Théorie des corps

Christophe Reutenauer
Laboratoire de combinatoire et d'informatique mathématique,
Université du Québec à Montréal
Case postale 8888, succursale Centre-ville
Montréal (Québec) H3C 3P8, Canada

9 octobre 2024

Table des matières

1 Introduction

C'était un ingénieur ! un mathématicien !!! où diable la sensibilité va-t-elle se nicher !
Hector Berlioz
Mémoires

Ces notes de cours s'appuient sur un manuscrit que j'ai rédigé voilà un demi-siècle ; celui-ci était fortement inspiré des livres classiques de Bartel Leendert van der Waerden [4] [1] et de de Serge Lang [2]. J'ai retrouvé ce manuscrit en cherchant, au fin fond de ma maison dans l'Aveyron, le manuscrit de ma thèse de doctorat (je n'ai pas retrouvé celui-ci).

Remerciements : Patricia Sorya, Simon Malenfant, et particulièrement Philip Pinard-Macmaniman pour avoir lu soigneusement, relevé de nombreuses coquilles et suggéré des changements.

1. Celles-ci s'appuient, comme le dit l'auteur dans sa préface, sur des notes de cours donnés par Emil Artin à Hambourg et par Emmy Noether à Erlangen, il y a un siècle environ ; nous voila donc en bonne compagnie

2 Extensions algébriques

En haut lieu, les mathématiques succèdent aux spéculations métaphysiques devenues vaines.
Manifeste du refus global
Borduas et al. 1948

2.1 Dimension d'une extension, sous-corps premier

Tous les corps considérés sont supposés commutatifs, avec au moins deux éléments (de manière équivalente, $0 \neq 1$). Un homomorphisme d'un corps vers un autre envoie 0 sur 0 et 1 sur 1 ; on en déduit qu'il est toujours injectif (exercice 2.1). S'il est aussi surjectif, c'est donc un *isomorphisme*. Si les deux corps sont égaux, on parle d'*automorphisme*.

Si Γ est un sous-corps du corps Δ, on dit aussi que Δ est un *sur-corps* ou une *extension* de Γ. Dans ce cas, Δ est un espace vectoriel sur Γ : la loi externe est induite par la multiplication de Δ. On note $[\Delta : \Gamma]$ sa dimension ; on l'appelle aussi le *degré de l'extension* $\Gamma \subset \Delta$. Comme exemples, on a $[\mathbb{C} : \mathbb{R}] = 2$ et $[\mathbb{R} : \mathbb{Q}] = \infty$ (Exercice 2.2).

Si K, L sont deux extensions du corps Δ, on dit qu'un isomorphisme d'anneau de K vers L est un Δ-*isomorphisme* si tout élément de Δ est fixé par l'isomorphisme. Dans ce cas, c'est aussi une application linéaire de K vers L en tant qu'espaces vectoriels sur Δ, et donc un isomorphisme d'espace vectoriel. Par exemple, la conjugaison complexe $z \mapsto \bar{z}$ est un $\mathbb{R}$-automorphisme de $\mathbb{C}$.

Théorème 2.1. *(multiplicativité de la dimension) Soient $K \subset L \subset M$ trois corps, chacun sous-corps du suivant. Alors $[M : K] = [M : L][L : K]$.*

Définition 2.1. *Soit Σ un corps. On appelle* corps premier *de Σ l'intersection de tous les sous-corps de Σ.*

Le corps premier de Σ est le plus petit sous-corps de Σ.

Théorème 2.2. *1. Si la caractéristique p de Σ est non nulle, alors p est premier et le sous-corps premier de Σ est isomorphe à $\mathbb{Z}/p\mathbb{Z}$.*

2. Si elle est nulle, alors le sous-corps premier de Σ est isomorphe à $\mathbb{Q}$.

3. Tout automorphisme de Σ fixe son sous-corps premier point par point.

On dit que ϕ *fixe E point par point* si la restriction de ϕ à E est l'identité ; c'est-à-dire $\forall x \in E$, $\phi(x) = x$.

Théorème 2.3. *Si la caractéristique p de Σ est non nulle, alors quel que soit f dans $\mathbb{N}$, on a : $\forall a, b \in \Sigma$, $(a+b)^{p^f} = a^{p^f} + b^{p^f}$ et $(a-b)^{p^f} = a^{p^f} - b^{p^f}$.*

Démonstration. Par la formule du binôme, on a $(a+b)^p = \sum_{k=0}^{k=p} \binom{p}{k} a^k b^{p-k} = a^p + b^p + \sum_{k=1}^{k=p-1} \binom{p}{k} a^k b^{p-k} = a^p + b^p$ car les coefficients binomiaux $\binom{p}{k}$ sont divisibles par p pour $k = 1, \ldots, p-1$. Ceci prouve la première formule du théorème pour $f = 1$ et le raisonnement se poursuit aisément par récurrence sur f. La second formule découle de la première et des égalités $(a-b)^{p^f} + b^{p^f} = ((a-b)+b)^{p^f} = a^{p^f}$. □

EXERCICES

Exercice 2.1. *Montrer que si f est un homomorphisme d'anneaux de K vers L, alors f envoie tout élément inversible de K sur un élement inversible de L. En déduire que si K est un corps, alors f est injectif.*

Exercice 2.2. *Montrer que $[\mathbb{R} : \mathbb{Q}] = \infty$.*

Exercice 2.3. *Soit E une partie du corps k. Montrer que l'intersection des sous-corps de k qui contiennent E est égal au plus petit sous-corps de k qui contient E. Ce corps est appelé le sous-corps de k* engendré *par E.*

2.2 Adjonction

Définition 2.2. *Soit Δ un sous-corps du corps Ω.*

1. Soit E une partie de Ω ; on note $\Delta(E)$ le sous-corps de Ω engendré par $\Delta \cup E$ et on dit que $\Delta(E)$ s'obtient de Δ par adjonction *des éléments de E.*

2. Si $E = \{u_1, \ldots, u_n\}$, on le note aussi $\Delta(u_1, \ldots, u_n)$; la notation $\Delta[u_1, \ldots, u_n]$ désigne le sous-anneau de Ω engendré par $\Delta \cup E$.

3. Si les E_i, $i = 1, \ldots, n$, sont des sous-corps de Ω contenant tous Δ comme sous-corps, $\Delta(\cup_i E_i)$ est noté aussi $E_1 \cdots E_n$, et appelé le composé *des sous-corps $E_1, \ldots, E_n$.*

Proposition 2.1. *(i) On a $\Delta(E_1 \cup E_2) = \Delta(E_1)(E_2)$.*

(ii) Si $E_1 \subset E_2$, alors $\Delta(E_1) \subset \Delta(E_2)$.

(iii) Si $\sigma : \Omega \to \Omega$ est un Δ-homomorphisme d'anneaux (c'est-à-dire $\sigma|\Delta$ est l'identité de Δ), alors $\sigma(\Delta(E)) = \Delta(\sigma(E))$.

On utilise dans la preuve qui suit le fait que, par définition, $\Delta(E)$ contient Δ et E ; et que c'est le plus petit sous-corps de Ω ayant cette propriété (donc si un sous-corps de Ω contient Δ et E, il contient $\Delta(E)$) : voir exercice 2.3.

Démonstration. (i) $\Delta(E_1)(E_2)$ contient $\Delta(E_1)$ et E_2, donc aussi Δ, E_1 et E_2, donc aussi Δ et $E_1 \cup E_2$, et enfin $\Delta(E_1 \cup E_2)$.

Réciproquement, $\Delta(E_1 \cup E_2)$ contient Δ et $E_1 \cup E_2$, donc Δ, E_1 et E_2, donc $\Delta(E_1)$ et E_2 et enfin $\Delta(E_1)(E_2)$.

(ii) $\Delta(E_2)$ est un sous-corps de Ω, qui contient Δ et E_1 (car il contient E_2) ; donc il contient $\Delta(E_1)$.

(iii) Supposons que σ soit un Δ-isomorphisme $\Omega_1 \to \Omega_2$ (deux corps), et E une partie de Ω_1. Alors $\sigma(\Delta(E))$ est un sous-corps de Ω_2 qui contient $\sigma(\Delta) = \Delta$ et $\sigma(E)$; donc il contient $\Delta(\sigma(E))$; nous avons donc l'inclusion $\Delta(\sigma(E)) \subset \sigma(\Delta(E))$. Appliquant cette inclusion au Δ-isomorphisme σ^{-1} et à la partie $\sigma(E)$ de Ω_2, nous obtenons l'inclusion $\Delta(\sigma^{-1}(\sigma(E)) \subset \sigma^{-1}(\Delta(\sigma(E))$; donc, appliquant σ de chaque côté, $\sigma(\Delta(E)) \subset (\Delta(\sigma(E))$. En conclusion : $\sigma(\Delta(E)) = (\Delta(\sigma(E))$

Revenons à (iii) : on applique ce que nous venons de prouver au Δ-isomorphisme $\sigma : \Omega \to \sigma(\Omega)$. □

EXERCICES

Exercice 2.4. *Montrer que pour obtenir le corps obtenu de $\mathbb{Q}$ en y adjoignant les $\sqrt{n}$, $n \in \mathbb{N}$, il suffit d'adjoindre à $\mathbb{Q}$ les $\sqrt{n}$ où n est sans carré (non divisible par un carré).*

Exercice 2.5. *Soit K un sous-corps de $\mathbb{C}$ et $n \in \mathbb{N}$. Montrer que $\{a + b\sqrt{n}, a, b \in K\}$ est un sous-corps de $\mathbb{C}$. En déduire que ce corps est de degré 1 ou 2 sur K et qu'il est égal à $K(\sqrt{n})$.*

Exercice 2.6. *Montrer que les deux sous-ensembles suivants sont des sous-corps de $\mathbb{C}$: $\{a + ib, a, b \in \mathbb{Q}\}, \{a + \frac{-1+i\sqrt{3}}{2}b, a, b \in \mathbb{Q}\}$. En déduire qu'ils sont égaux à $\mathbb{Q}(i)$ et $\mathbb{Q}(\frac{-1+i\sqrt{3}}{2})$.*

Exercice 2.7. *Montrer que l'équation $\sqrt{3} = x + y\sqrt{2}$ n'a pas de racine dans $\mathbb{Q}$. En déduire que $\sqrt{3}$ n'est pas dans $\mathbb{Q}(\sqrt{2})$ (utiliser l'exercice 2.5). En déduire que $[\mathbb{Q}(\sqrt{2})(\sqrt{3}) : \mathbb{Q}(\sqrt{2})] = 2$ (utiliser le même exercice) et que $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$. Montrer que $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$ forment une base de $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ sur $\mathbb{Q}$ (imiter la preuve du théorème 2.1).*

Exercice 2.8. *Montrer que pour tout $i, j = \pm 1$, la fonction $a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6} \mapsto a + ib\sqrt{2} + jc\sqrt{3} + ijd\sqrt{6}$, $a, b, c, d \in \mathbb{Q}$, est un automorphisme du corps de l'exercice précédent. Montrer que tout automorphisme de ce corps est de cette forme (montrer que $\sqrt{2}$ est envoyé sur $\pm$ lui-même, et idem pour $\sqrt{3}$).*

Exercice 2.9. *Quel est le degré sur* $\mathbb{Q}$ *du corps* $\mathbb{Q}(\sqrt{2}, i)$ *? Imiter ce qui se fait dans l'exercice 2.7.*

Exercice 2.10. *Montrer que* $\Delta(E)$ *est l'ensemble des éléments de* Ω *qui s'expriment comme des fractions rationnelles à coefficients dans* Δ *en un nombre fini d'éléments de* E*.*

2.3 Extension simple

On suppose que Δ est un sous-corps du corps Ω et que θ est un élément de Ω. Le corps $\Delta(\theta)$ est appelé une *extension simple* de Δ.

Définition 2.3. θ *est dit* algébrique sur Δ *s'il existe un polynôme non nul* $P \in \Delta[x]$ *tel que* $P(\theta) = 0$*. Si* θ *n'est pas algébrique sur* Δ*, on dit qu'il est* transcendant sur Δ.

Si $\theta \in \Delta$, il est algébrique sur Δ (on prend $P = x - \theta$).

Proposition 2.2. θ *est algébrique sur* Δ *si et seulement si les puissances de* θ *sont linéairement dépendantes sur* Δ*.*

Ainsi l'algèbre linéaire rentre dans le sujet.

L'extension simple $\Delta(\theta)$ de Δ est dite *algébrique* (resp. *transcendante*) si θ est algébrique (resp. transcendant).

On rappelle que tout idéal I de $\Delta[x]$ est *principal* : ceci signifie qu'il existe un polynôme φ dans $\Delta[x]$ tel que $I = (\varphi) = \{\varphi P, P \in \Delta[x]\}$. Un tel φ s'appelle alors un *générateur* de I. Tous les générateurs de I sont alors les polynômes $\alpha\varphi$, avec α dans Δ, non nul. Ces générateurs sont exactement les éléments de $I \setminus 0$ de degré minimum. Parmi ces générateurs, il y en a un qui est distingué, et unique : c'est celui dont le coefficient dominant vaut 1.

Théorème 2.4. *1. Si* θ *est algébrique sur* Δ*, alors* $\Delta(\theta)$ *est isomorphe à* $\Delta[x]/(\varphi)$*, où* $\varphi(x)$ *est un générateur de l'idéal* $\{P \in \Delta[x], P(\theta) = 0\}$ *de* $\Delta[x]$*.*

2. Si θ *est transcendant sur* Δ*, alors* $\Delta(\theta)$ *est isomorphe au corps des fractions rationnellles* $\Delta(x)$*.*

La preuve montrera que les isomorphismes sont des Δ-*homomorphismes*, c'est-à-dire qu'ils fixent chaque élément de Δ.

Lemme 2.1. *Si* f *est un* Δ*-isomorphisme, alors* $f(P(\theta)) = P(f(\theta))$ *pour tout polynôme à coefficients dans* Δ *: en effet,* $f(x) = \sum_i a_i x^i$*,* $a_i \in \Delta$*, donc* $f(P(\theta)) = f(\sum_i a_i \theta^i) = \sum_i f(a_i) f(\theta)^i = \sum_i a_i f(\theta)^i = P(f(\theta))$.

Preuve du Théorème 2.4. Soit f la fonction $\Delta[x] \to \Delta(\theta)$, $P \mapsto P(\theta)$. Il est bien défini, car $P(\theta)$ est bien un élément de $\Delta(\theta)$. De plus, c'est un Δ-homomorphisme d'anneaux ; en particulier, $\mathrm{Im}(f)$ contient Δ.

Supposons que θ soit algébrique. Alors f n'est pas injectif. L'idéal $\mathrm{Ker}(f)$ n'est pas nul : soit φ un générateur de cet idéal. Alors $\Delta[x]/(\varphi)$ est isomorphe à $\mathrm{Im}(f)$. Comme ce dernier anneau est un sous-anneau de Ω, il est intègre. Donc $\Delta[x]/(\varphi)$ est intègre et il s'ensuit que φ est un polynôme irréductible et par suite $\Delta[x]/(\varphi)$ est un corps, de même que $\mathrm{Im}(f)$; comme celui-ci contient Δ et θ, il contient $\Delta(\theta)$, et celui-ci est donc égal à $\mathrm{Im}(f)$.

Supposons que θ soit transcendant sur Δ. Alors f est injectif, $\Delta[x]$ est isomorphe à $\mathrm{Im}(f) = \Delta[\theta]$. Comme $\Delta(\theta)$ est un corps contenant le sous-anneau $\Delta[\theta]$ et qu'il est engendré par lui, ce corps est nécessairement isomorphe à $\Delta(x)$. □

Définition 2.4. *Dans le cas 1 du théorème, soit n le degré de φ. On l'appelle le* degré *de θ sur Δ et on dit que θ est* algébrique de degré n sur Δ. *Si φ est* unitaire *(c'est-à-dire de coefficient dominant 1), on l'appelle le* polynôme minimal *de θ sur Δ.*

Ce polynôme est uniquement déterminé par θ.

Proposition 2.3. *Le polynôme minimal de θ est l'unique polynôme irréductible unitaire dont θ est racine.*

Proposition 2.4. *Soit $\varphi(x)$ un polynôme irréductible unitaire dans $\Delta[x]$. Alors $k[x]/(\varphi)$ est une extension de k, où $\varphi(x)$ a la racine $\theta = x \mod \varphi$, et c'est l'extension simple $k(\theta)$.*

On sait ainsi construire une extension de k où un polynôme irréductible donné a une racine.

Proposition 2.5. *Si θ est algébrique de degré n sur Δ, alors chaque élément de $\Delta(\theta)$ s'écrit de manière unique sous la forme $P(\theta)$, où P est un polynôme dans $\Delta[x]$ de degré au plus n. La dimension du Δ-espace vectoriel $\Delta(\theta)$ est n. De plus, $\Delta(\theta) = \Delta[\theta]$.*

Définition 2.5. *Deux extensions simples $\Delta(\alpha)$ et $\Delta(\beta)$ de Δ sont dites* équivalentes *s'il existe un Δ-isomorphisme de l'une vers l'autre qui envoie α sur β.*

Théorème 2.5. *Deux extensions simples transcendantes sont toujours équivalentes.*

Démonstration. Elles sont en effet toutes deux Δ-isomorphes à $\Delta(x)$. □

Théorème 2.6. *Deux extensions simples algébriques $\Delta(\theta_1)$ et $\Delta(\theta_2)$ de Δ sont équivalentes si et seulement si θ_1 et θ_2 ont le même polynôme minimal sur Δ. Il existe alors un Δ-isomophisme $\Delta(\theta_1) \to \Delta(\theta_2)$ qui envoie θ_1 sur θ_2.*

Démonstration. Supposons que φ soit un polynôme irréductible ayant ces deux éléments comme racines. La fonction $P(\theta_1) \mapsto P(\theta_2)$, P polynôme de degré au plus $\deg(\varphi)$, est par la proposition un Δ-isomorphisme de $\Delta(\theta_1)$ vers $\Delta(\theta_2)$.

Réciproquement, soit f un Δ-isomorphisme de $\Delta(\theta_1)$ vers $\Delta(\theta_2)$ qui envoie θ_1 sur θ_2. Soit φ le polynôme minimal de θ_1 ; comme f est un Δ-isomorphisme, on $0 = f(\varphi(\theta_1)) = \varphi(f(\theta_1)) = \varphi(\theta_2)$. Donc les deux éléments ont le même polynôme minimal sur Δ. □

Théorème 2.7. *Soit φ un polynôme irréductible sur Δ. Il existe à équivalence près une et une seule extension algébrique simple $\Delta(\theta)$ telle que le polynôme minimal de θ soit φ.*

Démonstration. Nous avons déjà vu l'unicité. Pour l'existence, on remarque que le corps $\Delta[x]/(\varphi)$ répond à question : ce corps contient Δ comme sous-corps, car φ est de degré au moins 1 ; l'image θ de x par l'homomorphisme canonique $p : \Delta[x] \to \Delta[x]/(\varphi)$ (qui est un Δ-homomorphisme) a pour polynôme minimal φ ; de plus ce corps est égal à $\Delta(\theta)$. □

Théorème 2.8. *Il existe à équivalence près une et une seule extension transcendante simple de Δ.*

Démonstration. C'est le corps des fractions rationnelles $\Delta(x)$. □

EXERCICES

Exercice 2.11. *Montrer que $x^3 - 2$ est irréductible dans $\mathbb{Q}[x]$ (utiliser le critère d'Eisenstein, exercice 2.17). En déduire que $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$.*

Exercice 2.12. *Montrer que $\mathbb{Q}(\sqrt[3]{2}, \sqrt{3})$ est de degré 6 sur $\mathbb{Q}$ (montrer qu'il est divisible par 2 et 3, en utilisant l'exercice précédent ; montrer que ce corps est de degré au plus 3 sur $\mathbb{Q}(\sqrt{3})$).*

Exercice 2.13. *Pourquoi l'argument donné après la définition 2.3 ne marche-t-il pas si $\theta \in \Omega \setminus \Delta$?*

Exercice 2.14. *Soit k un corps. Soit f un polynôme irréductible dans $k[x]$, et g un polynôme non nul de degré inférieur à celui de f. En utilisant l'équation de Bezout pour les polynômes f et g, exprimer l'inverse de g* mod *f dans le corps $k[x]/(f)$ par un polynôme de degré $< \deg(f)$.*

Exercice 2.15. *Appliquer l'exercice précédent pour exprimer l'inverse de $\sqrt[3]{2}$ comme combinaison $\mathbb{Q}$-linéaire de $1, \sqrt[3]{2}, \sqrt[3]{4}$.*

Exercice 2.16. *Montrer que si α est envoyé sur β par un k-isomorphisme, alors ces deux éléments ont le même polynôme minimal sur k.*

Exercice 2.17. *Critère d'Eisenstein : soit p un nombre premier et $P(x) = a_n x^n + \cdots + a_1 x + a_0$ un polynôme à coefficients dans $\mathbb{Z}$ tels que p ne divise pas a_n, p divise $a_{n-1}, \ldots, a_1$ et p^2 ne divise pas a_0. Montrer que $P(x)$ est irréductible dans $\mathbb{Q}[x]$.*

Exercice 2.18. *Montrer que si k est de caractéristique 0, alors tout homomorphisme défini sur k est un $\mathbb{Q}$-automorphisme.*

Exercice 2.19. *Montrer que si θ est algébrique sur F, alors il l'est sur E et que le polynôme minimal de θ sur E divise celui sur F (ici F est un sous-corps de E, lui-même sous-corps de Ω, et $\theta \in \Omega$).*

Exercice 2.20. *Pour tout polynôme non constant sur k, construire une extension de k où il a une racine.*

Exercice 2.21. ** Soient K, L des extensions finies de k, toutes deux sous-corps d'un même corps. On suppose que $K = k(\alpha)$ et que $[KL : k] = [K : k][L : k]$. Montrer que $K \cap L = k$. Indication : Montrer que $[KL : L] = [K : k]$, que $KL = L(\alpha)$, que le polynôme minimal $f(x)$ de α sur k est irréductible sur L, donc sur $K \cap L$, que $K = (K \cap L)(\alpha)$ et enfin que $[K \cap L : k] = 1$.*

2.4 Extensions algébriques

Δ est un corps.

Définition 2.6. *Soit Σ une extension de Δ. On dit que Σ est une extension* finie *(resp.* algébrique*) si Σ est un espace vectoriel de dimension finie sur Δ (resp. si tout élément de Σ est algébrique sur Δ).*

Proposition 2.6. *Si la dimension sur Δ de Σ est n, alors tout élément de Σ est algébrique de degré au plus n sur Δ.*

Démonstration. En effet, si $\alpha \in \Sigma$, les éléments $1, \alpha, \ldots, \alpha^n$ sont linéairement dépendants sur Δ. □

Proposition 2.7. *Une extension de Δ est finie si et seulement si elle s'obtient de Δ par adjonction d'un nombre fini d'éléments algébriques sur Δ.*

Démonstration. Si Σ est une extension finie de Δ, de dimension n sur Δ, et si $\alpha \in \Sigma$, alors α est algébrique sur Δ (proposition 2.6). De plus, soit E une base de Σ vu comme espace vectoriel sur Δ. Alors clairement $\Sigma = \Delta(E)$.

Réciproquement, supposons que Σ s'obtienne de Δ en y adjoignant E, dont chaque élément est algébrique sur Δ. S'il n'y a qu'un seul élément dans E, l'extension est simple et la proposition découle dans ce cas de la proposition 2.5. Le cas général se déduit par récurrence, en utilisant le théorème 2.1, sachant que si θ est algébrique sur un corps, il l'est aussi sur tout surcorps. □

Corollaire 2.1. *Les somme, différence, produit et quotient d'éléments algébriques sont algébriques.*

Démonstration. En effet, si α, β sont algébriques sur Δ, le corps $\Delta(\alpha, \beta)$ est, d'après la proposition, une extension finie de Δ, donc tout élement y est algébrique. Ce corps contient les quatre éléments du corollaire. □

Corollaire 2.2. *Toute extension de Δ obtenue par adjonction d'élements algébriques est algébrique.*

Démonstration. En effet, tout élément est contenu dans une sous-extension obtenue par adjonction d'un nombre fini d'éléments, laquelle est donc finie par la proposition, donc algébrique, donc l'élément est algébrique. □

Proposition 2.8. *Si α est algébrique sur Σ et si Σ est une extension algébrique de Δ, alors α est algébrique sur Δ.*

Démonstration. Supposons que $\sum_{k=0}^{k=n} a_k \alpha^k = 0$ avec les a_k dans Σ, non tous nuls. Le corps $\Sigma' = \Delta(a_0, \ldots, a_n)$ est par la proposition 2.7 une extension finie de Δ ; comme α est algébrique sur Σ', la dimension de $\Sigma'(\alpha)$ sur Σ' est finie. Donc par le théorème 2.1, celle de $\Sigma'(\alpha)$ sur Δ est finie, et le corps $\Sigma'(\alpha)$ est algébrique sur Δ, et en particulier α l'est. □

Corollaire 2.3. *Une extension algébrique d'une extension algébrique de Δ est une extension algébrique de Δ.*

On peut donc dire que la notion d'extension algébrique est transitive.
EXERCICES

Exercice 2.22. *Montrer que si α est dans une extension de k, alors α est algébrique sur $k(\alpha^2)$. Montrer que si $\alpha \notin k(\alpha^2)$, alors $[k(\alpha) : k(\alpha^2)] = 2$.*

Exercice 2.23. *Montrer que si α et β sont algébriques de degré n, p respectivement, alors $\alpha+\beta$ est algébrique de degré au plus np.*

2.5 Corps de décomposition d'un polynôme

x est une indéterminée.

Nous avons vu que si $\varphi(x)$ est un polynôme à coefficients dans le corps Δ, alors il existe une extension finie de Δ où $\varphi(x)$ a une racine. En effet, si $\varphi(x)$ est irréductible sur Δ, alors on peut prendre le corps $\Delta[x]/(\varphi(x))$; x mod φ est une racine de φ, et la dimension sur Δ de l'extension est $\deg(\varphi)$. Si ϕ n'est pas irréductible, on prend un diviseur irréductible de φ, et on fait la construction précédente.

Si $\varphi \in \Delta[x]$ est irréductible, on appelle *corps de rupture* de $\varphi(x)$ une extension où φ a une racine θ, et qui est égale à $\Delta(\theta)$.

Définition 2.7. *Soit $f \in \Delta[x]$. On appelle* corps de décomposition *de f une extension Σ de Δ telle qu'il existe $a \in \Delta$ et $\alpha_1, \ldots, \alpha_n \in \Sigma$ tels que $f = a(x-\alpha_1)\cdots(x-\alpha_n)$ et que $\Sigma = \Delta(\alpha_1, \ldots, \alpha_n)$.*

Remarquez que Σ est une extension finie de Δ, par la proposition 2.7.

Si f satisfait l'équation ci-dessus, on dit que *f se décompose complètement (en facteurs linéaires)* dans Σ ; on dit aussi que *f a toutes ses racines dans Σ*. Le *multi-ensemble* (ce qui signifie un ensemble avec répétitions) $\{\alpha_1, \ldots, \alpha_n\}$ est appelé le *multi-ensemble des racines de f*.

Proposition 2.9. *Tout polynôme f a un corps de décomposition.*

Preuve par récurrence sur le degré de f. Si le degré est 1, on prend le corps Δ. Soit $n \geq 2$ le degré de f. Soit $\varphi \in \Delta[x]$ un diviseur irréductible de f. Il existe par le théorème 2.7 une extension simple $\Delta(\theta)$ telle que $\varphi(\theta) = 0$. Dans $\Delta(\theta)[x]$, on a $f = (x-\theta)g$, $g \in \Delta(\theta)[x]$. Comme g est de degré $n-1$, il existe par hypothèse de récurrence un sur-corps Σ de $\Delta(\theta)$ tel que $g = a(x-\theta_2)\cdots(x-\theta_n)$ et $\Sigma = \Delta(\theta)(\theta_2, \ldots, \theta_n)$. D'où $f = a(x-\theta)(x-\theta_2)\cdots(x-\theta_n)$ et, par la proposition 2.1, $\Sigma = \Delta(\theta, \theta_2 \ldots, \theta_n)$. □

Lemme 2.2. *Soient Δ et Γ deux corps et $f : \Delta \to \Gamma$ un isomorphisme. Soit F l'isomorphisme $\Delta[x] \to \Gamma[x]$ induit par f. Si $\varphi \in \Delta[x]$ est irréductible, alors $\bar{\varphi} = F(\varphi)$ est irréductible dans $\Gamma[x]$. Si dans des extensions respectives de Δ et Γ, α et $\bar{\alpha}$ sont des racines de φ et $\bar{\varphi}$ respectivement, alors f se prolonge en un isomorphisme $\bar{f} : \Delta(\alpha) \to \Gamma(\bar{\alpha})$ tel que $\bar{f}(\alpha) = \bar{\alpha}$.*

Démonstration. L'isomorphisme $\bar{f}$ cherché est donné par $\bar{f}(\sum a_k \alpha^k) = \sum f(a_k)\bar{\alpha}^k$, quels que soient a_k dans Δ. □

Proposition 2.10. *Soient Δ et Γ deux corps et $f : \Delta \to \Gamma$ un isomorphisme. Soit F l'isomorphisme $\Delta[x] \to \Gamma[x]$ induit par f. Soit $\varphi \in \Delta[x]$ et $\psi = F(\varphi)$. Soit $\Delta_1 = \Delta(\alpha_1, \ldots, \alpha_n)$ et $\Gamma_1 = \Gamma(\beta_1, \ldots, \beta_n)$ des corps de décomposition de φ et ψ respectivement, où $\{\alpha_1, \ldots, \alpha_n\}$ (resp. $\{\beta_1, \ldots, \beta_n\}$) est le multi-ensemble des racines de φ (resp. de ψ). Alors f se prolonge en un isomorphisme $\bar{f}$ de Δ_1 sur Γ_1 tel qu'il existe une permutation σ de $\{1, \ldots, n\}$ satisfaisant $\bar{f}(\alpha_i) = \beta_{\sigma(i)}$.*

Démonstration. Soit n le degré de φ et ψ. Si $n = 1$, alors $\Delta_1 = \Delta$, $\Gamma_1 = \Gamma$ et on prend $\bar{f} = f$. Soit $n \geq 2$ et supposons que le théorème soit vrai pour les degrés au plus $n - 1$. Soit φ_1 un diviseur irréductible de φ dans $\Delta[x]$. Alors $F(\varphi_1) = \psi_1$ est un diviseur irréductible de ψ dans $\Gamma[x]$. Soient α_i et β_j des racines de φ_1 et ψ_1 respectivement ; on peut sans perte de généralité supposer que $i = j = 1$. D'après le lemme précédent, il existe un isomorphisme $f_1 : \Delta(\alpha_1) \to \Gamma(\beta_1)$ prolongeant f et tel que $f_1(\alpha_1) = \beta_1$. Posons $\varphi = (x - \alpha_1)\varphi_2$ et $\psi = (x - \beta_1)\psi_2$, $\varphi_2 \in \Delta(\alpha_1)[x]$, $\psi_2 \in \Gamma(\beta_1)[x]$. Alors, notant F_1 l'isomorphisme $\Delta(\alpha_1)[x] \to \Gamma(\beta_1)[x]$ induit par f_1, on a $F_1(\varphi_2) = \psi_2$. Donc f_1 se prolonge par hypothèse de récurrence en un isomorphisme $\bar{f}$ de Δ_1 sur Γ_1, car Δ_1 (resp. Γ_1) est un corps de décomposition de φ_2 (resp. ψ_2) ; ceci implique aussi qu'il existe une permutation τ de $\{2, \ldots, n\}$ telle que $\bar{f}(\alpha_i) = \beta_{\tau(i)}$ pour $i = 2, \ldots, n$ et achève la preuve. □

Corollaire 2.4. *Tous les corps de décomposition de $\varphi \in \Delta[x]$ sont Δ-isomorphes.*

Démonstration. On prend dans la proposition $\Delta = \Gamma$ et pour f l'identité de Δ ; alors $\varphi = \psi$. □

Proposition 2.11. *Si deux corps de décomposition de φ sont contenus dans un même sur-corps Ω, alors ils sont égaux.*

Démonstration. Ceci résulte de l'unicité de la décomposition dans $\Omega[x]$ de φ en facteurs linéaires. □

EXERCICES

Exercice 2.24. *Montrer que les nombres $i\sqrt{3}$ et $1 + i\sqrt{3}$ sont racines du polynôme $x^4 - 2x^3 + 7x^2 - 6x + 12$. Existe-t-il un $\mathbb{Q}$-automorphisme du corps de décomposition de ce polynôme qui envoie l'une sur l'autre ?*

Exercice 2.25. *On suppose que la caractéristique de k est $\neq 2$. Montrer que le corps de décomposition du polynôme $ax^2 + bx + c \in k[x]$, $a \neq 0$, est $k(\sqrt{b^2 - 4ac})$.*

Exercice 2.26. *Montrer que le corps de décomposition de $f(x)$ est égal à celui de f^m, $m \geq 1$.*

Exercice 2.27. *Quel est le corps de décomposition sur $\mathbb{Q}$ du polynôme $(x^2-2)(x^2-8)$?*

2.6 Clôtures algébriques

k est un corps commutatif.

Définition 2.8. *1. Un corps est dit* algébriquement clos *si tout polynôme de degré au moins un y a une racine.*

2. Un sur-corps de k est une clôture algébrique *de k si c'est une extension algébrique qui est algébriquement close.*

On remarque qu'un corps est algébriquement clos si et seulement si tous les polynômes y ont toutes leurs racines (exercice 2.30) ; de manière équivalente, il n'a pas d'extension algébrique autre que lui-même (exercice 2.31).

Théorème 2.9. *Il existe une extension E de k qui est algébriquement close.*

Lemme 2.3. *Pour tout ensemble fini H de polynômes de degré ≤ 1 de $k[x]$, il existe une extension de k où chaque élément de H a une racine.*

Démonstration. Pour un polynôme P, on prend un diviseur irréductible Q de P ; alors Q, donc P, a la racine $x \mod Q$ dans l'extension $k[x]/(Q)$ de k. Quand on a plusieurs polynômes $P_1, P_2, \ldots$, on trouve d'abord une extension K_1 de k où P_1 a une racine, puis une extension K_2 de K_1 où P_2 a une racine (donc P_1, P_2 y ont chacun une racine), etc... □

Une *k-algèbre* est un anneau qui contient k en son centre. Exemples : $k[x], k[x,y]$, l'algèbre des matrices carrées sur k d'une taille donnée. Si A est une k-algèbre et $P(x) \in k[x]$, une racine de P dans A est un élément a de A tel que $P(a) = 0$. Par exemple, la matrice $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ est une racine du polynôme x^2+1. Tout quotient non nul d'une k-algèbre est une k-algèbre. Tout corps qui est une k-algèbre est une extension de k.

Lemme 2.4. *Soit T un ensemble de variables, $k[T]$ la k-algèbre des polynômes en les variables $t \in T$ à coefficients dans k, $t_1, \cdots, t_n$ n variables distinctes dans T, $P_1 = P_1(t_1), \ldots, P_n = P_n(t_n) \in k[T]$ (seule la variable t_i apparaît dans P_i). On suppose que dans une extension K de k, chaque polynôme P_i a une racine. Il n'existe pas de polynômes $Q_1, \ldots, Q_n \in k[T]$ tels que $\sum_i P_i Q_= 1$*

Démonstration. Soient α_i une racine de P_i dans une extension de k. Supposons qu'on ait $1 = \sum_i P_i Q_i$. Dans le membre droit apparaissent les variables t_i et d'autres variables. Remplaçons ces dernières par 0, et chaque variable t_i par α_i. On obtient $1 = 0$: contradiction. □

Lemme 2.5. *Pour tout ensemble H de polynômes de degré ≤ 1 de $k[x]$, il existe une k-algèbre A où chaque élément de H a une racine.*

Démonstration. On considère pour chaque polynôme $P \in H$ une variable t_P, et soit T l'ensemble de ces variables. Dans $k[T]$ on considère l'idéal I engendré par les polynômes $P(t_P)$. Alors l'idéal I est propre. En effet, s'il ne l'est pas, il existe des polynômes $P_1, \ldots, P_n \in k[x]$, et des polynômes $Q_1, \ldots, Q_n \in k[T]$ tels que $1 = \sum_i P_i(t_{P_i}) Q_i$. Les lemmes 2.3 et 2.4 nous donnent alors une contradiction.

Le quotient $A = k[T]/I$ est alors une k-algèbre, et la projection canonique $k[T] \to A, P \mapsto P \bmod I$, est un k-homomorphisme d'anneaux. Si $P \in H$, alors $P(t_P \bmod I) = P(t_P) \bmod I = 0$, donc $t_P \bmod I$ est une racine de P. □

Corollaire 2.5. *On peut rajouter dans la conclusion du lemme que A est un corps.*

Démonstration. On prend un idéal maximal de A : le quotient est un corps où tout polynôme dans H a une racine. □

Preuve du théorème 2.9. Le corollaire 2.5, appliqué à H = l'ensemble de tous les polynômes dans $k[x]$ de degré au moins 1, montre qu'il existe une extension E_1 de k où chaque polynôme sur k, de degré au moins 1, a une racine.

On construit ainsi une suite de corps $k = E_0 \subset E_1 \subset E_2 \ldots$, telle que pour tout $n \geq 0$, tout polynôme à coefficients dans E_n de degré au moins 1 a une racine dans E_{n+1}. Soit $E = \cup_{n \in \mathbb{N}} E_n$. C'est un corps. Tout polynôme de degré au moins 1 à coefficients dans E a ses coefficients dans un des E_n. Il a donc une racine dans E_{n+1}, donc dans E. Donc E est algébriquement clos. □

Corollaire 2.6. *Il existe une clôture algébrique de k.*

Démonstration. Soit E un corps algébriquement clos contenant k. Soit $\bar{k}$ l'ensemble des élements de E qui sont algébriques sur k. C'est un corps (Corollaire 2.1). Si f est un polynôme sur $\bar{k}$, de degré au moins un, il admet une racine dans E. Cet élément est algébrique sur $\bar{k}$. Il est donc algébrique

sur k (Proposition 2.8), donc il est dans $\bar{k}$. Celui-ci est donc algébriquement clos ; c'est donc une clôture algébrique de k. □

Nous démontrons maintenant l'unicité de la clôture algébrique.

Proposition 2.12. *Soit σ un homomorphisme de k dans L et f son extension canonique $k[x] \to L[x]$. Soit $k(\alpha)$ une extension algébrique simple de k et p le polynôme minimal de α. Le nombre de prolongements de σ en un homomorphisme $k(\alpha) \to L$ est égal aux nombres de racines distinctes dans L de $f(p)$.*

Démonstration. Si $\bar{\sigma}$ est un tel prolongement, on $0 = \bar{\sigma}(p(\alpha)) = f(p)(\bar{\sigma}(\alpha))$; donc $\bar{\sigma}(\alpha)$ est une racine de $f(p)$. Comme $\bar{\sigma}$ est un homomorphisme qui prolonge σ, il est entièrement déterminé par l'image de α.

Réciproquement, si β est une racine dans L de $f(p)$, alors le prolongement $\bar{\sigma}$ est défini par $\bar{\sigma}(\sum_i a_i\alpha^i) = \sum_i \sigma(a_i)\beta^i$, $a_i \in k$.

□

Théorème 2.10. *Soit E une extension algébrique de k et σ un homomorphisme de k dans L algébriquement clos. Il existe un prolongement $\bar{\sigma}$ de σ en un homomorphisme $E \to L$. Si de plus E est algébriquement clos et si L algébrique sur $\sigma(k)$, tout tel prolongement de σ est un isomorphisme.*

Nous utilisons dans la preuve le lemme de Zorn : tout ensemble inductif admet au moins un élément maximal. Un ensemble *inductif* est un ensemble ordonné non vide tel que toute partie totalement ordonnée ait un majorant.

Démonstration. Soit S l'ensemble des couples (F, τ), où F est un sous-corps de E contenant k comme sous-corps et où $\tau : F \to L$ est un homomorphisme qui prolonge σ. Alors $S \neq \emptyset$, car $(k, \sigma) \in S$. On définit une relation d'ordre $\leq$ sur S par : $(F, \tau) \leq (F', \tau')$ si F est un sous-corps de F' et si $\tau'|F = \tau$. Alors S est inductif. Par le lemme de Zorn, S a donc un élément maximal (K, λ). Si l'on avait $K \neq E$, alors il existerait $\alpha \in E \setminus K$ et la proposition précédente (appliquée à l'homomorphisme λ de K dans L) impliquerait une contradiction (car α est algébrique sur k donc sur K et L est algébriquement clos).

Supposons maintenant que E soit algébriquement clos et que L soit algébrique sur $\sigma(k)$. Alors $\bar{\sigma}(E)$ est algébriquement clos et L est algébrique sur $\bar{\sigma}(E)$. Donc $L = \bar{\sigma}(E)$ (on utilise le fait qu'un corps algébriquement clos n'a pas d'extension algébrique, sauf lui-même). □

Corollaire 2.7. *Deux clôtures algébriques E, E' de k sont k-isomorphes.*

Démonstration. On applique le théorème précédent à l'identité de k, avec L remplacé par E'. On obtient que l'identité de k se prolonge en un isomorphisme de E vers E', donc un k-isomorphisme. □

Notation pour la clôture algébrique : $\bar{k}$.

EXERCICES

Exercice 2.28. *Montrer que la proposition 2.13 n'est pas vraie si E n'est pas une extension algébrique (prendre $E = k(x)$ et $\sigma(x) = x^2$).*

Exercice 2.29. *Montrer que si E est un corps algébriquement clos, alors tout polynôme non constant a toutes ses racines dans E (ce qui veut dire par définition que ce polynôme s'écrit comme un produit de polynôme de degré 1).*

Exercice 2.30. *Montrer que E est un corps algébriquement clos si et seulement si tout polynôme irréductible sur E est de degré 1.*

Exercice 2.31. *Montrer que E est un corps algébriquement clos si et seulement s'il n'a pas d'autre extension algébrique que E.*

Exercice 2.32. *Montrer que si k est un corps dénombrable, alors sa clôture algébrique est dénombrable.*

2.7 Extensions normales

Proposition 2.13. *Soit E une extension algébrique de k et σ un homomorphisme de E vers E dont la restriction à k est l'identité. Alors σ est un automorphisme de E.*

Démonstration. Il suffit de montrer que σ est surjectif. Soit α dans E et p son polynôme minimal sur k. Soit K le sous- corps de E engendré par k et l'ensemble X des racines de p qui sont dans E : $K = k(X)$. Alors K est une extension finie de k (proposition 2.7). Toute racine de p est envoyée par σ sur une racine de p ; c'est-à-dire $\sigma(X) \subset X$. Donc, par la proposition 2.1, $\sigma(K) = \sigma(k(X)) = k(\sigma(X)) \subset k(X) = K$: σ envoie K dans lui-même. Or σ est k-linéaire. Comme K est un k-espace vectoriel de dimension finie et que $\sigma|K$ est injective, elle est aussi surjective et il existe donc $\beta \in K$ tel que $\sigma(\beta) = \alpha$. Donc σ est surjectif. □

On dit que K *est un corps de décomposition d'une famille de polynômes sur k* si ces polynômes se décomposent complètement dans K et si K est engendré sur k par leurs racines.

Proposition 2.14. *Soit K une extension algébrique de k, contenue comme sous-corps dans une clôture algébrique $\bar{k}$ de k. Les conditions suivantes sont équivalentes :*

(1) Tout homomorphisme $\sigma : K \to \bar{k}$, dont la restriction à k est l'identité de k, est un automorphisme de K.

(2) K est un corps de décomposition d'une famille de polynômes sur k.

(3) Tout polynôme irréductible sur k qui a une racine dans K se décompose complètement dans $K[x]$.

Démonstration. (1) implique (3) : soit $\alpha \in K$ et p_α son polynôme minimal sur k. Soit β une racine de ce polynôme dans $\bar{k}$. Il existe alors un isomorphisme $\sigma : k(\alpha) \to k(\beta)$ qui est l'identité sur k et tel que $\sigma(\alpha) = \beta$. Soit $\phi : k(\alpha) \to \bar{k}$ défini par $\phi(u) = \sigma(u)$. On peut d'après le théorème 2.10 prolonger ϕ en un homomorphisme $\bar{\phi} : K \to \bar{k}$; alors $\bar{\phi}$ est par hypothèse un automorphisme de K, donc $\beta \in K$.

(3) implique (2) : soient $(f_i)_{i\in I}$, la famille des polynômes minimaux sur k des éléments de K. Toutes leurs racines sont dans K et K est engendré sur k par ces racines. Donc K est un corps de décomposition de ces polynômes.

(2) implique (1) : soient $(f_i)_{i\in I}$, la famille des polynômes dont K est le corps de décomposition. Soit σ un homomorphisme de K vers $\bar{k}$, qui fixe k point par point. Si $f_i(\alpha) = 0$, $\alpha \in K$, $\sigma(\alpha)$ est racine de f_i, par le lemme 2.1. Donc $\sigma(\alpha)$ est dans K et $\sigma(K) \subset K$. D'après la proposition 2.13, σ est un automorphisme de K. □

Définition 2.9. *Une extension algébrique K de k qui satisfait une des trois conditions équivalentes de la proposition est dite* normale.

Si F, K sont deux sous-corps d'un même corps, rappelons que nous notons KF leur composé : $KF = F(K) = K(F)$.

Proposition 2.15. *Tous les corps dans cette proposition sont sous-corps de la clôture algébrique $\bar{k}$ de k.*

1. Si K est une extension normale de k et F un sur-corps de k, alors KF est une extension normale de F.

2. Si $k \subset E \subset K$ sont des corps, chacun sous-corps du suivant, tels que K est une extension normale de k, alors K est une extension normale de E.

3. Si K_1, K_2 sont des extensions normales de k, alors K_1K_2 et $K_1 \cap K_2$ sont des extensions normales de k.

Démonstration. 1. Par hypothèse, K est un corps de décomposition sur k d'une famille de polynômes sur k. Donc KF est un corps de décomposition pour ces polynômes, vus comme des polynômes sur F.

2. Par hypothèse, K est un corps de décomposition sur k d'une famille de polynômes sur k. Donc K est aussi un corps de décomposition de E de ces polynômes, vus comme polynômes sur E.

3. Soit σ un homomorphisme de K_1K_2 dans $\bar{k}$ dont la restriction à k est l'identité. Comme K_1, K_2 sont des extensions normales de k, la restriction de σ à K_i est un automorphisme de K_i, pour $i = 1, 2$. On a donc $\sigma(K_1K_2) = \sigma(K_1)\sigma(K_2) = K_1K_2$ et σ est un automorphisme de K_1K_2.

Si un polynôme irréductible sur k a une racine dans $K_1 \cap K_2$, alors il a toutes ses racines dans K_1 et aussi dans K_2. Donc dans leur intersection, qui est donc une extension normale de k. □

EXERCICES

Exercice 2.33. *Montrer que le corps obtenu de $\mathbb{Q}$ en y adjoignant des $\sqrt{n}$, $n \in \mathbb{N}$, est une extension normale de $\mathbb{Q}$.*

Exercice 2.34. *Soit $k(\alpha)$ une extension algébrique simple et f le polynôme minimal de α. Montrer que les trois propriétés suivantes sont équivalentes : (1) $k(\alpha)$ est une extension normale de k ; (2) toutes les racines de f sont dans $k(\alpha)$; (3) il existe des polynômes $f_i(x)$ sur k tels que $f(x) = \prod_i (x - f_i(\alpha))$. Donner des exemples de cette situation.*

Exercice 2.35. *Soit $K \subset L$ une extension algébrique. Soit S l'ensemble des polynômes sur K qui se décomposent entièrement dans L. Soit M le sous-corps de L engendré sur K par les racines des polynômes dans S. Montrer que M est la plus grande extension normale de K contenue dans L.*

Exercice 2.36. *Montrer que toute extension de degré 2 est normale.*

Exercice 2.37. *Montrer que $M = \mathbb{Q}(\sqrt[4]{2})$ est une extension de degré 4 de $\mathbb{Q}$, que $L = \mathbb{Q}(\sqrt{2})$ est une extension de degré 2 de $\mathbb{Q}$, et M une extension de degré 2 de L. Puis que M est une extension normale de L, que L et une extension normale de $\mathbb{Q}$, mais que M n'est pas une extension normale de $\mathbb{Q}$ (donc la notion d'extension normale n'est pas transitive).*

2.8 Racines de l'unité

Ici, Π est soit le corps $\mathbb{Q}$, auquel cas on pose $p = 0$, soit le corps $\mathbb{Z}/p\mathbb{Z}$, avec p premier.

Définition 2.10. *Soit h un entier naturel non nul.*

1. Une racine h-ème de l'unité *est une racine du polynôme $x^h - 1$ dans une extension de Π.*

2. Le corps des racines h-èmes de l'unité *est le corps de décomposition sur* Π *de* $x^h - 1$. *Notation :* Σ.

Proposition 2.16. *Les racines h-èmes de l'unité forment un groupe multiplicatif.*

On suppose dans la suite cas que $h \in \mathbb{N} \setminus p\mathbb{N}$: ça signifie que si $p = 0$, alors h est non nul ; et que si p est un nombre premier, h, p sont premiers entre eux.

Proposition 2.17. *Dans Σ, le polynôme $x^h - 1$ se factorise complètement et ses h racines sont distinctes.*

Il y a donc h racines h-èmes de l'unité dans Σ.

Démonstration. Le dérivé du polynôme $x^h - 1$ est hx^{h-1}. Il n'est pas nul (car $h \neq 0$ dans Π, par l'hypothèse sur h), donc sa seule racine est 0. Donc $x^h - 1$ et son dérivé n'ont pas de racines commune, ce qui implique que les racines de $x^h - 1$ sont simples (exercice 2.39). □

Définition 2.11. *Une* racine primitive h-ème de l'unité *est un générateur du groupe des racines h-èmes de l'unité dans Σ.*

Autrement dit : un élément de ce groupe dont l'ordre est h.

Théorème 2.11. *Il y a exactement $\varphi(h)$ racines primitives h-èmes dans Σ, où φ est l'indicateur d'Euler.*

Démonstration. Soit $h = \prod_i q_i^{\nu_i}$, où les q_i sont les facteurs premiers distincts de h et où les exposants sont ≥ 1. Il y a h racines h-èmes de l'unité et le polynôme $x^{h/q_i} - 1$ a au plus h/q_i racines ; comme $h > h/q_i$, il existe $a_i \in \Sigma$ tel que $a_i^h = 1$ et $a_i^{h/q_i} \neq 1$. Posons $b_i = a_i^{h/q_i^{\nu_i}}$. On a $b_i^{q_i^{\nu_i - 1}} = (a_i^{h/q_i^{\nu_i}})^{q_i^{\nu_i - 1}} = a_i^{h/q_i} \neq 1$. On a donc aussi $b_i^{q_i^{\nu_i}} = 1$, donc l'ordre de b_i divise $q_i^{\nu_i}$. Le calcul précédent montre que l'ordre de b_i ne divise pas $q_i^{\nu_i - 1}$, donc l'ordre de b_i est $q_i^{\nu_i}$.

Soit $\xi = \prod_i b_i$. Alors l'ordre de ξ est le produit de l'ordre des b_i, car ceux-ci sont premiers entre eux deux à deux (exercice 2.40). Donc l'ordre de ξ est h. Donc le groupe des racines h-èmes de l'unité est cyclique, de cardinalité h, et il est bien connu que dans un tel groupe, le nombre de générateurs est égal à $\varphi(h)$. □

Corollaire 2.8. *Le groupe des racines h-èmes de l'unité dans Σ est cyclique.*

Définition 2.12. *Soit $n = \varphi(h)$ et $\{\xi_1, \ldots, \xi_n\}$ l'ensemble des racines primitives h-èmes. Le* polynôme cyclotomique d'ordre h *est $\prod_{1 \leq i \leq n}(x - \xi_i)$. Notation : $\Phi_h(x)$.*

Proposition 2.18. *1. On a $x^h - 1 = \prod_{d|h} \Phi_d(x)$.*

2. Si $\psi_n(x)$, $n \geq 1$, $n \not\equiv 0 \mod p$, est une famille de polynômes, à coefficients dans une extension de Π, tels que pour tout $k \not\equiv 0 \mod p$, on ait $x^k - 1 = \prod_{d|k} \psi_d(x)$, alors pour tout k, on a $\psi_k = \Phi_k$.

Démonstration. 1. La formule découle de ce que toute racine h-ème de l'unité est d'ordre d, pour un certain d divisant h, donc une racine primitive d-ème. Remarquer que $d \not\equiv 0 \mod p$.

2. Pour $k = 1$, on obtient $\psi_1 = x - 1 = \Phi_1$. On suppose maintenant $k \geq 2$ et k non divisible par p. Alors $\psi_k = \prod_{d|k} \psi_d / \prod_{d|k, d \neq k} \psi_d = (x^k - 1) / \prod_{d|k, d \neq k} \Phi_d$ (par hypothèse de récurrence) $= \prod_{d|k} \Phi_d / \prod_{d|k, d \neq k} \Phi_d = \Phi_k$. □

Corollaire 2.9. *On a $\Phi_h = \prod_{d|h}(x^d - 1)^{\mu(h/d)}$ où μ est la fonction de Möbius.*

Démonstration. Notons ψ_h le membre de droite. Rappelons que $\sum_{d|h} \mu(d) = 0$ si $h \geq 2$, et que $\mu(1) = 1$. Soit h un entier naturel non divisible par p. Alors $\prod_{d|h} \psi_d = \prod_{d|h} \prod_{e|d}(x^e - 1)^{\mu(d/e)} = \prod_{e|h}(x^e - 1)^{\alpha_e}$, où $\alpha_e = \sum_{e|d|h} \mu(d/e) = \sum_{f|(h/e)} \mu(f)$. Donc $\alpha_e = 0$ si $h > e$ et $\alpha_h = 1$. Par suite, le produit considéré vaut donc $x^h - 1$. Le corollaire découle donc de la proposition. □

Corollaire 2.10. *Les coefficients des polynômes cyclotomiques sont dans $\mathbb{Z}$ ou $\mathbb{Z}/p\mathbb{Z}$.*

Démonstration. 1. Supposons que $K \subset L$ soit une extension de corps, ou que $K = \mathbb{Z}$ et $L = \mathbb{Q}$. Alors, si $P, Q \in K[x]$ et si P divise Q dans $L[x]$, alors P divise Q dans $K[x]$. Ceci découle de la division euclidienne dans le premier cas, et du lemme de Gauss pour les polynômes dans $\mathbb{Q}$ et $\mathbb{Z}$ dans le deuxième cas.

2. Supposons que $p = 0$. Le polynôme cyclotomique $\phi_h \in \Sigma[x] \subset \mathbb{C}[x]$ est par le corollaire précédent le quotient de deux polynômes à coefficients dans $\mathbb{Z}$. Il découle de 1. que le quotient est dans $\mathbb{Q}[x]$. Mais en tant que série formelle, il est à coefficients dans $\mathbb{Z}$, car les séries au dénominateur de la formule du Corollaire 2.9 sont inversibles, puisque que leur terme constant est -1.

3. Dans le cas où $p \neq 0$, on raisonne de manière analogue avec $K = \mathbb{Z}/p\mathbb{Z}$ et $L = \Sigma$. □

Proposition 2.19. *Si ξ est une racine h-ème de l'unité, alors $1+\xi+\ldots+\xi^{h-1}=0$ si $\xi\neq 1$, et ça vaut h si $\xi=1$.*

Démonstration. On a $0=\xi^h-1=(\xi-1)(\xi^{h-1}+\cdots+\xi+1)$. □

EXERCICES

Exercice 2.38. *Montrer que si $h=kp^\ell$, k,p premiers entrre eux, et que Σ est de caractéristique p, alors les racines h-èmes de l'unité dans Σ sont les racines k-èmes de l'unité.*

Exercice 2.39. *Montrer que si un polynôme a une racine au moins double, alors celle-ci est racine de son dérivé.*

Exercice 2.40. *Montrer que si a,b sont deux éléments d'un groupe commutatif, d'ordres α,β respectivement, premiers entre eux, alors ab est d'ordre $\alpha\beta$. Généraliser à plusieurs éléments. Indication : montrer d'abord que que l'intersection des deux sous-groupes engendrés par a et b est triviale.*

2.9 Corps finis

Proposition 2.20. *Soit Δ un corps fini de cardinalité q, p sa caractéristique et Π son sous-corps premier. Celui-ci est isomorphe à $\mathbb{Z}/p\mathbb{Z}$. On a $q=p^n$, où n est la dimension de Δ comme espace vectoriel sur Π.*

On pose $h=q-1$.

Proposition 2.21. *$\forall\alpha\in\Delta$, $\alpha^q=\alpha$ et si $\alpha\neq 0$, $\alpha^h=1$.*

Corollaire 2.11. *Δ est le corps de décomposition sur Π du polynôme x^q-x. En particulier, tous les corps à p^n éléments sont isomorphes.*

La deuxième assertion s'obtient par la proposition 2.4. On note $\mathbb{F}_q$ le corps à q éléments ; il est unique à isomorphisme près.

Théorème 2.12. *Soit p un nombre premier et $n\geq 1$. Il existe un corps ayant $q=p^n$ éléments.*

Démonstration. On note Δ le corps de décomposition sur $\mathbb{Z}/p\mathbb{Z}$ du polynôme x^q-x. Les identités (Théorème 2.3) $(a-b)^q=a^q-b^q$ et $(a/b)^q=a^q/b^q$ impliquent que Δ est égal à l'ensemble des racines de ce polynôme. Enfin, son dérivé est -1, donc x^q-x n'a pas de racine double, et par suite Δ a q éléments. □

Théorème 2.13. *Δ^* est un groupe cyclique.*

Cela découle du corollaire 2.8. Si α est un générateur du groupe Δ^*, alors α engendre Δ sur $\mathbb{F}_p$. Donc $\Delta = \mathbb{F}_p(\alpha)$ est une extension simple de $\mathbb{F}_p$.

Théorème 2.14. *Soit Δ un corps de cardinalité p^n.*

1. Tout sous-corps de Δ est de cardinalité p^m avec $m|n$.

2. Pour tout diviseur m de n, il existe un unique sous-corps Γ de Δ de cardinalité p^m ; il est constitué des racines dans Δ du polynôme $x^{p^m} - x$. De plus, $\alpha \in \Delta$ est dans Γ^* si et seulement si $\alpha^{p^m-1} = 1$.

Démonstration. 1. Soit Γ un sous-corps de Δ. C'est un sur-corps de Π, donc un espace vectoriel de dimension finie m sur lui, donc sa cardinalité est p^m. De plus, Δ est un espace de dimension finie r sur Γ, donc la cardinalité de Δ est la puissance r-ème de celle de Γ : $p^n = (p^m)^r \Rightarrow n = mr$.

2. Supposons que $n = mr$. Alors $p^m - 1$ divise $p^n - 1$, donc $x^{p^m-1} - 1$ divise $x^{p^n-1} - 1$ (exercice 2.41 utilisé deux fois) ; donc $x^{p^m} - x$ divise $x^{p^n} - x$. Donc $x^{p^m} - x$ se décompose entièrement dans Δ et ses racines forment un sous-corps de cardinalité p^m de Δ (cf. la preuve du théorème 2.12.

Soit maintenant Γ un sous-corps de Δ de cardinalité p^m. Soit $\alpha \in \Gamma^*$. Ce groupe a $p^m - 1$ élements, donc $\alpha^{p^m-1} = 1$. Réciproquement, si $\alpha \in \Delta$ satisfait cette égalité, alors α est racine du polynôme $x^{p^m} - x$. Ceci prouve l'unicité de Γ et la dernière assertion. □

En cours de preuve, on a prouvé la formule

$$x^{p^n} - x = \prod_{\alpha \in \mathbb{F}_{p^n}} (x - \alpha).$$

Par le théorème 2.3, la fonction $\alpha \mapsto \alpha^p$ est un automorphisme de Δ. On l'appelle *l'automorphisme de Frobenius.*

Théorème 2.15. *Il y a exactement n automorphismes du corps Δ. Ils forment un groupe cyclique, engendré par l'automorphisme de Frobenius.*

Démonstration. L'application $\phi_r : x \mapsto x^{p^r}$ est un automorphisme de Δ, car $\phi_r = \phi_1^r$ et que ϕ_1 est l'automorphisme de Frobenius. Ils sont distincts pour $r = 1, \ldots, n-1$, car il existe dans Δ^* (qui est cyclique) un élement α d'ordre $p^n - 1$: par suite, si l'on a $i \geq 1$ et si ϕ_1^i est l'identité, alors $\alpha^{p^i} = \alpha$, ce qui force $i \geq n$.

On a aussi $\Delta = \Pi(\alpha)$. Par suite α est algébrique de degré n sur Π. Tout automorphisme de Δ fixe Π, donc envoie α sur une racine de ce polynôme, et il existe donc au plus n automorphismes de Δ. □

EXERCICES

Exercice 2.41. *Montrer que si e divise d, alors $u^e - 1$ divise $u^d - 1$.*

Exercice 2.42. ** Soit k le corps fini à q éléments. Montrer que le corps de décomposition K du polynôme $x^{q^n} - x \in k[x]$ est le corps à q^n éléments, et que le groupe des k-automorphismes de K est cyclique d'ordre n, engendré par l'automorphisme $a \mapsto a^q$.*

2.10 Extensions séparables

k est un corps de caractéristique p.

Théorème 2.16. *Soit $f \in k[x]$, irréductible, et Γ la clôture algébrique de k.*

1. Si $p = 0$, alors les racines de f dans Γ sont simples.

2. Si $p > 0$, les racines de f dans Γ ont toutes la même multiplicité p^e ; celle-ci est > 1 si et seulement si $f(x) = g(x^p)$, $g \in k[x]$.

Démonstration. Si f a une racine multiple dans Γ, alors dans $\Gamma[x]$, f et f' ont un diviseur commun non trivial (à savoir $x - \alpha$, où α est la racine). Leur pgdc est donc non trivial. Or leur pgdc dans $\Gamma[x]$ est égal à celui dans $k[x]$ (par l'algorithme d'Euclide). Comme f est irréductible, leur pgdc ne peut être que f ou 1. Comme ce n'est pas 1, ça doit être f, et f divise f'. Comme le degré de f' est $<$ celui de f, on doit avoir $f' = 0$. Ceci prouve que la caractéristique p doit être > 0 : en effet, d'une part le degré de f est au moins 1 ; d'autre part, le dérivé d'un monôme x^r est rx^{r-1} et ne peut être nul que si $r = 0$ dans k. Ceci montre aussi que si x^r apparaît dans f, alors r est divisible par p. Donc $f(x) = g(x^p)$, $g \in k[x]$.

Soit e maximum tel que $f(x) = \psi(x^{p^e})$, $\psi \in k[x]$. Alors ψ est irréductible dans $k[x]$; il n'a pas de racine multiple dans Γ, par maximalité de e. On peut écrire $\psi(x) = a\prod(x - \beta_i)$ où les racines $\beta_i \in \Gamma$ de ψ sont distinctes. Soit α_i la racine p^e-ème de β_i (elle est unique car $\alpha \mapsto \alpha^{p^e}$ est injectif). Alors $f(x) = a\prod(x^{p^e} - \alpha_i^{p^e}) = a\prod(x - \alpha_i)^{p^e}$ et les α_i sont distincts. Donc les racines de f ont toutes la même multiplicité p^e. □

Nous dirons qu'un polynôme sur k *n'a que des racines simples* si toutes ses racines dans son corps de décomposition sont simples.

Définition 2.13. *1. Un polynôme $f \in k[x]$ est dit* séparable *s'il n'a que des racines simples.*

2. Un élément dans une extension de k, algébrique sur k, est dit séparable *sur k si son polynôme minimal sur k est séparable.*

3. Une extension algébrique de k est séparable *si tout élément en est séparable.*

Pour que α soit séparable, il suffit qu'il soit racine d'un polynôme séparable (non nécessairement irréductible) sur k.

Corollaire 2.12. *Si $k \subset E \subset F$ et si $\alpha \in F$ est séparable sur k, alors il l'est sur E.*

Démonstration. En effet, le polynôme minimal de α sur E divise celui de α sur k. □

Corollaire 2.13. *Si la caractéristique de k est nulle, toute extension algébrique de k est séparable.*

EXERCICES

Exercice 2.43. *Montrer que pour un polynôme $f(x) \in k[x]$, il a une racine double α dans une extension de k si et seulement si $f'(\alpha) = 0$.*

Exercice 2.44. *1. Montrer que dans un corps de caractéristique $p > 0$, avec e un entier ≥ 1, la fonction $\alpha \mapsto \alpha^{p^e}$ est injective.*

2.11 Degré de séparabilité

k est un corps.

Définition 2.14. *Soient K une extension algébrique de k et σ un homomorphisme $k \to L$, où L est un corps algébriquement clos. On appelle* degré de séparabilité *de K sur k, noté $[K : k]_s$, le nombre de prolongements de σ en un homomorphisme $K \to L$.*

On montre que ce nombre ne dépend ni de L, ni de σ : il ne dépend que de k et K.

Théorème 2.17. *(multiplicativité du degré de séparabilité) Soient $k \subset K \subset E$ des corps, chacun extension algébrique du précédent. Alors*

$$[E : k]_s = [E : K]_s[K : k]_s.$$

De plus $[K : k]_s \leq [K : k]$ si l'extension K de k est finie.

Démonstration. Soit σ un homomorphisme de k dans L algébriquement clos. Soient σ_i, $i \in I$, la famille des prolongements distincts de σ à K ; elle a $[K : k]_s$ éléments. Alors chaque σ_i a exactement $[E : K]_s$ prolongements distincts τ_{ij} à E. Donc l'ensemble des τ_{ij} est de cardinalité $[E : K]_s[K : k]_s$. Comme tout prolongement de σ à E est l'un des τ_{ij}, la formule s'en déduit.

Supposons que $[K : k]$ soit fini. Alors $K = k(\alpha_1, \ldots, \alpha_n)$. Posons $F_0 = k$ et récursivement $F_{\nu+1} = F_\nu(\alpha_{\nu+1})$, $\nu = 0, 1, \ldots, n-1$. En particulier $K = F_n$. D'après la proposition 2.12, on a $[F_{\nu+1} : F_\nu]_s \leq [F_{\nu+1} : F_\nu]$. D'où par multiplication $[K : k]_s \leq [K : k]$. □

Corollaire 2.14. *On suppose que E est une extension finie de k et K un corps intermédaire. On a $[E : k]_s = [E : k]$ si et seulement si $[E : K]_s = [E : K]$ et $[K : k]_s = [K : k]$.*

Proposition 2.22. *Un élément α algébrique d'une extension de k est séparable si et seulement si $[k(\alpha) : k]_s = [k(\alpha) : k]$.*

Démonstration. Cela découle de la proposition 2.12. □

Théorème 2.18. *Une extension finie E de k est séparable si et seulement si $[E : k]_s = [E : k]$.*

Démonstration. Supposons que $[E : k]_s = [E : k]$. La proposition et le corollaire précédents, joints à la multiplicativité, montre que α est séparable, quel que soit α dans E.

Réciproquement, supposons que tout α dans E soit séparable sur k. On peut écrire $E = k(\alpha_1, \ldots, \alpha_n)$. Chaque α_i est séparable sur k, donc sur $k(\alpha_1, \ldots, \alpha_{i-1})$. Donc les théorèmes 2.1 et 2.17 impliquent que $[E : k]_s = [E : k]$. □

Proposition 2.23. *Soit α algébrique sur k. Si $p = 0$, alors $[k(\alpha) : k] = [k(\alpha) : k]_s$. Si $p > 0$, soit p^e la multiplicité commune de toutes les racines du polynôme minimal de α ; alors $[k(\alpha) : k] = p^e[k(\alpha) : k]_s$.*

Démonstration. La première assertion vient du fait qu'en caractéristique nulle, le polynôme n'a que des racines simples.

Supposons maintenant que $p > 0$ et soit f le polynôme minimal. On a par le théorème 2.16 (voir sa preuve) $f(x) = \psi(x^{p^e})$ et ψ est irréductible et n'a que des racines simples. Donc d'une part $[k(\alpha) : k] = \deg(f) = p^e \deg(\psi)$ et d'autre part, $[k(\alpha) : k]_s = [k(\alpha) : k(\alpha^{p^e})]_s [k(\alpha^{p^e}) : k]_s$. Mais le premier facteur vaut 1, car le polynôme minimal de α sur $k(\alpha^{p^e})$ est $x^{p^e} - \alpha^{p^e}$ (sinon c'est un diviseur, ce qui contredit que le degré de α est $\deg(f)$, car $[k(\alpha^{p^e}) : k] = deg(\psi)$ puisque $\psi(\alpha^{p^e}) = 0$) ; et le deuxième facteur vaut $\deg(\psi)$, car ce polynôme est irréductible sur k et n'a que des racines simples, et α^{p^e} est l'une d'elles. □

Corollaire 2.15. *Pour toute extension finie E de k, $[E : k]_s$ divise $[E : k]$. Le quotient vaut 1 si $p = 0$ et c'est une puissance de p si $p > 0$.*

Démonstration. Si E est une extension simple, cela découle du résultat précédent. Dans le cas général, on le prouve par récurrence sur le nombre de générateurs, en utilisant la multiplicativité : théorèmes 2.1 et 2.17. □

Définition 2.15. *Pour K extension finie de k, on pose $[K : k]_i = [K : k]/[K : k]_s$.*

Corollaire 2.16. *Soit K extension finie de k. Elle est séparable si et seulement si $[K : k]_i = 1$. De plus $[K : k]_i$ est multiplicatif.*

Théorème 2.19. *Soit $K = k(\alpha_i, i \in I)$ une extension algébrique de k. Si chaque α_i est séparable sur k alors l'extension est séparable.*

Démonstration. Comme tout élément de K se trouve dans une sous-extension finiment engendrée de K, on peut supposer que I est fini. Dans ce cas on raisonne comme dans les trois dernières phrases de la preuve du théorème 2.18. □

Corollaire 2.17. *Si α, β sont séparables sur k, alors $\alpha - \beta$ et α/β sont séparables sur k.*

Théorème 2.20. *Soit $k \subset K \subset E$, chaque corps extension algébrique du précédent. E est séparable sur K et K séparable sur k si et seulement si E est séparable sur k.*

Démonstration. Supposons que E soit séparable sur K et K séparable sur k. Soit $\alpha \in E$. Soit f son polynôme minimal sur K ; il n'a que des racines simples. Soit C l'ensemble de ses coefficients. Alors α est séparable sur l'extension $k(C)$; ce corps est une extension finie de k. De plus chaque élément de C est séparable sur k donc $k(C)$ est séparable sur k (théorème 2.19). Donc $k(C)(\alpha)$ est séparable sur k par le corollaire 2.14. Donc α est séparable sur k, de même que E.

Réciproquement, supposons que E soit séparable sur k. Alors E est séparable sur K (car le polynôme minimal sur K divise celui sur k). De plus tout élément de K est clairement séparable sur k. □

Théorème 2.21. *Soit E une extension séparable sur k et F une extension de k, tous deux sous-corps du corps Ω. Alors EF est une extension séparable de F.*

Démonstration. Soit $\alpha \in E$. Alors α est séparable sur k, donc sur F. Donc EF est séparable sur F par le théorème 2.19. □

2.12 Le théorème de l'élément primitif

Théorème 2.22. *Une extension finie E de k est une extension simple si et seulement s'il n'y a qu'un nombre fini de corps intermédiaires $k \subset F \subset E$.*

On appelle α un *élément primitif de E sur k* si $E = k(\alpha)$.

Démonstration. Si k est un corps fini, E aussi, et l'extension est toujours simple (c'est une conséquence du théorème 2.13) ; de plus, il n'y a forcément qu'un nombre fini de corps intermédiaires.

On peut donc supposer que k est infini. Supposons qu'il n'y a qu'un nombre fini de corps intermédiaires. Soient $\alpha, \beta \in E$. L'ensemble des corps de la forme $k(\alpha + c\beta)$, $c \in k$, est fini. Il existe donc $c_1 \neq c_2$ dans k tels que $k(\alpha+c_1\beta) = k(\alpha+c_2\beta)$. On a $k(\alpha+c_1\beta) \subset k(\alpha, \beta)$. De plus, $\alpha+c_1\beta, \alpha+c_2\beta \in k(\alpha + c_1\beta)$. Donc $\beta = (\alpha + c_1\beta - (\alpha + c_2\beta))/(c_1 - c_2) \in k(\alpha + c_1\beta)$ et enfin $\alpha \in k(\alpha + c_1\beta)$. Donc $k(\alpha + c_1\beta) = k(\alpha, \beta)$.

Soit maintenant $E = k(\alpha_1, \ldots, \alpha_n)$. En utilisant ce qui précède, on montre par récurrence que $E = k(\alpha_1 + c_2\alpha_2 + \cdots + c_n\alpha_n)$ pour des éléments c_i dans k.

Réciproquement soit $E = k(\alpha)$ et soit f le polynôme minimal de α sur k. Soit F un corps intermédiaire et g_F le polynôme minimal de α sur F. Alors g_F divise f dans $F[x]$, donc dans $E[x]$. Soit F_0 le corps engendré sur k par les coefficients de g_F. Nous montrons plus loin que $F = F_0$; donc g_F détermine complètement F, ce qui implique que la fonction $F \mapsto g_F$ est injective. Comme g_F divise f dans $E[x]$, les g_F sont en nombre fini. Donc les corps F sont en nombre fini.

Montrons que $F = F_0$. On a $F_0 \subset F$ et donc g_F, étant irréductible dans $F[x]$, est a fortiori irréductible dans $F_0[x]$. Donc le degré de α sur F_0 est égal à celui sur F. On a $F(\alpha) = E = F_0(\alpha)$; donc $[E : F] = [E : F_0]$. Par multiplicativité (théorème 2.1), $[E : F_0] = [E : F][F : F_0]$; donc $[F : F_0] = 1$ et $F = F_0$. □

Corollaire 2.18. *Toute extension finie séparable de k est simple.*

Démonstration. On peut supposer que k est infini. Supposons que E soit séparable sur k. On est ramené au cas où $E = k(\alpha, \beta)$. Soient $\sigma_1, \ldots, \sigma_n$ les homomorphismes distincts de E dans $\bar{k}$ dont la restriction à k est l'identité de k. On a donc $n = [k(\alpha, \beta) : k]_s = [k(\alpha, \beta) : k]$. Soit $P(x) = \prod_{i\neq j}((\sigma_i(\beta) - \sigma_j(\beta))x + \sigma_i(\alpha) - \sigma_j(\alpha))$. On a $P \neq 0$. Il existe donc $c \in k$ tel que $P(c) \neq 0$. Donc les $\sigma_i(\alpha + c\beta)$ sont distincts. Soit f le polynôme minimal de $\alpha + c\beta$ sur k. Comme $\sigma_i(f) = f$, les $\sigma_i(\alpha + c\beta)$ sont des racines de f dans $\bar{k}$. Donc le degré de f est $\geq n$. Donc $[k(\alpha + c\beta)] : k] \geq n$. D'où $k(\alpha + c\beta) = E$. □

Exercice 2.45. *Soit L une extension séparable de K. Soit D une* dérivation *de K ; c'est une fonction additive qui satisfait la* formule de Leibniz $D(uv) = D(u)v + uD(v)$. *Montrer que D s'étend de manière unique en une dérivation de L.*

2.13 Corps parfaits

Théorème 2.23. *Les conditions suivantes sont équivalentes, pour un corps k.*

(i) Tout polynôme irréductible sur k est séparable.

(ii) Toute extension algébrique de k est séparable.

(iii) La caractéristique p de k est soit nulle, soit satisfait : $\forall a \in k$, il existe $b \in k$ tel que $b^p = a$.

La condition (iii) exprime que l'automorphisme de Frobenius est surjectif.

Démonstration. (i) implique (ii) découle des définitions et des résultats précédents.

(ii) implique (iii) : on peut supposer que $p > 0$. Soit $a \in k$ et soit b une racine, dans une extension de k, du polynôme $x^p - a$; donc $b^p = a$. Le polynôme minimal g de b sur k divise $x^p - a = x^p - b^p = (x-b)^p$. Il est donc de la forme $(x-b)^r$, $r \geq 1$. Comme il est séparable, on doit avoir $r = 1$ et par suite $b \in k$.

(iii) implique (i) : par le théorème 2.16 (2ème partie), $f = g(x^p)$, $g \in k[x]$; écrivant $g = \sum a_i x^i$, on obtient $f = \sum a_i x^{ip}$. Comme chaque coefficient dans k est une puissance p-ème dans k, f est lui même une puissance p-ème, donc réductible : ce qui n'est pas. □

Définition 2.16. *Un corps est dit* parfait *s'il satisfait aux conditions équivalentes du théorème.*

Corollaire 2.19. *Tout corps fini, ou algébriquement clos, ou de caractéristique 0, est parfait.*

2.14 Clôture normale

Théorème 2.24. *Soit E une extension finie de k, contenue dans $\bar{k}$. Alors la plus petite extension normale de k, contenue dans $\bar{k}$ et contenant E, est le sous-corps K de $\bar{k}$ engendré sur k par les $\sigma(E)$, où σ parcourt l'ensemble fini $\mathcal{S}$ des homomorphismes $\sigma : E \to \bar{k}$ tels que $\sigma|k$ est l'identité de k ; K*

est une extension finie de k. Si de plus E est séparable sur k, alors K l'est aussi.

Démonstration. Le fait que cet ensemble de prolongements soit fini découle de la proposition 2.12 et d'une récurrence sur le nombre de générateurs sur k de E.

Le corps K contient E car l'injection canonique $E \to \bar{k}$ est dans $\mathcal{S}$. Montrons que c'est une extension normale de k. Soit en effet un homomorphisme $\tau : K \to \bar{k}$ dont la restriction à k est l'identité. Alors sa restriction à $\sigma(E)$ est un homomorphisme de $\sigma(E)$ dans $\bar{k}$. Il existe donc $\sigma' \in \mathcal{S}$ tel que $\tau\sigma = \sigma'$. Donc τ est un automorphisme de K (car pour τ fixé, la fonction $\sigma \mapsto \sigma'$ de $\mathcal{S}$ dans lui-même est une bijection). Donc K est une extension normale de k.

C'est la plus petite extension normale de k avec les propriétés mentionnées : soit en effet L une extension normale de k qui contient E et qui est contenue dans $\bar{k}$. Soit $\sigma \in \mathcal{S}$. Alors σ a un prolongement à L, qui doit laisser L invariant. Donc $\sigma(E) \subset L$, puisque L est une extension normale de k. Donc $K \subset L$.

Pour la dernière assertion, on utilise le théorème 2.19, avec une récurrence. □

Le théorème s'étend au cas où E est une extension algébrique, non nécessairement finie ; $\mathcal{S}$ ne sera plus nécessairement fini. Le corps K s'appelle la *clôture normale de E*.

3 Théorie de Galois

Mais ce fut en vain que je cherchai tous les moyens de me livrer au sommeil, que je ne me permis pas plus de mouvement que n'en aurait un corps privé de vie, que j'essayai de donner un autre cours à mes idées, tantôt en récitant des vers de mémoire, tantôt en m'occupant de la solution d'un problème d'algèbre.

Walter Scott
Rob Roy

3.1 Extensions de Galois

Définition 3.1. *Une extension algébrique K de k est dite* de Galois *si elle est normale et séparable. Le groupe des automorphismes de K qui fixent k*

point par point s'appelle alors le groupe de Galois de K sur k, *et il est noté* $G(K/k)$.

Proposition 3.1. *Soit $\bar{k}$ une clôture algébrique de k, contenant K, extension de Galois de k. Alors le groupe de Galois de K sur k coïncide avec l'ensemble des k-homomorphismes $\sigma : K \to \bar{k}$. En particulier sa cardinalité est $[K : k]_s$.*

Démonstration. Comme K est normal sur k, tout k-homomorphisme $\sigma : K \to \bar{k}$ est un k- automorphisme de K (proposition 2.14). La deuxième assertion s'obtient en appliquant la définition 2.14 à l'injection $k \to \bar{k}$. □

Définition 3.2. *Soit K un corps et G un groupe d'automorphismes de K. On note K^G le sous-corps de K des $x \in K$ tels que $\forall \sigma \in G$, $\sigma(x) = x$. On l'appelle* le sous-corps fixé par G.

Théorème 3.1. *Soit K une extension de Galois de k et G son groupe de Galois. Alors $k = K^G$. Si F est un corps intermédiaire $k \subset F \subset K$, alors K est une extension de Galois de F. L'application $F \mapsto G(K/F)$ envoie l'ensemble des corps intermédiaires dans l'ensemble des sous-groupes de G et elle est injective.*

Le lecteur aura compris qu'on appelle *corps intermédiaire* tout sous-corps de K qui contient k.

Démonstration. L'inclusion $k \subset K^G$ découle des définitions. Réciproquement, soit $\alpha \in K^G$. Pour montrer que $\alpha \in k$, nous montrons que $[k(\alpha) : k] = 1$. Pour ce faire, il suffit de montrer que $[k(\alpha) : k]_s = 1$; en effet, ces deux nombre sont égaux, puisque $k(\alpha)$ est séparable sur k, puisque K l'est.

On a une injection $k \to \bar{k}$. Soit σ un k-homomorphisme $k(\alpha) \to \bar{k}$. Comme K est une extension algébrique de $k(\alpha)$, par le théorème 2.10, σ se prolonge en un homomorphisme $\bar{\sigma} : K \to \bar{k}$. Comme K est normal sur k, $\bar{\sigma}$ est un automorphisme de K. Donc $\bar{\sigma} \in G$. Par suite, $\sigma(\alpha) = \bar{\sigma}(\alpha) = \alpha$ (puisque $\alpha \in K^G$). Donc σ est l'identitité de $k(\alpha)$. Il y a donc un seul prolongement de l'injection canonique $k \to \bar{k}$ en un homomorphisme de $k(\alpha)$ dans $\bar{k}$. Il s'ensuit que le degré de séparabilité de $k(\alpha)$ sur k vaut 1.

Soit F un corps intermédiaire. Alors K est une extension de Galois de F (proposition 2.15 et théorème 2.20). Soit $H = G(K/F)$. C'est clairement un sous-groupe de G. De plus $K^H = F$ par ce qu'on vient de prouver. Donc l'application est injective. □

Définition 3.3. *Avec les notations du théorème, on dit que $G(K/F)$ est le* groupe associé à F, *et que le sous-groupe $H = G(K/F)$ de G* appartient au sous-corps F.

Corollaire 3.1. *Soit K une extension de Galois de k et, pour $i = 1, 2$, F_i un corps intermédiaire et $H_i = G(K/F_i)$.*

1. *Soit $F = F_1F_2$. Alors $G(K/F) = H_1 \cap H_2$.*
2. *Soit H le sous-groupe engendré par H_1 et H_2. Alors $K^H = F_1 \cap F_2$.*
3. *On a $F_1 \subset F_2$ si et seulement si $H_2 \subset H_1$.*

Démonstration. 0. Notons que par le théorème, on a $F_i = K^{H_i}$.

1. Tout σ dans $H_1 \cap H_2$ laisse F fixe point par point. Donc $\sigma \in G(K/F)$. Réciproquement, si $\sigma \in G(K/F)$, alors σ fixe F_i, $i = 1, 2$, donc $\sigma \in H_1 \cap H_2$.

2. Supposons que $x \in F_1 \cap F_2$. Alors x est fixé par chaque élément de H_i, $i = 1, 2$. Donc x est fixé par H (exercice 3.1), c'est-à-dire $x \in K^H$. Le reste du corollaire est facile est laissé au lecteur. □

Lemme 3.1. *Soit E une extension algébrique séparable de k et n tel que tout élément de E est de degré au plus n sur k. Alors $[E : k] \leq n$.*

Démonstration. Soit $\alpha \in E$ tel que $m = [k(\alpha) : k]$ soit maximum. S'il existait $\beta \in E \setminus k(\alpha)$, il existerait d'après le corollaire 3.17 un élément γ tel que $k(\alpha, \beta) = k(\gamma)$; alors $[k(\gamma) : k] = [k(\gamma) : k(\alpha)][k(\alpha) : k] > m$, une contradiction. Donc $E = k(\alpha)$. Par suite, E est de degré $m \leq n$. □

Théorème 3.2. *Soit K un corps et G un groupe fini d'automorphismes de K. Soit $k = K^G$. Alors K est une extension de Galois finie de k, $G(K/k) = G$ et $[K : k] = |G|$.*

Démonstration. Soit $\alpha \in K$ et $\{\sigma_1, \ldots, \sigma_r\}$ une partie H de G telle que les $\sigma_i(\alpha)$ soient distincts, et maximale (pour l'inclusion) pour cette propriété. Ceci implique que si $\tau \in G$, alors chaque $\tau\sigma_i(\alpha)$ est l'un des $\sigma_j(\alpha)$ (sinon on pourrait augmenter H de l'élément $\tau\sigma_i$). Donc $H = \{\tau\sigma_1, \ldots, \tau\sigma_r\}$. Par ailleurs α est aussi l'un des $\sigma_j(\alpha)$ (sinon on pourrait rajouter id à H). Donc α est racine du polynôme $f(x) = \prod_i (x - \sigma_i(\alpha))$; de plus, pour tout τ, $\tau(f) = f$ car τ permute l'ensemble des $\sigma_i(\alpha)$. Par suite chaque coefficient de f est fixé par chaque élément de G et donc $f \in k[x]$. Il s'ensuit que α est algébrique sur k. On en déduit aussi que α est séparable sur k car les racines de f sont distinctes. Donc tout élement de K est séparable, et K est séparable. On en déduit de plus que le polynôme minimal de α se décompose entièrement dans K ; donc K est normal sur k. De même, puisque tout α est racine d'un polynôme de degré $\leq |G|$, le lemme implique que $[K : k] \leq |G|$.

Par le théorème 2.18, on a $[K : k]_s \leq |G|$. Mais $G(K/k)$ contient G, donc par la proposition 3.1, $[K : k]_s = |G|$,$G(K/k) = G$, et enfin $[K : k] = |G|$. □

Corollaire 3.2. *Si K est une extension de Galois finie de k, alors $[K : k] = |G(K/k)|$.*

Démonstration. Soit $G = G(K/k)$. Alors G est fini, car $[K : k]_s = [K : k] < \infty$. D'après le théorème 3.1, on a $k = K^G$ et on applique alors le théorème précédent. □

Corollaire 3.3. *Soit K une extension finie de Galois de k et G son groupe de Galois. Alors tout sous- groupe H de G appartient à un certain corps intermédiaire F et $H = G(K/F)$.*

Démonstration. Soit $F = K^H$. D'après le théorème, K est une extension de Galois de F et H est son groupe de Galois sur F. □

Corollaire 3.4. *Dans une extension $k \subset K$ de Galois finie, on a bijection entre les sous-groupes du groupe de Galois et les corps intermédiaires. Elle est donnée par $H \mapsto K^H$ et la bijection réciproque est $F \mapsto G(K/F)$.*

On appelle *correspondance de Galois* cette bijection. Elle est décroissante pour l'inclusion. Le résultat suivant exprime que dans cette bijection les sous-groupes normaux correspondent aux corps intermédiaires qui sont des extensions de Galois de k.

Théorème 3.3. *Soit K une extension de Galois de k, de groupe de Galois G, F un corps intermédiaire, et $H = G(K/F)$. Alors F est une extension normale de k si et seulement si H est un sous-groupe normal de G. Dans ce cas, la fonction $\sigma \mapsto \sigma|F$ est un homomorphisme surjectif de G sur $G(F/k)$ et $G(F/k)$ est isomorphe à G/H.*

Démonstration. Supposons que F soit normal sur k et soit G' son groupe de Galois. La fonction $\sigma \mapsto \sigma|F$ est un homomorphisme de groupes qui envoie G dans G'. Son noyau est H. Celui-ci est donc normal dans G. De plus, tout $\tau \in G'$ peut se prolonger en un k-homomorphisme de K dans $\bar{k}$ (théorème 2.10), lequel est en fait un k-automorphisme de K (celui-ci est normal sur k) ; l'homomorphisme ci-dessus est donc surjectif et par suite $G(F/k)$ est isomorphe à G'.

Supposons que F ne soit pas normal sur k. Il existe alors un k-homomorphisme $\lambda : F \to \bar{k}$, qui n'est pas un automorphisme de F ; donc $\lambda(F) \neq F$; λ se prolonge en un homomorphisme de K dans $\bar{k}$, qui doit être un automorphisme $\bar{\lambda}$ de K. Par le théorème 3.1, les sous-groupes $H = G(K/F)$

et $G(K/\bar{\lambda}(F))$ de G ne sont pas égaux, car $F \neq \bar{\lambda}(F)$ (ce dernier est égal à $\lambda(F)$). Ils sont cependant conjugués, car $\sigma \in H$ si et seulement si σ fixe F si et seulement si $\bar{\lambda}\sigma\bar{\lambda}^{-1}$ fixe $\lambda(F)$ si et seulement si $\bar{\lambda}\sigma\bar{\lambda}^{-1} \in G(K/\bar{\lambda}(F))$. □

Corollaire 3.5. *Si le groupe de Galois de K sur k est abélien, alors tout corps intermédiaire est une extension de Galois de k.*

EXERCICES

Exercice 3.1. *Soit G un groupe agissant sur un ensemble K, et engendré par un sous-ensemble E. On suppose que chaque élément de E fixe chaque élément de K. Montrer qu'il en est de même pour chaque élément de G.*

Exercice 3.2. *Quel est le groupe de Galois de l'extension $\mathbb{R} \subset \mathbb{C}$?*

Exercice 3.3. *Quel est le groupe de Galois de l'extension $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2}, \exp(2i\pi/3))$?*

Exercice 3.4. *Montrer que le groupe de Galois sur $\mathbb{Q}$ de $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ est $(\mathbb{Z}/2\mathbb{Z})^2$.*

Exercice 3.5. *Soit L une extension galoisienne finie de K et $a \in L$. Montrer que $L \neq K(a)$ si et seulement s'il existe $\sigma \neq 1$ dans G tel que $\sigma(a) = a$.*

Exercice 3.6. *Soit G un groupe fini. Montrer que G est isomorphe à un groupe d'automorphismes de $L = k(x_1, \ldots, x_n)$. Montrer qu'il existe un sous-corps K de L tel que L soit une extension de Galois de K avec groupe G.*

Exercice 3.7. *Montrer que si $f \in \mathbb{R}[x]$ est irréductible, de degré 3, et n'a pas que des racines réelles, alors son corps de décomposition a pour groupe de Galois le groupe symétrique S_3 sur $\mathbb{Q}$. Montrer que $x^3 + 2x + 1$ est un tel polynôme.*

3.2 Propriétés des extensions de Galois

Théorème 3.4. *Soit K une extension de Galois de k, F une extension de k, et L une extension de K et F. Alors KF (resp. K) est une extension de Galois de F (resp. $K \cap F$). Soit $H = G(KF/F)$, $G = G(K/k)$. Si $\sigma \in H$, alors $\sigma|K \in G$ et, sous l'hypothèse que $[KF : F]$ est fini, l'application $\sigma \mapsto \sigma|K$ est un isomorphisme $H \to G(K/K \cap F)$. Ce dernier est un sous-groupe de $G(K/k)$.*

Démonstration. La première assertion découle de la proposition 2.15 (partie 1) et du théorème 2.21 et la seconde de la même proposition (partie 2) et du théorème 2.20.

Si $\sigma \in H$, alors $\sigma|K$ est un homomorphisme $K \to L$ tel que $\sigma|k = id_k$. Comme K est une extension normale de k, σ est un automorphisme de K (Definition 2.9 et Proporsition 2.14 (1)) et $\sigma|K \in G$. Si de plus $\sigma|K = id_K$, comme $\sigma|F = id_F$, on a $\sigma = id_{KF}$.

Donc $\sigma \mapsto \sigma|K$ est un homomorphisme de groupes injectif de H dans G. Soit H' son image. Donc H' fixe $F \cap K$ point par point ; réciproquement, si $\alpha \in K$ est fixé par H', il est fixé par H, donc $\alpha \in F$ (car $(KF)^H = F$, Théorème 3.1), d'où $\alpha \in K \cap F$. Nous en déduisons que $K \cap F = K^{H'}$.

Si $[K : k]$ est fini, ou si $[KF : F]$ est fini, alors H est fini, donc H' est fini, et d'après le théorème 3.2, $H' = G(K/K \cap F)$. □

Corollaire 3.6. *Avec les notations du théorème,* $[KF : F]$ *divise* $[K : k]$.

Démonstration. En effet, $|H|$ divise $|G|$ et on applique le corollaire 3.2. □

Théorème 3.5. *Soient* K_1, K_2 *des extensions de Galois finies de* k*, de groupes de Galois* G_1, G_2*, et qui sont sous-corps d'un même corps. Alors* K_1K_2 *est une extension de Galois de* k*. La fonction* $G = G(K_1K_2/k) \to G_1 \times G_2$*,* $\sigma \mapsto (\sigma|K_1, \sigma|K_2)$ *est un homomorphisme injectif. Si* $k = K_1 \cap K_2$*, c'est un isomorphisme.*

Démonstration. La première assertion découle de la proposition 2.15 (partie 3) et du théorème 2.19. La fonction est bien définie. Si $\sigma \in G$ se restreint en l'identité de K_i pour $i = 1, 2$, alors $\sigma = id_{K_1K_2}$, d'où l'injection. Supposons maintenant que $k = K_1 \cap K_2$. Si $\sigma_1 \in G_1$, il se prolonge par le théorème 3.4 en $\sigma \in G(K_1K_2/K_2)$. Alors $\sigma \in G$ et $\sigma|K_2 = id_{K_2}$. Donc $G_1 \times 1$ est contenu dans l'image de l'homomorphisme ; par symétrie $1 \times G_2$ aussi. L'homomorphisme est donc surjectif. □

Le corollaire suivant s'obtient par récurrence à partir du théorème.

Corollaire 3.7. *Soient* $K_1, \ldots, K_n$ *des extensions de Galois finies de* k*, contenues dans un même corps, de groupes de Galois* $G_1, \ldots, G_n$*. On suppose que* $\forall i = 1, \ldots, n-1, K_{i+1} \cap K_1 \cdots K_i = k$*. Alors* $K_1 \cdots K_n$ *est une extension de Galois de* k*, de groupe de Galois isomorphe à* $G_1 \times \ldots \times G_n$ *(par restriction).*

Corollaire 3.8. *Soit* K *une extension finie de Galois de* k*, de groupe de Galois* G*. Supposons que* G *soit isomorphe à un produit de groupes* $G_1 \times \cdots \times$

G_n. Soit K_i le sous-corps fixé par le groupe $G_1 \times \cdots \times G_{i-1} \times 1 \times G_{i+1} \times \cdots \times G_n$. Alors K_i est une extension de Galois de k et $\forall i = 1, \ldots, n-1, K_{i+1} \cap K_1 \ldots K_i = k$. De plus $K = K_1 \cdots K_n$.

Démonstration. D'après le corollaire 3.1 (partie 1), $K_1 \cdots K_n$ appartient à l'intersection de ces groupes, qui se réduit à l'identité de K ; donc $K = K_1 \cdots K_n$. Chaque sous-groupe ci-dessus est normal dans G, donc K_i est une extension de Galois de k. D'après le corollaire 3.1 (partie 2), une intersection de sous-corps appartient au sous-groupe engendré par leurs groupes ; il s'ensuit que $K_{i+1} \cap K_1 \ldots K_i = k$. □

EXERCICES

Exercice 3.8. *Soient K_1, K_2 des sous-corps de L, supposé être une extension de Galois finie de ces deux sous-corps, de groupe G_1, G_2 respectivement. Soit G le sous-groupe du groupe des automorphismes de L engendré par G_1 et G_2. Montrer que $K_1 \cap K_2 = L^G$ et que L est une extension de Galois de $K_1 \cap K_2$ si et seulement si G est fini ; et que dans ce cas, G en est le groupe de Galois.*

Exercice 3.9. *Soit $f(x)$ un polynôme irréductible dans $k[x]$ et K son corps de décomposition. On suppose que k est parfait et que f n'a que des monômes d'exposant pair. Montrer qu'il existe un σ dans le groupe de Galois de K sur k qui envoie toute racine de f sur son opposée.*

3.3 Groupe de Galois d'un polynôme

Si $f \in k[x]$ est un polynôme dont les racines sont distinctes (i.e. f est séparable), alors son corps de décomposition K est une extension de Galois de k. On appelle *groupe de Galois de f* le groupe de Galois de ce corps. Ce groupe permute les racines de f et on obtient ainsi un homomorphisme de groupe du groupe de Galois de f vers le groupe des permutations de ses racines, lequel homomorphisme est injectif, puisque le corps de décomposition est engendré par les racines de f.

Il en découle aussi que le degré de K sur k est au plus $n!$.

Exemple 3.1. *On suppose que $car(k) \neq 2$. Le groupe de Galois d'un polynôme de degré 2, qui n'a pas de racine dans k, est cyclique d'ordre 2.*

Exemple 3.2. *On suppose que $car(k) \neq 2, 3$. Pour un polynôme de degré 3, on peut se ramener à la forme $f(x) = x^3 + px + q$. On suppose que f n'a pas de racine dans k. Alors f est irréductible. Le degré de son corps de*

décomposition est 3 *ou* 6, *car il contient un sous-corps de degré* 3, *engendré par une des racines. Le groupe de Galois de* f *se plonge dans le groupe symétrique* S_3.

Considérons ses racines a_1, a_2, a_3, $\delta = (a_1 - a_2)(a_1 - a_3)(a_2 - a_3)$, *et* $\Delta = \delta^2$. *On a clairement* $\forall \sigma \in S_3$, $\sigma(\delta) = \pm\delta$ *est donc* $\sigma(\Delta) = \Delta$; *on en déduit que* $\Delta \in k$. *La quantité* δ *est fixée par les permutations paires seulement. Donc* $G = S_3$ *si et seulement si* δ *n'est pas dans* k, *c'est-à-dire si et seulement si* Δ *n'est pas un carré dans* k. *Dans le cas contraire,* G *est le groupe alterné* A_3.

Notons enfin que, puisque Δ *est une fonction symétrique des racines, on peut l'exprimer en fonction des coefficients de* f *: on montre que* $\Delta = -4p^3 - 27q^2$ *(exercice 3.10).*

Exemple 3.3. *Soit* $f(x) = x^4 - 2 \in \mathbb{Q}[x]$. *Par le critère d'Eisenstein, c'est un polynôme irréductible. Soit* α *une racine réelle. Alors* $\mathbb{Q}(\alpha)$ *est de degré* 4 *sur* $\mathbb{Q}$. *Comme* $i \notin \mathbb{Q}(\alpha)$, i *est de degré* 2 *sur ce corps, et par suite le corps* $K = \mathbb{Q}(\alpha, i)$ *est de degré* 8 *sur* $\mathbb{Q}$. *Ce* K *est le corps de décomposition de* f, *puisqu'il est engendré par ses quatre racines, qui sont* $\pm\alpha, \pm i\alpha$. *Soit* G *son groupe de Galois sur* $\mathbb{Q}$. *Il contient l'automorphisme de conjugaison complexe :* $\tau(z) = \bar{z}$.

Le corps $\mathbb{Q}(i)$ *est de degré* 2 *sur* $\mathbb{Q}$, *donc* K *est de degré* 4 *sur* $\mathbb{Q}(i)$, *engendré par* α ; *donc* $f(x)$ *est irréductible sur* $\mathbb{Q}(i)$. *On a un* $\mathbb{Q}(i)$*-automorphisme de* K *qui envoie* α *sur* $i\alpha$, *puisqu'ils ont le même polynôme minimal* f *sur* $\mathbb{Q}(i)$. *On a* $\sigma^n(\alpha) = i^n\alpha$, *donc les* σ^i, $i = 0, 1, 2, 3$ *forment un sous-groupe* H *d'ordre* 4 *de* G ; *ils fixent tous* i, *donc ils sont aussi distincts de* τ, *et on en déduit que* G *est la réunion de* H *et et de sa classe latérale* τH. *On remarque d'ailleurs que* H *est le groupe de Galois de l'extension* $\mathbb{Q}(i) \subset K$. *De plus* $\tau\sigma = \sigma^{-1}\tau$, *et* G *est donc non commutatif.*

Exemple 3.4. *Soient* $x_1, \ldots, x_n$ *des variables. Soit* $K = k(x_1, \ldots, x_n)$. *Les permutations dans* S_n *agissent comme des automorphismes de* K, *par permutation des variables. Soit* $F = K^{S_n}$. *Alors* K *est une extension de Galois de* F *de degré* $n!$ *avec groupe de Galois* S_n. *De plus, soient* e_i *les fonctions symétriques élémentaires des* x_i ; *clairement les* e_i *sont dans* F. *Donc le polynôme* $\prod_i (x - x_i) = \sum_i (-1)^i e_i x^{n-i}$ *est dans* $F[x]$; *son corps de décomposition sur* F *est* $k(x_1, \ldots, x_n)$. *Soit* F' *le corps* $k(e_1, \ldots, e_n)$. *Alors* $f \in F'[x]$ *et le corps de décomposition de* f *sur* F' *est* K ; *comme le degré cette extension est* $\leq n!$, *on doit avoir* $F = F'$, *puisque* $F' \subset F$.

On obtient donc aussi un cas particulier du théorème fondamental des fonctions symétriques *: le sous-corps de* $k(x_1, \ldots, x_n)$ *des fractions rationnelles symétriques en les* x_i *est égal à* $k(e_1, \ldots, e_n)$ *(en fait, on peut prouver*

que tout polynôme sur $\mathbb{Z}$ symétrique en les x_i est dans la $\mathbb{Z}$-algèbre engendrée par les e_i ; voir le livre de Macdonald [3], chapitre 1).

Les $e_i = e_i(x_1, \ldots, x_n)$ s'appellent les fonctions symétriques élémentaires *des racines $x_1, \ldots, x_n$. On a par exemple $e_1 = x_1 + \cdots + x_n$, $e_2 = \sum_{1 \leq i < j \leq n} x_i x_j, \ldots$, $e_n = x_1 \cdots x_n$. Ce sont, au signe près, les coefficients du polynôme de coefficient dominant 1 dont les racines sont les x_i.*

On a en particulier construit une extension de Galois dont le groupe est le groupe symétrique S_n. La même technique permet de construire une extension de Galois avec un groupe de Galois arbitraire (exercice 3.6).

Il n'est pas connu à ce jour si tout groupe fini est toujours le groupe de Galois d'une extension de Galois de $\mathbb{Q}$.

Exercice 3.10. *Montrer que Δ (exemple 3.2) est symétrique en les racines, et montrer qu'il s'exprime en fonction des fonctions symétriques élémentaires e_1, e_2, e_3 des racines : $\Delta = -4e_2^3 - 27e_3^2 = -4p^3 - 27q^2$.*

Exercice 3.11. *Montrer que le groupe de Galois de $x^3 - x + 1$ est S_3.*

Exercice 3.12. *Montrer que le groupe de Galois de $x^3 - 3x + 1$ est A_3.*

3.4 Une preuve que $\mathbb{C}$ est algébriquement clos

Tout polynôme sur $\mathbb{R}$ de degré impair a une racine dans $\mathbb{R}$ (voir l'exercice 3.14). On peut voir ceci en remarquant que ce polynôme tend vers $\pm\infty$ quand la variable fait de même. Par conséquent le théorème des valeurs intermédaires implique que le graphe du polynôme doit traverser l'axe des x et il a donc une racine.

Tout polynôme de degré 2 sur $\mathbb{C}$ a une racine dans $\mathbb{C}$ (voir l'exercice 3.15). Ceci grâce à la formule donnant ces racines, sachant que tout élément de $\mathbb{C}$ a une racine carrée dans $\mathbb{C}$ (exercice 3.13).

Il nous faut encore deux résultats de la théorie des groupes finis, qui se démontrent dans le cadre de la théorie de Sylow : tout groupe fini d'ordre $2^n m$, où m est impair, contient un sous-groupe d'ordre 2^n ; de plus, tout groupe d'ordre 2^k contient un sous-groupe d'ordre 2^{k-1}.

Pour montrer que $\mathbb{C}$ est algébriquement clos, il suffit de montrer que toute extension finie de $\mathbb{C}$ est de degré 1. Soit donc K une telle extension. C'est une extension finie de $\mathbb{R}$, de degré pair (par la formule de multiplicativité des degrés, théorème 2.1). On peut donc la plonger dans une extension de Galois F de $\mathbb{R}$. Soit G son groupe de Galois, de cardinalité $2^n m$, m impair, $n \geq 1$. Soit H un sous-groupe de cardinalité 2^n de G. Alors F est une extension de degré $|H|$ de son sous-corps F^H. Donc celui-ci est une extension de degré m

de $\mathbb{R}$. C'est une extension séparable, donc simple, de la forme $\mathbb{R}(\alpha)$. Mais m est impair, donc le polynôme minimal de α sur $\mathbb{R}$ a une racine dans $\mathbb{R}$, ce qui n'est possible, puisqu'il est irréductible, que si $m = 1$.

Il s'ensuit donc que F est une extension de $\mathbb{R}$ de degré 2^n, donc une extension de Galois de degré 2^{n-1} de $\mathbb{C}$. Supposons que $n \geq 2$. Son groupe de Galois possède un sous-groupe L de cardinalité 2^{n-2}. Alors F^L est une extension de degré 2 de $\mathbb{C}$, ce qui contredit que tout polynôme de degré 2 sur $\mathbb{C}$ a une racine dans $\mathbb{C}$. Donc on doit avoir $n = 1$ et $F = \mathbb{C}$; enfin $K = \mathbb{C}$.

Exercice 3.13. *On veut calculer les racines carrées dans $\mathbb{C}$ du nombre complexe $a + bi$. Si $z = x + iy$ est une telle racine carrée, montrer que $x^2 - y^2 = a$, $x^2 + y^2 = \sqrt{a^2 + b^2}$ et $2xy = b$. En déduire les valeurs de x^2, y^2, puis de x et y au signe près. Déterminer les deux racines cherchées en utilisant l'équation $2xy = b$.*

Exercice 3.14. *Montrer que $\mathbb{R}$ n'a pas d'extension de degré impair, sauf 1 (sans utiliser que $\mathbb{C}$ est algébriquement clos).*

Exercice 3.15. *Montrer que $\mathbb{C}$ n'a pas d'extension de degré 2 (sans utiliser que $\mathbb{C}$ est algébriquement clos).*

Exercice 3.16. *On appelle* nombre algébrique *tout nombre complexe qui est algébrique sur $\mathbb{Q}$ Montrer que l'ensemble $\bar{\mathbb{Q}}$ des nombres algébriques est un sous-corps de $\mathbb{C}$. Montrer que $\bar{\mathbb{Q}}$ est algébriquement clos. Montrer que $\bar{\mathbb{Q}}$ est dénombrable.*

3.5 Compléments sur les racines de l'unité

Une extension de Galois est *abélienne* si son groupe de Galois est abélien.

Théorème 3.6. *Soit ξ une racine primitive m-ème de l'unité, où* $\mathrm{car}(k)$ *ne divise pas m. Alors $k(\xi)$ est une extension abélienne de k.*

Démonstration. C'est une extension finie, normale et séparable, car elle est obtenue en adjoignant toutes les racines de $x^m - 1$; celles-ci sont simples, car le dérivé est mx^{m-1}, qui n'a pas de racine commune avec lui. Soit G le groupe de Galois. Soit σ dans G. Alors $\sigma(\xi)$ est une racine primitive m-ème de l'unité : $\sigma(\xi) = \xi^r$, r premier avec m ; r détermine entièrement σ. La fonction $\sigma \mapsto r$ de G dans le groupe des éléments inversible de l'anneau $\mathbb{Z}/m\mathbb{Z}$ est un homomorphisme injectif. Donc G est abélien. □

Dans la suite de cette section, on suppose que le corps de base est $\mathbb{Q}$.

Théorème 3.7. *Soit ζ une racine primitive n-ème de l'unité. Alors $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(n)$ et Φ_n est le polynôme minimal de ζ.*

Démonstration. Rappelons qu'un polynôme dans $\mathbb{Z}[x]$ est dit *primitif* si ses coefficients sont premiers entre eux ; de plus, le produit de deux polynômes primitifs est primitif (exercice 3.17).

On peut écrire $x^n - 1 = f(x)h(x)$ où $f, h \in \mathbb{Q}[x]$, f est le polynôme minimal de ζ. En chassant les dénominateurs et en utilisant le pgdc des coefficients de f, ainsi que que celui pour h, on se ramène à : (i) f, h sont primitifs dans $\mathbb{Z}[x]$; (ii) $fh = \alpha(x^n - 1)$, $\alpha \in \mathbb{Q}_+$. Alors fh est primitif, donc $\alpha = 1$.

On est donc ramené à $x^n - 1 = f(x)h(x)$, $f, h \in \mathbb{Z}[x]$, f est le polynôme minimal de ζ.

Soit p premier qui ne divise pas n. Montrons que $f(\zeta^p) = 0$. Sinon, on a $h(\zeta^p) = 0$. Donc ζ est racine $h(x^p)$ et par suite $f(x)$ divise $h(x^p)$: $h(x^p) = f(x)g(x)$. Par primitivité, g est à coefficients entiers. On a $h(x)^p \equiv h(x^p)$ mod p, donc $h(x)^p \equiv f(x)g(x)$ et h, f ne sont pas premiers entre eux modulo p. Or $x^n - 1 \equiv f(x)h(x)$ et $x^n - 1$, vu dans $(\mathbb{Z}/p\mathbb{Z})[x]$ aurait des racines multiples. Ça ne peut être vrai, car son dérivé nx^{n-1} a pour seule racine 0 (car il est non nul puisque p ne divise pas n).

Nous en déduisons que $f(\zeta^p) = 0$. Il s'ensuit que toute racine primitive n-ème de l'unité est racine de f. Donc son degré est $\geq \varphi(n)$. Mais on sait déjà qu'il est $\leq \varphi(n)$, car $\Phi_n(\zeta) = 0$, que Φ_n est de degré $\varphi(n)$ et à coefficients entiers (corollaire 2.10). □

Corollaire 3.9. *Les polynômes cyclotomiques sont irréductibles sur $\mathbb{Q}$.*

Corollaire 3.10. *Si n, m sont des entiers naturels premiers entre eux, et K, L les sous-corps de $\mathbb{C}$ engendrés par les racines m-èmes et n-èmes de l'unité respectivement, alors $K \cap L = \mathbb{Q}$.*

Démonstration. Soit ζ une racine primitive mn-ème de l'unité. Alors ζ^m et ζ^n sont des racines primitives de l'unité n-èmes et m-èmes respectivement. Par ailleurs, le produit d'une racine primitive n-ème de l'unité par une racine primitive n-ème de l'unité est une racine mn-ème de l'unité. On en déduit que $KL = M$, le corps engendré par les racines mn-èmes de l'unité.

Or $[M : \mathbb{Q}] = \varphi(mn) = \varphi(m)\varphi(n) = [K : \mathbb{Q}][L : \mathbb{Q}]$. Conclure avec l'exercice 2.21. □

Le résultat suivant découle alors de la preuve du théorème 3.6.

Corollaire 3.11. *Le groupe de Galois de $\mathbb{Q} \subset \mathbb{Q}(\zeta)$ est isomorphe au groupe des éléments inversible de l'anneau $\mathbb{Z}/n\mathbb{Z}$*

EXERCICES

Exercice 3.17. *Montrer que le produit de deux polynômes primitifs dans $\mathbb{Z}[x]$ est primitif (par l'absurde : p premier divise tous les coefficients de leur produit, considérer leur image dans $(\mathbb{Z}/p\mathbb{Z})[x]$).*

3.6 Indépendance linéaire des caractères

Définition 3.4. *Un* caractère d'un monoïde M dans un corps K *est un homomorphisme de monoïdes de M dans K^*.*

Notez que cette notion de caractère est plus restrictive que ce qu'on appelle caractère en théorie des représentations des groupes.

Théorème 3.8. *(Artin) Soient $\chi_1, \ldots, \chi_n$ des caractères distincts de M dans K. Ils sont K-linéairement indépendants.*

Démonstration. S'ils ne sont pas linéairement indépendants, il existe $a_1, \ldots, a_n$ non tous nuls dans K tels que $\sum_i a_i\chi_i = 0$. Sans restreindre la généralité, on peut supposer que les a_i sont tous non nuls et que, sous cette condition, cette relation est la plus courte possible (n minimum). Nous allons montrer que ce n minimum n'existe pas, ce qui prouvera le théorème.

On doit avoir $n \geq 2$, car $\chi_1(1) = 1$. On a $\chi_1 \neq \chi_2$, donc il existe $z \in M$ tel que $\chi_1(z) \neq \chi_2(z)$.

Pour tout $x \in M$, on a $\sum_i \chi_i(xz) = 0$. Comme $\chi_i(xz) = \chi_i(x)\chi_i(z)$, on a $\sum_i a_i\chi_i(z)\chi_i = 0$. Divisons cette relation par $\chi_1(z)$ et soustrayons la relation obtenue à celle de départ. On obtient $\sum_{i\geq 2}(a_i\frac{\chi_i(z)}{\chi_1(z)} - a_i)\chi_i = 0$. Comme $\chi_2(z) \neq \chi_1(z)$, le coefficient de χ_2 est non nul, et c'est une relation plus courte : contradiction. □

Corollaire 3.12. *Soient $\alpha_1, \ldots, \alpha_r$ des éléments non nuls et distincts d'un corps K, et soients $a_1, \ldots, a_r$ des éléments de K. Si pour tout entier naturel n, on a $\sum_i a_i\alpha_i^n = 0$, alors les a_i sont tous nuls.*

Démonstration. On considère les r caractères $\mathbb{N} \to K^*$, $n \mapsto \alpha_i^n$ et on applique le théorème. □

3.7 Norme et trace

Dans cette section, E est une extension finie de k. Si $\mathrm{car}(k) = p > 0$, on pose $[E : k]_i = p^e$ et si $\mathrm{car}(k) = 0$, on sait que $[E : k]_i = 1$ (cf. corollaire 2.15). Soit $r = [E : k]_s$.

Définition 3.5. *Soient $\sigma_1, \dots, \sigma_r$ les k-homomorphismes $E \to \bar{k}$. Soit $\alpha \in E$. La* norme *de α est $N_k^E(\alpha) = \prod_{\nu=1}^{\nu=r} \sigma_\nu(\alpha)^{[E:k]_i}$ et sa* trace *est $Tr_k^E(\alpha) = [E:k]_i \sum_{\nu=1}^{\nu=r} \sigma_\nu(\alpha)$.*

Remarque 3.1. *Si l'extension n'est pas séparable, alors $p^e = 0$ dans E, donc la trace est nulle.*

Si E est séparable, on $N_k^E(\alpha) = \prod_{\nu=1}^{\nu=r} \sigma_\nu(\alpha)$ et $Tr_k^E(\alpha) = \sum_{\nu=1}^{\nu=r} \sigma_\nu(\alpha)$.

Théorème 3.9. *1. La norme envoie 0 sur 0 et sa restriction à E^* est un homomorphisme de groupes multiplicatif $E^* \to k^*$. La trace est k-linéaire $E \to k$.*

2. Si F est un corps intermédiaire, alors $N_k^E = N_k^F \circ N_F^E$ et $Tr_k^E = Tr_k^F \circ Tr_F^E$.

3. Si $E = k(\alpha)$ et que $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ est le polynôme minimal de α sur k, alors $N_k^E(\alpha) = (-1)^n a_0$ et $Tr_k^E(\alpha) = -a_{n-1}$.

Démonstration. 1. Par la preuve de la proposition 2.23, $\alpha^{[k(\alpha),k]_i}$ est séparable sur k. Par le corollaire 2.16, $[k(\alpha),k]_i$ divise $[E:k]_i$. Donc $\beta = \alpha^{[E:k]_i}$ est séparable sur k. Par la proposition 2.12, les $\sigma_\nu(\beta)$ sont les conjugués de β, répétés chacun un même nombre de fois, car $[E:k]_s = [E : k(\alpha)]_s[k(\alpha) : k]_s$ (théorème 2.17). Le produit de ces conjugués est dans k. Donc la norme de α, qui est le produit de $\sigma_\nu(\beta)$, est dans k.

Le raisonnement est semblable pour la trace.

2. On peut supposer que E est un sous-corps de $\bar{k}$. Soient τ_j, $1 \le j \le s = [F:k]_s$, les homomorphismes $F \to \bar{k}$ qui prolongent l'identité de k. Soient δ_i, $1 \le i \le t = [E:F]_s$, les homomorphismes $E \to \bar{k}$ qui prolongent l'identité de F. Alors $\forall i, j$, $\tau_j \circ \delta_i$ est un homomorphisme $E \to \bar{k}$ qui prolonge l'identité de k. Si $\tau_j \circ \delta_i = \tau_{j'} \circ \delta_{i'}$, alors leur restriction à F sont égales, et comme celle des δ est l'identité de F, on $\tau_j = \tau_{j'}$, et comme τ_j est injectif, on a aussi $\delta_i = \delta_{i'}$. Ceci montre que les $\tau_j \circ \delta_i$ sont exactement tous les homomorphismes $E \to \bar{k}$ prolongeant l'identité de k, lesquels sont en effet au nombre de $[E:k]_s = [E:F]_s[F:k]_s = st$.

Par ailleurs $[E:k]_i = [E:F]_i[F:k]_i$.On en déduit que pour tout $\alpha \in E$, $N_k^F \circ N_F^E(\alpha) = N_k^F(\prod_i \delta_i(\alpha)^{[E:F]_i}) = \prod_j \tau_j(\prod_i \delta_i(\alpha)^{[E:F]_i})^{[F:k]_i} = (\prod_{i,j} \tau_j \circ \delta_i)(\alpha)^{[E:k]_i} = N_k^E(\alpha)$.

Pour la trace, le raisonnement est analogue.

3. Si $E = k(\alpha)$, alors $f(x) = ((x-\alpha_1)\cdots(x-\alpha_r))^{[E:k]_i}$, où les α_i sont les racines distinctes de f. On en déduit les relations cherchées, par la proposition 2.12. □

Théorème 3.10. *Soit E une extension finie séparable de k. Alors Tr_k^E est non nulle. L'application $(x,y) \mapsto Tr_k^E(xy)$, $E \times E \to k$, est une forme k-bilinéaire non dégénérée. Pour $x \in E$, soit Tr_x la fonction $y \mapsto Tr_k^E(xy)$; alors $\phi : E \to$ dual de E, $x \mapsto Tr_x$, est un isomorphisme du k-espace vectoriel E sur son dual.*

Démonstration. La forme bilinéaire est non dégénérée : supposons en effet que $Tr_k^E(xy) = 0$ pour tout $y \in E$. Alors $0 = \sum_{\nu=1}^{\nu=r} \sigma_\nu(xy) = \sum_{\nu=1}^{\nu=r} \sigma_\nu(x)\sigma_\nu(y)$ pour tout y dans E. Alors, d'après le théorème 3.8, on doit avoir $\sigma_\nu(x) = 0$, donc $x = 0$. Le reste du théorème en découle. □

Par dualité en algèbre linéaire, nous en déduisons le

Corollaire 3.13. *Soit $\{\omega_1, \ldots, \omega_n\}$ une base de E sur k. Il existe une unique base $\{\omega'_1, \ldots, \omega'_n\}$ telle que $Tr_k^E(\omega_i \omega'_j) = \delta_{ij}$ pour tous i, j (ici, δ_{ij} est le delta de Kronecker).*

Corollaire 3.14. *Soient $\sigma_1, \ldots, \sigma_n$ les k-homomorphismes de E dans $\bar{k}$. Soient $w_1, \ldots, w_n$ des éléments de E. Alors les vecteurs $\xi_i = (\sigma_i(w_1), \ldots, \sigma_i(w_n)) \in \bar{k}^n$, $i = 1, \ldots, n$, sont linéairement indépendants sur E si les $w_1, \ldots, w_n$ forment une k-base de E.*

Démonstration. Si les $w_1, \ldots, w_n$ forment une k-base de E, soient α_i des éléments de E tels que $\alpha_1\xi_1 + \cdots + \alpha_n\xi_n = 0$. Donc pour tout j, $(\alpha_1\sigma_1 + \cdots + \alpha_n\sigma_n)(w_j) = \alpha_1\sigma_1(w_j) + \cdots + \alpha_n\sigma_n(w_j)_n = 0$. On en déduit que $\alpha_1\sigma_1 + \cdots + \alpha_n\sigma_n = 0$. Par suite, les α_i sont tous nuls, par le théorème 3.8. □

Proposition 3.2. *Soit $E = k(\alpha)$ une extension séparable de k et f le polynôme minimal de α. On pose $f(x)/(x-\alpha) = \beta_0 + \beta_1 x + \cdots + \beta_{n-1}x^{n-1}$, $\beta_i \in E$. Alors la base duale de $1, \alpha, \cdots, \alpha^{n-1}$ pour la forme bilinéaire du corollaire 3.13 est $\beta_0/f'(\alpha), \ldots, \beta_{n-1}/f'(\alpha)$.*

Notez que $f'(\alpha)$ est non nul car f est séparable, donc α n'en est pas racine double.

Démonstration. Soient α_i, $i = 1, \ldots, n$, les racines distinctes de f. Alors pour tout $r = 0, \ldots, n-1$, on a $\sum_{1 \le i \le n} \frac{f(x)}{x-\alpha_i} \frac{\alpha_i^r}{f'(\alpha_i)} = x^r$. En effet, les deux membres sont de degré au plus $n-1$, et sont égaux pour les n valeurs distinctes α_j. En effet, écrivons que $f(x) = (x-\alpha_j)f_j(x)$; alors $f'(x) = f_j(x) + (x-\alpha_j)f'_j(x)$, donc $f'(\alpha_j) = f_j(\alpha_j)$, autrement dit $\frac{f(x)}{x-\alpha_j}|_{x \to \alpha_j} = f'(\alpha_j)$.

Définissions un application additive $Tr : E[x] \to E[x]$ telle que $Tr(\lambda x^r) = Tr_k^E(\lambda)x^r$.

Les polynômes $\frac{f(x)}{x-\alpha_i}\frac{\alpha_i^r}{f'(\alpha_i)}$, $i = 1\ldots,n$, sont conjugués par rapport à k (ils sont l'image de $\frac{f(x)}{x-\alpha}\frac{\alpha^r}{f'(\alpha)}$ par les n k-homomorphismes distincts $\sigma_1,\ldots,\sigma_n$ de E dans $\bar{k}$). D'où $Tr(\frac{f(x)}{x-\alpha}\frac{\alpha^r}{f'(\alpha)}) = \sum_{1\le i\le n}\sigma_i(\frac{f(x)}{x-\alpha}\frac{\alpha^r}{f'(\alpha)}) = \sum_{1\le i\le n}\frac{f(x)}{x-\alpha_i}\frac{\alpha_i^r}{f'(\alpha_i)}) = x^r$. En regardant le coefficient de x^i dans cette égalité, on trouve que $Tr_k^E(\alpha^r\frac{\beta_i}{f'(\alpha)}) = \delta_{ri}$. □

3.8 Extensions cycliques

Une extension de Galois est dite *cyclique* si son groupe de Galois est cyclique.

Théorème 3.11. *(Hilbert) Soit K une extension cyclique de k, de degré n, de groupe de Galois G engendré par σ, et soit $N = N_k^K$. Un élément de K^* est de norme 1 si et seulement s'il est de la forme $\beta/\sigma(\beta)$.*

Démonstration. On a $N(\alpha) = \prod_{1\le i\le n}\sigma^i(\alpha)$, donc si α est de la forme indiquée, sa norme est 1 (car $\sigma^n = 1$).

Réciproquement, supposons que $N(\alpha) = 1$. Pour $\theta \in K$, posons $\beta(\theta) = \theta+\alpha\sigma(\theta)+\alpha\sigma(\alpha)\sigma^2(\theta)+\cdots+\alpha\sigma(\alpha)\cdots\sigma^{n-2}(\alpha)\sigma^{n-1}(\theta)$. D'après le théorème 3.8, les n automorphismes dans G sont linéairement indépendants sur K ; il existe donc $\theta \in K$ tel que $\beta(\theta) \neq 0$.

Comme $\alpha\sigma(\alpha)\cdots\sigma^{n-1}(\alpha) = N(\alpha) = 1$, on a $\alpha\sigma(\beta(\theta)) = \alpha\sigma(\theta) + \alpha\sigma(\alpha)\sigma^2(\theta)+\alpha\sigma(\alpha)\sigma^2(\alpha)\sigma^3(\theta)+\cdots+\theta = \beta(\theta)$. Donc $\alpha = \beta(\theta)/\sigma(\beta(\theta))$. □

Théorème 3.12. *Soit k un corps, $n \in \mathbb{N}\setminus \mathrm{car}(k)\mathbb{N}$ et $\xi \in k$ une racine primitive n-ème de l'unité.*

1. Si K est une extension cyclique de k de degré n, il existe $a \in k$ tel que $K = k(\alpha)$ et que α est racine du polynôme $x^n - a$, irréductible sur k.

2. Soit $a \in k^*$ et α une racine de $x^n - a$. Alors $k(\alpha)$ est une extension cyclique de k, de degré d divisant n et $\alpha^d \in k$.

Démonstration. Soit σ un générateur de G. Comme $\xi \in k$, on a $N(\xi^{-1}) = (\xi^{-1})^n = 1$. D'après le théorème 3.11 appliqué à ξ^{-1}, il existe α tel que $\sigma(\alpha) = \xi\alpha$. Il s'ensuit que pour tout i, $\sigma^i(\alpha) = \xi^i\alpha$. Donc α a au moins n conjugués, ce qui implique que $[k(\alpha) : k] \ge n$. Donc $K = k(\alpha)$. De plus $\sigma(\alpha^n) = \sigma(\alpha)^n = (\xi\alpha)^n = \alpha^n$, donc $\alpha^n \in K^G = k$.

2. Pour tout i, $\xi^i\alpha$ est une racine de $x^n - a$. Donc ce polynôme a n racines distinctes dans $k(\alpha)$, qui est donc une extension de Galois de k. Soit

G son groupe de Galois. Pour $\sigma \in G$, $\sigma(\alpha)$ est une racine du polynôme, donc est de la forme $\omega_\sigma \alpha$, ω_σ racine n-ème de l'unité. L'application $\sigma \mapsto \omega_\sigma$ est un homomorphisme de G dans le groupe des racines n-èmes de l'unité ; elle est injective. Donc G est cyclique d'ordre d, avec $d|n$. Soit σ un générateur de G. Alors ω_σ est une racine primitive d-ème de l'unité. De plus $\sigma(\alpha^d) = \sigma(\alpha)^d = (\omega_\sigma \alpha)^d = \alpha^d$, donc $\alpha^d \in k(\alpha)^G = k$. □

Théorème 3.13. *(Artin) Soit K une extension cyclique de k, de degré n, de groupe de Galois G engendré par σ, et soit $Tr = Tr_k^K$. Un élément de K est de trace nulle si et seulement s'il est de la forme $\beta - \sigma(\beta)$.*

Démonstration. Si $\alpha = \beta - \sigma(\beta)$, alors $Tr(\alpha) = \sum_{1 \leq i \leq n} \sigma^i(\alpha) = 0$, car $\sigma^n = 1$.

Réciproquement, supposons que $Tr(\alpha) = 0$. Il existe $\theta \in K$ tel que $Tr(\theta) \neq 0$ (théorème 3.10). Soit $\beta = \frac{1}{Tr(\theta)}(\alpha\sigma(\theta) + (\alpha + \sigma(\alpha))\sigma^2(\theta) + \cdots + (\alpha + \sigma(\alpha) + \cdots + \sigma^{n-2}(\alpha))\sigma^{n-1}(\theta))$. Alors $\alpha = \beta - \sigma(\beta)$. □

Théorème 3.14. *(Artin-Schreier) Soit k un corps de caractéristique p non nulle.*

1. Soit K une extension cyclique de k, de degré p. Il existe $\alpha \in K$ tel que $K = k(\alpha)$ et que α est une racine du polynôme $x^p - x - a$, $a \in k$, irréductible sur k.

2. Soit $a \in k$. Définissons le polynôme $f(x) = x^p - x - a$. Alors on a une des deux propriétés suivantes :

(i) soit f a une racine dans k, et alors s'y factorise complètement ;

(ii) soit f est irréductible sur k et dans ce cas, α étant une de ses racines, $k(\alpha)$ est une extension cyclique de degré p de k.

Démonstration. 1. On $Tr(-1) = \sum_{1 \leq i \leq p} \sigma^i(-1) = \sum_{1 \leq i \leq p}(-1) = p(-1) = 0$. Par suite, le théorème 3.13 implique qu'il existe $\beta \in K$ tel que $1 = \sigma(\alpha) - \alpha$. Donc $\sigma(\alpha) = \alpha + 1$. Donc $\sigma^i(\alpha) = \alpha + i$ et α a p conjugués distincts. Donc $[k(\alpha) : k] \geq p$ ce qui implique que $K = k(\alpha)$. De plus $\sigma(\alpha^p - \alpha) = \sigma(\alpha)^p - \sigma(\alpha) = (\alpha + 1)^p - (\alpha + 1) = \alpha^p - \alpha$. Donc cet élément est dans k.

2. Si f a une racine α dans k, alors pour tout entier i, $\alpha + i \in k$ et de plus, $(\alpha + i)^p - (\alpha + i) = \alpha^p - \alpha + i^p - i = \alpha^p - \alpha$ (car $i^p - i = 0$ par le petit théorème de Fermat), donc $\alpha + i$ est aussi racine, et f a p racines distinctes dans k.

Supposons que f n'ait aucune racine dans k. Supposons aussi que f est réductible sur k : $f = gh$ avec $g, h \in k[x]$, $0 < deg(g) < p$. Soit α une racine de f. Alors $f(x) = \prod_{1 \leq i \leq p}(x - \alpha - i)$. Posons $g(x) = x^d + a_1 x^{d-1} + \cdots + a_d$.

Soient D l'ensemble des i tels que $\alpha+i$ soit racine de g. On a $Card(D) = d$, $0 < d < p$. Comme $g(x) = \prod_{i\in D}(x-\alpha-i)$, on a $a_1 = -\sum_{i\in D}(\alpha+i)$. Donc $a_1 = -d\alpha + j$, $j \in \mathbb{Z}$. Donc $\alpha \in k$, ce qui n'est pas.

Donc f est irréductible. Toutes ses racines sont dans $k(\alpha)$, qui est une extension de Galois de k. Comme $\alpha+1$ est racine, il existe un automophisme σ de $k(\alpha)$ tel que $\sigma(\alpha) = \alpha + 1$. Donc les automorphismes σ^i, $i = 1, \ldots, p$, sont distincts : ils forment le groupe de Galois. □

3.9 Extensions résolubles et résolubles par radicaux

Rappelons que d'après le théorème 2.24, la clôture normale d'une extension finie séparable est une extension de Galois.

Définition 3.6. *1. Une extension de Galois E de k est dite* résoluble *si elle est finie et si son groupe de Galois est résoluble.*

2. Une extension finie séparable E de k est dite résoluble *si sa clôture normale est une extension résoluble de k.*

Lemme 3.2. *L'extension séparable finie E de k est résoluble si et seulement s'il existe une extension de Galois résoluble de k, qui contient E.*

Démonstration. La condition est nécessaire, car la clôture normale de E est une extension de Galois de k (théorème 2.24), qui est résoluble par hypothèse.

Montrons que la condition est suffisante. Soit L une extension de Galois de k, dont le groupe est résoluble, et qui contient E. Soit K la clôture normale de E. On a la chaine d'extensions $k \subset E \subset K \subset L$. Comme K est une extension normale de k, le groupe $G(L/K)$ est un sous-groupe normal de $G(L/k)$ et $G(K/k)$ est un quotient de $G(L/k)$ (théorème 3.3) ; il est donc résoluble, comme quotient d'un groupe résoluble. □

Théorème 3.15. *1. Si E est une extension résoluble de k et F une extension de k, telles que E, F soient sous-corps d'un même corps, alors EF est une extension résoluble de F.*

2. Soit $k \subset F \subset E$ une chaîne d'extensions. Alors E est une extension résoluble de k si et seulement si E est une extension résoluble de F et F une extension résoluble de k.

3. Soient K_1, K_2 des sous-corps d'un même corps, et extensions résolubles de k. Alors K_1K_2 est une extension résoluble de k

Démonstration. 1. Soit K une extension de Galois de k avec groupe résoluble, et contenant E comme sous-corps (on utilise le lemme 3.2). Alors

KF est une extension de Galois finie de F et $G(KF/F)$ est isomorphe à $G(K/K\cap F)$ (théorème 3.4), lequel est un sous-groupe de $G(K/k)$. On peut donc conclure, car tout sous-groupe d'un groupe résoluble fini est résoluble.

2. Supposons que E est une extension résoluble de F et F une extension résoluble de k. Il existe une extension de Galois finie K de k, dont le groupe est résoluble et qui contient F. D'après 1., EK est une extension de résoluble de K. Il existe donc une extension de Galois finie résoluble L de K qui contient EK.

Soit σ un k-homomorphisme de L dans $\bar{k}$. Comme K est normal sur k, σ est un automorphisme de K. Donc $\sigma(L)$ est une extension de Galois résoluble de K. Soit $M = \prod_\sigma \sigma(L)$, où le produit est sur l'ensemble fini de ces homomorphismes. Il est clair que M contient L (on peut supposer que $L \subset \bar{k}$ et prendre $\sigma = id$) et qu'il est normal sur k. De plus L est séparable sur K et celui-ci sur k, donc L est séparable sur k (théorème 2.20). Donc $\sigma(L)$ est séparable sur k aussi, et enfin M (théorème 2.19). Celui-ci est donc une extension de Galois de k, donc sur K.

D'après le théorème 3.3, $G(K/k)$ est isomorphe à $G(M/k)/G(M/K)$. De plus, par le théorème 3.5, $G(M/K)$ est un sous-groupe de $\prod_\sigma G(\sigma(L)/K)$; il est donc résoluble. De plus $G(K/k)$ est résoluble. Donc, M est une extension de Galois résoluble de k. Donc E aussi, car $E \subset M$.

Réciproquement, supposons que E soit une extension résoluble de k. Clairement, son sous-corps F en est une aussi. Soit K une extension de Galois résoluble de k contenant E. Alors, par le théorème 3.3, $G(K/F)$ est un sous-groupe de $G(K/k)$, donc K est une extension résoluble de F, et enfin E aussi.

3. Découle et 1. et 2. □

Définition 3.7. *Une extension finie F de k est dite* résoluble par radicaux *si elle est séparable et s'il existe une suite finie de corps $k = E_0 \subset E_1 \ldots \subset E_m = E$, chacun sous corps du suivant, avec F sous-corps de E, telle que chaque E_{i+1} s'obtienne de E_i par une des opérations suivantes : on rajoute une racine de l'unité ; on ajoute à E_i une racine de $x^n - a$, $a \in E_i$, n premier à la caractéristique de k ; on rajoute une racine de $x^p - x - a$, $a \in E_i$, $p = \mathrm{car}(k) > 0$.*

Théorème 3.16. *Le théorème précédent est encore vrai si on remplace partout "extension résoluble" par "extension résoluble par radicaux".*

Théorème 3.17. *Soit E une extension finie séparable de k. Alors E est une extension résoluble par radicaux de k si et seulement si c'est une extension résoluble de k.*

Démonstration. Supposons que E soit une extension résoluble de k. Il existe alors une extension de Galois résoluble K de k dont E est un sous-corps. Soit m le produit des nombres premiers, $\neq \mathrm{car}(k)$, divisant $[K : k]$. Soit $F = k(\xi)$ où est ξ est une racine primitive m- ème de 1. D'après le théorème 3.6, F est une extension abélienne de k. Donc KF est une extension résoluble de F. Il existe donc dans $G(KF/F)$ une suite normale dont chaque quotient est un groupe cyclique d'ordre premier. Donc, par le théorème 3.3, il existe entre F et KF une suite finie croissante de sous-corps telle que chaque sous-corps est une extension cyclique d'ordre premier du précédent. Par les théorèmes 3.12, 3.14 et 2.8, on conclut que KF est une extension résoluble par radicaux de F, donc aussi de k. Comme KF est une extension de E, E est par définition une extension résoluble par radicaux de k.

Réciproquement supposons que E soit une extension résoluble par radicaux de k. Pour tout k-homomorphisme σ de E dans $\bar{k}$, l'extension $\sigma(E)$ de k est aussi résoluble par radicaux. Donc la plus petite extension de Galois K de k contenant E l'est aussi. Soit m comme ci-dessus. Soit $F = k(\xi)$ où ξ une racine primitive m-ème de l'unité. Alors KF est une extension résoluble par radicaux de F. Il existe donc une suite finie croissante de sous-corps de F jusqu'à KF telle que chaque extension intermédiaire est de degré premier. Les théorèmes 3.12, 3.14 et 2.8 montrent alors que KF est une extension de Galois résoluble de F, car la racine de l'unité est dans F. Donc, comme F est une extension abélienne de k, KF est une extension de Galois résoluble de k (Théorème 3.15). Or $G(K/k)$ est un quotient de $G(KF/k)$, donc K est une extension de Galois résoluble de k et enfin, E est une extension résoluble de k (Lemme 3.2). □

3.10 Théorie de Kummer

Définition 3.8. *Soit K une extension de Galois de k de groupe G. Soit $m \in \mathbb{N}$. On dit que K est d'*exposant *m si $\sigma^m = 1$ pour tout $\sigma \in G$.*

On suppose dans la suite que m n'est pas un multiple de $\mathrm{car}(k)$ et que k contient le groupe Z_m de toutes les racines m-èmes de l'unité.

Définition 3.9. *Tous les corps considérés sont des sous-corps de $\bar{k}$.*

On note $k(a^{1/m})$ le corps engendré sur k par une racine m-ème de $a \in k$.

On note k^{*m} le sous-groupe multiplicatif de k^* formé des puissances m-ème des éléments de k.

Soit A un sous-groupe de k^* tel que $k^{*m} \subset A \subset k^*$. On note $k(A^{1/m})$, ou K_A, le composé de tous les corps $k(a^{1/m})$ avec $a \in A$.

Théorème 3.18. *Le corps K_A est une extension abélienne d'exposant m de k. Soit G son groupe de Galois. On a une application $\mathbb{Z}$-bilinéaire $G \times A \to Z_m$, $(\sigma, a) \mapsto < \sigma, a >= \omega_\sigma^a$, où $\sigma(\alpha) = \omega_\sigma^a \alpha$, $\alpha^m = a$. On $a < \sigma, a >= \sigma(\alpha)/\alpha$. Le noyau à gauche de l'application bilinéaire est 1 et celui à droite est k^{*m}. L'extension K_A de k est finie si et seulement si $[A : k^{*m}]$ est fini et dans ce cas, ce nombre est le degré de l'extension.*

Démonstration. Soit $a \in A$ et $\alpha \in K_A$ tel que $\alpha^m = a$. Le polynôme $x^m - a$ se décompose dans K_A en facteurs linéaires distincts et par suite K_A est une extension de Galois de k. Soit $\sigma \in G$. Alors $\sigma(\alpha) = \omega_\sigma^a \alpha$ où ω_σ^a est une racine m-ème de l'unité. L'application $\sigma \mapsto (\omega_\sigma^a)_{a \in A}$ est un homomorphisme injectif $G \to Z_m^A$. Donc G est commutatif.

On a $\omega_\sigma^a = \sigma(\alpha)/\alpha$. De plus, ω_σ^a est indépendant de α : en effet, si $\alpha'^m = a$, alors $\alpha' = \xi\alpha$, $\xi \in Z_m$; donc $\sigma(\alpha') = \xi\sigma(\alpha) = \xi\omega_\sigma^a\alpha = \omega_\sigma^a\alpha'$.

Posons $< \sigma, \alpha >= \omega_\sigma^a$. Considérons l'application $(\sigma, a) \mapsto < \sigma, a >$. Si $a, b \in k$, $\alpha^m = a$, $\beta^m = b$, alors $(\alpha\beta)^m = ab$, donc $\sigma(\alpha\beta)/\alpha\beta = (\sigma(\alpha)/\alpha)(\sigma(\beta)/\beta)$, donc l'application est bilinéaire.

Si $< \sigma, a >= 1$ pour tout $a \in A$, alors pour tout $\alpha \in K_A$ tel que $\alpha^m \in A$, on $\sigma(\alpha) = \alpha$, donc $\sigma = 1$. Le noyau à gauche est donc 1.

Si $a \in A$ et si $a^{1/m}$ n'est pas dans k, il existe un k-automorphisme τ de $k(a^{1/m})$ qui n'est pas l'identité. On peut le prolonger en un automorphisme σ de K_A. On a alors $< \sigma, a >= \sigma(\alpha)/\alpha \neq 1$, $\alpha^m = a$. Donc le noyau à droite est k^{*m}. □

Théorème 3.19. *Mêmes notations que dans le théorème précédent. L'application $A \mapsto K_A$ est une bijection de l'ensemble des sous-groupes de k contenant k^{*m} vers l'ensemble des extensions abéliennes de k d'exposant m.*

Démonstration. Soient A_1, A_2 des sous-groupes de k^* contenant k^{*m}. Supposons que $A_1 \subset A_2$. Alors $K_{A_1} \subset K_{A_2}$. Réciproquement, supposons qu'on ait cette dernière inclusion. Soit $b \in A_1$. Alors $k(b^{1/m}) \subset K_{A_1}$. Donc $k(b^{1/m}$ est contenue dans une sous-extension finie de K_{A_2}. On est donc ramené à $[K_{A_2} : k]$ fini. Soit A_3 le sous-groupe de k^* engendré par A_2 et b. Donc $K_{A_2} = K_{A_3}$. D'après le théorème, le degré de cette extension est $[A_2 : k^{*m}] = [A_3 : k^{*m}]$. Donc $A_2 = A_3$ et $b \in A_2$. Donc $A_1 \subset A_2$.

Ceci implique l'injectivité de l'application. Pour la surjectivité, soit K une extension abélienne d'exposant m de k. Soit E une sous-extension de K, finie sur k, de groupe G ; celui-ci est forcément abélien, d'exposant m. Il s'ensuit que $G = G_1 \times \cdots \times G_n$, où les G_i sont cycliques d'ordre divisant m. Soit E_i le sous-corps de E fixé par le produit des G_j, excluantG_i, sous-groupe de G. Alors E_i est une extension de Galois de k, et $E = E_1 \cdots E_n$

(Corollaire 3.8). De plus $G(E_i/k) \simeq G(E/k)/G(E/E_i) \simeq G_i$, qui est cyclique d'ordre divisant m. D'après le théorème 3.12, chaque E_i s'obtient de k en y adjoignant une racine d-ème de l'unité, avec $d|n$, donc aussi en y ajoutant une puissance m-ème de l'unité (quitte à élever l'élément de k à la puissance m/d. Donc K s'obtient par adjonction des racines m-êmes de $b_j \in k$, $j \in J$. Soit A le sous-groupe multiplicatif de k^* engendré par les b_j et k^{*m}. Si $b = b'a^m$, $a, b \in k$, alors $k(b^{1/m}) = k(b'^{1/m})$. On en déduit que $K_A = K$. □

On suppose dans la suite que $m = p = \mathrm{car}(k) > 0$.

Définition 3.10. *On définit un homomorphisme additif $\mathcal{P} : k \to k$ par $\mathcal{P}(a) = a^p - a$. On note $\mathcal{P}^{-1}(a)$ l'ensemble des racines du polynôme $x^p - x - a$. Si A est un sous-groupe additif de k contenant $\mathcal{P}(k)$, on note $K_A = k(\mathcal{P}^{-1}(B))$.*

Théorème 3.20. *Soit k un corps de caractéristique $p > 0$. L'application $A \mapsto K_A$ est une bijection de l'ensemble des sous-groupes additifs de k contenant $\mathcal{P}(k)$ et l'ensemble des extensions abéliennes de k d'exposant p. Soit G le groupe de Galois de K_A sur k. On a une application bilinéaire $G \times A \to \mathbb{Z}/p\mathbb{Z}$, $(\sigma, a) \mapsto < \sigma, a >$. Si $\mathcal{P}(\alpha) = a$, alors $< \sigma, a >= \sigma(\alpha) - \alpha$, $\alpha^p = a$. Le noyau à gauche est 1 et celui à droite est $\mathcal{P}(k)$. L'extension K_A est finie sur k si et seulement si $[A : \mathcal{P}(k)]$ l'est, et dans ce cas, ce dernier nombre est le degré de l'extension.*

Démonstration. Analogue à celle des deux théorèmes précédents. □

3.11 L'équation $x^n - a = 0$

Théorème 3.21. *Soit k un corps, n un entier ≥ 2 et $a \in k^*$. On suppose que pour tout p premier divisant n, $a \notin k^p$; de plus, si $n \in 4\mathbb{N}$, alors $a \notin -4k^4$. Alors $x^n - a$ est irréductible dans $k[x]$.*

Lemme 3.3. *On suppose que $x^u - a$ est irréductible dans $k[x]$, que α en est une racine, et que $x^v - \alpha$ est irréductible dans $k(\alpha)[x]$. Alors $x^{uv} - a$ est irréductible dans $k[x]$.*

Démonstration. Soit A une racine de $x^v - \alpha$. Comme ce polynôme est irréductible, on $[k(\alpha)(A) : k(\alpha)] = v$. Pour la même raison, $[k(\alpha) : k] = u$. Or $A^v = \alpha$, donc $k(\alpha)(A) = k(A)$. D'où $[k(A) : k] = [k(A] : k(\alpha)][k(\alpha) : k] = vu$. Comme A est racine de $x^{uv} - 1$, ce polynôme est irréductible dans $k[x]$. □

Démonstration du théorème 3.21. 1. Supposons d'abord que $n = p^r$, p premier.

1.1 On suppose dans un premier temps que $p = \mathrm{car}(k)$ et on va prouver par récurrence sur r que si a n'est pas une puissance p-ème dans k, alors $x^{p^r} - a$ est irréductible dans $k[x]$. Si $r = 1$: supposons par l'absurde que $x^p - a = Q(x)R(x)$, avec $0 < \deg(Q) < p$, $Q, R \in k[x]$, unitaires. Alors, dans $k(\alpha)$, avec $\alpha^p = a$, on a $Q(x) = (x-\alpha)^{\deg(Q)}$. Donc, en considérant le terme de degré $\deg(Q) - 1$, on voit que $-\deg(Q)\alpha \in k$. Comme p ne divise pas $\deg(Q)$, on obtient $\alpha \in k$, ce qui n'est pas. Donc $x^p - a$ est irréductible sur k.

On suppose maintenant que $r \geq 2$ et que le résultat est vrai pour $r-1$. Soit α tel que $\alpha^p = a$; alors $\alpha \notin k$. Si l'on avait $\alpha = \beta^p$, $\beta \in k(\alpha)$, alors, en utilisant la norme N de $k(\alpha)$ sur k, on obtiendrait : $-a = (-1)^p N(\alpha) = (-1)^p N(\beta)^p$, donc $a = (-1)^{p+1} N(\beta)^p$, ce qui par hypothèse n'est possible que si $p = 2$; mais dans ce cas, on aurait aussi $a = -a = N(\beta)^2$, ce qui n'est pas non plus. Donc par hypothèse de récurrence, $x^{p^{r-1}} - \alpha$ est irréductible dans $k(\alpha)[x]$). Si l'on avait dans $k[x]$, $x^{p^r} - a = Q(x)R(x)$, $0 < \deg(Q) < p^r$, alors $(x^{p^{r-1}} - \alpha)^p = Q(x)R(x)$, donc $Q(x) = (x^{p^{r-1}} - \alpha)^q$, $0 < q < p$, et en considérant le terme de degré $x^{(q-1)p^{r-1}}$, on voit que $\alpha \in k$, ce qui absurde. Donc $x^{p^r} - a$ est irréductible dans $k[x]$.

1.2 On suppose maintenant que p n'est pas la caractéristique de k. La récurrence est toujours sur r.

Supposons que $r = 1$ et qu'on ait $x^p - a = g(x)h(x)$, $g, h \in k[x]$ unitaires, $0 < \deg(g) = q < p$. Soit γ le terme constant de g. Dans une extension de k, soit ζ une racine primitive p-ème de l'unité, et α une racine p-ème de a. Dans cette extension on a $x^p - a = \prod_{1 \leq i \leq p}(x - \zeta^i \alpha)$, donc $\gamma = (-1)^q \alpha^q \zeta^s$, $s \in \mathbb{N}$. Il existe $u, v \in \mathbb{Z}$ tels que $up + vq = 1$. Donc $\gamma^{vp} = (-1)^{qvp} \alpha^{qvp} \zeta^{svp} = (-1)^{qvp} \alpha^{p - up^2} = (-1)^{qvp} a / a^{up}$, donc $a = (a^u \gamma^v (-1)^{qv})^p \in k^p$, une contradiction. Nous en concluons que $x^p - a$ est irréductible dans $k[x]$.

Supposons maintenant que $r \geq 2$ et que le résultat est vrai pour $r - 1$; soit α dans une extension de k tel que $\alpha^p = a$. On a par hypothèse $\alpha \notin k$. Si l'on avait $\alpha = \beta^p$, $\beta \in k(\alpha)$, alors, puisque le polynôme minimal de α est $x^p - a$, $-a = N(\alpha)(-1)^p = (-1)^p N(\beta)^p$.

Si p est impair, on obtient une contradiction et ceci force $\alpha \notin k(\alpha)^p$. Nous en concluons par hypothèse de récurrence que $x^{p^{r-1}} - \alpha$ est irréductible sur $k(\alpha)$ (car p^{r-1} n'est pas un multiple de 4). Le lemme montre alors que $x^{p^r} - a$ est irréductible dans k.

Si par contre p est pair, alors $p = 2$, et $-a = N(\beta)^2$ est un carré dans k. Ecrivons $-a = b^2$, $b \in k$. Comme a n'est pas un carré dans k, -1 non plus. Soit i une racine carrée de -1 dans une extension de k. Dans $k(i)$,

on a $x^{2^r} - a = x^{2^r} + b^2 = (x^{2^{r-1}} + ib)(x^{2^{r-1}} - ib)$. Si l'un des facteurs $x^{2^{r-1}} \pm ib$ est réductible sur $k(i)$, alors par hypothèse de récurrence, soit $\pm ib$ est un carré dans $k(i)$, soit est dans $-4k(i)^4$. Dans les deux cas, $\pm ib$ est un carré dans $k(i)$: $\pm ib = (c + di)^2 = c^2 + 2cdi - d^2$, $c, d \in k$. Donc $c^2 = d^2$ ou $c = \pm d$, et $\pm ib = 2cdi = \pm 2c^2 i$. Prenant le carré, on voit que $a = -b^2 = -4c^4$, contradiction. Donc les deux facteurs sont irréductibles. Donc, par factorialité de $k(i)[x]$, $x^{2^r} + b^2$ est irréductible sur k.

2. On suppose maintenant que $n = p^r m$, avec $m \geq 2$ et p premier impair ne divisant pas m, et que le résultat est vrai pour m. Soit $\alpha \notin k$ tel que $\alpha^m = a$. Alors $[k(\alpha) : k] = m$. Si $\alpha = \beta^p$, $\beta \in k(\alpha)$, alors $-a = (-1)^m N(\alpha) = (-1)^m N(\beta)^p$, donc $a = (-1)^{m+1} N(\beta)^p$, ce qui implique que $a \in k^p$ (clair si m impair ; si m pair, $a = -N(\beta)^p = (-N(\beta))^p$), contradiction. Donc $\alpha \notin k(\alpha)^p$. Donc $x^{p^r} - \alpha$ est irréductible dans $k(\alpha)[x]$. Par le lemme, le polynôme $x^n - a$ est irréductible dans $k[a]$. □

Corollaire 3.15. *Etant donné un premier p et un entier $r \geq 1$, pour que $x^{p^r} - a$ soit irréductible dans $k[x]$, il suffit que $a \notin k^{*p}$ et que soit $p = \mathrm{car}(k)$, soit $p \neq 2$.*

Corollaire 3.16. *Si $\bar{k}$ est une extension propre et finie de k, alors k est de caractéristique nulle et $\bar{k} = k(i)$, $i^2 = -1$.*

EXERCICES

Exercice 3.18. *Montrer que si n est un multiple de 4 et que $a \in -4k^4$, alors $x^n - a$ n'est pas irréductible dans $k[x]$. Indications : $x^4 + 4b^4 = (x^2 - 2bx + 2b^2)(x^2 + 2bx + 2b^2)$. Montrer que la réciproque du théorème 3.21 est vraie.*

3.12 Cohomologie de Galois

Définition 3.11. *Soit G un groupe agissant par automorphismes sur un groupe abélien A. L'action est notée $\sigma.a$ ($\sigma \in G, a \in A$) et $a \mapsto \sigma.a$ est donc pour σ fixé un automorphisme de A.*

1. Un 1-cocycle de G dans A *est une famille $(\alpha_\sigma)_{\sigma \in G}$ d'élements de A telle que $\alpha_{\tau\sigma} = \alpha_\sigma + \sigma.\alpha_\tau$ pour tous σ, τ dans G. L'ensemble des 1-cocycles est noté $Z^1(G, A)$.*

2. Un 1-cobord de G dans A *est une famille $(\alpha_\sigma)_{\sigma \in G}$ d'éléments de A telle qu'il existe $\beta \in A$ avec $\alpha_\sigma = \sigma(\beta) - \beta$ pour tout $\sigma \in G$. L'ensemble des 1-cobords est noté $B^1(G, A)$.*

L'ensemble $Z^1(G,A)$ est un groupe sous l'addition, et $B^1(G,A)$ en est un sous-groupe. Le quotient $Z^1(G,A)/B^1(G,A)$ est appelé le *premier groupe de cohomologie*, noté $H^1(G,A)$.

Théorème 3.22. *Soit K une extension de Galois finie de k, de groupe G. Pour l'action naturelle de G sur le groupe multiplicatif K^*, on a $H^1(G,K^*) = 1$. Pour l'action naturelle de G sur le groupe additif K, on a $H^1(G,K) = 0$.*

Démonstration. Soit $(\alpha_\sigma)_{\sigma\in G}$ un 1-cocycle de G dans K^*. La relation ci-dessus s'écrit (multiplicativement) : $\alpha_{\tau\sigma} = \alpha_\sigma \sigma(\alpha_\tau)$. D'après l'indépendance linéaire des caractères (théorème 3.8), il existe $\theta \in K$ tel que $0 \neq \beta = \sum_{\tau\in G} \alpha_\tau \tau(\theta)$. Alors $\sigma(\beta) = \sum_{\tau\in G} \sigma(\alpha_\tau)\sigma\tau(\theta) = \sum_\tau \alpha_{\sigma\tau}\alpha_\sigma^{-1}\sigma\tau(\theta) = \alpha_\sigma^{-1}\sum_\tau \alpha_{\sigma\tau}\sigma\tau(\theta) = \alpha_\sigma^{-1}\beta$. Donc $\alpha_\sigma = \beta/\sigma(\beta) = \sigma(\beta^{-1})/\beta^{-1}$. Donc (α_σ) est un 1-cobord.

Soit maintenant un 1-cocycle (α_σ) de G dans K. Il existe un θ dans K tel que $Tr(\theta) \neq 0$. On pose $\beta = (1/Tr(\theta))\sum_{\tau\in G} \alpha_\tau\tau(\theta)$. On montre alors que $\alpha_\sigma = \beta - \sigma(\beta) = \sigma(-\beta) - (-\beta)$. Donc (α_σ) est un 1-cobord. □

3.13 Indépendance algébrique d'homomorphismes

On suppose dans cette section que K est un corps infini (de cardinalité infinie).

Définition 3.12. *Soit A un groupe commutatif et K un corps. Soient $\lambda_1,\dots,\lambda_n$ des homomorphismes additifs $A \to K$. Ils sont dits* algébriquement dépendants sur K *s'il existe un polynôme $f(x_1,\dots,x_n)$ non nul sur K tel que $\forall a \in A$, $f(\lambda_1(a),\dots,\lambda_n(a)) = 0$.*

Définition 3.13. *Un polynôme $f(x_1,\dots,x_n)$ est dit* additif *s'il induit une fonction additive $K^n \to K$.*

Remarque 3.2. *Soit $f(x_1,\dots,x_n)$ un polynôme sur K et $y_1,\dots,y_n$ des nouvelles variables. Utilisons la notation $X = (x_1,\dots,x_n)$, $Y = (y_1,\dots,y_n)$. Alors le degré total en les x_i de $g(X,Y) = f(X+Y) - f(X) - f(Y)$ est strictement plus petit que celui de f ; de même pour le degré partiel en chaque x_i.*

Théorème 3.23. *(Artin) Soient $\lambda_1,\dots,\lambda_n$ des homomorphismes additifs $A \to K$. S'ils sont algébriquement dépendants sur K, alors il existe un polynôme additif $f(x_1,\dots,x_n)$ non nul sur K tel que $\forall a \in A$, $f(\lambda_1(a),\dots,\lambda_n(a)) = 0$.*

Démonstration. Considérons un polynôme $f(x_1, \ldots, x_n)$ non nul sur K tel que $\forall a \in A$, $f(\lambda_1(a), \ldots, \lambda_n(a)) = 0$, et de degré total minimum. Utilisons la notation $\Lambda(x) = (\lambda_1(x), \ldots, \lambda_n(x))$. Posons $g(X, Y) = f(X+Y) - f(X) - f(Y)$. On a $\forall a, b \in A$, $g(\Lambda(a), \Lambda(b)) = f(\Lambda(a) + \Lambda(b)) - f(\Lambda(a)) - f(\Lambda(b))$. Comme Λ est additif, ceci vaut $f(\Lambda(a+b)) - f(\Lambda(a)) - f(\Lambda(b)) = 0$.

Supposons que g ne soit pas nulle. Supposons aussi que $\forall \xi \in K^n$, $\forall y \in A$, $g(\xi, \Lambda(y)) = 0$. Par hypothèse, il existe ξ' dans K^n tel que $g(\xi', y) \neq 0$. Soit $P(Y) = g(\xi', Y)$. Alors le degré total de P en les y_i est plus petit que le degré total de f en les x_i. Or $\forall a \in A$, $g(\xi', \Lambda(a)) = 0$. On a donc une contradiction avec la minimalité du degré de f.

On peut donc supposer qu'il existe ξ dans K^n et b dans A tel que $g(\xi, \Lambda(b)) \neq 0$. Soit $P(X) = g(X, \Lambda(b))$. Alors P est non nul, son degré total est plus petit que celui de f et $P(\Lambda(a)) = 0$ pour tout $a \in A$. On a aussi une contradiction.

Tout ceci montre que $g = 0$ donc f est additif. □

Proposition 3.3. *Soit $f(X)$ un polynôme additif. Soit $f_i(x_i) = f(0, \ldots, 0, x_i, 0 \ldots, 0)$ (le x_i en i-ème position). Alors $f(X) = \sum_i f_i(x_i)$.*

Démonstration. $f(X) - \sum_i f_i(x_i)$ s'annule pour tous les $X = (a_1, \ldots, a_n)$. On conclut car K est infini. □

Proposition 3.4. *Soit $f(x)$ un polynôme additif d'une variable. Si la caractéristique est nulle, alors f est linéaire. Si la caractéristique est p, alors f est une combinaison K-linéaire de monômes x^{p^ν}.*

Démonstration. Soit ax^r un monôme dans f, avec $a \in K^*$. Soit $g(x, y) = f(x+y) - f(x) - g(y)$. On a $g = 0$. La partie homogène de degré $r > 1$ dans g est $0 = a((x+y)^r - x^r - y^r) = rx^{r-1}y + \ldots$. Donc $r = 0$ dans K. Donc r doit être un multiple de la caractéristique $p \neq 0$: $r = p^m s$, s premier avec p. □

Théorème 3.24. *Soit G un groupe fini d'automorphismes de K. Alors ils sont algébriquement indépendants sur K.*

Démonstration. En caractéristique nulle, on est ramené par le théorème 3.23 à l'indépendance linéaire des caractères, théorème 3.8. Supposons que la caractéristique soit $p > 0$. Supposons que les $\sigma \in G$ soient algébriquement dépendants. Par les théorème 3.23 et propositions 3.3 et 3.4, ceci implique une relation du type : $\forall x \in K$, $\sum_{\sigma \in G, r \geq 0} a_{\sigma,r} \sigma(x)^{p^r} = 0$ avec des $a_{\sigma,r}$ dans K.

La fonction $x \mapsto \sigma(x)^{p^r}$ est un automorphisme de K. Par l'indépendance linéaire des caractères (théorème 3.8), il s'ensuit qu'il existe $\sigma, \tau \in G$ et $r, s \in \mathbb{N}$ tels que $\sigma^r = \tau^s$ et soit $\sigma \neq \tau$, soit $r \neq s$. On peut supposer $r \leq s$. Pour tout $x \in K$, on a $\sigma(x)^{p^r} = \tau(x)^{p^s} = (\tau(x)^{p^{s-r}})^{p^r}$. Comme la fonction $y \mapsto y^{p^r}$ est injective dans K, on a pour tout $x \in K$, $\sigma(x) = \tau(x)^{p^{s-r}} = \tau(x^{p^{s-r}})$. Posons $\phi = \tau^{-1}\sigma$. Alors $\phi(x) = x^{p^{s-r}}$. Or $\phi^n = 1$ pour un certain n. Donc $x = x^{p^{n(s-r)}}$ pour tout x dans K. Comme K est infini, il faut que $s = r$ et finalement $\phi = 1$, d'où $\sigma = \tau$, ce qui n'est pas. □

3.14 Le théorème de la base normale

Théorème 3.25. *Soit K une extension de Galois finie de k et G son groupe. Il existe $w \in K$ tel que les $\sigma(w)$, $\sigma \in G$, forment une k-base de K.*

Remarque 3.3. *De manière équivalente, la représentation k-linéaire de G, agissant sur K, est la représentation régulière.*

Démonstration. 1. On suppose que K est infini. Pour $\sigma \in G$, soit x_σ une indéterminé. On considère le polynôme $f(x_\sigma, \sigma \in G)$ égal au déterminant de la matrice $(x_{\alpha^{-1}\beta})_{\alpha,\beta \in G}$, dont les lignes et les colonnes sont indexées par G. Ce polynôme n'est pas nul, car la matrice se spécialise en la matrice unité si on remplace x_{id} par 1 et les autres x_σ par 0. D'après le théorème 3.24, il existe $w \in K$ tel que $f(\sigma(w), \sigma \in G)$ n'est pas nul.

Montrons que les $\beta(w), \beta \in G$ forment une base de K sur k. Supposons qu'il existe une k-combinaison linéaire non triviale, mais nulle, des $\beta(w)$: $\sum_\beta a_\beta \beta(w) = 0$. Donc pour tout $\alpha \in G$, on a $\sum_\beta a_\beta \alpha^{-1}\beta(w) = 0$. Ce qui contredit la non nullité du déterminant, car les colonnes de la matrice seraient k-linéairement dépendantes.

2. On suppose que K est fini. Soit $q = |k|$ et $n = [K : k]$. On sait que G est cyclique, engendré par l'automorphisme $\sigma : \alpha \mapsto \alpha^q$. Donc G est l'ensemble des n automorphismes σ^i, $i = 0, \ldots, n-1$. Ils sont linéairement indépendants sur k (théorème 3.8). Donc le polynôme minimal de σ est de degré n. On utilise alors l'exercice 3.19. □

EXERCICES

Exercice 3.19. *Montrer que si V est un espace vectoriel de dimension finie n sur k et si le polynôme minimal de $f \in End_k(V)$ est de degré n (i.e il est égal à son polynôme caractéristique), alors il existe $w \in V$ qui engendre V sous l'action de f. Indication : utiliser la théorie de diviseurs principaux de f. Ou alors, plus artisanalement, se ramener au cas où le polynôme est une puissance d'un polynôme irréductible.*

3.15 Correspondance de Galois pour les extensions infinies

Voir [1] 3.12.

4 Applications

Dieu me pardonne, dit Bussy, je crois qu'il parle tout seul. Allons, ce n'est ni un ivrogne ni un fou : c'est un mathématicien qui cherche la solution d'un problème.

Alexandre Dumas
La dame de Monsoreau

4.1 Théorème de Lüroth

Théorème 4.1. *Tout sous-corps de $k(x)$, contenant k comme sous-corps propre, est isomorphe à $k(x)$.*

Si $u = f(x)/g(x) \in k(x)$, $u \notin k$, $f, g \in k[x]$ premiers entre eux, alors on appelle *degré de u* le nombre $deg(u) := max(deg(f), deg(g))$.

Proposition 4.1. *Si $u \in k(x)$, $u \notin k$, alors x est algébrique sur $k(u)$ de degré $deg(u)$.*

Démonstration. L'élément x est racine du polynôme $f(t) - ug(t) \in k(u)[t]$, de degré $deg(u)$ en t ; ce polynôme est non nul, car u n'est pas dans k ; donc x est algébrique sur $k(u)$ de degré au plus $deg(u)$.

Notons que $k(x,t)$ est de degré de transcendance 2 sur k, donc $k(u,t)$ aussi. Donc u, t sont algébriquement indépendants. Si le polynôme précédent n'est pas irréductible dans $k(u)[t]$, on peut le factoriser dans $k(u)[t]$, et par le lemme de Gauss, aussi dans $k[u,t]$. Comme il est linéaire en u, ceci n'est possible que si f, g ne sont pas premiers entre eux. Donc le polynôme est irréductible et comme son degré en t est égal à $max(deg(f), deg(g))$, le résultat s'en déduit. □

Corollaire 4.1. *les conditions suivantes sont équivalentes, pour $u \in k(x)$:*

1. *u est de degré 1.*
2. *$u = \frac{ax+b}{cx+d}$, avec $a, b, c, d \in k$ et $ad - bc \neq 0$.*
3. *$x \mapsto u$ induit un automorphisme de $k(x)$.*

Démonstration du théorème 4.1. Soit F un sous-corps de $k(x)$, contenant k strictement. Il existe $u \in F \setminus k$. Alors x est algébrique sur $k(u)$. Donc x est algébrique sur F. Soit $\phi(t) = t^n + u_1(x)t^{n-1} + \cdots + u_n(x)$ le polynôme minimal de x sur F. En multipliant les fractions rationelles u_i par leur plus petit dénominateur commun, nous obtenons un polynôme $\Phi(t,x) = v_0(x)t^n + v_1t^{n-1} + \ldots + v_n(x) \in k[t,x]$ tel que les polynômes $v_i(x)$ dans $k[x]$ n'ont pas de diviseur commun et que $v_0 \neq 0$. Donc Φ, vu comme élément de $k[x][t]$, est un polynôme primitif. Les u_i ne sont pas tous constants et il existe j tel que $u_j \notin k$. D'après la proposition, le degré de x sur $k(u_j)$ est $m = deg(u_j)$, tandis que son degré sur F est n. Donc $m = [k(x) : k(u_j)] = [k(x) : F][F : k(u_j)] = n[F : k(u_j)]$, et pour prouver le théorème il suffit de prouver que $m = n$, car alors $F = k(u_j)$.

Ecrivons $u_j = a(x)/b(x)$ avec des polynômes a, b dans $k(x)$ premiers entre eux. Le degré en x de Φ est $\geq deg(a), deg(b)$. On peut supposer que le coefficient dominant de b est 1 et la proposition implique que $m = max(deg(a), deg(b))$. Le polynôme $a(t) - u_jb(t)$ dans $F[t]$ a la racine x, donc il est divisible par $\phi(t)$ dans $F[t]$: $a(t) - u_j(x)v(t) = q(t)\phi(t)$, $q(t) \in F[t]$. Remplaçons u_j par a/b et multiplions par $b(x)$: $(*)$ $a(t)b(x) - a(x)b(t) = Q(x,t)\Phi(x,t)$ où Q est un polynôme en x. Comme ϕ et $a(t)b(x) - a(x)b(t)$ sont dans $k[x][t]$ et que le premier est primitif, on déduit du lemme de Gauss que $Q \in k[x][t]$. Le polynôme $a(t)b(x) - a(x)b(t)$ a degré m en x, et Φ a degré au moins m en x. Donc Q est indépendant de x. Supposons que Q dépend de t. Il a alors une racine α dans une extension de k. Donc $a(\alpha)b(x) - a(x)b(\alpha) = 0$. Si $b(\alpha) = 0$, alors $a(\alpha) = 0$, ce qui implique que a, b ne sont pas premiers entre eux. Donc $b(\alpha) \neq 0$. Donc $u_j(x) = a(x)/b(x) = a(\alpha)/b(\alpha)$ et donc $u_j(x)$ est algébrique sur k, et x aussi, une contradiction. Ceci montre Q est indépendant de t. Donc $m = n$ en comparant les degrés en t de l'équation $(*)$. □

5 Appendice : lemme de Zorn

5.1 Notions sur les ensembles ordonnés

Définition 5.1. *Soit X un ensemble muni d'un ordre $\leq$.*

- Deux éléments x, y de X sont dits comparables *si $x \leq y$ ou $y \leq x$.*

- Un sous-ensemble Y de X est dit majoré *s'il existe $x \in X$ tel que $\forall y \in Y, y \leq x$.*

- Une chaine *dans X est une partie de X qui est totalement ordonnée par l'ordre induit.*

- *Un élément* maximal *dans X est un élément x tel que pour tout $y \in X$, si $x \leq y$, alors $y = x$.*

Exercice 5.1. *Dans l'ensemble des parties X d'un ensemble à n éléments, ordonné par inclusion, quelle est la cardinalité maximum des chaines ?*

Exercice 5.2. *Soit X l'ensemble des parties $\neq E$ d'un ensemble E, ordonné par inclusion ; quels sont les éléments maximaux de X ? Même question pour l'ensemble des sous-espaces vectoriels propres d'un espace vectoriel V, l'ordre étant l'inclusion ; on peut commencer par le cas où la dimension de V est finie.*

5.2 Ensembles inductifs et lemme de Zorn

Définition 5.2. *Un ensemble ordonné est dit* inductif *si toute chaine y est majorée.*

Théorème 5.1. *(Lemme de Zorn) Tout ensemble ordonné inductif non vide possède un élément maximal.*

Le lemme de Zorn se déduit de l'axiome du choix en utilisant la théorie des ordinaux. Nous ne ferons pas ici cette démonstration.

5.3 Application : existence d'un idéal maximal

Un idéal bilatère *maximal* d'un anneau *commutatif unitaire* est un idéal propre qui n'est contenu strictement dans aucun idéal propre.

Théorème 5.2. *Tout idéal propre d'un anneau est contenu dans un idéal maximal.*

Démonstration. Soit A cet anneau, et I un déal propre de A. On considère l'ensemble des idéaux propres de A, qui contiennent I, et on ordonne cet ensemble par inclusion. C'est un ensemble inductif : toute chaine est majorée par la réunion de ses éléments ; cette réunion, notée J, est en effet un idéal ; J est propre, car sinon 1 est dans J, donc dans un des élément de la chaine, lequel ne serait pas propre. De plus, J contient I. □

6 Solutionnaire (esquisses)

J'ai connu un agrégé en mathématiques, qui, répugnant au service de l'artillerie, décida de voler la montre d'un Oberleutenant pour pouvoir se caser dans la prison de la place. Il avait agi ainsi après mûre réflexion. La guerre ne lui disait rien. Expédier les obus et tuer des agrégés en mathématiques de l'autre côté du front, il considérait cela comme parfaitement idiot.

Jaroslav Hasek
Le brave soldat Chvéïk

Exercice 2.1 Si x est l'inverse de y, alors $f(x)f(y) = f(xy) = f(1) = 1$ donc $f(x)$ est l'inverse de $f(y)$. Si x est dans le noyau de f, alors x ne peut pas être inversible : sinon, soit y son inverse ; alors $f(y)$ est l'inverse de 0, contradiction. Donc f est injectif dans le cas où K est un corps.

Exercice 2.2 Si $\mathbb{R}$ était de dimension finie n sur $\mathbb{Q}$, alors comme espaces vectoriels sur $\mathbb{Q}$, on aurait isomorphisme entre $\mathbb{Q}^n$ est $\mathbb{R}$. Alors $\mathbb{R}$ serait dénombrable, contradiction.

Exercice 2.3 Soit K cette intersection et L le plus petit sous-corps de k qui contient E. Comme L contient E et que K est l'intersection des sous-corps qui contiennent E, on a $K \subset L$. Réciproquement, K contient E, et comme L est le plus petit sous-corps qui contient E, on a $L \subset K$.

Exercice 2.4 Soit K le corps obtenu en adjoignant à $\mathbb{Q}$ tous les $\sqrt{m}$ où m est sans carré ($m = 2, 3, 5, 6, 7, 10, 11, 13, \ldots$). Si n est divisible par un carré, on peut écire $n = d^2m$, m sans carré ; alors $\sqrt{n} = d\sqrt{m}$ et donc $n \in K$.

Exercice 2.5 Si $\sqrt{n}$ est dans K, alors cet ensemble est K, et on peut donc exclure ce cas. Pour montrer que cet ensemble est un corps, il suffit de montrer qu'il est fermé par somme et produit (c'est routinier) et par inversion. Soit donc $a + b\sqrt{n} \neq 0$. On a $(a + b\sqrt{n})(a - b\sqrt{n}) = a^2 - b^2n \neq 0$, car n n'est pas un carré dans K. Donc $\frac{a-b\sqrt{n}}{a^2-b^2n}$ est l'inverse de $a + b\sqrt{n}$.

L'ensemble considéré étant un corps contenant K et $\sqrt{n}$, il contient $K(\sqrt{n})$ et il est bien sûr aussi contenu dans lui. Ils sont égaux. La dimension de $K(\sqrt{n})$ sur K est 2, car on a comme base 1 et $\sqrt{n}$.

Exercice 2.6 On a $(a + b\frac{-1+i\sqrt{3}}{2})(a + b\frac{-1-i\sqrt{3}}{2}) = (\frac{2a-b}{2} + \frac{bi\sqrt{3}}{2})(\frac{2a-b}{2} - \frac{bi\sqrt{3}}{2}) = \frac{1}{4}(4a^2 + b^2 - 4ab + 3b^2 = a^2 - ab + b^2$. Cette *forme quadratique* en a, b n'est nulle que pour $a = b = 0$. Donc tout élément non nul du deuxième ensemble a un inverse.

Exercice 2.7 Pour l'équation, élever au carré, utiliser l'irrationalité de $\sqrt{2}$ et le fait que $3/2$ n'est pas un carré dans $\mathbb{Q}$ (pourquoi ?).

Exercice 2.20 On prend le corps $k[x]/(\varphi)$, où φ est un diviseur irréductible du polynôme donné.

Exercice 2.24 Non, car les polynômes minimaux de ces deux nombres sont différents ; ils sont de degré 2 et faciles à calculer.

Exercice 2.33 C'est le corps obtenu en adjoignant à $\mathbb{Q}$ toutes les racines de tous les polynômes $x^2 - n$, $n \in \mathbb{N}$.

Exercice 2.34 (1) implique (2) : comme c'est une extension normale et que f y a la racine α, toutes les racines de f y sont (définition 2.9). (2) implique (3) : toutes les racines de f sont dans $k(\alpha)$, donc elles sont de la forme $g(\alpha)$ pour un certain polynôme g sur k (proposition 2.5). (3) implique (1) : $k(\alpha)$ est le corps de décomposition de $f(x)$.

Exemples : α de degré 2 sur k. Une extension simple de $\mathbb{Q}$ par une racine de l'unité $\exp(2i\pi/n)$, car les autres racines n-èmes de l'unité sont des puissances de celle-ci, et c'est donc le corps de décomposition de $x^n - 1$.

Exercice 2.35 Soit M' une extension normale de K contenue dans L. Soir $a \in M'$, et soit P son polynôme minimal sur K. Toutes les racines de P sont dans M' (définition 2.9), donc dans L, et $p \in S$; donc les racines de P sont dans M, et en particulier $a \in M$.

Références

[1] J. R. Bastida, Field extensions and Galois theory, Addison Wesley, 1984. 55

[2] S. Lang, Algebra. 2

[3] I. Macdonald, Symmetric functions and Hall polynomials, Oxford University Press, 1979. 37

[4] B.L. van der Waerden, Moderne Algebra.

2