance de Galois, il suit que $\text{Im}(\rho) = \text{Gal}(\mathbb{L}/\mathbb{K}\mathbb{F} \cap \mathbb{L})$. Le théorème des irrationalités naturelles se précise donc : ρ est un isomorphisme de $\text{Gal}(\mathbb{L}\mathbb{F}/\mathbb{K}\mathbb{F})$ sur $\text{Gal}(\mathbb{L}/\mathbb{K}\mathbb{F} \cap \mathbb{L})$. En particulier : $[\mathbb{L}\mathbb{F} : \mathbb{K}\mathbb{F}] = [\mathbb{L} : \mathbb{K}\mathbb{F} \cap \mathbb{L}]$.

9. (*) *Groupe de Galois d'une composée*

Reprenons les notations de la proposition 7 (**1.5**). En appliquant l'item précédent avec $\mathbb{L} = \mathbb{L}_1$ et $\mathbb{F} = \mathbb{L}_2$, il vient : $[\mathbb{L}_1\mathbb{L}_2 : \mathbb{L}_2] = [\mathbb{L}_1 : \mathbb{L}_1 \cap \mathbb{L}_2]$. L'image de ρ est contenue dans :

$$\begin{aligned} & \frac{\text{Gal}(\mathbb{L}_1/\mathbb{K}) \times \text{Gal}(\mathbb{L}_2/\mathbb{K})}{\text{Gal}(\mathbb{L}_1 \cap \mathbb{L}_2/\mathbb{K})} \\ &= \{(\sigma_1, \sigma_2) \in \text{Gal}(\mathbb{L}_1/\mathbb{K}) \times \text{Gal}(\mathbb{L}_2/\mathbb{K}) ; \sigma_1|_{\mathbb{L}_1 \cap \mathbb{L}_2} = \sigma_2|_{\mathbb{L}_1 \cap \mathbb{L}_2}\}, \end{aligned}$$

que l'on appelle le *produit de Gal*(\mathbb{L}_1/\mathbb{K}) *par Gal*(\mathbb{L}_2/\mathbb{K}) *amalgamé par Gal*($\mathbb{L}_1 \cap \mathbb{L}_2/\mathbb{K}$). Elle a pour cardinal l'ordre du produit amalgamé précédent, c'est-à-dire :

$$[\mathbb{L}_1\mathbb{L}_2 : \mathbb{K}] = [\mathbb{L}_1 : \mathbb{L}_1 \cap \mathbb{L}_2] \times [\mathbb{L}_2 : \mathbb{K}] = \frac{[\mathbb{L}_1 : \mathbb{K}] \times [\mathbb{L}_2 : \mathbb{K}]}{[\mathbb{L}_1 \cap \mathbb{L}_2 : \mathbb{K}]}.$$

On peut donc renforcer la proposition 7 : $\text{Gal}(\mathbb{L}_1\mathbb{L}_2/\mathbb{K})$ est isomorphe à

$$\frac{\text{Gal}(\mathbb{L}_1/\mathbb{K}) \times \text{Gal}(\mathbb{L}_2/\mathbb{K})}{\text{Gal}(\mathbb{L}_1 \cap \mathbb{L}_2/\mathbb{K})}.$$

10. (*) *Un premier exemple d'équation non résoluble par radicaux*

Soit $P \in \mathbb{K}[X]$ non constant. Rappelons (chapitre **2**, **3.3**), que P est résoluble par radicaux sur \mathbb{K} s'il existe des nombres premiers n_1, \dots, n_r et des éléments a_1, \dots, a_r de \mathbb{C} tels que :

$$\forall i \in \{0, \dots, r-1\}, \quad a_{i+1}^{n_{i+1}} \in \mathbb{K}(a_1, \dots, a_i) \quad \text{et} : \quad D_{\mathbb{K}}P \subset \mathbb{K}(a_1, \dots, a_r).$$

Soient $p \geq 5$ un nombre premier, \mathbb{K} un sous-corps de \mathbb{C} , $P \in \mathbb{K}[X]$ de degré p , irréductible sur \mathbb{K} admettant exactement $p-2$ racines réelles et deux racines complexes conjuguées. On sait (exemple 10, **2.1**) que le groupe $\text{Gal}_{\mathbb{K}}P$ est isomorphe à \mathcal{S}_p , donc que $[D_{\mathbb{K}}P : \mathbb{K}] = p!$. Nous allons en déduire que P n'est pas résoluble par radicaux sur \mathbb{K} . Ce résultat contient le théorème d'Abel-Ruffini sur l'impossibilité de la résolution par radicaux de l'équation du cinquième degré. La démonstration qui suit est assez artisanale. Dans le chapitre **5**,

nous retrouverons cet énoncé de manière beaucoup plus satisfaisante, comme corollaire de la caractérisation galoisienne des équations résolubles par radicaux.

Raisonnons par l'absurde. Pour $i \in \{0, \dots, r\}$, posons $\mathbb{K}_i = \mathbb{K}(a_1, \dots, a_i)$. Soit j le plus petit élément de l'ensemble des i de $\{1, \dots, r\}$ tels que P soit réductible sur \mathbb{K}_i . Posons $\mathbb{K}' = \mathbb{K}_{j-1}$: P est irréductible sur \mathbb{K}' mais réductible sur $\mathbb{K}'(a_j)$ et $b = a_j^{n_j}$ est dans \mathbb{K}' .

Le polynôme $X^{n_j} - b$ n'a pas de racine dans \mathbb{K}' , donc est irréductible sur \mathbb{K}' (chapitre 1, 2.2, proposition 1). Il s'ensuit que $[\mathbb{K}'(a_j) : \mathbb{K}'] = n_j$. Si n_j et p étaient premiers entre eux, P resterait irréductible sur $\mathbb{K}'(a_j)$ (chapitre 2, 2.1, remarque 6). Il s'ensuit que $n_j \wedge p \neq 1$, d'où, comme n_j et p sont premiers, $p = n_j$. Ainsi $[\mathbb{K}'(a_j) : \mathbb{K}'] = p$.

Puisque P est réductible sur $\mathbb{K}'(a_j)$, la proposition 12 du chapitre 2 (4.1) entraîne que $[D_{\mathbb{K}'(a_j)}P : \mathbb{K}'(a_j)] \leq (p-1)!$. L'égalité $[\mathbb{K}'(a_j) : \mathbb{K}'] = p$ et la multiplicativité des degrés entraînent alors que $[D_{\mathbb{K}'(a_j)}P : \mathbb{K}'] \leq p!$. Or, $D_{\mathbb{K}'}P \subset D_{\mathbb{K}'(a_j)}P$ et, grâce à l'exemple 10 de 2.1, de l'égalité $[D_{\mathbb{K}'}P : \mathbb{K}'] = p!$. On en déduit que $[D_{\mathbb{K}'(a_j)}P : \mathbb{K}'(a_j)] = (p-1)!$.

La démonstration de la proposition 12 du chapitre 2 montre que, si Q est un polynôme de degré $n \geq 2$ sur \mathbb{K} tel que $[D_{\mathbb{K}}Q : \mathbb{K}] = (n-1)!$, alors Q est produit d'un polynôme irréductible de degré $n-1$ par un polynôme de degré 1, donc a une racine dans \mathbb{K} . Revenant à la situation qui nous occupe, on a donc que P admet une racine dans $\mathbb{K}'(a_j)$. Les racines de P sont donc toutes contenues dans la clôture normale de $\mathbb{K}'(a_j)$ sur \mathbb{K}' , i.e. dans $\mathbb{K}'(\varepsilon, a_j)$ où ε est une racine primitive p -ième de 1. Ainsi $D_{\mathbb{K}'}P \subset \mathbb{K}'(\varepsilon, a_j)$. Comme $[\mathbb{K}'(a_j, \varepsilon) : \mathbb{K}'] \leq p(p-1) < p!$, on obtient la contradiction désirée.

Exercice 48. ③ À quelle condition l'extension $\mathbb{Q}(e^{2i\pi/n})/\mathbb{Q}$ contient-elle une unique sous-extension quadratique ?

Exercice 49. ③ Caractériser les extensions galoisiennes finies dont le groupe est produit direct de deux sous-groupes non triviaux.

Exercice 50. ③ Soit $r \geq 3$ un entier. On rappelle que $(\mathbb{Z}/2^r\mathbb{Z})^*$ est produit direct d'un groupe cyclique d'ordre 2 et d'un groupe cyclique d'ordre 2^{r-2} . En déduire les sous-extensions quadratiques de \mathbb{K}/\mathbb{Q} où $\mathbb{K} = \mathbb{Q}(e^{\frac{2i\pi}{2^r}})$.

Exercice 51. ④ Soient $P \in \mathbb{K}[X]$ séparable et irréductible, x une racine de P dans Ω . Montrer que $D_{\mathbb{K}}P = \mathbb{K}(x)$ si et seulement si le stabilisateur de x (dans l'action de $\text{Gal}_{\mathbb{K}}P$ sur les racines) est trivial; montrer que cette propriété est satisfaite si $\text{Gal}_{\mathbb{K}}P$ est abélien.

Exercice 52. ④ Soient $P \in \mathbb{K}[X]$ séparable, x une racine de P dans Ω .

a) Montrer que $\mathbb{K}(x)$ ne contient aucune extension intermédiaire de \mathbb{K} si et seulement si le stabilisateur de x est un sous-groupe maximal de $\text{Gal}_{\mathbb{K}}P$.

b) Supposons P de degré n et de groupe S_n . Montrer que $\mathbb{K}(x)$ est une extension de degré n de \mathbb{K} sans extension intermédiaire.

c) Montrer qu'il existe un sous-corps \mathbb{L} de $\mathbb{K}(X_1, \dots, X_n)$ tel que

$$[\mathbb{K}(X_1, \dots, X_n) : \mathbb{L}] = n,$$

et qu'il n'y ait aucun corps entre \mathbb{L} et $\mathbb{K}(X_1, \dots, X_n)$.

Exercice 53. ③ Déduire le théorème de l'élément primitif du critère de Steinitz et de la correspondance de Galois.

Exercice 54. ④ Reprenons les notations de l'exemple 6. Soient F_1 et F_2 dans \mathbb{K}_X . On suppose que l'ensemble des $\sigma.F_2$ pour σ dans G_{F_1} est de cardinal m , on note $F_{2,1}, \dots, F_{2,m}$ ses éléments.

Montrer que $\prod_{i=1}^m (T - F_{2,i})$ appartient à $\mathbb{K}_\Sigma(F_1)[T]$.

On a ainsi établi une généralisation de l'exemple 6, due elle aussi à Lagrange : « soient F_1 et F_2 deux fractions rationnelles ; si F_2 prend m valeurs quand on lui applique les permutations qui fixent F_1 , alors F_2 vérifie une équation de degré m sur le corps engendré par F_1 ».

Exercice 55. ④ Soit $P \in \mathbb{K}[X]$ irréductible séparable de degré 4. Montrer que $D_{\mathbb{K}}P/\mathbb{K}$ ne contient aucune sous-extension de degré 2 si et seulement si $\text{Gal}_{\mathbb{K}}P$ est isomorphe à A_4 .

Exercice 56. ⑤ On se place dans les conditions de l'exercice 20 de 1.4.

a) Décrire les éléments de $\mathcal{K}_{\mathbb{K}(\sqrt{u_1}, \dots, \sqrt{u_m})/\mathbb{K}}$.

b) Décrire et dénombrer les sous-extensions de l'extension précédente. Étudier asymptotiquement leur nombre lorsque m tend vers $+\infty$.

(*) Détermination de corps fixes

Soient \mathbb{F} un corps, G un groupe fini d'automorphismes de \mathbb{F} . Supposons connu un sous-corps \mathbb{F}' de \mathbb{F} contenu dans \mathbb{F}^G tel que $[\mathbb{F} : \mathbb{F}'] \leq |G|$. Le théorème d'Artin implique alors :

$$\mathbb{F}^G = \mathbb{F}'.$$

Au vu de la seconde preuve du théorème, il est clair que cet argument est indépendant des notions de normalité et de séparabilité. Illustrons-le.

1. Retour sur les fractions symétriques

Adoptons les notations de 2.2. Le groupe \mathcal{S}_n se réalise comme groupe d'automorphismes de \mathbb{K}_X . Le corps fixe contient \mathbb{K}_Σ . D'autre part, \mathbb{K}_X est un corps de décomposition d'un polynôme de degré n sur \mathbb{K}_Σ , donc est de degré au plus $n!$ sur ce corps. On retrouve à nouveau le théorème des fractions rationnelles symétriques.

2. Fractions rationnelles invariantes par des groupes finis d'homographies

(a) Les deux applications $F(X) \mapsto F(1-X)$ et $F(X) \mapsto F(1/X)$ engendrent un sous-groupe G de $\text{Aut}(\mathbb{K}(X))$ de cardinal 6 (et isomorphe à \mathcal{S}_3). Soient \mathbb{K}' le sous-corps de $\mathbb{K}(X)$ fixe par G ,

$$T = \frac{(X^2 - X + 1)^3}{X^2(X-1)^2}.$$

On vérifie que $T \in \mathbb{K}'$, d'où : $\mathbb{K}(T) \subset \mathbb{K}'$. Mais X vérifie une équation de degré 6 sur $\mathbb{K}(T)$ donc :

$$[\mathbb{K}(X) : \mathbb{K}(T)] \leq 6, \quad \text{puis} \quad \mathbb{K}' = \mathbb{K}(T).$$

(b) Ici $\mathbb{K} = \mathbb{C}(X)$. Soient

$$\sigma : F(X) \mapsto F\left(e^{2i\pi/n}X\right) \quad \text{et} \quad \tau : F(X) \mapsto F(1/X).$$

On vérifie que σ et τ engendrent un sous-groupe G de $\text{Aut}(\mathbb{C}(X))$ de cardinal $2n$ (qui est en fait un groupe diédral de cardinal $2n$). Soient \mathbb{K}' le sous-corps de $\mathbb{K}(X)$ fixe par G . Comme $T = X^n + 1/X^n \in \mathbb{K}'$, on a $\mathbb{C}(T) \subset \mathbb{K}'$. Mais X vérifie $X^{2n} - TX^n + 1 = 0$, d'où $[\mathbb{C}(X) : \mathbb{C}(T)] \leq 2n$, puis $\mathbb{K}' = \mathbb{C}(T)$.

Exercice 57. ④ Soient

$$\begin{aligned}\mathbb{K}_1 &= \{F \in \mathbb{F}_q(X), F(X+b) = F(X) \text{ si } b \in \mathbb{F}_q\}, \\ \mathbb{K}_2 &= \{F \in \mathbb{F}_q(X), F(aX+b) = F(X) \text{ si } b \in \mathbb{F}_q, a \in \mathbb{F}_q^*\}, \\ \mathbb{K}_3 &= \left\{ F \in \mathbb{F}_q(X), F\left(\frac{aX+b}{cX+d}\right) = F(X) \text{ si } \begin{array}{l} (a, b, c, d) \in \mathbb{F}_q^4 \\ ad - bc \neq 0 \end{array} \right\}.\end{aligned}$$

Montrer :

- $\mathbb{K}_1 = \mathbb{F}_q(T_1)$ avec $T_1 = X^q - X$,
- $\mathbb{K}_2 = \mathbb{F}_q(T_2)$ avec $T_2 = T_1^{q-1}$,
- $\mathbb{K}_3 = \mathbb{F}_q(T_3)$ avec $T_3 = \frac{(X^{q^2} - X)^{q+1}}{(X^q - X)^{q^2+1}}$.

Exercice 58. ④ On fait agir sur $\mathbb{F} = \mathbb{C}(X_1, \dots, X_n)$ le groupe $\mathbb{Z}/n\mathbb{Z}$ de générateur σ donné par $\sigma(X_i) = X_{i+1}$, en convenant que $X_{n+1} = X_1$. Pour $1 \leq j \leq n$, on pose

$$Y_j = \sum_{k=1}^n e^{2i\pi kj/n} X_k, T_j = \frac{Y_1 Y_j}{Y_{j+1}},$$

en convenant que $Y_{n+1} = Y_1$. Montrer que $\mathbb{F}^{\langle \sigma \rangle} = \mathbb{C}(T_1, \dots, T_n)$.

3.3 Le second volet de la correspondance

Le second volet de la correspondance de Galois identifie les sous-groupes normaux de $\text{Gal}(\mathbb{L}/\mathbb{K})$ et les quotients correspondants. Autrement dit, il traduit en termes de sous-corps la « structure normale » de G .

Théorème 10. Soit \mathbb{L}/\mathbb{K} une extension galoisienne finie. Si $\mathbb{K}' \in \mathcal{K}_{\mathbb{L}/\mathbb{K}}$, le sous-groupe $\text{Gal}(\mathbb{L}/\mathbb{K}')$ est normal dans $\text{Gal}(\mathbb{L}/\mathbb{K})$ si et seulement si l'extension \mathbb{K}'/\mathbb{K} est normale (i.e., ici, galoisienne). Dans ce cas, le quotient est isomorphe à $\text{Gal}(\mathbb{K}'/\mathbb{K})$.

Preuve. Il suffit de combiner la proposition 5 (1.5) et le lemme suivant.

Lemme 7. Soient \mathbb{L}/\mathbb{K} une extension galoisienne finie, \mathbb{K}' dans $\mathcal{K}_{\mathbb{L}/\mathbb{K}}$ et σ dans $\text{Gal}(\mathbb{L}/\mathbb{K})$. Alors²³

$$\sigma \circ \text{Gal}(\mathbb{L}/\mathbb{K}') \circ \sigma^{-1} = \text{Gal}(\mathbb{L}/\sigma(\mathbb{K}')).$$

En particulier, $\text{Gal}(\mathbb{L}/\mathbb{K}')$ est normal dans $\text{Gal}(\mathbb{L}/\mathbb{K})$ si et seulement si \mathbb{K}'/\mathbb{K} est normale.

Preuve du lemme. Le premier point résulte de l'égalité :

$$\mathbb{L}^{\sigma \circ \text{Gal}(\mathbb{L}/\mathbb{K}') \circ \sigma^{-1}} = \sigma(\mathbb{K}')$$

et de l'injectivité de la correspondance de Galois. Le second s'en déduit.

Exercice 59. ① Soient $n \in \mathbb{N}^*$, d un diviseur de n . On peut montrer qu'un groupe abélien fini de cardinal n a autant de sous-groupes de cardinal d que de sous-groupes de cardinal n/d . Qu'en déduit-on en termes d'extensions ?

23. Deux extensions de \mathbb{K} isomorphes comme \mathbb{K} -algèbres sont dites \mathbb{K} -conjuguées. Le lemme 5 dit que deux sous-extensions d'une extension galoisienne finie sont \mathbb{K} -conjuguées si et seulement si leurs images par la correspondance de Galois sont des sous-groupes conjugués de $\text{Gal}(\mathbb{L}/\mathbb{K})$.

Exercice 60. ② Soient \mathbb{L}/\mathbb{K} une extension galoisienne finie, S et S' deux p -Sylow de $\text{Gal}(\mathbb{L}/\mathbb{K})$. Que dire des corps \mathbb{L}^S et $\mathbb{L}^{S'}$?

Exercice 61. ② Soient p un nombre premier, r un élément de \mathbb{N}^* , \mathbb{L}/\mathbb{K} une extension galoisienne dont le groupe de Galois est cyclique d'ordre p^r . Quel est le cardinal de $\mathcal{K}_{\mathbb{L}/\mathbb{K}}$? Montrer que l'inclusion est un ordre total sur $\mathcal{K}_{\mathbb{L}/\mathbb{K}}$.

Exercice 62. ③ Soient \mathbb{L}/\mathbb{K} une extension galoisienne finie, \mathbb{K}' dans $\mathcal{K}_{\mathbb{L}/\mathbb{K}}$, $\mathbb{L}' = \mathbb{L}^{D(G)}$ où $D(G)$ est le groupe dérivé de $\text{Gal}(\mathbb{L}/\mathbb{K})$. Montrer que \mathbb{K}'/\mathbb{K} est abélienne si et seulement si $\mathbb{K}' \subset \mathbb{L}'$. Ainsi, \mathbb{L}' est l'unique sous-extension abélienne maximale de \mathbb{L}/\mathbb{K} .

Exercice 63. ④ Soient \mathbb{L}/\mathbb{K} une extension galoisienne finie, H un sous-groupe de $\text{Gal}(\mathbb{L}/\mathbb{K})$ de normalisateur $N_G(H)$. Montrer que $\text{Gal}(\mathbb{L}^H/\mathbb{K})$ est isomorphe à $N_G(H)/H$.

Exercice 64. ④ Soient n un élément de \mathbb{N}^* et $x = \sqrt{2 + \sqrt{2 + \dots + \sqrt{2}}}$ (n racines carrées). Exprimer x sous la forme $2 \cos(\theta)$. Montrer que l'extension $\mathbb{Q}(x)/\mathbb{Q}$ est galoisienne, déterminer son groupe de Galois.

Voici une application immédiate du théorème 10.

Proposition 13. Si \mathbb{L}/\mathbb{K} est une extension abélienne (resp. cyclique), et si \mathbb{K}' est un sous-corps de \mathbb{L} contenant \mathbb{K} , l'extension \mathbb{K}'/\mathbb{K} est abélienne (resp. cyclique), en particulier galoisienne.

Preuve. Les sous-groupes d'un groupe abélien sont tous normaux et les quotients d'un groupe abélien (resp. cyclique) sont abéliens (resp. cycliques).

Exemple. Toute extension de \mathbb{Q} contenue dans une extension cyclotomique est abélienne et donc galoisienne. Ainsi, aucune extension cyclotomique de \mathbb{Q} ne contient $\sqrt[n]{2}$ si n est un entier ≥ 3 . Réciproquement, le difficile théorème de Kronecker-Weber assure que toute extension abélienne de \mathbb{Q} est contenue dans une extension cyclotomique.²⁴

Exercice 65. ② Soit \mathbb{L}/\mathbb{K} une extension galoisienne dont le groupe de Galois est isomorphe au groupe \mathcal{H}_8 des quaternions. Montrer que si \mathbb{K}' appartient à $\mathcal{K}_{\mathbb{L}/\mathbb{K}}$, alors \mathbb{K}'/\mathbb{K} est galoisienne.

Exercice 66. ④ a) Soit \mathbb{K} un corps dont toute extension galoisienne finie est abélienne (resp. cyclique). Montrer que toute extension séparable finie de \mathbb{K} est abélienne (resp. cyclique).

Un corps dont toute extension galoisienne finie est cyclique est dit corps de Moriya ; les corps finis, les corps algébriquement clos et \mathbb{R} sont de Moriya.

b) Montrer que toute extension finie d'un corps de Moriya est de Moriya.

c) Montrer que, si \mathbb{K} est un corps de Moriya et $m \in \mathbb{N}^*$, \mathbb{K} admet au plus une extension séparable de degré m contenue dans Ω .

d) Réciproquement, montrer que si, pour tout m dans \mathbb{N}^* , il existe au plus une extension séparable de degré m de \mathbb{K} contenue dans ω , alors \mathbb{K} est de Moriya.

e) Soient x un nombre irrationnel algébrique, \mathbb{K} un sous-corps de $\overline{\mathbb{Q}}$ ne contenant pas x et maximal pour l'inclusion parmi les sous-corps de $\overline{\mathbb{Q}}$ possédant cette propriété (l'existence d'un tel corps résulte de la forme dénombrable du lemme de Zorn). Montrer que \mathbb{K} est de Moriya, que $\mathbb{K}(x)/\mathbb{K}$ est de degré premier divisant $[\mathbb{Q}(x) : \mathbb{Q}]$.

24. L'exemple 4 de 3.2 établit ce résultat pour une extension quadratique.

Si \mathbb{K} est un corps et G un groupe fini, on dit que G est un *groupe de Galois sur \mathbb{K}* si et seulement s'il existe une extension galoisienne de \mathbb{K} de groupe G . L'énoncé ci-après est une conséquence immédiate du théorème 10.

Proposition 14. *Si le groupe fini G est un groupe de Galois sur \mathbb{K} , il en est de même de ses quotients.*

Remarque *La théorie de Galois des extensions algébriques infinies*

Krull a étendu la théorie de Galois aux extensions algébriques infinies. Un des sens de la correspondance fonctionne bien : si \mathbb{L}/\mathbb{K} est galoisienne infinie, le cas général du théorème de prolongement des morphismes (chapitre 3, section 4, théorème 4) montre que, pour tout élément \mathbb{K}' de $\mathcal{K}_{\mathbb{L}/\mathbb{K}}$, on a

$$\mathbb{L} \text{Gal}(\mathbb{L}/\mathbb{K}') = \mathbb{K}'.$$

L'autre sens pose problème : il existe des sous-groupes de $\text{Gal}(\mathbb{L}/\mathbb{K})$ qui ne sont pas de la forme $\text{Gal}(\mathbb{L}/\mathbb{K}')$. On comprend la situation en munissant $\text{Gal}(\mathbb{L}/\mathbb{K})$ d'une topologie adéquate, dite *topologie profinie*, qui en fait un groupe topologique compact et totalement discontinu. La correspondance de Galois établit alors une bijection entre les sous-extensions de \mathbb{L}/\mathbb{K} et les sous-groupes fermés de $\text{Gal}(\mathbb{L}/\mathbb{K})$.

Cette généralisation de la théorie de Galois classique a été explicitée par Krull vers 1930. Elle est conceptuellement très satisfaisante et ne présente pas de difficulté majeure une fois acquis le cas fini. Sans véritablement y entrer, indiquons que les ensembles $\text{Gal}(\mathbb{L}/\mathbb{K}')$ pour \mathbb{K}' parcourant $\mathcal{K}_{\mathbb{L}/\mathbb{K}}$ forment une base de voisinage de l'identité pour la topologie profinie et que, si \mathbb{L}/\mathbb{K} est infinie, $\text{Gal}(\mathbb{L}/\mathbb{K})$ contient toujours beaucoup de sous-groupes non fermés.²⁵

Si \mathbb{K} est parfait, Ω/\mathbb{K} est une extension galoisienne dont le groupe décrit les relations entre toutes les équations algébriques à coefficients dans \mathbb{K} . Cette extension est en général infinie, de sorte que la description de ses sous-extensions nécessite la théorie de Krull. Comme on l'a dit dans l'introduction, le groupe de Galois absolu de \mathbb{Q} , c'est-à-dire $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ demeure largement mystérieux. La cyclotomie en décrit les quotients abéliens.²⁶

Exercice 67. ③ *Soit \mathbb{L}/\mathbb{K} une extension galoisienne infinie. Détailler la preuve du fait que, si \mathbb{K}' est un sous-corps de \mathbb{L} contenant \mathbb{K} :*

$$\mathbb{L} \text{Gal}(\mathbb{L}/\mathbb{K}') = \mathbb{K}'.$$

L'exercice suivant, réservé au lecteur familier des corps finis, donne un exemple significatif de groupe de Galois d'une extension infinie.

Exercice 68. ⑤ *Soient $p \in \mathcal{P}$, $\mathbb{K} = \mathbb{F}_p$, \mathbb{L} une clôture algébrique de \mathbb{K} . Décrire $\text{Gal}(\mathbb{L}/\mathbb{K})$*

4 (*) Deux exemples de groupes de Galois sur \mathbb{Q}

Soient G un groupe fini, \mathbb{K} un corps. Disons que G est un *groupe de Galois sur \mathbb{Q}* s'il existe une extension galoisienne \mathbb{L} de \mathbb{K} telle que $\text{Gal}(\mathbb{L}/\mathbb{K})$ soit isomorphe à G . Le théorème 10 entraîne aussitôt le lemme suivant.

Lemme 8. *Soient \mathbb{K} un corps, G un groupe fini. Si G est un groupe de Galois sur \mathbb{K} , il en est de même de tout quotient de G .*

25. On montre par exemple que les sous-groupes fermés infinis de $\text{Gal}(\mathbb{L}/\mathbb{K})$ ne sont pas dénombrables.

26. C'est le contenu du théorème de Kronecker-Weber.

On sait par ailleurs que tout groupe fini de cardinal n se plonge dans \mathcal{S}_n (théorème de Cayley). L'étude de l'équation générale (4.2) permet d'en déduire que, si G est un groupe d'ordre n , G est le groupe de Galois de $\mathbb{K}(X_1, \dots, X_n)/\mathbb{L}$ pour un certain sous-corps \mathbb{L} de $\mathbb{K}(X_1, \dots, X_n)$ contenant $\mathbb{K}(\Sigma_1, \dots, \Sigma_n)$.

Si on impose le corps de base, la question est délicate. Ainsi, le « problème inverse de la théorie de Galois » consiste à demander si tout groupe fini G est un groupe de Galois sur \mathbb{Q} , autrement dit si tout groupe fini est quotient de $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

En 2022, ce problème n'est pas résolu. Nous allons présenter deux cas particuliers simples.

4.1 Les groupes abéliens finis

Nous allons établir le théorème suivant.

Théorème 11. *Soit G un groupe abélien fini. Alors G est un groupe de Galois sur \mathbb{Q} .*

Preuve. Pour $n \in \mathbb{N}^*$, $\text{Gal}_{\mathbb{Q}}(X^n - 1) = \text{Gal}_{\mathbb{Q}}(\Phi_n)$ est isomorphe à $\mathbb{Z}/n\mathbb{Z}^*$. On en déduit le théorème 11 en utilisant le lemme 8 et le résultat suivant.

Lemme 9. *Si G est un groupe fini, il existe $n \in \mathbb{N}^*$ tel que G soit un quotient de $\mathbb{Z}/n\mathbb{Z}^*$.*

Le lemme 9 est lui-même conséquence du cas particulier ci-après du théorème de la progression arithmétique, dont nous indiquons une preuve directe.

Lemme 10. *Soit $m \in \mathbb{N}^*$. Il existe une infinité de nombres premiers p congrus à 1 modulo m .*

Preuve du lemme 9. Le théorème de structure des groupes abéliens finis assure que G est isomorphe à un groupe $C_1 \times \dots \times C_r$ où $r \in \mathbb{N}^*$ et où, pour tout i , C_i est un groupe cyclique. Notons m_i l'ordre de C_i . Le lemme 10 fournit des nombres premiers distincts p_1, \dots, p_r tels que, pour tout i , on ait $p_i \equiv 1 [m_i]$. Si $i \in \{1, \dots, r\}$, le groupe $\mathbb{Z}/p_i\mathbb{Z}^*$ est cyclique d'ordre $p_i - 1$ et admet donc un quotient d'ordre m_i , donc isomorphe à C_i . Si $n = \prod_{i=1}^r p_i$, le groupe $\mathbb{Z}/n\mathbb{Z}^*$ est isomorphe à $\prod_{i=1}^r \mathbb{Z}/p_i\mathbb{Z}^*$ et admet donc un quotient isomorphe à G .

Preuve du lemme 10. Soit $k \in \mathbb{N}^*$ supérieur ou égal à m . Nous allons produire un nombre premier p congru à 1 modulo m et strictement supérieur à k . On considère à cet effet un diviseur premier p de $\Phi_m(k!)$. Comme le terme constant de Φ_m est ± 1 , $\Phi_m(k!)$ est premier à $k!$, ce qui implique que $p > k$. En particulier, p est premier à m .

D'autre part, la réduction modulo p du polynôme Φ_m admet une racine dans \mathbb{F}_p , à savoir la classe x de $k!$ modulo p . Il suffit d'établir que l'ordre ω de x dans \mathbb{F}_p^* est égal à m pour conclure que m divise l'ordre $p - 1$ de \mathbb{F}_p^* . Puisque Φ_m divise $X^m - 1$ dans $\mathbb{Z}[X]$, on a bien sûr que $x^m = 1$ et ω divise m . Reste à voir qu'il y a égalité. C'est là que joue le fait que p est premier à m . En effet, si on avait $\omega < m$, x serait racine de $X^\omega - 1$; on disposerait donc d'un diviseur d de ω tel que x soit racine de la réduction modulo p de Φ_d . Comme $\Phi_m \times \Phi_d$ divise $X^m - 1$ dans $\mathbb{Z}[X]$, x serait racine double de la réduction de $X^m - 1$ modulo p , ce qui entraînerait que p divise m (dérivation).

En 1954, Shafarevich a établi une généralisation difficile du théorème 11 : tout groupe résoluble fini est un groupe de Galois sur \mathbb{Q} (Shafarevich, 1954). La réponse est positive pour de nombreux autres groupes.

4.2 Les groupes symétriques

Le théorème ci-après remonte à Hilbert, la démonstration proposée à Van der Waerden.²⁷

Théorème 12. *Si $n \in \mathbb{N}^*$, \mathcal{S}_n est un groupe de Galois sur \mathbb{Q} .*

Preuve. Sans nuire à la généralité, supposons que $n \geq 3$. On rappelle que, pour tout $m \in \mathbb{N}^*$ et tout nombre premier p , $\mathbb{F}_p[X]$ contient un polynôme irréductible de degré m . Grâce à ce résultat et au théorème chinois, on obtient des polynômes unitaires de degré n , P_2, P_3, P_5 de $\mathbb{Z}[X]$ tels que :

- la réduction de P_2 dans $\mathbb{F}_2[X]$ est irréductible ;
- la réduction de P_3 dans $\mathbb{F}_3[X]$ est produit d'un polynôme irréductible unitaire de degré $n - 1$ et d'un polynôme de degré 1 ;
- la réduction de P_5 dans $\mathbb{F}_5[X]$ est produit d'un polynôme irréductible unitaire de degré 2 et d'un polynôme irréductible de degré impair ou de deux polynômes irréductibles unitaires distincts de degrés impair.

Le théorème chinois donne un polynôme unitaire P de degré n de $\mathbb{Z}[X]$ congru modulo p à P_p pour $p \in \{2, 3, 5\}$; on peut d'ailleurs simplement prendre $P = -15P_2 + 10P_3 + 6P_5$. Le théorème 6 entraîne que $\text{Gal}_{\mathbb{Q}}(P)$ contient un n -cycle, un $n - 1$ -cycle et une transposition. Le lemme ci-après permet de conclure que $\text{Gal}_{\mathbb{Q}}(P)$ est isomorphe à \mathcal{S}_n .

Lemme 11. *Soient $n \geq 3$ un entier, G un sous-groupe transitif de \mathcal{S}_n contenant un $n - 1$ -cycle et une transposition. Alors $G = \mathcal{S}_n$.*

En particulier, si un sous-groupe de \mathcal{S}_n contient une transposition, un $n - 1$ -cycle et un n -cycle, il est égal à \mathcal{S}_n .

Preuve du lemme 11. Soient γ (resp. τ) un $n - 1$ -cycle (resp. une transposition) appartenant à G . Supposons, sans nuire à la généralité, que le point qui n'est pas dans le support de γ est n . Notons $\tau = (ij)$, $i < j$. Si $j = n$, le caractère transitif de l'action de $\langle \gamma \rangle$ sur $\{1, \dots, n - 1\}$ montre que

$$\{\gamma^k \circ \tau \circ \gamma^{-k} ; 0 \leq k \leq n - 1\} = \{(\ell n) ; \ell \in \{1, \dots, n - 1\}\}.$$

Cet ensemble de transpositions engendre \mathcal{S}_n . Si $j \neq n$, on prend g dans G envoyant j sur n et on remarque que $g \circ \tau \circ g^{-1} = (g(i)n)$, ce qui ramène au cas précédent.

Exercice 69. ③ *Soit $P = X^5 + 20X - 16$. On note G le groupe de Galois de P sur \mathbb{Q} , vu comme sous-groupe de \mathcal{S}_5 .*

- a) Calculer le discriminant de P et montrer que $G \subset \mathcal{A}_5$.
- b) En réduisant P modulo 2, 3 et 7, montrer que $G = \mathcal{A}_5$.

Exercice 70. ④ *Soit $P = X^7 - X - 1$. On note G le groupe de Galois de P sur \mathbb{Q} , vu comme sous-groupe de \mathcal{S}_7 .*

- a) Montrer que l'image P_2 de P dans $\mathbb{F}_2(X)$ n'a pas de racine dans \mathbb{F}_8 et en déduire que P_2 est irréductible sur \mathbb{F}_2 .
- b) Soit P_3 l'image de P dans $\mathbb{F}_3[X]$. Montrer que les seules racines de P_3 dans \mathbb{F}_9 sont les racines de $X^2 + X - 1$ et que ces racines sont simples.
- c) Conclure que $G = \mathcal{S}_7$.

²⁷. Qui a en fait établi que la plupart des polynômes unitaires de degré n de $\mathbb{Z}[X]$ ont \mathcal{S}_n pour groupe de Galois sur \mathbb{Q} .

Voici une conséquence du théorème 12.

Corollaire 3. *Si G est un groupe fini, il existe deux corps de nombres \mathbb{K} et \mathbb{L} tels que \mathbb{L} soit extension galoisienne de groupe G de \mathbb{K} .*

Preuve. Prenons $m \in \mathbb{N}^*$ tel que \mathcal{S}_m contienne un sous-groupe G_m isomorphe à G .²⁸ Soient par ailleurs P un polynôme unitaire irréductible de degré m de $\mathbb{Z}[X]$ tel que l'action de $\text{Gal}_{\mathbb{Q}}(P)$ sur l'ensemble des racines de P identifie $\text{Gal}_{\mathbb{Q}}(P)$ à \mathcal{S}_m , $L = D_{\mathbb{Q}}P$. Si \mathbb{K} est le sous-corps \mathbb{L}^{G_m} de \mathbb{L} , alors L/L^{G_m} est galoisienne de groupe G_m .

5 (*) Appendice : le théorème de la base normale

L'énoncé ci-après donne une description intéressante de l'action du groupe de Galois d'une extension galoisienne finie. Utilisé dans certains cas par Dedekind, il a été établi en 1932 par Noether et Deuring.

Théorème 13. *Soit \mathbb{L}/\mathbb{K} une extension galoisienne finie de degré n et de groupe de Galois G . Il existe alors x dans \mathbb{L} tel que $(g(x))_{g \in G}$ soit une base du \mathbb{K} -espace vectoriel \mathbb{L} .²⁹*

Une base normale de \mathbb{L} sur \mathbb{K} est une \mathbb{K} -base de \mathbb{L} formée d'éléments K -conjugués, i.e. de la forme $(g(x))_{g \in G}$. L'énoncé précédent assure donc l'existence d'une telle base.

Preuve du théorème si \mathbb{L}/\mathbb{K} est cyclique, valable en particulier si \mathbb{K} est fini. Soit σ un générateur de G . D'après le théorème d'indépendance des morphismes, $(\sigma^j)_{0 \leq j \leq n-1}$ est une famille \mathbb{K} -libre d'endomorphismes de \mathbb{L} . Le polynôme minimal de l'endomorphisme σ est donc $X^n - 1$. Il est alors classique qu'il existe un élément x de \mathbb{L} tel que le polynôme minimal de σ relatif à x soit $X^n - 1$, i.e. tel que $(x, \sigma(x), \dots, \sigma^{n-1}(x))$ soit une base de \mathbb{L} sur \mathbb{K} .

Preuve du théorème si \mathbb{K} est infini. Notons $G = \{g_1, \dots, g_n\}$. L'indépendance sur \mathbb{L} des g_i et le lemme 7 donnent (e_1, \dots, e_n) dans \mathbb{L}^n tel que

$$A = (g_i(e_j))_{1 \leq i, j \leq n} \in \text{GL}_n(\mathbb{L}).$$

La preuve du lemme d'Artin montre que $e = (e_1, \dots, e_n)$ est une \mathbb{K} -base de \mathbb{L} . Soit \det la fonction déterminant relative à cette base. Il suffit de montrer l'existence de $(x_1, \dots, x_n) \in \mathbb{K}^n$ tel que :

$$\det \left(g_1 \left(\sum_{j=1}^n x_j e_j \right), \dots, g_n \left(\sum_{j=1}^n x_j e_j \right) \right) \neq 0.$$

Soit alors

$$\Delta : \quad \mathbb{L}^n \quad \longrightarrow \quad \mathbb{K} \\ (x_1, \dots, x_n) \quad \longmapsto \quad \det \left(\sum_{j=1}^n x_j g_1(e_j), \dots, \sum_{j=1}^n x_j g_n(e_j) \right).$$

L'application Δ est polynomiale, et l'inversibilité de A montre que

$$\left(\sum_{j=1}^n x_j g_1(e_j), \dots, \sum_{j=1}^n x_j g_n(e_j) \right)$$

28. Par exemple, $m = |G|$ convient grâce au théorème de Cayley, obtenu en faisant agir G sur lui-même par translation.

29. Plus conceptuellement, le théorème de la base normale traduit le fait que la représentation linéaire de G dans le \mathbb{K} -espace vectoriel \mathbb{L} associée à l'action naturelle de G sur \mathbb{L} est équivalente à la représentation régulière de G , c'est-à-dire que \mathbb{L} est isomorphe à $\mathbb{K}[G]$ comme $\mathbb{K}[G]$ -module.

décrit \mathbb{L}^n avec (x_1, \dots, x_n) , donc que Δ n'est pas identiquement nulle. Le corps \mathbb{K} étant infini, Δ n'est pas identiquement nulle sur \mathbb{K}^n , d'où le résultat désiré.

Remarques

1. *Base normale et élément primitif*

Si les \mathbb{K} -conjugués de x forment une base de \mathbb{L} sur \mathbb{K} , x est de degré $[\mathbb{L} : \mathbb{K}]$ sur \mathbb{K} , donc $\mathbb{L} = \mathbb{K}(x)$: le théorème de la base normale implique celui de l'élément primitif pour les extensions galoisiennes.

2. *Généricité*

La démonstration du théorème que l'ensemble des éléments x de \mathbb{L} tels que $(g(x))_{g \in \text{Gal}(\mathbb{L}/\mathbb{K})}$ soit une \mathbb{K} -base de \mathbb{L} est le complémentaire d'une sous-variété algébrique de \mathbb{L} vu comme \mathbb{K} -espace vectoriel.

3. *Base normale et correspondance de Galois*

Le théorème de la base normale permet d'expliciter la sous-extension correspondant à un sous-groupe donné dans la correspondance de Galois. Soit x un élément de \mathbb{L} tel que $(g(x))_{g \in G}$ forme une base de \mathbb{L} sur \mathbb{K} . Soit y un élément de \mathbb{L} . On écrit :

$$y = \sum_{g \in G} \lambda(g)g(x)$$

où les $\lambda(g)$ sont dans K .

Soit maintenant H un sous-groupe de G . Si $h \in H$:

$$h(y) = \sum_{g \in G} \lambda(h^{-1}g)g(x).$$

Par suite, y est fixe par H si et seulement si :

$$\forall h \in H, \quad \lambda(h^{-1}g) = \lambda(g)$$

autrement dit si et seulement si λ est constante sur les classes à gauche selon H . Pour toute classe à gauche Λ selon H , posons :

$$a_\Lambda = \sum_{g \in \Lambda} g(x).$$

Ce qui précède montre que les a_Λ pour Λ parcourant l'ensemble quotient G/H forment une base du sous-corps de \mathbb{L} fixe par H .

4. *Interprétation en termes de représentations*

Avec les notations du théorème 13, \mathbb{L} définit une \mathbb{K} -représentation de G . Le théorème assure que cette représentation est équivalente à la représentation régulière de G .

Le résultat de l'exercice ci-après est souvent attribué à Zolotarev.

Exercice 71. ④ Soient $p \in \mathcal{P}$, $n \in \mathbb{N}^*$, $q = p^n$, $\text{Frob}_{\mathbb{F}_q/\mathbb{F}_p}$ l'endomorphisme de Frobenius de l'extension $\mathbb{F}_q/\mathbb{F}_p$. Quelle est la signature de $\text{Frob}_{\mathbb{F}_q/\mathbb{F}_p}$ vu comme une permutation de \mathbb{F}_q ?

Exercice 72. ④ Soient \mathbb{L}_1 et \mathbb{L}_2 deux extensions finies de \mathbb{K} contenues dans Ω , toutes deux distinctes de \mathbb{K} , $x \in \mathbb{L}_1$ (resp. $y \in \mathbb{L}_2$) tel que $(g(x))_{g \in \text{Gal}(\mathbb{L}_1/\mathbb{K})}$ (resp. $(g(y))_{g \in \text{Gal}(\mathbb{L}_2/\mathbb{K})}$) forme une \mathbb{K} -base de \mathbb{L}_1 (resp. \mathbb{L}_2). Montrer que la famille $(g(x+y))_{g \in \text{Gal}(\mathbb{L}_1\mathbb{L}_2/\mathbb{K})}$ n'est pas une base de $\mathbb{L}_1\mathbb{L}_2$ sur \mathbb{K} .