Par ***Vincent Dumoncel***
Septembre 2021

Théorie de Galois

Le but de ce document est de fournir une introduction presque exhaustive à la théorie de Galois. Son contenu repose sur de multiples sources, la principale étant le cours de *Théorie de Galois* dispensé à l'EPFL par Thomas Gerber au semestre d'automne 2020.
Le chapitre 1 porte des rappels sur les anneaux de polynômes et sur plusieurs critères d'irréductibilité. Une étude précise des irréductibles à coefficients dans un corps fini est présentée. Les chapitres 2 et 3 introduisent eux la notion centrale d'extensions de corps, et les principales propriétés qu'elles peuvent avoir : algébricité, normalité et séparabilité. Le chapitre 4 est le coeur de ce cours : on introduit le groupe de Galois d'un polynôme et on démontre le théorème de correspondance galoisienne. Le chapitre 5 traite lui de plusieurs applications de la théorie, la principale étant la résolubilité des équations polynomiales par radicaux.
Les résultats et définitions sont illustrés avec de nombreux exemples et remarques, et une liste d'exercices figure à la fin de chaque chapitre. Bonne lecture !

1811 – 1832

1 Racines et polynômes irréductibles

1.1 Tests de racines

Soit K un corps.
Il est facile d'établir que si $a \in K$ est racine d'un polynôme $f \in K[X]$, alors $X - a$ divise f, et donc f n'est pas irréductible. Ainsi, pour discuter de l'éventuelle irréductibilité d'un polynôme f, une première approche est de chercher ses racines.

Proposition 1.1 Soit $f \in K[X]$, de degré supérieur ou égal à 2.
(i) Si f est irréductible dans $K[X]$, alors f n'a pas de racines dans K.
(ii) Supposons que f est de degré 2 ou 3. Alors f est irréductible dans $K[X]$ si, et seulement si, f n'a pas de racines dans K.

Preuve. (i) Comme discuté ci-dessus, si $a \in K$ est une racine de f, $X - a$ divise f, qui n'est donc pas irréductible.
(ii) L'implication $\Longrightarrow$ est le point (i). Pour voir $\Longleftarrow$, raisonnons par l'absurde, et supposons qu'il existe $g, h \in K[X] \setminus K$ tels que $f(X) = g(X)h(X)$. Alors $\deg(f) = \deg(gh) = \deg(g)+\deg(h)$ et comme f est de degré 2 ou 3, on a nécessairement $\deg(g) = 1$ ou $\deg(h) = 1$. Disons, sans perte de généralité, que $\deg(g) = 1$. On peut alors écrire $g(X) = aX + b$, avec $a \in K^*$, $b \in K$. On voit ainsi que $a^{-1}b \in K$ est une racine de g, donc de f, ce qui est exclu par hypothèse. Donc, si on a une décomposition $f(X) = g(X)h(X)$, alors $g \in K^*$ ou $h \in K^*$, et donc f est irréductible. □

Exemples. (i) $f(X) = X^3 + X^2 + X + 1$ n'est pas irréductible dans $\mathbb{Q}[X]$, puisque $f(-1) = 0$.
(ii) $f(X) = X^2 + X + 1$ est irréductible dans $\mathbb{F}_2[X]$, puisque $f(0) = f(1) = 1 \neq 0$ et que f est de degré 2.

Dans le point (ii) de la proposition 1.1, le fait que K soit un corps et que f soit de degré 2 ou 3 sont deux hypothèses essentielles. Par exemple, $f(X) = 3(X^2 + 1) \in \mathbb{Z}[X]$ n'a pas de racines dans $\mathbb{Z}$, et pourtant f n'est pas irréductible. De même, $f(X) = X^4 + 1 \in \mathbb{R}[X]$ n'a pas de racines dans $\mathbb{R}$, et pourtant f n'est pas irréductible puisque $f(X) = (X^2 - \sqrt{2}X + 1)(X^2 + \sqrt{2}X + 1)$.

On a donc besoin d'outils pour trouver facilement les racines d'un polynôme.

Proposition 1.2 Soit $f(X) = a_nX^n + \cdots + a_1X + a_0 \in \mathbb{Z}[X]$.
Si $r = \frac{p}{q} \in \mathbb{Q}$ est une racine de f, alors p divise a_0 et q divise a_n.

Preuve. On a

$$0 = f(r) = a_n\left(\frac{p}{q}\right)^n + \cdots + a_1\frac{p}{q} + a_0 \Longrightarrow 0 = q^n f(r) = a_np^n + a_{n-1}qp^{n-1} + \cdots + a_1q^{n-1}p + a_0q^n$$
$$\Longrightarrow -a_0q^n = a_np^n + a_{n-1}qp^{n-1} + \cdots + a_1q^{n-1}p$$

Or p divise $a_np^n + a_{n-1}qp^{n-1} + \cdots + a_1q^{n-1}p$, donc p divise a_0q^n, et comme p et q sont premiers entre eux, p divise a_0. Un argument analogue montre que q divise a_n. □

Exemple. Le polynôme $f(X) = X^3 + 3X^2 - 7X + 2$ n'a pas de racines dans $\mathbb{Q}$, puisque une éventuelle racine est un diviseur de 2. Or on vérifie facilement que $f(-1)$, $f(1)$, $f(-2)$, $f(2) \neq 0$. Comme f est de degré 3, il est irréductible dans $\mathbb{Q}[X]$.

1.2 Lemmes de Gauss, critère d'Eisenstein

Soit A un anneau intègre.

Définition 1.3 Un polynôme $f \in A[X]$ est *primitif* si tous ses coefficients sont premiers entre eux.

Par exemple, $f(X) = 3X^2 + 3X - 12 \in \mathbb{Z}[X]$ n'est pas primitif, puisque 3 divise tous les coefficients de f. En revanche, $g(X) = X^3 - 5$ est primitif.

Lemme 1.4 (1er lemme de Gauss) Si $f, g \in \mathbb{Z}[X]$ sont primitifs, alors $fg \in \mathbb{Z}[X]$ est primitif.

Preuve. Soient donc $f, g \in \mathbb{Z}[X]$ primitifs. Pour voir que fg est aussi primitif, il suffit de montrer qu'aucun premier $p \in \mathbb{Z}$ ne divise simultanément tous les coefficients de fg. Supposons par l'absurde qu'un tel premier p existe. Soit $\pi\colon \mathbb{Z} \longrightarrow \mathbb{Z}/p\mathbb{Z}$ le morphisme de réduction modulo p, et soit $\overline{\pi}\colon \mathbb{Z}[X] \longrightarrow \mathbb{Z}/p\mathbb{Z}[X]$ le morphisme naturel d'anneaux induit par π. Comme f est primitif, p ne divise pas tous les coefficients de f, donc $\overline{\pi}(f) \neq 0$. De même, $\overline{\pi}(g) \neq 0$. Comme $\overline{\pi}$ est un morphisme et que $\mathbb{Z}/p\mathbb{Z}[X]$ est intègre, $\overline{\pi}(fg) = \overline{\pi}(f)\overline{\pi}(g) \neq 0$. D'autre part, p divise tous les coefficients de fg, donc $\overline{\pi}(fg) = 0$, ce qui est absurde. On conclut qu'un tel premier p ne peut pas exister, et donc que fg est primitif. □

Lemme 1.5 (2ème lemme de Gauss) Soit $f \in \mathbb{Z}[X] \setminus \mathbb{Z}$ irréductible. Alors f est irréductible dans $\mathbb{Q}[X]$.

Ces deux premiers résultats permettent alors d'établir un premier critère important pour décider de l'irréductibilité de certains polynômes.

Proposition 1.6 (Critère d'Eisenstein) Soit $f = a_n X^n + \cdots + a_1 X + a_0 \in \mathbb{Z}[X]$, $n \geq 1$.
Supposons qu'il existe un nombre premier $p \in \mathbb{Z}$ tel que
(i) p ne divise pas a_n
(ii) p divise $a_0, \ldots, a_{n-1}$.
(iii) p^2 ne divise pas a_0.
Alors f est irréductible dans $\mathbb{Q}[X]$.

Preuve. D'abord, quitte à diviser tous les coefficients de f, on peut le supposer primitif et, par le 2ème lemme de Gauss, il suffit de montrer que f est irréductible dans $\mathbb{Z}[X]$. Supposons donc, pour obtenir une contradiction, que

$$f(X) = g(X)h(X)$$

avec $g(X)$, $h(X) \in \mathbb{Z}[X]$ et $1 \leq \deg(g)$, $\deg(h) < \deg(f)$. En écrivant explicitement $g(X) = g_d X^d + \cdots + g_0$ et $h(X) = h_m X^m + \cdots + h_0$, on a $a_0 = g_0 h_0$. Comme $p \mid a_0$ est premier, $p \mid g_0$ ou $p \mid h_0$ et comme $p^2 \nmid a_0$, p ne peut pas diviser simultanément g_0 et h_0. Disons, sans restreindre la généralité, que $p \nmid g_0$ et $p \mid h_0$. Ensuite, vu que $p \nmid a_n = g_d h_m$, $p \nmid h_m$. Définissons donc $r := \min\{j \in \{0, \ldots, m\} \mid p \nmid h_j\}$. On obtient alors les inégalités $0 < r \leq m < n$. D'autre part, on a

$$a_r = g_0 h_r + g_1 h_{r-1} + \cdots + g_r h_0$$

où p divise $h_0, \ldots, h_{r-1}$ par définition de r et où p divise a_r par hypothèse. Il suit que p divise la différence $a_r - g_1 h_{r-1} - \cdots - g_r h_0 = g_0 h_r$. Comme p est premier, p divise g_0 ou p divise h_r, ce qui est une contradiction par ce qui précède. On conclut donc que de tels polynômes $g(X)$, $h(X) \in \mathbb{Z}[X]$ n'existent pas, et ainsi f est irréductible. □

Exemples. (i) Le polynôme $f(X) = X^3 - 2$ est irréductible, par le critère d'Eisenstein avec $p = 2$.
(ii) Plus généralement, le polynôme $X^n - p$ est irréductible pour tout $n \geq 1$ et tout premier $p \in \mathbb{Z}$.
(iii) Là encore, $f(X) = X^5 + 3X^3 + 15X^2 - 6$ est irréductible, par Eisenstein avec le premier $p = 3$.
(iv) On ne peut pas utiliser le critère d'Eisenstein avec $p = 2$ pour décider de l'irréductibilité de $X^4 + 8$, puisque $2^2 = 4$ divise aussi 8.

1.3 Critère de réduction modulo p

Lorsqu'il n'est pas possible d'utiliser Eisenstein, un autre critère de réduction modulo p est disponible.

Proposition 1.7 Soit $f(X) = a_n X^n + \cdots + a_1 X + a_0 \in \mathbb{Z}[X]$ primitif.
S'il existe $p \in \mathbb{Z}$ un premier tel que p ne divise pas a_n et tel que $\overline{f}$, la réduction modulo p de f, est irréductible dans $\mathbb{Z}/p\mathbb{Z}[X]$, alors f est irréductible dans $\mathbb{Q}[X]$.

Preuve. Par le lemme 1.5, il est suffisant de montrer que f est irréductible dans $\mathbb{Z}[X]$. On montre en fait la contraposée : supposons que $f(X) \in \mathbb{Z}[X]$ est primitif et non irréductible. Il existe donc $g(X)$, $h(X) \in \mathbb{Z}[X]$ tels que $f(X) = g(X)h(X)$ et $g(X)$, $h(X) \notin (\mathbb{Z}[X])^* = \mathbb{Z}^* = \{-1, 1\}$. De plus, comme f est primitif, g et h ne peuvent pas être constants. Donc

$1 \leq \deg(g), \deg(h) < \deg(f)$. On considère alors $\overline{\pi}\colon \mathbb{Z}[X] \longrightarrow \mathbb{Z}/p\mathbb{Z}[X]$ le morphisme de réduction modulo p, induit par la projection $\pi\colon \mathbb{Z} \longrightarrow \mathbb{Z}/p\mathbb{Z}$. Alors

$$\overline{f} = \overline{\pi}(f) = \overline{\pi}(gh) = \overline{\pi}(g)\overline{\pi}(h).$$

En écrivant $g(X) = g_d X^d + \cdots + g_0$ et $h(X) = h_m X^m + \cdots + h_0$, on a $a_n = g_d h_m$ et comme $p \nmid a_n$, $p \nmid g_d$ et $p \nmid h_m$. Donc après réduction, $\overline{\pi}(g)$ et $\overline{\pi}(h)$ sont aussi de degré au moins 1. Comme les inversibles de $\mathbb{Z}/p\mathbb{Z}[X]$ ont degré 0, on en déduit que $\overline{\pi}(g), \overline{\pi}(h) \notin (\mathbb{Z}/p\mathbb{Z}[X])^*$, ce qui montre que $\overline{f}$ n'est pas irréductible, et conclut la preuve. □

Exemple. Le polynôme $f(X) = 3X^2 + 7X + 1$ est irréductible dans $\mathbb{Q}[X]$, puisque sa réduction modulo 2, $\overline{f}(X) = X^2 + X + 1$ est irréductible dans $\mathbb{F}_2[X]$.

1.4 Polynômes à coefficients dans d'autres anneaux

Les anneaux $\mathbb{Z}$ et $K[X]$, où K est un corps, ont beaucoup de propriétés en commun. Il est alors naturel de considérer $K[X,Y] = K[X][Y] = K[Y][X]$ comme un analogue de $\mathbb{Z}[X]$. Ainsi, nos tests d'irréductibilité, en particulier le critère d'Eisenstein et la réduction modulo p, peuvent être formulés pour $K[X,Y]$, en voyant un élément de $K[X,Y]$ comme un polynôme en une variable dont les coefficients sont des polynômes en l'autre variable.

Proposition 1.8
(i) (Eisenstein) Si $f(X,Y) \in K[X,Y]$ est unitaire en X et, lorsque qu'écrit $f(X,Y) = X^n + a_{n-1}(Y)X^{n-1} + \cdots + a_1(Y)X + a_0(Y)$ dans $K[Y][X]$, il existe un polynôme irréductible $\pi(Y) \in K[Y]$ tel que $\pi(Y) \mid a_i(Y)$ pour tout $i = 0, \ldots, n-1$ et $\pi(Y)^2 \nmid a_0(Y)$, alors $f(X,Y)$ est irréductible dans $K[X,Y]$.
(ii) (Réduction mod $\pi(Y)$) Si $f(X,Y) \in K[X,Y]$ est unitaire en X et s'il existe un polynôme irréductible $\pi(Y) \in K[Y]$ tel que $\overline{f}(X,Y) \in (K[Y]/(\pi(Y)))[X]$ est irréductible, alors $f(X,Y)$ est irréductible dans $K[X,Y]$.

Exemples. (i) Le polynôme $X^n + (Y+5)X + (Y-1) \in \mathbb{Q}[X,Y]$ est irréductible, puisque quand on le réduit modulo $\pi(Y) = Y+1$, qui est bien un irréductible de $\mathbb{Q}[Y]$, il devient $X^n + 4X - 2$, qui est un irréductible de $(\mathbb{Q}[Y]/(Y+1))[X] \simeq \mathbb{Q}[X]$ par le critère d'Eisenstein avec $p = 2$.
(ii) De même, $X^n - Y$ est irréductible dans $\mathbb{C}[X,Y]$, par le critère d'Eisenstein avec $\pi(Y) = Y$.

1.5 Quotients d'anneaux de polynômes, construction de racines

Si un polynôme $f \in K[X]$ est irréductible, il n'a pas de racines dans K. Le but de cette section est alors de construire explicitement un corps dans lequel f a une, ou des, racine(s).
Il est souhaitable de voir les deux sous-sections suivantes comme des préparatifs à l'introduction des notions de corps de rupture et de corps de décomposition, qui seront discutées aux chapitre 3.
Pour cela, on a besoin de quelques résultats élémentaires d'algèbre. Leurs preuves sont faciles, et sont donc laissées en exercice.

Proposition 1.9 Soit K un corps.
(i) L'anneau $K[X]$ est euclidien, en particulier principal et factoriel.
(ii) Dans $K[X]$, l'idéal $(f(X))$ engendré par f est maximal si, et seulement si, f est irréductible.
(iii) Soient A un anneau commutatif et I un idéal. Le quotient A/I est un corps si, et seulement si, I est maximal.
(iv) Le quotient $K[X]/(f(X))$ est un corps si, et seulement si, f est irréductible dans $K[X]$.

1.5.1 Racines dans un corps plus grand

Théorème 1.10 Soit K un corps, et $f(X) \in K[X] \setminus K$.
Il existe un corps F dans lequel f a une racine α. De plus, F contient K comme sous-corps.

Preuve. Comme $K[X]$ est factoriel, tout polynôme f est produit d'irréductibles, et il suffit donc de montrer le résultat dans le cas où $f(X) = \pi(X)$ est irréductible. Posons $F := K[X]/(\pi(X))$, qui est un corps par la proposition 1.5.

L'élément $\alpha := \overline{X} \in F$, la classe d'équivalence représentée par le polynôme X, est une racine de f, puisque

$$f \in (f(X)) \Longrightarrow \overline{f(X)} = 0 \Longleftrightarrow f(\overline{X}) = 0$$

où la dernière équivalence résulte des définitions des lois de compositions dans un anneau quotient. Pour la deuxième assertion, il suffit d'observer que les classes d'équivalence représentées par les polynômes constants forment un sous-corps isomorphe à K. □

Exemple. Soit $f(X) = X^2 + 1 \in \mathbb{R}[X]$. Alors f est irréductible dans $\mathbb{R}[X]$, et n'a donc pas de racines dans $\mathbb{R}$. Le corps $\mathbb{R}[X]/(X^2+1)$ contient une racine α de f, à savoir $\overline{X}$, et on a la relation $\overline{X}^2 = -1$. En fait, $\mathbb{R}[X]/(X^2+1)$ est une version algébrique des nombres complexes $\mathbb{C}$: les classes d'équivalences de ce quotient ont toutes un représentant de la forme $a\overline{X} + b$, avec $\overline{X}^2 = -1$.

En répétant la construction du théorème 1.10, on peut constuire, à partir de K, un corps qui contient toutes les racines de f.

Corollaire 1.11 Soit K un corps, et $f(X) = c_n X^n + \cdots + c_1 X + c_0 \in K[X]$, de degré $n \geq 1$.
Il existe un corps L, contenant K comme sous-corps, tel que $f(X) = c_n(X - \alpha_1)\dots(X - \alpha_n)$ dans $L[X]$.

Preuve. On raisonne par récurrence sur $n \geq 1$. Si $n = 1$, $f(X) = c_1 X + c_0$ a une racine dans K, donc on pose $L = K$ et $f(X) = c_1(X - (-c_1^{-1}c_0))$. Soit $n \geq 1$ et $f(X) \in K[X]$. Par le théorème 1.10, il existe un corps F dans lequel f a une racine, disons α_1. Il existe alors un polynôme $g(X) \in F[X]$ tel que $f(X) = (X - \alpha_1)g(X)$. Maintenant g a aussi c_n pour coefficient dominant et $\deg(g) = n - 1 < \deg(f)$. Par hypothèse de récurrence, il existe un corps L contenant F, et donc contenant K aussi, tel que $g(X) = c_n(X - \alpha_2)\dots(X - \alpha_n)$ dans $L[X]$. On a alors, dans $L[X]$, $f(X) = c_n(X - \alpha_1)\dots(X - \alpha_n)$, et la preuve est terminée. □

Dans l'exemple ci-dessus, le corps $\mathbb{R}[X]/(X^2+1)$ contient aussi la deuxième racine de X^2+1, à savoir $-\overline{X}$. Ce n'est pas toujours le cas : par exemple $\mathbb{Q}[X]/(X^3 - 2)$ contient une racine de $X^3 - 2$, mais pas les autres. Lorsque cela arrive, il est nécessaire d'itérer la construction du théorème 1.10 pour obtenir un corps plus grand qui contient toutes les racines.

Néanmoins, la situation pour $\mathbb{F}_p[X]$ est plus simple : nous verrons ci-dessous qu'un corps qui contient une racine d'un irréductible de $\mathbb{F}_p[X]$ doit contenir toutes les autres racines. Voilà deux exemples.

Exemples. (i) Le polynôme $X^3 - 2$ est irréductible dans $\mathbb{F}_7[X]$. Il a une racine dans $F = \mathbb{F}_7[X]/(X^3 - 2)$, qui est $\alpha = \overline{X}$. Ses deux autres racines dans F sont 2α et 4α.
(ii) $X^3 + X^2 + 1$ est irréductible dans $\mathbb{F}_5[X]$, et a une racine α dans $F = \mathbb{F}_5[X]/(X^3 + X^2 + 1)$. Ses autres racines sont $2\alpha^2 + 3\alpha$ et $3\alpha^2 + \alpha + 4$.

A partir de maintenant, notre but est de comprendre les irréductibles de $\mathbb{F}_p[X]$, de les compter et de trouver leurs racines.

1.5.2 La puissance p en caractéristique p

L'opération la plus importante en caractéristique p est l'élévation à la puissance p, autrement dit l'application $x \longmapsto x^p$, parce qu'elle est multiplicative et additive.

Lemme 1.12 Soit A un anneau intègre de caractéristique $p > 0$.
(i) Pour tous a, $b \in A$, $(a + b)^p = a^p + b^p$.
(ii) Si $a^p = b^p$, alors $a = b$.

Preuve. (i) Par le théorème binomial, on a

$$(a + b)^p = a^p + \sum_{k=1}^{p-1} \binom{p}{k} a^k b^{p-k} + b^p$$

et comme p divise $\binom{p}{k}$ pour tout $k = 1, \dots, n-1$, tous les termes intermédiaires s'annulent et $(a + b)^p = a^p + b^p$.
(ii) Par hypothèse, on a $0 = a^p - b^p = (a - b)^p$ et comme A est intègre, on a directement $a - b = 0$, donc $a = b$. □

Lemme 1.13 Soit F un corps qui contient $\mathbb{F}_p$. Soit $c \in F$.
Alors $c \in \mathbb{F}_p$ si, et seulement si, $c^p = c$.

Preuve. Immédiat. □

Théorème 1.14 Pour tout $f(X) \in \mathbb{F}_p[X]$, pour tout $r \geq 0$, $f(X^{p^r}) = f(X)^{p^r}$.
Si F est un corps de caractéristique p autre que $\mathbb{F}_p$, l'assertion précédente est en général fausse dans $F[X]$.

Preuve. Notons $f(X) = c_n X^n + \cdots + c_1 X + c_0 \in \mathbb{F}_p[X]$. Utilisant le point (i) du lemme 1.12 et le fait que $c_i^p = c_i$, on trouve

$$\begin{aligned} f(X)^p &= (c_n X^n + \cdots + c_1 X + c_0)^p \\ &= c_n^p (X^p)^n + \cdots + c_1^p X^p + c_0^p \\ &= c_n (X^p)^n + \cdots + c_1 X^p + c_0 \\ &= f(X^p) \end{aligned}$$

Appliquant cela r fois, on en déduit la première assertion du théorème. Ensuite, si F est un corps de caractéristique p qui n'est pas $\mathbb{F}_p$, on peut choisir $c \in F \setminus \mathbb{F}_p$. Alors $c^p \neq c$ par le lemme 1.13, donc le polynôme $f(X) = c$ ne vérifie pas $f(X^p) = f(X)^p$. □

Corollaire 1.15 Si $f(X) \in \mathbb{F}_p[X]$ a des racines distinctes, on a $\{\alpha_1^p, \ldots, \alpha_n^p\} = \{\alpha_1, \ldots, \alpha_n\}$.

Preuve. Soit $S := \{\alpha_1, \ldots, \alpha_n\}$. D'abord, comme $f(X)^p = f(X^p)$ par le théorème 1.14, la puissance $p-$ième d'une racine de f est encore une racine de f. Ainsi, l'élévation à la puissance p définit une fonction $\varphi \colon S \longrightarrow S$. Par le point (ii) du lemme 1.12, φ est injective, et comme S est fini, φ est nécessairement surjective. C'est donc une permutation de S. □

Exemple. Soit $f(X) = X^3 + X^2 + 1 \in \mathbb{F}_5[X]$, et α, $2\alpha^2 + 3\alpha$, $3\alpha^2 + \alpha + 4$ ses racines dans $F = \mathbb{F}_5[X]/(X^3 + X^2 + 1)$. On vérifie facilement que $\alpha^5 = 3\alpha^2 + \alpha + 4$, $(2\alpha^2 + 3\alpha)^5 = \alpha$, $(3\alpha^2 + \alpha + 4)^5 = 2\alpha^2 + 3\alpha$.

1.5.3 Racines d'irréductibles de $\mathbb{F}_p[X]$

Dans cette sous-section, nous rendons explicites les relations entre les racines d'un polynôme irréductible de $\mathbb{F}_p[X]$. Pour résumer, on peut obtenir toutes les racines à partir d'une seule en prenant successivement les puissances $p-$ièmes. L'énoncé précis est le théorème 1.19.

Lemme 1.16 Soit $f(X) \in \mathbb{F}_p[X]$ de degré n. Le quotient $\mathbb{F}_p[X]/(f(X))$ a p^n éléments.

Preuve. Les éléments de $\mathbb{F}_p[X]/(f(X))$ sont des classes d'équivalences représentées par les restes des divisions euclidiennes des éléments de $\mathbb{F}_p[X]$ par $f(X)$. Ces représentants sont de la forme

$$c_{n-1} X^{n-1} + \cdots + c_1 X + c_0$$

avec $c_0, \ldots, c_{n-1} \in \mathbb{F}_p$. Il y a p^n tels représentants. □

Lemme 1.17 Si F est un corps fini avec q éléments, alors $c^q = c$ pour tout $c \in F$.

Preuve. Si $c = 0$, il n'y a rien à montrer.
Si $c \neq 0$, $c \in (F^*, \cdot)$ qui est un groupe multiplicatif de cardinalité $q - 1$, donc $c^{q-1} = 1$ par le théorème de Lagrange.
Multipliant cette dernière équation par c, on a bien $c^q = c$. □

Théorème 1.18 Soit $\pi(X) \in \mathbb{F}_p[X]$ irréductible de degré d.
(i) Dans $\mathbb{F}_p[X]$, $\pi(X) \mid X^{p^d} - X$.
(ii) Pour $n \geq 0$, $\pi(X) \mid X^{p^n} - X$ si, et seulement si, $d \mid n$.

Preuve. (i) Comme $\pi(X)$ est irréductible, $\mathbb{F}_p[X]/(\pi(X))$ est un corps, qui compte p^d éléments par le lemme 1.16. Par le lemme 1.17, $\overline{X}^{p^d} = \overline{X}$ dans $\mathbb{F}_p[X]/(\pi(X))$ ou, de manière équivalente, $X^{p^d} \equiv X \bmod \pi(X)$, *i.e.* $\pi(X)$ divise $X^{p^d} - X$.
(ii) Commençons par montrer $\Longleftarrow$. Soit $k \in \mathbb{Z}$ tel que $n = kd$. Utilisant la congruence $X^{p^d} \equiv X \bmod \pi(X)$ k fois, on a

$$X^{p^n} = X^{p^{kd}} = (X^{p^d})^{p^{(k-1)d}} \equiv X^{p^{(k-1)d}} \equiv X^{p^{(k-2)d}} \equiv ... \equiv X^{p^d} \equiv X \mod \pi(X)$$

et donc $\pi(X) \mid X^{p^n} - X$. Réciproquement, supposons que $X^{p^n} \equiv X \bmod \pi(X)$. Soient q, $r \in \mathbb{Z}$ tels que $n = dq + r$, avec $0 \leq r < d$. On a alors $X^{p^n} = X^{p^{dq+r}} = (X^{p^{dq}})^{p^r} \equiv X^{p^r} \bmod \pi(X)$ puisque $d \mid dq$. Combinant les congruences $X^{p^n} \equiv X \bmod \pi(X)$ et $X^{p^n} \equiv X^{p^r} \bmod \pi(X)$, on obtient

$$X^{p^r} \equiv X \mod \pi(X)$$

Ainsi, dans le quotient $\mathbb{F}_p[X]/(\pi(X))$, la classe de X est un élément égal à sa propre p^r-puissance. Combinant cela avec le théorème 1.14, on obtient que pour tout $f(X) \in \mathbb{F}_p[X]$,

$$f(X)^{p^r} \equiv f(X) \mod \pi(X).$$

Autrement dit, tous les éléments de $\mathbb{F}_p[X]/(\pi(X))$ sont égaux à leur p^r-puissance. Supposons donc par l'absurde que $r > 0$, et considérons le polynôme $T^{p^r} - T$. On vient de montrer que tous les éléments de $\mathbb{F}_p[X]/(\pi(X))$ en sont des racines. Comme $\mathbb{F}_p[X]/(\pi(X))$ a p^d éléments et que $T^{p^r} - T$ a au plus p^r racines, on déduit que $p^d \leq p^r$, donc $d \leq r$. Mais par division euclidienne $r < d$. Ceci est la contradiction voulue. Ainsi $r = 0$ et $d \mid n$. □

Théorème 1.19 Soit $\pi(X) \in \mathbb{F}_p[X]$ irréductible de degré d et soit $F \supset \mathbb{F}_p$ un corps dans lequel $\pi(X)$ a une racine α. Alors $\pi(X)$ a α, α^p, $\alpha^{p^2}, \ldots, \alpha^{p^{d-1}}$ pour racines, et ces d racines sont distinctes. Plus précisément, pour i, $j \geq 0$, on a $\alpha^{p^i} = \alpha^{p^j} \Longleftrightarrow i \equiv j \bmod d$.

Preuve. Comme $\pi(X^p) = \pi(X)^p$ par le théorème 1.14, on voit que α^p est aussi une racine de $\pi(X)$, et de même pour $\alpha^{p^2}, \ldots, \alpha^{p^{d-1}}$ par itération. Par la preuve précédente, $\alpha^{p^d} = \alpha$ et le cycle recommence. Pour l'équivalence, si $i \equiv j \bmod d$, il existe $k \in \mathbb{Z}$ tel que $i - j = dk$ et on écrit

$$\alpha^{p^i} = \alpha^{p^{i-j+j}} = (\alpha^{p^{i-j}})^{p^j} = (\alpha^{p^{dk}})^{p^j} = \alpha^{p^j}.$$

Pour le sens direct, supposons sans perdre de généralité que $i \leq j$, et écrivons $j = i + k$ où $k \geq 0$. Alors il vient

$$\alpha^{p^i} = \alpha^{p^{i+k}} = (\alpha^{p^k})^{p^i}.$$

Le point (ii) du lemme 1.12, appliqué i fois, donne $\alpha = \alpha^{p^k}$, donc α est racine de $X^{p^k} - X$. Ainsi, $\pi(X)$ divise $X^{p^k} - X$ (voir exercice 14 ci-dessous) et donc, par le théorème 1.18, d divise k, donc d divise $j-i$, *i.e.* $i \equiv j \bmod d$. □

Exemples. (i) Le polynôme $X^3 + X + 1$ est irréductible dans $\mathbb{F}_2[X]$, et a une racine α dans $\mathbb{F}_2[X]/(X^3 + X + 1)$. Ses autres racines sont α^2 et $\alpha^4 = \alpha \cdot \alpha^3 = \alpha(\alpha + 1) = \alpha^2 + \alpha$.
(ii) De même, $X^3 + X^2 + 1$ est irréductible dans $\mathbb{F}_5[X]$, et a une racine α dans $F = \mathbb{F}_5[X]/(X^3 + X^2 + 1)$. Ses autres racines sont α^5 et α^{25}. En utilisant que $\alpha^3 = -\alpha^2 - 1$, on calcule

$$\alpha^5 = \alpha^2\alpha^3 = \alpha^2(-\alpha^2 - 1) = -\alpha^4 - \alpha^2 = -\alpha(-\alpha^2 - 1) - \alpha^2 = -\alpha^2 - 1 + \alpha - \alpha^2 = 3\alpha^2 + \alpha + 4$$
$$\alpha^{25} = (\alpha^5)^2 = (3\alpha^2 + \alpha + 4)^2 = 4\alpha^4 + \alpha^2 + 1 + (-\alpha^2 - 1) - \alpha^2 + 3\alpha = 2\alpha^2 + 3\alpha$$

comme annoncé ci-dessus.

1.6 Les irréductibles de $\mathbb{F}_p[X]$

Une jolie application des résultats précédents est le suivant : il décrit les polynômes irréductibles de $\mathbb{F}_p[X]$ comme les facteurs irréductibles d'un certain polynôme.

Théorème 1.20 Soit $n \geq 1$.
Dans $\mathbb{F}_p[X]$, on a

$$X^{p^n} - X = \prod_{d \mid n} \prod_{\deg(\pi) = d} \pi(X)$$

où $\pi(X)$ est unitaire et irréductible.

Preuve. Par le théorème 1.18, les polynômes irréductibles de degré d un diviseur de n apparaissent dans la factorisation de $X^{p^n} - X$. Ces facteurs irréductibles doivent de plus être unitaires puisque $X^{p^n} - X$ l'est. Il reste donc à montrer que chacun de ces facteurs apparaît exactement une fois. Soit $\pi(X)$ l'un de ces facteurs. Il existe un corps F dans lequel $\pi(X)$ a une racine α. On travaille dans $F[X]$. Comme α est racine de $\pi(X)$ et que $\pi(X)$ divise $X^{p^n} - X$, α est racine de $X^{p^n} - X$, donc $\alpha^{p^n} = \alpha$. On écrit alors

$$X^{p^n} - X = X^{p^n} - X - 0 = X^{p^n} - X - (\alpha^{p^n} - \alpha) = (X - \alpha)^{p^n} - (X - \alpha) = (X - \alpha)((X - \alpha)^{p^n - 1} - 1)$$

Le second facteur dans la dernière expression ne s'annule pas en α, donc $(X - \alpha)^2$ ne divise pas $X^{p^n} - X$ dans $F[X]$. Ainsi, $\pi(X)^2$ ne divise pas $X^{p^n} - X$ dans $\mathbb{F}_p[X]$. □

Exemple. Factorisons $X^{2^n} - X$ dans $\mathbb{F}_2[X]$ pour $n = 1, 2, 3, 4$. On a

$$\begin{aligned}
X^2 - X &= X(X + 1) \\
X^4 - X &= X(X + 1)(X^2 + X + 1) \\
X^8 - X &= X(X + 1)(X^3 + X + 1)(X^3 + X^2 + 1) \\
X^{16} - X &= X(X - 1)(X^2 + X + 1)(X^4 + X + 1)(X^4 + X^3 + 1)(X^4 + X^3 + X^2 + X + 1)
\end{aligned}$$

1.7 Exercices

Exercice 1. Soit $f(X) = X^4 + 3X^2 + 3X + 9 \in \mathbb{Q}[X]$.

(i) Est-ce que f a une racine dans $\mathbb{Q}$?
(ii) Soit $\overline{f}(X)$ la réduction modulo 2 de f. Factoriser $\overline{f}(X)$ dans $\mathbb{F}_2[X]$.
(iii) Déduire de (i) et (ii) que f est irréductible dans $\mathbb{Q}[X]$.

Exercice 2. Soit K un corps.

(i) Montrer que $f(X) \in K[X]$ est irréductible si, et seulement si, $f(X+1) \in K[X]$ est irréductible.
(ii) En déduire que $f(X) \in K[X]$ est irréductible si, et seulement si, $f(X+k) \in K[X]$ est irréductible pour tout $k \in \mathbb{Z}$.

Exercice 3. Montrer que les polynômes suivants sont irréductibles sur $\mathbb{Q}$.

(i) $f(X) = X^5 - 4X + 2$.
(ii) $f(X) = X^n + a$, où a est un entier sans facteur carré, et $a \neq \pm 1$.
(iii) $f(X) = X^{p-1} + X^{p-2} + \cdots + X + 1$, où p est un nombre premier.

Exercice 4. Factoriser les polynômes suivants en produit d'irréductibles de $\mathbb{Q}[X]$, et justifier que les facteurs donnés sont bien irréductibles.

(i) $X^3 - 8$
(ii) $X^{1000} - 6$
(iii) $X^4 + 4$
(iv) $2X^3 + 5X^2 + 5X + 3$
(v) $X^5 + 6X^2 - 9X + 12$
(vi) $X^{73} - 1$
(vii) $X^{73} + 1$
$(viii)$ $X^{24} - 1$

Exercice 5. Les polynômes suivants sont-ils irréductibles dans $\mathbb{F}_5[X]$?

(i) $f_1(X) = X - 3$
(ii) $f_2(X) = 3X^2 + 2X + 1$
(iii) $f_3(X) = 2X^3 - 3X^2 + X + 1$

Exercice 6. Les polynômes suivants sont-ils irréductibles dans $\mathbb{Q}[X]$?

(i) $f(X) = X^5 + X^4 + X^3 + X^2 + X + 1$
(ii) $g(X) = X^4 + X^3 + X^2 + 6X + 1$
(iii) $h(X) = X^3 - 4X^2 + 3X + 1$
(iv) $i(X) = X^6 + X + 1$

Exercice 7. Dresser la liste des polynômes irréductibles unitaires de degré ≤ 3 dans $\mathbb{F}_2[X]$, $\mathbb{F}_3[X]$ et $\mathbb{F}_5[X]$.

Exercice 8. Décomposer les polynômes suivants comme produit d'irréductibles de $\mathbb{F}_3[X]$.

(i) $f(X) = X^2 + X + 1$
(ii) $g(X) = X^3 + X + 2$
(iii) $h(X) = X^4 + X^3 + X + 1$

Exercice 9. Montrer que, pour tout $n \geq 2$, il existe un polynôme irréductible de degré n dans $\mathbb{Q}[X]$. Est-ce vrai pour $\mathbb{R}[X]$? $\mathbb{C}[X]$?

Exercice 10. Montrer que les polynômes suivants sont irréductibles dans $\mathbb{C}[X, Y]$.

(i) $f(X, Y) = X^n + Y^n - 1$, pour tout $n \geq 1$.

(*ii*) $f(X,Y) = X^3 + Y^2X^2 - YX - Y^3 + Y^2$
(*iii*) $f(X,Y) = X^5 - YX^2 + X^2 + YX + 2X + Y + 5$

Exercice 11. Démontrer la proposition 1.9.

Exercice 12. Soient K un corps, et $f(X)$, $g(X) \in K[X] \setminus K$.
Montrer que f et g sont premiers entre eux si, et seulement si, ils n'ont aucune racine commune dans un corps plus grand qui contient K.

Exercice 13. Soit $f(X) = X^3 + X + 1 \in \mathbb{F}_2[X]$.

(*i*) Montrer que f est irréductible, et que $F = \mathbb{F}_2[X]/(f(X))$ est un corps.
(*ii*) Quel est le cardinal de F ? Lister tous ses éléments.
(*iii*) Trouver l'inverse de $\alpha = \overline{X}$ dans F.

Exercice 14. Soit $\pi(X) \in K[X]$ irréductible et soit α une racine de $\pi(X)$ dans un corps plus grand.
Pour $h(X) \in K[X]$, montrer que $h(\alpha) = 0$ si, et seulement si, $\pi(X)$ divise $h(X)$ dans $K[X]$.

Exercice 15.

(*i*) Vérifier que $f(X) = X^4 + X + 1$ est irréductible dans $\mathbb{F}_2[X]$.
(*ii*) Donner un corps F dans lequel f a une racine.
Trouver toutes les racines de f, et les écrire comme combinaison linéaire de 1, α, α^2 et α^3.
(*iii*) Vérifier le corollaire 1.15 dans ce cas.
(*iv*) Donner $|F|$ et faire la liste des éléments de F.

Exercice 16. En utilisant l'exercice 7, factoriser $X^3 - X$ et $X^9 - X$ dans $\mathbb{F}_3[X]$.

Exercice 17. Soit $N_p(n)$ le nombre de polynômes irréductibles unitaires de degré n dans $\mathbb{F}_p[X]$.
Dans cet exercice on établit une formule explicite pour $N_p(n)$.

(*i*) Donner $N_p(1)$.
(*ii*) A l'aide du théorème 1.20, exprimer p^n en fonction des $N_p(d)$ pour les d divisant n.
(*iii*) En déduire une formule explicite pour $N_p(n)$.
(*iv*) Combien y-a-t-il de polynômes irréductibles unitaires de degré 12 dans $\mathbb{F}_{19}[X]$?
(*v*) Calculer $N_3(3)$ et vérifier que votre liste de l'exercice 7 est complète.

Exercice 18. Montrer que pour tout $n \geq 1$, il existe un polynôme irréductible de degré n dans $\mathbb{F}_p[X]$.

2 Extensions de corps

2.1 Extensions et degrés

Désormais, et pour toute la suite, un corps est un anneau commutatif unitaire non nul dont tous les éléments sont inversibles. Un morphisme d'anneaux $\sigma\colon K \longrightarrow L$ entre deux corps est appelé morphisme de corps.

Le premier résultat de cette section motivera la définition d'extension.

Lemme 2.1 Tout morphisme de corps est injectif.

Preuve. Soit $\sigma\colon K \longrightarrow L$ un tel morphisme. Alors $\mathrm{Ker}(\sigma)$ est un idéal de K, et comme K est un corps, ses seuls idéaux sont $\{0\}$ et K, donc σ est injectif ou $\sigma \equiv 0$. Comme $\sigma(1) = 1 \neq 0$, la seconde possibilité est exclue, et σ est injectif. □

Définition 2.2 Soit K un corps. Une *extension* de K est la donnée d'un corps L et d'un morphisme de corps $\sigma\colon K \longrightarrow L$. On la note L/K, et on la représente par le diagramme

$$\begin{array}{c} L \\ | \\ K \end{array}$$

Une *tour d'extensions* est une suite finie de corps $K_1, \ldots, K_n$ telle que, pour tout $i = 1, \ldots, n-1$, K_{i+1}/K_i est une extension de corps.

Exemples. (i) Via les inclusions naturelles $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$, $\mathbb{R}$ et $\mathbb{C}$ sont des extensions de $\mathbb{Q}$, et $\mathbb{C}$ est une extension de $\mathbb{R}$.
(ii) Comme $X^2 - 2 \in \mathbb{Q}[X]$ est irréductible, le quotient $\mathbb{Q}[X]/(X^2-2)$ est un corps qui contient une racine de $X^2 - 2$ et $\mathbb{Q}$ comme sous-corps. Cette extension est en général notée $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$.
(iii) Soit K un corps. L'anneau $K[X]$ se plonge dans son corps des fractions, noté $K(X)$, le corps des fractions rationnelles. En particulier, $K \subset K(X)$, et $K(X)$ est une extension de K.

Par le lemme 2.1, le morphisme $\sigma\colon K \longrightarrow L$ associé à une extension K/L est injectif. On peut donc identifier K à son image par σ, c'est-à-dire supposer que K est un sous-corps de L. Pour cette raison, on appelle σ un plongement.
De la même façon, on peut voir une tour d'extensions comme une suite croissante de corps $K_1 \subset \cdots \subset K_n$.

Etant donné un corps K, un de ses sous-corps joue un rôle particulier.

Définition 2.3 Soit K un corps.
L'intersection de tous les sous-corps de K est appelée *sous-corps premier* de K, et est notée $\Pi(K)$.

Le sous-corps premier est le plus petit sous-corps de K pour l'inclusion.

Proposition 2.4 Soit K un corps. Alors $\Pi(K) \simeq \mathbb{Q}$, ou $\Pi(K) \simeq \mathbb{F}_p$ pour un nombre premier p.

Preuve. Soit $\gamma\colon \mathbb{Z} \longrightarrow K$ le morphisme d'anneaux défini par $\gamma(n) := n \cdot 1_K$. Comme $\mathrm{Im}(\gamma)$ est un sous-anneau de K et que K est intègre, $\mathrm{Im}(\gamma)$ est intègre, donc le quotient $\mathbb{Z}/\mathrm{Ker}(\gamma)$ est intègre par le 1er théorème d'isomorphisme. Ainsi, $\mathrm{Ker}(\gamma)$ est un idéal premier de $\mathbb{Z}$, donc $\mathrm{Ker}(\gamma) = \{0\}$ ou $\mathrm{Ker}(\gamma) = p\mathbb{Z}$ pour un nombre premier p. Si $\mathrm{Ker}(\gamma) = \{0\}$, γ est injectif et se prolonge en un morphisme de corps $\overline{\gamma}\colon \mathbb{Q} \longrightarrow K$ en posant, pour $r = \frac{p}{q} \in \mathbb{Q}$, $\overline{\gamma}(r) := \gamma(p)(\gamma(q))^{-1}$. Alors $\mathrm{Im}(\overline{\gamma}) \simeq \mathbb{Q}$. Comme $\Pi(K)$ est le plus petit sous-corps de K, on a $\Pi(K) \subset \mathrm{Im}(\overline{\gamma})$. Mais $\mathbb{Q}$ n'a pas de sous-corps strict, ce qui implique $\Pi(K) = \mathrm{Im}(\overline{\gamma}) \simeq \mathbb{Q}$. Si $\mathrm{Ker}(\gamma) = p\mathbb{Z}$ pour un nombre premier p, alors $\mathrm{Im}(\gamma) \simeq \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ est un sous-corps de K, donc $\Pi(K) \subset \mathrm{Im}(\gamma)$. Comme $\mathbb{F}_p$ n'a pas de sous-corps strict, on en déduit que $\Pi(K) = \mathrm{Im}(\gamma) \simeq \mathbb{F}_p$. □

Définition 2.5 Soit K un corps.
La *caractéristique* de K est le nombre entier $\mathrm{char}(K)$ défini comme

$$\mathrm{char}(K) = \begin{cases} 0 & \text{si } \Pi(K) \simeq \mathbb{Q} \\ p & \text{si } \Pi(K) \simeq \mathbb{F}_p \end{cases}.$$

Exemples. (i) On a $\mathrm{char}(\mathbb{Q}) = \mathrm{char}(\mathbb{R}) = \mathrm{char}(\mathbb{C}) = 0$ et $\mathrm{char}(\mathbb{F}_p[X]) = \mathrm{char}(\mathbb{F}_p(X)) = p$.
(ii) Si $f(X) \in \mathbb{F}_p[X]$ est irréductible, alors $\mathrm{char}(\mathbb{F}_p[X]/(f(X))) = p$.

Définition 2.6 Soit L/K une extension de corps et $A \subset L$. On note
(i) $K[A]$ l'intersection de tous les sous-anneaux de L contenant A et K.
(ii) $K(A)$ l'intersection de tous les sous-corps de L contenant A et K.
(iii) Si $A = \{a_1, \ldots, a_n\}$, on écrit $K[a_1, \ldots, a_n]$ au lieu de $K[A]$, $K(a_1, \ldots, a_n)$ au lieu de $K(A)$, et on dit que l'extension $K(A)/K$ est *de type fini*. En particulier, si $A = \{a\}$, l'extension $K(a)/K$ est dite *monogène*, ou *simple*.

Par définition, $K[A]$ est le plus petit sous-anneau de L contenant A et K. De même, $K(A)$ est le plus petit sous-corps de L contenant A et K.

Lemme 2.7 Soit L/K une extension de corps. Alors L est une $K-$algèbre.
En particulier, L est un $K-$espace vectoriel.

Preuve. Soit $\sigma\colon K \longrightarrow L$ un plongement associé à L/K. On définit une multiplication externe via

$$\begin{aligned} K \times L &\longrightarrow L \\ (x, y) &\longmapsto \sigma(x)y. \end{aligned}$$

On vérifie facilement les axiomes définissant une structure de $K-$algèbre. □

Définition 2.8 Soit L/K une extension de corps.
(i) La dimension de L en tant que $K-$espace vectoriel est appelé le *degré* de l'extension, et est noté $[L : K]$.
(ii) L'extension L/K est dite *finie* si $[L : K] < \infty$. Sinon, elle est dite *infinie*.
(iii) Une extension de degré 2 est appelée extension *quadratique*.

Exemples. (i) On vérifie facilement que $[L : K] = 1 \iff L = K$.
(ii) L'ensemble $\{1, i\}$ est une base de $\mathbb{C}$ comme $\mathbb{R}-$espace vectoriel, donc $\mathbb{C}/\mathbb{R}$ est quadratique.
(iii) En tant que $\mathbb{Q}-$espace vectoriel, $\mathbb{R}$ est de dimension infinie, *i.e.* $[\mathbb{R} : \mathbb{Q}] = \infty$.
(iv) Si K est un corps, l'extension $K(X)/K$ est infinie.

Le résultat suivant est essentiel, et décrit comment se comporte le degré pour des tours d'extensions.

Théorème 2.9 (de la base téléscopique) Soient L/K et M/L deux extensions de corps.
Soient $\{e_i \mid i \in I\}$ une base L sur K et $\{f_j \mid j \in J\}$ une base M sur L.
Alors $\{e_i f_j \mid (i, j) \in I \times J\}$ est une base de M sur K.

Preuve. Montrons d'abord que $\{e_i f_j \mid (i, j) \in I \times J\}$ est une famille libre. Soient $x_{i,j} \in K$ tels que $\sum_{(i,j)\in I\times J} x_{i,j} e_i f_j = 0$.

Cette dernière équation peut se réécrire $\sum_{j\in J} \left(\sum_{i\in I} x_{i,j} e_i \right) f_j = 0$, ce qui implique

$$\sum_{i\in I} x_{i,j} e_i = 0, \ \forall j \in J$$

par indépendance linéaire des f_j. Comme $\{e_i \mid i \in I\}$ est une base de L sur K, on en déduit que $x_{i,j} = 0$ pour tout $j \in J$ et tout $i \in I$. Soit ensuite $z \in M$. La famille $\{f_j \mid j \in J\}$ engendre M sur L, donc il existe une famille $\{\lambda_j\}_{j\in J}$ d'éléments de L tels que $z = \sum_{j\in J} \lambda_j f_j$. Or, pour tout $j \in J$, on peut écrire $\lambda_j = \sum_{i\in I} x_{i,j} e_i$ pour une famille $\{x_{i,j}\}_{i\in I}$

d'élément de K, puisque $\{e_i \mid i \in I\}$ est une base de L sur K. Tout cela mis ensemble donne

$$z = \sum_{j\in J} \lambda_j f_j = \sum_{j\in J} \Big(\sum_{i\in I} x_{i,j} e_i \Big) f_j = \sum_{(i,j)\in I\times J} x_{i,j} e_i f_j$$

ce qui montre que $\{e_i f_j \mid (i,j) \in I \times J\}$ est une famille génératrice de M sur K. Cela termine la preuve. □

On déduit directement le corollaire suivant.

Corollaire 2.10 (multiplicativité des degrés) Soient L/K et M/L deux extensions finies. Alors $[M : K] = [M : L][L : K]$.

2.2 Extensions monogènes

Dans cette sous-section, on s'intéresse aux extensions monogènes. La définition suivante est cruciale pour la suite.

Définition 2.11 Soit L/K une extension de corps, et $a \in L$.
On dit que a est *algébrique* sur K s'il existe un polynôme $f \in K[X] \setminus \{0\}$ tel que $f(a) = 0$. Dans le cas contraire, a est *transcendant* sur K.
L'extension L/K est *algébrique* si tout $a \in L$ est algébrique. Sinon, L/K est dite *transcendante*.

Exemples. (i) L'extension $\mathbb{C}/\mathbb{R}$ est algébrique, puisque tout $z = x + iy \in \mathbb{C}$ est racine de $f(X) = X^2 - 2xX + (x^2 + y^2)$, polynôme à coefficients dans $\mathbb{R}[X]$.
(ii) Le nombre $\sqrt{2}$ est algébrique sur $\mathbb{Q}$ puisqu'il est racine du polynôme $X^2 - 2$.
(iii) Le nombre $\pi \in \mathbb{R}$ est transcendant sur $\mathbb{Q}$, et l'extension $\mathbb{Q}(\pi)/\mathbb{Q}$ est transcendante.
(iv) L'extension de corps $K(X)/K$ est transcendante, car X est transcendant sur K.

Pour l'étude des extensions monogènes algébriques, considérons pour $a \in L$ le morphisme d'évaluation

$$\begin{aligned} \varphi_a \colon K[X] &\longrightarrow L \\ p &\longmapsto p(a) \end{aligned}$$

et son noyau $I(a) := \{p \in K[X] \mid p(a) = 0\}$, l'ensemble des polynômes annulateurs de a. Avec ces notations, a est algébrique sur K si et seulement si $I(a) \neq \{0\}$. De plus, comme φ_a est un morphisme d'anneaux, son noyau $I(a)$ est un idéal, et comme $K[X]$ est principal, il existe $f \in K[X] \setminus \{0\}$ tel que $I(a) = (f(X))$. De plus, f est unique s'il est choisi unitaire. Ainsi, tout polynôme annulateur de a est un multiple de f.

Définition 2.12 Soit L/K une extension de corps, et $a \in L$ algébrique sur K.
L'unique polynôme unitaire $f \in K[X]\setminus\{0\}$ tel que $f(a) = 0$ et tel que f divise h pour tout $h \in K[X]$ vérifiant $h(a) = 0$ est appelé le *polynôme minimal* de a.

Proposition 2.13 Soit $a \in L$ algébrique sur K.
Le polynôme minimal f de a est caractérisé par les propriétés équivalentes suivantes :
(i) $f \in K[X]$, f est unitaire, $f(a) = 0$ et $\deg(f) \leq \deg(h)$ pour tout $h \in K[X] \setminus \{0\}$ vérifiant $h(a) = 0$.
(ii) $f \in K[X]$, f est unitaire, $f(a) = 0$, et f est irréductible.

Preuve. (i) Clairement, si f est le polynôme minimal de a au sens de la définition 2.12, f vérifie les conditions voulues. Réciproquement, soit $p \in K[X]$ unitaire, annulateur de a, et de degré minimal parmi les polynômes non-nuls annulateurs de a. Puisque $f(a) = 0$, on a donc $\deg(p) \leq \deg(f)$. Or f divise p, donc $\deg(p) = \deg(f)$ et $p = uf$ pour $u \in K^*$. Comme p et f sont tous deux unitaires, on a donc $u = 1_K$, et $p = f$ est le polynôme minimal de a.
(ii) Montrons déjà que le polynôme minimal f de a est irréductible. Soit $f(X) = g(X)h(X)$ une décomposition de f dans $K[X]$. Alors on obtient

$$0 = f(a) = g(a)h(a)$$

ce qui implique $g(a) = 0$ ou $h(a) = 0$. Sans restriction, disons $h(a) = 0$. Alors f divise h (par définition du polynôme minimal), et h divise f par hypothèse, donc $f = uh$ pour un certain $u \in K^*$. Ainsi, $g = u \in K^*$, et f est irréductible.

Réciproquement, soit $p \in K[X]$ unitaire, irréductible et tel que $p(a) = 0$. Alors f divise p, donc il existe $g \in K[X]$ tel que $p = gf$, et comme p est irréductible, on en déduit que $g = u \in K^*$. Donc $p = uf$. Comme p et f sont tous deux unitaires, on a $u = 1_K$, et $p = f$ est le polynôme minimal de a. □

Exemples. (i) Directement, $X^2 + 1 \in \mathbb{R}[X]$ est le polynôme minimal de i sur $\mathbb{R}$, puisqu'il est unitaire irréductible et a i comme racine.
(ii) Le polynôme $X^n - p$, où $n \geq 1$ et p est premier, est le polynôme minimal de $\sqrt[n]{p}$ sur $\mathbb{Q}$, puisqu'il est unitaire, irréductible par Eisenstein, et a $\sqrt[n]{p}$ pour racine.
(iii) Le polynôme minimal de $\omega := e^{i\frac{2\pi}{3}}$ est $X^2 + X + 1$.

Le polynôme minimal d'un élément $a \in L$ permet de calculer facilement le degré de l'extension $K(a)/K$.

Théorème 2.14 Soit $a \in L$ algébrique sur K, f son polynôme minimal, et $n := \deg(f)$.
(i) On a un isomorphisme de corps $K[a] = K(a) \simeq K[X]/(f(X))$.
(ii) L'ensemble $\{1, a, a^2, \ldots, a^{n-1}\}$ est une $K-$base de $K(a)$. En particulier, $[K(a) : K] = n$.

Preuve. (i) Considérons le morphisme d'évaluation $\varphi_a \colon K[X] \longrightarrow L$ introduit ci-dessus. On vérifie facilement que son image est $K[a]$. On a noté son noyau $I(a) = (f(X))$, et on a donc un isomorphisme d'anneaux $K[a] \simeq K[X]/(f(X))$. Comme f est irréductible, $K[X]/(f(X))$ est un corps, donc $K[a]$ est un corps, qui contient K et a. Or $K(a)$ est le plus petit sous-corps de L qui contient K et a, donc $K(a) \subset K[a]$. L'autre inclusion étant évidente, on a bien $K[a] = K(a)$, ce qui montre (i).
(ii) Montrons d'abord l'indépendance linéaire de cette famille. Soient $\lambda_0, \ldots, \lambda_{n-1} \in K$ tels que $\sum_{i=0}^{n-1} \lambda_i a^i = 0$. Cela signifie que le polynôme $h(X) = \sum_{i=0}^{n-1} \lambda_i X^i \in K[X]$ est annulateur de a. Comme il a degré $n-1 < \deg(f)$, il est identiquement nul, et donc $\lambda_0 = \cdots = \lambda_{n-1} = 0$. Ensuite, cette famille est génératrice de $K(a)$. En effet, soit $b \in K(a) = K[a] = \mathrm{Im}(\varphi_a)$. On peut donc écrire $b = h(a)$ pour un certain polynôme $h(X) \in K[X]$. Par division euclidienne, il existe $q, r \in K[X]$ tels que $h = qf + r$, avec $\deg(r) \leq n - 1$. En écrivant explicitement $r(X) = r_{n-1}X^{n-1} + \cdots + r_1 X + r_0$ et en utilisant que $f(a) = 0$, on a

$$b = h(a) = r(a) = r_{n-1}a^{n-1} + \cdots + r_1 a + r_0 \in \langle 1, a, \ldots, a^{n-1} \rangle$$

ce qui montre bien que $\{1, a, \ldots, a^{n-1}\}$ engendre $K(a)$. C'est donc une $K-$base de $K(a)$. □

Terminons cette section avec un cas particulier important d'extensions simples.

Proposition 2.15 Soit K une extension quadratique de $\mathbb{Q}$.
Alors il existe $d \in \mathbb{Z} \setminus \{0, 1\}$ tel que $K = \mathbb{Q}(\sqrt{d})$, où $\sqrt{d}$ désigne un nombre complexe de carré d.

Preuve. Soit $a \in K \setminus \mathbb{Q}$, de sorte que $[\mathbb{Q}(a) : \mathbb{Q}] = 2$ et $K = \mathbb{Q}(a)$, par l'exercice 2(ii). Notons $f(X) = X^2 + \beta X + \gamma \in \mathbb{Q}[X]$ le polynôme minimal de a. Considérons son discriminant $\beta^2 - 4\gamma =: b^2$, de sorte que a, racine de f, s'écrive $a = \frac{-\beta+b}{2}$. Cela implique $b = 2a + \beta$, et $K = \mathbb{Q}(a) = \mathbb{Q}(b)$. Maintenant, $\beta^2 - 4\gamma \in \mathbb{Q}$, donc on peut écrire $\beta^2 - 4\gamma = \frac{p}{q}$ avec $p \in \mathbb{Z}$ et $q \geq 1$. Alors le nombre $c = qb$ vérifie $c^2 = pq$, et $K = \mathbb{Q}(b) = \mathbb{Q}(c)$. Ecrivons $pq = m^2 d$, où d est sans facteur carré et $m \geq 1$, de sorte que $(\frac{c}{m})^2 = d$. On obtient finalement $K = \mathbb{Q}(c) = \mathbb{Q}(\frac{c}{m}) = \mathbb{Q}(\sqrt{d})$. Notons aussi que $d \neq 0, 1$ puisque $K \neq \mathbb{Q}$. □

2.3 Extensions algébriques

Cette sous-section est consacrée à l'étude des extensions algébriques.
Tout d'abord, un argument élémentaire d'algèbre linéaire permet d'établir le lemme suivant.

Lemme 2.16 Toute extension finie est algébrique.

Preuve. Soit donc L/K une extension de corps finie. Notons $n := [L : K]$, et soit $a \in L$.
La famille $\{1, a, a^2, \ldots, a^n\}$ possède $n + 1$ éléments, elle est donc liée sur K. Ainsi, il existe $u_0, \ldots, u_n \in K$ tels que

$\sum_{i=0}^{n} u_i a^i = 0$, et le polynôme $h(X) = \sum_{i=0}^{n} u_i X^i$ est annulateur de a. □

La réciproque de ce résultat est fausse : il existe une extension algébrique de $\mathbb{Q}$ de degré infini. C'est l'objet de l'exercice 15 ci-dessous. En fait, pour qu'une extension algébrique soit finie, il suffit qu'elle soit en plus de type fini.

Théorème 2.17 L'extension L/K est finie si, et seulement si, il existe $a_1, \ldots, a_n \in L$ algébriques sur K tels que $L = K(a_1, \ldots, a_n)$.

Preuve. Supposons pour commencer que L/K est finie. En choisissant $\{a_1, \ldots, a_n\}$ une $K-$base de L, on a $L = K(a_1, \ldots, a_n)$. De plus $\{a_1, \ldots, a_n\}$ sont algébriques sur K puisque, L/K étant finie, elle est algébrique par le lemme 2.16. Réciproquement, supposons que $L = K(a_1, \ldots, a_n)$ avec $a_1, \ldots, a_n$ algébriques sur K, et considérons la tour d'extensions

$$K \subset K(a_1) \subset K(a_1)(a_2) = K(a_1, a_2) \subset \cdots \subset K(a_1, \ldots, a_n) = L.$$

Par le théorème 2.14, le degré de $K(a_1, \ldots, a_i)/K(a_1, \ldots, a_{i-1})$ est égal au degré m_i du polynôme minimal de a_i sur $K(a_1, \ldots, a_{i-1})$. Ce degré est fini car borné par $\tilde{m}_i$ le degré du polynôme minimal de a_i sur K, qui existe puisque a_i est algébrique sur K par hypothèse. Par le corollaire 2.10, le degré de L/K est alors $m_1 \ldots m_n$, et L/K est bien finie. □

Corollaire 2.18
(i) Soit $A \subset L$. L'extension $K(A)/K$ est algébrique si, et seulement si, a est algébrique sur K pour tout $a \in A$.
(ii) L'ensemble $\tilde{K} := \{a \in L \mid a \quad \text{algébrique sur} \quad K\}$ est un sous-corps de L, appelé la fermeture algébrique de K.

Preuve. (i) Si $K(A)/K$ est algébrique, il est évident que tout élément de A est algébrique. Réciproquement, si tout élément de A est algébrique sur K, alors $K(a_1, \ldots, a_n)/K$ est algébrique pour tous $a_1, \ldots, a_n \in A$, pour tout $n \geq 1$, et puisque

$$K(A) = \bigcup_{\substack{n \geq 1 \\ a_1, \ldots, a_n \in A}} K(a_1, \ldots, a_n)$$

il suit que $K(A)/K$ est algébrique.
(ii) Soient $a, b \in \tilde{K}$. Alors $K(a, b)/K$ est algébrique par (i), et contient $a + b$, ab et a^{-1} pour $a \neq 0$. Cela signifie exactement que $\tilde{K}$ est un sous-corps de L. □

Finalement on déduit de tous nos résultats la transitivité de l'algébricité.

Théorème 2.19 Soient $K \subset L \subset M$ une tour d'extensions.
M/K est algébrique si, et seulement si, M/L et L/K sont algébriques.

Preuve. Le sens direct est évident. Réciproquement, supposons M/L, L/K algébriques, et soit $a \in M$. Puisque $a \in M$ est algébrique sur L, il existe un polynôme $f(X) = \sum_{i=0}^{n} b_i X^i \in L[X]$ tel que $f(a) = 0$. On a la tour d'extensions suivante

$$K \subset K(b_0, \ldots, b_n) \subset K(b_0, \ldots, b_n)(a) = K(b_0, \ldots, b_n, a)$$

La première est de type fini et les b_i, éléments de L, sont algébriques sur K par hypothèse. Le théorème 2.17 nous assure alors que $K(b_0, \ldots, b_n)/K$ est finie. La deuxième l'est aussi par le théorème 2.17, puisque a est algébrique sur $K(b_0, \ldots, b_n)$, avec f comme polynôme annulateur. Par multiplicativité des degrés, l'extension $K(b_0, \ldots, b_n, a)/K$ est finie, donc algébrique, et la preuve est terminée. □

2.4 Exercices

Exercice 1. Soient L/K une extension de corps, et A, $B \subset L$. Montrer que

(i) $A \subset K(A)$
(ii) $A \subset B \Longrightarrow K(A) \subset K(B)$
(iii) $K(K(A)) = K(A)$
(iv) $K(A)(B) = K(A \cup B) = K(B)(A)$

Exercice 2. (i) Montrer qu'une extension finie est de type finie, mais que la réciproque est fausse.
(ii) Montrer qu'une extension de degré un nombre premier est simple.

Exercice 3. Montrer que $\mathbb{Q}(i, \sqrt{3})$ est simple.

Exercice 4. Soit K un corps de caractéristique différente de 2, et L/K une extension de corps.
Montrer que $[L : K] = 2$ si, et seulement si, il existe $\Delta \in K$ qui n'est pas un carré dans K et $\delta \in L$ tel que $\delta^2 = \Delta$ et $L = K(\delta)$.

Exercice 5. Soient K un corps, L/K une extension et α, $\beta \in L$.

(i) Montrer que $[K(\alpha, \beta) : K(\alpha)] \leq [K(\alpha) : K]$.
(ii) Donner un exemple où l'inégalité précédente est stricte, et un exemple où l'inégalité précédente est une égalité.

Exercice 6. Trouver les degrés d'extension suivants :

(i) $[\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}]$
(ii) $[\mathbb{Q}(\sqrt{1 + \sqrt{3}}) : \mathbb{Q}]$
(iii) $[\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{6}) : \mathbb{Q}]$
(iv) $[\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) : \mathbb{Q}]$, $[\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) : \mathbb{Q}(\sqrt{2})]$ et $[\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) : \mathbb{Q}(\sqrt[3]{2})]$

Exercice 7. Calculer $[\mathbb{Q}(\omega) : \mathbb{Q}]$, où $\omega := e^{\frac{2\pi i}{3}}$. Est-ce que $\sqrt{3} \in \mathbb{Q}(\omega)$? $i \in \mathbb{Q}(\omega)$? $\omega \in \mathbb{Q}(i)$?

Exercice 8. Soient α, $\beta \in \mathbb{C}$ tels que $[\mathbb{Q}(\alpha) : \mathbb{Q}] = [\mathbb{Q}(\beta) : \mathbb{Q}] < \infty$.
Montrer que si $\alpha \in \mathbb{Q}(\beta)$, alors $\mathbb{Q}(\alpha) = \mathbb{Q}(\beta)$.

Exercice 9. Est-ce que $\mathbb{Q}(\sqrt[4]{2})$ et $\mathbb{Q}(i\sqrt[4]{2})$ sont isomorphes ?

Exercice 10. (i) Trouver le polynôme minimal de $\sqrt{3}$ et $\sqrt[4]{2}$ sur $\mathbb{Q}(\sqrt{2})$.
(ii) Trouver le polynôme minimal de $\sqrt{2} + \sqrt[3]{2}$ sur $\mathbb{Q}$.

Exercice 11. Soit $\alpha := \sqrt[3]{2} \in \mathbb{R}$.

(i) Soit $\beta \in \mathbb{Q}(\alpha) \setminus \mathbb{Q}$. Montrer que β est de degré 3 sur $\mathbb{Q}$. Est-ce que $\mathbb{Q}(\beta) = \mathbb{Q}(\alpha)$?
(ii) Soit $\gamma := 2 - \alpha$. Quel est le polynôme minimal de γ sur $\mathbb{Q}(\alpha)$? sur $\mathbb{Q}$?

Exercice 12. Déterminer $[\mathbb{Q}(\sqrt{2} + \sqrt[3]{2 + \sqrt{2}}) : \mathbb{Q}]$.

Exercice 13. Soient L/K une extension de corps et $a \in L$ algébrique sur K, tel que $[K(a) : K]$ est impair.
Montrer que a^2 est algébrique sur K et que $K(a^2) = K(a)$.
Montrer, à l'aide d'un contre-exemple, que cela est faux si $[K(a) : K]$ n'est pas impair.

Exercice 14. Le but de cet exercice est de trouver un nombre complexe $z \in \mathbb{C}$ tel que $\overline{z} \notin \mathbb{Q}(z)$.

(i) Soit $\omega := e^{\frac{2\pi i}{3}}$, $\alpha = \sqrt[3]{2}$ et $z := \omega\alpha$. Calculer $[\mathbb{Q}(z) : \mathbb{Q}]$ et $[\mathbb{Q}(\omega) : \mathbb{Q}]$.
(ii) Par l'absurde, supposons que $\overline{z} \in \mathbb{Q}(z)$. Montrer que cela implique $\omega \in \mathbb{Q}(z)$.
(iii) En déduire une contradiction, et conclure que $\overline{z} \notin \mathbb{Q}(z)$.

Exercice 15. Soit $\tilde{\mathbb{Q}}$ l'ensemble des nombres complexes algébriques sur $\mathbb{Q}$.
Montrer que $\tilde{\mathbb{Q}}$ est une extension algébrique infinie de $\mathbb{Q}$.

Exercice 16. Soit $a > 0$.
Montrer que a est transcendant sur $\mathbb{Q}$ si, et seulement si, $\sqrt{a}$ est transcendant sur $\mathbb{Q}$.

Exercice 17. Soit L/K une extension de corps, et $f \in K[X] \setminus K$.
Montrer que si $\alpha \in L$ est transcendant sur K, alors $f(\alpha)$ est transcendant sur K.

3 Extensions normales et séparables

3.1 Corps de rupture, corps de décomposition

Soit K un corps et $f \in K[X]$ un polynôme non constant. Le but de cette section est de rendre plus précise la construction du théorème 1.10 et de construire une extension de K dans laquelle f admet des racines.

Définition 3.1 Une extension L de K est un *corps de rupture* pour f s'il existe $a \in L$ tel que $f(a) = 0$ et $L = K(a)$.

En d'autres termes, un corps de rupture pour f est un corps obtenu à partir de K en y adjoignant une racine.

Exemples. (i) Si $\deg(f) = 1$, K est un corps de rupture de f sur K.
(ii) Le corps $\mathbb{C} = \mathbb{R}(i)$ est un corps de rupture de $X^2 + 1$ sur $\mathbb{R}$.
(iii) Le corps $\mathbb{Q}(\sqrt[4]{2})$ est un corps de rupture de $X^4 - 2$ sur $\mathbb{Q}$. Notons que ce corps contient une autre racine de f, $-\sqrt[4]{2}$, mais pas les deux autres, $i\sqrt[4]{2}$ et $-i\sqrt[4]{2}$.
(iv) Le corps $\mathbb{F}_2(\alpha)$, où $\alpha^2 + \alpha + 1 = 0$, est un corps de rupture de $X^2 + X + 1$ sur $\mathbb{F}_2$.

Comme discuté au chapitre 1, la méthode pour construire un corps dans lequel f a une racine est connue : il suffit de quotienter $K[X]$ par l'idéal engendré par $f(X)$, ou l'un de ses facteurs irréductibles. L'existence d'un corps de rupture est donc déjà acquise. Son unicité, dans un certain sens, reste à démontrer, et nécessite le lemme suivant.

Lemme 3.2 Soient K' un corps, $\sigma\colon K \longrightarrow K'$ un isomorphisme de corps, et $\tilde{\sigma}\colon K[X] \longrightarrow K'[X]$ le prolongement canonique de σ. Soit $f \in K[X] \setminus K$, et $\tilde{f} := \tilde{\sigma}(f)$. Soient enfin $L = K(a)$ un corps de rupture de f sur K et $L' = K'(a')$ un corps de rupture de $\tilde{f}$ sur K'.
Alors il existe un unique isomorphisme de corps $\tau\colon L \longrightarrow L'$ tel que $\tau(a) = a'$ et $\tau_{|K} = \sigma$.

Preuve. Pour commencer, notons $\varphi\colon K[X]/(f(X)) \longrightarrow L$ et $\varphi'\colon K'[X]/(\tilde{f}(X)) \longrightarrow L'$ les isomorphismes construits dans la preuve du théorème 2.14. La situation se schématise comme suit :

$$\begin{array}{ccccc} K & \hookrightarrow & K[X]/(f(X)) & \xrightarrow{\varphi} & K(a) = L \\ \downarrow{\scriptstyle \sigma} & & \downarrow{\scriptstyle \overline{\sigma}} & & \\ K' & \hookrightarrow & K'[X]/(\tilde{f}(X)) & \xrightarrow{\varphi'} & K'(a') = L' \end{array}$$

Pour rendre le premier carré commutatif, on définit $\overline{\sigma}$ par

$$\overline{\sigma}(g + (f(X))) = \tilde{\sigma}(g) + (\tilde{f}(X)).$$

On vérifie facilement que $\overline{\sigma}$ est un morphisme de corps bien défini, donc injectif par le lemme 2.1, et surjectif puisque $\tilde{\sigma}$ est un isomorphisme. Ainsi, $\overline{\sigma}$ est un isomorphisme de corps. Pour compléter le deuxième carré, on pose alors $\tau := \varphi' \circ \overline{\sigma} \circ \varphi^{-1}$, qui est un isomorphisme comme composition d'isomorphismes. On a également

$$\tau(a) = \varphi' \circ \overline{\sigma}(\varphi^{-1}(a)) = \varphi' \circ \overline{\sigma}(X + (f(X))) = \varphi'(X + (\tilde{f}(X))) = a'$$

et

$$\tau(k) = \varphi' \circ \overline{\sigma}(\varphi^{-1}(k)) = \varphi' \circ \overline{\sigma}(k + (f(X))) = \varphi'(\tilde{\sigma}(k) + (\tilde{f}(X))) = \tilde{\sigma}(k) = \sigma(k)$$

pour tout $k \in K$, et donc τ est unique. □

On peut maintenant établir le théorème suivant.

Théorème 3.3 Soit $f \in K[X]$ irréductible.
(i) Il existe un corps de rupture de f sur K.
(ii) Soient $L = K(a)$, $L' = K'(a')$ deux corps de rupture de f sur K.
Alors il existe un unique isomorphisme $\tau\colon L \longrightarrow L'$ tel que $\tau(a) = a'$ et $\tau_{|K} = \mathrm{id}_K$.

Preuve. (i) C'est le théorème 1.10.
(ii) Il suffit d'appliquer le lemme 3.2 avec $K' = K$ et $\sigma = \mathrm{id}_K$. □

Définition 3.4 Une extension L de K est appelée *corps de décomposition* de f sur K s'il existe $c, a_1, \ldots, a_n \in L$ tels que $f(X) = c(X - a_1)\ldots(X - a_n)$ et $L = K(a_1, \ldots, a_n)$.

Exemples. (i) Si $\deg(f) = 1$, alors K est un corps de décomposition de f sur K.
(ii) Si $\deg(f) = 2$, alors tout corps de rupture est aussi un corps de décomposition de f sur K.
En effet, soit $f(X) = a_2X^2 + a_1X + a_0 \in K[X]$ et $L = K(a)$ un corps de rupture pour f. Alors $f(a) = 0$ et on vérifie facilement que $f(b) = 0$ pour $b = -a - \frac{a_1}{a_2} \in K(a)$. Ainsi, $f(X) = a_2(X - a)(X - b)$ dans $K(a, b) = K(a) = L$.
Par exemple, $\mathbb{C} = \mathbb{R}(i)$ est un corps de décomposition de $X^2 + 1$ sur $\mathbb{R}$.
(iii) De même, $\mathbb{Q}(\sqrt[4]{2}, i) = \mathbb{Q}(\sqrt[4]{2})(i)$ est un corps de décomposition de $X^4 - 2$ sur $\mathbb{Q}$.
(iv) Le théorème 1.19 dit précisément que, si $\pi(X) \in \mathbb{F}_p[X]$ est irréductible, alors un corps de rupture est aussi un corps de décomposition de π sur $\mathbb{F}_p$.
(v) Soit p un premier, $n \geq 1$, et $q = p^n$. Soit $f(X) = X^q - X \in \mathbb{F}_p[X]$. Alors L est un corps fini à q éléments si, et seulement si, L est un corps de décomposition de f sur $\mathbb{F}_p$.

On a un résultat similaire au lemme 3.2 pour les corps de décomposition.

Lemme 3.5 Soient K' un corps, $\sigma\colon K \longrightarrow K'$ un isomorphisme de corps, et $\tilde{\sigma}\colon K[X] \longrightarrow K'[X]$ le prolongement canonique de σ. Soit $f \in K[X] \setminus K$, et $\tilde{f} := \tilde{\sigma}(f)$. Soient $L = K(a_1, \ldots, a_n)$ un corps de décomposition de f sur K et $L' = K'(a'_1, \ldots, a'_n)$ un corps de décomposition de $\tilde{f}$ sur K'.
Alors il existe un isomorphisme de corps $\tau\colon L \longrightarrow L'$ tel que $\tau_{|K} = \sigma$ et $\tau(a_i) = a'_{\pi(i)}$ pour une certaine permutation $\pi \in S_n$.

Preuve. On raisonne par récurrence sur $n = \deg(f)$. Si $n = 1$, alors $L = K$, $L' = K'$ et on choisit $\tau = \sigma$. Soit donc $n > 1$. Notons h le produit des facteurs de degré 1 de f dans $K[X]$, de sorte que f s'écrive $f = gh$ avec g sans racines dans K. Ainsi, $\deg(g) \geq 2$. Choisissons alors un facteur irréductible $k \in K[X]$ de g, de degré $d \geq 2$. Soit a une racine de k dans L. En particulier, a est une racine de f donc disons, quitte à renuméroter, que $a = a_1$. Puisque k est un irréductible de $K[X]$, c'est, à un scalaire non-nul près, le polynôme minimal de a_1, donc $[K(a_1) : K] = d$. Maintenant, $\tilde{k} = \tilde{\sigma}(k)$ divise $\tilde{f}$ dans $K'[X]$. Soit a' une racine de $\tilde{k}$ dans L'. En particulier, a' est une racine de $\tilde{f}$, donc $a' = a'_i$ pour un certain $i \in \{1, \ldots, n\}$. Par le lemme 3.2, σ se prolonge en un isomorphisme de corps $\tau_1\colon K(a_1) \longrightarrow K'(a'_i)$, et $\tau_1(a_1) = a'_i$. De plus, L est un corps de décomposition de f sur $K(a_1)$, et L' est un corps de décomposition de $\tilde{f}$ sur $K'(a'_i)$. Comme $L/K(a_1)$ est de degré $\frac{n}{d} \leq n - 1$, on peut appliquer l'hypothèse de récurrence, et τ_1 se prolonge en un isomorphisme de corps $\tau\colon L \longrightarrow L'$ tel que $\tau(a_j) = a'_{\overline{\pi}(j)}$ pour une certaine bijection $\overline{\pi}\colon \{2, \ldots, n\} \longrightarrow \{1, \ldots, n\} \setminus \{i\}$. En particulier, τ prolonge σ, et il suffit de poser $\pi(1) = i$, $\pi(j) = \overline{\pi}(j)$ pour $j \in \{2, \ldots, n\}$ pour avoir la permutation souhaitée. □

Théorème 3.6 Soit $f \in K[X]$, et $n = \deg(f) \geq 1$.
(i) Il existe un corps de décomposition de f sur K.
(ii) Soient $L = K(a_1, \ldots, a_n)$ et $L' = K(a'_1, \ldots, a'_n)$ deux corps de décomposition de f sur K.
Alors il existe un isomorphisme de corps $\tau\colon L \longrightarrow L'$ tel que $\tau_{|K} = \mathrm{id}_K$ et $\tau(a_i) = a'_{\pi(i)}$ pour une certaine permutation $\pi \in S_n$.

Preuve. (i) C'est le corollaire 1.11.
(ii) Il suffit d'appliquer le lemme 3.5 avec $K = K'$ et $\sigma = \mathrm{id}_K$. □

Exemples. (i) Si $\deg(f) = 1$, n'importe quel corps de décomposition de f sur K a degré 1 sur K et est isomorphe à K.
(ii) N'importe quel corps de décomposition de $X^2 + 1$ sur $\mathbb{R}$ est une extension quadratique de $\mathbb{R}$ et est isomorphe à $\mathbb{C}$.
(iii) Un corps de décomposition de $X^4 - 2$ sur $\mathbb{Q}$ est de degré 8 et est isomorphe à $\mathbb{Q}(\sqrt[4]{2}, i)$.
(iv) L'exemple ci-dessus et le théorème 3.6 impliquent l'existence et l'unicité, à isomorphisme près, d'un corps fini à $q = p^n$ éléments, pour tout premier p et $n \geq 1$.

Les théorèmes 3.3 et 3.6 motivent alors la définition suivante.

Définition 3.7 Soient L/K et L'/K deux extensions. Un morphisme de corps $\sigma\colon L \longrightarrow L'$ (ou isomorphisme, ou automorphisme) tel que $\sigma_{|K} = \mathrm{id}_K$ est appelé un $K-$*morphisme* (ou $K-$isomorphisme, ou $K-$automorphisme).
On note $\mathrm{Hom}(L/K, L'/K)$ (ou $\mathrm{Aut}(L/K, L'/K)$) l'ensemble des $K-$morphismes de L vers L' (ou des $K-$isomorphismes de L vers L').

3.2 Clôture algébrique

Considérons le corps $\mathbb{C}$ des nombres complexes, et la question suivante : quelles sont ses extensions finies ?
Intuitivement, dans $\mathbb{C}$, tout marche bien. N'importe quel polynôme a une racine, donc il n'est pas nécessaire de construire des corps de rupture, et tout polynôme irréductible est de degré 1, donc les extensions de $\mathbb{C}$ de la forme $\mathbb{C}[X]/(f(X))$ sont toutes de degré 1, donc égales à $\mathbb{C}$. En fait, toutes ces propriétés sont équivalentes.

Proposition 3.8 Soit K un corps. Les assertions suivantes sont équivalentes :
(i) Tout polynôme non constant de $K[X]$ est scindé sur K.
(ii) Tout polynôme non constant de $K[X]$ admet une racine dans K.
(iii) Les seuls polynômes irréductibles de $K[X]$ sont ceux de degré 1.
(iv) Toute extension algébrique de K est égale à K.

Preuve. L'implication $(i) \Longrightarrow (ii)$ est claire.
$(ii) \Longrightarrow (iii)$: Soit $f \in K[X]$ irréductible. En particulier, f est non constant, donc il existe $a \in K$ racine de f. Alors $X-a$ divise f, donc $f(X) = g(X)(X-a)$ pour un certain $g(X) \in K[X]$. Comme f est irréductible, $g(X) \in (K[X])^* = K^*$, donc $\deg(g) = 0$, d'où $\deg(f) = 0 + 1 = 1$.
$(iii) \Longrightarrow (ii)$: Soit $f(X) \in K[X]$ non constant. Si $\deg(f) = 1$, alors $f(X) = aX + b$ avec $a \in K^*$ et $b \in K$, et $a^{-1}b \in K$ est une racine de f. Sinon, $\deg(f) \geq 2$ et donc f n'est pas irréductible. Ainsi, il existe deux polynômes g, $h \in K[X]$, de degré au moins 1, tels que $f(X) = g(X)h(X)$. Si g ou h a degré 1 (ou les deux si f a degré 2), alors il a une racine a dans K, et a est aussi une racine pour f. Sinon, g et h ont tous les deux degré au moins 2, et ils sont donc réductibles. On continue alors cette procédure, qui s'arrête en temps fini puisque $\deg(f) < \infty$, jusqu'à avoir un facteur de degré 1 dans la factorisation de f. Ce facteur de degré 1 a une racine dans K, qui est alors une racine pour f.
$(ii) \Longrightarrow (i)$: Soit $f(X) \in K[X]$, et $n := \deg(f)$. On raisonne par récurrence sur n. Si $n = 1$, alors $f(X) = aX + b = a(X - (-a^{-1}b))$ est bien scindé sur K. Soit donc $n > 1$. Par (ii), f a une racine a dans K, donc il existe $g(X) \in K[X]$ tel que $f(X) = (X-a)g(X)$. Alors, $\deg(g) = n - 1 < n$, et par hypothèse de récurrence g est scindé sur K. Ainsi, f est scindé sur K.
$(i) \Longrightarrow (iv)$: Soit L/K algébrique. Soit $a \in L$. Il existe alors un polynôme $f(X) \in K[X]$ annulateur de a. Comme f est scindé sur K, toutes ses racines sont dans K, en particulier $a \in K$. Donc $L \subset K$, et $L = K$.
$(iv) \Longrightarrow (ii)$: Soit $f(X) \in K[X]$ non constant, et soit $g(X)$ un facteur irréductible de f. Par le théorème 3.3, il existe un corps de rupture L pour g, *i.e.* une extension L de K telle que $L = K(a)$ et $g(a) = 0$. En particulier, L/K est algébrique par le corollaire 2.18 puisque a est algébrique sur K. Par hypothèse, on a alors $L = K(a) = K$, donc $a \in K$, et g a une racine dans K, qui est aussi une racine pour f. □

Définition 3.9 Un corps K vérifiant l'une (et donc toutes) des propriétés ci-dessus est appelé *algébriquement clos.*

Exemples. (i) Le corps $\mathbb{C}$ est algébriquement clos, par le théorème fondamental de l'algèbre. En particulier, la seule extension finie de $\mathbb{C}$ est $\mathbb{C}$.
(ii) Un corps algébriquement clos est infini, par l'exercice 11 ci-dessous. En particulier, $\mathbb{F}_{p^n}$ n'est pas algébriquement clos pour tout p premier et $n \geq 1$.

Lemme 3.10 Soient L/K une extension de corps, M un corps algébriquement clos, et $\sigma\colon K \longrightarrow M$ un morphisme de corps.
Pour tout $a \in L$ algébrique sur K, il existe un morphisme de corps $\tau\colon K(a) \longrightarrow M$ qui prolonge σ.

Preuve. Soit $f(X) \in K[X]$ le polynôme minimal de a sur K et notons, comme dans le lemme 3.2, $\tilde{\sigma}\colon K[X] \longrightarrow M[X]$ le prolongement canonique de σ, et $\tilde{f} := \tilde{\sigma}(f)$. Puisque M est algébriquement clos, $\tilde{f}$ a une racine b dans M. Comme f est unitaire et irréductible sur K, $\tilde{f}$ est unitaire et irréductible sur $\sigma(K)$. C'est donc le polynôme minimal de b sur $\sigma(K)$. Par le lemme 3.2, il existe un morphisme $\tau\colon K(a) \longrightarrow \sigma(K)(b)$ tel que $\tau(a) = b$ et $\tau_{|K} = \sigma$. □

Définition 3.11 Soit L/K une extension de corps.
L est une *clôture algébrique* de K si L/K est algébrique et si L est algébriquement clos.

Exemple. Le corps $\mathbb{C}$ est une clôture algébrique de $\mathbb{R}$.

Il convient maintenant de se demander si, étant donné un corps K, une clôture algébrique de K existe toujours. C'est l'objet du théorème suivant, dont la preuve abstraite repose sur l'axiome du choix. Nous l'omettons ici.

Théorème 3.12 (Steinitz) Soit K un corps.
(i) Il existe une clôture algébrique de K.
(ii) Soient L et L' deux clôtures algébriques de K. Alors il existe un $K-$isomorphisme $\sigma\colon L \longrightarrow L'$.

On note alors en général $\overline{K}$ la clôture algébrique de K. Terminons cette section avec la remarque suivante : le théorème de Steinitz permet une deuxième preuve de l'existence d'un corps de décomposition pour un polynôme $f \in K[X] \setminus K$. Il suffit de considérer $K(Z)$, où Z est l'ensemble des racines de f dans $\overline{K}$. Reposant sur le théorème 3.12, cette preuve est, en contrepartie, peu intuitive et constructive. En revanche, la preuve du théorème 3.6 (du corollaire 1.11) donne une méthode explicite pour constuire un corps de décomposition, facilement applicable dans des cas concrets.

3.3 Extensions normales

Définition 3.13 Une extension L/K est appelée *normale* si elle est algébrique et si tout polynôme irréductible de $K[X]$ possédant une racine dans L est scindé dans $L[X]$, autrement dit a toutes ses racines dans L.

Exemples. (i) Toute extension quadratique est normale.
En effet, si $[L : K] = 2$, alors L/K est algébrique et si $f \in K[X]$ est irréductible et a une racine $a \in L$, on a

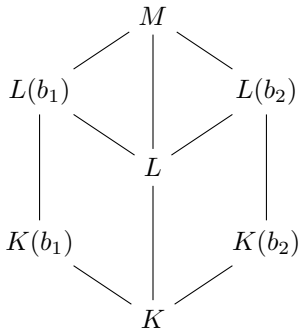
$$\deg(f) = [K(a) : K] \leq [L : K] = 2$$

et un corps de rupture pour f est aussi un corps de décomposition pour f, par les exemples précédents. Donc f a toutes ses racines dans L.
(ii) $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ n'est pas normale, puisque $f = X^4 - 2$ est irréductible dans $\mathbb{Q}[X]$ et a deux racines dans $\mathbb{Q}(\sqrt[4]{2})$, mais ses autres racines sont complexes, et ne sont donc pas dans $\mathbb{Q}(\sqrt[4]{2}) \subset \mathbb{R}$.

Voilà un critère très utile en pratique pour montrer qu'une extension de corps est normale.

Théorème 3.14 Soit L/K une extension finie.
Alors L/K est normale si, et seulement si, L est un corps de décomposition d'un polynôme $f \in K[X] \setminus K$.

Preuve. Supposons pour commencer que L/K est normale. Par le théorème 2.17, L/K est de type fini, donc il existe $a_1, \ldots, a_n \in L$ algébriques sur K tels que $L = K(a_1, \ldots, a_n)$. Soit f_i le polynôme minimal de a_i sur K, et soit $f = f_1 \ldots f_n$. Soit enfin Z l'ensemble des racines de f (qui existe dans $\overline{K}$), et $K(Z)$ un corps de décomposition pour f sur K. Comme f_i est irréductible et a une racine dans L, et que L/K est normale, f_i a toutes ses racines dans L, et donc f a toutes ses racines dans L. Ainsi, $Z \subset L$. Bien sûr, $K \subset L$. Or $K(Z)$ est le plus petit corps contenant K et Z. Par minimalité, on déduit que $K(Z) \subset L$. D'autre part, $\{a_1, \ldots, a_n\} \subset Z$, donc $L = K(a_1, \ldots, a_n) \subset K(Z)$. En conclusion, $L = K(Z)$ est bien le corps de décomposition de f sur K. Réciproquement, supposons qu'il existe un polynôme $f \in K[X]$ non constant dont L est un corps de décomposition. Soit $g \in K[X]$ irréductible et M une extension de L telle que M est un corps de décomposition de g sur L. Soient b_1, $b_2 \in M$ deux racines de g. On a alors les extensions suivantes.



Par le lemme 3.2, avec $K = K'$ et $\sigma = \mathrm{id}_K$, il existe un $K-$isomorphisme de corps $\tau\colon K(b_1) \longrightarrow K(b_2)$. Puisque L est un corps de décomposition de L sur K, $L(b_i)$ est un corps de décomposition de f sur $K(b_i)$, pour $i = 1, 2$. On peut donc

appliquer le lemme 3.5, et prolonger τ en un $K-$isomorphisme de corps $\varphi\colon L(b_1) \longrightarrow L(b_2)$ Comme $\varphi_{|K} = \tau_{|K} = \mathrm{id}_K$, φ est un isomorphisme de $K-$espaces vectoriels, ce qui implique l'égalité des dimensions

$$[L(b_1) : K] = [L(b_2) : K]$$

Par multiplicativité des degrés, on a $[L(b_1) : L][L : K] = [L(b_1) : K] = [L(b_2) : K] = [L(b_2) : L][L : K]$, d'où

$$[L(b_1) : L] = [L(b_2) : L].$$

Supposons maintenant que $b_1 \in L$. Alors $[L(b_1) : L] = 1$, donc $[L(b_2) : L] = 1$, et donc $b_2 \in L$. Cela montre que L/K est normale, et termine la démonstration. □

Exemples. (i) L'extension $\mathbb{Q}(i, \sqrt{3})/\mathbb{Q}$ est normale, puisque c'est un corps de décomposition de $(X^2 + 1)(X^2 - 3)$.
(ii) Par le théorème 1.19, $\mathbb{F}_p[X]/(\pi(X))$, où $\pi(X)$ est irréductible de degré d, est un corps de décomposition de $\pi(X)$ sur $\mathbb{F}_p$. C'est donc une extension normale de $\mathbb{F}_p$.

On déduit alors facilement le corollaire suivant.

Corollaire 3.15 Soit $K \subset L \subset M$ une tour d'extensions, telle que M/K est finie et normale. Alors
(i) M/L est normale.
(ii) Pour tout $K-$morphisme $\tau\colon L \longrightarrow M$, il existe un $K-$automorphisme $\sigma\colon M \longrightarrow M$ tel que $\sigma_{|L} = \tau$.

Preuve. (i) Comme M/K est normale, M est le corps de décomposition sur K d'un polynôme f, par le théorème 3.14. En particulier, M est un corps de décomposition de f sur L.
(ii) M est également un corps de décomposition de f sur $\tau(L) \subset M$. Par le lemme 3.5, il existe un isomorphsime $\sigma\colon M \longrightarrow M$ prolongeant $\tau\colon L \longrightarrow \tau(L)$. De plus, $\sigma_{|K} = \tau_{|K} = \mathrm{id}_K$, *i.e.* σ est un $K-$automorphisme. □

En revanche, dans une tour d'extensions $K \subset L \subset M$ avec M/K normale, l'extension L/K n'est pas normale en général. Par exemple, pour $K = \mathbb{Q}$, $L = \mathbb{Q}(\sqrt[3]{2})$ et $M = \mathbb{Q}(\sqrt[3]{2}, \omega)$, où $\omega = e^{i\frac{2\pi}{3}}$, M/K est bien normale puisque c'est le corps de décomposition de $X^3 - 2$ sur $\mathbb{Q}$, mais L/K n'est pas normale, puisque $X^3 - 2$ a une racine dans L mais ne scinde pas sur L. De plus, la normalité n'est pas transitive en général. Considérons $K = \mathbb{Q}$, $L = \mathbb{Q}(\sqrt{2})$ et $M = \mathbb{Q}(\sqrt[4]{2})$. Les extensions L/K et M/L sont toutes deux quadratiques, donc normales, mais M/K n'est pas normale comme vu ci-dessus.

Définition 3.16 Soit L/K une extension algébrique.
Une *clôture normale* de L/K est une extension M de L telle que :
(i) M/K est normale.
(ii) Pour toute tour d'extensions $K \subset L \subset M' \subset M$ telle que M'/K est normale, on a $M' = M$.

Par exemple, $M = \mathbb{Q}(\sqrt[3]{2}, \omega)$ est une clôture normale de l'extension $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$.

En d'autres termes, une clôture normale de L/K est une extension M de K qui est normale, et qui est la plus petite extension de K avec cette propriété. Une clôture normale existe toujours, et est unique à isomorphisme près.

Théorème 3.17 Soit L/K finie.
(i) Il existe une clôture normale M de L/K telle que M/K est finie.
(ii) Soit N une clôture normale de L/K. Alors il existe un $K-$isomorphisme $\sigma\colon M \longrightarrow N$.

Preuve. Comme L/K est finie, elle est de type finie, et il existe $a_1, \ldots, a_n \in L$ tels que $L = K(a_1, \ldots, a_n)$. Soit alors $f_i \in K[X]$ le polynôme minimal de a_i sur K, et posons $f = f_1 \ldots f_n \in K[X]$.
(i) Soit M un corps de décomposition de f sur L, de sorte que $f = \prod_{i=1}^{r}(X - b_i)$, avec $b_i \in M$, et $M = L(b_1, \ldots, b_r)$. Alors $M = L(b_1, \ldots, b_r) = K(a_1, \ldots, a_n)(b_1, \ldots, b_r) = K(a_1, \ldots, a_n, b_1, \ldots, b_r)$. Comme a_i est une racine de f dans L, donc dans M, a_i est un certain b_j, donc $r \geq n$ et

$$M = K(b_1, \ldots, b_r).$$

Ainsi, M est un corps de décomposition de f sur K. De plus, M/K est de type fini, avec $b_1, \ldots, b_r$ algébriques sur K. Par le théorème 2.17, M/K est finie. Par le théorème 3.14, M/K est normale. Soit ensuite M' tel que $K \subset L \subset M' \subset M$,

avec M'/K normale. Comme f_i a une racine a_i dans L, donc dans M', f_i est scindé sur M', puisque M'/K est normale. Ainsi f est scindé sur M'. Donc M' contient toutes les racines de f, d'où $M' \supset K(b_1, \ldots, b_r) = M$. On conclut que $M' = M$.
(ii) Soit N une autre clôture normale de L/K. Alors chaque f_i est scindé sur M et sur N, et donc f est scindé sur M et sur N. Soient $b_1, \ldots, b_r$ les racines de f dans M et $c_1, \ldots, c_r$ les racines de f dans N. Posons $M' = K(b_1, \ldots, b_r)$ et $N' = K(c_1, \ldots, c_r)$. Alors $L \subset M'$, $L \subset N'$ et M'/K, N'/K sont normales. Par minimalité, on a donc $M' = M$ et $N' = N$. Ainsi, M et N sont deux corps de décomposition de f sur K, et par le lemme 3.5 il existe un $K-$isomorphisme $\sigma\colon M \longrightarrow N$. □

Donnons pour terminer cette section une autre caractérisation des extensions normales finies.

Théorème 3.18 Soit L/K une extension finie.
Alors L/K est normale si, et seulement si, pour toute tour d'extensions $K \subset L \subset M$ et tout $K-$morphisme $\sigma\colon L \longrightarrow M$, on a $\sigma(L) = L$.

Preuve. Supposons L/K normale. Soit $a \in L$ et $f \in K[X]$ le polynôme minimal de a sur K. Alors $f(a) = 0$, donc $\sigma(f(a)) = 0$ et comme σ est un morphisme de corps fixant les coefficients de f, cette égalité s'écrit aussi $f(\sigma(a)) = 0$. Donc $\sigma(a)$ est aussi une racine de f, et comme L/K est normale, on déduit $\sigma(a) \in L$. Cela montre $\sigma(L) \subset L$. De plus, $\sigma\colon L \longrightarrow \sigma(L)$ est un isomorphsime de $K-$espaces vectoriels, donc $[\sigma(L) : K] = [L : K]$. Combinant cela avec $\sigma(L) \subset L$, on déduit $\sigma(L) = L$. Réciproquement, soit $f \in K[X]$ irréductible et $a \in L$ tel que $f(a) = 0$. Soit M une clôture normale de L/K. Puisque $a \in M$, et que M/K est normale, f est scindé sur M. Soit $a' \in M$ tel que $f(a') = 0$. Par le lemme 3.2, il existe un $K-$isomorphisme $\tau\colon K(a) \longrightarrow K(a')$ tel que $\tau(a) = a'$. D'après le corollaire 3.15(ii), il existe un $K-$automorphisme $\sigma\colon M \longrightarrow M$ tel que $\sigma_{|K(a)} = \tau$. Par hypothèse, on a $\sigma(L) = L$. Ainsi,

$$a' = \tau(a) = \sigma(a) \in \sigma(L) = L$$

et donc L/K est normale. □

3.4 Extensions séparables

Soit L/K une extension de corps. Pour $f = \sum_{i=0}^{n} c_i X^i \in K[X]$, on note $f' := \sum_{i=1}^{n} i c_i X^{i-1}$ le polynôme dérivé de f. L'application $f \longmapsto f'$ est $K-$linéaire et on a, pour tous $f, g \in K[X]$, $(fg)' = f'g + fg'$. Rappelons de plus qu'une racine $a \in L$ de $f \in K[X]$ est une racine *multiple* de f si $(X - a)^2$ divise f dans $L[X]$, et *simple* sinon.

Lemme 3.19 Soit $f \in K[X] \setminus K$ et $a \in L$ tel que $f(a) = 0$.
(i) L'élément $a \in L$ est une racine multiple de f si, et seulement si, $f'(a) = 0$.
(ii) Supposons que f est irréductible. Alors a est une racine multiple de f si, et seulement si, $f' = 0$.

Preuve. Comme a est une racine de f, on peut écrire $f(X) = (X - a)^r g(X)$, où $g(X) \in K[X]$ est tel que $g(a) \neq 0$. Alors $f'(X) = r(X - a)^{r-1} g(X) + (X - a)^r g'(X)$.
(i) Si a est une racine multiple de f, $r \geq 2$, et $f'(a) = 0$. Si a est une racine simple de f, $r = 1$, et $f'(a) = g(a) \neq 0$.
(ii) Supposons que a est une racine multiple de f, donc $f'(a) = 0$ par (i). Posons $I := (f(X)) + (f'(X))$. Alors $(f(X)) \subset I$, et pour tout $h \in I$, $h(a) = 0$, donc I ne contient pas les polynômes constants. En particulier, $I \neq K[X]$. Comme f est irréductible, $(f(X))$ est maximal dans $K[X]$, donc le fait que $(f(X)) \subseteq I \subsetneq K[X]$ implique $I = (f(X))$. Cela entraîne que $f' \in I = (f(X))$. Comme $\deg(f') < \deg(f)$, on a forcément $f' = 0$. Réciproquement, si $f' = 0$, alors $f'(a) = 0$, donc a est une racine multiple de f par (i). □

Définition 3.20 Soit $f \in K[X] \setminus K$.
Le polynôme f est *séparable* s'il n'a que des racines simples dans un corps de décomposition de f sur K. Sinon, f est dit *inséparable*.

Le lemme 3.19 dit précisément que, si f est irréductible, alors f est inséparable si et seulement si $f' = 0$.

Exemples. (i) Le polynôme $X^2 + 1 \in \mathbb{Q}[X]$ est séparable, de même que $X^4 + 1$.
(ii) De même, $X^2 - X \in \mathbb{R}[X]$ est séparable.

(*iii*) Dans $\mathbb{F}_3[X]$, $X^3+1=(X+1)^3$ n'est pas séparable.
(*iv*) Soit p un premier et $K=\mathbb{F}_p(Y)$, le corps des fractions rationnelles en Y sur $\mathbb{F}_p$. Soit $f(X)=X^p-Y\in K[X]$. Alors f est irréductible par Eisenstein (proposition 1.8(*i*)). On a $f'=pX^{p-1}=0$, donc f est inséparable par le lemme 3.19.

La proposition suivante donne deux critères utiles pour détecter la séparabilité de beaucoup de polynômes.

Proposition 3.21 Soit K un corps.
(*i*) Si $\mathrm{char}(K)=0$, alors tout polynôme irréductible de $K[X]$ est séparable.
(*ii*) Si $\mathrm{char}(K)=p$, alors un irréductible $f\in K[X]$ est séparable si, et seulement si, $f\notin K[X^p]$.

Preuve. (*i*) Soit $f\in K[X]$ irréductible. En particulier, f est non constant. Donc $f'\neq 0$ puisque $\mathrm{char}(K)=0$. Ainsi, f est séparable par le lemme 3.19.
(*ii*) Soit $f\in K[X]$ irréductible. On montre que f est inséparable si et seulement si $f\in K[X^p]$. Si f est inséparable, alors $f'=0$. En écrivant $f(X)=c_nX^n+c_{n-1}X^{n-1}+\cdots+c_1X+c_0$, la condition $f'=0$ signifie que $ic_i=0$ dans K pour tout $0\leq i\leq n$. Cela implique que p divise i si $c_i\neq 0$, donc les coefficients non-nuls de f sont ceux devant les monômes de degré divisible par p. En particulier, $n=\deg(f)$ est un multiple de p, que l'on écrit $n=pm$. On a alors

$$f(X)=c_{pm}(X^p)^m+c_{p(m-1)}(X^p)^{m-1}+\cdots+c_pX^p+c_0=g(X^p)$$

avec $g\in K[X]$. Ainsi, $f\in K[X^p]$. Réciproquement, si $f\in K[X^p]$, alors $f(X)=g(X^p)$, où $g\in K[X]$. Alors $f'=pX^{p-1}g'(X^p)=0$, et f est inséparable par le lemme 3.19. □

Exemple. Soit $K=\mathbb{F}_3(Y)$, et soient $f(X)=X^7+Y^2X^5+Y$, $g(X)=X^6+YX^3+Y$. Alors f et g sont tous deux irréductibles, par le critère d'Eisenstein généralisé avec $\pi(Y)=Y$. Cependant, f est séparable puisque ce n'est pas un polynôme en X^3, alors que $g(X)=h(X^3)$, où $h(X)=X^2+YX+Y$, est inséparable par la proposition 3.21. On peut aussi directement appliquer le lemme 3.19 pour montrer que f est séparable : sa dérivée $f'(X)=X^6+2Y^2X^4$ est non-identiquement nulle.

Définition 3.22 Soit L/K une extension de corps.
(*i*) Un élément $a\in L$ est *séparable sur* K si a est algébrique sur K et si le polynôme minimal de a sur K est séparable.
(*ii*) L'extension L/K est *séparable* si tout $a\in L$ est séparable sur K.

En particulier, une extension séparable est toujours algébrique.

Exemples. (*i*) Les nombres $\sqrt{2}$ et $\sqrt{3}$ sont séparables sur $\mathbb{Q}$, puisque leurs polynômes minimaux X^2-2 et X^2-3 sont tous deux séparables sur $\mathbb{Q}$.
(*ii*) Soient p un nombre premier et $K=\mathbb{F}_p(Y)$, le corps des fractions rationnelles en Y sur $\mathbb{F}_p$.
Soient $f(X)=X^p-Y\in K[X]$, et $L=K[X]/(f(X))$. Alors l'élément $a:=X+(f(X))\in L$ a pour polynôme minimal f sur K, qui n'est pas séparable, donc a n'est pas séparable sur K, et l'extension L/K n'est pas séparable.

Définition 3.23 Un corps K est appelé *parfait* si toutes ses extensions algébriques sont séparables.

Exemples. (*i*) Si $\mathrm{char}(K)=0$, alors K est parfait, par la proposition 3.21(*i*). En particulier, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ sont parfaits.
(*ii*) L'exemple ci-dessus montre précisément que $K=\mathbb{F}_p(Y)$ n'est pas parfait, puisque l'extension L/K, avec $L=K[X]/(f(X))$ et $f(X)=X^p-Y$, est finie, donc algébrique, mais inséparable.

Remarquons ensuite que les sous-extensions d'une extension séparable sont séparables. Plus précisément, si $K\subset L\subset M$ est une tour d'extensions avec M/K séparable, alors M/L et L/K sont séparables. En effet, L/K est clairement séparable. De plus, si $a\in M$, le polynôme minimal g de a sur L divise le polynôme minimal f de a sur K. Comme f est séparable, puisque M/K est séparable, g l'est aussi. Un des buts de cette section est d'établir la réciproque de ce résultat, la transitivité de la séparabilité : si L/K et M/L sont séparables, alors M/K est séparable.

On donne maintenant deux critères importants pour montrer qu'un corps est parfait.

Proposition 3.24 Soit K un corps. Les assertions suivantes sont équivalentes :
(i) K est parfait.
(ii) Tout polynôme irréductible de $K[X]$ est séparable.
(iii) $\overline{K}/K$ est séparable.

Preuve. $(i) \implies (ii)$: Soit $f \in K[X]$ irréductible. Alors $L := K[X]/(f(X))$ est un corps, et L/K est une extension finie de K, donc algébrique, donc séparable puisque K est parfait. En particulier, l'élément $a := X + (f(X)) \in L$ est séparable, et f est son polynôme minimal, donc f est séparable.
$(ii) \implies (iii)$: Soit $\alpha \in \overline{K}$. Alors α est algébrique sur K, et son polynôme minimal est irréductible dans $K[X]$, donc séparable par hypothèse. Ainsi α est séparable sur K, et $\overline{K}/K$ est séparable.
$(iii) \implies (i)$: Soit L/K une extension algébrique. On a la tour d'extensions $K \subset L \subset \overline{K}$, et comme $\overline{K}/K$ est séparable, L/K est séparable. Ainsi K est parfait. □

Proposition 3.25 Soit K un corps. K est parfait si, et seulement si, $\mathrm{char}(K) = 0$ ou $\mathrm{char}(K) = p \neq 0$ et $K = K^p$.

Preuve. $\Longleftarrow$: Si $\mathrm{char}(K) = 0$, K est parfait comme vu ci-dessus. Supposons donc $\mathrm{char}(K) = p \neq 0$ et $K = K^p$. Par la proposition 3.24, pour montrer que K est parfait, il suffit de montrer que tout polynôme irréductible de $K[X]$ est séparable. Soit donc $f \in K[X]$ irréductible. Par l'absurde, supposons f inséparable. Par la proposition 3.21(ii), f est un polynôme en X^p : $f(X) = \sum_{j=0}^{m} b_j X^{pj}$. Par hypothèse, $K = K^p$, donc pour tout $0 \leq j \leq m$, il existe $a_j \in K$ tel que $a_j^p = b_j$. Ainsi

$$f(X) = \sum_{j=0}^{m} b_j X^{pj} = \sum_{j=0}^{m} a_j^p X^{pj} = \left(\sum_{j=0}^{m} a_j X^j \right)^p$$

ce qui contredit l'irréductibilité de f. Ainsi, f est séparable, et comme expliqué ci-dessus, K est parfait.
$\Longrightarrow$: On montre la contraposée. Si $K \neq K^p$ alors, comme $K^p \subset K$, on peut choisir $a \in K \setminus K^p$. Alors le polynôme $X^p - a$ a une seule racine dans un corps de décomposition : si $\alpha^p = a$, alors $X^p - a = X^p - \alpha^p = (X - \alpha)^p$. De plus, $X^p - a$ est irréductible dans $K[X]$: un facteur non trivial unitaire de $X^p - a$ est de la forme $(X - \alpha)^m$, pour un certain $m \in \{1, \ldots, p-1\}$. Le coefficient de X^{m-1} dans $(X - \alpha)^m$ est $-m\alpha$, donc $-m\alpha \in K$, donc $\alpha \in K$, donc $a = \alpha^p \in K^p$, une contradiction. Ainsi, $X^p - a$ est un polynôme irréductible et inséparable de $K[X]$, donc K n'est pas parfait par la proposition 3.24. □

Corollaire 3.26 Les corps finis sont parfaits.

Preuve. Soit K un corps fini, de caractéristique $p > 0$ un nombre premier. L'application $x \longmapsto x^p$ est injective, puisque

$$a^p = b^p \implies 0 = a^p - b^p = (a - b)^p \implies a - b = 0 \implies a = b$$

Comme K est fini, $x \longmapsto x^p$ est donc aussi surjective, et ainsi $K = K^p$. On conclut que K est parfait par la proposition 3.25. □

Le théorème suivant est crucial, et décrit précisément la structure des extensions finies séparables.

Théorème 3.27 (de l'élément primitif) Soit L/K une extension finie et séparable. Alors il existe $a \in L$ tel que $L = K(a)$. En particulier, si $\mathrm{char}(K) = 0$ et si L/K est finie, alors il existe $a \in L$ tel que $L = K(a)$.

Un élément $a \in L$ générateur d'une extension L/K est appelé élément primitif.

Preuve. On distingue les cas K fini et K infini.
(i) Si K est fini, alors L est aussi fini puisque L/K est finie. Ainsi, par l'exercice 23, L^* est cyclique, donc il existe $a \in L^*$ tel que $L^* = \langle a \rangle$. Alors $L = K(a)$, et L est simple.
(ii) Supposons alors que K est infini. Par le théorème 2.17, il existe $a_1, \ldots, a_n \in L$ tels que $L = K(a_1, \ldots, a_n)$. Comme L/K est séparable, $a_1, \ldots, a_n$ sont séparables sur K. Si $n = 1$, alors $L = K(a_1)$ et la preuve est terminée. Supposons $n = 2$, et notons $a_1 = b$, $a_2 = c$. Soient f et g les polynômes minimaux de b et c sur K respectivement, et notons $l = \deg(f)$, $m = \deg(g)$. Soit M la clôture normale de L/K. Dans $M[X]$, on a les décompositions

$$f(X) = \prod_{i=1}^{l} (X - b_i), \; g(X) = \prod_{j=1}^{m} (X - c_j)$$

où b_i, $c_j \in M$ et $b_1 = b$, $c_1 = c$. Puisque f et g sont séparables, les b_i, respectivement les c_j, sont deux-à-deux distincts. Considérons le polynôme h défini comme

$$h(X) = \prod_{i=2}^{l} \prod_{j=1}^{m} ((b - b_i)X + (c - c_j)) \in M[X]$$

Puisque $h \neq 0$ et que K est infini, il existe $d \in K^*$ tel que $h(d) \neq 0$. Posons alors $a := bd + c \in L$. Par substitution de variable, on a $g(a - dX) = \prod_{j=1}^{m} (a - dX - c_j)$ et on voit que b est racine de $g(a - dX)$:

$$g(a - db) = \prod_{j=1}^{m} (a - db - c_j) = \prod_{j=1}^{m} (c - c_j) = g(c) = 0.$$

De plus, on a $h(d) = \prod_{i=2}^{l} \prod_{j=1}^{m} ((b - b_i)d + (c - c_j)) = \prod_{i=2}^{l} \prod_{j=1}^{m} (a - b_i d - c_j) = \prod_{i=2}^{l} g(a - db_i)$ et comme $h(d) \neq 0$, b_i n'est pas racine de $g(a - dX)$ si $i \geq 2$. Comme $f(X)$ et $g(a - dX)$ ont une seule racine en commun, on en déduit que $\mathrm{pgcd}_{M[X]}(f(X), g(a - dX)) = X - b$, et en fait $\mathrm{pgcd}_{K(a)[X]}(f(X), g(a - dX)) = X - b$. Cela implique $b \in K(a)$, et donc aussi $c \in K(a)$. Finalement, on conclut que $K(b, c) = K(a)$, et le théorème est démontré pour le cas $n = 2$. Pour le cas général, on raisonne par récurrence en utilisant que $K(a_1, \ldots, a_n) = K(a_1, \ldots, a_{n-1})(a_n)$ et le cas $n = 2$. □

Néanmoins, pour une extension finie et séparable, l'unicité de l'élément primitif est en général fausse. Un exemple est donné par l'exercice 26 ci-dessous.

Exemple. L'extension $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$ est finie et séparable, et égale à $\mathbb{Q}(\sqrt{2} + \sqrt{3})$.

On va maintenant donner une autre caractérisation des extensions séparables finies, qui repose sur un lien entre la séparabilité et le nombre de prolongements de morphismes de corps. Pour motiver ce lien, voici deux exemples.
Il y a deux façons de plonger $\mathbb{Q}(\sqrt{2})$ dans $\mathbb{R}$: envoyer $\sqrt{2}$ sur lui-même ou sur son opposé. Le fait qu'il y ait deux plongements est dû au fait qu'il y a deux racines de $X^2 - 2$ dans $\mathbb{R}$. De même, il y a deux façons de plonger $\mathbb{Q}(\sqrt{2})$ dans $\mathbb{C}$. En revanche, il n'y a qu'une seule façon de plonger $\mathbb{Q}(\sqrt[3]{2})$ dans $\mathbb{R}$, puisqu'il n'y a qu'une seule racine de $X^3 - 2$ dans $\mathbb{R}$. Si on élargit le corps d'arrivée à $\mathbb{C}$, on obtient les deux autres racines de $X^3 - 2$, et il y a trois manières de plonger $\mathbb{Q}(\sqrt[3]{2})$ dans $\mathbb{C}$. Le nombre de plongements de $\mathbb{Q}(\sqrt{2})$ et $\mathbb{Q}(\sqrt[3]{2})$ dans $\mathbb{R}$ et $\mathbb{C}$ est lié au nombres de racines différentes de $X^2 - 2$ et $X^3 - 2$ dans $\mathbb{R}$ et $\mathbb{C}$, et le fait que le nombre de racines différentes soit égal au degré du polynôme vient du fait que ces polynômes sont séparables.

Lemme 3.28 Soit $K \subset L \subset M \subset N$ une tour d'extensions, avec N/K normale et finie.
(i) $|\mathrm{Hom}(L/K, N/K)| < \infty$.
(ii) $|\mathrm{Hom}(M/K, N/K)| = |\mathrm{Hom}(M/L, N/L)||\mathrm{Hom}(L/K, N/K)|$.

Preuve. (i) Par le théorème 2.17, comme L/K est finie, on peut écrire $L = K(a_1, \ldots, a_n)$ avec $a_i \in L$ algébriques sur K. Soit f_i le polynôme minimal de a_i sur K. Un élément $\sigma \in \mathrm{Hom}(L/K, N/K)$ est uniquement déterminé par $\sigma(a_1), \ldots, \sigma(a_n)$. Comme $\sigma(a_i)$ doit être une racine de f_i, il n'y a qu'un nombre fini de possibilités.
(ii) Notons explicitement $\mathrm{Hom}(L/K, N/K) = \{\sigma_1, \ldots, \sigma_r\}$ et $\mathrm{Hom}(M/L, N/L) = \{\rho_1, \ldots, \rho_s\}$, sans répétitions. Par le corollaire 3.15(ii), chaque σ_i s'étend en un $K-$automorphisme de N, *i.e.* il existe $\sigma_i' \in \mathrm{Aut}(N/K)$ tel que $\sigma_{i|L}' = \sigma_i$. Pour établir l'affirmation voulue, on va montrer que $\mathrm{Hom}(M/K, N/K) = \{\sigma_i' \circ \rho_j \mid 1 \leq i \leq r, 1 \leq j \leq s\}$, sans répétitions. Soit $\varphi \in \mathrm{Hom}(M/K, N/K)$. Alors $\varphi_{|L} \in \mathrm{Hom}(L/K, N/K)$, donc $\varphi_{|L} = \sigma_i$ pour un certain $i \in \{1, \ldots, r\}$. Alors $(\sigma_i')^{-1} \circ \varphi \colon M \longrightarrow N$ est un $L-$morphisme de corps, donc $(\sigma_i')^{-1} \circ \varphi = \rho_j$ pour un certain $j \in \{1, \ldots, s\}$. Il suit que $\varphi = \sigma_i' \circ \rho_j$. L'autre inclusion étant claire, on a l'égalité voulue. Pour voir que cette liste est sans répétitions, on montre que

$$\sigma_i' \circ \rho_j = \sigma_k' \circ \rho_l \Longleftrightarrow (i, j) = (k, l)$$

Clairement, si $(i, j) = (k, l)$, alors $\sigma_i' \circ \rho_j = \sigma_k' \circ \rho_l$. Réciproquement,

$$\begin{aligned} \sigma_i' \circ \rho_j = \sigma_k' \circ \rho_l &\Longrightarrow \sigma_{i|L}' = \sigma_{k|L}' \\ &\Longrightarrow \sigma_i = \sigma_k \\ &\Longrightarrow i = k \\ &\Longrightarrow \rho_j = \rho_l \end{aligned}$$

$$\implies j = l$$

Ainsi, $\mathrm{Hom}(M/K, N/K) = \{\sigma_i' \circ \rho_j \mid 1 \leq i \leq r, 1 \leq j \leq s\}$ sans répétitions et on déduit

$$|\mathrm{Hom}(M/K, N/K)| = |\{\sigma_i' \circ \rho_j \mid 1 \leq i \leq r, 1 \leq j \leq s\}| = rs = |\mathrm{Hom}(M/L, N/L)||\mathrm{Hom}(L/K, N/K)|$$

ce qui conclut la preuve. □

Théorème 3.29 Soit $K \subset L \subset N$ une tour d'extensions avec N/K normale et finie. Soit $a \in L$.
Alors on a

$$|\mathrm{Hom}(K(a)/K, N/K)| \leq [K(a) : K].$$

De plus, les assertions suivantes sont équivalentes :
(i) $|\mathrm{Hom}(K(a)/K, N/K)| = [K(a) : K]$.
(ii) $K(a)/K$ est séparable.
(iii) a est séparable sur K.

Preuve. Soit $a \in L$ et f son polynôme minimal sur K. Soit $Z := \{b \in N \mid f(b) = 0\}$ l'ensemble des racines de f dans N. Un élément $\sigma \in \mathrm{Hom}(K(a)/K, N/K)$ est uniquement déterminé par $\sigma(a)$. Comme $\sigma(a) \in N$, on a

$$|\mathrm{Hom}(K(a)/K, N/K)| = |Z| \leq \deg(f) = [K(a) : K].$$

$(i) \iff (iii)$: On a égalité dans l'inégalité précédente si Z compte $\deg(f)$ éléments, *i.e.* si toutes les racines de f sont simples. Donc $|\mathrm{Hom}(K(a)/K, N/K)| = [K(a) : K] \iff f$ est séparable $\iff a$ est séparable sur K.
$(ii) \implies (iii)$ est évident.
$(iii) \implies (ii)$: Soit $b \in K(a)$. On a $[K(a) : K] = [K(a) : K(b)][K(b) : K]$ et, par le lemme 3.28 avec la tour $K \subset K(b) \subset K(a) \subset N$,

$$|\mathrm{Hom}(K(a)/K, N/K)| = |\mathrm{Hom}(K(a)/K(b), N/K(b))||\mathrm{Hom}(K(b)/K, N/K)|.$$

Soit f le polynôme minimal de a sur K et g le polynôme minimal de a sur $K(b)$. Alors g divise f dans $K(b)[X]$, et comme f est séparable, g l'est aussi. a est donc séparable sur K et sur $K(b)$, et en utilisant l'implication $(iii) \implies (i)$, cela donne que $|\mathrm{Hom}(K(a)/K, N/K)| = [K(a) : K]$ et $|\mathrm{Hom}(K(a)/K(b), N/K(b))| = [K(a) : K(b)]$. Combinant ces deux égalités avec ce qui précède, on obtient

$$|\mathrm{Hom}(K(b)/K, N/K)| = [K(b) : K]$$

et, en utilisant cette fois l'implication $(i) \implies (iii)$, on conclut que b est séparable sur K. □

Comme une extension finie est une suite finie d'extensions monogènes, on peut facilement généraliser ce théorème par récurrence.

Théorème 3.30 Soit $K \subset L \subset N$ une tour d'extensions avec N/K normale et finie.
Alors on a

$$|\mathrm{Hom}(L/K, N/K)| \leq [L : K].$$

De plus, les assertions suivantes sont équivalentes :
(i) $|\mathrm{Hom}(L/K, N/K)| = [L : K]$.
(ii) L'extension L/K est séparable.

Preuve. On raisonne par récurrence sur $[L : K]$. Si $[L : K] = 1$, alors $L = K$ et il n'y a rien à montrer. Supposons $[L : K] > 1$. Soit $a \in L \setminus K$ et la tour d'extension $K \subset K(a) \subset L \subset N$. Par le lemme 3.28, $|\mathrm{Hom}(L/K, N/K)| = |\mathrm{Hom}(L/K(a), N/K(a))||\mathrm{Hom}(K(a)/K, N/K)|$. Or $[L : K(a)] < [L : K]$, donc par hypothèse de récurrence, $|\mathrm{Hom}(L/K(a), N/K(a)$ $[L : K(a)]$, et par le théorème 3.29, $|\mathrm{Hom}(K(a)/K, N/K)| \leq [K(a) : K]$. On obtient alors

$$|\mathrm{Hom}(L/K, N/K)| = |\mathrm{Hom}(L/K(a), N/K(a))||\mathrm{Hom}(K(a)/K, N/K)| \leq [L : K(a)][K(a) : K] = [L : K].$$

$(i) \implies (ii)$: Supposons $|\mathrm{Hom}(L/K, N/K)| = [L : K]$. Soit $a \in L$, et la tour d'extensions $K \subset K(a) \subset L \subset N$. Par le théorème 3.29, pour montrer que a est séparable sur K, il suffit de voir que $|\mathrm{Hom}(K(a)/K, N/K)| = [K(a) : K]$. On remarque que

$$[L : K(a)][K(a) : K] = [L : K]$$

$$
\begin{aligned}
&= |\mathrm{Hom}(L/K, N/K)| \\
&= |\mathrm{Hom}(L/K(a), N/K(a))||\mathrm{Hom}(K(a)/K, N/K)| \\
&\leq [L : K(a)]|\mathrm{Hom}(K(a)/K, N/K)|
\end{aligned}
$$

La deuxième égalité est l'hypothèse, la troisième est le lemme 3.28, et l'inégalité est le premier point de cette preuve. Cela implique que $[K(a) : K] \leq |\mathrm{Hom}(K(a)/K, N/K)|$. Or par le théorème 3.29, on a l'inégalité inverse

$$|\mathrm{Hom}(K(a)/K, N/K)| \leq [K(a) : K]$$

donc $|\mathrm{Hom}(K(a)/K, N/K)| = [K(a) : K]$, et a est séparable sur K.
$(ii) \Longrightarrow (i)$: Par le théorème 2.17, on peut écrire $L = K(a_1, \ldots, a_n)$ avec a_i algébrique sur K. Considérons alors la tour d'extensions $K \subset K(a_1) \subset K(a_1, a_2) \subset ... \subset K(a_1, \ldots, a_n) = L$. Pour simplifier, notons $K_i = K_{i-1}(a_i)$, pour tout $1 \leq i \leq n$, et $K_0 := K$. Soit f_i le polynôme minimal de a_i sur K. Le polynôme minimal g_i de a_i sur K_{i-1} divise f_i, et comme f_i est séparable puisque L/K est séparable, g_i l'est aussi. Donc a_i est séparable sur K_{i-1}, ce qui implique $|\mathrm{Hom}(K_i/K_{i-1}, N/K_{i-1})| = [K_i : K_{i-1}]$ par le théorème 3.29. Ainsi,

$$[L : K] = [K_n : K] = \prod_{i=1}^{n} [K_i : K_{i-1}] = \prod_{i=1}^{n} |\mathrm{Hom}(K_i/K_{i-1}, N/K_{i-1})| = |\mathrm{Hom}(L/K, N/K)|,$$

où la dernière égalité découle d'une itération du lemme 3.28(ii). □

On obtient le corollaire suivant, dont le point (i) est la transitivité de la séparabilité.

Corollaire 3.31 Soit L/K une extension finie.
(i) Soit $K \subset K' \subset L$ une tour d'extensions.
L'extension L/K est séparable si, et seulement si, K'/K et L/K' sont séparables.
(ii) Soit $L = K(a_1, \ldots, a_n)$ avec $a_1, \ldots, a_n$ algébriques sur L.
Alors L/K est séparable si, et seulement si, $a_1, \ldots, a_n$ sont séparables sur K.
(iii) L'ensemble $\{a \in L \mid a \quad \text{est séparable sur} \quad K\}$ est un sous-corps de L, appelé la clôture séparable de K dans L.

Preuve. $(i) \Longrightarrow$ a été montré ci-dessus.
$\Longleftarrow$: Supposons K'/K, L/K' séparables, et soit N la clôture normale de L/K. Le théorème 3.30 implique que $[L : K'] = |\mathrm{Hom}(L/K', N/K')|$ et $[K' : K] = |\mathrm{Hom}(K'/K, N/K)|$. Par le lemme 3.28 et la multiplicativité des degrés, on obtient

$$[L : K] = [L : K'][K' : K] = |\mathrm{Hom}(L/K', N/K')||\mathrm{Hom}(K'/K, N/K)| = |\mathrm{Hom}(L/K, N/K)|$$

ce qui prouve que L/K est séparable, par le théorème 3.30.
$(ii) \Longrightarrow$ est clair.
$\Longleftarrow$: On raisonne par récurrence sur n le nombre de générateurs.
Si $n = 1$, alors $L = K(a_1)$, et si a_1 est séparable sur K, alors L/K est séparable par le théorème 3.29. Si $n > 1$, supposons sans restriction que $a_1 \notin K$, et notons $K' = K(a_1)$, de sorte que K'/K est séparable. Comme $a_2, \ldots, a_n$ sont séparables sur K, ils le sont également sur K', et l'hypothèse de récurrence implique que L/K' est séparable. Par (i), on conclut que L/K est séparable.
(iii) Soient $a, b \in L$ séparables sur K. Alors $K(a, b)/K$ est séparable par (ii), et contient $a + b$, ab et a^{-1} si $a \neq 0$. La séparabilité est donc préservée par les lois de composition de corps. □

3.5 Exercices

Exercice 1. Soient $f(X) = X^2 - 2$ et $g(X) = X^2 - 4X + 2 \in \mathbb{Q}[X]$.
Montrer que f et g sont irréductibles dans $\mathbb{Q}[X]$. Montrer qu'ils ont tous deux un corps de rupture contenu dans $\mathbb{R}$, que l'on notera $\mathbb{Q}(a)$ et $\mathbb{Q}(b)$ respectivement. Comparer $\mathbb{Q}(a)$ et $\mathbb{Q}(b)$.

Exercice 2. Soit K un corps, $f \in K[X]$ et $n := \deg(f) \geq 1$.

(i) Montrer que f est irréductible dans $K[X]$ si, et seulement si, pour toute extension L/K avec $[L : K] \leq \frac{n}{2}$, f n'a pas de racines dans L.
(ii) Supposons f irréductible, et soit L/K une extension de degré $[L : K] = m$. Montrer que si m et n sont premiers entre eux, alors f est irréductible dans $L[X]$.
(iii) Déduire que $X^5 - 9X^3 + 15X + 6$ est irréductible sur $\mathbb{Q}(\sqrt{2}, \sqrt{3})$.

Exercice 3. Déterminer un corps de décomposition des polynômes suivants de $\mathbb{Q}[X]$, et calculer les degrés d'extension correspondants.

(i) $X^4 - 1$
(ii) $X^4 + 1$
(iii) $X^4 - 4X^2 + 2$
(iv) $(X^2 - 2)(X^2 + 3)$
(v) $X^3 - 5X^2 + 9X - 5$

Exercice 4. Soit p un nombre premier, $n \geq 1$, et $q = p^n$. Soit $f(X) = X^q - X \in \mathbb{F}_p[X]$.

(i) Montrer que L est un corps fini à q éléments si, et seulement si, L est un corps de décomposition de f sur $\mathbb{F}_p$.
(ii) En déduire l'existence et l'unicité, à isomorphisme près, d'un corps fini à q éléments.

Exercice 5. Soient $P(X) = X^2 + 1$, $Q(X) = X^2 - 1$ et $R(X) = X^2 - 2$.
Déterminer le corps de décomposition de P, Q et R sur $\mathbb{F}_3$ et sur $\mathbb{F}_5$.

Exercice 6. Trouver un polynôme de $\mathbb{Q}[X]$ dont le corps de décomposition est $\mathbb{Q}(i + \sqrt{3})$.

Exercice 7. Soient K un corps, $f \in K[X]$, et $n := \deg(f) \geq 1$. Soit L un corps de décomposition de f sur K.
Montrer que $[L : K]$ divise $n!$.

Exercice 8. Soient p un premier, et $n, m \geq 1$.
Montrer que $\mathbb{F}_{p^m}$ est une extension de $\mathbb{F}_{p^n}$ si, et seulement si, n divise m.

Exercice 9. Pour p un premier, représenter tous les sous-corps entre $\mathbb{F}_p$ et $\mathbb{F}_{p^{18}}$.

Exercice 10. Montrer que $X^3 + X + 1$ est irréductible sur $\mathbb{F}_2$.
Montrer ensuite qu'il est irréductible sur $\mathbb{F}_{16}$, puis sur $\mathbb{F}_{32}$. Est-il irréductible sur $\mathbb{F}_{64}$?

Exercice 11. Montrer qu'un corps algébriquement clos est infini.

Exercice 12. Soient L un corps algébriquement clos, K un sous-corps de L.

(i) Montrer que le corps $\tilde{K} = \{a \in L \mid a \quad \text{algébrique sur} \quad K\}$ est une clôture algébrique de K.
(ii) Montrer que toute extension finie de $\mathbb{Q}$ est isomorphe à un sous-corps de $\tilde{\mathbb{Q}}$.

Exercice 13. Soit p un nombre premier, $K_0 = \mathbb{F}_p$ et $K_n = \mathbb{F}_{p^{n!}}$ pour tout $n \geq 1$, réalisé comme un corps de décomposition de $X^{p^{n!}} - X$ sur $\mathbb{F}_p$.

(i) Montrer que $K_{n-1} \subset K_n$ pour tout $n \geq 1$.
(ii) Soit $\overline{\mathbb{F}_p} := \bigcup_{n \geq 0} K_n$, $d \geq 1$ et $q = p^d$. Montrer que $\overline{\mathbb{F}_p}$ est une clôture algébrique de $\mathbb{F}_q$.

Exercice 14. Montrer que $\mathbb{Q}(\sqrt{2}, i\sqrt{3}, \sqrt[3]{5})$ est une extension normale de $\mathbb{Q}$. Quelle est son degré ?

Exercice 15. Sans utiliser le corollaire 3.15, montrer que $\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q}(\sqrt[3]{2})$ est normale.

Exercice 16. Les extensions suivantes sont-elles normales ?

(i) $\mathbb{Q}(\sqrt{2}+\sqrt{3})/\mathbb{Q}$
(ii) $\mathbb{Q}(\sqrt[3]{7})/\mathbb{Q}$
(iii) $\mathbb{Q}(\sqrt{2+\sqrt{2}})/\mathbb{Q}$
(iv) $\mathbb{Q}(\sqrt{1+\sqrt{3}})/\mathbb{Q}$
(v) $\mathbb{F}_2(\alpha)/\mathbb{F}_2$, où $\alpha^3+\alpha+1=0$.
(vi) $\mathbb{Q}(e^{\frac{2\pi i}{n}})/\mathbb{Q}$, où $n \geq 1$.

Exercice 17. Montrer que $f(X) \in K[X] \setminus \{0\}$ est séparable si, et seulement si, il est premier avec $f'(X)$ dans $K[X]$.
Indication : utiliser l'exercice 12 du chapitre 1.

Exercice 18. Déterminer si les polynômes suivants sont séparables.

(i) $X^4 - 2X - 14 \in \mathbb{Q}[X]$
(ii) $X^3 + Y^2X^2 - YX - Y^3 + Y^2 \in \mathbb{C}[X, Y]$
(iii) $X^5 - YX^2 + X^2 + YX + 2X + Y + 5 \in \mathbb{C}[X, Y]$
(iv) $X^4 + 1 \in \mathbb{F}_2[X]$

Exercice 19. Soit $f(X) = X^n - a$, où $a \in K^*$.
Trouver une condition nécessaire et suffisante sur n pour que $f \in K[X]$ soit séparable.

Exercice 20. Soit K un corps de caractéristique p, et $a \in K$.
Montrer que $X^p - X - a$ est séparable. Plus généralement, montrer que $g(X^p) + cX$, où $g \in K[X]$ et $c \in K^*$, est séparable. En déduire que $X^{p^d} - X$ et $X^{p^2} + aX^p + bX$ $(b \neq 0)$ sont séparables.

Exercice 21. Soient K, L deux corps, $\sigma\colon K \longrightarrow L$ un morphisme de corps, et $\tilde{\sigma}\colon K[X] \longrightarrow L[X]$ son prolongement canonique.
Montrer que $f(X) \in K[X]$ est séparable si, et seulement si, $\tilde{\sigma}(f) \in L[X]$ est séparable.

Exercice 22. Soit K un corps de caractéristique $p > 0$, et soit L/K une extension de degré $n \geq 1$.
Montrer que si n et p sont premiers entre eux, alors L/K est séparable.

Exercice 23. En utilisant le théorème 1.19 et la proposition 3.24 notamment, donner une autre preuve du corollaire 3.26.

Exercice 24. Montrer que si K est un corps fini, alors $(K^*, \cdot)$ est cyclique.

Exercice 25. Soit L/K une extension finie.
Montrer que si L/K est normale et séparable, alors L est un corps de décomposition d'un polynôme irréductible séparable de $K[X]$.

Exercice 26. Pour chacune des extensions suivantes, trouver un élément $a \in L$ tel que $L = K(a)$.

(i) $L = \mathbb{Q}(\sqrt{2}, i)$, $K = \mathbb{Q}$
(ii) $L = \mathbb{Q}(\sqrt{3}, \sqrt{5}, \sqrt{15})$, $K = \mathbb{Q}$
(iii) $L = \mathbb{Q}(\sqrt{2}, \sqrt[3]{2})$, $K = \mathbb{Q}$
(iv) $L = \mathbb{Q}(\sqrt[3]{2}, \omega)$, $K = \mathbb{Q}$

Exercice 27. Trouver deux éléments primitifs différents pour l'extension $\mathbb{Q}(\sqrt{2}, \sqrt[3]{2})/\mathbb{Q}$.

Exercice 28. Soit L/K une extension finie.
Montrer que L/K est simple si, et seulement si, elle contient un nombre fini de corps intermédiaires.

Exercice 29. Montrer que toute sous-extension d'une extension simple finie est simple.

Exercice 30. En utilisant le théorème de l'élément primitif, démontrer que pour tout $n \geq 1$, il existe un polynôme irréductible de degré n dans $\mathbb{F}_p[X]$ (*cf.* exercice 18, chapitre 1).

4 Théorie de Galois

4.1 Groupes de Galois, extensions galoisiennes

Soit L/K une extension de corps. On vérifie que l'ensemble

$$\mathrm{Aut}(L/K) = \{\sigma\colon L \longrightarrow L \mid \sigma_{|K} = \mathrm{id}_K\}$$

muni de la composition des applications forme un groupe, appelé le groupe de Galois de L/K, et noté $\mathrm{Gal}(L/K)$.
On notera de plus $\mathrm{Aut}(K) = \mathrm{Aut}(K/\Pi(K))$.

Proposition 4.1 Soit $\in \mathrm{Gal}(L/K)$ et $f \in K[X]$. Soit $a \in L$ tel que $f(a) = 0$. Alors $f(\sigma(a)) = 0$.
Autrement dit, le groupe de Galois agit par permutation des racines de f dans L.

Preuve. Notons $f(X) = c_n X^n + \cdots + c_1 X + c_0 \in K[X]$.
Comme σ est un morphisme de corps, on a

$$f(\sigma(a)) = \sum_{i=0}^{n} c_i(\sigma(a))^i = \sigma\Big(\sum_{i=0}^{n} c_i a^i\Big) = \sigma(f(a)) = \sigma(0) = 0.$$

Pour la deuxième égalité, on utilise le fait que σ est un $K-$automorphisme, donc $\sigma(c_i) = c_i$ pour tout $0 \leq i \leq n$. □

Exemples. (i) Comme $\mathbb{C} = \mathbb{R}(i)$, un élément $\sigma \in \mathrm{Gal}(\mathbb{C}/\mathbb{R})$ est uniquement déterminé par $\sigma(i)$. Comme $\sigma(i)$ doit être une racine de $X^2 + 1 \in \mathbb{R}[X]$, on a $\sigma(i) = i$ ou $\sigma(i) = -i$. On vérifie facilement que les deux possibilités donnent bien des automorphismes de corps. Le premier est l'identité sur $\mathbb{C}$, le second est la conjugaison complexe, et $\mathrm{Gal}(\mathbb{C}/\mathbb{R}) = \{\mathrm{id}_{\mathbb{C}}, \sigma\} \simeq \langle\sigma\rangle \simeq \mathbb{Z}/2\mathbb{Z}$, où $\sigma(x + iy) = x - iy$, pour tous $x, y \in \mathbb{R}$.
(ii) De la même façon, un $\mathbb{Q}-$automorphisme $\sigma \in \mathrm{Gal}(\mathbb{Q}(\sqrt{5})/\mathbb{Q})$ est déterminé par $\sigma(\sqrt{5})$, qui doit être une racine de $X^2 - 5$. Ainsi, $\sigma(\sqrt{5}) = \pm\sqrt{5}$, et $\mathrm{Gal}(\mathbb{Q}(\sqrt{5})/\mathbb{Q}) = \{\mathrm{id}_{\mathbb{Q}(\sqrt{5})}, \sigma\} \simeq \mathbb{Z}/2\mathbb{Z}$, où $\sigma(a + b\sqrt{5}) = a - b\sqrt{5}$, pour tous $a, b \in \mathbb{Q}$.
(iii) Le corps $\mathbb{Q}(\sqrt[4]{2})$ contient deux racines de $X^4 - 2$, $\sqrt[4]{2}$ et $-\sqrt[4]{2}$. Cela implique que $\mathrm{Gal}(\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}) = \{\mathrm{id}_{\mathbb{Q}(\sqrt[4]{2})}, \sigma\} \simeq \mathbb{Z}/2\mathbb{Z}$, où $\sigma(\sqrt[4]{2}) = -\sqrt[4]{2}$.

La définition suivante est la plus importante du cours.

Définition 4.2 Une extension de corps L/K est *galoisienne* si elle est normale et séparable.

Exemples. (i) Les extensions $\mathbb{C}/\mathbb{R}$, $\mathbb{Q}(\sqrt{p})/\mathbb{Q}$, où p est un nombre premier, sont des extensions galoisiennes.
(ii) De même, $\mathbb{F}_2(\alpha)/\mathbb{F}_2$, avec $\alpha^3 + \alpha + 1 = 0$, est galoisienne.
(iii) Soit K un corps parfait. Toute extension normale de K est galoisienne.
(iv) En revanche, $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ n'est pas galoisienne, puisqu'elle n'est pas normale.

On remarque que si L/K est une extension galoisienne finie, alors $|\mathrm{Gal}(L/K)| = [L : K]$. Cela découle du théorème 3.30. La réciproque est vraie, c'est le corollaire 4.6 ci-dessous.

Proposition 4.3 Soit L un corps et $G \subset \mathrm{Aut}(L)$.
Alors, l'ensemble

$$L^G = \{a \in L \mid \sigma(a) = a,\ \forall \sigma \in G\}$$

est un sous-corps de L, appelé le *sous-corps des points fixes* de G.

Preuve. On montre facilement que, pour tout $\sigma \in G$, l'ensemble $\mathrm{Fix}(\sigma) := \{a \in L \mid \sigma(a) = a\}$ est un sous-corps de L.
On conclut en remarquant que $L^G = \bigcap_{\sigma \in G} \mathrm{Fix}(\sigma)$. □

Le sous-corps des points fixes caractérise en fait complètement une extension galoisienne.

Théorème 4.4 Soient L/K une extension algébrique, et $G = \mathrm{Gal}(L/K)$.
L/K est galoisienne si, et seulement si, $K = L^G$.

Preuve. $\Longrightarrow$: Supposons L/K galoisienne. Par définition de G, on a clairement $K \subset L^G$. Soit donc $a \in L^G$. Comme a est séparable sur K, le théorème 3.29 nous assure que $[K(a) : K] = |\mathrm{Hom}(K(a)/K, L/K)|$. Soit donc $\sigma \in \mathrm{Hom}(K(a)/K, L/K)$. Par le corollaire 3.15(*ii*), il existe $\sigma' \in G$ tel que $\sigma'_{|K(a)} = \sigma$. Comme $a \in L^G$, $a = \sigma'(a) = \sigma(a)$. Ainsi, σ fixe K et a, donc σ fixe $K(a)$. Cela implique $[K(a) : K] = |\mathrm{Hom}(K(a)/K, L/K)| = 1$, d'où $a \in K$.
$\Longleftarrow$: Réciproquement, supposons $K = L^G$. Soit $a \in L$ et f son polynôme minimal sur K, qui existe puisque L/K est algébrique. Notons $a_1, \ldots, a_m \in L$ les racines distinctes de f dans L, et posons $g(X) = \prod_{i=1}^{m}(X - a_i) \in L[X]$. Comme G permute les a_i, les coefficients de g, qui sont des expressions symétriques en les a_i, sont fixés par G. Ils sont donc dans $L^G = K$, d'où $g \in K[X]$. Comme $g(a) = 0$, f divise g. D'autre part, $\deg(g) = m \leq \deg(f)$. Finalement, $f = g$, et f n'a que des racines simples, toutes contenues dans L. Cela montre que L/K est galoisienne, et conclut la preuve. □

Théorème 4.5 Soit L un corps, et $H \leqslant \mathrm{Aut}(L)$ un sous-groupe fini.
Alors L/L^H est finie, de degré $|H|$, et galoisienne, de groupe de Galois $\mathrm{Gal}(L/L^H) = H$.

Preuve. Notons $K = L^H$. Soit $a \in L$, et notons $\{a_1, \ldots, a_m\}$ l'orbite de a sous l'action de H. Posons $h_a(X) = \prod_{i=1}^{m}(X - a_i)$. Par le même argument que dans la preuve précédente, $h_a \in K[X]$. Comme $h_a(a) = 0$, a est algébrique sur K, et le polynôme minimal f de a sur K divise h_a dans $K[X]$. Ainsi, f est séparable et a toutes ses racines dans L. De plus, $[K(a) : K] = \deg(f) \leq m \leq |H|$. Cela montre déjà que L/K est séparable, et tout $a \in L$ a degré au plus $|H|$. Soit maintenant $n := \max\{[K(a) : K] \mid a \in L\}$, de sorte que $n \leq |H|$, et soit $\alpha \in L$ tel que $[K(\alpha) : K] = n$. Montrons que $L = K(\alpha)$. Soit $b \in L$. Comme α et b sont algébriques sur K, le théorème 2.17 nous assure que $K(\alpha, b)/K$ est finie. De plus, comme L/K est séparable, toutes ses sous-extensions sont séparables, donc $K(\alpha, b)/K$ est séparable. On peut donc appliquer le théorème de l'élément primitif, et il existe $\gamma \in L$ telle que $K(\alpha, b) = K(\gamma)$. Alors

$$n \geq [K(\gamma) : K] = [K(\alpha, b) : K] \geq [K(\alpha) : K] = n$$

d'où on tire que $K(\gamma) = K(\alpha, b) = K(\alpha)$, et donc $b \in K(\alpha)$. Donc $L = K(\alpha)$. Cela implique $[L : K] = [K(\alpha) : K] = n \leq |H|$, et L/K est bien finie. Ensuite, la première partie de cette preuve montre que L est un corps de décomposition du polynôme minimal de γ sur K. En conséquence, L/K est normale, et donc galoisienne. Cela implique $|\mathrm{Gal}(L/K)| = [L : K]$ et on peut alors conclure puisque H est un sous-groupe de $\mathrm{Gal}(L/K)$:

$$|H| \leq |\mathrm{Gal}(L/K)| = [L : K] \leq |H|.$$

Ainsi $[L : K] = |H|$ et $H = \mathrm{Gal}(L/K)$. □

Corollaire 4.6 Soit L/K une extension finie.
L'extension L/K est galoisienne si, et seulement si, $|\mathrm{Gal}(L/K)| = [L : K]$.

Preuve. Le sens $\Longrightarrow$ a été vu ci-dessus.
$\Longleftarrow$: Notons $G = \mathrm{Gal}(L/K)$. On a alors $K \subset L^G$ et par le théorème 4.5, $[L : L^G] = |G| = [L : K]$. Ainsi $K = L^G$. Par le théorème 4.4, ceci implique que L/K est galoisienne. □

4.2 Correspondance de Galois

On a maintenant tous les outils nécessaires pour établir le résultat central de ce cours : la correspondance galoisienne.

Soit L/K une extension galoisienne finie. Introduisons les ensembles

$$\mathcal{G} = \{\text{sous-groupes de } \mathrm{Gal}(L/K)\},\ \mathcal{K} = \{\text{sous-corps de } L \text{ contenant } K\}$$

et les applications $\Phi\colon \mathcal{G} \longrightarrow \mathcal{K}$, $\Phi(H) = L^H$, $\Psi\colon \mathcal{K} \longrightarrow \mathcal{G}$, $\Psi(M) = \mathrm{Gal}(L/M)$.

La proposition 4.3 assure que Φ est bien définie. De plus, pour tout $M \in \mathcal{K}$, L/M est finie, normale (corollaire 3.15) et séparable (corollaire 3.31). Elle est donc galoisienne finie, et $\mathrm{Gal}(L/M) \leqslant \mathrm{Gal}(L/K)$. L'application Ψ est donc aussi bien définie.

Théorème 4.7 (correspondance de Galois) Soit L/K une extension galoisienne finie. Notons $G = \mathrm{Gal}(L/K)$.
(i) Les applications Φ et Ψ sont bijectives, et inverses l'une de l'autre.
(ii) Pour tous H_1, $H_2 \in \mathcal{G}$, $H_1 \leqslant H_2 \iff L^{H_2} \subset L^{H_1}$.
(iii) Pour tous M_1, $M_2 \in \mathcal{K}$, $M_1 \subset M_2 \iff \mathrm{Gal}(L/M_2) \leqslant \mathrm{Gal}(L/M_1)$.
(iv) Pour tout $M \in \mathcal{K}$ et tout $\sigma \in G$, $\sigma(M) \in \mathcal{K}$ et $\mathrm{Gal}(L/\sigma(M)) = \sigma\mathrm{Gal}(L/M)\sigma^{-1}$.
(v) Pour tout $M \in \mathcal{K}$, M/K est normale si, et seulement si, $\mathrm{Gal}(L/M) \lhd G$.
(vi) Soit $M \in \mathcal{K}$ avec M/K normale. Alors $\mathrm{Gal}(M/K) \simeq G/\mathrm{Gal}(L/M)$.

Preuve. (i) Soit d'abord $M \in \mathcal{K}$. $\Phi(\Psi(M)) = L^{\Psi(M)} = L^{\mathrm{Gal}(L/M)} = M$ par le théorème 4.4, puisque L/M est galoisienne. Ainsi $\Phi \circ \Psi = \mathrm{id}_{\mathcal{K}}$. Réciproquement, soit $H \in \mathcal{G}$. On a $\Psi(\Phi(H)) = \mathrm{Gal}(L/L^H) = H$ par le théorème 4.5. Donc $\Psi \circ \Phi = \mathrm{id}_{\mathcal{G}}$, et (i) est montré.
(ii) $\Longrightarrow$: Soit $a \in L^{H_2}$. Alors a est fixé par tout élément de H_2. En particulier, a est fixé par tout élément de H_1, donc $a \in L^{H_1}$.
$\Longleftarrow$: Réciproquement, soit $\tau \in H_1$. Soit $a \in L^{H_2}$. Alors par hypothèse $L^{H_2} \subset L^{H_1}$, donc $a \in L^{H_1}$, et comme $\tau \in H_1$, on a $\tau(a) = a$. Donc $\tau \in H_2$.
(iii) $\Longrightarrow$: Soit $\tau \in \mathrm{Gal}(L/M_2)$. Alors τ est un automorphisme de L qui fixe M_2. En particulier, τ fixe M_1. Donc $\tau \in \mathrm{Gal}(L/M_1)$.
$\Longleftarrow$: Soit $a \in M_1$. Tout élément de $\mathrm{Gal}(L/M_1)$ fixe a. En particulier, tout élément de $\mathrm{Gal}(L/M_2)$ fixe a, ce qui signifie que $a \in M_2$.
(iv) Soit $M \in \mathcal{K}$. Il est clair que $\sigma(M) \in \mathcal{K}$. De plus

$$\begin{aligned}\tau \in \mathrm{Gal}(L/\sigma(M)) &\iff \forall a \in M,\ \tau(\sigma(a)) = \sigma(a)\\ &\iff \forall a \in M,\ \sigma^{-1}\tau(\sigma(a)) = a\\ &\iff \sigma^{-1}\tau\sigma \in \mathrm{Gal}(L/M)\\ &\iff \tau \in \sigma\mathrm{Gal}(L/M)\sigma^{-1}\end{aligned}$$

ce qui démontre $\mathrm{Gal}(L/\sigma(M)) = \sigma\mathrm{Gal}(L/M)\sigma^{-1}$.
(v) Soit $M \in \mathcal{K}$. Si M/K est normale, alors $\sigma(M) = M$ pour tout $\sigma \in G$ par le théorème 3.18. On a donc $\mathrm{Gal}(L/M) = \mathrm{Gal}(L/\sigma(M)) = \sigma\mathrm{Gal}(L/M)\sigma^{-1}$ pour tout $\sigma \in G$, par le point (iv). $\mathrm{Gal}(L/M)$ est alors normal dans G. Réciproquement, si $\mathrm{Gal}(L/M)$ est normal dans G, alors $\mathrm{Gal}(L/\sigma(M)) = \mathrm{Gal}(L/M)$ pour tout $\sigma \in G$. Cela implique $\sigma(M) = M$ pour tout $\sigma \in G$. On en déduit que M/K est normale.
(vi) Comme M/K est normale, on a $\sigma(M) = M$ pour tout $\sigma \in G$. On peut alors définir l'application

$$\begin{aligned}\varphi\colon G &\longrightarrow \mathrm{Gal}(M/K)\\ \sigma &\longmapsto \sigma_{|M}\end{aligned}$$

C'est un morphisme de groupes, surjectif par le corollaire 3.15(ii), de noyau $\mathrm{Ker}(\varphi) = \mathrm{Gal}(L/M)$. Le 1er théorème d'isomorphisme permet de conclure. □

Ce théorème appelle deux remarques importantes. Premièrement, si les sous-groupes du groupe de Galois sont en correspondance bijective avec les sous-corps de l'extension, cette correspondance est "inversée". Le point (ii) du théorème nous dit que plus le sous-groupe du groupe de Galois est petit, plus le corps de points fixes correspondant est grand. Le point (iii) exprime lui, dans l'autre sens, que plus le sous-corps des points fixes est petit, plus grand est le sous-groupe du groupe de Galois qui lui correspond. Deuxièmement, l'hypothèse que L/K est finie est essentielle : le théorème 4.7 est faux en général pour les extensions infinies. Un exemple important figure en exercices.

Définition 4.8 Soit K un corps et $f \in K[X] \setminus K$.
Le *groupe de Galois* de f, noté $\mathrm{Gal}(f)$, est le groupe $\mathrm{Gal}(L/K)$, où L est un corps de décomposition de f sur K.

L'idée cruciale de Galois a été de voir le groupe $\mathrm{Gal}(L/K)$ comme des permutations des racines de f.

Théorème 4.9 Soient K un corps, et $f \in K[X] \setminus K$ séparable.
Soit L un corps de décomposition de f sur K, et notons Z l'ensemble des racines de f dans L, de sorte que $L = K(Z)$.
(i) L/K est finie et galoisienne.
(ii) $\mathrm{Gal}(f)$ agit fidèlement sur Z. En particulier, $\mathrm{Gal}(f)$ s'identifie à un sous-groupe de $S(Z)$.
(iii) $\mathrm{Gal}(f)$ agit transitivement sur Z si, et seulement si, f est irréductible.

Preuve. Notons $Z = \{a_1, \dots, a_n\}$, sans répétitions.
(i) Comme $L = K(a_1, \dots, a_n)$ avec $a_1, \dots, a_n$ algébriques sur K, L/K est finie par le théorème 2.17. Ensuite, comme f est séparable et que $a_1, \dots, a_n$ sont racines de f, $a_1, \dots, a_n$ sont séparables sur K, donc L est séparable par le corollaire 3.31(ii). Enfin, comme L est un corps de décomposition de f sur K, L/K est normale par le théorème 3.14. En conséquence, L/K est galoisienne.
(ii) La proposition 4.1 montre que $\mathrm{Gal}(f)$ agit par permutation des racines de f dans L. Plus précisément, l'action de groupes s'écrit

$$\begin{aligned} \cdot \colon \mathrm{Gal}(f) \times Z &\longrightarrow Z \\ (\sigma, a_i) &\longmapsto \sigma \cdot a_i := \sigma(a_i) \end{aligned}$$

Pour montrer que cette action est fidèle, prenons $\sigma \in \mathrm{Gal}(f)$ tel que $\sigma \cdot a_i = a_i$ pour tout $1 \leq i \leq n$. Autrement dit, $\sigma(a_i) = a_i$ pour tout $1 \leq i \leq n$. Comme σ fixe K et tous les a_i, σ fixe $K(a_1, \dots, a_n) = L$. Donc $\sigma = \mathrm{id}_L$ est l'élément neutre de $\mathrm{Gal}(f)$, et l'action est fidèle. Elle induit donc un morphisme de groupes injectif $\varphi \colon \mathrm{Gal}(f) \hookrightarrow S(Z)$, et $\mathrm{Gal}(f) \simeq \mathrm{Im}(\varphi) \leqslant S(Z)$.
(iii) Supposons d'abord f irréductible. Par le lemme 3.2, pour tous $1 \leq i \neq j \leq n$, il existe un $K-$morphisme $\tau \colon K(a_i) \longrightarrow L$ tel que $\tau(a_i) = a_j$. Par le corollaire 3.25(ii), τ se prolonge en un élément $\sigma \in \mathrm{Gal}(L/K) = \mathrm{Gal}(f)$ qui envoie a_i sur a_j, donc l'action de $\mathrm{Gal}(f)$ sur Z est transitive. Réciproquement, supposons que f n'est pas irréductible, et soient f_i et f_j deux facteurs irréductibles de f. Soient a_i une racine de f_i et a_j une racine de f_j. Alors f_i et f_j sont les polynômes minimaux de a_i et a_j sur K. Pour tout $\sigma \in \mathrm{Gal}(f)$, $\sigma(a_i)$ a le même polynôme minimal que a_i. Donc il n'existe aucun $\sigma \in \mathrm{Gal}(f)$ tel que $\sigma(a_i) = a_j$. L'action du groupe de Galois sur Z n'est donc pas transitive. □

4.3 Correspondance de Galois : exemples concrets

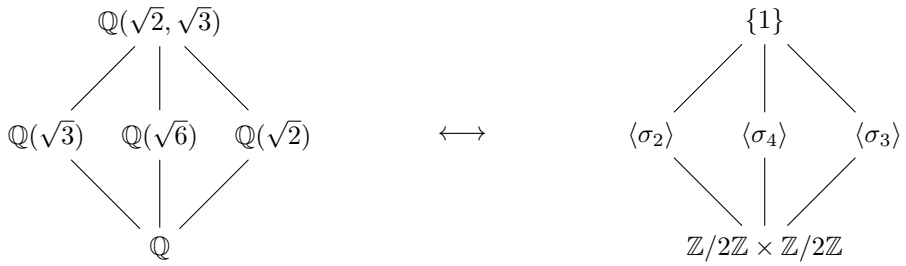
(i) Considérons l'extension $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$.
Soit $f = X^2 - 2$. Alors f est irréductible sur $\mathbb{Q}$, et $\mathbb{Q}(\sqrt{2})$ est son corps de décomposition, donc $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ est normale. Elle est de plus finie, de degré 2, donc algébrique, donc séparable puisque $\mathbb{Q}$ est parfait.
Ainsi, $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ est galoisienne et $|\mathrm{Gal}(f)| = [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$, donc $\mathrm{Gal}(f) \simeq \mathbb{Z}/2\mathbb{Z}$. On obtient la correspondance de Galois suivante :

$$\begin{array}{ccc} \mathbb{Q}(\sqrt{2}) & & \{1\} \\ | & \longleftrightarrow & | \\ \mathbb{Q} & & \mathbb{Z}/2\mathbb{Z} \end{array}$$

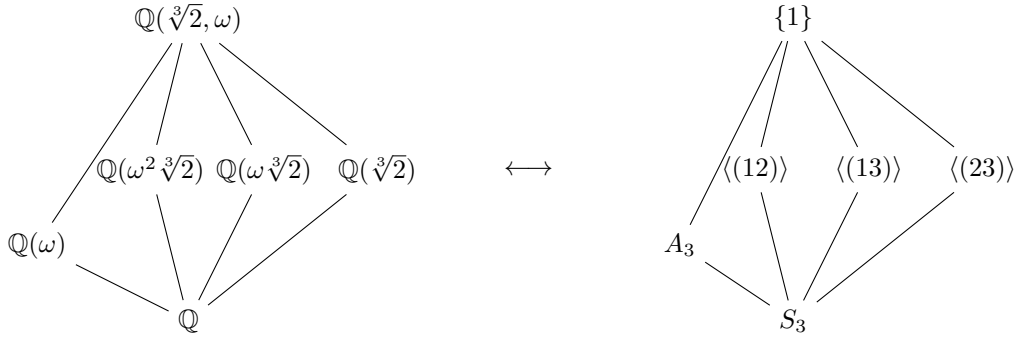
(ii) Considérons le corps $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ comme une extension de $K = \mathbb{Q}$.
Soit $f = (X^2 - 2)(X^2 - 3)$. Le corps L est un corps de décomposition de f sur K, donc L/K est normale, et comme elle est algébrique (car finie), elle est séparable puisque K est parfait. Ainsi, L/K est galoisienne, et $|\mathrm{Gal}(f)| = [L : K] = 4$.
Un élément $\sigma \in \mathrm{Gal}(f)$ est déterminé par $\sigma(\sqrt{2})$ et $\sigma(\sqrt{3})$. Comme $\sigma(\sqrt{2})$ doit être une racine de $X^2 - 2$, on a $\sigma(\sqrt{2}) = \pm\sqrt{2}$, et de même $\sigma(\sqrt{3}) = \pm\sqrt{3}$. Cela implique que $\mathrm{Gal}(f)$ ne contient que des éléments d'ordre 1 ou 2, d'où $\mathrm{Gal}(f) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.
Ainsi, $\mathrm{Gal}(f)$ contient trois sous-groupes d'ordre 2 et d'indice 2, donc L contient trois sous-extensions quadratiques de K. Clairement, L contient $\mathbb{Q}(\sqrt{2})$ et $\mathbb{Q}(\sqrt{3})$. De plus, $\sqrt{2}\sqrt{3} = \sqrt{6} \in L$, donc L contient aussi $\mathbb{Q}(\sqrt{6})$.
Regardons maintenant le sous-groupe $\langle \sigma_2 \rangle \simeq \mathbb{Z}/2\mathbb{Z} \leqslant \mathrm{Gal}(f)$, où $\sigma_2(\sqrt{2}) = -\sqrt{2}$ et $\sigma_2(\sqrt{3}) = \sqrt{3}$. Un élément $\alpha \in L$ a la forme générale $\alpha = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$ avec $a, b, c, d \in K$. Alors

$$\begin{aligned} \alpha \in L^{\langle \sigma_2 \rangle} \iff \sigma_2(\alpha) = \alpha &\iff a - b\sqrt{2} + c\sqrt{3} - d\sqrt{6} = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \\ &\iff b = d = 0 \end{aligned}$$

donc $\alpha = a + c\sqrt{3} \in \mathbb{Q}(\sqrt{3})$. On en déduit que le sous-corps de points fixes correspondant à $\langle \sigma_2 \rangle$ est $\mathbb{Q}(\sqrt{3})$.
De la même façon, on montre que $L^{\langle \sigma_3 \rangle} = \mathbb{Q}(\sqrt{2})$ et $L^{\langle \sigma_4 \rangle} = \mathbb{Q}(\sqrt{6})$, où $\sigma_3(\sqrt{2}) = \sqrt{2}$, $\sigma_3(\sqrt{3}) = -\sqrt{3}$, $\sigma_4(\sqrt{2}) = -\sqrt{2}$, $\sigma_4(\sqrt{3}) = -\sqrt{3}$.
Finalement on a la correspondance de Galois suivante :



(*iii*) Soit l'extension de corps $\mathbb{Q}(\sqrt[3]{2},\omega)/\mathbb{Q}$, et $f = X^3 - 2 \in \mathbb{Q}[X]$.
Le polynôme f est irréductible sur $\mathbb{Q}$, et ses racines sont $\sqrt[3]{2}$, $\omega\sqrt[3]{2}$ et $\omega^2\sqrt[3]{2}$. Le corps $\mathbb{Q}(\sqrt[3]{2},\omega)$ est alors un corps de décomposition de f sur $\mathbb{Q}$, et donc $\mathbb{Q}(\sqrt[3]{2},\omega)/\mathbb{Q}$ est normale. Elle est de plus finie, donc algébrique, donc séparable puisque $\mathbb{Q}$ est parfait. Elle est donc galoisienne. En particulier, $|\mathrm{Gal}(f)| = [\mathbb{Q}(\sqrt[3]{2},\omega) : \mathbb{Q}] = 6$. De plus, $\mathrm{Gal}(f)$ s'identifie à un sous-groupe de S_3, qui est aussi d'ordre 6. On conclut que $\mathrm{Gal}(f) \simeq S_3$.
Maintenant, S_3 a un sous-groupe d'ordre 3 et d'indice 2, A_3, et trois sous-groupes d'ordre 2 et d'indice 3, $\langle(12)\rangle$, $\langle(13)\rangle$ et $\langle(23)\rangle$.
Par correspondance galoisienne, $\mathbb{Q}(\sqrt[3]{2},\omega)$ contient donc une extension quadratique de $\mathbb{Q}$ et trois extensions cubiques de $\mathbb{Q}$. Clairement, $\mathbb{Q}(\sqrt[3]{2},\omega)$ contient $\mathbb{Q}(\omega)$, qui est de degré 2 sur $\mathbb{Q}$, et qui correspond donc à A_3. De plus, $\mathbb{Q}(\sqrt[3]{2},\omega)$ contient aussi $\mathbb{Q}(\sqrt[3]{2})$, $\mathbb{Q}(\omega\sqrt[3]{2})$ et $\mathbb{Q}(\omega^2\sqrt[3]{2})$, et ces trois extensions sont distinctes puisque deux racines distinctes de f ne peuvent pas appartenir à une même extension cubique de $\mathbb{Q}$.
En numérotant les racines, on peut déterminer la correspondance entre sous-corps de points fixes et sous-groupes : disons que $\sqrt[3]{2}$ est la 1ère racine, $\omega\sqrt[3]{2}$ la deuxième et $\omega^2\sqrt[3]{2}$ la troisième. Alors (12) fixe $\omega^2\sqrt[3]{2}$ et $\mathbb{Q}$, donc $\mathbb{Q}(\omega^2\sqrt[3]{2})$ est contenu dans le sous-corps fixé par $\langle(12)\rangle$. Comme $[\mathbb{Q}(\omega^2\sqrt[3]{2}) : \mathbb{Q}] = 3 = [S_3 : \langle(12)\rangle]$, on en déduit que $\mathbb{Q}(\sqrt[3]{2},\omega)^{\langle(12)\rangle} = \mathbb{Q}(\omega^2\sqrt[3]{2})$. De même on a $\mathbb{Q}(\sqrt[3]{2},\omega)^{\langle(13)\rangle} = \mathbb{Q}(\omega\sqrt[3]{2})$ et $\mathbb{Q}(\sqrt[3]{2},\omega)^{\langle(23)\rangle} = \mathbb{Q}(\sqrt[3]{2})$. La correspondance de Galois se représente alors comme



Ensuite, l'extension $\mathbb{Q}(\sqrt[3]{2},\omega)/\mathbb{Q}(\omega)$ est normale (corollaire 3.15(i)). Elle est donc galoisienne, et $|\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2},\omega)/\mathbb{Q}(\omega))| = [\mathbb{Q}(\sqrt[3]{2},\omega) : \mathbb{Q}(\omega)] = 3$, ce qui implique $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2},\omega)/\mathbb{Q}(\omega)) \simeq \mathbb{Z}/3\mathbb{Z} \simeq A_3$. Comme $A_3 \lhd S_3$, on retrouve ainsi, grâce au théorème 4.7(v) que $\mathbb{Q}(\omega)/\mathbb{Q}$ est normale, de groupe de Galois

$$\mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q}) \simeq S_3/\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2},\omega)/\mathbb{Q}(\omega)) \simeq S_3/A_3 \simeq \mathbb{Z}/2\mathbb{Z}.$$

On voit également que les trois autres sous-extensions cubiques de $\mathbb{Q}$ ne sont pas normales, puisque les sous-groupes correspondants ne sont pas normaux dans S_3.

(*iv*) Soit p un nombre premier, $n \geq 1$, et considérons l'extension $\mathbb{F}_{p^n}/\mathbb{F}_p$.
Comme $\mathbb{F}_{p^n}$ est un corps de décomposition de $X^{p^n} - X$ sur $\mathbb{F}_p$, $\mathbb{F}_{p^n}/\mathbb{F}_p$ est normale. $\mathbb{F}_p$ étant parfait, toutes ses extensions algébriques sont séparables, et donc $\mathbb{F}_{p^n}/\mathbb{F}_p$ est galoisienne. En particulier, $|\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)| = [\mathbb{F}_{p^n} : \mathbb{F}_p] = n$.
Notons

$$\begin{aligned} \sigma_p \colon \mathbb{F}_{p^n} &\longrightarrow \mathbb{F}_{p^n} \\ x &\longmapsto x^p \end{aligned}$$

l'automorphisme de Frobenius.

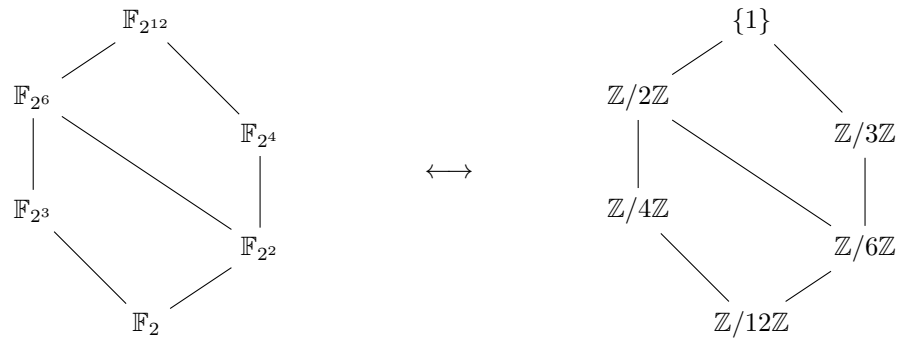
Théorème 4.10 L'automorphisme σ_p est un générateur de $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$. En particulier, $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) \simeq \mathbb{Z}/n\mathbb{Z}$.

Preuve. D'abord, pour tout $a \in \mathbb{F}_p$, on a $a^p = a$, donc σ_p fixe le corps de base $\mathbb{F}_p$.
C'est de plus un morphisme de corps, injectif par le lemme 2.1, et donc aussi surjectif puisque $\mathbb{F}_{p^n}$ est fini. Donc $\sigma_p \in \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$. Comme $|\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)| = n$, il suffit de montrer que σ_p a ordre n pour prouver le théorème.
Soit donc $r \geq 1$ l'ordre de σ_p. Alors r divise $|\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)| = n$, donc $r \leq n$. De plus,

$$\sigma_p^r = \mathrm{id}_{\mathbb{F}_{p^n}} \Longrightarrow \forall x \in \mathbb{F}_{p^n},\ \sigma_p^r(x) = x \Longrightarrow \forall x \in \mathbb{F}_{p^n},\ x^{p^r} - x = 0$$

et donc tout $x \in \mathbb{F}_{p^n}$ est racine de $X^{p^r} - X$. Or $X^{p^r} - X$ a degré p^r, donc a au plus p^r racines dans $\mathbb{F}_{p^n}$. Ainsi, $p^n \leq p^r$, d'où on tire que $n \leq r$. Cela implique $n = r$, et termine la démonstration. □

Une extension avec un groupe de Galois cyclique d'ordre n a un treillis de sous-corps ressemblant au treillis de sous-groupes de $\mathbb{Z}/n\mathbb{Z}$, avec un sous-corps de degré d sur le corps de base correspondant à l'unique sous-groupe d'indice d dans $\mathbb{Z}/n\mathbb{Z}$, où d est un diviseur de n.
Par exemple, pour $\mathbb{F}_{2^{12}}/\mathbb{F}_2$, on a $\mathrm{Gal}(\mathbb{F}_{2^{12}}/\mathbb{F}_2) = \langle \sigma_2 \rangle \simeq \mathbb{Z}/12\mathbb{Z}$, et la correspondance de Galois se représente comme



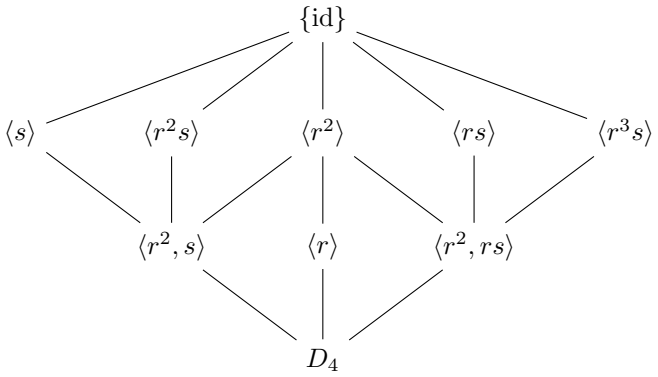
(v) On s'intéresse maintenant à l'extension L/K, où $L = \mathbb{Q}(\sqrt[4]{2}, i)$ et $K = \mathbb{Q}$. Soit $f = X^4 - 2$.
L est un corps de décomposition de f sur K, donc L/K est normale, et comme K est parfait, L/K est séparable, donc galoisienne. En particulier, $|\mathrm{Gal}(L/K)| = [L : K] = 8$.
Ensuite, un élément $\sigma \in \mathrm{Gal}(L/K)$ est uniquement déterminé par $\sigma(\sqrt[4]{2})$ et $\sigma(i)$. $\sigma(\sqrt[4]{2})$ doit être une racine de f, donc $\sigma(\sqrt[4]{2}) \in \{\sqrt[4]{2}, -\sqrt[4]{2}, i\sqrt[4]{2}, -i\sqrt[4]{2}\}$, et $\sigma(i)$ doit être une racine de $X^2 + 1$, donc $\sigma(i) \in \{i, -i\}$. Soient r et s les deux éléments de $\mathrm{Gal}(L/K)$ déterminés par

$$r(\sqrt[4]{2}) = i\sqrt[4]{2},\ r(i) = i,\ s(\sqrt[4]{2}) = \sqrt[4]{2},\ s(i) = -i.$$

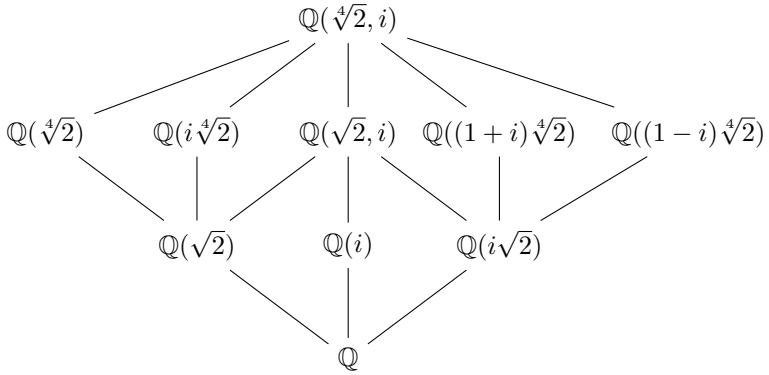
En calculant les différentes puissances et produits de r et s à $\sqrt[4]{2}$ et i, on peut décrire explicitement les 7 éléments non-triviaux de $\mathrm{Gal}(L/K)$:

$$\begin{aligned}
&r(\sqrt[4]{2}) = i\sqrt[4]{2},\ r(i) = i\\
&r^2(\sqrt[4]{2}) = -\sqrt[4]{2},\ r^2(i) = i\\
&r^3(\sqrt[4]{2}) = -i\sqrt[4]{2},\ r^3(i) = i\\
&s(\sqrt[4]{2}) = \sqrt[4]{2},\ s(i) = -i\\
&rs(\sqrt[4]{2}) = i\sqrt[4]{2},\ rs(i) = -i\\
&r^2s(\sqrt[4]{2}) = -\sqrt[4]{2},\ r^2s(i) = -i\\
&r^3s(\sqrt[4]{2}) = -i\sqrt[4]{2},\ r^3s(i) = -i
\end{aligned}$$

De plus, un calcul en $\sqrt[4]{2}$ et en i montre que $r^4 = s^2 = \mathrm{id}_L$ et $rs = sr^{-1}$. Cela montre que $\mathrm{Gal}(L/K) \simeq D_4$, où D_4 peut être vu comme le groupe des 8 symétries du carré dont les sommets sont les quatre racines de f dans le plan complexe : r est une rotation de $\frac{2\pi}{4} = \frac{\pi}{2}$ radians dans le sens trigonométrique, et s est la conjugaison complexe, qui est une réflexion par rapport à la diagonale du carré qui relie $\sqrt[4]{2}$ et $-\sqrt[4]{2}$.
Maintenant, le treillis des sous-groupes de D_4 est le suivant



et le treillis des sous-corps de L prend alors la même forme



Pour trouver les générateurs des extensions qui apparaissent dans ce diagramme, et vérifier que les sous-corps de points fixes correspondent aux bons sous-groupes, on procède comme suit : tout d'abord il est clair que L contient $\mathbb{Q}(i)$ et $\mathbb{Q}(\sqrt[4]{2})$. Comme r fixe i et que $[\mathbb{Q}(i):\mathbb{Q}]=2=[D_4:\langle r\rangle]$, on doit avoir $L^{\langle r\rangle}=\mathbb{Q}(i)$. De même, on montre que $L^{\langle s\rangle}=\mathbb{Q}(\sqrt[4]{2})$.
Ensuite, on sait que $\mathbb{Q}(\sqrt[4]{2})$ contient $\mathbb{Q}(\sqrt{2})$ comme sous-corps, et vu que $[\mathbb{Q}(\sqrt{2}):\mathbb{Q}]=2$, $\mathbb{Q}(\sqrt{2})$ doit correspondre à un des deux sous-groupes restants d'indice 2 : $\langle r^2,s\rangle$ ou $\langle r^2,rs\rangle$. Or on calcule que

$$s(\sqrt{2})=s(\sqrt[4]{2}^2)=s(\sqrt[4]{2})^2=\sqrt[4]{2}^2=\sqrt{2}\Longrightarrow rs(\sqrt{2})=r(\sqrt{2})=r(\sqrt[4]{2}^2)=r(\sqrt[4]{2})^2=(i\sqrt[4]{2})^2=-\sqrt{2}$$

donc $\sqrt{2}$ n'est pas fixé par rs, ce qui exclut la seconde possibilité. Ainsi $L^{\langle r^2,s\rangle}=\mathbb{Q}(\sqrt{2})$.
Ensuite, L contient i et $\sqrt{2}$, donc L contient $i\sqrt{2}$, donc L contient $\mathbb{Q}(i\sqrt{2})$. Comme $[\mathbb{Q}(i\sqrt{2}):\mathbb{Q}]=2$, ce sous-corps correspond au sous-groupe restant d'indice 2 dans D_4, *i.e.* $L^{\langle r^2,rs\rangle}=\mathbb{Q}(i\sqrt{2})$.
Pour trouver les autres générateurs, on écrit un élément $\alpha\in L$ comme combinaison linéaire des éléments d'une base de L et on regarde ce que le fait d'être dans un sous-corps fixé par un sous-groupe implique sur les coefficients.
Une base de L sur K est $\{1,\sqrt[4]{2},\sqrt[4]{2}^2,\sqrt[4]{2}^3,i,i\sqrt[4]{2},i\sqrt[4]{2}^2,i\sqrt[4]{2}^3\}$, donc α prend la forme

$$\alpha=a+b\sqrt[4]{2}+c\sqrt[4]{2}^2+d\sqrt[4]{2}^3+ei+fi\sqrt[4]{2}+gi\sqrt[4]{2}^2+hi\sqrt[4]{2}^3$$

Si α est dans le sous-corps fixé par $\langle r^2s\rangle$, alors $r^2s(\alpha)=\alpha$, donc

$$a-b\sqrt[4]{2}+c\sqrt[4]{2}^2-d\sqrt[4]{2}^3-ei+fi\sqrt[4]{2}-gi\sqrt[4]{2}^2+hi\sqrt[4]{2}^3=a+b\sqrt[4]{2}+c\sqrt[4]{2}^2+d\sqrt[4]{2}^3+ei+fi\sqrt[4]{2}+gi\sqrt[4]{2}^2+hi\sqrt[4]{2}^3$$

ce qui implique $b=d=e=g=0$, donc α prend la forme $\alpha=a+c\sqrt[4]{2}^2+fi\sqrt[4]{2}+hi\sqrt[4]{2}^3\in\mathbb{Q}(i\sqrt[4]{2})$. Cela montre que $L^{\langle r^2s\rangle}\subset\mathbb{Q}(i\sqrt[4]{2})$, et comme $\langle r^2s\rangle$ est d'indice 4 dans D_4 et que $\mathbb{Q}(i\sqrt[4]{2})$ est de degré 4 sur $\mathbb{Q}$, on doit avoir $L^{\langle r^2s\rangle}=\mathbb{Q}(i\sqrt[4]{2})$.
De même, un calcul montre que la condition $rs(\alpha)=\alpha$ implique $b=f$, $c=e=0$ et $d=-h$, donc α s'écrit plus simplement $\alpha=a+b\sqrt[4]{2}+d\sqrt[4]{2}^3+bi\sqrt[4]{2}+gi\sqrt[4]{2}^2-di\sqrt[4]{2}^3=a+b(\sqrt[4]{2}+i\sqrt[4]{2})+d(\sqrt[4]{2}^3-\sqrt[4]{2}^3)+gi\sqrt{2}$, et a, b, d et g sont des rationnels arbitraires. Pour choisir quelque chose de simple, on pose $a=d=g=0$ et $b=1$, de sorte que $\alpha=\sqrt[4]{2}+i\sqrt[4]{2}=(1+i)\sqrt[4]{2}$. On vient donc de montrer que $\mathbb{Q}(\alpha)\subset L^{\langle rs\rangle}$.
Or

$$\alpha=(1+i)\sqrt[4]{2}\Longrightarrow\alpha^2=2i\sqrt{2}\Longrightarrow\alpha^4=-8$$

donc $X^4+8\in\mathbb{Q}[X]$ est annulateur de α. En réduisant modulo 5 on vérifie de plus qu'il est irréductible, et c'est donc le polynôme minimal de α sur $\mathbb{Q}$. Ainsi, $\mathbb{Q}(\alpha)$ est de degré 4 sur $\mathbb{Q}$, et comme $\langle rs\rangle$ est d'indice 4 dans D_4, on doit avoir $\mathbb{Q}(\alpha)=L^{\langle rs\rangle}$. On procède de même pour trouver toutes les sous-extensions de L, et on a alors un diagramme complet.

4.4 Groupes de Galois comme groupes de permutations

Comme les exemples ci-dessus le montrent, établir une correspondance galoisienne nécessite de connaître le groupe de Galois, sa structure et ses sous-groupes. Le but de cette section est d'établir, avec de nouveaux outils, des résultats pour déterminer de façon plus systématique un groupe de Galois.

4.4.1 Le groupe S_p comme groupe de Galois

On donne un premier critère valide pour les extensions galoisiennes de degré un nombre premier p. Pour cela, on a besoin de quelques résultats sur les groupes symétriques et leurs générateurs.

Lemme 4.11 Dans S_p, une permutation d'ordre p est un $p-$cycle.

Preuve. Soit $\pi \in S_p$ d'ordre p. On peut écrire π en produits de cycles à supports disjoints, $\pi = \pi_1 \dots \pi_r$. Notons de plus n_i la longueur du cycle π_i, pour $1 \leq i \leq r$.
Alors $p = \mathrm{o}(\pi) = \mathrm{ppcm}(n_1, \dots, n_r)$. Comme p est premier et que n_i divise p, on a donc $n_i = 1$ ou $n_i = p$.
Si $n_i = 1$, la permutation correspondante π_i n'a aucun effet dans l'écriture de π, et on peut donc la supprimer.
π est donc un produit de $p-$cycles à supports disjoints. Comme dans S_p deux cycles de longueur p ne peuvent pas être disjoints, on en déduit que π n'est formé que d'un seul $p-$cycle, comme voulu. □

Lemme 4.12 Soit $n \geq 1$, et $\sigma = (12 \dots n) \in S_n$.
Si $1 \leq a < b \leq n$ et si $\mathrm{pgcd}(b-a, n) = 1$, alors (ab) et σ engendrent S_n.

Preuve. On commence par observer que σ^{b-a} est aussi un $n-$cycle, qui envoie a sur b :

$$\sigma^{b-a}(a) = \sigma^{b-a-1}(a+1) = ... = \sigma(a + (b-a-1)) = \sigma(b-1) = b.$$

Ensuite, on a $\langle \sigma \rangle = \langle \sigma^{b-a} \rangle$. L'inclusion $\langle \sigma \rangle \supset \langle \sigma^{b-a} \rangle$ est claire puisque $\sigma^{b-a} \in \langle \sigma \rangle$.
Pour l'inclusion inverse, on utilise le fait que $\mathrm{pgcd}(b-a, n) = 1$: par le théorème de Bézout, il existe $x, y \in \mathbb{Z}$ tels que $1 = (b-a)x + ny$. Alors

$$\sigma = \sigma^1 = \sigma^{(b-a)x+ny} = (\sigma^{b-a})^x (\sigma^n)^y = (\sigma^{b-a})^x$$

puisque $\sigma^n = 1$. Cela montre que $\sigma \in \langle \sigma^{b-a} \rangle$, et donc $\langle \sigma \rangle \subset \langle \sigma^{b-a} \rangle$. Ainsi $\langle (ab), \sigma \rangle = \langle (ab), \sigma^{b-a} \rangle = \langle (ab), (ab \dots) \rangle$ et, en re-numérotant les éléments permutés (*i.e.* faire une conjugaison dans S_n), (ab) devient (12) et $(ab \dots)$ devient $(12 \dots n)$.
On conclut donc que $\langle (ab), \sigma \rangle = \langle (12), (12 \dots n) \rangle = S_n$. □

Le lemme 4.12 n'est pas vrai en général si $\mathrm{pgcd}(b-a, n) > 1$. Par exemple, dans S_4, (13) et (1234) engendre un sous-groupe propre d'ordre 8, isomorphe à D_4.

Corollaire 4.13 Soit $p \geq 2$ premier.
Un $p-$cycle et une transposition arbitraire engendrent S_p.

Preuve. Quitte à re-numéroter, on peut supposer que le $p-$cycle est $(12 \dots p)$. Notons $\sigma = (ab)$ une transposition arbitraire.
On a bien sûr $\mathrm{pgcd}(b-a, p) = 1$, et le lemme 4.12 nous indique que σ et $(12 \dots p)$ engendrent S_p. □

On établit alors facilement le résultat voulu.

Théorème 4.14 Soit $p \geq 2$ premier.
Soit $f \in \mathbb{Q}[X]$ irréductible, de degré p, avec exactement deux racines non-réelles. Alors $\mathrm{Gal}(f) \simeq S_p$.

Preuve. Soit $L = \mathbb{Q}(r_1, \dots, r_p)$ un corps de décomposition de f sur $\mathbb{Q}$. Par le théorème 4.9(*iii*), $\mathrm{Gal}(f)$ s'identifie à un sous-groupe de S_p. De plus,

$$|\mathrm{Gal}(f)| = [L : \mathbb{Q}] = [L : \mathbb{Q}(r_1)][\mathbb{Q}(r_1) : \mathbb{Q}] = [L : \mathbb{Q}(r_1)]p$$

donc p divise $|\mathrm{Gal}(f)|$. Par le théorème de Cauchy, $\mathrm{Gal}(f)$ contient un élément d'ordre p, qui est un $p-$cycle par le lemme 4.11. Ensuite, en considérant L comme un sous-corps de $\mathbb{C}$, la restriction de la conjugaison complexe à L est un élément de $\mathrm{Gal}(f)$. Comme f a exactement deux racines complexes conjuguées, la conjugaison les permute et fixe les autres racines réelles, ce qui correspond à une transposition dans S_p. Ainsi, $\mathrm{Gal}(f)$ comme sous-groupe de S_p contient un $p-$cycle et une transposition. Il suffit d'utiliser le corollaire 4.13 pour conclure que $\mathrm{Gal}(f) \simeq S_p$. □

Exemples. (i) $f = X^3 - X - 1$ est de degré 3 et irréductible sur $\mathbb{Q}$ puisque sa réduction modulo 2 est irréductible. Une étude de fonctions montre qu'il n'a qu'une racine réelle, et donc deux racines complexes. Le théorème 4.14 s'applique alors, et $\mathrm{Gal}(f) \simeq S_3$.
(ii) Le polynôme $f = X^5 - 4X - 1$ est irréductible dans $\mathbb{Q}[X]$ puisqu'il est irréductible modulo 5. Il a trois racines réelles, donc $\mathrm{Gal}(f) \simeq S_5$.
(iii) On montre facilement que les polynômes $X^3 - 3X - 1$ et $X^3 - 4X - 1$ sont irréductibles sur $\mathbb{Q}$, et ont tous deux trois racines réelles. On ne peut donc pas utiliser le théorème 4.14 pour déterminer le groupe de Galois.

Remarque. La condition "f irréductible" dans le théorème 4.14 est nécessaire. Par exemple, $f = X^5 - 6X^4 + 12X^3 - 12X^2 + 11X - 6$ a trois racines réelles et deux racines complexes, mais son groupe de Galois est isomorphe à $\mathbb{Z}/2\mathbb{Z}$, puisque $f = (X-1)(X-2)(X-3)(X^2+1)$.

4.4.2 Discriminant

Pour identifier plus facilement un groupe de Galois comme sous-groupe de S_n, il est pratique de pouvoir déterminer si ce groupe de Galois est en fait inclus dans A_n.

Définition 4.15 Soit $f \in K[X]$ de degré $n \geq 1$.
Si f se décompose dans un corps de décomposition comme $f(X) = c(X - r_1)...(X - r_n)$, son *discriminant*, noté Δ_f ou $\mathrm{disc}(f)$, est défini par

$$\Delta_f = \prod_{i<j} (r_j - r_i)^2 = \left(\prod_{i<j} (r_j - r_i) \right)^2$$

On vérifie facilement que $\Delta_f \in K$ et que $\Delta_f \neq 0 \iff f$ est séparable.
Pour des polynômes de degré petit, on peut donner des formules explicites pour calculer le discriminant :

$$\begin{aligned}
&\mathrm{disc}(X^2 + aX + b) = a^2 - 4b \\
&\mathrm{disc}(X^3 + aX + b) = -4a^3 - 27b^2 \\
&\mathrm{disc}(X^3 + aX^2 + bX + c) = a^2b^2 + 18abc - 4b^3 - 4a^3c - 27c^2 \\
&\mathrm{disc}(X^4 + aX + b) = -27a^4 + 256b^3 \\
&\mathrm{disc}(X^5 + aX + b) = 256a^5 + 3125b^4
\end{aligned}$$

En fait, de manière plus générale, pour deux entiers $n, m \geq 1$ et $d = \mathrm{pgcd}(m, n)$, on a

$$\mathrm{disc}(X^n + aX^m + b) = (-1)^{\frac{n(n-1)}{2}} b^{m-1} ((-1)^{\frac{n}{d}-1} m^{\frac{m}{d}} (n-m)^{\frac{n-m}{d}} a^{\frac{n}{d}} + n^{\frac{n}{d}} b^{\frac{n-m}{d}})^d$$

Théorème 4.16 Soit K un corps de caractéristique différente de 2.
Soit $f \in K[X] \setminus K$ unitaire et séparable de degré n, et soit L un corps de décomposition de f sur K.
Alors $\mathrm{Gal}(f)$ est isomorphe à un sous-groupe de A_n si, et seulement si, Δ_f est un carré dans K.

Preuve. f est séparable, donc ses racines $r_1, \ldots, r_n$ sont distinctes dans $L = K(r_1, \ldots, r_n)$, et comme $r_1, \ldots, r_n$ sont séparables, L/K est séparable. De plus, L est un corps de décomposition de f sur K donc L/K est normale. Elle est donc galoisienne, et $K = L^{\mathrm{Gal}(L/K)}$ par le théorème 4.4. Il suffit alors d'observer que

$$\begin{aligned}
\Delta_f \quad \text{est un carré dans } K \quad &\iff \prod_{i<j} (r_j - r_i) \in K \\
&\iff \prod_{i<j} (r_j - r_i) \in L^{\mathrm{Gal}(L/K)}
\end{aligned}$$

$$\begin{aligned}
&\iff \forall \sigma \in \mathrm{Gal}(L/K),\ \sigma\Big(\prod_{i<j}(r_j - r_i)\Big) = \prod_{i<j}(r_j - r_i)\\
&\iff \forall \sigma \in \mathrm{Gal}(L/K),\ \prod_{i<j}(\sigma(r_j) - \sigma(r_i)) = \prod_{i<j}(r_j - r_i)\\
&\iff \forall \sigma \in \mathrm{Gal}(L/K),\ \varepsilon(\sigma)\prod_{i<j}(r_j - r_i) = \prod_{i<j}(r_j - r_i)\\
&\iff \forall \sigma \in \mathrm{Gal}(L/K),\ \varepsilon(\sigma) = 1\\
&\iff \forall \sigma \in \mathrm{Gal}(L/K),\ \sigma \in A_n
\end{aligned}$$

Cela est l'énoncé voulu. □

Ici, on a fait un léger abus de notation en dénotant par σ à la fois les éléments de $\mathrm{Gal}(L/K)$ et les éléments du sous-groupe de S_n isomorphe à $\mathrm{Gal}(L/K)$.

Corollaire 4.17 Soit K un corps de caractéristique différente de 2.
Soit $f \in K[X]$ unitaire, irréductible et séparable de degré 3.
Alors

$$\mathrm{Gal}(f) \simeq \begin{cases} A_3 & \text{si } \Delta_f \text{ est un carré dans } K \\ S_3 & \text{sinon} \end{cases}$$

Preuve. Comme f est irréductible, le théorème 4.9(*iii*) nous indique que $\mathrm{Gal}(f)$ est isomorphe à un sous-groupe transitif de S_3. Or les seuls sous-groupes transitifs de S_3 sont S_3 et A_3, par l'exercice 15 ci-dessous.
Si Δ_f est un carré dans K, $\mathrm{Gal}(f)$ est un sous-groupe de A_3 par le théorème 4.16, et donc $\mathrm{Gal}(f) \simeq A_3$. Sinon, $\mathrm{Gal}(f)$ n'est pas contenu dans A_3, et la seule possibilité restante est $\mathrm{Gal}(f) \simeq S_3$. □

Exemples. (*i*) On a établi ci-dessus avec le théorème 4.14 que $f = X^3 - X - 1$ a S_3 comme groupe de Galois. On peut retrouver ce résultat grâce au corollaire 4.17 : le discriminant de $X^3 - X - 1$ est -23, qui n'est pas un carré dans $\mathbb{Q}$, donc $\mathrm{Gal}(f) \simeq S_3$.
(*ii*) En revanche, le théorème 4.14 ne nous permettait pas de déterminer le groupe de Galois de X^3-3X-1 et X^3-4X-1. C'est maintenant possible : $X^3 - 3X - 1$ a $81 = 9^2$ comme discriminant, donc a A_3 pour groupe de Galois, tandis que $\mathrm{disc}(X^3 - 4X - 1) = 229$, donc le groupe de Galois de $X^3 - 4X - 1$ est S_3.

Le corollaire 4.17 est très utile en pratique, mais son utilisation appelle tout de même quelques remarques importantes. Tout d'abord, l'hypothèse "f irréductible" est essentielle. Par exemple, $f = X^3 - 7X - 6 \in \mathbb{Q}[X]$ vérifie $\Delta_f = 20^2$, mais $\mathrm{Gal}(f) \simeq \{1\} \neq A_3$, puisque f est réductible : $f = (X + 1)(X + 2)(X - 3)$. De même, $g = X^3 - 2X - 1$ a discriminant 5, mais son groupe de Galois n'est pas S_3, puisque $g = (X - 1)(X^2 + X - 1)$. En fait, $\mathrm{Gal}(g) \simeq \mathbb{Z}/2\mathbb{Z}$.
Ensuite, le corollaire est faux en caractéristique 2. Par exemple, $f(X) = X^3 + YX + Y \in \mathbb{F}_2[X]$ est irréductible par le critère d'Eisenstein généralisé, séparable, et a discriminant Y^2, mais son groupe de Galois est S_3.
Enfin, pour un polynôme f de degré 3 de la forme $f = X^3 + aX^2 + bX + c$, on peut poser $Y = X + \frac{1}{3}a$, et vérifier que $f = Y^3 + pY + q$. On peut donc se restreindre aux polynômes de cette forme. Pour ceux-là, on a $f' = 3Y^2 + p$, et la condition "f séparable" du corollaire 4.17 est satisfaite dès que $\mathrm{char}(K) \neq 3$.

4.4.3 Cubique résolvante

Pour classifier les groupes de Galois des polynômes irréductibles de degré 4, on a déjà besoin de connaître les sous-groupes transitifs de S_4. On note $V = \{\mathrm{id}, (12)(34), (13)(24), (23)(14)\} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ le sous-groupe de Klein.

Proposition 4.18 Les sous-groupes transitifs de S_4 sont S_4, A_4, V, D_4 et $\langle\sigma\rangle \simeq \mathbb{Z}/4\mathbb{Z}$, où σ est un des six 4-cycles.

Preuve. Soit $G \leqslant S_4$ un sous-groupe transitif de S_4. Alors, comme $G \curvearrowright \{1, 2, 3, 4\}$ est transitive, elle définit une unique orbite, et la formule des orbites implique que $4 \mid |G|$. Les possibilités sont donc $|G| \in \{4, 8, 12, 24\}$.
Si $|G| = 24$, alors $G = S_4$. Si $|G| = 12$, alors $G = A_4$. Si $|G| = 8$, la classification des groupes d'ordre 8 et le fait que G est un sous-groupe de S_4 implique que $G \simeq D_4$. Pour finir, on traite le cas $|G| = 4$.
Si G est cyclique, alors $G = \langle\sigma\rangle$, où σ est d'ordre 4, et les éléments d'ordre 4 dans S_4 sont les 4−cycles. Sinon, $G \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, et donc $G = V$. □

Il existe d'autres sous-groupes de S_4 isomorphes à V, tel que $\{\mathrm{id}, (12), (34), (12)(34)\}$, mais ils ne sont pas transitifs.

Le discriminant Δ_f d'un polynôme f irréductible séparable de degré 3 nous permet de déterminer son groupe de Galois. Dire que le discriminant est un carré dans le corps de base K est équivalent à dire que le polynôme $X^2 - \Delta_f$ scinde dans K. Pour résumer, le groupe de Galois d'un polynôme de degré 3 dépend du comportement d'un certain polynôme de degré 2. De la même façon, on verra que le groupe de Galois d'un polynôme de degré 4 dépend du comportement d'un certain polynôme de degré 3.

Soit donc à nouveau K un corps de caractéristique différente de 2, et $f = X^4 + c_1X^3 + c_2X^2 + c_3X + c_4 \in K[X]$ irréductible. Notons alors que $f' = 4X^3 + 3c_1X^2 + 2c_2X + c_3 \neq 0$ puisque $\mathrm{char}(K) \neq 2$. Le lemme 3.19(*ii*) implique alors que f est séparable. Ainsi, contrairement aux cas des polynômes de degré 3, nous n'aurons pas à faire l'hypothèse que nos polynômes sont séparables : cela est une conséquence directe du fait que $\mathrm{char}(K) \neq 2$.
Soit ensuite L un corps de décomposition de f sur K et notons a_1, a_2, a_3 et a_4 les racines de f dans L. Posons

$$b_1 = a_1a_2 + a_3a_4,\ b_2 = a_1a_3 + a_2a_4,\ b_3 = a_1a_4 + a_2a_3$$

On reconnaît dans la définition des b_i les permutations (12)(34), (13)(24) et (14)(23) qui forment le groupe V. Ainsi, si on est capable d'identifier les automorphismes du groupe de Galois qui fixent les b_i, on pourra faire un lien entre le groupe de Galois et V.

Définition 4.19 La *cubique résolvante* de f est le polynôme R_f défini comme $R_f(X) = (X-b_1)(X-b_2)(X-b_3) \in L[X]$.

On vérifie alors que $R_f(X) = X^3 - c_2X^2 + (c_1c_3 - 4c_4)X - (c_1^2c_4 + c_3^2 - 4c_2c_4)$. En particulier, $R_f \in K[X]$.

Lemme 4.20 On a $\Delta_{R_f} = \Delta_f$. En particulier, R_f est séparable.

Preuve. On observe que $b_1 - b_2 = a_1a_2 - a_1a_3 - a_2a_4 + a_3a_4 = (a_1 - a_4)(a_2 - a_3)$.
De même, $b_1 - b_3 = (a_1 - a_3)(a_2 - a_4)$ et $b_2 - b_3 = (a_1 - a_2)(a_3 - a_4)$. La définition du discriminant fournit alors

$$\Delta_{R_f} = (b_1 - b_2)^2(b_1 - b_3)^2(b_2 - b_3)^2 = (a_1 - a_4)^2(a_2 - a_3)^2(a_1 - a_3)^2(a_2 - a_4)^2(a_1 - a_2)^2(a_3 - a_4)^2 = \Delta_f.$$

Comme f est séparable, $\Delta_f \neq 0$, ce qui implique $\Delta_{R_f} \neq 0$, et donc R_f est séparable. □

On peut alors énoncer la classification des groupes de Galois des polynômes de degré 4.

Théorème 4.21 Soit K un corps de caractéristique différente de 2.
Soit $f \in K[X]$ unitaire et irréductible de degré 4.
Alors

$$\mathrm{Gal}(f) \simeq \begin{cases} S_4 & \text{si } R_f \text{ est irréductible sur } K \text{ et que } \Delta_f \text{ n'est pas un carré dans } K \\ A_4 & \text{si } R_f \text{ est irréductible sur } K \text{ et que } \Delta_f \text{ est un carré dans } K \\ V & \text{si } R_f \text{ est scindé sur } K \\ D_4 & \text{si } R_f \text{ a exactement une racine dans } K \text{ et que } f \text{ est irréductible sur } K(\sqrt{\Delta_f}) \\ \mathbb{Z}/4\mathbb{Z} & \text{si } R_f \text{ a exactement une racine dans } K \text{ et que } f \text{ n'est pas irréductible sur } K(\sqrt{\Delta_f}) \end{cases}$$

Preuve. Soit L un corps de décomposition de f sur K et M un corps de décomposition de R_f sur K, de sorte que $M = K(b_1, b_2, b_3) \subset K(a_1, a_2, a_3, a_4) = L$. Ensuite, L/K est séparable puisque les a_i sont séparables, donc L/K est galoisienne. En particulier, $|\mathrm{Gal}(f)| = [L : K]$.
De plus, M/K est normale, donc $\mathrm{Gal}(L/M)$ est un sous-groupe normal de $\mathrm{Gal}(L/K)$, et

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

Notons de plus ρ: $\mathrm{Gal}(L/K) \longrightarrow S_4$ le morphisme injectif fourni par le théorème 4.9(*iii*). Alors, au vu de la définition des b_i, les éléments de $\mathrm{Gal}(L/K)$ fixant les b_i sont ceux dont l'image par ρ est un élément de V, *i.e.* sont les éléments de $\mathrm{Gal}(L/K)$ appartenant à $\rho^{-1}(V)$. Mais d'autre part, un élément de $\mathrm{Gal}(L/K)$ fixant les b_i fixe en fait $K(b_1, b_2, b_3) = M$, et est donc dans $\mathrm{Gal}(L/M)$. On a donc établi l'égalité $(*)$

$$\mathrm{Gal}(L/M) = \mathrm{Gal}(L/K) \cap \rho^{-1}(V).$$

On raisonne alors par disjonction de cas.
(i) R_f est irréductible sur K et Δ_f n'est pas un carré dans K : on a les égalités

$$|\mathrm{Gal}(f)| = [L:K] = [L:K(a_1)][K(a_1):K] = [L:K(a_1)]\deg(f) = 4[L:K(a_1)]$$
$$|\mathrm{Gal}(f)| = [L:K] = [L:K(b_1)][K(b_1):K] = [L:K(b_1)]\deg(R_f) = 3[L:K(b_1)]$$

donc $|\mathrm{Gal}(f)|$ est divisible par 3 et 4. Comme 3 et 4 sont premiers entre eux, $|\mathrm{Gal}(f)|$ est divisible par $3 \cdot 4 = 12$. Cela implique que $\mathrm{Gal}(f) \simeq A_4$ ou $\mathrm{Gal}(f) \simeq S_4$. Mais Δ_f n'est pas un carré dans K, donc $\mathrm{Gal}(f)$ n'est pas isomorphe à un sous-groupe de A_4 par le théorème 4.16. On conclut donc que $\mathrm{Gal}(f) \simeq S_4$.
(ii) R_f est irréductible sur K et Δ_f est un carré dans K : le même raisonnement que ci-dessus est valable, et $\mathrm{Gal}(f) \simeq A_4$ ou $\mathrm{Gal}(f) \simeq S_4$. Or Δ_f est un carré dans K, donc $\mathrm{Gal}(f)$ est un sous-groupe de A_4 par le théorème 4.16. Il reste donc la seule possibilité $\mathrm{Gal}(f) \simeq A_4$.
(iii) R_f est scindé sur K : dans ce cas $M = K$, et l'égalité $(*)$ ci-dessus s'écrit $\mathrm{Gal}(L/K) = \mathrm{Gal}(L/K) \cap \rho^{-1}(V)$, ce qui implique $\mathrm{Gal}(L/K) \subset \rho^{-1}(V)$. On en tire que $\mathrm{Gal}(f) = \mathrm{Gal}(L/K) \simeq \rho(\mathrm{Gal}(L/K)) \leqslant V$, donc $\mathrm{Gal}(f)$ est d'ordre 1, 2 ou 4. Le même raisonnement que en (i) montre que 4 divise $|\mathrm{Gal}(f)|$. On conclut que $\mathrm{Gal}(f) \simeq V$.
(iv) R_f a exactement une racine dans K et f est irréductible sur $K(\sqrt{\Delta_f})$: M/K est de degré 2, donc $\mathrm{Gal}(M/K)$ est d'ordre 2, donc non-isomorphe à un sous-groupe de A_3. Par le théorème 4.16, cela signifie que Δ_{R_f} n'est pas un carré dans K. Or, par le lemme 4.20, $\Delta_{R_f} = \Delta_f$, donc Δ_f n'est pas un carré dans K. Ainsi, $K(\sqrt{\Delta_f})/K$ est de degré 2, donc normale, donc $\mathrm{Gal}(K(\sqrt{\Delta_f})/K)$ est normal dans $\mathrm{Gal}(L/K)$ par le théorème 4.7(v), et on a

$$\mathrm{Gal}(L/K)/\mathrm{Gal}(K(\sqrt{\Delta_f})/K) \simeq \mathrm{Gal}(L/K(\sqrt{\Delta_f}))$$

Le groupe $\mathrm{Gal}(K(\sqrt{\Delta_f})/K)$ est donc d'indice 2 dans $\mathrm{Gal}(L/K)$. Comme f est irréductible sur $K(\sqrt{\Delta_f})$, $|\mathrm{Gal}(L/K(\sqrt{\Delta_f}))|$ est divisible par $\deg(f) = 4$, donc $|\mathrm{Gal}(L/K)|$ est divisible par $2 \cdot 4 = 8$. Cela entraîne $\mathrm{Gal}(L/K) \simeq D_4$ ou $\mathrm{Gal}(L/K) \simeq S_4$.
Si $\mathrm{Gal}(L/K) \simeq S_4$, on a alors $\mathrm{Gal}(K(\sqrt{\Delta_f})/K) \simeq A_4$ (le seul sous-groupe d'indice 2 de S_4), et donc l'isomorphisme ci-dessus indique que

$$\mathrm{Gal}(L/K(\sqrt{\Delta_f})) \simeq S_4/A_4 \simeq \mathbb{Z}/2\mathbb{Z}$$

qui n'est pas un sous-groupe transitif de S_4. Cela contredit le théorème 4.9(iii). On ne peut donc pas avoir $\mathrm{Gal}(L/K) \simeq S_4$. Il ne reste que la possibilité $\mathrm{Gal}(f) = \mathrm{Gal}(L/K) \simeq D_4$.
(v) R_f a exactement une racine dans K et f n'est pas irréductible sur $K(\sqrt{\Delta_f})$: $\mathrm{Gal}(L/K)$ doit avoir un ordre divisible par 4, avec un sous-groupe $\mathrm{Gal}(K(\sqrt{\Delta_f})/K)$ d'indice 2. De plus, puisque f n'est pas irréductible sur $K(\sqrt{\Delta_f})$, ce sous-groupe doit être non-transitif. Enfin, on utilise que $|\mathrm{Gal}(K(\sqrt{\Delta_f})/K)| = 2$ pour conclure que $\mathrm{Gal}(L/K) \simeq \mathbb{Z}/4\mathbb{Z}$ et $\mathrm{Gal}(K(\sqrt{\Delta_f})/K) \simeq \mathbb{Z}/2\mathbb{Z}$. □

Exemples. (i) $f = X^4 - X - 1 \in \mathbb{Q}[X]$ est irréductible sur $\mathbb{F}_2$, donc irréductible sur $\mathbb{Q}$. Son discriminant est -283, qui n'est pas un carré dans $\mathbb{Q}$, donc $\mathrm{Gal}(f) \simeq S_4$.
(ii) Le polynôme $X^4 + 8X + 12 \in \mathbb{Q}[X]$ est irréductible sur $\mathbb{Q}$. Il n'a pas de racines rationnelles, et une éventuelle factorisation avec deux polynômes de degré 2 est incompatible avec sa factorisation mod 5 :

$$X^4 + 8X + 12 \equiv (X-4)(X^3 + 4X^2 + X + 2) \mod 5$$

Sa cubique résolvante est $X^3 - 48X - 64$ qui est irréductible sur $\mathbb{Q}$ puisque irréductible mod 5. De plus, le discriminant de $X^4 + 8X + 12$ est $331776 = 576^2$, donc le théorème 4.21 implique que $\mathrm{Gal}(X^4 + 8X + 12) \simeq A_4$.
(iii) Soit $f = X^4 + 36X + 63$. On vérifie que f est irréductible sur $\mathbb{Q}$, et que sa cubique résolvante est $R_f = X^3 - 252X - 1296 = (X-18)(X+6)(X+12)$, donc $\mathrm{Gal}(f) \simeq V$.

Comme pour le corollaire 4.17, la condition "f irréductible" du théorème 4.21 est essentielle : par exemple, $X^4 + 4$ a discriminant 128^2 et sa cubique résolvante vaut $X^3 - 16X = X(X-4)(X+4)$, ce qui suggère que $\mathrm{Gal}(X^4 + 4) \simeq V$. Pourtant, $X^4 + 4 = (X^2 - 2X + 2)(X^2 + 2X + 2)$ est réductible. En fait, on peut montrer que $\mathbb{Q}(i)$ est un corps de décomposition de $X^4 + 4$ sur $\mathbb{Q}$, et son groupe de Galois est alors cyclique d'ordre 2, engendré par la conjugaison complexe.

Terminons ce chapitre en énonçant le problème de Galois inverse, en deux variantes.

Problème 4.22 (problème de Galois inverse) Soit G un groupe fini.
(i) Existe-t-il une extension galoisienne L/K telle que $\mathrm{Gal}(L/K) \simeq G$?
(ii) Existe-t-il une extension galoisienne $L/\mathbb{Q}$ telle que $\mathrm{Gal}(L/\mathbb{Q}) \simeq G$?

4.5 Exercices

Exercice 1. Soit K un corps de caractéristique différente de 2.
Montrer que toute extension quadratique L/K est galoisienne.

Exercice 2. Soit K un corps.

(i) Montrer que toute extension finie et séparable de K peut être plongée dans une extension galoisienne de K.
(ii) Montrer qu'une extension finie inséparable de K ne peut pas être plongée dans une extension galoisienne de K.

Exercice 3. Soit K un corps, $\overline{K}$ sa clôture algébrique et $G = \mathrm{Gal}(\overline{K}/K)$.
Montrer que K est parfait si, et seulement si, $\overline{K}^G = K$.

Exercice 4. Soit p un premier, $K = \mathbb{F}_p(Y)$ et $f(X) = X^p - Y \in K[X]$. Soit $L = K[X]/(f(X))$.
En utilisant le corollaire 4.6, montrer que L/K n'est pas galoisienne.

Exercice 5. Pour tout $n \geq 2$, trouver un polynôme séparable $f \in \mathbb{Q}[X]$ de degré $2n$, sans racines rationnelles, tel que $\mathrm{Gal}(f) \simeq \mathbb{Z}/2\mathbb{Z}$.

Exercice 6. Soient $K \subset L \subset M$ des extensions finies de corps.

(i) Supposons que M/L et L/K sont galoisiennes. Est-ce que M/K est galoisienne ?
(ii) Supposons que M/K est galoisienne. Est-ce que M/L est galoisienne ? Est-ce que L/K est galoisienne ?
(iii) Supposons que M/K est galoisienne et que $\mathrm{Gal}(M/K)$ est abélien. Est-ce que M/L est galoisienne ? Est-ce que L/K est galoisienne ?

Exercice 7. Soit $L = \mathbb{Q}(\sqrt{2}, i)$.
Justifier que $L/\mathbb{Q}$ est galoisienne, déterminer $\mathrm{Gal}(L/\mathbb{Q})$ et la correspondance de Galois associée. Quels sont les sous-corps M de L contenant $\mathbb{Q}$ tels que $M/\mathbb{Q}$ est normale ?

Exercice 8. Soit $a = \sqrt{2 + \sqrt{2}}$ et f son polynôme minimal sur $\mathbb{Q}$.
Calculer f, déterminer son corps de décomposition et $\mathrm{Gal}(f)$, et détailler la correspondance de Galois associée.

Exercice 9. Soit $f(X) = X^4 - 12X^2 + 18 \in \mathbb{Q}[X]$, et L un corps de décomposition de f sur $\mathbb{Q}$.

(i) Identifier L et donner $[L : \mathbb{Q}]$.
(ii) Est-ce que $\mathrm{Gal}(f)$ est isomorphe à $\mathbb{Z}/4\mathbb{Z}$, V, ou un autre groupe ?
(iii) Donner un générateur de chacune des extensions intermédiaires entre L et $\mathbb{Q}$.

Exercice 10. Soit p un nombre premier.
Déterminer la correspondance de Galois pour l'extension $\mathbb{F}_{p^{18}}/\mathbb{F}_p$.

Exercice 11. Soit p un nombre premier, et L un corps de décomposition de $X^3 - p \in \mathbb{Q}[X]$.
Déterminer $\mathrm{Gal}(L/\mathbb{Q})$, lister tous les sous-corps de L, tous les sous-groupes de $\mathrm{Gal}(L/\mathbb{Q})$, et détailler la correspondance de Galois associée.

Exercice 12. Soit η une racine primitive 5-ième de l'unité.
Calculer le polynôme minimal de η sur $\mathbb{Q}$, son corps de décomposition L, et $\mathrm{Gal}(L/\mathbb{Q})$. Expliciter la correspondance de Galois associée.

Exercice 13. Déterminer le groupe de Galois de $X^6 - 2 \in \mathbb{Q}[X]$.

Exercice 14. Le but de cet exercice est de montrer que le théorème 4.7 (correspondance de Galois) est faux pour les extensions infinies. Soit p un premier, $K = \mathbb{F}_p$ et $L = \overline{\mathbb{F}_p}$ sa clôture algébrique. Soit $\sigma \colon L \longrightarrow L$, $x \longmapsto x^p$ l'endomorphisme de Frobenius. Posons $H := \langle \sigma \rangle \leqslant \mathrm{Gal}(L/K)$.

(i) Justifier que L/K est galoisienne infinie.

(*ii*) Déterminer L^H.
Soit $L' = \bigcup_{n\geq 0} \mathbb{F}_{p^{2^n}}$.
(*iii*) Montrer que $L' \subset L$ et que $L' \neq L$. *Indication* : On pourra utiliser que $L = \bigcup_{n\geq 0} \mathbb{F}_{p^{n!}}$.
(*iv*) En déduire que $\mathrm{Gal}(L/L')$ est non trivial.
(*v*) Montrer que $\mathrm{Gal}(L/L') \not\subseteq H$ et que $H \neq \mathrm{Gal}(L/K)$.
(*vi*) Montrer que H n'est le groupe de Galois d'aucune sous-extension de L/K, c'est-à-dire qu'il n'existe pas de sous-corps M de L contenant K tel que $H = \mathrm{Gal}(L/M)$.

Exercice 15. Montrer que (12) et $(12\dots n)$ engendrent S_n.

Exercice 16. Montrer que les seuls sous-groupes transitifs de S_3 sont A_3 et S_3.

Exercice 17. Montrer qu'un sous-groupe transitif de S_n contenant une transposition et un $(n-1)-$cycle est égal à S_n.

Exercice 18. Pour $f = X^3 - aX - 1 \in \mathbb{Q}[X]$, où $1 \leq a \leq 6$, déterminer $\mathrm{Gal}(f)$.

Exercice 19. Soit $k \in \mathbb{Z}$, et $a := k^2 + k + 7$.
Montrer que $X^3 - aX + a$ est irréductible sur $\mathbb{Q}$, et que son groupe de Galois est isomorphe à A_3.

Exercice 20. Déterminer le groupe de Galois sur $\mathbb{Q}$ des polynômes suivants.

(*i*) $X^3 - 7X - 1$
(*ii*) $X^3 - 7X^2 + 14X - 7$
(*iii*) $X^3 - 7X^2 + 14X - 8$
(*iv*) $X^3 - X^2 - 2X + 1$

Déterminer aussi le groupe de Galois de $X^3 + X + 1$ sur $\mathbb{F}_5$.

Exercice 21. Combien existe-t-il de sous-groupes isomorphes à $\mathbb{Z}/4\mathbb{Z}$ dans S_4 ?

Exercice 22. Déterminer le groupe de Galois sur $\mathbb{Q}$ des polynômes suivants.

(*i*) $X^4 + 2X + 2$
(*ii*) $X^4 + 5X + 5$
(*iii*) $X^4 + 3X + 20$
(*iv*) $X^4 + 24X + 36$
(*v*) $X^4 + 24X + 73$

Exercice 23. Soit K un corps de caractéristique différente de 2, et $f = X^4 + bX^2 + d \in K[X]$ irréductible.
Montrer que si d est un carré dans K, alors $\mathrm{Gal}(f) \simeq V$.

Exercice 24. Soit $p \in \mathbb{Z}$ un nombre premier, et $f = X^n - p \in \mathbb{Q}[X]$. Prouver que $\mathrm{Gal}(f)$ n'est pas abélien.
Plus généralement, montrer que si $f \in \mathbb{Q}[X]$ est irréductible et a au moins une racine réelle et une racine complexe non-réelle, alors $\mathrm{Gal}(f)$ n'est pas abélien.

5 Applications de la théorie de Galois

Cette section est consacrée à plusieurs applications de la théorie de Galois, comme la résolubilité des équations par radicaux, les corps cyclotomiques ou le théorème fondamental de l'algèbre.

5.1 Extensions simples, éléments primitifs

La théorie de Galois fournit une méthode très efficace pour montrer qu'un élément d'une extension galoisienne est primitif, *i.e.* générateur de l'extension.

Théorème 5.1 Soit L/K une extension finie et galoisienne.
Pour tout $\gamma \in L$, $[K(\gamma) : K]$ est le cardinal de l'orbite de γ sous l'action du groupe de Galois $\mathrm{Gal}(L/K)$.
En particulier, γ est un élément primitif de L/K si, et seulement si, $|\{\sigma(\gamma) \mid \sigma \in \mathrm{Gal}(L/K)\}| = [L : K]$.

Preuve. Comme γ est séparable sur K, $[K(\gamma) : K]$ est le nombre de racines du polynôme minimal f de γ sur K, et ces racines sont toutes dans L puisque L/K est galoisienne. Or on a vu en proposition 4.1 que $\mathrm{Gal}(L/K)$ agit par permutation des racines de f dans L. Donc $[K(\gamma) : K] = |\{\sigma(\gamma) \mid \sigma \in \mathrm{Gal}(L/K)\}|$.
Ensuite, si γ est un élément primitif de L/K, alors $L = K(\gamma)$, donc $|\{\sigma(\gamma) \mid \sigma \in \mathrm{Gal}(L/K)\}| = [K(\gamma) : K] = [L : K]$.
Réciproquement, si $|\{\sigma(\gamma) \mid \sigma \in \mathrm{Gal}(L/K)\}| = [L : K]$, alors on a $[K(\gamma) : K] = [L : K]$, ce qui signifie que L et $K(\gamma)$ sont deux $K-$espaces vectoriels de même dimension. Comme $K(\gamma) \subset L$, ils doivent nécessairement coïncider, d'où $L = K(\gamma)$, donc γ est un élément primitif de L/K. □

Exemple. L'extension $\mathbb{Q}(i, \sqrt{5})/\mathbb{Q}$ est galoisienne, de degré 4. C'est le corps des racines de $f = (X^2 + 1)(X^2 - 5)$ et son groupe de Galois est isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Un élément $\sigma \in \mathrm{Gal}(f)$ est déterminé par $\sigma(i)$ et $\sigma(\sqrt{5})$. On voit alors que l'orbite de $i + \sqrt{5}$ sous l'action de $\mathrm{Gal}(f)$ est constitué de quatre éléments : $i + \sqrt{5}$, $i - \sqrt{5}$, $-i + \sqrt{5}$ et $-i - \sqrt{5}$. Le théorème précédent donne donc $\mathbb{Q}(i, \sqrt{5}) = \mathbb{Q}(i + \sqrt{5})$.

5.2 Corps cyclotomiques

Soit K un corps et $n \geq 1$. Soit $f = X^n - 1 \in K[X]$.

Définition 5.2 On appelle $n-$ième *corps cyclotomique* sur K tout corps de décomposition de f sur K.

Si L est un $n-$ième corps cyclotomique sur K, on notera $U_n(L) := \{a \in L \mid a^n = 1\}$ l'ensemble des racines de f dans L. Commençons par établir les premières propriétés des extensions cyclotomiques.

Proposition 5.3 Soit L un $n-$ième corps cyclotomique sur K.
(i) $U_n(L)$ est un groupe cyclique. De plus, si $a \in U_n(L)$ est tel que $U_n(L) = \langle a \rangle$, alors $L = K(a)$.
(ii) Si $\mathrm{char}(K) \nmid n$, alors $|U_n(L)| = n$.
(iii) Si $\mathrm{char}(K) = p \neq 0$ et si $n = p^l m$ avec $p \nmid m$, alors $U_n(L) = U_m(L)$. En particulier, L est un $m-$ième corps cyclotomique.
(iv) L/K est une extension galoisienne.

Preuve. (i) Tout d'abord, on montre facilement que $U_n(L)$ est un sous-groupe fini de L^*, et comme L^* est abélien, $U_n(L)$ est abélien. Soit $a \in U_n(L)$ d'ordre maximal d parmi les éléments de $U_n(L)$.
Par le théorème de Lagrange, d divise $|U_n(L)|$, d'où en particulier $d \leq |U_n(L)|$. D'autre part, pour tout $b \in U_n(L)$, on a $b^d = 1$, donc b est racine de $X^d - 1$. Cela implique $|U_n(L)| \leq d$, et finalement $d = |U_n(L)|$. On conclut que $U_n(L) = \langle a \rangle$ et $L = K(U_n(L)) = K(\langle a \rangle) = K(a)$.
(ii) $f' = nX^{n-1} \neq 0$ puisque $\mathrm{char}(K) \nmid n$. Ainsi f est séparable par le lemme 3.19 et a donc n racines distinctes, ce qui signifie $|U_n(L)| = n$.
(iii) Puisque $\mathrm{char}(K) = p$, on a les équivalences

$$a^n = 1 \iff a^n - 1 = 0 \iff a^{p^l m} - 1 = 0 \iff (a^m - 1)^{p^l} = 0 \iff a^m - 1 = 0 \iff a^m = 1$$

donc $U_n(L) = U_m(L)$.
(iv) L est un corps de décomposition de f sur K, donc L/K est normale. Comme f est séparable et que le polynôme minimal g de a sur K divise f dans $K[X]$, g est aussi séparable, donc a est séparable sur K, et le corollaire 3.31(ii) nous assure que $L = K(a)$ est séparable. L/K est donc galoisienne.

Un générateur a du groupe $U_n(L)$ est appelé une *racine primitive n-ième de l'unité*.
Pour travailler avec des corps cyclotomiques, on a aussi besoin de la *fonction indicatrice d'Euler*, dont on rappelle la définition et quelques propriétés.

Définition 5.4 Pour $n \geq 1$, $\varphi(n)$ est l'entier défini comme

$$\varphi(n) = |\{1 \leq m \leq n \mid \text{pgcd}(m, n) = 1\}|.$$

Proposition 5.5 (propriétés de la fonction indicatrice d'Euler)
(i) Soit $n \geq 1$. Alors $\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^*|$.
(ii) Soit $n \geq 1$ et G un groupe cyclique à n éléments. Alors $\varphi(n) = |\{g \in G \mid \langle g \rangle = G\}|$.
(iii) Soient n, $m \geq 1$ premiers entre eux. Alors $\varphi(nm) = \varphi(n)\varphi(m)$.
(iv) Soit p un premier et $k \geq 1$. Alors $\varphi(p^k) = (p-1)p^{k-1}$.

Preuve. (i) Soit $n \geq 1$. Soit $m \in \{1, \ldots, n\}$.
Par le théorème de Bézout,

$$\text{pgcd}(m, n) = 1 \iff \exists x, y \in \mathbb{Z},\ mx + ny = 1 \iff \exists x \in \mathbb{Z},\ [m][x] = [1] \iff [m] \in (\mathbb{Z}/n\mathbb{Z})^*$$

d'où $\varphi(n) = |\{1 \leq m \leq n \mid \text{pgcd}(m, n) = 1\}| = |(\mathbb{Z}/n\mathbb{Z})^*|$.
(ii) Puisque G est cyclique d'ordre n, $G \simeq \mathbb{Z}/n\mathbb{Z} = \{[0], [1], \ldots, [n-1]\}$. Comme ci-dessus, on montre avec le théorème de Bézout que $[m] \in G$ est un générateur si et seulement si $\text{pgcd}(m, n) = 1$. Cela permet de conclure.
(iii) Comme n et m sont premiers entre eux, le théorème des restes chinois nous assure qu'il existe un isomorphisme d'anneaux $\mathbb{Z}/nm\mathbb{Z} \simeq \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$. Il existe donc aussi un isomorphisme pour les groupes d'unités :

$$(\mathbb{Z}/nm\mathbb{Z})^* \simeq (\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z})^* = (\mathbb{Z}/n\mathbb{Z})^* \times (\mathbb{Z}/m\mathbb{Z})^*.$$

Le point (i) montre l'affirmation, puisqu'alors

$$\varphi(nm) = |(\mathbb{Z}/nm\mathbb{Z})^*| = |(\mathbb{Z}/n\mathbb{Z})^* \times (\mathbb{Z}/m\mathbb{Z})^*| = |(\mathbb{Z}/n\mathbb{Z})^*||(\mathbb{Z}/m\mathbb{Z})^*| = \varphi(n)\varphi(m).$$

(iv) Tout d'abord, on montre facilement que $x \leq p^k$ n'est pas premier avec p^k si et seulement si x est un multiple de p. Pour compter tous les nombres premiers avec p^k entre 1 et p^k, il suffit donc de retirer les multiples de p. Il y en a exactement $\left\lfloor \frac{p^k}{p} \right\rfloor = p^{k-1}$. Donc $\varphi(p^k) = p^k - p^{k-1} = (p-1)p^{k-1}$. □

Le point (ii) de la proposition 5.5, combiné avec (ii) de la proposition 5.3, dit exactement que si $\text{char}(K) \nmid n$, il y a $\varphi(n)$ racines primitives $n-$ièmes de l'unité.
La fonction indicatrice d'Euler joue un rôle clé pour de nombreux sujets en mathématiques. D'autres propriétés importantes de φ sont en exercices.

Théorème 5.6 Soient $n \geq 1$, K un corps tel que $\text{char}(K) \nmid n$, et L un $n-$ième corps cyclotomique.
Il existe un morphisme de groupes injectif $\text{Gal}(L/K) \hookrightarrow (\mathbb{Z}/n\mathbb{Z})^*$. En particulier, $\text{Gal}(L/K)$ est abélien.

Preuve. Soit $a \in U_n(L)$ tel que $\langle a \rangle = U_n(L)$.
Pour tout $\sigma \in \text{Gal}(L/K)$, on a $\langle \sigma(a) \rangle = U_n(L)$, donc on peut écrire $\sigma(a) = a^j$ pour un certain j vérifiant $\text{pgcd}(n, j) = 1$. Alors $[j] \in (\mathbb{Z}/n\mathbb{Z})^*$, et on définit l'application

$$\begin{aligned} \alpha \colon \text{Gal}(L/K) &\longrightarrow (\mathbb{Z}/n\mathbb{Z})^* \\ \sigma &\longmapsto [j] \end{aligned}$$

Soient σ, $\tau \in \text{Gal}(L/K)$. Ecrivons $\sigma(a) = a^j$, $\tau(a) = a^k$ où j et k sont premiers avec n. Alors $(\tau\sigma)(a) = a^{kj}$, ce qui implique

$$\alpha(\tau\sigma) = [kj] = [k][j] = \alpha(\tau)\alpha(\sigma)$$

et α est bien un morphisme de groupes.
Il est de plus injectif, puisque si σ, $\tau \in \mathrm{Gal}(L/K)$ sont tels que $\alpha(\sigma) = \alpha(\tau)$, alors $[j] = [k]$, donc $j - k$ est un multiple de n, que l'on écrit $j - k = mn$. Alors

$$a^{j-k} = a^{mn} = (a^n)^m = 1^m = 1 \Longrightarrow a^j = a^k \Longrightarrow \sigma(a) = \tau(a).$$

Comme σ et τ coïncide sur K et sur a, elles coïncident sur $K(a) = L$, d'où $\sigma = \tau$.
Ainsi, $\mathrm{Gal}(L/K)$ s'identifie à un sous-groupe de $(\mathbb{Z}/n\mathbb{Z})^*$, et comme tous les sous-groupes d'un groupe abélien sont abéliens, $\mathrm{Gal}(L/K)$ est abélien. □

Définition 5.7 Soit L un $n-$ième corps cyclotomique sur K, avec $\mathrm{char}(K) \nmid n$.
Soient $a_1, \ldots, a_{\varphi(n)} \in U_n(L)$ les racines primitives $n-$ième de l'unité.
Le polynôme

$$\Phi_n(X) := \prod_{i=1}^{\varphi(n)} (X - a_i)$$

est appelé $n-$ième *polynôme cyclotomique*.

En particulier, il suit de cette définition que $\deg(\Phi_n) = \varphi(n)$.

Proposition 5.8 Soit L un $n-$ième corps cyclotomique sur K, avec $\mathrm{char}(K) \nmid n$. Notons $K_0 = \Pi(K)$.
(i) $\Phi_n \in K_0[X]$.
(ii) Dans $L[X]$, on a $X^n - 1 = \prod_{d|n} \Phi_d$.

Preuve. (i) Soit $a \in U_n(L)$ une racine primitive $n-$ième de l'unité, et $L_0 := K_0(a) \subset L$, de sorte que L_0 est un $n-$ième corps cyclotomique sur K_0. Par la proposition 5.3(iv), L_0/K_0 est galoisienne. Comme les coefficients de Φ_n sont des expressions symétriques en les a_i, ils sont fixés par tout $\sigma \in \mathrm{Gal}(L_0/K_0)$. Ils sont donc dans $L_0^{\mathrm{Gal}(L_0/K_0)} = K_0$.
(ii) Soit d un diviseur de n, et on écrit $n = dk$ avec $k \in \mathbb{Z}$. Soit $a \in U_d(L)$.
Alors $a^n = a^{dk} = (a^d)^k = 1^k = 1$, ce qui signifie que $a \in U_n(L)$, donc $U_d(L) \subset U_n(L)$. En particulier, $U_n(L)$ contient toutes les racines primitives $d-$ième de l'unité : ce sont exactement les éléments d'ordre d de $U_n(L)$. Il vient alors

$$X^n - 1 = \prod_{a \in U_n(L)} (X - a) = \prod_{d|n} \prod_{o(a)=d} (X - a) = \prod_{d|n} \Phi_d$$

ce qui est le résultat voulu. □

Dans le cas particulier $K = \mathbb{Q}$, on peut faire une analyse plus précise des corps cyclotomiques, et identifier complètement le groupe de Galois associé. On a pour cela besoin du lemme suivant.

Lemme 5.10 Soient f, g, $h \in \mathbb{Q}[X] \setminus \{0\}$ tels que $f \in \mathbb{Z}[X]$, $f = gh$, et f, g sont unitaires. Alors g, $h \in \mathbb{Z}[X]$.

Théorème 5.11 Soient $K = \mathbb{Q}$, $\zeta = \exp(\frac{2\pi i}{n}) \in \mathbb{C}$ et $L = \mathbb{Q}(\zeta)$.
(i) $\Phi_n \in \mathbb{Z}[X]$.
(ii) Φ_n est le polynôme minimal de ζ sur $\mathbb{Q}$. En particulier, Φ_n est irréductible dans $\mathbb{Q}[X]$.
(iii) $[L : K] = \varphi(n)$.
(iv) $\mathrm{Gal}(L/K) \simeq (\mathbb{Z}/n\mathbb{Z})^*$.

Preuve. (i) Par la proposition 5.8(ii), on a $X^n - 1 = \prod_{d|n} \Phi_d = g(X)\Phi_n(X)$, où on a posé $g(X) := \prod_{d|n,\ d<n} \Phi_d$.
$X^n - 1$ est à coefficients entiers et unitaires, et g est unitaire comme produit de polynômes unitaires. Le lemme 5.10 nous indique alors que g, $\Phi_n \in \mathbb{Z}[X]$.
(ii) Soit f le polynôme minimal de ζ sur K. Alors f divise $X^n - 1$ dans $\mathbb{Q}[X]$, ce que l'on écrit $X^n - 1 = fh$ avec $h \in \mathbb{Q}[X]$. $X^n - 1$ est unitaire et à coefficients entiers, et f est unitaire. Par le lemme 5.10, il suit que f, $h \in \mathbb{Z}[X]$.
On montre ensuite que si $a \in L$ est une racine de f et que p est un premier tel que $p \nmid n$, alors a^p est aussi une racine de f. Comme $a^n = 1$, on a $(a^n)^p = 1$, ce qui s'écrit aussi $(a^p)^n - 1 = 0$. Donc

$$0 = (a^p)^n - 1 = f(a^p)h(a^p) \Longrightarrow f(a^p) = 0 \quad \text{ou} \quad h(a^p) = 0.$$

Par l'absurde, supposons $f(a^p) \neq 0$. Donc $h(a^p) = 0$, ce qui signifie que a est racine de $h(X^p)$. Or $f(a) = 0$ et f est irréductible dans $\mathbb{Q}[X]$, donc f est le polynôme minimal de a sur $\mathbb{Q}$, donc f divise $h(X^p)$ dans $\mathbb{Q}[X]$.
On obtient l'égalité $(*)$

$$h(X^p) = fg$$

pour un certain $g \in \mathbb{Q}[X]$. De nouveau, comme $h(X^p) \in \mathbb{Z}[X]$ et que h, f sont unitaires, le lemme 5.10 nous assure que $g \in \mathbb{Z}[X]$. On peut alors réduire l'équation $(*)$ modulo p pour obtenir

$$(\overline{\pi}(h))^p = \overline{\pi}(h(X^p)) = \overline{\pi}(f(X)g(X)) = \overline{\pi}(f(X))\overline{\pi}(g(X))$$

où on a noté $\overline{\pi}\colon \mathbb{Z}[X] \longrightarrow \mathbb{F}_p[X]$ la réduction modulo p induite par la surjection canonique $\pi\colon \mathbb{Z} \longrightarrow \mathbb{F}_p$.
Soit alors $k \in \mathbb{F}_p[X]$ un facteur irréductible de $\overline{\pi}(f(X))$. k divise $(\overline{\pi}(h))^p$ dans $\mathbb{F}_p[X]$, donc k divise $\overline{\pi}(h)$ dans $\mathbb{F}_p[X]$.
Mais alors k^2 divise $\overline{\pi}(f)\overline{\pi}(h) = \overline{\pi}(fh) = \overline{\pi}(X^n - 1) = X^n - 1$ dans $\mathbb{F}_p[X]$, donc $X^n - 1 \in \mathbb{F}_p[X]$ possède une racine double, ce qui contredit sa séparabilité.
On peut alors conclure : une racine primitive $n-$ième de l'unité s'écrit ζ^j pour un certain j vérifiant $\mathrm{pgcd}(j, n) = 1$. Elle s'obtient donc par élévations successives de ζ à des puissances p, où p est premier et ne divise pas n. L'assertion que l'on vient de montrer nous dit alors que toutes les racines primitives $n-$ième de l'unité sont des racines de f. Ainsi, $\deg(f) \geq \deg(\Phi_n) = \varphi(n)$, mais d'autre part f divise Φ_n et ces deux polynômes sont unitaires, ce qui implique $f = \Phi_n$.
(iii) On déduit de (ii) et du théorème 2.14 que $[L : K] = \deg(\Phi_n) = \varphi(n)$.
(iv) Le théorème 5.6 fournit un morphisme de groupes injectif $\mathrm{Gal}(L/K) \hookrightarrow (\mathbb{Z}/n\mathbb{Z})^*$.
Comme de plus, $|\mathrm{Gal}(L/K)| = [L : K] = \varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^*|$, cette injection est aussi une surjection, et on a un isomorphisme de groupes $\mathrm{Gal}(L/K) \simeq (\mathbb{Z}/n\mathbb{Z})^*$. □

5.3 Extensions cycliques

Dans cette section, on caractérise, sous une condition sur le corps de base K, les extensions galoisiennes finies dont le groupe de Galois est cyclique. On aura besoin de ce résultat pour la section 5.4.

Définition 5.12 Soit L/K une extension galoisienne finie.
On dit que L/K est *cyclique* (resp. abélienne, résoluble) si $\mathrm{Gal}(L/K)$ est cyclique (resp. abélien, résoluble).

Exemples. (i) Toute extension quadratique de $\mathbb{Q}$ est cyclique, abélienne et résoluble, puisque le groupe de Galois d'une telle extension est isomorphe à $\mathbb{Z}/2\mathbb{Z}$.
(ii) Toute extension finie de $\mathbb{F}_p$, où p est premier, est cyclique (en particulier abélienne et résoluble). C'est le théorème 4.10.
(iii) Soit K un corps de caractéristique différente de 2. Si $f \in K[X]$ est un polynôme unitaire irréductible de degré 4 dont la cubique résolvante scinde complètement sur K, et que L est un corps de décomposition de f sur K, l'extension L/K est abélienne et résoluble, puisque $\mathrm{Gal}(L/K) \simeq V$ par le théorème 4.21, qui est abélien et résoluble. Une telle extension n'est en revanche pas cyclique.
(iv) Si L est un corps de décomposition de $f = X^5 - X - 1$ sur $\mathbb{Q}$, alors $L/\mathbb{Q}$ n'est ni cyclique ni abélienne ni résoluble, puisque $\mathrm{Gal}(L/\mathbb{Q}) = \mathrm{Gal}(f) \simeq S_5$.

La correspondance galoisienne établit un pont entre la théorie des corps et la théorie des groupes. Dès lors, toutes les résultats connus de théorie des groupes se traduisent en des énoncés similaires en théorie de Galois. Voilà un exemple ci-dessous. D'autres figurent en exercices.

Proposition 5.13 Soit L/K une extension finie galoisienne, et M un corps tel que $K \subset M \subset L$.
(i) Si L/K est abélienne, alors L/M et M/K sont abéliennes.
(ii) Si L/K est cyclique, alors L/M et M/K sont cycliques.

Preuve. (i) Comme $\mathrm{Gal}(L/K)$ est abélien, tous ses sous-groupes sont normaux, donc $\mathrm{Gal}(L/M) \lhd \mathrm{Gal}(L/K)$, et M/K est normale par le théorème 4.7(v). Elle est de plus séparable puisque L/K l'est et que toutes les sous-extensions d'une extension séparable sont séparables. Elle est donc galoisienne.
On conclut avec le point (vi) du théorème 4.7, qui nous assure que

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

et en remarquant que le quotient d'un groupe abélien par un sous-groupe est un groupe abélien.
De même, tous les sous-groupes d'un groupe abélien sont abélien, donc L/M est abélienne.
(ii) Il suffit de rappeler que les sous-groupes et quotients d'un groupe cyclique sont cycliques. □

Pour le résultat principal de cette partie, on a besoin d'introduire la notion de caractère d'un groupe.

Définition 5.14 Soit K un corps et G un groupe.
Un *caractère* de G à valeurs dans K est un morphisme de groupes $\sigma\colon G \longrightarrow K^*$.

Lemme 5.15 (Indépendance linéaire des caractères) Soit K un corps, G un groupe, et $\sigma_1, \ldots, \sigma_n$ des caractères de G à valeurs dans K deux-à-deux distincts.
Si $a_1, \ldots, a_n \in K$ vérifient $\sum_{i=1}^{n} a_i\sigma_i(g) = 0$ pour tout $g \in G$, alors $a_i = 0$ pour tout $1 \leq i \leq n$.

Preuve. On procède par récurrence sur $n \geq 1$.
Pour $n = 1$, on a $a_1\sigma_1(g) = 0$ pour tout $g \in G$. En particulier pour $g = e_G$, on a $0 = a_1\sigma_1(e_G) = a_1 \cdot 1_K = a_1$, le résultat souhaité. Supposons alors $n > 1$, et soient $a_1, \ldots, a_n \in K$ tels que $(*)$

$$\sum_{i=1}^{n} a_i\sigma_i(g) = 0,\ \forall g \in G.$$

Comme σ_1 et σ_n sont distincts, il existe $h \in G$ tel que $\sigma_1(h) \neq \sigma_n(h)$. L'hypothèse implique alors l'égalité

$$\sum_{i=1}^{n} a_i\sigma_i(gh) = 0,\ \forall g \in G$$

ce qui s'écrit aussi $(**)$ $\sum_{i=1}^{n} a_i\sigma_i(g)\sigma_i(h) = 0$ pour tout $g \in G$.
En multipliant $(*)$ par $\sigma_n(h)$ et en soustrayant l'équation obtenue à $(**)$, on obtient

$$\sum_{i=1}^{n-1} a_i\sigma_i(g)(\sigma_i(h) - \sigma_n(h)) = 0,\ \forall g \in G.$$

L'hypothèse de récurrence implique alors que $a_i(\sigma_i(h) - \sigma_n(h)) = 0$ pour tout $1 \leq i \leq n-1$. En particulier, pour $i = 1$ on a $a_1(\sigma_1(h) - \sigma_n(h)) = 0$, et comme $\sigma_1(h) - \sigma_n(h) \neq 0$, on doit avoir $a_1 = 0$. L'équation $(*)$ s'écrit alors

$$\sum_{i=2}^{n} a_i\sigma_i(g) = 0,\ \forall g \in G.$$

et en utilisant encore une fois l'hypothèse de récurrence, on conclut aussi que $a_i = 0$ pour tout $2 \leq i \leq n$. □

Voilà alors le résultat principal de cette section.

Théorème 5.16 Soient $n \geq 1$ et K un corps contenant une racine primitive $n-$ième de l'unité, et tel que $\mathrm{char}(K) \nmid n$.
(i) Soient $c \in K^*$ et L un corps de décomposition de $X^n - c$ sur K. Alors L/K est cyclique, de degré un diviseur de n.
(ii) Soit L/K une extension cyclique de degré n. Alors il existe $a \in L$ tel que $L = K(a)$ et $a^n \in K$.
En particulier, L est un corps de décomposition de $X^n - a^n$.

Preuve. (i) Déjà, par définition de L, L/K est normale. En notant $f = X^n - c$, on a $f' = nX^{n-1} \neq 0$ puisque $\mathrm{char}(K) \nmid n$. Le lemme 3.19(i) nous dit alors que f est séparable, ce qui implique que L/K est séparable. Elle est ainsi galoisienne.
Soient ensuite $z \in K$ une racine primitive $n-$ième de l'unité et $a \in L$ une racine de f. Alors

$$f(za) = (za)^n - c = z^n a^n - c = a^n - c = 0$$

donc za est aussi une racine de f. Il suit que a, za, $z^2a, \ldots, z^{n-1}a$ sont toutes les racines de f dans L, et donc $L = K(a)$.
Tout élément $\sigma \in \mathrm{Gal}(L/K) = \mathrm{Gal}(f)$ est alors déterminé par $\sigma(a)$, qui doit être une racine de f. Ainsi, pour tout $\sigma \in \mathrm{Gal}(L/K)$, $\sigma(a) = z^j a$ pour un certain $j \in \{0, \ldots, n-1\}$. On définit alors l'application

$$\alpha\colon \mathrm{Gal}(L/K) \longrightarrow \mathbb{Z}/n\mathbb{Z}$$

$$\sigma \longmapsto [j]$$

où j est l'élément de $\{0, \dots, n-1\}$ tel que $\sigma(a) = z^j a$.
Soient σ, $\tau \in \mathrm{Gal}(L/K)$, que l'on écrit $\sigma(a) = z^j a$ et $\tau(a) = z^k a$. Alors $(\sigma\tau)(a) = \sigma(z^k a) = z^k \sigma(a) = z^{j+k} a$, et il suit que

$$\alpha(\sigma\tau) = [j+k] = [j] + [k] = \alpha(\sigma) + \alpha(\tau)$$

ce qui montre que α est un morphisme de groupes.
Il est de plus injectif, puisque si $\alpha(\sigma) = \alpha(\tau)$, alors $[j] = [k]$, donc il existe $m \in \mathbb{Z}$ tel que $j - k = mn$. On a ainsi

$$z^{j-k} a = z^{mn} a = (z^n)^m a = a \Longrightarrow z^j a = z^k a \Longrightarrow \sigma(a) = \tau(a).$$

Comme σ et τ coïncident sur K et sur a, elles coïncident sur $K(a) = L$. Donc $\sigma = \tau$, et α est injective. Cela montre que $\mathrm{Gal}(L/K)$ est isomorphe à un sous-groupe de $\mathbb{Z}/n\mathbb{Z}$, et est donc cyclique. Son ordre, qui correspond au degré de L/K, est alors un diviseur de n par le théorème de Lagrange.
(ii) Soit $\sigma \in \mathrm{Gal}(L/K)$ tel que $\langle \sigma \rangle = \mathrm{Gal}(L/K)$, et soit $z \in K$ une racine primitive $n-$ième de l'unité.
Les applications id_L, $\sigma, \dots, \sigma^{n-1}$ sont des caractères de L^* à valeurs dans L. Comme $z^i \neq 0$ pour tout $0 \leq i \leq n-1$, le lemme 5.15 nous assure que $\displaystyle\sum_{i=0}^{n-1} z^i \sigma^i \neq 0$. Il existe donc $x \in L^*$ tel que $\displaystyle\sum_{i=0}^{n-1} z^i \sigma^i(x) \neq 0$, et on pose $a := \displaystyle\sum_{i=0}^{n-1} z^i \sigma^i(x)$.
On a alors

$$\sigma(a) = \sigma\left(\sum_{i=0}^{n-1} z^i \sigma^i(x) \right) = \sum_{i=0}^{n-1} z^i \sigma^{i+1}(x) = \frac{1}{z} \sum_{i=0}^{n-1} z^{i+1} \sigma^{i+1}(x) = \frac{1}{z} a$$

d'où on tire que $\sigma(a^n) = (\sigma(a))^n = \left(\frac{1}{z} a\right)^n = \frac{1}{z^n} a^n = a^n$ puisque $z^n = 1$. Comme a^n est fixé par σ, a^n est fixé par tout élément $\tau \in \mathrm{Gal}(L/K)$, et est donc dans $L^{\mathrm{Gal}(L/K)} = K$ par le théorème 4.4.
Il reste à établir que $L = K(a)$. Pour tout $0 \leq i \leq n-1$, on a $\sigma^i(a) = z^{-i} a$. Comme les $z^{-i} a$ sont deux-à-deux distincts, on en déduit que $|\mathrm{Hom}(K(a)/K, L/K)| \geq n$. Comme L/K est galoisienne, elle est séparable, donc $a \in L$ est séparable, et le théorème 3.29 fournit l'égalité $|\mathrm{Hom}(K(a)/K, L/K)| = [K(a) : K]$. Ainsi, $[K(a) : K] \geq n = [L : K]$. D'autre part, comme $K(a) \subset L$, on doit avoir $[K(a) : K] \leq [L : K]$. En conclusion, $[K(a) : K] = [L : K]$ et $L = K(a)$.
En particulier, L contient bien a, za, $z^2 a, \dots, z^{n-1} a$ les racines de $X^n - a^n$. C'est donc un corps de décomposition de $X^n - a^n$. □

Exemple. Soit p un nombre premier, et $\zeta_p = \exp(\frac{2\pi i}{p}) \in \mathbb{C}$ une racine primitive $p-$ième de l'unité. Soit $c \neq 0 \in \mathbb{Q}(\zeta_p)$, et L un corps de décomposition de $X^p - c$ sur $\mathbb{Q}(\zeta_p)$. Alors $L/\mathbb{Q}(\zeta_p)$ est cyclique de degré p, et $\mathrm{Gal}(L/\mathbb{Q}(\zeta_p)) \simeq \mathbb{Z}/p\mathbb{Z}$.

Terminons cette discussion par trois remarques.

Remarques. (i) Le théorème 5.16(ii) dans le cas particulier $K = \mathbb{Q}$ et $n = 2$ est une reformulation de la proposition 2.15, qui détaillait la structure des extensions quadratiques de $\mathbb{Q}$.
(ii) Ensuite, il est possible de généraliser ces résultats aux extensions abéliennes : c'est la théorie de Kummer. En fait, comme un groupe abélien fini est un produit direct de groupes cycliques, il faut alors adjoindre différentes racines $n-$ièmes. Dans une autre direction, la théorie d'Artin-Schreier étudie les extensions cycliques dans le cas où $\mathrm{char}(K) \mid n$.
(iii) L'étude est beaucoup plus difficile sans l'hypothèse que K contient une racine primitive $n-$ième de l'unité. Le cas $c = 1$ a tout de même été abordé en section 5.2, avec les corps cyclotomiques.

5.4 Résolubilité par radicaux

Dans cette partie, on établit qu'en caractéristique nulle, une équation polynomiale est résoluble par radicaux si et seulement si le groupe de Galois du polynôme correspondant est résoluble.

Commençons par expliciter la terminologie "résoluble par radicaux".

Définition 5.17 Soient L/K une extension algébrique, et $f \in K[X] \setminus K$.
(i) L/K est appelée *extension par radicaux* s'il existe $a_1, \dots, a_n \in L$ et $r_1, \dots, r_n \geq 1$ tels que $L = K(a_1, \dots, a_n)$, $a_1^{r_1} \in K$ et $a_i^{r_i} \in K(a_1, \dots, a_{i-1})$ pour tout $2 \leq i \leq n$.
(ii) Un élément $a \in L$ est appelé *radical* sur K s'il existe une extension par radicaux M/K telle que $M \subset L$ et $a \in M$.
(iii) L'équation $f = 0$ est dite *résoluble par radicaux* s'il existe un radical $a \in L$ sur K tel que $f(a) = 0$.

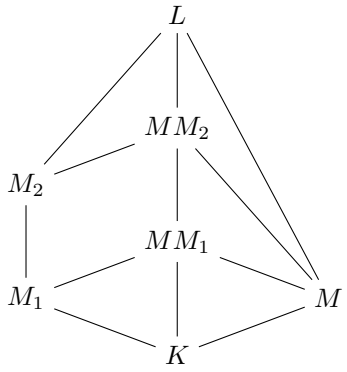
Exemples. (i) $\mathbb{Q}(\sqrt[n]{p})/\mathbb{Q}$, où p est un nombre premier et $n \geq 1$, est une extension par radicaux.
(ii) Soit L un corps cyclotomique sur K. Alors L/K est une extension par radicaux, par la proposition 5.3.
(iii) Si $\mathrm{char}(K) \nmid n$ et si K contient une racine primitive $n-$ième de l'unité, alors toute extension cyclique de K est une extension par radicaux, par le point (ii) du théorème 5.16.

Remarque. De la définition, et par multiplicativité des degrés, il suit qu'une extension par radicaux est toujours finie, en particulier algébrique. En particulier, $\mathbb{Q}(\pi)/\mathbb{Q}$, $\mathbb{Q}(e)/\mathbb{Q}$ ne sont pas des extensions par radicaux.

Dans la suite, si L_1/K et L_2/K sont deux sous-extensions de L/K, on notera $L_1L_2 \coloneqq K(L_1 \cup L_2)$ le *compositum* de L_1 et L_2. Clairement, on a $L_1L_2 = L_1(L_2) = L_2(L_1)$. En d'autres mots, L_1L_2 est le plus petit sous-corps de L qui contient L_1 et L_2.

Lemme 5.18 Soient L/K une extension finie et M, M_1, M_2 des sous-extensions de L/K telles que $M_1 \subset M_2$.
Si M_2/M_1 est galoisienne, alors MM_2/MM_1 est galoisienne, et il existe un morphisme de groupes injectif $\mathrm{Gal}(MM_2/MM_1) \hookrightarrow \mathrm{Gal}(M_2/M_1)$.

Preuve. La situation se schématise comme



Déjà, comme M_2/M_1 est normale, il existe $f \in M_1[X] \setminus M_1$ tel que M_2 est un corps de décomposition de f sur M_1, par le théorème 3.14. Notons $a_1, \ldots, a_n \in M_2$ les racines de f dans M_2, de sorte que $M_2 = M_1(a_1, \ldots, a_n)$. Il suit que

$$MM_2 = MM_1(a_1, \ldots, a_n)$$

donc MM_2 est un corps de décomposition de $f \in MM_1[X]$ sur MM_1, et MM_2/MM_1 est normale, toujours par le théorème 3.14. Ensuite, M_2/M_1 est séparable, donc a_i est séparable sur M_1 (corollaire 3.31), pour tout $1 \leq i \leq n$. Comme le polynôme minimal de a_i sur MM_1 divise le polynôme minimal de a_i sur M_1, et que celui-ci est séparable, a_i est aussi séparable sur MM_1, donc $MM_2 = MM_1(a_1, \ldots, a_n)$ est séparable, par le corollaire 3.31(ii).
L'application

$$\begin{aligned} \alpha \colon \mathrm{Gal}(MM_2/MM_1) &\longrightarrow \mathrm{Gal}(M_2/M_1) \\ \sigma &\longmapsto \sigma_{|M_2} \end{aligned}$$

est bien définie : si $\sigma \in \mathrm{Gal}(MM_2/MM_1)$, alors σ fixe MM_1, en particulier M_1, et $\sigma(M_2) = M_2$ puisque σ permute les racines de f et que M_2 est le corps des racines de f. Donc $\sigma_{|M_2} \in \mathrm{Gal}(M_2/M_1)$.
Soient ensuite σ, $\tau \in \mathrm{Gal}(MM_2/MM_1)$, et $a \in M_2$. Alors

$$\alpha(\sigma\tau)(a) = (\sigma\tau)_{|M_2}(a) = (\sigma\tau)(a) = \sigma(\tau(a))$$

Or, comme $\sigma(M_2) = \tau(M_2) = M_2$, on a $\tau(a) \in M_2$ et donc $\sigma(\tau(a)) \in M_2$. On peut alors écrire que

$$\alpha(\sigma\tau)(a) = \sigma(\tau(a)) = \sigma_{|M_2}(\tau_{|M_2}(a)) = (\sigma_{|M_2} \circ \tau_{|M_2})(a) = (\alpha(\sigma) \circ \alpha(\tau))(a)$$

et on déduit $\alpha(\sigma\tau) = \alpha(\sigma) \circ \alpha(\tau)$, ce qui montre que α est un morphisme de groupes.
Enfin, α est injectif puisque si $\sigma \in \mathrm{Gal}(MM_2/MM_1)$ est tel que $\sigma_{|M_2} = \mathrm{id}_{M_2}$, alors σ fixe M et M_2, donc aussi MM_2, donc $\sigma = \mathrm{id}_{MM_2}$. Cela conclut la preuve. □

Théorème 5.19 Soient L/K une extension finie et M la clôture normale de L/K.
S'il existe une tour d'extensions

$$K = L_0 \subset L_1 \subset \ldots \subset L_{m-1} \subset L_m = L$$

telle que L_i/L_{i-1} est cyclique pour tout $1 \leq i \leq m$, alors M/K est galoisienne et $\mathrm{Gal}(M/K)$ est résoluble.

Preuve. Puisque L_i/L_{i-1} est cyclique, elle est en particulier séparable, donc L/K est séparable par le corollaire 3.31(i). Elle est de plus finie par hypothèse. On peut donc appliquer le théorème de l'élément primitif, qui assure l'existence d'un $a \in L$ tel que $L = K(a)$. Soit $f \in K[X]$ le polynôme minimal de a sur K. Par définition de M, f est scindé dans $M[X]$. Soit $L \subset M' \subset M$ le corps des racines de f, que l'on écrit $M' = K(a_1, a_2, \dots, a_n)$ avec $a_1 = a$, $a_2, \dots, a_n \in M$ les racines de f. Par le théorème 3.14, M'/K est normale, donc par minimalité de M on a en fait $M' = M = K(a_1, \dots, a_n)$. Comme a est séparable sur K (puisque $a \in L$), les autres racines de f sont aussi séparables sur K, donc M/K est séparable par le corollaire 3.31(ii). Cela établit que M/K est galoisienne.
Montrons maintenant que $\mathrm{Gal}(M/K)$ est résoluble. Pour montrer l'existence dans $\mathrm{Gal}(M/K)$ d'une suite de sous-groupes satisfaisant la définition de résolubilité, on utilise la correspondance galoisienne, et on va montrer l'existence d'une tour d'extensions entre K et M vérifiant les bonnes propriétés. Notre hypothèse nous donne déjà des sous-extensions entre K et L. On va donc construire des corps intermédiaires entre L et M en adjoignant à L les racines de f.
Posons, pour tout $1 \leq i \leq n$, $M^{(i)} = L(a_1, \dots, a_i)$. En particulier, $M^{(1)} = L$ et $M^{(n)} = M$.
Montrons par récurrence sur i que $M^{(i)}$ vérifie la condition du théorème, c'est-à-dire qu'il existe des sous-extensions

$$K = M_0^{(i)} \subset M_1^{(i)} \subset ... \subset M_t^{(i)} = M^{(i)}$$

avec $M_j^{(i)}/M_{j-1}^{(i)}$ cyclique pour tout $1 \leq j \leq t$.
Pour $i = 1$, c'est l'hypothèse du théorème. Soit alors $i \geq 1$, et supposons la propriété vraie pour $M^{(i)}$.
Comme f est irréductible, $\mathrm{Gal}(M/K)$ agit transitivement sur $\{a_1, a_2, \dots, a_n\}$, donc il existe $\sigma \in \mathrm{Gal}(M/K)$ tel que $\sigma(a_1) = a_{i+1}$. On a alors la tour d'extensions

$$M^{(i)} = M^{(i)}\sigma(L_0) \subset M^{(i)}\sigma(L_1) \subset ... \subset M^{(i)}\sigma(L_m) = M^{(i)}\sigma(L)$$

où $M^{(i)}\sigma(L) = M^{(i)}\sigma(K(a)) = M^{(i)}\sigma(a) = M^{(i)}(a_{i+1}) = M^{(i+1)}$.
Maintenant $\sigma(L_j)/\sigma(L_{j-1})$ est cyclique pour tout $1 \leq j \leq m$, *i.e.* $\mathrm{Gal}(\sigma(L_j)/\sigma(L_{j-1}))$ est cyclique. Par le lemme 5.18, $\mathrm{Gal}(M^{(i)}\sigma(L_j)/M^{(i)}\sigma(L_{j-1}))$ s'injecte dans $\mathrm{Gal}(\sigma(L_j)/\sigma(L_{j-1}))$, donc est également cyclique. On a donc construit une tour d'extensions cycliques entre $M^{(i)}$ et $M^{(i+1)}$. Par hypothèse de récurrence il existe également une tour d'extensions cycliques entre K et $M^{(i)}$. Tout cela mis ensemble montre l'existence d'une tour d'extensions cycliques entre K et $M^{(i+1)}$, ce qui prouve le pas de récurrence. En particulier, pour $i = n$, on a une tour d'extensions cycliques, donc aussi abéliennes, entre K et M. Comme expliqué ci-dessus, cela montre que $\mathrm{Gal}(M/K)$ est résoluble. □

Avec le théorème de correspondance galoisienne, le prochain résultat est le plus important de ce cours.

Théorème 5.20 (Galois) Soit K un corps de caractéristique nulle. Soit $f \in K[X] \setminus K$ irréductible.
L'équation $f = 0$ est résoluble par radicaux si, et seulement si, $\mathrm{Gal}(f)$ est résoluble.

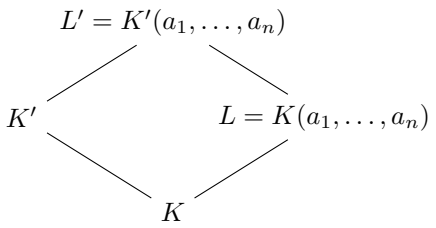
Preuve. $\Longrightarrow$: Supposons pour commencer que $f = 0$ est résoluble par radicaux. Il existe donc une extension par radicaux L de K contenant une racine a de f. On peut alors écrire $L = K(a_1, \dots, a_l)$ avec $a_1^{r_1} \in K$ et $a_i^{r_i} \in L_{i-1}$, où $L_{i-1} = K(a_1, \dots, a_{i-1})$, pour tout $2 \leq i \leq l$.
Posons $r = r_1...r_l$ et soit L' un corps de décomposition de $X^r - 1$ sur L. Soient $\zeta_1, \dots, \zeta_r \in L'$ les racines de $X^r - 1$, et notons $K' = K(\zeta_1, \dots, \zeta_r) \subset L'$. Alors K' est un corps de décomposition de $X^r - 1$ sur K, *i.e.* K' est un $r-$ième corps cyclotomique. Le théorème 5.6 assure alors que K'/K est abélienne, en particulier résoluble. Par le point (iii) de l'exercice 8 ci-dessous, il existe donc une tour d'extensions

$$K = K'_0 \subset K'_1 \subset ... \subset K'_m = K'$$

avec K'_i/K'_{i-1} cyclique pour tout $1 \leq i \leq m$. Posons alors $L'_0 = K'$ et $L'_i = K'(a_1, \dots, a_i) = L'_{i-1}(a_i)$, pour tout $1 \leq i \leq l$.
Comme $a_i^{r_i} \in L_{i-1} \subset L'_{i-1}$ et que $X^{r_i} - 1$ est scindé dans $L'_{i-1}[X]$, L'_i est un corps de décomposition de $X^{r_i} - a_i^{r_i}$ sur L'_{i-1}, donc L'_i/L'_{i-1} est cyclique par le théorème 5.16(i). On a donc trouvé une tour d'extensions cycliques entre K et L'. Comme de plus L'/K est finie, on peut appliquer le théorème 5.19, qui nous assure que M/K est galoisienne, de groupe de Galois $\mathrm{Gal}(M/K)$ résoluble, et où M dénote la clôture normale de L'/K. Enfin, si on note $N \subset M$ un corps de décomposition de f sur K (N est forcément contenu dans M puisque f a une racine, a, dans $L \subset M$, et que M/K est normale, donc f scinde dans $M[X]$), on a que N/K est séparable comme sous-extension d'une extension séparable, et normale par le théorème 3.14. N/K est donc galoisienne, et le théorème 4.7(vi) fournit

$$\mathrm{Gal}(f) = \mathrm{Gal}(N/K) \simeq \mathrm{Gal}(M/K)/\mathrm{Gal}(M/N)$$

Comme $\mathrm{Gal}(M/K)$ est résoluble et que la résolubilité est stable par passage au quotient, $\mathrm{Gal}(f)$ est résoluble.
$\Longleftarrow$: Notons $n = \deg(f)$ et $r = n!$. Soit K' un corps de décomposition de $X^r - 1$ sur K, et L' un corps de décomposition de f sur K'. Notons également $a_1, \dots, a_n \in L'$ les racines de f, et $L = K(a_1, \dots, a_n) \subset L'$.



Comme $\mathrm{Gal}(f)$ est résoluble, il existe (exercice $8(iii)$) une tour d'extensions

$$K = L_0 \subset L_1 \subset ... \subset L_m = L$$

avec L_i/L_{i-1} cyclique pour tout $1 \leq i \leq m$. Le lemme 5.18 fournit alors une tour d'extensions

$$K' = K'L_0 \subset K'L_1 \subset ... \subset K'L_m = K'L = L'$$

avec $K'L_i/K'L_{i-1}$ cyclique pour tout $1 \leq i \leq m$. Soit $i \in \{1, \ldots, m\}$ fixé. En notant $r_i := [K'L_i : K'L_{i-1}]$, on a

$$r_i \mid [L_i : L_{i-1}] \mid [L : K] = |\mathrm{Gal}(f)| \mid n! = r.$$

On en tire que $X^{r_i} - 1 \mid X^r - 1$. Comme $X^r - 1$ est scindé dans $K'[X]$, $X^{r_i} - 1$ est scindé dans $K'L_{i-1}[X]$. En particulier, $K'L_{i-1}$ contient une racine primitive r_i-ième de l'unité, donc par le théorème $5.16(ii)$ il existe $b_i \in K'L_i$ tel que $K'L_i = K'L_{i-1}(b_i)$ avec $b_i^{r_i} \in K'L_{i-1}$. Cela signifie que L'/K' est une extension par radicaux. Comme K' est un $r-$ième corps cyclotomique sur K, K'/K est aussi une extension par radicaux, par l'exemple ci-dessus. On déduit de l'exercice 10 ci-dessous que L'/K est une extension par radicaux.
Ainsi, comme $L \subset L'$, toute racine de f est un radical sur K, donc $f = 0$ est résoluble par radicaux. □

Corollaire 5.21 Sur un corps de caractéristique nulle, toute équation polynomiale de degré 1, 2, 3 ou 4 est résoluble par radicaux.

Preuve. Pour $n \in \{1, 2, 3, 4\}$, le groupe de Galois d'un polynôme de degré n est isomorphe à un sous-groupe de S_n, qui est résoluble. □

En revanche, en degré au moins 5, on peut avoir des équations non résolubles. Déjà, comme S_n n'est pas résoluble pour $n \geq 5$, il suffit de déterminer un polynôme de degré dont le groupe de Galois est S_n. Par exemple, on peut montrer que $\mathrm{Gal}(X^n - X - 1) \simeq S_n$. C'est un résultat difficile, dont la preuve va au-delà de ces notes. Cela traite néanmoins une partie du problème $4.22(ii)$.

Exemples. (i) On a établi ci-dessus que le groupe de Galois de $X^5 - 4X - 1$ est isomorphe à S_5, qui n'est pas résoluble. L'équation $X^5 - 4X - 1 = 0$ n'est donc pas résoluble par radicaux.
(ii) Soit $f = X^5 - X^3 - 2X^2 + 2$. On remarque que $f = (X^3 - 2)(X - 1)(X + 1)$, donc $\mathrm{Gal}(f) = \mathrm{Gal}(X^3 - 2) \simeq S_3$, qui est résoluble, donc $f = 0$ est résoluble par radicaux.
(iii) Le théorème 4.14 permet de montrer que $\mathrm{Gal}(2X^5 - 5X^4 + 5) \simeq S_5$. L'équation $2X^5 - 5X^4 + 5 = 0$ n'est donc pas résoluble par radicaux.

5.5 Le théorème fondamental de l'algèbre

La théorie de Galois permet de donner une autre preuve du théorème fondamental de l'algèbre. Pour cela, on a besoin des faits suivants, considérés comme connus.

(i) Tout polynôme de $\mathbb{R}[X]$ de degré impair a une racine dans $\mathbb{R}$. En particulier, un polynôme de degré impair ≥ 3 n'est pas irréductible.
(ii) Tout nombre complexe non-nul a une racine carrée dans $\mathbb{C}$. Autrement dit, pour tout $z \in \mathbb{C}^*$, il existe $w \in \mathbb{C}^*$ tel que $w^2 = z$.
(iii) **(1er théorème de Sylow)** Si G est un groupe fini tel que $|G| = p^n m$ avec p un nombre premier ne divisant pas m, alors il existe un $p-$Sylow dans G d'ordre p^n.
(iv) Si G est un $p-$groupe fini non-trivial, alors G a un sous-groupe d'indice p.

Théorème 5.22 Le corps $\mathbb{C}$ est algébriquement clos.

Preuve. Par la proposition 3.8, il suffit de montrer que tout irréductible de $\mathbb{C}[X]$ est de degré 1. Il suffit pour cela de montrer que la seule extension finie de $\mathbb{C}$ est $\mathbb{C}$ lui-même. Soit donc $E/\mathbb{C}$ une extension finie.
L'extension $E/\mathbb{R}$ est finie. Comme on est en caractéristique nulle, $E/\mathbb{R}$ est aussi séparable. On peut alors utiliser le point (i) de l'exercice 2 du chapitre 4, et plonger E dans une extension galoisienne K de $\mathbb{R}$. On a alors la tour d'extensions $\mathbb{R} \subset \mathbb{C} \subset K$, et par multiplicativité des degrés, $[K : \mathbb{R}]$ est pair. Notons alors $G = \mathrm{Gal}(K/\mathbb{R})$, et écrivons $|G| = 2^m k$, où k est impair. Par le point (iii) ci-dessus, il existe H un sous-groupe de G d'ordre 2^m. Introduisons aussi $F := \mathbb{R}^H$ le sous-corps de points fixes correspondant à H. En particulier, $[F : \mathbb{R}]$ est égal à l'indice de H dans G, donc $[F : \mathbb{R}] = k$ est impair. Soit ensuite $\alpha \in F$. On a

$$\mathbb{R} \subset \mathbb{R}(\alpha) \subset F \Longrightarrow k = [F : \mathbb{R}] = [F : \mathbb{R}(\alpha)][\mathbb{R}(\alpha) : \mathbb{R}]$$

et comme k est impair, $[\mathbb{R}(\alpha) : \mathbb{R}]$ est aussi impair. Ainsi, le polynôme minimal de α sur $\mathbb{R}$ est irréductible dans $\mathbb{R}[X]$ et degré impair, donc est forcément de degré 1 par le point (i) ci-dessus. Donc $[\mathbb{R}(\alpha) : \mathbb{R}] = 1$ et $\alpha \in \mathbb{R}$, d'où $F = \mathbb{R}$.
Ainsi, $k = 1$, donc $|G| = 2^m = |H|$ et $G = H$ est un $2-$groupe.
$\mathrm{Gal}(K/\mathbb{C})$ a ordre

$$|\mathrm{Gal}(K/\mathbb{C})| = [K : \mathbb{C}] = \frac{[K : \mathbb{R}]}{[\mathbb{C} : \mathbb{R}]} = \frac{2^m}{2} = 2^{m-1}.$$

Si $m \geq 2$, alors $\mathrm{Gal}(K/\mathbb{C})$ est un $2-$groupe non-trivial, donc a un sous-groupe d'indice 2 par le point (iv) ci-dessus. Le sous-corps de points fixes correspondant est alors une extension quadratique de $\mathbb{C}$, donc prend la forme $\mathbb{C}(\sqrt{d})$ pour un certain $d \in \mathbb{C}^*$. Or tout nombre complexe non-nul a une racine carrée, donc $[\mathbb{C}(\sqrt{d}) : \mathbb{C}] = 1 \neq 2$.
On conclut donc que $m = 1$, ce qui implique $[K : \mathbb{C}] = 1$ et donc $K = \mathbb{C}$. Comme $\mathbb{C} \subset E \subset K$, on a aussi $E = \mathbb{C}$, ce qui conclut la preuve. □

5.6 Constructions à la règle et au compas

Dans cette partie, on utilise nos résultats précédents pour répondre aux trois grands problèmes de géométrie de l'Antiquité. Ceux-ci s'énoncent de la façon suivante.
(i) Est-il possible de dupliquer un cube, *i.e.* de construire à la règle et au compas un cube de volume le double de celui d'un cube donné ?
(ii) La quadrature du cercle est-elle possible, *i.e.* est-il possible, à la règle et au compas, de construire un carré de même aire que celle d'un cercle donné ?
(iii) En général, est-il possible de trisecter un angle ?

Soit E un ensemble fini de points du plan. On note $\mathcal{D}_E$ l'ensemble des droites passant par deux points distincts de E, et $\mathcal{C}_E$ l'ensemble des cercles centré en un point de E et de rayon une distance entre deux points distincts de E.

Définition 5.23 Un point P du plan est dit
(i) *constructible en une étape à partir de* E s'il est intersection de deux éléments distincts de $\mathcal{D}_E \cup \mathcal{C}_E$.
(ii) *constructible en* n *étapes à partir de* E s'il existe une suite finie $P_1, \ldots, P_n = P$ de points du plan telle que, pour tout $i = 1, \ldots, n$, P_i est constructible en une étape à partir de $E \cup \{P_1, \ldots, P_{i-1}\}$.

Avant de caractériser plus précisément les points constructibles, deux remarques sont à faire.

Remarques. (i) Par définition, tous les points de E sont constructibles en une étape.
(ii) Un point constructible en n étapes à partir de E sera simplement appelé "point constructible" . De plus, notons que si $|E| = 1$, l'ensemble des points constructibles à partir de E est réduit à E. On peut donc supposer que $|E| \geq 2$. En fait, dans la suite on prendra $|E| = 2$.

Prenons donc $|E| = 2$ et identifions le plan à $\mathbb{R}^2$ en le munissant d'un repère orthonormé, construit à partir des deux points de E, supposés à distance 1. En d'autres termes, E consiste des points $(0, 0)$ et $(1, 0)$.

Définition 5.24 Un nombre réel $a \in \mathbb{R}$ est *constructible* si le point $(a, 0)$ du plan est constructible.

Remarque. Notons que $a \in \mathbb{R}$ est constructible si et seulement si $(0, a)$ est constructible. Ainsi a est constructible si et seulement si a est la coordonnée d'un point constructible.

Proposition 5.25 Tout nombre rationnel est constructible.

Preuve. Comme $(1, 0)$ est constructible par définition, tout point de la forme $(n, 0)$ avec $n \in \mathbb{Z}$ est constructible. Soit donc $\frac{p}{q}$ un nombre rationnel. Les points $(p, 0)$ et $(0, q)$ sont constructibles. On trace alors la droite ℓ passant par ces deux points, et ensuite la parallèle à ℓ passant par $(0, 1)$. Cette droite intersecte la droite passant par $(0, 0)$ et $(1, 0)$ au point $(\frac{p}{q}, 0)$. Donc $\frac{p}{q}$ est constructible. □

En fait, l'ensemble des points constructibles à partir de E a naturellement une structure de corps.

Proposition 5.26 L'ensemble des nombres constructibles est un sous-corps de $\mathbb{R}$.

Preuve. Il s'agit de montrer que si a, $b \in \mathbb{R}$ sont constructibles, alors $-a$, $a + b$, ab et a^{-1} sont constructibles.
Par exemple, si $(a, 0)$ est constructible, le cercle centré en $(0, 0)$ et de rayon la distance entre $(0, 0)$ et $(a, 0)$ intersecte l'axe horizontal en $(a, 0)$ et en $(-a, 0)$. Cela prouve que $-a$ est constructible si a l'est. De même, si $(a, 0)$ et $(b, 0)$ sont deux constructibles, le cercle centré en $(a, 0)$ et de rayon la distance entre $(0, 0)$ et $(b, 0)$ intersecte l'axe horizontal en les points $(a - b, 0)$ et $(a + b, 0)$, donc $a \pm b$ sont tous deux constructibles. Les constructions sont similaires pour a^{-1} (où $a \neq 0$) et ab. □

En particulier, par la proposition 5.25, ce sous-corps de $\mathbb{R}$ contient $\mathbb{Q}$. Le lemme suivant sera également utile.

Lemme 5.27 Si $a \geq 0$ est constructible, alors $\sqrt{a}$ est constructible.

Preuve. Comme $(1, 0)$, $(a, 0)$ sont constructibles, il suit des résultats précédents que $(\frac{a+1}{2}, 0)$ est constructible. Traçons maintenant le cercle $\mathcal{C}$ centré en ce point et de rayon la distance entre ce point et $(0, 0)$. Traçons également la parallèle à l'axe vertical passant par $(1, 0)$. Cette droite intersecte $\mathcal{C}$ en les points $(1, \sqrt{a})$ et $(1, -\sqrt{a})$. Cela conclut la preuve. □

On a maintenant tous les outils nécessaires pour prouver le résultat suivant, crucial.

Lemme 5.28 Soit $S \subset \mathbb{R}$ un ensemble de nombres constructibles. Soit $K = \mathbb{Q}(S)$.
(i) Soit $(a, b) \in \mathbb{R}^2$ un point constructible en une étape à partir de S. Alors soit a, $b \in K$, soit a et b sont dans une certaine extension quadratique de K.
(ii) Tout élément de K est constructible. De plus, si $K \subset F$ est une extension quadratique de K, tout point de F est constructible.

Preuve. (i) Il y a plusieurs cas à traiter ici. Supposons pour commencer que (a, b) est le point d'intersection de deux droites ℓ et ℓ' passant par des points dont les coordonnées sont dans S. Le couple (a, b) est donc la solution d'un système de la forme

$$\begin{cases} \ell : \alpha x + \beta y + \gamma = 0 \\ \ell' : \alpha' x + \beta' y + \gamma' = 0 \end{cases}$$

où α, β, γ, α', β' et γ' sont dans K. Aussi, puisque $\ell \neq \ell'$, $\alpha\beta' - \alpha'\beta \neq 0$ et le système a en effet une solution. On voit alors que cette solution s'écrit

$$\begin{pmatrix} a \\ b \end{pmatrix} = \frac{1}{\alpha\beta' - \alpha'\beta} \begin{pmatrix} \beta' & -\beta \\ -\alpha' & \alpha \end{pmatrix} \begin{pmatrix} -\gamma \\ -\gamma' \end{pmatrix}$$

et en particulier a, $b \in K$.
Maintenant si (a, b) est le point d'intersection d'une droite ℓ et d'un cercle $\mathcal{C}$, (a, b) est solution d'un système de la forme

$$\begin{cases} \ell : \alpha x + \beta y + \gamma = 0 \\ \mathcal{C} : (x - s_1)^2 + (y - s_2)^2 = r^2 \end{cases}$$

avec α, β, γ, s_1, s_2, $r \in K$. Sans restriction, disons que $\beta \neq 0$. Alors $y = \frac{1}{\beta}(-\gamma - \alpha x)$, et ré-injecter cela dans la deuxième équation fournit $(x - s_1)^2 + (\frac{1}{\beta}(-\gamma - \alpha x) - s_2)^2 = r^2$, et donc soit $a \in K$ soit a est dans une extension quadratique de K.

Enfin, si (a,b) est le point d'intersection de deux cercles, (a,b) est solution d'un système de la forme

$$\begin{cases} \mathcal{C}_1 : x^2+y^2+\delta x+\varepsilon y+\varphi=0 \\ \mathcal{C}_2 : x^2+y^2+\delta' x+\varepsilon' y+\varphi'=0 \end{cases}$$

avec δ, ε, φ, δ', ε', $\varphi' \in K$. Ce système équivaut à

$$\begin{cases} \mathcal{C}_1 : x^2+y^2+\delta x+\varepsilon y+\varphi=0 \\ \mathcal{C}_2 : (\delta'-\delta)x+(\varepsilon'-\varepsilon)y+(\varphi'-\varphi)=0 \end{cases}$$

et on est ainsi ramené au cas précédent.
(ii) Comme tous les éléments de S sont constructibles, et que tous les rationnels sont constructibles, tous les éléments de $K=\mathbb{Q}(S)$ sont constructibles. Soit ensuite $K \subset F$ de degré 2, et $a \in L \setminus K$, de sorte que son polynôme minimal $f=X^2+\beta X+\gamma \in K[X]$ soit de degré 2. Alors $a=\frac{-\beta\pm\sqrt{\beta^2-4\gamma}}{2}$, et comme l'ensemble des nombres constructibles est stable pour la somme, le produit et l'extraction de racines carrées (par la proposition 5.26 et le lemme 5.27), il suit que a est constructible. Cela conclut la preuve. □

On peut alors énoncer le résultat central de cette section, dont la preuve ne présente plus de difficultés.

Théorème 5.29 (Wantzel) Un nombre réel $c \in \mathbb{R}$ est constructible si et seulement s'il existe une tour d'extensions

$$\mathbb{Q}=K_0 \subset K_1 \subset \cdots \subset K_r$$

avec $c \in K_r$ et $[K_i : K_{i-1}]=2$ pour tout $i=1,\dots,r$.

Preuve. $\Longrightarrow$: Supposons pour commencer que c est constructible, *i.e.* $P=(c,0)$ est constructible. Par définition, il existe une suite de points $P_0,\dots,P_m=P$ tels que $P_0 \in \mathbb{Q}^2$ et $P_i=(a_i,b_i)$ est constructible en une étape à partir de $\mathbb{Q}^2 \cup \{P_1,\dots,P_{i-1}\}$, pour tout $i=1,\dots,m$. Posons alors

$$\tilde{K}_0 := \mathbb{Q} \quad \text{et} \quad \tilde{K}_i := \tilde{K}_{i-1}(a_i,b_i).$$

Par le lemme 5.28(i), on a alors $[\tilde{K}_i : \tilde{K}_{i-1}] \in \{1,2\}$, pour tout $i=1,\dots,m$. Si $[\tilde{K}_i : \tilde{K}_{i-1}]=1$, alors $\tilde{K}_{i-1}=\tilde{K}_i$ et il suffit donc de considérer les $\tilde{K}_i$ distincts pour obtenir la tour d'extensions annoncée.
$\Longleftarrow$: Réciproquement, on montre que c est constructible par récurrence sur r.
Si $r=0$, $c \in \mathbb{Q}$ et la proposition 5.25 permet de conclure. Supposons donc $r \geq 1$. Comme $[K_r : K_{r-1}]=2$, il existe $\beta \in K_{r-1}$ tel que $K_r=K_{r-1}(\sqrt{\beta})$. Par hypothèse de récurrence, β est constructible, donc sa racine carrée l'est aussi par le lemme 5.27, et le lemme 5.28(ii) assure alors que tous les éléments de K_r sont constructibles. En particulier, c est constructible. □

De là, le corollaire suivant est immédiat.

Corollaire 5.30 Si $c \in \mathbb{R}$ est constructible, alors c est algébrique sur $\mathbb{Q}$ et $[\mathbb{Q}(c) : \mathbb{Q}]$ est une puissance de 2.

Preuve. Par le théorème 5.29, il existe une tour d'extensions

$$\mathbb{Q}=K_0 \subset K_1 \subset \cdots \subset K_r$$

avec $c \in K_r$, et chaque extension est quadratique. Cela implique que $[K_r : \mathbb{Q}]$ est une puissance de 2, par multiplicativité des degrés. Aussi, $\mathbb{Q}(c)$ est un sous-corps de K_r, donc $[\mathbb{Q}(c) : \mathbb{Q}]$ divise $[K_r : \mathbb{Q}]$, et il en suit que $[\mathbb{Q}(c) : \mathbb{Q}]$ est aussi une puissance de 2. En particulier, l'extension $\mathbb{Q}(c)/\mathbb{Q}$ est finie, donc algébrique par le lemme 2.16, et c est donc algébrique sur $\mathbb{Q}$. □

Remarque. La réciproque du corollaire 5.30 est fausse. Il existe des nombres réels algébriques sur $\mathbb{Q}$ et générant une extension finie de $\mathbb{Q}$ de degré une puissance de 2, mais non constructibles. Un exemple d'un tel nombre figure en exercices.

Ce critère permet de conclure à l'impossibilité de certaines constructions géométriques, questions remontant à l'Antiquité.

Theorème 5.31 (i) Il est impossible de dupliquer un cube de côté 1 à la règle et au compas.
(ii) La quadrature du cercle de rayon 1 est impossible.
(iii) Il est impossible de trisecter un angle de $\frac{\pi}{3}$ radians à la règle et au compas.

Preuve. (i) S'il est possible de dupliquer un cube de côté 1 à la règle et au compas, le nombre $\sqrt[3]{2}$ est constructible. Ainsi, par le corollaire 5.30, $[\mathbb{Q}(\sqrt[3]{2} : \mathbb{Q}] = 3$ est une puissance de 2, ce qui est absurde.
(ii) Si la quadrature du cercle est réalisable à la règle et au compas, le nombre $\sqrt{\pi}$ est constructible, donc $\pi = \sqrt{\pi}\sqrt{\pi}$ est constructible par la proposition 5.26. Le corollaire 5.30 nous indique alors que π est algébrique sur $\mathbb{Q}$, ce qui est une contradiction.
(iii) Si un angle de $\frac{\pi}{3}$ radians peut être trisecté, le nombre $\alpha := \cos(\frac{\pi}{9})$ est constructible. En utilisant la formule trigonométrique $\cos(3\theta) = 4\cos^3(\theta) - 3\cos(\theta)$, il vient

$$\frac{1}{2} = \cos\left(\frac{\pi}{3}\right) = 4\alpha^3 - 3\alpha.$$

Ainsi α est algébrique sur $\mathbb{Q}$, et $f = X^3 - \frac{3}{4}X - \frac{1}{8}$ est annulateur de α. Directement, on vérifie que f n'a pas de racines dans $\mathbb{Q}$, et est donc le polynôme minimal de α sur $\mathbb{Q}$. Cela implique que $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$ n'est pas une puissance de 2, ce qui contredit le corollaire 5.30. □

Jusqu'ici, tous les résultats démontrés ne font appel que à des propriétés élémentaires des extensions de corps, démontrées dans le chapitre 2 pour la plupart. Le dernier problème que l'on évoque ici nécessite lui la correspondance de Galois. Il s'agit d'une caractérisation des polygones réguliers constructibles à la règle et au compas.

Théorème 5.32 Le polygone régulier à n côtés est constructible si et seulement si $\varphi(n)$ est une puissance de 2.

Comme dans la section 5.2, φ désigne la fonction indicatrice d'Euler.

Preuve. On remarque pour commencer que le polygone régulier à n côtés est constructible si et seulement si le nombre $\xi = \exp(\frac{2\pi i}{n})$ est constructible.
$\Longrightarrow$: Supposons ξ constructible. Alors $\varphi(n) = [\mathbb{Q}(\xi) : \mathbb{Q}]$ est une puissance de 2 par le corollaire 5.30.
$\Longleftarrow$: Si $\varphi(n)$ est une puissance de 2, alors $\varphi(n) = [\mathbb{Q}(\xi) : \mathbb{Q}] = |\mathrm{Gal}(\mathbb{Q}(\xi)/\mathbb{Q})|$ est une puissance de 2, donc il existe une suite décroissante de sous-groupes dans $\mathrm{Gal}(\mathbb{Q}(\xi)/\mathbb{Q})$, de la forme

$$\mathrm{Gal}(\mathbb{Q}(\xi)/\mathbb{Q}) = G_0 \geq G_1 \geq \cdots \geq G_{N-1} \geq G_N = \{e\}$$

avec $[G_{i-1} : G_i] = 2$ pour tout $i = 1, \ldots, N$. Par la correspondance de Galois (théroèem 4.7), il existe donc une suite de sous-corps

$$\mathbb{Q} = K_0 \subset K_1 \subset \cdots \subset K_N = \mathbb{Q}(\xi)$$

telle que $[K_i : K_{i-1}] = 2$ pour tout $i = 1, \ldots, N$. Le théorème 5.29 assure alors la constructibilité de ξ, qui donne la constructibilité du polygone régulier à n côtés. Cela conclut la preuve. □

Comme il est facile de calculer $\varphi(n)$ en fonction de la décomposition de n en facteurs premiers, on peut obtenir une caractérisation plus explicite.

Corollaire 5.33 Le polygone régulier à n côtés est constructible si et seulement si $n = 2^k p_1 \ldots p_l$, où $p_1, \ldots, p_l$ sont des nombres premiers impairs distincts tels que $p_i - 1$ est une puissance de 2 pour tout $i = 1, \ldots, l$.

Preuve. En écrivant $n = 2^k p_1^{k_1} \ldots p_l^{k_l}$, la proposition 5.5 donne

$$\varphi(n) = 2^{k-1} \prod_{i=1}^{l} (p_i - 1) p_i^{k_i - 1}$$

et le théorème 5.32 permet de conclure. □

5.7 Exercices

Exercice 1.

(i) Montrer que $\sqrt[4]{2}+i$ est un élément primitif pour $\mathbb{Q}(\sqrt[4]{2},i)/\mathbb{Q}$.
(ii) Montrer que $\sqrt[4]{2}+i\sqrt[4]{2}$ n'est pas un élément primitif de $\mathbb{Q}(\sqrt[4]{2},i)/\mathbb{Q}$. Trouver son polynôme minimal.

Exercice 2. Soient $p_1,\dots,p_n$ des nombres premiers distincts.

Montrer que $\mathbb{Q}(\sqrt{p_1},\dots,\sqrt{p_n})/\mathbb{Q}$ a degré 2^n. Montrer que cette extension est galoisienne et identifier le groupe de Galois.
Montrer que $\mathbb{Q}(\sqrt{p_1},\dots,\sqrt{p_n})=\mathbb{Q}(\sqrt{p_1}+\cdots+\sqrt{p_n})$.

Exercice 3. Soit $n\geq 1$.
Montrer que si $n=p_1^{\varepsilon_1}\dots p_k^{\varepsilon_k}$ est sa décomposition en produits de facteurs premiers, alors $\varphi(n)=n\prod_{i=1}^{k}\left(1-\frac{1}{p_i}\right)$.

Exercice 4.

(i) Montrer que, pour tout $n\geq 1$, pour tout $k\geq 1$, $\varphi(n^k)=n^{k-1}\varphi(n)$.
(ii) Montrer que, si m divise n, alors $\varphi(m)$ divise $\varphi(n)$.

Exercice 5. Soient n, $m\geq 1$, avec $m\leq n$.

(i) Montrer que si n et m sont premiers entre eux, alors n et $n-m$ sont premiers entre eux.
(ii) En déduire que si $n\geq 3$, alors $\varphi(n)$ est pair.
(iii) En déduire que $\dfrac{n\varphi(n)}{2}=\displaystyle\sum_{\substack{m<n\\ \mathrm{pgcd}(m,n)=1}} m$.

Exercice 6. Démontrer le théorème d'Euler : pour tout $n\geq 1$ et tout entier a premier avec n, $a^{\varphi(n)}\equiv 1 \mod n$.

Exercice 7. Soient $a=\sqrt[4]{5}\in\mathbb{C}$, et $b=a+ia$. Soit M la clôture normale de $\mathbb{Q}(b)/\mathbb{Q}$.

(i) Est-ce que $M/\mathbb{Q}$ est cyclique ? abélienne ? résoluble ?
(ii) Trouver un sous-corps L de M tel que $\mathrm{Gal}(M/L)$ est cyclique d'ordre 4.

Exercice 8. Démontrer les assertions suivantes.

(i) Soit L/K une extension cyclique, et $n=[L:K]$. Pour tout diviseur d de n, il existe un unique corps M tel que $K\subset M\subset L$, $[M:K]=d$ et L/M, M/K sont cycliques.
(ii) Soit L/K une extension résoluble. Pour tout corps $K\subset M\subset L$, L/M est résoluble.
Si de plus M/K est normale, alors M/K est aussi résoluble.
(iii) Soit L/K résoluble. Il existe une tour d'extensions

$$K=L_0\subset L_1\subset \ldots\subset L_m=L$$

telle que L_i/L_{i-1} est cyclique pour tout $1\leq i\leq m$.
(iv) Soit L/K une extension telle que $[L:K]=p^n$, avec p un nombre premier. Alors L/K est résoluble.
(v) Soit L/K une extension telle que $\mathrm{Gal}(L/K)\simeq S_n$, avec $n\geq 5$. Alors L/K n'est pas résoluble.

Exercice 9. Soit $K=\mathbb{Q}$.

(i) Donner un exemple d'une extension abélienne de K.
(ii) Donner un exemple d'une extension nilpotente de K, mais non-abélienne.
(iii) Donner un exemple d'une extension résoluble de K, mais non-nilpotente.
(iv) Pouvez-vous donner des exemples d'extensions finies de $K=\mathbb{F}_p$ similaires à (ii) et (iii) ?

Exercice 10. A l'aide d'un contre-exemple, montrer que la conclusion du point (i) du théorème 5.16 est fausse sans l'hypothèse que K contient une racine primitive $n-$ième de l'unité.

Exercice 11. Soit $f = X^6 - 2 \in \mathbb{Q}[X]$.

(i) Déterminer un corps de décomposition L de f sur $\mathbb{Q}$.
(ii) Calculer $|\mathrm{Gal}(L/\mathbb{Q})|$ et $\mathrm{Gal}(L/\mathbb{Q}(\omega))$.

Exercice 12. Montrer que si L/K et M/L sont deux extensions par radicaux, alors M/K est une extension par radicaux.

Exercice 13. Soient K un corps, et L_1/K, L_2/K deux extensions galoisiennes finies.

(i) Montrer que L_1L_2/K est galoisienne.
(ii) Montrer qu'il existe un morphisme de groupes injectif $\mathrm{Gal}(L_1L_2/K) \hookrightarrow \mathrm{Gal}(L_1/K) \times \mathrm{Gal}(L_2/K)$.
(iii) En déduire que le compositum de deux extensions abéliennes de K est une extension abélienne de K.
(iv) Montrer que le point précédent est faux si on remplace "abélienne" par "cyclique". Et si on remplace "abélienne" par "résoluble" ?

Exercice 14. Soient K un corps, et L_1/K, L_2/K deux extensions galoisiennes finies.

(i) Montrer que l'application $\theta\colon \mathrm{Gal}(L_1L_2/L_2) \longrightarrow \mathrm{Gal}(L_1/L_1 \cap L_2)$, $\sigma \longmapsto \sigma_{|L_1}$ est un homomorphisme de groupes bien défini. Montrer de plus qu'il est injectif.
(ii) Montrer que, dans K, $L_1^{\mathrm{Im}(\theta)} = L_1 \cap L_2$. Déduire que $\mathrm{Gal}(L_1L_2/L_2) \simeq \mathrm{Gal}(L_1/L_1 \cap L_2)$.
(iv) En déduire la formule $[L_1L_2 : K] = \frac{[L_1:K][L_2:K]}{[L_1 \cap L_2:K]}$.

Exercice 15. Soient m, n deux entiers naturels, et $d := \mathrm{pgcd}(m,n)$, $\ell := \mathrm{ppcm}(m,n)$.
Montrer que $\mathbb{Q}(\xi_n)\mathbb{Q}(\xi_m) = \mathbb{Q}(\xi_\ell)$ et $\mathbb{Q}(\xi_n) \cap \mathbb{Q}(\xi_m) = \mathbb{Q}(\xi_d)$, où ξ_i désigne une racine primitive $i-$ième de l'unité, pour $i \in \{n, m, l, d\}$.

Exercice 16. Soient p, q deux nombres premiers distincts, $n := pq$ et ξ une racine primitive $n-$ième de l'unité. Soit $K = \mathbb{Q}(\xi)$, $f = (X^p - 2)(X^q - 2) \in K[X]$ et N un corps de décomposition de f sur K.
Montrer que N/K est cyclique.

Exercice 17. Dans cet exercice on étudie le corps de décomposition de $X^n - a$, et son groupe de Galois, sur un corps F qui ne contient pas une racine primitive $n-$ième de l'unité.
Soit donc F un corps, $a \in F$, et $X^n - a \in F[X]$. Supposons que $\mathrm{char}(F)$ ne divise pas n.

(i) Montrer que le corps de décomposition de $X^n - a$ sur F est $F(\omega, \alpha)$, où $\alpha^n = a$ et ω est une racine primitive $n-$ième de l'unité.
(ii) Soit $N = F(\omega, \alpha)$, $K = F(\alpha)$, $L = F(\omega)$. Montrer que L/F est galoisienne et que N/L est cyclique.
(iii) Supposons que $(X - \omega)(X - \omega^{-1})$ est le polynôme minimal de ω sur F, et que $[N : L] = n$. Montrer qu'il existe $\sigma \in \mathrm{Gal}(N/F)$ tel que $\sigma(\alpha) = \omega\alpha$, $\sigma(\omega) = \omega$ et $\tau \in \mathrm{Gal}(N/F)$ tel que $\tau(\alpha) = \alpha$, $\tau(\omega) = \omega^{-1}$.
(iv) Montrer qu'alors $\mathrm{Gal}(N/F) \simeq D_n$, le groupe diédral à $2n$ éléments.

Exercice 18. Pour les polynômes $f \in \mathbb{Q}[X]$ suivants, déterminer si l'équation $f = 0$ est résoluble par radicaux.

(i) $f = X^5 - X^3 - 5X^2 + 5$
(ii) $f = X^5 - 10X + 5$
(iii) $f = X^5 + 2X^3 + X^2 + X + 1$
(iv) $f = X^6 - 2$
(v) $f = X^7 - X^5 - 4X^3 - X^2 + 4X + 1$

Exercice 19. Soit $c \in \mathbb{R}$ algébrique sur $\mathbb{Q}$, et soit N la clôture normale de $\mathbb{Q}(c)/\mathbb{Q}$.

(i) Montrer que si $[N : \mathbb{Q}]$ est une puissance de 2, alors c est constructible.
(ii) Réciproquement, montrer que si c est constructible, alors $[N : \mathbb{Q}]$ est une puissance de 2.

Exercice 20. Soit $c \in \mathbb{R}$ une racine d'un polynôme de degré 4 irréductible sur $\mathbb{Q}$, et soit N la clôture normale de $\mathbb{Q}(c)/\mathbb{Q}$.

(i) Montrer que si $\mathrm{Gal}(N/\mathbb{Q})$ est isomorphe à D_4 ou à un groupe d'ordre 4, alors c est constructible.
(ii) Montrer que si $\mathrm{Gal}(N/\mathbb{Q})$ est isomorphe à A_4 ou S_4, alors c n'est pas constructible.

Exercice 21. Dans cet exercice, on démontre que la réciproque du corollaire 5.30 est fausse en général.
Soit $f = X^4 - 4X^2 + 2 \in \mathbb{Q}[X]$.

(i) Montrer que f n'a pas de racines dans $\mathbb{Q}$ et exactement deux racines dans $\mathbb{R}$. Notons-les a_1 et a_2.
(ii) En déduire qu'il existe α, β, γ, $\delta \in \mathbb{R}$ tels que $f = (X^2 + \alpha X + \beta)(X^2 + \gamma X + \delta)$.
(iii) Montrer que le nombre $b = \beta + \delta$ est algébrique sur $\mathbb{Q}$, et que $[\mathbb{Q}(b) : \mathbb{Q}] = 3$.
(iv) Vérifier que f est irréductible sur $\mathbb{Q}$ et que $[\mathbb{Q}(a_1) : \mathbb{Q}] = [\mathbb{Q}(a_2) : \mathbb{Q}] = 4$.
(v) Montrer que parmi a_1 et a_2, au moins un n'est pas constructible.
(vi) En déduire qu'en fait, ni a_1 ni a_2 n'est constructible.

Exercice 22. Montrer que $\cos(\frac{2\pi}{n})$ et $\sin(\frac{2\pi}{n})$ sont algébriques sur $\mathbb{Q}$, et que $\mathbb{Q}(\cos(\frac{2\pi}{n}))/\mathbb{Q}$ est galoisienne.
Que dire à propos de $\mathbb{Q}(\sin(\frac{2\pi}{n}))/\mathbb{Q}$?

Exercice 23.

(i) Trouver le polynôme minimal de $\cos(\frac{2\pi}{5})$ sur $\mathbb{Q}$. En déduire que $\cos(\frac{2\pi}{5}) = \frac{-1+\sqrt{5}}{4}$.
(ii) Est-il possible de trisecter $\frac{2\pi}{5}$ à la règle et au compas ?