INTRODUCTION À LA THÉORIE DE GALOIS ET LA GÉOMÉTRIE ALGÉBRIQUE

Jan Nekovář

I. THÉORIE DE GALOIS

Références: [Es], [Ti 1,2], [Ga], [Ar], [Sa]

Introduction

Le problème principal est la résolution des équations polynomiales à une variable

$$x^n + a_1 x^{n-1} + \cdots + a_n = 0.$$

On s'interesse surtout à la résolution "par radicaux", c'est-à-dire à la résolution qui n'utilise que des racines $\sqrt[m]{a}$.

Il est bien connu depuis le $16^{\text{ème}}$ siècle que l'on peut résoudre par radicaux des équations de degré $n \leq 4$. Par contre, selon un résultat célèbre d'Abel, l'équation générale de degré $n \geq 5$ n'est pas résoluble par radicaux.

L'idée principale de la théorie de Galois est d'associer à chaque équation son groupe de symétrie. Cette construction permet de traduire des propriétés de l'équation (telles que la résolubilité par radicaux) aux propriétés du groupe associé.

Le cours ne suivra pas le chemin historique. L'ouvrage [Ti 1, 2] est une référence agréable pour l'histoire du sujet.

1. Résolution des équations – exemples

Dans ce chapitre introductif nous rappelons au lecteur comment résoudre des équations de degré $2, 3, 4$ par la méthode de Lagrange, en utilisant leurs symétries. Nous allons aussi étudier les équations $X^n = 1$.

(1.1) Considérons une équation

$$x^n + a_1 x^{n-1} + \cdots + a_n = 0 \tag{1.1.1}$$

de degré $n \geq 1$ à coefficients complexes $a_1, \ldots, a_n \in \mathbf{C}$. Selon un résultat fondamental de Gauss, l'équation (1.1.1) admet précisement n racines complexes $x_1, \ldots, x_n$ (qui ne sont pas, en général, distinctes) dans le sens que l'on à l'identité polynomiale

$$x^n + a_1 x^{n-1} + \cdots + a_n = (x - x_1) \cdots (x - x_n). \tag{1.1.2}$$

En dévelopant le terme à droite et en comparant les coefficients, on obtient les relation suivantes:

$$a_1 = -\sigma_1, \qquad a_2 = \sigma_2 \qquad \ldots \qquad a_n = (-1)^n \sigma_n, \tag{1.1.3}$$

où

$$\begin{aligned}
\sigma_1 &= x_1 + \cdots + x_n = \sum_i x_i \\
\sigma_2 &= x_1x_2 + x_1x_3 + \cdots + x_{n-1}x_n = \sum_{i<j} x_ix_j \\
&\cdots \\
\sigma_k &= \sum_{1\le i_1<\cdots<i_k\le n} x_{i_1}\cdots x_{i_k} \\
&\cdots \\
\sigma_n &= x_1\cdots x_n
\end{aligned} \tag{1.1.4}$$

sont les **polynômes symétriques élémentaires** des racines $x_1, \ldots, x_n$. Autrement dit, la résolution de l'équation (1.1.1) équivaut à la résolution du système (1.1.4) avec $\sigma_k = (-1)^k a_k$.

Les fonctions (1.1.4) sont symétriques en $x_1, \ldots, x_n$ (voir 1.7.3 ci-dessous pour la définition formelle); selon Lagrange, on cherche à résoudre les équations (1.1.4) en brisant progressivement leur symétrie. Comme nous allons expliquer, cette méthode réussit si $n \le 4$.

(1.2) Équations de degré 2. Il faut résoudre le système

$$x_1 + x_2 = -a_1, \qquad x_1x_2 = a_2. \tag{1.2.1}$$

On considère la fonction

$$y = x_1 - x_2 \tag{1.2.2}$$

qui n'est pas symétrique en x_1 et x_2, mais dont le carré l'est:

$$y^2 = (x_1 - x_2)^2 = x_1^2 + x_2^2 - 2x_1x_2 = (x_1 + x_2)^2 - 4x_1x_2 = \sigma_1^2 - 4\sigma_2 = a_1^2 - 4a_2, \tag{1.2.3}$$

d'où les formules bien connues:

$$y = \pm\sqrt{a_1^2 - 4a_2}, \qquad x_1, x_2 = \frac{1}{2}((x_1 + x_2) \pm y) = \frac{1}{2}(-a_1 \pm \sqrt{a_1^2 - 4a_2}) \tag{1.2.4}$$

(1.3) Équations de degré 3

(1.3.1) Il faut résoudre l'équation

$$x^3 + a_1x^2 + a_2x + a_3 = 0, \tag{1.3.1.1}$$

c'est-à-dire le système

$$\sigma_1 = x_1 + x_2 + x_3 = -a_1, \qquad \sigma_2 = x_1x_2 + x_1x_3 + x_2x_3 = a_2, \qquad \sigma_3 = x_1x_2x_3 = -a_3. \tag{1.3.1.2}$$

Il est naturel de généraliser (1.2.2) de la manière suivante: on prend

$$\begin{aligned}
y_1 &= x_1 + \rho x_2 + \rho^2 x_3 \\
y_2 &= x_1 + \rho^2 x_2 + \rho x_3,
\end{aligned} \tag{1.3.1.3}$$

où

$$\rho = e^{2\pi i/3} = \tfrac{-1+i\sqrt{3}}{2}, \qquad \rho^2 = \rho^{-1} = e^{-2\pi i/3} = \tfrac{-1-i\sqrt{3}}{2} = -1 - \rho$$

sont les racines cubiques (primitives) de l'unité.

Quelles sont les symétries des fonctions y_1, y_2? Si l'on échange x_1 et x_2 (resp., x_2 et x_3), les fonctions y_1, y_2 seront transformées selons les formules

$$y_1 \mapsto x_2 + \rho x_1 + \rho^2 x_3 = \rho y_2, \qquad y_2 \mapsto x_2 + \rho^2 x_1 + \rho x_3 = \rho^2 y_1$$

resp.,

$$y_1 \mapsto x_1 + \rho x_3 + \rho^2 x_2 = y_2, \qquad y_2 \mapsto x_1 + \rho^2 x_3 + \rho x_2 = y_1.$$

Il en résulte que les fonctions $y_1 y_2$ et $y_1^3 + y_2^3$ sont symétriques en x_1, x_2, x_3:

$$\begin{aligned} y_1 y_2 &= x_1^2 + x_2^2 + x_3^2 - x_1x_2 - x_1x_3 - x_2x_3 \\ y_1^3 + y_2^3 &= 2(x_1^3 + x_2^3 + x_3^3) + 12x_1x_2x_3 - 3(x_1^2x_2 + x_1x_2^2 + x_1^2x_3 + x_1x_3^2 + x_2^2x_3 + x_2x_3^2) \end{aligned} \tag{1.3.1.4}$$

Peut-on les exprimer en fonction de $\sigma_1, \sigma_2, \sigma_3$? Posons

$$s_k = x_1^k + x_2^k + x_3^k, \qquad s_{2,1} = x_1^2x_2 + x_1x_2^2 + x_1^2x_3 + x_1x_3^2 + x_2^2x_3 + x_2x_3^2,$$

donc

$$y_1 y_2 = s_2 - \sigma_2, \qquad y_1^3 + y_2^3 = 2s_3 + 12\sigma_3 - 3s_{2,1}.$$

On peut exprimer s_2, s_3 et $s_{2,1}$ en fonction de σ_1, σ_2 et σ_3: on a

$$\begin{aligned} \sigma_1^2 &= (x_1 + x_2 + x_3)^2 = x_1^2 + x_2^2 + x_3^2 + 2(x_1x_2 + x_1x_3 + x_2x_3) = s_2 + 2\sigma_2 \\ \sigma_1\sigma_2 &= (x_1 + x_2 + x_3)(x_1x_2 + x_1x_3 + x_2x_3) = s_{2,1} + 3x_1x_2x_3 = s_{2,1} + 3\sigma_3 \\ \sigma_1 s_2 &= (x_1 + x_2 + x_3)(x_1^2 + x_2^2 + x_3^2) = (x_1^3 + x_2^3 + x_3^3) + s_{2,1} = s_3 + s_{2,1}, \end{aligned} \tag{1.3.1.5}$$

d'où

$$s_2 = \sigma_1^2 - 2\sigma_2, \qquad s_{2,1} = \sigma_1\sigma_2 - 3\sigma_3, \qquad s_3 = \sigma_1 s_2 - s_{2,1} = \sigma_1^3 - 3\sigma_1\sigma_2 + 3\sigma_3 \tag{1.3.1.6}$$

et

$$y_1 y_2 = \sigma_1^2 - 3\sigma_2, \qquad y_1^3 + y_2^3 = 2\sigma_1^3 - 9\sigma_1\sigma_2 + 27\sigma_3 \tag{1.3.1.7}$$

(on verra plus tard que tout polynôme symétrique $F(x_1, \ldots, x_n)$ s'exprime en fonction de $\sigma_1, \ldots, \sigma_n$).

En résumé, les cubes y_1^3, y_2^3 sont les racines de l'équation quadratique

$$(t - y_1^3)(t - y_2^3) = t^2 - (2\sigma_1^3 - 9\sigma_1\sigma_2 + 27\sigma_3)t + (\sigma_1^2 - 3\sigma_2)^3 = 0 \tag{1.3.1.8}$$

et l'on a

$$y_1 y_2 = \sigma_1^2 - 3\sigma_2. \tag{1.3.1.9}$$

(1.3.2) Les formules de Cardan. On peut simplifier (1.3.1.1) en

$$x^3 + px + q = 0 \tag{1.3.2.1}$$

par la substitution $x \mapsto x + a_1/3$. En appliquant la méthode de 1.3.1 à l'équation (1.3.2.1), on a

$$\sigma_1 = 0, \qquad \sigma_2 = p, \qquad \sigma_3 = -q,$$

donc (1.3.1.7) s'écrit

$$y_1 y_2 = -3p, \qquad y_1^3 + y_2^3 = -27q \tag{1.3.2.2}$$

et y_1^3, y_2^3 sont les racines de l'équation quadratique

$$(t-y_1^3)(t-y_2^3) = t^2 + 27qt - 27p^3 = 0, \tag{1.3.2.3}$$

d'où

$$y_1^3, y_2^3 = 27\left(-\frac{q}{2} \pm \sqrt{\left(\frac{p}{3}\right)^3 + \left(\frac{q}{2}\right)^2}\right). \tag{1.3.2.4}$$

Il résulte de

$$y_1 + y_2 = 3x_1, \qquad \rho^2 y_1 + \rho y_2 = 3x_2, \qquad \rho y_1 + \rho^2 y_2 = 3x_3 \tag{1.3.2.5}$$

que les racines x_1, x_2, x_3 sont données par les formules suivantes (dites "**de Cardan**"):

$$\begin{aligned} x_1 &= \sqrt[3]{-\frac{q}{2} + \sqrt{\left(\frac{p}{3}\right)^3 + \left(\frac{q}{2}\right)^2}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\left(\frac{p}{3}\right)^3 + \left(\frac{q}{2}\right)^2}} \\ x_2 &= \rho^2\sqrt[3]{-\frac{q}{2} + \sqrt{\left(\frac{p}{3}\right)^3 + \left(\frac{q}{2}\right)^2}} + \rho\sqrt[3]{-\frac{q}{2} - \sqrt{\left(\frac{p}{3}\right)^3 + \left(\frac{q}{2}\right)^2}} \\ x_3 &= \rho\sqrt[3]{-\frac{q}{2} + \sqrt{\left(\frac{p}{3}\right)^3 + \left(\frac{q}{2}\right)^2}} + \rho^2\sqrt[3]{-\frac{q}{2} - \sqrt{\left(\frac{p}{3}\right)^3 + \left(\frac{q}{2}\right)^2}} \end{aligned} \tag{1.3.2.6}$$

Ici, les racines cubiques sont normalisées par la première équation de (1.3.2.2), i.e. par

$$\sqrt[3]{-\frac{q}{2} + \sqrt{\left(\frac{p}{3}\right)^3 + \left(\frac{q}{2}\right)^2}} \cdot \sqrt[3]{-\frac{q}{2} - \sqrt{\left(\frac{p}{3}\right)^3 + \left(\frac{q}{2}\right)^2}} = -\frac{p}{3}. \tag{1.3.2.7}$$

(1.3.3) Exemple. Considérons l'équation

$$x^3 - 8x - 8 = 0, \tag{1.3.3.1}$$

qui a une racine évidente $x_1 = -2$, donc se factorise

$$x^3 - 8x - 8 = (x+2)(x^2 - 2x - 4) = (x+2)(x - (1+\sqrt{5}))(x - (1-\sqrt{5})),$$

c'est-à-dire

$$x_1 = -2, \qquad x_2 = 1 + \sqrt{5}, \qquad x_3 = 1 - \sqrt{5}. \tag{1.3.3.2}$$

D'autre part, les formules de Cardan pour $p = q = -8$ montrent que

$$\begin{aligned} x_1 &= \sqrt[3]{4 + \frac{4i}{9}\sqrt{15}} + \sqrt[3]{4 - \frac{4i}{9}\sqrt{15}} \\ x_2 &= \rho^2\sqrt[3]{4 + \frac{4i}{9}\sqrt{15}} + \rho\sqrt[3]{4 - \frac{4i}{9}\sqrt{15}} \\ x_3 &= \rho\sqrt[3]{4 + \frac{4i}{9}\sqrt{15}} + \rho^2\sqrt[3]{4 - \frac{4i}{9}\sqrt{15}} \end{aligned} \tag{1.3.3.3}$$

avec la normalisation

$$\sqrt[3]{4 + \frac{4i}{9}\sqrt{15}} \cdot \sqrt[3]{4 - \frac{4i}{9}\sqrt{15}} = \frac{8}{3}.$$

Il n'est pas du tout évident que l'on peut simplifier les valeurs (1.3.3.3) et obtenir (1.3.3.2) ! Bien sûr, les formules (1.3.1.3) montrent que

$$y_1, y_2 = -3 \pm i\sqrt{15},$$

d'où

$$\sqrt[3]{4 \pm \frac{4i}{9}\sqrt{15}} = -1 \pm \frac{i\sqrt{15}}{3}, \tag{1.3.3.4}$$

mais il n'est pas possible de déduire (1.3.3.4) sans avoir déjà trouvé les racines (1.3.3.2).

En général, si $p, q \in \mathbf{Q}$, on peut écrire les racines cubiques dans (1.3.2.6) sous la forme simplifiée $a + \sqrt{b}$ (avec $a, b \in \mathbf{Q}$) si et seulement si l'équation (1.3.2.1) admet une racine rationnelle $x_1 \in \mathbf{Q}$. La méthode suivante nous permetra de trouver toutes les racines rationnelles.

(1.3.4) Proposition. *Soit $\alpha = \frac{a}{b}$ une racine du polynôme $f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n$, où $a, b, a_0, \ldots, a_n \in \mathbf{Z}$, $a_0 b \neq 0$, $\operatorname{pgcd}(a, b) = 1$. Alors $b|a_0$ (b divise a_0) et $a|a_n$. En particulier, si $a_0 = 1$, alors on a $\alpha \in \mathbf{Z}$ et $\alpha|a_n$.*

Preuve. On déduit de l'égalité

$$0 = b^n f\left(\tfrac{a}{b}\right) = a_0a^n + a_1a^{n-1}b + \cdots + a_{n-1}ab^{n-1} + a_nb^n$$

que

$$\begin{aligned} a \text{ divise } & -a(a_0a^{n-1} + a_1a^{n-2}b + \cdots + a_{n-1}b^{n-1}) = a_nb^n \\ b \text{ divise } & -b(a_1a^{n-1} + \cdots + a_{n-1}ab^{n-2} + a_nb^{n-1}) = a_0a^n. \end{aligned}$$

Il en résulte que a divise a_n et b divise a_0, car $\operatorname{pgcd}(a, b^n) = \operatorname{pgcd}(b, a^n) = 1$.

(1.3.5) Corollaire. *Soient $c, n \in \mathbf{Z}$ des entiers, $n \geq 1$. Alors on a:*

$$\sqrt[n]{c} \in \mathbf{Q} \iff \sqrt[n]{c} \in \mathbf{Z} \quad (\iff \text{ il existe } a \in \mathbf{Z} \text{ tel que } c = a^n).$$

Preuve. On applique 1.3.4 au polynôme $f(x) = x^n - c$.

(1.3.6) Exemple : $\sqrt{2}, \sqrt{5}, \sqrt[3]{2} \notin \mathbf{Q}$.

(1.4) Équations de degré 4

(1.4.1) Il faut résoudre l'équation

$$x^4 + a_1x^3 + a_2x^2 + a_3x + a_4 = 0.$$

Par la substitution $x \mapsto x + a_1/4$ on se ramène au cas $a_1 = 0$, c'est-à-dire à l'équation

$$x^4 + px^2 + qx + r = 0, \tag{1.4.1.1}$$

pour laquelle

$$\sigma_1 = 0, \qquad \sigma_2 = p, \qquad \sigma_3 = -q, \qquad \sigma_4 = r. \tag{1.4.1.2}$$

En généralisant (1.3.1.3), considérons le comportement des expressions linéaires

$$x_1 + ix_2 - x_3 - ix_4, \qquad x_1 - x_2 + x_3 - x_4, \qquad x_1 - ix_2 - x_3 + ix_4$$

par rapport aux changements de variables

$$x_1 \longleftrightarrow x_2, \qquad x_2 \longleftrightarrow x_3, \qquad x_3 \longleftrightarrow x_4. \tag{1.4.1.3}$$

Il est facile de voir que l'ensemble de polynômes linéaires

$$u_1 = x_1 + x_2 - x_3 - x_4, \qquad u_2 = x_1 + x_3 - x_2 - x_4, \qquad u_3 = x_1 + x_4 - x_2 - x_3$$

est conservé – au signe près – par les substitutions (1.4.1.3). Il en résulte que les coefficients du polynôme cubique

$$(u - u_1^2)(u - u_2^2)(u - u_3^2) \tag{1.4.1.4}$$

sont symétriques en x_1, x_2, x_3, x_4. Les coefficients de (1.4.1.4) sont déterminés dans ([Es], 10.8). Ici, nous allons considérer un polynôme légèrement modifié:

$$(y - y_1)(y - y_2)(y - y_3) = y^3 + b_1 y^2 + b_2 y + b_3, \tag{1.4.1.5}$$

où

$$y_1 = x_1x_2 + x_3x_4, \qquad y_2 = x_1x_3 + x_2x_4, \qquad y_3 = x_1x_4 + x_2x_3.$$

En fait, on a

$$\begin{aligned} -(u_1/2)^2 &= -(x_1 + x_2)^2 = (x_1 + x_2)(x_3 + x_4) = y_2 + y_3 \\ -(u_2/2)^2 &= -(x_1 + x_3)^2 = (x_1 + x_3)(x_2 + x_4) = y_1 + y_3 \\ -(u_3/2)^2 &= -(x_1 + x_4)^2 = (x_1 + x_4)(x_2 + x_3) = y_1 + y_2, \end{aligned} \tag{1.4.1.6}$$

car $x_1 + x_2 + x_3 + x_4 = \sigma_1 = 0$. Les coefficients de (1.4.1.5) sont égaux à

$$\begin{aligned} -b_1 &= y_1 + y_2 + y_3 = \sigma_2 \\ b_2 &= y_1y_2 + y_1y_3 + y_2y_3 = x_1^2x_2x_3 + \cdots + x_2x_3x_4^2 = s_{2,1,1} \\ -b_3 &= y_1y_2y_3 = (x_1^3x_2x_3x_4 + \cdots + x_1x_2x_3x_4^3) + (x_1^2x_2^2x_3^2 + \cdots + x_2^2x_3^2x_4^2) = s_{3,1,1,1} + s_{2,2,2}, \end{aligned}$$

où l'on a posé

$$s_{i_1,\cdots,i_k} = \text{“la symétrisation de } x_1^{i_1} \cdots x_k^{i_k}\text{”}$$

(voir 1.7.5 ci-dessous pour une définition formelle). Les formules

$$\begin{aligned} &\sigma_1\sigma_3 = (x_1 + \cdots + x_4)(x_1x_2x_3 + \cdots + x_2x_3x_4) = s_{2,1,1} + 4x_1x_2x_3x_4 = s_{2,1,1} + 4\sigma_4 \\ &\sigma_3^2 = (x_1x_2x_3 + \cdots + x_2x_3x_4)^2 = x_1^2x_2^2x_3^2 + \cdots + x_2^2x_3^2x_4^2 + 2(x_1^2x_2^2x_3x_4 + \cdots + x_2x_3x_3^2x_4^2) = s_{2,2,2} + 2\sigma_2\sigma_4 \\ &\sigma_4 s_2 = x_1x_2x_3x_4(x_1^2 + \cdots + x_4^2) = x_1^3x_2x_3x_4 + \cdots + x_1x_2x_3x_4^3 = s_{3,1,1,1} \end{aligned} \tag{1.4.1.7}$$

montrent que l'on a en général (sans que l'on suppose $\sigma_1 = 0$)

$$s_{2,1,1} = \sigma_1\sigma_3 - 4\sigma_4, \qquad s_{2,2,2} = \sigma_3^2 - 2\sigma_2\sigma_4, \qquad s_{3,1,1,1} = \sigma_4 s_2 = \sigma_4(\sigma_1^2 - 2\sigma_2) \tag{1.4.1.8}$$

et

$$b_1 = -\sigma_2, \qquad b_2 = \sigma_1\sigma_3 - 4\sigma_4, \qquad b_3 = -\sigma_1^2\sigma_4 + 4\sigma_2\sigma_4 - \sigma_3^2,$$

donc

$$b_1 = -p, \qquad b_2 = -4r, \qquad b_3 = 4pr - q^2$$

dans le cas (1.4.1.2). En résumé, les expressions y_1, y_2, y_3 sont les racines de l'équation cubique

$$y^3 - py^2 - 4ry + (4pr - q^2) = 0 \tag{1.4.1.9}$$

(“**l'équation cubique résolvante** de l'équation quartique (1.4.1.1)”). Dès que l'on sait résoudre (1.4.1.9), on déduit de (1.4.1.6) les valeurs de $x_i + x_j$ $(i \neq j)$, donc celles de x_i.

(1.4.2) Exercice. *Déterminer les coefficients de (1.4.1.4).*

(1.5) Discriminant des polynômes de degré $2, 3, 4$

(1.5.1) Par définition, le **discriminant** du polynôme unitaire

$$f(x) = x^n + a_1 x^{n-1} + \cdots a_n = (x - x_1) \cdots (x - x_n)$$

à racines $x_1, \ldots, x_n$ est égal à

$$\mathrm{disc}(f) = \prod_{1 \leq i < j \leq n} (x_i - x_j)^2. \tag{1.5.1.1}$$

On verra dans 1.7.11 que $\mathrm{disc}(f)$ s'écrit comme une fonction polynomiale des coefficients $a_1, \ldots, a_n$.

(1.5.2) Pour $n = 2$, la formule (1.2.3) montre que

$$\mathrm{disc}(x^2 + ax + b) = a^2 - 4b.$$

(1.5.3) Exercice. *Soit $n = 3$. Avec la notation de 1.3.1, montrer que $-27\mathrm{disc}(f)$ est égal au discriminant du polynôme quadratique (1.3.1.8). En déduire une formule explicite pour* $\mathrm{disc}(f)$*. En particulier, montrer que*

$$\mathrm{disc}(x^3 + px + q) = -4p^3 - 27q^2.$$

(1.5.4) Exercice. *Soit $n = 4$. Avec la notation de 1.4.1, montrer que le discriminant du polynôme f dans (1.4.1.1) est égal au discriminant de son équation cubique résolvante (1.4.1.9). En déduire une formule explicite pour* $\mathrm{disc}(f)$*. En particulier, montrer que*

$$\mathrm{disc}(x^4 + qx + r) = -27q^4 + 256r^3.$$

(1.5.5) Exercice. *Deviner la valeur de* $\mathrm{disc}(x^n + ax + b)$*.*

(1.6) Racines de l'unité

(1.6.1) Pour tout entier $n \geq 1$, les racines n-ième de l'unité

$$\mu_n = \{\zeta \in \mathbf{C} \,|\, \zeta^n = 1\}$$

sont les racines du polynôme

$$X^n - 1 = \prod_{\zeta \in \mu_n} (X - \zeta).$$

Géométriquement, μ_n sont les sommets d'un polygône régulier inscrit dans le cercle unité.

Les polynômes $X^n - 1$ se factorisent de manière très naturelle:

$$\begin{aligned}
X - 1 &= \Phi_1 \\
X^2 - 1 &= (X-1)(X+1) = \Phi_1\Phi_2 \\
X^3 - 1 &= (X-1)(X^2+X+1) = \Phi_1\Phi_3 \\
X^4 - 1 &= (X-1)(X+1)(X^2+1) = \Phi_1\Phi_2\Phi_4 \\
X^5 - 1 &= (X-1)(X^4+X^3+X^2+X+1) = \Phi_1\Phi_5 \\
X^6 - 1 &= (X-1)(X+1)(X^2+X+1)(X^2-X+1) = \Phi_1\Phi_2\Phi_3\Phi_6 \\
X^7 - 1 &= (X-1)(X^6+X^5+X^4+X^3+X^2+X+1) = \Phi_1\Phi_7 \\
X^8 - 1 &= (X-1)(X+1)(X^2+1)(X^4+1) = \Phi_1\Phi_2\Phi_4\Phi_8 \\
X^9 - 1 &= (X-1)(X^2+X+1)(X^6+X^3+1) = \Phi_1\Phi_3\Phi_9 \\
X^{10} - 1 &= (X-1)(X+1)(X^4+X^3+X^2+X+1)(X^4-X^3+X^2-X+1) = \Phi_1\Phi_2\Phi_5\Phi_{10} \\
X^{11} - 1 &= (X-1)(X^{10}+X^9+X^8+X^7+X^6+X^5+X^4+X^3+X^2+X+1) = \Phi_1\Phi_{11} \\
X^{12} - 1 &= (X-1)(X+1)(X^2+X+1)(X^2-X+1)(X^4-X^2+1) = \Phi_1\Phi_2\Phi_3\Phi_6\Phi_{12},
\end{aligned} \tag{1.6.1.1}$$

où

$$\begin{array}{lll}\Phi_1(X)=X-1 & \Phi_5(X)=X^4+X^3+X^2+X+1 & \Phi_9(X)=X^6+X^3+1\\ \Phi_2(X)=X+1 & \Phi_6(X)=X^2-X+1 & \Phi_{10}(X)=X^4-X^3+X^2-X+1\\ \Phi_3(X)=X^2+X+1 & \Phi_7(X)=X^6+\cdots+1 & \Phi_{11}(X)=X^{10}+\cdots+1\\ \Phi_4(X)=X^2+1 & \Phi_8(X)=X^4+1 & \Phi_{12}(X)=X^4-X^2+1\end{array} \tag{1.6.1.2}$$

(1.6.2) Question. *Quelle est la règle générale?*

(1.6.3) On pose $\mathbf{e}(z)=e^{2\pi iz}$ et $\zeta_n=\mathbf{e}(\frac{1}{n})$; alors on a

$$\mu_n=\{\mathbf{e}\left(\tfrac{a}{n}\right)\mid 1\le a\le n\}=\{\zeta_n^a\mid 1\le a\le n\}. \tag{1.6.3.1}$$

Toute fraction $\frac{a}{n}$ dans (1.6.3.1) s'écrit comme une fraction irréductible $\frac{b}{d}$, où d divise n. On en déduit une décomposition disjointe

$$\mu_n=\bigcup_{d|n}\{\mathbf{e}\left(\tfrac{b}{d}\right)\mid 1\le b\le d,\ \mathrm{pgcd}(b,d)=1\}=\bigcup_{d|n}\mu_d^0, \tag{1.6.3.2}$$

où l'on a noté

$$\mu_d^0=\{\mathbf{e}\left(\tfrac{b}{d}\right)\mid 1\le b\le d,\ \mathrm{pgcd}(b,d)=1\}=\{\zeta\in\mu_d\mid(\forall j=1,\dots,d-1)\ \zeta^j\neq 1\}$$

l'ensemble des **racines primitives d-ièmes de l'unité**. Par exemple, on a

$$\mu_1^0=\{1\},\qquad \mu_2^0=\{-1\},\qquad \mu_3^0=\{\rho,\rho^2\},\qquad \mu_4^0=\{i,-i\},\qquad \mu_6^0=\{-\rho,-\rho^2\}, \tag{1.6.3.3}$$

où $\rho=e^{2\pi i/3}$. Observons que pour $n=1,2,3,4,6$, l'ensemble des racines du polynôme $\Phi_n(X)$ est égal à μ_n^0 ! La proposition suivante montre qu'il s'agit d'une propriété générale et que les factorisations dans (1.6.1.1) sont déterminées par les décompositions (1.6.3.2).

(1.6.4) Proposition. *Soit $n\ge 1$; posons*

$$\Phi_n(X)=\prod_{\zeta\in\mu_n^0}(X-\zeta)\in\mathbf{C}[X].$$

Les polynômes $\Phi_n(X)$ ont les propriétés suivantes:
(i) $\prod_{d|n}\Phi_d(X)=X^n-1$.
(ii) $\deg(\Phi_n)=\varphi(n)=n\prod_{p|n}\left(1-\frac{1}{p}\right)$ *(p premier).*
(iii) $\Phi_n(X)\in\mathbf{Z}[X]$.
(iv) *Si p est un nombre premier et $k\ge 1$ un entier, alors on a*

$$\Phi_p(X)=\frac{X^p-1}{X-1}=X^{p-1}+X^{p-2}+\cdots+1,\qquad \Phi_{p^k}(X)=\Phi_p(X^{p^{k-1}})=\frac{X^{p^k}-1}{X^{p^{k-1}}-1}.$$

(v) $\Phi_n(0)=1$ *(resp., $=-1$) si $n>1$ (resp., si $n=1$).*
(vi) *Si $n>1$, alors on a $X^{\deg(\Phi_n)}\Phi_n(1/X)=\Phi_n(X)$.*

Preuve. (i), (ii) Ceci résulte de (1.6.3.2). On en déduit (iii) par récurrence.
(iv) La première (resp., la deuxième) formule est une conséquence de (i) pour $n=p$ (resp., pour $n=p^k,p^{k-1}$).
(v) On a

$$\zeta\in\mu_n^0\implies\zeta^{-1}\in\mu_n^0, \tag{1.6.4.1}$$

d'où

$$\Phi_n(0) = \prod_{\substack{\zeta\in\mu_n^0\\ \zeta=\zeta^{-1}}} (-\zeta) \prod_{\substack{\zeta\in\mu_n^0\\ \zeta\neq\zeta^{-1}}} (-\zeta) = \prod_{\substack{\zeta\in\mu_n^0\\ \zeta=\zeta^{-1}}} (-\zeta) = \begin{cases} -1, & n=1 \\ 1, & n>1 \end{cases}$$

(car $(-\zeta)(-\zeta^{-1}) = 1$).
(vi) Ceci résulte de (v) et (1.6.4.1).

(1.6.5) Équations réciproques. La proposition 1.6.4(vi) affirme que le polynôme $\Phi_n(X)$ $(n > 1)$ est réciproque. Rappelons qu'un polynôme

$$f(X) = a_0X^n + a_1X^{n-1} + \cdots + a_n \qquad (a_j \in \mathbf{C},\ a_0 \neq 0)$$

est **réciproque** si

$$(\forall j)\ \ a_j = a_{n-j}\ \ \big(\iff\ \ f(x) = x^n f\left(\tfrac{1}{x}\right)\big).$$

Si c'est le cas, on a

$$f(\alpha) = 0 \iff f\left(\tfrac{1}{\alpha}\right) = 0 \qquad (\alpha \in \mathbf{C})$$

et l'on peut simplifier l'équation $f(X) = 0$ en introduisant une nouvelle variable $Y = X + X^{-1}$.

(1.6.6) Exemple : $\Phi_5 = 0$. L'équation

$$\Phi_5(X) = X^4 + X^3 + X^2 + X + 1 = 0 \tag{1.6.6.1}$$

s'écrit

$$(X^2 + X^{-2}) + (X + X^{-1}) + 1 = (Y^2 - 2) + Y + 1 = Y^2 + Y - 1 = 0 \tag{1.6.6.2}$$

(où $Y = X+X^{-1}$). Les racines de (1.6.6.1) (resp., de (1.6.6.2)) sont $X_a = \zeta_5^a$ (resp., $Y_b = \zeta_5^b+\zeta_5^{-b} = 2\cos\frac{2\pi b}{5}$) pour $a = 1, 2, 3, 4$ (resp., $b = 1, 2$). Il en résulte que

$$\{2\cos\tfrac{2\pi}{5}, 2\cos\tfrac{4\pi}{5}\} = \{\tfrac{-1\pm\sqrt{5}}{2}\};$$

les inégalités $\cos\frac{2\pi}{5} > 0 > \cos\frac{4\pi}{5}$ montrent alors que

$$\zeta_5 + \zeta_5^{-1} = 2\cos\tfrac{2\pi}{5} = \tfrac{\sqrt{5}-1}{2}, \qquad \zeta_5^2 + \zeta_5^{-2} = 2\cos\tfrac{4\pi}{5} = \tfrac{-\sqrt{5}-1}{2},$$

d'où

$$\zeta_5 - \zeta_5^2 - \zeta_5^3 + \zeta_5^4 = \sqrt{5}$$

et

$$\zeta_5^2 - \tfrac{\sqrt{5}-1}{2}\zeta_5 + 1 = 0, \quad \mathrm{Im}(\zeta_5) > 0 \quad\Longrightarrow\quad \zeta_5 = \tfrac{\sqrt{5}-1+i\sqrt{10+2\sqrt{5}}}{4}.$$

(1.6.7) Exemple : $\Phi_7 = 0$. La même méthode s'applique à l'équation

$$X^{-3}\Phi_7(X) = (X^3 + X^{-3}) + (X^2 + X^{-2}) + (X + X^{-1}) + 1 = 0. \tag{1.6.7.1}$$

D'après 1.6.9 ci-dessous, (1.6.7.1) s'écrit

$$(Y^3 - 3Y) + (Y^2 - 2) + Y + 1 = Y^3 + Y^2 - 2Y - 1 = 0 \tag{1.6.7.2}$$

(où $Y = X + X^{-1}$). On va chercher les racines $x_j = \zeta_7^j + \zeta_7^{-j} = 2\cos\frac{2\pi j}{7}$ $(j = 1, 2, 3)$ de l'équation cubique (1.6.7.2) par la méthode de 1.3.1: on considère les nombres

$$\begin{aligned} y_1 &= x_1 + \rho x_2 + \rho^2 x_3 = \zeta_7 + \rho^2\zeta_7^3 + \rho\zeta_7^2 + \zeta_7^6 + \rho^2\zeta_7^4 + \rho\zeta_7^5 \\ y_2 &= x_1 + \rho^2 x_2 + \rho x_3 = \zeta_7 + \rho\zeta_7^3 + \rho^2\zeta_7^2 + \zeta_7^6 + \rho\zeta_7^4 + \rho^2\zeta_7^5 \end{aligned} \tag{1.6.7.3}$$

(bien sûr, $x_1 + x_2 + x_3 = -\sigma_1 = -1$).

La suite des exposants dans (1.6.7.3) est engendrée par la multiplication successive par 3:

$$1 \mapsto 3 \mapsto 3\cdot 3 \equiv 2 \pmod 7 \mapsto 6 \mapsto 3\cdot 6 \equiv 4 \pmod 7 \mapsto 3\cdot 4 \equiv 5 \pmod 7,$$

donc

$$y_1 = \sum_{j=1}^{6} \rho^{2j}\zeta_7^{(3^j)} = \sum_{j=1}^{6} \rho^{2j}\sigma^j(\zeta_7), \qquad y_2 = \sum_{j=1}^{6} \rho^{j}\zeta_7^{(3^j)} = \sum_{j=1}^{6} \rho^{j}\sigma^j(\zeta_7), \tag{1.6.7.4}$$

où

$$\sigma : \mu_7 \longrightarrow \mu_7, \qquad \sigma(\zeta) = \zeta^3, \qquad\qquad (\zeta \in \mu_7)$$

engendre une permutation cyclique de μ_7^0:

$$\sigma : \zeta_7 \mapsto \zeta_7^3 \mapsto \zeta_7^2 \mapsto \zeta_7^6 \mapsto \zeta_7^4 \mapsto \zeta_7^5 \mapsto \zeta_7.$$

L'application σ fournit un exemple d'un élément du "groupe de Galois" de l'équation $\Phi_7(X) = 0$.

On déduit de (1.3.1.7-8) que

$$y_1y_2 = (-1)^2 - 3(-2) = 7, \qquad y_1^3 + y_2^3 = 2(-1)^3 - 9(-1)(-2) + 27 = 7 \implies (t - y_1^3)(t - y_2^3) = t^2 - 7t + 7^3,$$

donc

$$y_1^3, y_2^3 = 7\left(\tfrac{1\pm 3i\sqrt{3}}{2}\right) = 7(2+3\rho), 7(2+3\rho^2),$$

ce qui permet d'exprimer x_1, x_2, x_3 en fonction de $\sqrt[3]{7(2+3\rho)}$ et $\sqrt[3]{7(2+3\rho^2)}$.

On peut remplacer ρ, ρ^2 dans (1.6.7.4) par n'importe quel élément $\alpha \in \mu_6$: soit

$$u(\alpha) = \sum_{j=1}^{6} \alpha^j\zeta_7^{(3^j)} = \sum_{j=1}^{6} \alpha^j\sigma^j(\zeta_7), \qquad\qquad (\alpha \in \mu_6).$$

Par exemple, on a

$$\begin{aligned} u(1) &= \zeta_7 + \zeta_7^2 + \zeta_7^3 + \zeta_7^4 + \zeta_7^5 + \zeta_7^6 = -1 \\ u(-1) &= \zeta_7 + \zeta_7^2 + \zeta_7^4 - (\zeta_7^{-1} + \zeta_7^{-2} + \zeta_7^{-4}), \end{aligned}$$

donc

$$\begin{aligned} u(1)^2 &= (\zeta_7 + \zeta_7^2 + \zeta_7^4)^2 + (\zeta_7^{-1} + \zeta_7^{-2} + \zeta_7^{-4})^2 + 2(3 + u(1)) = 1 \\ u(-1)^2 &= (\zeta_7 + \zeta_7^2 + \zeta_7^4)^2 + (\zeta_7^{-1} + \zeta_7^{-2} + \zeta_7^{-4})^2 - 2(3 + u(1)) = u(1)^2 - 4(3 + u(1)) = -7. \end{aligned}$$

Le signe de $u(-1)$ est déterminé par l'inégalité

$$\mathrm{Im}(u(-1)) = 2\sin\tfrac{2\pi}{7} + 2\sin\tfrac{4\pi}{7} + 2\sin\tfrac{8\pi}{7} > 0,$$

d'où

$$\zeta_7 + \zeta_7^2 - \zeta_7^3 + \zeta_7^4 - \zeta_7^5 - \zeta_7^6 = i\sqrt{7}.$$

***(1.6.8) Question.** *On a calculé que*

$$\zeta_3 - \zeta_3^2 = i\sqrt{3}, \qquad \zeta_5 - \zeta_5^2 - \zeta_5^3 + \zeta_5^4 = \sqrt{5}, \qquad \zeta_7 + \zeta_7^2 - \zeta_7^3 + \zeta_7^4 - \zeta_7^5 - \zeta_7^6 = i\sqrt{7}.$$

Quelle est la règle générale?

(1.6.9) Exercice. *Montrer que, pour tout entier $n \geq 0$,*
(i) *Il existe un (unique) polynôme $P_n(y) \in \mathbf{Z}[y]$ tel que $x^n + x^{-n} = P_n(x + x^{-1})$. ($P_0 = 2$, $P_1 = y$, $P_2 = y^2 - 2$, $P_3 = y^3 - 3y, \ldots$).*
(ii) *Pour tout $\theta \in \mathbf{R}$, on a $P_n(2\cos\theta) = 2\cos(n\theta) \implies P_n(y) = 2T_n(y/2)$, où $T_n(x)$ est le n-ième polynôme de Čebyšev (= Tchebycheff = Chebyshev = ...).*

(1.7) Polynômes symétriques

(1.7.1) Groupe symétrique S_n (rappel). Une **permutation** de $\{1, \ldots, n\}$ est une application bijective $\sigma : \{1, \ldots, n\} \longrightarrow \{1, \ldots, n\}$. Les permutations de $\{1, \ldots, n\}$ forment un groupe S_n pour l'opération de composition $\sigma\tau = \sigma \circ \tau$, c'est-à-dire $(\sigma\tau)(i) = \sigma(\tau(i))$.

Le **signe** d'une permutation $\sigma \in S_n$ ($n \geq 2$) est défini par la formule

$$\mathrm{sgn}(\sigma) = (-1)^{|\{(i,j)\,|\,1 \leq i < j \leq n,\, \sigma(i) > \sigma(j)\}|}.$$

L'application

$$\mathrm{sgn} : S_n \longrightarrow \{\pm 1\}$$

est un homomorphisme de groupes, dont le noyau est le **groupe alterné** $A_n = \mathrm{Ker}(\mathrm{sgn}) \subset S_n$. On a $|S_n| = n!$, $|A_n| = n!/2$.

On écrit un élément $\sigma \in S_n$ soit sous la forme

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix},$$

soit comme un produit de cycles (= orbites sous l'action de σ). Par exemple, l'élément

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 5 & 3 & 6 & 2 & 1 \end{pmatrix} \in S_6$$

est le produit des cycles

$$1 \mapsto 4 \mapsto 6 \mapsto 1, \qquad 2 \mapsto 5 \mapsto 2, \qquad 3 \mapsto 3,$$

donc

$$\sigma = (146)(25)(3).$$

(1.7.2) Action de S_n sur les polynômes. Soit R un anneau (commutatif, unitaire). L'anneau $R[x_1, \ldots, x_n]$ de polynômes à n variables sur R admet une action naturelle de S_n (à gauche):

$$(\sigma \cdot f)(x_1, \ldots, x_n) = f(x_{\sigma(1)}, \ldots, x_{\sigma(n)}) \qquad (\sigma \in S_n,\, f \in R[x_1, \ldots, x_n]).$$

Si $R = K$ est un corps, la même formule définit l'action de S_n sur le corps des fonctions rationnelles

$$K(x_1, \ldots, x_n) = \{\tfrac{f}{g}\,|\,f, g \in K[x_1, \ldots, x_n],\, g \neq 0\}.$$

(1.7.3) Définition. *Un polynôme $f \in R[x_1, \ldots, x_n]$ (resp., une fonction rationnelle $f \in K(x_1, \ldots, x_n)$, si $R = K$ est un corps) est dit(e)* **symétrique** *si l'on a $(\forall \sigma \in S_n)\ \ \sigma \cdot f = f$. Les polynômes (resp.,*

les fonctions rationnelles) symétriques forment un anneau (resp., un corps) noté $R[x_1,\dots,x_n]^{S_n}$ *(resp.,* $K(x_1,\dots,x_n)^{S_n}$*).*

(1.7.4) Exemple : Les polynômes $x_1x_2x_3$, $x_1^7+x_2^7+x_3^7 \in R[x_1,x_2,x_3]$ sont symétriques, mais $x_1^2x_2+x_2^2x_3+x_3^2x_1$ ne l'est pas.

(1.7.5) Monômes symétrisés. Pour tout ensemble (ordoné) $I=(i_1,\dots,i_n)$ d'entiers $i_1\ge i_2\ge\cdots\ge i_n\ge 0$, on pose

$$s_I = s_{i_1,\dots,i_n} = \sum_{f\in A_I} f \in R[x_1,\dots,x_n]^{S_n}, \qquad \text{où} \qquad A_I = \{\sigma\cdot(x_1^{i_1}\cdots x_n^{i_n}) \,|\, \sigma\in S_n\}.$$

Afin de simplifier la notation, on va souvent omettre les valeurs $i_k=0$. Par exemple,

$$s_1=\sigma_1, \qquad s_{1,1}=\sigma_2, \qquad s_{1,1,1}=\sigma_3, \qquad \dots$$

sont les polynômes symétriques élémentaires (1.1.4) et

$$s_k = x_1^k+\cdots+x_n^k, \qquad s_{2,1}=x_1^2x_2+x_1x_2^2+x_1^2x_3+x_1x_3^2+\cdots+x_{n-1}^2x_n+x_{n-1}x_n^2.$$

Si $I=(i_1,\dots,i_n)$ et $J=(j_1,\dots,j_n)$ (où $i_1\ge i_2\ge\cdots\ge i_n\ge 0$, $j_1\ge j_2\ge\cdots\ge j_n\ge 0$), on définit

$$I+J=(i_1+j_1,\dots,i_n+j_n).$$

Si $I\ne J$, alors on dit que $I<J$ (resp., $I>J$) si l'on a $i_1=j_1,\dots,i_k=j_k$ et $i_{k+1}<j_{k+1}$ (resp., et $i_{k+1}>j_{k+1}$), $0\le k<n$.

(1.7.6) Exercice. (i) *Tout polynôme symétrique* $f\in R[x_1,\dots,x_n]^{S_n}$ *est une combinaison linéaire (finie)* $f=\sum c_Is_I$, $c_I\in R$.
(ii) *Pour tous* I,J, *on a*

$$s_Is_J = s_{I+J} + \sum_{K<I+J} c_Ks_K \qquad\qquad (c_K\in R).$$

[Ceci est une généralisation de (1.3.1.5) et (1.4.1.7).]

(1.7.7) Théorème. *On a* $R[\sigma_1,\dots,\sigma_n]=R[x_1,\dots,x_n]^{S_n}$*, et les éléments* $\sigma_1,\dots,\sigma_n$ *sont algébriquement indépendants sur* R*. Autrement dit, tout polynôme symétrique (sur* R*) s'écrit de manière unique comme un polynôme (sur* R*) en les variables* $\sigma_1,\dots,\sigma_n$*.*

Preuve. Existence: On généralise la preuve des formules (1.3.1.6) et (1.4.1.8). D'après 1.7.6(i), il suffit de montrer que $(\forall I)$ $s_I\in R[\sigma_1,\dots,\sigma_n]$. Comme $s_{0,\dots,0}=1$, on peut supposer que $I=(i_1=\cdots i_k>i_{k+1}\ge\cdots\ge i_n\ge 0$ $(1\le k\le n)$ et que l'on a déjà démontré que $s_K\in R[\sigma_1,\dots,\sigma_n]$ pour tout $K<I$. On écrit $I=I'+J$, où $I'=(1,\dots,1,0,\dots,0)$ (où 1 apparaît k-fois). Il résulte de 1.7.6(ii) que l'on a

$$s_I = \sigma_k s_J + \sum_{K<I} c_Ks_K \qquad\qquad (c_K\in R),$$

ce qui appartient à $R[\sigma_1,\dots,\sigma_n]$ par l'hypothèse de récurrence.
Unicité: Pour tout ensemble d'exposants $A=(a_1,\dots,a_n)$, $a_1,\dots,a_n\ge 0$, on a

$$\sigma^A := \sigma_1^{a_1}\cdots\sigma_n^{a_n} = s_I + \sum_{J<I} c_Js_J, \qquad I=I(A)=(a_1+\cdots+a_n, a_2+\cdots+a_n,\dots,a_n), \qquad (c_J\in R). \tag{1.7.7.1}$$

Soit

$$g(y_1,\dots,y_n)=\sum g_{a_1,\dots,a_n}y_1^{a_1}\cdots y_n^{a_n} = \sum_A g_A\, y^A$$

un polynôme non nul. L'ensemble $\{I(A)\,|\,g_A \neq 0\}$ admet un plus grand élément par rapport à l'ordre "<" (nécessairement unique!) $I = I(A)$ (pour une seule valeur de A, $g_A \neq 0$). Il résulte de (1.7.7.1) que $g(\sigma_1, \ldots, \sigma_n)$ contient le monôme $g_A s_I$, donc $g(\sigma_1, \ldots, \sigma_n) \neq 0$.

(1.7.8) Exemple : On va exprimer $s_{2,2} = x_1^2x_2^2 + x_1^2x_3^2 + \cdots + x_{n-1}^2x_n^2$ en fonction de $\sigma_1, \ldots, \sigma_n$. Comme

$$\sigma_2^2 = s_{1,1}^2 = (x_1x_2 + x_1x_3 + \cdots + x_{n-1}x_n)^2 = (x_1^2x_2^2 + \cdots) + 2(x_1^2x_2x_3 + \cdots) + 6(x_1x_2x_3x_4 + \cdots) =$$
$$= s_{2,2} + 2s_{2,1,1} + 6\sigma_4,$$
$$\sigma_1\sigma_3 = s_1s_{1,1,1} = (x_1 + \cdots + x_n)(x_1x_2x_3 + \cdots) = (x_1^2x_2x_3 + \cdots) + 4(x_1x_2x_3x_4 + \cdots) =$$
$$= s_{2,1,1} + 4\sigma_4,$$

on obtient

$$s_{2,1,1} = \sigma_1\sigma_3 - 4\sigma_4, \qquad s_{2,2} = \sigma_2^2 - 2\sigma_1\sigma_3 + 2\sigma_4.$$

(1.7.9) Corollaire. *Soit K un corps. Alors on a $K(\sigma_1, \ldots, \sigma_n) = K(x_1, \ldots, x_n)^{S_n}$.*

Preuve. Soient $f, g \in K[x_1, \ldots, x_n]$, $g \neq 0$, tels que $f/g \in K(x_1, \ldots, x_n)^{S_n}$. Si $g \in K[x_1, \ldots, x_n]^{S_n}$, alors on a $f \in K[x_1, \ldots, x_n]^{S_n}$ aussi, donc $f, g \in K[\sigma_1, \ldots, \sigma_n]$ d'après 1.7.7. Si $g \notin K[x_1, \ldots, x_n]^{S_n}$, alors le produit $\prod_{\sigma \in S_n}(\sigma \cdot g)$ est un polynôme symétrique et on se ramène au cas précedent à l'aide de la formule suivante :

$$\frac{f}{g} = \frac{f \prod_{\sigma \in S_n - \{e\}}(\sigma \cdot g)}{\prod_{\sigma \in S_n}(\sigma \cdot g)}.$$

(1.7.10) Proposition (Formules de Newton). *Pour tout entier $k \geq 1$, posons $s_k = x_1^k + \cdots + x_n^k$. Alors on a*

$$s_k - \sigma_1 s_{k-1} + \cdots + (-1)^{k-1}\sigma_{k-1}s_1 + (-1)^k k\sigma_k = 0 \qquad (k \geq 1)$$

(bien sûr, $\sigma_k = 0$ si $k > n$).

Preuve. On va travailler avec des séries formelles $\sum a_j t^j$ à coefficients $a_j \in \mathbf{Z}[x_1, \ldots, x_n]$. Posons

$$f(t) = (1 - x_1t) \cdots (1 - x_nt) = 1 - \sigma_1 t + \sigma_2 t^2 - \cdots + (-1)^n \sigma_n t^n;$$

on a

$$-t\,\frac{f'(t)}{f(t)} = \sum_{i=1}^{n} \frac{x_i t}{1 - x_i t} = \sum_{i=1}^{n} \sum_{k=1}^{\infty} t^k x_i^k = \sum_{k=1}^{\infty} s_k t^k,$$

d'où

$$(1 - \sigma_1 t + \sigma_2 t^2 - \cdots + (-1)^n \sigma_n t^n)(s_1 t + s_2 t^2 + \cdots) = \sigma_1 t - 2\sigma_2 t^2 + \cdots + (-1)^{n-1} n \sigma_n t^n.$$

On note que le coefficient de t^k dans le produit à gauche est égal à

$$s_k - \sigma_1 s_{k-1} + \cdots + (-1)^{k-1}\sigma_{k-1}s_1,$$

ce qui termine la démonstration.

(1.7.11) Discriminant. Soit $n \geq 2$. Le polynôme

$$\Delta := \prod_{i<j}(x_i - x_j) \in \mathbf{Z}[x_1, \ldots, x_n]$$

n'est pas symétrique, car

$$\Delta \cdot \sigma = \mathrm{sgn}(\sigma)\Delta \qquad (\sigma \in S_n),$$

mais

$$\Delta^2 = \prod_{i<j}(x_i - x_j)^2 \in \mathbf{Z}[x_1, \ldots, x_n]^{S_n} = \mathbf{Z}[\sigma_1, \ldots, \sigma_n]$$

l'est. En écrivant Δ^2 en fonction des coefficients $a_k = (-1)^k \sigma_k$ du polynôme

$$f = x^n + a_1 x^{n-1} + \cdots + a_n = (x - x_1) \cdots (x - x_n) \in \mathbf{Z}[a_1, \ldots, a_n][t],$$

on obtient le **discriminant** $\mathrm{disc}(f) \in \mathbf{Z}[a_1, \ldots, a_n]$ de f.

2. Extensions de corps – exemples et définitions

Dans la théorie algébrique des équations on considère souvent l'ensemble de tous les nombres "engendrés" par les racines d'une équation – ils forment *un corps*.

(2.1) Exemples

(2.1.1) Définition. *Un nombre complexe $\alpha \in \mathbf{C}$ est* **algébrique** *s'il existe un polynôme $f(X) \in \mathbf{Q}[X]-\{0\}$ tel que $f(\alpha)=0$; sinon, α est* **transcendant**.

(2.1.2) Exemples : (i) Pour tout entier $n \geq 1$ et $a \in \mathbf{Q}$, $\alpha = \sqrt[n]{a}$ est algébrique ($f(X) = X^n - a$).
(ii) $\alpha = \sqrt{2}+\sqrt{3}$ est algébrique (voir 2.1.7).
(iii) $\alpha = \sqrt{2}+\sqrt[3]{3}$ est algébrique (exercice: trouver $f(X)$ tel que $f(\alpha)=0$).
(iv) L'ensemble des nombres algébriques est dénombrable (exercice), donc la "majorité" des nombres complexes sont transcendants.

(2.1.3) Étant doné un nombre algébrique α, il est naturel de considérer tous les nombres qui s'expriment "rationnellement" en fonction de α. Voici un exemple :

(2.1.3.1) Exemple : Soit $\alpha = \sqrt{2}$. Posons

$$\mathbf{Q}[\sqrt{2}] = \{g(\sqrt{2}) \,|\, g \in \mathbf{Q}[X]\} \subset \mathbf{C},$$

ce qui est un sous-anneau de $\mathbf{C}$. Si

$$g(X) = a_0X^{2n} + a_1X^{2n-1} + \cdots + a_{2n} \qquad\qquad (a_i \in \mathbf{Q}),$$

alors on a

$$g(\sqrt{2}) = (2^n a_0 + 2^{n-1}a_2 + \cdots + a_{2n}) + (2^{n-1}a_1 + \cdots + a_{2n-1})\sqrt{2} = A + B\sqrt{2} \qquad (A, B \in \mathbf{Q}),$$

d'où

$$\mathbf{Q}[\sqrt{2}] = \{A + B\sqrt{2} \,|\, A, B \in \mathbf{Q}\}.$$

(2.1.3.2) Proposition. *$\mathbf{Q}[\sqrt{2}]$ est un corps.*

Preuve. Il faut démontrer que l'inverse $(A+B\sqrt{2})^{-1} \in \mathbf{C}$ de tout élément non nul $A+B\sqrt{2} \in \mathbf{Q}[\sqrt{2}]-\{0\}$ s'écrit aussi sous la forme $C+D\sqrt{2}$ ($C, D \in \mathbf{Q}$), ce qui résulte de la formule

$$\frac{1}{A+B\sqrt{2}} = \frac{A-B\sqrt{2}}{(A+B\sqrt{2})(A-B\sqrt{2})} = \frac{A-B\sqrt{2}}{A^2-2B^2} \in \mathbf{Q}[\sqrt{2}] \qquad (2.1.3.2.1)$$

(on a $A+B\sqrt{2} \neq 0 \iff (A,B) \neq (0,0) \iff A - B\sqrt{2} \neq 0$, car $\sqrt{2} \notin \mathbf{Q}$, d'après 1.3.5).

(2.1.4) Proposition-Définition. (i) *Soient $R \subset R'$ des anneaux et $\alpha_1, \ldots, \alpha_n \in R'$. Alors*

$$R[\alpha_1, \ldots, \alpha_n] := \{g(\alpha_1, \ldots, \alpha_n) \,|\, g = g(X_1, \ldots, X_n) \in R[X_1, \ldots, X_n]\} \subset R'$$

est le plus petit sous-anneau de R' contenant R et $\alpha_1, \ldots, \alpha_n$. On l'appelle le sous-anneau de R' engendré sur R par $\alpha_1, \ldots, \alpha_n$.
(ii) *Soient $K \subset K'$ des corps et $\alpha_1, \ldots, \alpha_n \in K'$. Alors*

$$K(\alpha_1, \ldots, \alpha_n) := \{\tfrac{g(\alpha_1,\ldots,\alpha_n)}{h(\alpha_1,\ldots,\alpha_n)} \,|\, g, h \in K[X_1, \ldots, X_n],\ h(\alpha_1, \ldots, \alpha_n) \neq 0\} \subset K'$$

est le plus petit sous-corps de K' contenant K et $\alpha_1, \ldots, \alpha_n$. On l'appelle le sous-corps de K' engendré sur K par $\alpha_1, \ldots, \alpha_n$.

Preuve. (i) L'ensemble $R[\alpha_1, \ldots, \alpha_n] \supset R$ est évidemment un anneau. Si $R \subset A \subset R'$ est un anneau contenant $\alpha_1, \ldots, \alpha_n$, alors on a $\alpha_1^{k_1} \cdots \alpha_n^{k_n} \in A$ (pour tous les entiers $k_1, \ldots, k_n \geq 0$), d'où $A \supset R[\alpha_1, \ldots, \alpha_n]$. On démontre (ii) de même manière.

(2.1.5) On peut reformuler 2.1.3.2 en disant que $\mathbf{Q}[\sqrt{2}] = \mathbf{Q}(\sqrt{2})$.

(2.1.6) Question. *Soit $\alpha \in \mathbf{C}$ une racine du polynôme $X^3 - 2$. Déterminer $\mathbf{Q}[\alpha]$. Est-ce qu'on a $\mathbf{Q}[\alpha] = \mathbf{Q}(\alpha)$ (c'est-à-dire $\mathbf{Q}[\sqrt[3]{2}] = \mathbf{Q}(\sqrt[3]{2})$) ?*

(2.1.7) Exemple : Comme en 2.1.3.1, on a

$$\mathbf{Q}[\sqrt{2}, \sqrt{3}] = \{A + B\sqrt{2} + C\sqrt{3} + D\sqrt{6} \mid A, B, C, D \in \mathbf{Q}\}.$$

Soit $\alpha = \sqrt{2} + \sqrt{3}$; on a $\alpha^{-1} = \sqrt{3} - \sqrt{2}$ et $\sqrt{2} = \frac{1}{2}(\alpha - \alpha^{-1})$, $\sqrt{3} = \frac{1}{2}(\alpha + \alpha^{-1})$. L'identité $(\alpha^2 - 5)^2 - 24 = 0$ montre que $\alpha^{-1} = 10\alpha - \alpha^3 \in \mathbf{Q}[\alpha]$, d'où

$$\mathbf{Q}[\sqrt{2}, \sqrt{3}] = \mathbf{Q}[\alpha, \alpha^{-1}] = \mathbf{Q}[\alpha].$$

On verra ci-dessous que $\mathbf{Q}[\alpha]$ est un corps, donc

$$\mathbf{Q}[\sqrt{2}, \sqrt{3}] = \mathbf{Q}[\alpha] = \mathbf{Q}(\alpha) = \mathbf{Q}(\sqrt{2}, \sqrt{3}).$$

(2.1.8) Lemme. $\sqrt{5} \notin \mathbf{Q}(\sqrt{2})$.

Preuve. Si $\sqrt{5} = A + B\sqrt{2}$ $(A, B \in \mathbf{Q})$, alors on a

$$5 = (A + B\sqrt{2})^2 = A^2 + 2B^2 + 2AB\sqrt{2} \in \mathbf{Q},$$

donc $AB = 0$ (car $\sqrt{2} \notin \mathbf{Q}$). Si $A = 0$ (resp., si $B = 0$), alors on obtient $\sqrt{10} = 2B \in \mathbf{Q}$ (resp., $\sqrt{5} = A \in \mathbf{Q}$), ce qui contredit 1.3.5.

(2.2) Représentations matricielles

(2.2.1) Exemple : La formule

$$\mathbf{C} \hookrightarrow M_2(\mathbf{R}), \qquad a + ib \mapsto \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \qquad (a, b \in \mathbf{R}) \tag{2.2.1.1}$$

fournit une "représentation" des nombres complexes par des matrices réelles d'ordre 2. Autrement dit, l'application (2.2.1.1) est compatible avec les opérations d'addition et de multiplication. Par exemple, on a

$$(a + bi)(c + di) = (ac - bd) + (ad + bc)i, \qquad \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \begin{pmatrix} c & -d \\ d & c \end{pmatrix} = \begin{pmatrix} ac - bd & -(ad + bc) \\ bc + ad & -bd + ac \end{pmatrix}.$$

En fait, la matrice (2.2.1.1) représent l'action de multiplication par $a + bi$ sur $\mathbf{C} = \mathbf{R} \cdot 1 + \mathbf{R} \cdot i$ dans la base $\{1, i\}$:

$$(a + bi) \cdot 1 = a \cdot 1 + b \cdot i, \qquad (a + bi) \cdot i = -b \cdot 1 + a \cdot i.$$

(2.2.2) Exemple : On sait que $L = \mathbf{Q}[\sqrt{2}] \subset \mathbf{C}$ est un espace vectoriel sur $\mathbf{Q}$ avec une base $\{1, \sqrt{2}\}$.

(2.2.2.1) Définition. *Pour $\beta = A + B\sqrt{2} \in L$, soit*

$$m_\beta : L \longrightarrow L, \qquad m_\beta(x) = \beta x$$

l'application "multiplication par β".

(2.2.2.2) L'application m_β et $\mathbf{Q}$-linéaire, $m_\beta \in \mathrm{End}_{\mathbf{Q}}(L)$. Dans la base $\{1, \sqrt{2}\}$, elle est donnée par les formules

$$m_\beta : \begin{array}{rcl} 1 \mapsto \beta & = & A \cdot 1 + B \cdot \sqrt{2} \\ \sqrt{2} \mapsto \beta\sqrt{2} & = & 2B \cdot 1 + A \cdot \sqrt{2}, \end{array}$$

donc elle est représentée par la matrice

$$M(\beta) = M(A + B\sqrt{2}) = \begin{pmatrix} A & 2B \\ B & A \end{pmatrix}$$

(comparer avec (2.2.1.1) !). Les matrices $M(\beta)$ ont les propriétés suivantes.

(2.2.2.3) Si $m_\alpha = m_\beta$, alors on a $\alpha = \beta$ (car $\alpha = m_\alpha(1)$). Dans le langage matriciel: si $M(\alpha) = M(\beta)$, alors on a $\alpha = \beta$.

(2.2.2.4) Soient $\alpha, \beta \in L$. Alors on a $(\alpha + \beta)x = \alpha x + \beta x,\ \alpha(\beta x) = (\alpha\beta)x$ pour tout $x \in L$, d'où

$$m_\alpha + m_\beta = m_{\alpha+\beta}, \qquad m_\alpha \circ m_\beta = m_{\alpha\beta}, \qquad M(\alpha) + M(\beta) = M(\alpha + \beta), \qquad M(\alpha)M(\beta) = M(\alpha\beta).$$

(2.2.2.5) Voici une preuve "abstraite" du fait que L est un corps : si $\beta \in L - \{0\}$, alors on a $\beta x \neq 0$ pour tout $x \in L - \{0\}$ (car il n'y a pas de diviseurs de zéro dans $\mathbf{C}$). Il en résulte que l'application $m_\beta : L \longrightarrow L$ est injective, donc surjective (puisque $\dim_{\mathbf{Q}}(L) < \infty$). En particulier, il existe $x \in L$ tel que $\beta x = 1$, donc $\beta^{-1} \in \mathbf{C}$ appartient bien à L.

(2.2.2.6) La propriété 2.2.2.4 permet de calculer l'inverse β^{-1} d'un élément $\beta = A + B\sqrt{2} \in L - \{0\}$: l'identité $M(\beta^{-1})M(\beta) = M(1) = I$ entraîne que

$$M(\beta^{-1}) = M(\beta)^{-1} = \begin{pmatrix} A & 2B \\ B & A \end{pmatrix}^{-1} = \frac{1}{A^2 - 2B^2} \begin{pmatrix} A & -2B \\ -B & A \end{pmatrix} = M\left(\frac{A - B\sqrt{2}}{A^2 - 2B^2}\right),$$

d'où la formule (2.1.3.2.1) (en utilisant (2.2.2.3)).

(2.2.2.7) L'elément $\beta = A + B\sqrt{2} \in L$ est une racine de léquation quadratique

$$(X - A)^2 - (B\sqrt{2})^2 = X^2 - 2AX + (A^2 - 2B^2) = 0.$$

On note que $2A = \mathrm{Tr}(M(\beta)), A^2 - 2B^2 = \det(M(\beta))$, donc

$$X^2 - 2AX + (A^2 - 2B^2) = \det(X \cdot I - M(\beta))$$

n'est rien d'autre que le polynôme caractéristique de la matrice $M(\beta)$.

(2.2.3) Exemple : Considérons $L = \mathbf{Q}[\sqrt[3]{2}] = \{A + B\sqrt[3]{2} + C\sqrt[3]{4} \mid A, B, C \in \mathbf{Q}\}$, où $\sqrt[3]{2} \in \mathbf{C}$ est une racine fixée du polynôme $f(X) = X^3 - 2$.

(2.2.3.1) On admet le fait que $1, \sqrt[3]{2}, \sqrt[3]{4}$ sont linéairement indépendants sur $\mathbf{Q}$ (voir 3.2.2 ci-dessous), donc forment une base de L comme $\mathbf{Q}$-espace vectoriel. Comme en 2.2.2.2, la multiplication par tout $\beta = A + B\sqrt[3]{2} + C\sqrt[3]{4} \in L$ définit une application $\mathbf{Q}$-linéaire $m_\beta : L \longrightarrow L$, $m_\beta(x) = \beta x$. Les formules

$$m_\beta(1) = \beta, \qquad m_\beta(\sqrt[3]{2}) = 2C \cdot 1 + A \cdot \sqrt[3]{2} + B \cdot \sqrt[3]{4}, \qquad m_\beta(\sqrt[3]{4}) = 2B \cdot 1 + 2C \cdot \sqrt[3]{2} + A \cdot \sqrt[3]{4}$$

montrent que la matrice de m_β dans la base $\{1, \sqrt[3]{2}, \sqrt[3]{4}\}$ de L est égale à

$$M(\beta) = \begin{pmatrix} A & 2C & 2B \\ B & A & 2C \\ C & B & A \end{pmatrix}.$$

La même méthode que plus haut montre que $M(\alpha)M(\beta) = M(\alpha\beta)$ et que L est un corps (donc $\mathbf{Q}[\sqrt[3]{2}] = \mathbf{Q}(\sqrt[3]{2})$).

(2.2.3.2) Calcul de β^{-1} ($\beta \in L - \{0\}$). On peut utiliser soit la formule $M(\beta^{-1}) = M(\beta)^{-1}$, soit la division euclidienne : par exemple, soit

$$\beta = 3 - 2\sqrt[3]{2} + \sqrt[3]{4} = g(\sqrt[3]{2}), \qquad g(X) = X^2 - 2X + 3.$$

On applique l'algorithme d'Euclide aux polynômes $f(X) = X^3 - 2$ et $g(X)$:

$$X^3 - 2 = (X^2 - 2X + 3)(X + 2) + (X - 8)$$
$$X^2 - 2X + 3 = (X - 8)(X + 6) + 51,$$

d'où

$$51 = (X^2 + 8X + 13)(X^2 - 2X + 3) - (X + 6)(X^3 - 2) = h(X)g(X) - (X + 6)f(X).$$

En substituant $X = \sqrt[3]{2}$, on obtient

$$\beta\, h(\sqrt[3]{2}) = g(\sqrt[3]{2})h(\sqrt[3]{2}) = 51 \implies \beta^{-1} = \frac{h(\sqrt[3]{2})}{51} = \frac{13 + 8\sqrt[3]{2} + \sqrt[3]{4}}{51}.$$

(2.2.3.3) On verra ci-dessous que β est une racine du polynôme caractéristique

$$\det(X \cdot I - M(\beta)) = X^3 - 3AX^2 + 3(A^2 - 2BC)X - (A^3 + 2B^3 + 4C^3 - 6ABC) \in \mathbf{Q}[X]$$

de la matrice $M(\beta)$.

(2.3) Corps – exemples

(2.3.1) Rappel. Un **corps** F est un anneau (commutatif, unitaire) tel que $F \neq 0$ et $F - \{0\} = F^*$, c'est-à-dire que tout élément non nul de F est inversible.

(2.3.2) Exemples des corps. $\mathbf{Q}, \mathbf{R}, \mathbf{C}, \mathbf{Q}(\sqrt{2}) = \{A + B\sqrt{2} \mid A, B \in \mathbf{Q}\}$, $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$ (si p est un nombre premier).

(2.3.3) Caractéristique d'un corps. Soit F un corps. Pour tout entier $n \geq 1$ on pose

$$n \cdot 1_F = \underbrace{1_F + \cdots + 1_F}_{n-\text{fois}}, \qquad (-n) \cdot 1_F = -(\underbrace{1_F + \cdots + 1_F}_{n-\text{fois}})$$

(où 1_F est l'unité de F). Il y a deux possibilitées:

(car $= 0$) $\quad (\forall n \geq 1) \quad n \cdot 1_F \neq 0$.

On dit que "**la caractéristique de F est égale à zéro**", $\mathrm{car}(F) = 0$. Dans ce cas, $\mathbf{Q}$ est un sous-corps de F par la formule

$$\frac{m}{n} \mapsto \frac{m \cdot 1_F}{n \cdot 1_F}, \qquad (m, n \in \mathbf{Z},\ n \geq 1).$$

(car $= p$) $\quad (\exists n \geq 1) \quad n \cdot 1_F = 0$.

Le plus petit entier $n \geq 1$ ayant cette propriété s'appelle **la caractéristique de** F, $\mathrm{car}(F) = n$.

Exercice: $\mathrm{car}(F) = p$ est un **nombre premier**.

Dans ce cas, $\mathbf{F}_p$ est un sous-corps de F par la formule

$$a \cdot 1_{\mathbf{F}_p} \mapsto a \cdot 1_F \qquad (a = 1, 2, \ldots, p).$$

(2.3.4) Exemple d'un corps ayant 4 éléments. On prends $F \supset \mathbf{F}_2$, $F = \{0, 1, \alpha, \alpha + 1\}$, où $1 + 1 = 0$ et $\alpha^2 = \alpha + 1$.

(2.4) Extensions de corps

(2.4.1) Définition. *Soient $K \subset L$ des corps. On dit que L/K est une* **extension de corps**. *L est naturellement un espace vectoriel sur K; une* **base de** *L/K (resp., le* **degré de** *L/K, noté $[L : K] \in \mathbf{N} \cup \{\infty\}$) est une base de L (resp., la dimension de L) comme K-espace vectoriel.*

(2.4.2) Exemples : (i) $[\mathbf{C} : \mathbf{R}] = 2$; $\{1, i\}$ (ou $\{2 - 3i, i + 17\}$) est une base de $\mathbf{C}/\mathbf{R}$.
(ii) $[\mathbf{Q}(\sqrt{2}) : \mathbf{Q}] = 2$; $\{1, \sqrt{2}\}$ (ou $\{4 - \sqrt{2}, 5\sqrt{2} + 7\}$) est une base de $\mathbf{Q}(\sqrt{2})/\mathbf{Q}$.

(2.4.3) Lemme (Multiplicativité des degrés). *Soient $K \subset L \subset M$ des corps et $\{\ell_i\}_{i \in I}$ (resp., $\{m_j\}_{j \in J}$) une base de L/K (resp., une base de M/L). Alors $S = \{\ell_i m_j\}_{(i,j) \in I \times J}$ est une base de M/K. En particulier,*

$$[M : K] = |I \times J| = |I| \cdot |J| = [L : K][M : L].$$

Preuve. L'ensemble S engendre M comme K-espace vectoriel, puisque tout $m \in M$ s'écrit comme

$$m = \sum_{j \in J} y_j m_j \qquad (y_j \in L)$$

et tout y_j s'écrit comme

$$y_j = \sum_{i \in I} x_{ij} \ell_i \qquad (x_{ij} \in K),$$

d'où

$$m = \sum_{i \in I} \sum_{j \in J} x_{ij} \ell_i m_j \qquad (x_{ij} \in K).$$

S est en ensemble libre (sur K), puisque si

$$\sum_{i \in I} \sum_{j \in J} x_{ij} \ell_i m_j = \sum_{j \in J} \left(\sum_{i \in I} x_{ij} \ell_i \right) m_j = 0 \qquad (x_{ij} \in K),$$

alors on a

$$(\forall j \in J) \qquad \sum_{i \in I} x_{ij} \ell_i = 0$$

(car les m_j sont linéairement indépendants sur L), donc $x_{ij} = 0$ pour tous i, j (car les ℓ_i sont linéairement indépendants sur K).

(2.4.4) Exemple : Si $K = \mathbf{Q}$, $L = \mathbf{Q}(\sqrt{2})$, $M = \mathbf{Q}(\sqrt{2}, \sqrt{5}) = L(\sqrt{5})$, alors on a $[L : K] = 2$. Grâce à 2.1.8, on sait que $\sqrt{5} \notin L$. Comme en 2.1.3, il en résulte que $\{1, \sqrt{5}\}$ est une base de M/L, donc $[M : L] = 2$ et $[\mathbf{Q}(\sqrt{2}, \sqrt{5}) : \mathbf{Q}] = 2 \cdot 2 = 4$.

(2.4.5) Définition. *Soit L/K une extension de corps.*
(i) *Un élément $\alpha \in L$ est* **algébrique sur** *K s'il existe un polynôme $f(X) \in K[X] - \{0\}$ tel que $f(\alpha) = 0$; sinon, α est* **transcendant sur** *K.*
(ii) *L'extension L/K est* **algébrique** *si tout élément $\alpha \in L$ est algébrique sur K.*
(iii) *L'extension L/K est* **de degré fini** *si $[L : K] < \infty$.*
(iv) *L'extension L/K est* **de type fini** *s'il existe un ensemble fini $\{\alpha_1, \ldots, \alpha_n\} \subset L$ tel que $L = K(\alpha_1, \ldots, \alpha_n)$.*

(2.4.6) Proposition. *Soit L/K une extension des corps de degré fini. Alors*
(i) *L/K est une extension de type fini.*
(ii) *L/K est une extension algébrique.*

Preuve. (i) L admet une base finie (comme K-espace vectoriel) $\alpha_1, \ldots, \alpha_n$; on a $L = K(\alpha_1, \ldots, \alpha_n)$.

(ii) Soit $n = [L : K] < \infty$. Pour tout $\alpha \in L$, les éléments $1, \alpha, \ldots, \alpha^n$ sont linéairement dépendants sur K, donc il existe une relation

$$a_0 \cdot 1 + a_1 \cdot \alpha + \cdots + a_n \cdot \alpha^n = 0 \qquad\qquad (a_i \in K,\ (\exists i_0)\ a_{i_0} \neq 0).$$

(2.4.7) En fait, on a démontré que tout élément de L est algébrique de degré $\leq [L : K]$ sur K.

(2.4.8) On va démontrer ci-dessous que toute extension algébrique de type fini est de degré fini.

(2.4.9) Si $\alpha \in L$ est transcendant sur K, alors les éléments $1, \alpha, \alpha^2, \ldots \in K[\alpha] \subset K(\alpha)$ sont linéairement indépendants sur K; il en résulte que $[K(\alpha) : K] = \infty$.

3. Extensions simples de corps

Une extension de corps L/K est **simple** si $L = K(\alpha)$ est engendré sur K par un seul élément.

(3.1) Le polynôme minimal

Soient $K \subset E$ des corps et $\alpha \in E$ un élément de E.

(3.1.1) Lemme-Définition. *Supposons que α est algébrique sur K. Alors:*
(i) *L'ensemble de polynômes*

$$\{g \in K[X] \,|\, g \neq 0,\, g(\alpha) = 0\}$$

étant non vide, il contient un polynôme unitaire f de degré minimum.
(ii) *Soit $g \in K[X]$. Alors*

$$g(\alpha) = 0 \iff f|g \ (\iff \exists h \in K[X] \quad fh = g).$$

(iii) *Le polynôme f en (i) est unique; on l'appelle* **le polynôme minimal de α sur K;** *on dit que* $\deg(f)$ *est* **le degré de α sur K.**
(iv) *Le polynôme f est irréductible sur K (= dans $K[X]$).*
(v) *Si $g \in K[X]$ est un polynôme unitaire et irréductible (sur K) tel que $g(\alpha) = 0$, alors on a $g = f$.*

(3.1.2) Exemples de polynômes minimaux : (i) Si $\alpha \in K$, alors on a $f(X) = X - \alpha$.
(ii) Si $K = \mathbf{R}$, $E = \mathbf{C}$ et $\alpha = i$, alors on a $f(X) = X^2 + 1$.
(iii) Si $K = \mathbf{Q}$, $E = \mathbf{C}$ et $\alpha = \sqrt{2}$ (ou $\alpha = -\sqrt{2}$), alors on a $f(X) = X^2 - 2$.
(iv) Si $K = \mathbf{Q}$, $E = \mathbf{C}$ et $\alpha \in \mathbf{C}$ est une racine du polynôme $g(X) = X^3 - 2$. On verra en 3.1.4 ci-dessous que $g(X)$ est irréductible dans $\mathbf{Q}[X]$, donc $f = g$ d'après 3.1.1(v).

Preuve de 3.1.1. Il n'y a rien à démontrer en (i).
(ii) On applique l'algorithme de division aux polynômes g et f: il existe $h, r \in K[X]$ tels que

$$g(X) = f(X)h(X) + r(X), \qquad (\deg(r) < \deg(f)).$$

En substituant $X = \alpha$ on obtient $r(\alpha) = 0$, d'où $r = 0$ grâce à la minimalité de $\deg(f)$.
(iii) Si $f_1 \in K[X]$ satisfait aux mêmes conditions que f, alors on a $f|f_1$ et $f_1|f$ d'après (ii), donc $f_1 = cf$ ($c \in K^*$). Les polynômes f et f_1 étant unitaires, on a $c = 1$.
(iv) Si $f = gh$ avec $g, h \in K[X] - \{0\}$ et $\deg(g), \deg(h) < \deg(f)$, alors on a soit $g(\alpha) = 0$, soit $h(\alpha) = 0$, ce qui contredit la minimalité de $\deg(f)$.
(v) On a $f|g$ d'après (ii). Il résulte de l'irréductibilité de g que $g = cf$ ($c \in K^*$); on conclut que $c = 1$ comme en (iii).

(3.1.3) Critères d'irréductibilité. (i) *Un polynôme $f \in K[X] - \{0\}$ est irréductible sur $K \iff f$ n'est divisible par aucun polynôme $g \in K[X] - K$ de degré $\deg(g) \leq \deg(f)/2$. En particulier, un polynôme cubique ($\deg(f) = 3$) est irréductible sur $K \iff f$ n'a pas de racine dans K.*
(ii) *Soit $f = a_0X^n + a_1X^{n-1} + \cdots + a_n \in \mathbf{Z}[X]$. On suppose qu'il existe un nombre premier p tel que $p \nmid a_0$ et que l'image de f dans $\mathbf{Z}/p\mathbf{Z}[X]$ soit irréductible. Alors $f = cf_1$, où $c = \mathrm{pgcd}(a_0, \ldots, a_n)$ et $f_1 \in \mathbf{Z}[X]$ est irréductible dans $\mathbf{Z}[X]$.*
(iii) *("Critère d'Eisenstein") Soit $f = X^n + a_1X^{n-1} + \cdots + a_n \in \mathbf{Z}[X]$. On suppose qu'il existe un nombre premier p tel que $(\forall i)$ $p|a_i$ et $p^2 \nmid a_n$ (on dit que f est un* **polynôme d'Eisenstein** *par rapport à p). Alors f est irréductible dans $\mathbf{Z}[X]$.*
(iv) *(Gauss) Si un polynôme $f \in \mathbf{Z}[X]$ est irréductible dans $\mathbf{Z}[X]$, alors f est irréductible dans $\mathbf{Q}[X]$.*

"Preuve". (i), (ii) Exercice. (iii), (iv) On va démontrer une version plus générale dans la deuxième partie du cours.

(3.1.4) Exemples : (i) Le polynôme $X^3 - 2$ est irréductible dans $\mathbf{Q}[X]$, car il n'a pas de racine dans $\mathbf{Q}$ (d'après 1.3.5).

(ii) $X^n - 2$ ($n \geq 1$) est un polynôme d'Eisenstein par rapport à 2, donc irréductible dans $\mathbf{Q}[X]$.
(iii) Si p est un nombre premier, alors

$$\Phi_p(X+1) = \frac{(X+1)^p - 1}{X} = X^{p-1} + \binom{p}{1} X^{p-2} + \cdots + \binom{p}{p-1}$$

est un polynôme d'Eisenstein par rapport à p, donc irréductible dans $\mathbf{Q}[X]$.

(3.1.5) Exercice. (i) *Soit $a \in \mathbf{Z}$, $3 \nmid a$. Montrer que le polynôme $X^3 - X + a$ est irréductible dans $\mathbf{Q}[X]$.*
(ii) *Soit p un nombre premier et $k \geq 1$ un entier. Montrer que $\Phi_{p^k}(X+1)$ est un polynôme d'Eisenstein par rapport à p, donc irréductible dans $\mathbf{Q}[X]$.*

(3.2) Extensions algébriques simples

Soient $K \subset E$ des corps et $\alpha \in E$.

(3.2.1) Proposition. *Soit α algébrique sur K; on note $f(X) = X^d + a_1 X^{d-1} + \cdots + a_d \in K[X]$ son polynôme minimal sur K ($d = \deg(f) \geq 1$). Alors*
(i) *Les éléments $1, \alpha, \ldots, \alpha^{d-1}$ forment une base de $K[\alpha]$ comme K-espace vectoriel.*
(ii) *L'anneau $K[\alpha]$ est un* **anneau intègre***:*

$$ab = 0 \implies a = 0 \text{ ou } b = 0 \qquad\qquad (a, b \in K[\alpha]).$$

(iii) *L'anneau $K[\alpha]$ est un corps, donc $K(\alpha) = K[\alpha]$.*
(iv) *Le degré de l'extension de corps $K(\alpha)/K$ est égal à $[K(\alpha) : K] = d = \deg(f)$. Plus précisement, les éléments $1, \alpha, \ldots, \alpha^{d-1}$ forment une base de $K(\alpha)/K$.*
(v) *Pour tout corps intermédiaire $K \subset L \subset E$, on a $[L(\alpha) : L] \leq [K(\alpha) : K]$.*

(3.2.2) Exemple : Soient $n \geq 1$ et $\alpha = \sqrt[n]{2} \in \mathbf{C}$ une racine fixée du polynôme $f(X) = X^n - 2$. Comme $f(X)$ est le polynôme minimal de $\sqrt[n]{2}$ sur $\mathbf{Q}$ (d'après 3.1.4(ii) et 3.1.1(v)), il en résulte que $1, \sqrt[n]{2}, \ldots, (\sqrt[n]{2})^{n-1}$ est une base de $\mathbf{Q}(\sqrt[n]{2})/\mathbf{Q}$ et $[\mathbf{Q}(\sqrt[n]{2}) : \mathbf{Q}] = n$.

Preuve de 3.2.1. (i) En multipliant l'identité

$$\alpha^d = -a_1 \alpha^{d-1} - \cdots - a_d$$

par α^i ($i \geq 0$), on montre par récurrence que

$$(\forall i \geq 0) \quad \alpha^{d+i} \in K \cdot 1 + \cdots + K \cdot \alpha^{d-1} = \{u_0 \cdot 1 + u_1 \cdot \alpha + \cdots + u_{d-1} \cdot \alpha^{d-1} \mid u_i \in K\},$$

d'où

$$K[\alpha] = K \cdot 1 + \cdots + K \cdot \alpha^{d-1}.$$

Les éléments $1, \alpha, \ldots, \alpha^{d-1}$ sont linéairement indépendants sur K: si

$$u_0 \cdot 1 + u_1 \cdot \alpha + \cdots + u_{d-1} \cdot \alpha^{d-1} = 0 \qquad\qquad (u_i \in K),$$

alors on a $u_0 = \cdots = u_{d-1} = 0$, d'après la minimalité de $\deg(f) = d$.
(ii) $K[\alpha] \subset E$ est un sous-anneau d'un corps.
(iii) L'argument de 2.2.2.5 s'applique: pour tout $\beta \in K[\alpha] - \{0\}$, l'application

$$m_\beta : K[\alpha] \longrightarrow K[\alpha], \qquad m_\beta(x) = \beta x$$

est K-linéaire et injective (d'après (ii)), donc surjective, car $\dim_K(K[\alpha]) = d < \infty$. En particulier, il existe $x \in K[\alpha]$ tel que $\beta x = 1$, d'où $\beta^{-1} = x \in K[\alpha]$.
(iv) Ceci résulte de (i) et (iii).

(v) Soit $f_L \in L[X]$ le polynôme minimal de α sur L. D'après 3.1.1(ii), f est divisible par f_L dans $L[X]$, donc

$$[L(\alpha) : L] = \deg(f_L) \leq \deg(f) = [K(\alpha) : K].$$

(3.2.3) Corollaire. *α est algébrique sur K $\iff$ $[K(\alpha) : K] < \infty$.*

(3.2.4) Proposition. (i) *Si le corps K est un sous-anneau d'un anneau intègre R ayant dimension finie comme K-espace vectoriel, alors R est un corps.*
(ii) *Si R est un anneau intègre ayant un nombre fini d'éléments, alors R est un corps.*

Preuve. (i) La méthode de 2.2.2.5 s'applique: pour tout $\beta \in R-\{0\}$, l'application $m_\beta : R \longrightarrow R$, $m_\beta(x) = \beta x$ est injective (l'anneau R étant intègre), donc surjective, puisque $\dim_K(R) < \infty$. Il en résulte qu'il existe $x \in R$ tel que $\beta x = m_\beta(x) = 1$, donc β admet un inverse dans R.
(ii) Exercice (la même méthode s'applique).

(3.2.5) Corollaire. *Si $\alpha, \beta \in E$ sont des éléments algébriques sur K, alors tout élément de $K[\alpha, \beta]$ (par exemple $\alpha \pm \beta, \alpha\beta$) est aussi algébrique sur K.*

Preuve. Soit $d \geq 1$ (resp., $e \geq 1$) le degré du polynôme minimal de α (resp., de β) sur K; alors on a

$$K[\alpha] = \{\sum_{i=0}^{d-1} a_i \alpha^i \,|\, a_i \in K\}, \qquad K[\beta] = \{\sum_{j=0}^{e-1} b_j \beta^j \,|\, b_j \in K\}.$$

Il en résulte que l'anneau $K[\alpha, \beta]$ est égal à

$$K[\alpha, \beta] = \{\sum_{i=0}^{d-1} \sum_{j=0}^{e-1} c_{ij} \alpha^i \beta^j \,|\, c_{ij} \in K\} \subset E,$$

donc $c = \dim_K K[\alpha, \beta] \leq de < \infty$. Pour tout $\gamma \in K[\alpha, \beta]$ les éléments $1, \gamma, \ldots, \gamma^c$ sont linéairement dépendants sur K, donc il existe une relation linéaire non triviale $u_0 + u_1\gamma + \cdots + u_c\gamma^c = 0$ ($u_i \in K$). Bien sûr, l'anneau $K[\alpha, \beta]$ est un corps (grâce à 3.2.4(i)), donc une extension de degré fini de K.

(3.2.6) Proposition. *Soient $\alpha_1, \ldots, \alpha_n \in E$ des éléments algébriques sur K; posons $d_i = [K(\alpha_i) : K]$.*
(i) $K(\alpha_1, \ldots, \alpha_n) = K[\alpha_1, \ldots, \alpha_n]$, $[K(\alpha_1, \ldots, \alpha_n) : K] \leq d_1 d_2 \cdots d_n$
(en particulier, l'extension de corps $K(\alpha_1, \ldots, \alpha_n)/K$ est algébrique).
(ii) *Si* $\operatorname{pgcd}(d_1, d_2) = 1$, *alors on a $K(\alpha_1) \cap K(\alpha_2) = K$ et $[K(\alpha_1, \alpha_2) : K] = d_1 d_2$.*

Preuve. (i) Considérons la tour d'extensions

$$K = K_0 \subset K_1 \subset \cdots \subset K_{i-1} \subset K_i = K_{i-1}(\alpha_i) \subset \cdots \subset K_n = K(\alpha_1, \ldots, \alpha_n).$$

On vient de voir en 3.2.1(v) que tout élément α_i ($1 \leq i \leq n$) est algébrique sur $K_{i-1} = K(\alpha_1, \ldots, \alpha_{i-1})$, de degré $\leq [K(\alpha_i) : K] = d_i$. En appliquant 3.2.1(iii), on obtient $K_i = K_{i-1}[\alpha_i]$, d'où $K_n = K[\alpha_1, \ldots, \alpha_n]$ par récurrence et

$$[K_n : K_0] = \prod_{i=1}^{n} [K_i : K_{i-1}] = \prod_{i=1}^{n} [K_{i-1}(\alpha_i) : K_{i-1}] \leq \prod_{i=1}^{n} [K(\alpha_i) : K] = \prod_{i=1}^{n} d_i < \infty.$$

(ii) Considérons les corps

$$K \subset E = K(\alpha_1) \cap K(\alpha_2) \subset K(\alpha_i) \subset F = K(\alpha_1, \alpha_2) \qquad (i = 1, 2).$$

D'après 2.4.3, on a les divisibilités suivantes:

$$[E : K] \big| d_1,\ [E : K] \big| d_2 \Longrightarrow [E : K] \big| \operatorname{pgcd}(d_1, d_2) = 1 \Longrightarrow [E : K] = 1 \Longrightarrow E = K$$
$$d_1 \big| [F : K],\ d_2 \big| [F : K] \Longrightarrow d_1 d_2 = \operatorname{ppcm}(d_1, d_2) \big| [F : K].$$

D'autre part,

$$[F : K(\alpha_2)] = [K(\alpha_2)(\alpha_1) : K(\alpha_2)] \leq [K(\alpha_1) : K] = d_1$$

(d'après 3.2.1(v)), d'où

$$[F : K] = [F : K(\alpha_2)] \cdot [K(\alpha_2) : K] \leq d_1 d_2.$$

Il en résulte que $[F : K] = d_1 d_2$.

(3.2.7) Exemple : (i) Soient $\alpha_1, \alpha_2, \alpha_3 \in \mathbf{C}$ les racines complexes du polynôme $X^3 - 2$ (par exemple, on prend $\alpha_1 \in \mathbf{R}$, $\alpha_2 = \rho\alpha_1$, $\alpha_3 = \rho^2\alpha_1$). Alors on a $\mathbf{Q} \subset \mathbf{Q}(\alpha_1) \subset \mathbf{Q}(\alpha_1, \alpha_2, \alpha_3) = \mathbf{Q}(\alpha_1, \rho)$, où $[\mathbf{Q}(\alpha_1) : \mathbf{Q}] = 3$ (d'après 3.2.2) et $[\mathbf{Q}(\alpha_1, \rho) : \mathbf{Q}(\alpha_1)] = 2$ (ce degré est ≤ 2, car $\rho^2 + \rho + 1 = 0$; d'autre part, il est > 1, puisque $\rho \notin \mathbf{R} \Longrightarrow \rho \notin \mathbf{Q}(\alpha_1)$). Il en résulte que $[\mathbf{Q}(\alpha_1, \alpha_2, \alpha_3) : \mathbf{Q}] = 3 \cdot 2 = 6$ (on pourrait également appliquer 3.2.6(ii), puisque $\mathrm{pgcd}([\mathbf{Q}(\alpha_1) : \mathbf{Q}], [\mathbf{Q}(\rho) : \mathbf{Q}]) = \mathrm{pgcd}(3, 2) = 1$).
(ii) On a $\mathbf{Q}(\alpha_1) \cap \mathbf{Q}(\alpha_2) = \mathbf{Q}(\alpha_1) \cap \mathbf{Q}(\rho) = \mathbf{Q}$, mais

$$[\mathbf{Q}(\alpha_1) : \mathbf{Q}] = [\mathbf{Q}(\alpha_2) : \mathbf{Q}] = 3, \qquad [\mathbf{Q}(\alpha_1, \alpha_2) : \mathbf{Q}] = 6 \neq 3 \cdot 3.$$

(3.2.8) Exercice. *Soit K un sous-corps de $\mathbf{C}$ et $a, b \in K^*$. Montrer:*
(i) $K(\sqrt{a})^{*2} \cap K^* = K^{*2} \cup aK^{*2}$.
(ii) $K(\sqrt{a}) = K(\sqrt{b}) \iff a/b \notin K^{*2}$.
(iii) $K(\sqrt{a}, \sqrt{b})^{*2} \cap K^* = K^{*2} \cup aK^{*2} \cup bK^{*2} \cup abK^{*2}$.
(iv) $[K(\sqrt{a}, \sqrt{b}) : K] = 4 \iff a, b, ab \notin K^{*2}$. *Si c'est le cas, alors $1, \sqrt{a}, \sqrt{b}, \sqrt{ab}$ est une base de $K(\sqrt{a}, \sqrt{b})/K$.*
(v) *Si L/K est une extension de corps de degré 2 ($L \subset \mathbf{C}$), alors il existe $c \in K^*$, $c \notin K^{*2}$ tel que $L = K(\sqrt{c})$.*
(vi) *Les corps $L = K, K(\sqrt{a}), K(\sqrt{b}), K(\sqrt{ab}), K(\sqrt{a}, \sqrt{b})$ sont les seuls corps intermédiaires $K \subseteq L \subseteq K(\sqrt{a}, \sqrt{b})$.*

(3.2.9) Représentation matricielle. Soit L/K une extension de corps de degré fini $n = [L : K]$. Fixons une base $\omega_1, \ldots, \omega_n$ de L/K. Pout tout $\beta \in L$, on note $M(\beta) \in M_n(K)$ la matrice de l'application $m_\beta : L \longrightarrow L$ ($m_\beta(x) = \beta x$) dans la base $\{\omega_i\}$. Comme en 2.2.2, les matrices $M(\beta)$ ont les propriétés suivantes:

(3.2.9.1) $(\forall \beta \in K) \quad m_\beta = \beta \cdot \mathrm{id}, \qquad M(\beta) = \beta \cdot I.$
(3.2.9.2) $(\forall \alpha, \beta \in L) \quad m_\alpha + m_\beta = m_{\alpha+\beta}, \qquad m_\alpha \circ m_\beta = m_{\alpha\beta}, \qquad M(\alpha) + M(\beta) = M(\alpha+\beta), \qquad M(\alpha)M(\beta) = M(\alpha\beta).$
(3.2.9.3) $(\forall \alpha, \beta \in L) \quad \alpha = \beta \iff m_\alpha = m_\beta \iff M(\alpha) = M(\beta).$

Autrement dit, l'application $\beta \mapsto m_\beta$ (resp., $\beta \mapsto M(\beta)$) est un homomorphisme injectif d'anneaux (plus précisement, un homomorphisme injectif de K-algèbres)

$$m : L \hookrightarrow \mathrm{End}_K(L) \qquad \text{(resp., } M : L \hookrightarrow M_n(K)\text{)}.$$

(3.2.10) Proposition. *Sous les hypothèses de 3.2.9, soit $\beta \in L$. Le polynôme caractéristique*

$$P_\beta(X) = P_{\beta, L/K}(X) = \det(X \cdot I - M(\beta)) \in K[X]$$

de la matrice $M(\beta)$ ne dépend pas de la base $\{\omega_i\}$, et l'on a $P_\beta(\beta) = 0$.
[Ceci est une généralisation de 2.2.2.7.]

Preuve. Un changement de base de L/K est donné par une matrice inversible $g \in GL_n(K)$; dans la nouvelle base, l'application m_β est représentée par la matrice $gM(\beta)g^{-1}$, dont le polynôme caractéristique est égal à cel de $M(\beta)$. On a

$$\begin{aligned} 0 &= P_\beta(M(\beta)) && \text{(Thm de Cayley} - \text{Hamilton)} \\ &= M(P_\beta(\beta)) && \text{(d'après (3.2.9.2))}, \end{aligned}$$

d'où $P_\beta(\beta) = 0$ (d'après (3.2.9.3)).

(3.2.11) Exemples : (i) Si $\beta \in K$, alors on a $P_\beta(X) = (X-\beta)^n = (X-\beta)^{[L:K]}$.
(ii) Si $L = K(\sqrt{d})$, où $d \in K^*$, $d \notin K^{*2}$; alors on a $[L:K] = 2$. On calcule la matrice $M(\beta) = M(A+B\sqrt{d})$ $(A, B \in K)$ dans la base $1, \sqrt{d}$ de L/K comme en 2.2.2.2: on obtient

$$M(A+B\sqrt{d}) = \begin{pmatrix} A & dB \\ B & A \end{pmatrix},$$

donc $P_\beta(X) = X^2 - 2AX + (A^2 - dB^2)$ (cf. 2.2.2.7).
(iii) Si $L/K = \mathbf{Q}(\sqrt[4]{2})/\mathbf{Q}$ et $\beta = \sqrt{2} = (\sqrt[4]{2})^2$, alors la matrice $M(\beta)$ dans la base $1, (\sqrt[4]{2})^2, \sqrt[4]{2}, (\sqrt[4]{2})^3$ de L/K est égale à

$$M(\sqrt{2}) = \begin{pmatrix} 0 & 2 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

donc $P_{\sqrt{2}}(X) = \det(X \cdot I - M(\sqrt{2})) = (X^2-2)^2 = X^4 - 4X^2 + 4$. Ici, $X^2 - 2$ est le polynôme minimal de $\beta = \sqrt{2}$ sur $K = \mathbf{Q}$.
(iv) En général, soit

$$g(X) = X^d + a_1 X^{d-1} + \cdots + a_d \qquad (a_i \in K)$$

le polynôme minimal de β sur K. Fixons une base $\omega_1, \ldots, \omega_e$ de $L/K(\beta)$; alors $\beta^i \omega_j$ $(0 \le i \le d-1, 1 \le j \le e)$ est une base de L/K. La matrice $M(\beta)$ dans cette base est égale à

$$\begin{pmatrix} A & 0 & \ldots & 0 \\ 0 & A & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & A \end{pmatrix}$$

Ici on l'a noté

$$A = \begin{pmatrix} 0 & 0 & \ldots & 0 & -a_d \\ 1 & 0 & \ldots & 0 & -a_{d-1} \\ 0 & 1 & \ldots & 0 & -a_{d-2} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & 1 & -a_1 \end{pmatrix}$$

Comme $\det(X \cdot I - A) = g(X)$, on a

$$P_\beta(X) = \det(X \cdot I - A)^e = g(X)^{[L:K(\beta)]}.$$

En particulier, si $L = K(\beta)$, alors on a $P_\beta(X) = g(X)$.

(3.2.12) Exercice. *Soient $L/K = \mathbf{Q}(\sqrt[3]{3})/\mathbf{Q}$ et $\beta = A + B\sqrt[3]{3} + C\sqrt[3]{9} \in L$ $(A, B, C \in \mathbf{Q})$. Déterminer $P_\beta(X)$ et le polynôme minimal de β sur $\mathbf{Q}$.*

(3.2.13) Définition (Norme, Trace). *Sous les hypothèses de 3.2.9, la* **norme** *(resp.,* **la trace***) de β dans l'extension L/K est définie comme*

$$N_{L/K}(\beta) = \det(M(\beta)), \qquad Tr_{L/K}(\beta) = Tr(M(\beta)).$$

(3.2.14) Exemples : (i) Si $\beta \in K$, alors on a $N_{L/K}(\beta) = \beta^{[L:K]}$, $Tr_{L/K}(\beta) = [L:K] \cdot \beta$.
(ii) Soient $L = K(\sqrt{d})$ et $\beta = A + B\sqrt{d}$ comme en 3.2.11(ii); alors on a

$$N_{L/K}(A + B\sqrt{d}) = A^2 - dB^2 = (A + B\sqrt{d})(A - B\sqrt{d})$$
$$Tr_{L/K}(A + B\sqrt{d}) = 2A = (A + B\sqrt{d}) + (A - B\sqrt{d}).$$

(iii) Soient $K = \mathbf{Q}$, $L = \mathbf{Q}(\sqrt[3]{2})$ et $\beta = A + B\sqrt[3]{2} + C\sqrt[3]{4}$ $(A, B, C \in \mathbf{Q})$. On déduit de 2.2.3.1 que

$$N_{L/K}(\beta) = A^3 + 2B^3 + 4C^3 - 6ABC, \qquad Tr_{L/K}(\beta) = 3A.$$

(3.2.15) Exercice. *Sous les hypothèses de 3.2.9,*
(i) $(\forall \alpha, \beta \in L)$ $\quad Tr_{L/K}(\alpha + \beta) = Tr_{L/K}(\alpha) + Tr_{L/K}(\beta), \quad N_{L/K}(\alpha\beta) = N_{L/K}(\alpha)N_{L/K}(\beta)$.
Autrement dit, la norme (resp., la trace) définit un homomorphisme de groupes $N_{L/K} : L^* \longrightarrow K^*$ (resp., $Tr_{L/K} : L \longrightarrow K$).
(ii) $(\forall \alpha \in K,\, \beta \in L)$ $\quad Tr_{L/K}(\alpha\beta) = \alpha Tr_{L/K}(\beta), \quad N_{L/K}(\alpha\beta) = \alpha^{[L:K]} N_{L/K}(\beta)$.
(iii) *Si M/L est une extension de degré fini, alors on a:*
$(\forall \gamma \in M)$ $\quad N_{L/K}(N_{M/L}(\gamma)) = N_{M/K}(\gamma), \quad Tr_{L/K}(Tr_{M/L}(\gamma)) = Tr_{M/K}(\gamma)$.

(3.3) Rappel : Homomorphismes d'anneaux et idéaux

Tous les anneaux seront commutatifs et unitaires.

(3.3.1) Soient R, R' des anneaux. Une application $f : R \longrightarrow R'$ est un **homomorphisme d'anneaux** si l'on a

$$(\forall x, y \in R) \qquad f(x + y) = f(x) + f(y), \qquad f(xy) = f(x)f(y), \qquad f(1) = 1$$

$(\Longrightarrow f(0) = 0)$. Les ensembles

$$\mathrm{Ker}(f) = \{x \in R \,|\, f(x) = 0\}, \qquad \mathrm{Im}(f) = \{f(x) \,|\, x \in R\}$$

s'appellent **le noyau** (resp., **l'image**) de f. L'homomorphisme f est injectif $\iff$ $\mathrm{Ker}(f) = 0$.

(3.3.2) Lemme-Définition. *Un sous-ensemble I d'un anneau R est égal au noyau d'un homomorphisme d'anneaux $f : R \longrightarrow R'$ $\iff$ I a les propriétés suivantes:*
(i) $I \neq \emptyset$, $(\forall x, y \in I)$ $x - y \in I$ $\quad (\iff$ $(I, +)$ *est un sous-groupe de* $(R, +))$.
(ii) $x \in I, r \in R \Longrightarrow rx \in I$.
Un sous-ensemble de R ayant ces propriétés s'appelle **un idéal** *de R.*

Preuve. L'ensemble $\mathrm{Ker}(f)$ est non vide (car $0 \in \mathrm{Ker}(f)$) et l'on a

$$(\forall x, y \in \mathrm{Ker}(f))\ (\forall r \in R) \quad f(x - y) = f(x) - f(y) = 0, \quad f(rx) = f(r)f(x) = 0,$$

donc $\mathrm{Ker}(f)$ est un idéal de R. Réciproquement, étant donné un idéal I de R, soit R/I l'ensemble quotient de R par rapport à l'équivalence suivante:

$$x \equiv y \ (\mathrm{mod}\, I) \iff x - y \in I$$

(R/I est une généralisation naturelle de $\mathbf{Z}/n\mathbf{Z}$). Les propriétés (i), (ii) entraînent que

$$\left\{ \begin{array}{l} x \equiv y \ (\mathrm{mod}\, I) \\ x' \equiv y' \ (\mathrm{mod}\, I) \end{array} \right\} \Longrightarrow \left\{ \begin{array}{l} x + x' \equiv y + y' \ (\mathrm{mod}\, I) \\ xx' \equiv yy' \ (\mathrm{mod}\, I) \end{array} \right\}$$

(par exemple, $xx' - yy' = x(y - y') + (x - x')y' \in I$). Il en résulte que l'ensemble R/I, muni des opérations $\overline{x} + \overline{y} = \overline{x + y}$, $\overline{x} \cdot \overline{y} = \overline{xy}$ (où l'on a noté $\overline{x} \in R/I$ la classe d'équivalence de $x \in R$) est un anneau. L'application naturelle $\pi(x) = \overline{x}$ est un homomorphisme d'anneaux $\pi : R \longrightarrow R/I$ (surjectif) et $\mathrm{Ker}(\pi) = I$.

(3.3.3) Exemples : (i) L'idéal **principal** engendré par $a \in R$ est défini comme

$$(a) = \{ar \,|\, r \in R\}\,.$$

Par exemple, $0 = (0) = \{0\}$ et $(1) = R$. Si R est un anneau intègre (voir 3.2.1(ii)), alors on a

$$(a) = (b) \quad \Longleftrightarrow \quad (\exists u \in R^*) \quad a = bu \qquad\qquad (a, b \in R - \{0\}).$$

Ici, on a noté $R^* = \{u \in R \,|\, (\exists v \in R)\ uv = 1\}$ l'ensemble d'éléments inversibles de R.
(ii) Étant donnés $a_1, \ldots, a_n \in R$, le plus petit idéal de R contenant $a_1, \ldots, a_n \in R$ est égal à

$$(a_1, \ldots, a_n) = \{a_1 r_1 + \cdots + a_n r_n \,|\, r_1 \ldots, r_n \in R\}\,.$$

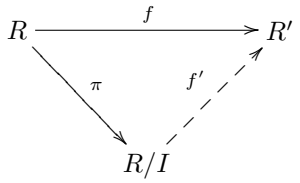
(3.3.4) Définition. *Un* **anneau principal** *(en anglais "principal ideal domain", ou "PID") est un anneau intègre dont tous les idéaux sont principaux.*

(3.3.5) Lemma. *Les anneaux* $\mathbf{Z}$ *et* $K[X]$ *(où* K *est un corps) sont principaux.*

Preuve. Il suffit de montrer que tout idéal non nul $I \neq (0)$ est principal. L'ensemble $I - \{0\}$ contient un élément b avec $|b|$ (resp., $\deg(b)$) minimal. On a $(b) \subseteq I$; il faut démontrer que $I \subseteq (b)$. Pour tout $a \in I$, la division euclidienne montre que l'on a $a = bq + r$, où $|r| < |b|$ (resp., $\deg(r) < \deg(b)$). Il résulte de la propriété minimale de b que l'élément $r = a - bq \in I$ est égal à $r = 0$, d'où $a = bq \in (b)$.

(3.3.6) La propriété universelle de R/I. Soit $I \subset R$ un idéal. On peut caractériser l'homomorphisme canonique $\pi : R \longrightarrow R/I$ $(\pi(x) = \overline{x})$ par la propriété universelle suivante:

> Pour tout homomorphisme d'anneaux $f : R \longrightarrow R'$ avec $I \subseteq \mathrm{Ker}(f)$ il existe un unique homomorphisme d'anneaux $\overline{f} : R/I \longrightarrow R'$ tel que $f = \overline{f} \circ \pi$ ($\Longleftrightarrow$ $(\forall x \in R)\ f(x) = \overline{f}(\overline{x})$), autrement dit tel que le diagramme suivant soit commutatif :



(3.3.7) Un **isomorphisme** d'anneaux $f : R \longrightarrow R'$ est un homomorphisme d'anneaux pour lequel il existe un homomorphisme d'anneaux $g : R' \longrightarrow R$ tel que $g \circ f = \mathrm{id}_R$, $f \circ g = \mathrm{id}_{R'}$ ($\Longleftrightarrow$ f est un homomorphisme d'anneaux **bijectif**).

(3.3.8) Théorème d'Isomorphisme. *Pour tout homomorphisme d'anneaux* $f : R \longrightarrow R'$*, l'homomorphisme induit*

$$\overline{f} : R/\mathrm{Ker}(f) \longrightarrow \mathrm{Im}(f), \qquad \overline{f}(\overline{x}) = f(x)$$

(défini par la propriété universelle 3.3.6) est un isomorphisme.

(3.4) Extensions simples – version algébrique

Soient $K \subset E$ des corps.

(3.4.1) Fixons $\alpha \in E$. L'application

$$\mathrm{ev}_\alpha : K[X] \longrightarrow E, \qquad g(X) \mapsto g(\alpha)$$

("l'évaluation en α") est un homomorphisme d'anneaux dont l'image est égale à $\mathrm{Im}(\mathrm{ev}_\alpha) = K[\alpha]$. Si α est transcendant sur K, alors on a $\mathrm{Ker}(\mathrm{ev}_\alpha) = 0$ et ev_α induit un isomorphisme d'anneaux $K[X] \xrightarrow{\sim} K[\alpha]$.

Si α est algébrique sur K, alors $I = \mathrm{Ker}(\mathrm{ev}_\alpha)$ est un idéal $I \neq (0), (1)$ de $K[X]$, donc $I = (f)$ pour un (unique) polynôme unitaire $f \in K[X]$ de degré $\deg(f) \geq 1$. D'après 3.3.8, l'application ev_α induit un isomorphisme d'anneaux

$$\overline{\mathrm{ev}_\alpha} : K[X]/(f) \xrightarrow{\sim} K[\alpha], \qquad \overline{g(X)} \mapsto g(\alpha),$$

où l'on a noté $\overline{g(X)}$ l'image de $g(X) \in K[X]$ dans $K[X]/(f)$. On sait, bien sûr, que $K[\alpha] = K(\alpha)$, ce qui résulte aussi de 3.4.3(iii) ci-dessous.

Ceci fournit une démonstration abstraite de 3.1.1(i)-(iii); en particulier, f est le polynôme minimal de α sur K.

(3.4.2) Exemple : Si $K = \mathbf{R}$, $E = \mathbf{C}$ et $\alpha = i$, alors ev_i induit un isomorphisme d'anneaux

$$\overline{\mathrm{ev}_i} : \mathbf{R}[X]/(X^2+1) \xrightarrow{\sim} \mathbf{R}[i] = \mathbf{R}(i) = \mathbf{C}, \qquad \overline{g(X)} \mapsto g(i).$$

(3.4.3) Lemme. *Soit $f \in K[X]$, $d = \deg(f) \geq 1$; posons $R = K[X]/(f)$. Alors on a :*
(i) *$f(\overline{X}) = 0$ et les éléments $1, \overline{X}, \ldots, \overline{X}^{d-1}$ forment une base de R comme K-espace vectoriel.*
(ii) *Si f est réductible sur K, alors R n'est pas un anneau intègre.*
(iii) *Si f est irréductible sur K, alors R est un corps.*

Preuve. (i) On a $f(\overline{X}) = \overline{f(X)} = 0$. Tout polynôme $g \in K[X]$ s'écrit de manière unique sous la forme

$$g = af + b, \qquad a, b \in K[X], \qquad \deg(b) < d$$

($\Longrightarrow \overline{g} = \overline{b}$). Il en résulte que l'application $b \mapsto \overline{b}$ induit une bijection K-linéaire

$$K \cdot 1 + K \cdot X \cdots + K \cdot X^{d-1} = \{b \,|\, b \in K[X],\ \deg(b) < d\} \xrightarrow{\sim} \{\overline{b} \,|\, b \in K[X],\ \deg(b) < d\} = R.$$

(ii) Si $f = gh$ avec $g, h \in K[X]$, $\deg(g), \deg(h) < d$, alors on a $\overline{g}, \overline{h} \neq 0$ mais $\overline{g}\,\overline{h} = \overline{f} = 0$ dans R.
(iii) Soit $r \in R - \{0\}$; on a $r = \overline{g}$, où $g \in K[X] - \{0\}$, $\deg(g) < d$. D'après 3.3.5, l'idéal $(f, g) = (h)$ est principal. Le polynôme f étant irréductible (sur K) et $h | f$, il existe une constante $c \in K^*$ telle que $h = cf$ ou $h = c$. Le premier cas $h = cf$ est impossible, car $h | g$ et $\deg(g) < d$. Il en résulte qu'il existe $a, b \in K[X]$ tels que $af + bg = 1$, d'où $\overline{b}\overline{g} = 1$; autrement dit tout $r = \overline{g} \in R - \{0\}$ est inversible dans R.

(3.4.4) Remarques. (i) La preuve ci-dessus de 3.4.3(iii) a suivi la méthode de 2.2.3.2; on peut également utiliser l'argument de 2.2.2.5 (sous la forme 3.2.4).
(ii) En 3.4.3(i) (resp., (ii)), on a redémontré 3.1.1(iv) (resp., 3.2.1(iv)).

(3.4.5) Corollaire. *Soit $f \in K[X]$ un polynôme unitaire irréductible (sur K), de degré $d = \deg(f) \geq 1$; posons $E = K[X]/(f)$.*
(i) *L'anneau E est un corps contenant K.*
(ii) *$E = K(\alpha)$, où $\alpha = \overline{X}$ est l'image de X dans E.*
(iii) *f est le polynôme minimal de α sur K.*
(iv) *$1, \alpha, \ldots, \alpha^{d-1}$ ($= 1, \overline{X}, \ldots, \overline{X}^{d-1}$) est une base de E/K et $[E : K] = d$.*

(3.4.6) Exemples : (i) $K = \mathbf{Q}$, $f(X) = X^3 - 2$. Le polynôme f étant irréductible sur $\mathbf{Q}$ d'après 3.1.4(i), l'anneau $E = \mathbf{Q}[X]/(X^3 - 2)$ est un corps. Pour toute racine complexe $\alpha_0, \alpha_1, \alpha_2 \in \mathbf{C}$ de f ($\alpha_j = \rho^j \sqrt[3]{2}$, $j = 0, 1, 2$, $\sqrt[3]{2} \in \mathbf{R}$), l'évaluation en α_j induit un isomorphisme de corps

$$\overline{\mathrm{ev}_{\alpha_j}} : E \xrightarrow{\sim} \mathbf{Q}(\alpha_j), \qquad \overline{g(X)} \mapsto g(\alpha_j).$$

(ii) Si $K = \mathbf{F}_p$ et $f(X) \in \mathbf{F}_p[X]$ est un polynôme irréductible (sur $\mathbf{F}_p$) de degré $\deg(f) = n \geq 1$, alors $E = \mathbf{F}_p[X]/(f)$ est un corps et $[E : \mathbf{F}_p] = n$, ce qui entraîne que $|E| = p^n$ (voir 4.1.2 ci-desssous).
(iii) En particulier, le polynôme $f(X) = X^2 + X + 1 \in \mathbf{F}_2[X]$ est irréductible sur $\mathbf{F}_2$ (car $f(0) = f(1) \neq 0$), donc $E = \mathbf{F}_2[X]/(X^2 + X + 1)$ est un corps ayant $2^2 = 4$ éléments (cf. 2.3.4).

(3.4.7) Définition. *Soit $f \in K[X]$ un polynôme de degré $n \geq 1$. Une extension L/K s'appelle un* **corps de décomposition** *de f sur K si f se décompose $f(X) = c(X-\alpha_1)\cdots(X-\alpha_n)$ dans $L[X]$ (où $c \in K^*$ et $\alpha_1, \ldots, \alpha_n \in L$) et si L est engendré sur K par les racines α_i de f: $L = K(\alpha_1, \ldots, \alpha_n)$ (d'après 3.2.6, l'extension L/K est de degré fini). [On aimerait dire que "***le*** *corps de décomposition de f sur K est* **le** *corps engendré sur K par* **les** *racines de f", mais le problème c'est que les racines de f ne sont pas données à priori.]*

(3.4.8) Proposition. *Soit $f \in K[X]$ un polynôme de degré $n \geq 1$. Alors il existe un corps de décomposition de f sur K.*

Preuve. Soit $f_1 | f$ ($f_1 \in K[X]$) un facteur non constant irréductible (sur K) de f. D'après 3.4.3, $K_1 = K[X]/(f_1(X))$ est un corps de degré fini sur K, f_1 admet une racine $\alpha_1 = \overline{X} \in K_1$ et $K_1 = K(\alpha)$. En appliquant la même procedure au polynôme $f(X)/(X-\alpha_1)$ sur K_1 etc., on arrivera à un corps de décomposition de f (sur K).

(3.4.9) En fait, il existe un corps contenant K dans lequel **tout** polynôme $f \in K[X]$ se décompose. Plus précisement:

(3.4.9.1) Définition. *Un corps L est* **algébriquement clos** *si tout polynôme non constant $f \in L[X]$ a une racine $\alpha \in L$.*

(3.4.9.2) Exemple : Le corps $\mathbf{C}$ est algébriquement clos.

(3.4.9.3) Lemme. *Soient L un corps et $f \in L[X]$ un polynôme de degré $n \geq 1$. Si L et algébriquement clos, alors on a $f(X) = c(X-\alpha_1)\cdots(X-\alpha_n)$ ($c, \alpha_i \in L$).*

Preuve. Il existe une racine $\alpha_1 \in L$ de f, donc $f(X) = (X-\alpha_1)f_1(X)$ dans $L[X]$. Si $\deg(f_1) \geq 1$, on continue avec $f_1(X)$ etc.; on arrivera à la factorisation cherchée.

(3.4.9.4) On va démontrer dans la deuxième partie du cours que tout corps K possède une extension algébriquement clos $L \supset K$, qui est algébrique sur K (une "clôture algébrique" de K). Par exemple, si K est un sous-corps de $\mathbf{C}$, alors on peut prendre $L = \{\alpha \in \mathbf{C} \mid \alpha \text{ algébrique sur } K\}$.

(3.5) Homomorphismes de corps

Étant donné une relation algébrique valable dans un corps K, on peut en déduire d'autres relations en appliquant des homomorphismes de corps $\sigma : K \longrightarrow L$. Par exemple :

(3.5.1) Exemples : (i) $(2+i)^2 = 3+4i \Longrightarrow (2-i)^2 = 3-4i$.
(ii) $(2+\sqrt{3})^3 = 26+15\sqrt{3} \Longrightarrow (2-\sqrt{3})^3 = 26-15\sqrt{3}$.
(iii) $(1+\sqrt[3]{2}-\sqrt[3]{4})^2 = -3+4\sqrt[3]{2}-\sqrt[3]{4} \Longrightarrow (1+\rho\sqrt[3]{2}-\rho^2\sqrt[3]{4})^2 = -3+4\rho\sqrt[3]{2}-\rho^2\sqrt[3]{4}$.

(3.5.2) Lemme. *Soient K, L des corps et $\sigma : K \longrightarrow L$ un homomorphisme d'anneaux. Alors on a:*
(i) $(\forall x \in K^*) \quad \sigma(x) \in L^*$ et $\sigma(x^{-1}) = \sigma(x)^{-1}$.
(ii) *σ est injectif.*
(iii) *σ est un isomorphisme (d'anneaux) $\iff$ σ est bijectif $\iff$ σ est surjectif.*

Preuve. (i) $(\exists y \in K^*) \quad xy = 1 \Longrightarrow \sigma(x)\sigma(y) = \sigma(1) = 1 \Longrightarrow \sigma(x^{-1}) = \sigma(y) = \sigma(x)^{-1}$. Il en résulte que $\mathrm{Ker}(\sigma) = \{0\}$, d'où (ii) (ce qui entraîne (iii)).

(3.5.3) Terminologie. (i) On dit souvent que σ en 3.5.2 est un **homomorphisme de corps** (ou un **plongement de corps**, puisque σ est automatiquement injectif). Si σ est un isomorphisme d'anneaux, on dit que σ est un **isomomorphisme de corps**.
(ii) Soient $K \subset K'$ et $L \subset L'$ des extensions de corps. On dit qu'un homomorphisme de corps $\tau : K' \longrightarrow L'$ **prolonge** $\sigma : K \longrightarrow L$ si $(\forall x \in K) \quad \tau(x) = \sigma(x)$ ($\iff \tau|_K = \sigma$, où l'on a noté $\tau|_K$ la restriction de τ à K):

$$\begin{array}{ccc} L & \hookrightarrow & L' \\ \uparrow{\scriptstyle \sigma} & & \uparrow{\scriptstyle \tau} \\ K & \hookrightarrow & K' \end{array}$$

Si $K = L$ et si $\tau : K' \longrightarrow L'$ prolonge $\mathrm{id} : K \longrightarrow K$ ($\iff$ $(\forall x \in K)\ \tau(x) = x$), on dit que τ est un **homomorphisme de K-algèbres**. Posons

$$\mathrm{Hom}_{K-\mathrm{Alg}}(K', L') = \{\tau : K' \longrightarrow L' \,|\, \tau \text{ est un homomorphisme de } K-\text{algèbres}\}$$
$$\mathrm{Isom}_{K-\mathrm{Alg}}(K', L') = \{\tau \in \mathrm{Hom}_{K-\mathrm{Alg}}(K', L') \,|\, \tau \text{ est un isomomorphisme de corps}\}.$$

La **propriété fondamentale** suivante généralise 3.5.1: si $\tau \in \mathrm{Hom}_{K-\mathrm{Alg}}(K', L')$ et $\alpha_1, \ldots, \alpha_n \in K'$, alors on a, pour tout polynôme $f = \sum c_{i_1,\ldots,i_n} X_1^{i_1} \cdots X_n^{i_n} \in K[X_1 \ldots, X_n]$,

$$\tau\left(f(\alpha_1, \ldots, \alpha_n)\right) = \tau\left(\sum c_{i_1,\ldots,i_n} \alpha_1^{i_1} \cdots \alpha_n^{i_n}\right) = \sum c_{i_1,\ldots,i_n} \tau(\alpha_1)^{i_1} \cdots \tau(\alpha_n)^{i_n} = f\left(\tau(\alpha_1), \ldots, \tau(\alpha_n)\right);$$

en particulier,

$$f(\alpha_1, \ldots, \alpha_n) = 0 \iff f\left(\tau(\alpha_1), \ldots, \tau(\alpha_n)\right) = 0.$$

(3.5.4) Exemples : (i) ("Conjugaison complexe") $\sigma(a + ib) = a - ib$ $(a, b \in \mathbf{R})$, $\sigma \in \mathrm{Isom}_{\mathbf{R}-\mathrm{Alg}}(\mathbf{C}, \mathbf{C})$.
(ii) $\sigma(a + b\sqrt{2}) = a - b\sqrt{2}$ $(a, b \in \mathbf{Q})$, $\sigma \in \mathrm{Isom}_{\mathbf{Q}-\mathrm{Alg}}(\mathbf{Q}(\sqrt{2}), \mathbf{Q}(\sqrt{2}))$.
(iii) Si $\sigma : K \longrightarrow L$ est un homomorphisme de corps de caractéristique $\mathrm{car} = 0$ (resp., $\mathrm{car} = p > 0$), alors σ est automatiquement un $\mathbf{Q}$-homomorphisme (resp., un $\mathbf{F}_p$-homomorphisme) de corps, puisque on a

$$\sigma\left(\frac{m \cdot 1_K}{n \cdot 1_K}\right) = \frac{m \cdot \sigma(1_K)}{n \cdot \sigma(1_K)} = \frac{m \cdot 1_L}{n \cdot 1_L} \qquad (m, n \in \mathbf{Z},\ \mathrm{car}(K) \nmid n).$$

(iv) Soient $\alpha_j = \rho^j \alpha_0$ $(j = 0, 1, 2)$ les racines complexes du polynôme $X^3 - 2$. Comme en 3.4.6(i), on a (pour chaque $j = 0, 1, 2$), un $\mathbf{Q}$-isomorphisme de corps

$$\overline{\mathrm{ev}_{\alpha_j}} : E \xrightarrow{\sim} \mathbf{Q}(\alpha_j),$$

où $E = \mathbf{Q}[X]/(X^3 - 2)$. Il en résulte que l'application

$$\sigma_j = \overline{\mathrm{ev}_{\alpha_j}} \circ (\overline{\mathrm{ev}_{\alpha_0}})^{-1} : \mathbf{Q}(\alpha_0) \longrightarrow \mathbf{Q}(\alpha_j)$$
$$\sigma_j : A + B\alpha_0 + C\alpha_0^2 \mapsto A + B\alpha_j + C\alpha_j^2 \qquad (A, B, C \in \mathbf{Q})$$

est aussi un $\mathbf{Q}$-isomorphisme de corps, ce qui explique 3.5.1(iii). On écrit souvent "$\sigma_j : \alpha_0 \mapsto \alpha_j$", car l'homomorphisme σ_j est déterminé par $\sigma_j(\alpha_0)$.
(v) Soient $\sigma : F \xrightarrow{\sim} F'$ un isomomorphisme de corps et $f \in F[X]$ un polynôme irréductible (sur F) non constant. Alors l'application $g = \sum a_i X^i \mapsto {}^\sigma g = \sum \sigma(a_i) X^i$ induit un isomomorphisme de corps $\sigma' : F[X]/(f) \xrightarrow{\sim} F'[X]/({}^\sigma f)$ prolongeant σ.
(vi) En particulier, si $F(\alpha)/F$ et $F'(\alpha')/F'$ sont des extensions simples telles que le polynôme minimal de α sur F (resp., de α' sur F') soit égal à f (resp., à ${}^\sigma f$), alors l'application $\sigma_1 = \overline{\mathrm{ev}_{\alpha'}} \circ \sigma' \circ (\overline{\mathrm{ev}_\alpha})^{-1} : F(\alpha) \xrightarrow{\sim} F'(\alpha')$ est un isomomorphisme de corps prolongeant $\sigma : F \xrightarrow{\sim} F'$:

$$\begin{array}{rccccc}
\overline{\mathrm{ev}}_\alpha : & F[X]/(f) & \xrightarrow{\sim} & F(\alpha) & \hookleftarrow & F \\
& \downarrow{\scriptstyle \wr\sigma'} & & \downarrow{\scriptstyle \wr\sigma_1} & & \downarrow{\scriptstyle \wr\sigma} \\
\overline{\mathrm{ev}_{\alpha'}} : & F'[X]/({}^\sigma f) & \xrightarrow{\sim} & F'(\alpha') & \hookleftarrow & F'
\end{array}$$

(3.5.5) Proposition. *Soient $\sigma : F \xrightarrow{\sim} F'$ un isomomorphisme de corps,*

$$f = \sum_{i=0}^{n} a_i X^i \in F[X] \qquad (n = \deg(f) \geq 1), \qquad {}^\sigma f = \sum_{i=0}^{n} \sigma(a_i) X^i \in F'[X]$$

et K (resp., K') un corps de décomposition du polynôme f (resp., ${}^\sigma f$) sur F (resp., sur F'). Alors il existe un isomorphisme de corps $\tau : K \xrightarrow{\sim} K'$ prolongeant σ.

(3.5.6) Corollaire (Unicité de corps de décomposition). *Si K, K' sont des corps de décomposition du même polynôme non constant $f \in F[X]$ sur F, alors il existe un F-isomorphisme de corps $K \xrightarrow{\sim} K'$.*

Preuve de 3.5.5. Soit $f_1 | f$, $f_1 \in F[X]$, un facteur non constant de f, irréductible sur F ($\Longrightarrow$ le polynôme ${}^\sigma f_1 \in F'[X]$ est irréductible sur F' et divise ${}^\sigma f$). Il existe $\alpha \in K$, $\alpha' \in K'$ tels que $f_1(\alpha) = 0$, ${}^\sigma f_1(\alpha') = 0$. Posons $F_1 = F(\alpha) \subset K$, $F_1' = F'(\alpha') \subset K'$. Comme en 3.5.4(vi) on construit un isomorphisme de corps $\sigma_1 : F_1 \xrightarrow{\sim} F_1'$ prolongeant σ. Le corps K (resp., K') étant un corps de décomposition du polynôme $f(X)/(X-\alpha)$ (resp., ${}^\sigma f(X)/(X-\alpha')$) sur F_1 (resp., sur F_1'), on conclut par récurrence sur le degré de f.

(3.5.7) Sous les hypothèses de 3.5.5, le polynôme f se factorise dans K comme $f(X) = c(X-\alpha_1)\cdots(X-\alpha_n)$ ($c \in F^*$, $\alpha_i \in K$), donc ${}^\sigma f(X) = c(X - \tau(\alpha_1))\cdots(X-\tau(\alpha_n))$, car τ prolonge σ.

En particulier, l'isomorphisme τ induit une bijection entre l'ensemble des racines de f dans K et l'ensemble des racines de ${}^\sigma f$ dans K' (y compris les multiplicités).

(3.5.8) Définition. *Soit F un corps. Un polynôme $f \in F[X]$ de degré $n \geq 1$ est* **séparable** *si ses racines dans un corps de décomposition de f sur F sont distinctes ($\Longleftrightarrow$ si ses racines dans tout corps sur lequel f se factorise comme $c(X-\alpha_1)\cdots(X-\alpha_n)$ sont distinctes, d'après 3.5.6).*

(3.5.9) Définition. *La dérivée d'un polynôme $f = \sum_{i=0}^n a_i X^i \in F[X]$ est définie comme $f' = \sum_{i=1}^n i a_i X^{i-1} \in F[X]$ (où $ia_i = (i \cdot 1_F)a_i$).*

(3.5.10) Lemme. *Soient $F \subset K$ des corps, $f \in F[X]$ et $\alpha \in K$. Alors on a:*
(i) *Le polynôme $f(X) - f(\alpha) - (X-\alpha)f'(X) \in K[X]$ est divisible dans $K[X]$ par $(X-\alpha)^2$.*
(ii) *α est une racine multiple de $f \iff f(\alpha) = f'(\alpha) = 0$.*

Preuve. (i) Exercice [*on se ramène par linéarité au cas $f(X) = X^n$, $n \geq 0$*]. (ii) Si α est une racine multiple de f, alors on a $f(\alpha) = 0$ et $f(X)$ est divisible dans $K[X]$ par $(X-\alpha)^2$, donc $(X-\alpha)f'(X)$ l'est aussi (d'après (i)). Il en résulte que $X - \alpha$ divise $f'(X)$, donc $f'(\alpha) = 0$. D'autre part, si $f(\alpha) = f'(\alpha) = 0$, alors $X-\alpha$ divise $f'(X)$, donc $(X-\alpha)^2$ divise $f(X)$ d'après (i).

(3.5.11) Corollaire. *Soit F un corps. Un polynôme non constant $f \in F[X]$ est séparable $\iff$ l'idéal (f, f') de $F[X]$ engendré par f, f' est égal à $(f, f') = (1)$.*

Preuve. L'idéal $(f, f') = (g)$ est principal, engendré par un polynôme unitaire g (bien sûr, $g = \mathrm{pgcd}(f, f')$). Si $g \neq 1$, alors on a $\deg(g) \geq 1$, donc g possède une racine α dans une extension $K \supset F$, d'où $f(\alpha) = f'(\alpha) = 0$. Si $g = 1$, alors il existe $a, b \in F[X]$ tels que $a(X)f(X) + b(X)f'(X) = 1$. Il en résulte que $b(\alpha)f'(\alpha) = 1$ ($\Longrightarrow f'(\alpha) \neq 0$) pour toute racine α de f.

4. Corps finis

On va classifier les corps finis (= les corps ayant un nombre fini d'éléments).

(4.1) Corps finis – exemples

(4.1.1) Lemme. *Soit F un corps. Alors: F est un corps fini $\iff$ $\mathrm{car}(F) = p > 0$ et $n = [F : \mathbf{F}_p] < \infty$. Si c'est le cas, on a $|F| = p^n = q$, et tout élément de F^* (resp., de F) est une racine du polynôme $X^{q-1} - 1 \in \mathbf{F}_p[X]$ (resp., $X^q - X \in \mathbf{F}_p[X]$).*

Preuve. Si $\mathrm{car}(F) = p$ et $n = [F : \mathbf{F}_p] < \infty$, alors F est isomorphe à $\mathbf{F}_p^n$ comme $\mathbf{F}_p$-espace vectoriel, donc $|F| = |\mathbf{F}_p|^n = p^n$. Si $\mathrm{car}(F) = p$ et $[F : \mathbf{F}_p] = \infty$ (resp., si $\mathrm{car}(F) = 0$), alors F contient $\mathbf{F}_p^n$ pour tout $n \geq 1$ (resp., F contient $\mathbf{Q}$), d'où $|F| = \infty$.

Si $|F| = q < \infty$, alors F^* est un groupe fini d'ordre $q-1$, donc $(\forall a \in F^*)\ a^{q-1} = 1$ ($\iff a^q = a$). Si $a \in F - F^*$, alors on a $a = 0 \implies a^q = a$.

(4.1.2) Lemme. *Soient p un nombre premier et $f \in \mathbf{F}_p[X]$ un polynôme irréductible de degré $n \geq 1$. Alors on a :*
(i) *L'anneau $F = \mathbf{F}_p[X]/(f)$ est un corps fini, $|F| = p^n$. [On verra ci-dessous que tout corps fini s'écrit sous cette forme.]*
(ii) *Le polynôme f divise $X^{p^n} - X$ dans $\mathbf{F}_p[X]$.*

Preuve. (i) D'après 3.4.3, F est un corps et $[F : \mathbf{F}_p] = n$, d'où $|F| = p^n$. (ii) Soit $\overline{X}$ l'image de X dans F. On a $\overline{X}^{p^n} - \overline{X} = 0$ d'après 4.1.1, donc $f | (X^{p^n} - X)$.

(4.1.3) Exemples : (i) $(p = 2, n = 2)$ Dans $\mathbf{F}_2[X]$, on a $X^4 - X = X(X-1)f(X)$, où $f(X) = X^2 + X + 1$. Le polynôme f est irréductible dans $\mathbf{F}_2[X]$, car $f(0), f(1) \neq 0$ (en fait, f est le seul polynôme irréductible (unitaire) de degré 2 dans $\mathbf{F}_2[X]$, d'après 4.1.2(ii)). Il en résulte que $F = \mathbf{F}_2[X]/(X^2 + X + 1)$ est un corps ayant 4 éléments.
(ii) $(p = 2, n = 3)$ Les polynômes $f_1(X) = X^3 + X + 1$, $f_2(X) = X^3 + X^2 + 1$ sont irréductible dans $\mathbf{F}_2[X]$ (car $f_j(0), f_j(1) \neq 0$) et on a $X^8 - X = X(X-1)f_1(X)f_2(X) \in \mathbf{F}_2[X]$. On obtient donc deux corps $F_j = \mathbf{F}_2[X]/(f_j)$ $(j = 1, 2)$ ayant $2^3 = 8$ éléments. La formule $f_2(X) = f_1(X + 1)$ montre qu'il y a un isomorphisme de corps

$$F_1 = \mathbf{F}_2[X]/(f_1) \xrightarrow{\sim} F_2 = \mathbf{F}_2[X]/(f_2), \qquad \overline{X} \mapsto \overline{X} + 1.$$

(iii) $(p = 2, n = 5)$ Les polynômes $g_1(X) = X^5 + X + 1$ et $g_2(X) = X^5 + X^2 + 1$, sont-ils irréductible dans $\mathbf{F}_2[X]$? Comme $g_j(0), g_j(1) \neq 0$, ils n'ont pas de facteur de degré 1. Le seul polynôme irréductible de degré 2 étant $f = X^2 + X + 1$, il suffit d'appliquer l'algorithme de division à g_j et f; on obtient

$$X^5 + X + 1 = (X^2 + X + 1)(X^3 + X^2 + 1)$$
$$X^5 + X^2 + 1 = (X^2 + X + 1)(X^3 + X^2) + 1,$$

donc g_1 (resp., g_2) est réductible (resp., irréductible) dans $\mathbf{F}_2[X]$. Il en résulte que $\mathbf{F}_2[X]/(X^5 + X^2 + 1)$ est un corps ayant $2^5 = 32$ éléments.
(iv) $(p = 3, n = 2)$ Le polynôme $X^9 - X$ se factorise dans $\mathbf{F}_3[X]$ comme $X^9 - X = X(X-1)(X+1)hh_+h_-$, où $h(X) = X^2 + 1$ et $h_\pm(X) = h(X \pm 1) = X^2 \mp X - 1$. Les polynômes $h, h_\pm$ sont irréductible dans $\mathbf{F}_3[X]$, car $h(0), h(\pm 1) \neq 0$. On obtient donc trois corps $E = \mathbf{F}_3[X]/(h)$, $E_\pm = \mathbf{F}_3[X]/(h_\pm)$ ayant $3^2 = 9$ éléments et des isomorphismes de corps

$$E = \mathbf{F}_3[X]/(h) \xrightarrow{\sim} E_\pm = \mathbf{F}_3[X]/(h_\pm), \qquad \overline{X} \longrightarrow \overline{X} \pm 1.$$

(4.1.4) Exercice. *Montrer que l'anneau $F = \mathbf{F}_3[X]/(X^4 + X^2 + X + 1)$ est un corps. Déterminer le degré $[F : \mathbf{F}_3]$ et le nombre d'éléments de F. Soit $y = x^3 - 1 \in F$, où l'on a noté x l'image de X dans F. Déterminer $y^{-1} \in F$, le polynôme minimal de y sur $\mathbf{F}_3$ et l'ordre de x et y dans F^*.*

(4.2) Construction de corps finis

(4.2.1) Rappel : groupes abéliens finis. Soit A un groupe abélien fini; alors A est isomorphe au produit de groupes cycliques. Plus précisement, si $|A| = p^n > 1$ est une puissance d'un nombre premier p, alors A est isomorphe à

$$A \xrightarrow{\sim} \mathbf{Z}/p^{a_1}\mathbf{Z} \times \cdots \times \mathbf{Z}/p^{a_k}\mathbf{Z} \qquad (a_i \geq 1,\, a_1 + \cdots + a_k = n).$$

Si $|A| = p_1^{n_1} \cdots p_r^{n_r}$, où $p_1, \ldots, p_r$ sont des nombres premiers distincts (et $n_i \geq 1$), alors A est isomorphe à

$$A \xrightarrow{\sim} A(p_1) \times \cdots \times A(p_r),$$

où $A(p_i)$ est un groupe abélien d'ordre $|A(p_i)| = p_i^{n_i}$.

(4.2.2) Lemme. *Soit F un corps. Alors tout sous-groupe multiplicatif fini $A \subset F^*$ est cyclique.*

Preuve. On peut supposer que $|A| = p_1^{n_1} \cdots p_r^{n_r} > 1$. Fixons un nombre premier $p = p_i$ qui divise $|A|$; alors il existe un homomorphisme de groupes abéliens

$$A(p) \xrightarrow{\sim} \mathbf{Z}/p^{a_1}\mathbf{Z} \times \cdots \times \mathbf{Z}/p^{a_k}\mathbf{Z} \qquad (a_i \geq 1),$$

d'où

$$p^k = |\{x \in A(p) \,|\, x^p = 1\}| \leq |\{x \in A \,|\, x^p = 1\}| \leq |\{x \in F \,|\, x^p - 1 = 0\}| \leq p$$

(car le nombre de racines du polynôme $X^p - 1$ contenues dans le corps F est au plus égal à $\deg(X^p - 1) = p$), donc $k = 1$ et le groupe $A(p) = A(p_i) \xrightarrow{\sim} \mathbf{Z}/p_i^{n_i}\mathbf{Z}$ est cyclique. D'après le "Lemme chinois", le groupe

$$A \xrightarrow{\sim} \mathbf{Z}/p_1^{n_1}\mathbf{Z} \times \cdots \times \mathbf{Z}/p_r^{n_r}\mathbf{Z} \xrightarrow{\sim} \mathbf{Z}/p_1^{n_1} \cdots p_r^{n_r}\mathbf{Z}$$

est cyclique aussi.

(4.2.3) Corollaire. *Soit F un corps fini ayant $q = p^n$ éléments. Alors on a:*
(i) *Le groupe F^* est cyclique d'ordre $q - 1$.*
(ii) *Si le groupe F^* est engendré par $\alpha \in F^*$, alors on a $F = \mathbf{F}_p(\alpha)$ ($\Longrightarrow F \xrightarrow{\sim} \mathbf{F}_p[X]/(f)$, où f est le polynôme minimal de α sur $\mathbf{F}_p$).*
(iii) *F est un corps de décomposition du polynôme $X^{q-1} - 1$ (est aussi de $X^q - X$) sur $\mathbf{F}_p$.*

Preuve. (i) Ceci résulte de 4.2.2. (ii) Tout élément $a \in F - \{0\}$ s'écrit comme $a = \alpha^j$ ($j \geq 0$), donc $F = \mathbf{F}_p[\alpha] = \mathbf{F}_p(\alpha)$. (iii) Le polynôme $X^q - X$ a q racines distinctes dans F (à savoir les éléments de F), qui engendrent F comme une extension de $\mathbf{F}_p$.

(4.2.4) Lemme-Définition. *Si F est un corps de caractéristique* $\mathrm{car}(F) = p > 0$, *alors on a*

$$(\forall x, y \in F) \qquad (x \pm y)^p = x^p \pm y^p, \qquad (xy)^p = x^p y^p.$$

Autrement dit, l'application

$$\varphi : F \longrightarrow F, \qquad \varphi(x) = x^p$$

est un homomorphisme de corps; on l'appelle **l'application de Frobenius**.

Preuve. On a

$$(x \pm y)^p = \sum_{i=0}^{p} \binom{p}{i} x^i (\pm y)^{p-i} = x^p + (\pm y)^p = x^p \pm y^p,$$

car $(\pm 1)^p = -1$ dans F (même si $p = 2$) et $\binom{p}{i}$ est divisible par $p = \mathrm{car}(F)$ pour $i \neq 0, p$.

(4.2.5) Corollaire. *Pour tout entier $n \geq 1$, l'application*

$$\varphi^n = \underbrace{\varphi \circ \cdots \circ \varphi}_{n-\text{fois}} : F \longrightarrow F, \qquad \varphi^n(x) = x^{p^n}$$

est un homomorphisme de corps. Si $|F| = p^n$, alors on a $\varphi^n = \mathrm{id}$.

(4.2.6) Lemme. *Soit E un corps de caractéristique $\mathrm{car}(E) = p > 0$ dans lequel le polynôme $g(X) = X^{p^n} - X$ se décompose $g(X) = (X - \alpha_1) \cdots (X - \alpha_{p^n})$ ($\alpha_i \in E$). Alors l'ensemble de racines de g*

$$F = \{\alpha \in E \,|\, \alpha^{p^n} = \alpha\} = \{\alpha \in E \,|\, \varphi^n(\alpha) = \alpha\}$$

est un sous-corps de E et $|F| = p^n$.

Preuve. D'après 4.2.4-5, si $x, y \in F$, alors on a

$$(x \pm y)^{p^n} = x^{p^n} \pm y^{p^n} = x \pm y, \qquad (xy)^{p^n} = x^{p^n} y^{p^n} = xy, \qquad (x/y)^{p^n} = x^{p^n}/y^{p^n} = x/y \quad (y \neq 0),$$

donc F est un sous-corps de E. Le polynôme g étant séparable (grâce à 3.5.11, car $g'(X) = -1$), on a $|F| = \deg(g) = p^n$.

(4.2.7) Corollaire. *Si E est un corps de décomposition du polynôme $X^{p^n} - X$ ($n \geq 1$) sur $\mathbf{F}_p$, alors on a $|E| = p^n$.*

Preuve. En utilisant la notation de 4.2.6, le corps E est engendré sur $\mathbf{F}_p$ par l'ensemble F; mais F étant un corps, on a $E = F$.

(4.3) Théorème principal

(4.3.1) Théorème. *Soit p un nombre premier.* (i) *Pour tout entier $n \geq 1$ il existe un corps ayant p^n éléments; il est unique à un isomorphisme près. On note $\mathbf{F}_{p^n}$ (ou $GF(p^n)$) un tel corps.*
(ii) *Soient $m, n \geq 1$ des entiers. Il existe un plongement de corps $\sigma : \mathbf{F}_{p^m} \hookrightarrow \mathbf{F}_{p^n}$ si et seulement si $m|n$. Si c'est le cas, alors l'image de σ est égale à $\{x \in \mathbf{F}_{p^n} \,|\, x^{p^m} = x\}$.*

Preuve. (i) On a démontré l'existence de $\mathbf{F}_{p^n}$ en 4.2.7; son unicité résulte de 3.5.6. (ii) Si $m|n$, alors on a $(p^m - 1)|(p^n - 1)$, donc le polynôme $X^{p^m} - X$ divise $X^{p^n} - X$. Il en résulte qu'un corps de décomposition de $X^{p^n} - X$ contient un corps de décomposition de $X^{p^m} - X$. D'autre part, s'il existe un plongement de corps $\sigma : \mathbf{F}_{p^m} \hookrightarrow \mathbf{F}_{p^n}$, alors $F = \sigma(\mathbf{F}_{p^m})$ est un sous-corps de $\mathbf{F}_{p^n}$ et $p^n = |\mathbf{F}_{p^n}| = |F|^d = p^{md}$, où $d = [\mathbf{F}_{p^n} : F]$ (comme en 4.1.1), donc $n = md$.

(4.3.2) Corollaire. (i) *Si $f \in \mathbf{F}_p[X]$ est un polynôme irréductible de degré $m \geq 1$, alors f divise $X^{p^n} - X$ dans $\mathbf{F}_p[X]$ si et seulement si $m|n$.*
(ii) *Pour $m \geq 1$, soit A_m l'ensemble de polynômes unitaires irréductibles $f \in \mathbf{F}_p[X]$ de degré $\deg(f) = m$. Alors A_m est non vide et l' on a*

$$(\forall n \geq 1) \qquad X^{p^n} - X = \prod_{m|n} \prod_{f \in A_m} f, \qquad p^n = \sum_{m|n} m|A_m|$$

[Ceci est une généralisation de (4.1.3).]

Preuve. (i) Soit $f \in A_m$ ($m \geq 1$). Si $m|n$, alors on a $f|(X^{p^m} - X)|(X^{p^n} - X)$ (d'après 4.1.2(ii) et la preuve de 4.3.1(ii)). Si, d'autre part, $f|(X^{p^n} - X)$, alors $F = \mathbf{F}_p[X]/(f) = \mathbf{F}_{p^m}$ est contenu dans un corps de décomposition de $X^{p^n} - X$ sur $\mathbf{F}_p$ (= dans $\mathbf{F}_{p^n}$), donc $m|n$ (d'après 4.3.1(ii)). (ii) La factorisation de $X^{p^n} - X$ résulte de (i) et du fait que le polynôme $X^{p^n} - X$ est séparable; on conclut en comparant les degrés des polynômes à gauche et à droite.

(4.3.3) Exercice. *Déterminer les valeurs $|A_m|$ pour $p = 2$ et $m \leq 9$.*

(4.3.4) Exercice. *Généraliser 4.3.2 en remplaçant $\mathbf{F}_p[X]$ par $\mathbf{F}_{p^r}[X]$.*

5. Séparabilité

(5.1) Éléments conjugués

(5.1.1) Définition. *Soit $\alpha \in \mathbf{C}$ un nombre algébrique. Les* **conjugués** *de α sont les racines complexes du polynôme minimal $f \in \mathbf{Q}[X]$ de α sur $\mathbf{Q}$.*

(5.1.2) Exemples : (1) $\alpha \in \mathbf{Q}$, $f = X - \alpha$: $\{\alpha\}$.
(2) $\alpha = \sqrt{2}$, $f = X^2 - 2$: $\{\sqrt{2}, -\sqrt{2}\}$.
(3) $\alpha = \sqrt[3]{2}$, $f = X^3 - 2$: $\{\sqrt[3]{2}, \rho\sqrt[3]{2}, \rho^2\sqrt[3]{2}\}$.
(4) $\alpha = \sqrt{2} + \sqrt{3}$, $f = X^4 - 10X^2 + 1$: $\{\sqrt{2}+\sqrt{3}, \sqrt{2}-\sqrt{3}, -\sqrt{2}+\sqrt{3}, -\sqrt{2}-\sqrt{3}\}$.

(5.1.3) Définition. *Soient $K \subset L$ des corps, $\alpha \in L$ un élément algébrique sur K, $f \in K[X]$ le polynôme minimal de α sur K, E un corps de décomposition de f sur K contenant α. Les* **conjugués de α sur K** *(dans E) sont les racines de f dans E.*

(5.1.4) Exemples (nombre de conjugués): (i) Dans 5.1.2(n) ($1 \leq n \leq 4$), le nombre de conjugués de α (sur $\mathbf{Q}$) $= [\mathbf{Q}(\alpha) : \mathbf{Q}] = n$.
(ii) Soient $L = \mathbf{F}_p(t) \supset \mathbf{F}_p(t^p) = K$, où t est une variable. Le polynôme minimal $f(X) = X^p - t^p \in K[X]$ de $\alpha = t \in L$ sur K n'est pas séparable, car $f(X) = (X-t)^p \in L[X]$. Il en résulte que t est le seul conjugué de t sur K.

(5.1.5) Proposition. *Soient $K \subset L$, $\alpha \in L$ et $f \in K[X]$ comme en 5.1.3.*
(i) *Pour tout corps $M \supset K$, on a*

$$\mathrm{Hom}_{K-\mathrm{Alg}}(K(\alpha), M) = \{\sigma_\beta : K(\alpha) \longrightarrow M \mid \beta \in M,\ f(\beta) = 0\}, \qquad \sigma_\beta : g(\alpha) \mapsto g(\beta) \qquad (g \in K[X])$$

(c'est-à-dire qu'un K-homomorphisme de corps $K(\alpha) \longrightarrow M$ est déterminé par l'image de α, qui est une racine de f dans M). On écrit parfois "$\sigma_\beta : \alpha \mapsto \beta$".
(ii) *En particulier,* $|\mathrm{Hom}_{K-\mathrm{Alg}}(K(\alpha), M)| = |\{\text{racines } \beta \in M \text{ de } f\}| \leq \deg(f) = [K(\alpha) : K]$.
(iii) *On a* $|\mathrm{Hom}_{K-\mathrm{Alg}}(K(\alpha), M)| = [K(\alpha) : K] \iff$ *f est séparable et M contient un corps de décomposition de f (sur K).*

Preuve. Il suffit de démontrer (i), car (i) $\Longrightarrow$ (ii) $\Longrightarrow$ (iii). Pour tout $\sigma \in \mathrm{Hom}_{K-\mathrm{Alg}}(K(\alpha), M)$, on a $f(\sigma(\alpha)) = \sigma(f(\alpha)) = 0$, donc $\beta = \sigma(\alpha) \in M$ est une racine de f et $(\forall g \in K[X])\quad \sigma(g(\alpha)) = g(\sigma(\alpha)) = g(\beta)$. Réciproquement, pour toute racine $\beta \in M$ de f, l'application

$$\sigma_\beta = \overline{\mathrm{ev}_\beta} \circ (\overline{\mathrm{ev}_\alpha})^{-1} : K(\alpha) \xrightarrow{\sim} K[X]/(f) \xrightarrow{\sim} K(\beta) \subset M$$

est un homomorphisme de corps sur K et $\sigma_\beta(\alpha) = \overline{\mathrm{ev}_\beta}(\overline{X}) = \beta$.

(5.1.6) Exemples : (i) $K = \mathbf{Q}$, $L = \mathbf{Q}(\sqrt{2}, \sqrt{3}) = \mathbf{Q}(\sqrt{2}+\sqrt{3})$, $\alpha = \sqrt{2}+\sqrt{3}$, $M = \mathbf{C}$: on a

$$\mathrm{Hom}_{\mathbf{Q}-\mathrm{Alg}}(\mathbf{Q}(\sqrt{2},\sqrt{3}), \mathbf{C}) = \{\sigma_1, \sigma_2, \sigma_3, \sigma_4\}, \qquad \sigma_j : g(\sqrt{2}+\sqrt{3}) \mapsto g(\alpha_j) \qquad (g \in \mathbf{Q}[X]),$$

où $\{\alpha_1, \alpha_2, \alpha_3, \alpha_4\} = \{\pm\sqrt{2} \pm \sqrt{3}\}$.
(ii) $K = \mathbf{Q}$, $L = M = \mathbf{Q}(\sqrt[3]{2})$. Comme $\sqrt[3]{2}$ est la seule racine de $f(X) = X^3 - 2$ dans L, il n'y a qu'un seul K-homomorphisme de corps $L \longrightarrow L$, à savoir l'identité $\mathrm{id} : L \longrightarrow L$ ($\mathrm{id}(x) = x$ pour tout $x \in L$).

(5.2) Extensions séparables

(5.2.1) Définition. *Soit L/K une extension algébrique.*
(i) *Un élément $\alpha \in L$ est* **séparable sur** *K si son polynôme minimale sur K l'est.*
(ii) *L'extension L/K est* **séparable** *si tout élément $\alpha \in L$ est séparable sur K.*
(iii) *Le corps K est* **parfait** *si toute extension algébrique L/K est séparable ($\iff$ tout polynôme irréductible dans $K[X]$ est séparable).*

(5.2.2) Exemples : (i) $\sqrt{2}, \sqrt[3]{2}$ sont séparables sur $\mathbf{Q}$.
(ii) $t \in \mathbf{F}_p(t)$ n'est pas séparable sur $\mathbf{F}_p(t^p)$ (voir 5.1.4(ii)), donc l'extension $\mathbf{F}_p(t)/\mathbf{F}_p(t^p)$ n'est pas séparable.
(iii) Si L/K est séparable et $K \subset F \subset L$, alors les extensions intermédiaires F/K et L/F sont aussi séparables.
(iv) En particulier, si F est une extension algébrique d'un corps parfait K, alors F est aussi parfait.

(5.2.3) Proposition. *Soit K un corps.*
(i) *Si $f \in K[X]$ est un polynôme irréductible non constant, alors on a*

$$f \text{ est séparable } \iff f' \neq 0 \iff \begin{cases} \mathrm{car}(K) = 0 \\ \mathrm{car}(K) = p > 0 \text{ et } f(X) \neq g(X^p),\ g \in K[X]. \end{cases}$$

(ii) *Si $\mathrm{car}(K) = 0$ ou $|K| < \infty$, alors le corps K est parfait.*

Preuve. (i) Posons $g = \mathrm{pgcd}(f, f')$ (= le polynôme unitaire qui engendre l'idéal $(f, f') = (g)$ de $K[X]$). L'irréductibilité de f entraîne que $g = c$ ou $g = cf$ $(c \in K^*)$; il résulte de 3.5.11 que:

$$f \text{ n'est pas séparable } \iff \deg(g) > 0 \iff g = cf \iff f \big| f' \iff f' = 0$$

(puisque $g|f'$ et $\deg(f') < \deg(f)$). Si $\mathrm{car}(K) = 0$, alors on a $f' \neq 0$. Si $\mathrm{car}(K) = p > 0$, alors on a

$$f' = 0 \iff f(X) = \sum_{i=0}^{n} b_i X^{pi} = g(X^p), \qquad g(X) = \sum_{i=0}^{n} b_i X^i \in K[X].$$

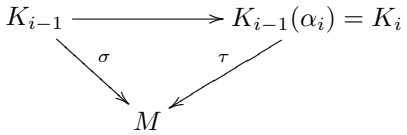
(ii) Le cas $\mathrm{car}(K) = 0$ résulte de (i). Si $|K| < \infty$, il faut démontrer que tout polynôme irréductible non constant $f \in K[X]$ est séparable. L'anneau $F = K[X]/(f)$ est un corps fini; le même argument que en 4.1.2 montre que f divise $X^q - X$ dans $K[X]$ (où $q = |F|$), mais le polynôme $g(X) = X^q - X$ est séparable, puisqu'il a $q = \deg(g)$ racines distinctes dans F (à savoir les éléments de F).

(5.2.4) Proposition. *Soit L/K une extension de degré fini.*
(i) *Pour toute extension de corps M/K, on a* $|\mathrm{Hom}_{K-\mathrm{Alg}}(L, M)| \leq [L : K]$.
(ii) *L'extension L/K est séparable $\iff$ il existe une extension M/K telle que* $|\mathrm{Hom}_{K-\mathrm{Alg}}(L, M)| = [L : K]$ *(en général, $M \neq L$; voir 5.1.6(ii)).*
(iii) *Pour toute extension de corps K'/K il existe une extension M/K' telle que* $\mathrm{Hom}_{K-\mathrm{Alg}}(L, M) \neq \emptyset$.

Preuve. Si $L = K(\alpha)$ est une extension simple de K, alors (i) et (ii) résultent de 5.1.5(ii) et (iii), respectivement. En général, $L = K(\alpha_1, \ldots, \alpha_n)$; posons $K_i = K(\alpha_1, \ldots, \alpha_i) = K_{i-1}(\alpha_i)$:

$$K = K_0 \subset K_1 \subset \cdots \subset K_{i-1} \subset K_{i-1}(\alpha_i) = K_i \subset \cdots \subset K_n = L.$$

(i) Fixons $i \in \{1, \ldots, n-1\}$. D'après 5.1.5(ii), tout élément $\sigma \in \mathrm{Hom}_{K-\mathrm{Alg}}(K_{i-1}, M)$ admet au plus $[K_{i-1}(\alpha_i) : K_{i-1}] = [K_i : K_{i-1}]$ prolongements $\tau \in \mathrm{Hom}_{K-\mathrm{Alg}}(K_i, M)$:



donc

$$|\mathrm{Hom}_{K-\mathrm{Alg}}(K_i, M)| \leq [K_i : K_{i-1}] \cdot |\mathrm{Hom}_{K-\mathrm{Alg}}(K_{i-1}, M)|. \tag{5.2.4.1}$$

En multipliant les inégalités (5.2.4.1), on obtient

$$|\mathrm{Hom}_{K-\mathrm{Alg}}(L, M)| \leq \left(\prod_{i=1}^{n} [K_i : K_{i-1}]\right) |\mathrm{Hom}_{K-\mathrm{Alg}}(K, M)| = [L : K].$$

(ii) Si l'extension L/K n'est pas séparable, on peut choisir les éléments $\alpha_1, \ldots, \alpha_n$ tels que α_1 ne sois pas séparable sur K. D'après 5.1.5(ii), on a

$$|\mathrm{Hom}_{K-\mathrm{Alg}}(K_1, M)| = |\mathrm{Hom}_{K-\mathrm{Alg}}(K(\alpha_1), M)| < [K(\alpha_1) : K] = [K_1 : K]$$

(pour toute extension M/K); les inégalités (5.2.4.1) alors montrent que

$$|\mathrm{Hom}_{K-\mathrm{Alg}}(L, M)| < \left(\prod_{i=1}^{n} [K_i : K_{i-1}]\right) = [L : K].$$

Si l'extension L/K est séparable, soit $f_i \in K[X]$ (resp., $g_i \in K_{i-1}[X]$) le polynôme minimal (séparable !) de α_i sur K (resp., sur K_{i-1}). On définit, par récurrence, $M_0 = K$, $M_i =$ un corps de décomposition de f_i sur M_{i-1} $(1 \leq i \leq n)$, $M = M_n$. Le polynôme g_i a $\deg(g_i) = [K_i : K_{i-1}]$ racines distinctes dans M; on déduit de 5.1.5(iii) que tout élément $\sigma \in \mathrm{Hom}_{K-\mathrm{Alg}}(K_{i-1}, M)$ admet $[K_i : K_{i-1}]$ prolongements $\tau \in \mathrm{Hom}_{K-\mathrm{Alg}}(K_i, M)$, donc

$$|\mathrm{Hom}_{K-\mathrm{Alg}}(K_i, M)| = [K_i : K_{i-1}] \cdot |\mathrm{Hom}_{K-\mathrm{Alg}}(K_{i-1}, M)| \qquad (1 \leq i \leq n)$$
$$|\mathrm{Hom}_{K-\mathrm{Alg}}(L, M)| = \left(\prod_{i=1}^{n} [K_i : K_{i-1}]\right) |\mathrm{Hom}_{K-\mathrm{Alg}}(K, M)| = [L : K].$$

(iii) Posons $M'_0 = K'$, $M'_i =$ un corps de décomposition de f_i sur M'_{i-1} $(1 \leq i \leq n)$, $M = M'_n$. Alors tout élément $\sigma \in \mathrm{Hom}_{K-\mathrm{Alg}}(K_{i-1}, M)$ admet un prolongement $\tau \in \mathrm{Hom}_{K-\mathrm{Alg}}(K_i, M)$ (d'après 5.1.5(ii)), d'où

$$|\mathrm{Hom}_{K-\mathrm{Alg}}(L, M)| \geq |\mathrm{Hom}_{K-\mathrm{Alg}}(K, M)| = 1.$$

(5.2.5) Corollaire. (i) *Soient L/K une extension algébrique et $\alpha \in L$. Si α est séparable sur K, alors l'extension $K(\alpha)/K$ est séparable.*
(ii) *Si F/K et L/F sont des extensions séparables de degré fini, alors l'extension L/K est aussi séparable.*

Preuve. (i) Soit M un corps de décomposition (sur K) du polynôme minimal $f \in K[X]$ de α sur K. On déduit de 5.1.5(iii) que

$$|\mathrm{Hom}_{K-\mathrm{Alg}}(K(\alpha), M)| = \deg(f) = [K(\alpha) : K],$$

d'où le résultat (en appliquant 5.2.4(ii)).
(ii) Exercice.

(5.2.6) Théorème de l'élément primitif. *Soit L/K une extension séparable (ce qui est automatique si $\mathrm{car}(K) = 0$) de degré fini. Alors il existe $\alpha \in L$ (un "élément primitif") tel que $L = K(\alpha)$.*

Preuve. Si $|K| < \infty$, alors $L = K(\alpha)$, où α est un générateur du groupe cyclique fini L^*. Supposons que $|K| = \infty$. D'après 5.2.4(ii), il existe une extension M/K et $n = [L : K]$ homomorphismes distincts $\sigma_1, \ldots, \sigma_n \in \mathrm{Hom}_{K-\mathrm{Alg}}(L, M)$. Pour tous $1 \leq i < j \leq n$, $\mathrm{Ker}(\sigma_i - \sigma_j) \subsetneq L$ est un K-sous-espace vectoriel strict de L. Lemma 5.2.7 ci-dessous montre qu'il existe $\alpha \in L$ tel que $i \neq j \Longrightarrow \sigma_i(\alpha) \neq \sigma_j(\alpha)$, donc

$$n = [L : K] \geq [K(\alpha) : K] \geq |\{\text{racines de } f \text{ dans } M\}| \geq |\{\sigma_1(\alpha), \ldots, \sigma_n(\alpha)\}| = n,$$

où l'on a noté $f \in K[X]$ le polynôme minimal de α sur K; il en résulte que $[L : K(\alpha)] = 1$, donc $L = K(\alpha)$.

(5.2.7) Lemme. *Soient K un corps infini, V un K-espace vectoriel et $V_1, \dots, V_k \subsetneq V$ des sous-espaces vectoriels stricts de V. Alors $V \neq V_1 \cup \cdots \cup V_k$.*

Preuve. Récurrence sur k: le cas $k = 1$ étant trivial, on peut supposer que $k > 1$ et $V = V_1 \cup \cdots \cup V_k$. Il existe $u \in V$, $u \notin V_k$ ($\Longrightarrow u \in V_1 \cup \cdots \cup V_{k-1}$) et, par l'hypothèse de récurrence, $v \in V$, $v \notin V_1 \cup \cdots \cup V_{k-1}$ ($\Longrightarrow v \in V_k$). L'ensemble $\{u + av \,|\, a \in K\}$ est infini, donc il existe $1 \leq j \leq k$ et $a, b \in K$, $a \neq b$, tels que $u + av, u + bv \in V_j \Longrightarrow (a - b)v \in V_j \Longrightarrow v \in V_j \Longrightarrow u \in V_j$, ce qui est impossible.

(5.2.8) Proposition. *Sous les hypothèses de 5.2.6, supposons que $L = K(\alpha_1, \dots, \alpha_m)$ et $|K| = \infty$. Alors il existe $c = (c_1, \dots, c_m) \in K^m$ tel que $L = K(\alpha_c)$, où l'on a noté $\alpha_c = c_1\alpha_1 + \cdots + c_m\alpha_m$.*

Preuve. Le polynôme

$$P(X_1, \dots, X_m) = \prod_{1 \leq i < j \leq n} (X_1(\sigma_i(\alpha_1) - \sigma_j(\alpha_1)) + \cdots + X_m(\sigma_i(\alpha_m) - \sigma_j(\alpha_m))) \in M[X_1, \dots, X_m]$$

n'est pas nul, donc il existe $c = (c_1, \dots, c_m) \in K^m$ tel que

$$0 \neq P(c_1, \dots, c_m) = \prod_{1 \leq i < j \leq n} (\sigma_i(\alpha_c) - \sigma_j(\alpha_c))$$

(puisque $|K| = \infty$). On conclut que $L = K(\alpha_c)$ comme plus haut.

(5.2.9) Exercice. *Soient x, y des variables et $L = \mathbf{F}_p(x, y) \supset K = \mathbf{F}_p(x^p, y^p)$. Montrer que, pour tout $\alpha \in L$, $[K(\alpha) : K] \leq p < p^2 = [L : K]$, donc $L \neq K(\alpha)$.*

(5.2.10) Lemme. *Soit L/K une extension algébrique séparable. Si $n := \max\{[K(\alpha) : K] \,|\, \alpha \in L\}$ est fini, alors on a $[L : K] = n$.*

Preuve. Fixons $\alpha \in L$ tel que $[K(\alpha) : K] = n$. Pour tout $\beta \in L$, il existe $\gamma \in K(\alpha, \beta)$ tel que $K(\alpha, \beta) = K(\gamma)$ (d'après 5.2.6). Il en résulte que $[K(\alpha, \beta) : K] = [K(\gamma) : K] \leq n = [K(\alpha) : K]$, donc $\beta \in K(\alpha)$. On en déduit que $L = K(\alpha)$ et $[L : K] = n$.

(5.2.11) Exercice. *Soit K un corps de caractéristique $\mathrm{car}(K) = p > 0$. Montrer que K est parfait $\iff$ $K^* = K^{*p}$ (c'est-à-dire que K est parfait $\iff$ l'application de Frobenius $\varphi : K \longrightarrow K$ est un isomorphisme de corps). En déduire que tout corps fini est parfait.*

(5.3) Norme, Trace, Discriminant

(5.3.1) Exemples : (i) $L/K = \mathbf{C}/\mathbf{R}$, $\beta = a + ib$ ($a, b \in \mathbf{R}$). Dans la base $\{1, i\}$ de $\mathbf{C}/\mathbf{R}$, on a

$$M(\beta) = \begin{pmatrix} a & -b \\ b & a \end{pmatrix},$$

$P_\beta(X) = \det(X \cdot I - M(\beta)) = X^2 - 2aX + (a^2 + b^2) = (X - (a + ib))(X - (a - ib))$. En fait,

$$g \begin{pmatrix} a & -b \\ b & a \end{pmatrix} g^{-1} = \begin{pmatrix} a + ib & 0 \\ 0 & a - ib \end{pmatrix}, \qquad g = \begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix}.$$

(ii) Soient $L/K = \mathbf{Q}(\sqrt[3]{2})/\mathbf{Q}$, où $\sqrt[3]{2} \in \mathbf{C}$ est une racine fixée de $X^3 - 2$, $\beta = a + b\sqrt[3]{2} + c\sqrt[3]{4} \in L$ ($a, b, c \in \mathbf{Q}$). Dans la base $\{1, \sqrt[3]{2}, \sqrt[3]{4}\}$, on a

$$M(\beta) = \begin{pmatrix} a & 2c & 2b \\ b & a & 2c \\ c & b & a \end{pmatrix}$$

(cf. 2.2.3.1) et

$$P_\beta(X) = \det(X \cdot I - M(\beta)) = (X-\beta_0)(X-\beta_1)(X-\beta_2), \qquad \beta_j = a + b\rho^j \sqrt[3]{2} + c\rho^{2j}\sqrt[3]{4}$$

(car $P_\beta(X) = P_{\beta_j}(X)$ pour chaque $j = 0, 1, 2$ et $P_{\beta_j}(\beta_j) = 0$, d'après 3.2.10).

(5.3.2) Proposition. *Soient L/K une extension séparable de degré fini et M/K une extension telle que $|\mathrm{Hom}_{K-\mathrm{Alg}}(L, M)| = [L : K] = n$. Alors on a, pour tout $\beta \in L$,*

$$P_{L/K,\beta}(X) = \prod_{i=1}^{n}(X - \sigma_i(\beta)), \qquad Tr_{L/K}(\beta) = \sum_{i=1}^{n}\sigma_i(\beta), \qquad N_{L/K}(\beta) = \prod_{i=1}^{n}\sigma_i(\beta),$$

où $\{\sigma_1, \ldots, \sigma_n\} = \mathrm{Hom}_{K-\mathrm{Alg}}(L, M)$.

Preuve. Soit $f \in K[X]$ le polynôme minimal de β sur K. D'après 3.2.11(iv), on a

$$P_{L/K,\beta}(X) = P_{K(\beta)/K,\beta}(X)^e = f(X)^e,$$

où $e = [L : K(\beta)] = n/d$, $d = \deg(f) = [K(\beta) : K]$. Le polynôme f a d racines distinctes $\beta_1, \ldots, \beta_d \in M$:

$$f(X) = (X - \beta_1)\cdots(X - \beta_d),$$

où $\beta_j = \tau_j(\beta)$, $\mathrm{Hom}_{K-\mathrm{Alg}}(K(\beta), M) = \{\tau_1, \ldots, \tau_d\}$. D'après 5.2.4(ii), tout homomorphisme τ_j admet e prolongements distincts $\tau' \in \mathrm{Hom}_{K-\mathrm{Alg}}(L, M)$. Il en résulte que toute racine β_j apparait e-fois parmi les valeurs $\sigma_1(\beta), \ldots, \sigma_n(\beta)$, donc

$$\begin{aligned} P_{L/K,\beta}(X) = (X-\beta_1)^e \cdots (X-\beta_d)^e = \prod_{i=1}^{n}(X - \sigma_i(\beta)) = \\ = X^n - Tr_{L/K}(\beta)X^{n-1} + \cdots + (-1)^n N_{L/K}(\beta), \end{aligned}$$

d'où le résultat.

(5.3.3) Plus précisement, on peut montrer qu'il existe une matrice $g \in GL_n(M)$ telle que

$$(\forall \beta \in L) \qquad gM(\beta)g^{-1} = \begin{pmatrix} \sigma_1(\beta) & \ldots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \ldots & \sigma_n(\beta) \end{pmatrix}$$

(cf. 5.3.1(i)).

(5.3.4) Proposition. *Soit $K(\alpha)/K$ une extension algébrique simple. Supposons que le polynôme minimal $f \in K[X]$ de α sur K soit séparable, de degré $n = \deg(f)$. Alors on a*

$$N_{K(\alpha)/K}(f'(\alpha)) = (-1)^{n(n-1)/2}\mathrm{disc}(f).$$

Preuve. Il existe une extension M/K telle que $\mathrm{Hom}_{K-\mathrm{Alg}}(L, M) = \{\sigma_1, \ldots, \sigma_n\}$; alors on a

$$N_{K(\alpha)/K}(f'(\alpha)) = \prod_{i=1}^{n}\sigma_i(f'(\alpha)) = \prod_{i=1}^{n} f'(\sigma_i(\alpha)) = \prod_{i=1}^{n} f'(\alpha_i),$$

où l'on a noté $\{\alpha_1, \ldots, \alpha_n\} = \{\sigma_1(\alpha), \ldots, \sigma_n(\alpha)\}$ l'ensemble de racines de f dans M. On en déduit que

$$N_{K(\alpha)/K}\,(f'(\alpha)) = \prod_{i=1}^{n} f'(\alpha_i) = \prod_{i=1}^{n}\prod_{j\neq i}(\alpha_i - \alpha_j) = (-1)^{(n-1)n/2}\prod_{i<j}(\alpha_i - \alpha_j)^2 = (-1)^{(n-1)n/2}\mathrm{disc}(f).$$

(5.3.5) Exemple : Soient p, q des variables, $K = \mathbf{Q}(p,q)$, $f(X) = X^3 + pX + q \in K[X]$, $K(\alpha) = K[X]/(f)$, $\alpha = \overline{X}$ (= l'image de X). Dans la base $1, \alpha, \alpha^2$ de $K(\alpha)/K$, la matrice $M(f'(\alpha)) = M(3\alpha^2 + p)$ est égale à

$$\begin{pmatrix} p & -3q & 0 \\ 0 & -2p & -3q \\ 3 & 0 & -2p \end{pmatrix},$$

puisque

$$\begin{aligned} (3\alpha^2 + p) \cdot 1 &= p \cdot 1 + 0 \cdot \alpha + 3 \cdot \alpha^2 \\ (3\alpha^2 + p) \cdot \alpha &= 3\alpha^3 + p\alpha = 3(-p\alpha - q) + p\alpha = -3q \cdot 1 - 2p \cdot \alpha + 0 \cdot \alpha^2 \\ (3\alpha^2 + p) \cdot \alpha^2 &= 0 \cdot 1 - 3q \cdot \alpha - 2p \cdot \alpha^2, \end{aligned}$$

donc

$$(-1)^{3\cdot 2/2}\mathrm{disc}(X^3 + pX + q) = \begin{vmatrix} p & -3q & 0 \\ 0 & -2p & -3q \\ 3 & 0 & -2p \end{vmatrix} = 4p^3 + 27q^2.$$

(5.3.6) Exercice. *Déterminer* $\mathrm{disc}(X^n + aX + b)$ $(n \geq 2)$.

(5.3.7) Définition. *Soient L/K une extension de degré fini et $\omega_1, \ldots, \omega_n$ $(n = [L : K])$ une base de L/K. Le* **discriminant** *de la base $\{\omega_i\}$ est défini comme*

$$D(\omega_1, \ldots, \omega_n) = \det(A), \qquad A = (A_{ij})_{1 \leq i,j \leq n} \in M_n(K), \qquad A_{ij} = Tr_{L/K}(\omega_i \omega_j).$$

(5.3.8) Exemples : (i) Si $L = K(\sqrt{d})$, $\omega_1 = 1$, $\omega_2 = \sqrt{d}$, alors on a

$$D(1, \sqrt{d}) = \begin{vmatrix} 2 & 0 \\ 0 & 2d \end{vmatrix} = 4d.$$

(ii) Si $\omega'_1, \ldots, \omega'_n$ est une autre base de L/K, alors on a

$$A' = (Tr_{L/K}(\omega'_i \omega'_j)) = {}^t g A g,$$

où $g = (g_{ij}) \in GL_n(K)$ est la matrice de changement de base:

$$\omega'_i = \sum_{k=1}^{n} g_{ki} \omega_k.$$

En particulier,

$$\begin{aligned} D(\omega'_1, \ldots, \omega'_n) &= \det(g)^2 D(\omega_1, \ldots, \omega_n) \\ D(\omega'_1, \ldots, \omega'_n) \neq 0 &\iff D(\omega_1, \ldots, \omega_n) \neq 0 \end{aligned}$$

(iii) Si l'extension L/K est séparable, il existe une extension M/K telle que $\mathrm{Hom}_{K-\mathrm{Alg}}(L, M) = \{\sigma_1, \ldots, \sigma_n\}$; alors on a

$$A_{ij} = \sum_{k=1}^{n} \sigma_k(\omega_i \omega_j) = \sum_{k=1}^{n} \sigma_k(\omega_i)\sigma_k(\omega_j) = \sum_{k=1}^{n} B_{ki} B_{kj},$$

$$A = {}^t B B, \qquad B = (B_{ij})_{1 \leq i,j \leq n} = (\sigma_i(\omega_j)) \in M_n(M), \qquad D(\omega_1, \ldots, \omega_n) = \det(B)^2.$$

(iv) Sous les hypothèses de (iii), il existe $\alpha \in L$ tel que $L = K(\alpha)$. Les éléments $1, \alpha, \ldots, \alpha^{n-1}$ forment une base de L/K et l'on a

$$D(1, \alpha, \ldots, \alpha^{n-1}) = \det(B)^2 = \begin{vmatrix} 1 & \alpha_1 & \cdots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \cdots & \alpha_2^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha_n & \cdots & \alpha_n^{n-1} \end{vmatrix}^2 = \prod_{i<j} (\alpha_i - \alpha_j)^2 = \mathrm{disc}(f) \neq 0,$$

où $\alpha_i = \sigma_i(\alpha) \in M$ sont les racines du polynôme minimal $f \in K[X]$ (séparable !) de α sur K.

(5.3.9) Proposition. *Soient L/K une extension de degré fini et $\omega_1, \ldots, \omega_n$ une base de L/K.*
(i) *Si L/K est séparable, alors on a $D(\omega_1, \ldots, \omega_n) \neq 0$.*
(ii) *Si L/K n'est pas séparable, alors on a $Tr_{L/K} = 0$ et $D(\omega_1, \ldots, \omega_n) = 0$.*

Preuve. (i) Ceci résulte de 5.3.8(ii) et (iv).
(ii) Il suffit de démontrer que $Tr_{L/K} = 0$. Fixons $\alpha \in L$ qui n'est pas séparable sur K. On déduit de 5.2.3(ii) que le polynôme minimal de α sur K s'écrit comme $f(X) = g(X^p)$ ($p = \mathrm{car}(K)$, $g \in K[X]$); alors on a $0 = f(\alpha) = g(\alpha^p)$, donc

$$p \cdot [K(\alpha^p) : K] \leq p \cdot \deg(g) = \deg(f) = [K(\alpha) : K].$$

D'autre part, α est une racine du polynôme $X^p - \alpha^p \in K(\alpha^p)[X]$ de degré p, donc

$$[K(\alpha) : K]/[K(\alpha^p) : K] = [K(\alpha) : K(\alpha^p)] \leq p.$$

On en déduit que $[K(\alpha) : K(\alpha^p)] = p$ et que $1, \alpha, \ldots, \alpha^{p-1}$ est une base de $K(\alpha)/K(\alpha^p)$. Comme

$$Tr_{L/K} = Tr_{K(\alpha^p)/K} \circ Tr_{K(\alpha)/K(\alpha^p)} \circ Tr_{L/K(\alpha)}$$

(d'après 3.2.15(iii)), il suffit de démontrer que $Tr_{K(\alpha)/K(\alpha^p)} = 0$. Soit $\beta = a_0 + a_1\alpha + \cdots + a_{p-1}\alpha^{p-1} \in K(\alpha)$ ($a_i \in K(\alpha^p)$). Les éléments diagonaux de la matrice $M(\beta)$ (par rapport à la base $1, \alpha, \ldots, \alpha^{p-1}$) sont tous égaux à a_0, donc $Tr_{K(\alpha)/K(\alpha^p)}(\beta) = pa_0 = 0$.

6. Groupes de Galois

(6.1) Extensions normales

(6.1.1) Exemples : (i) Il y a deux homomorphismes de corps (sur $\mathbf{Q}$) $\mathbf{Q}(\sqrt{2}) \longrightarrow \mathbf{C}$, à savoir

$$\sigma_0, \sigma_1 : \mathbf{Q}(\sqrt{2}) \longrightarrow \mathbf{C}, \qquad \sigma_j(a+b\sqrt{2}) = a + b(-1)^j\sqrt{2} \qquad\qquad (a, b \in \mathbf{Q}).$$

Leurs images dans $\mathbf{C}$ sont les mêmes: $\sigma_0(\mathbf{Q}(\sqrt{2})) = \sigma_1(\mathbf{Q}(\sqrt{2}))$.
(ii) Il y a trois homomorphismes de corps (sur $\mathbf{Q}$) $\mathbf{Q}(\sqrt[3]{2}) \longrightarrow \mathbf{C}$, à savoir

$$\tau_0, \tau_1, \tau_2 : \mathbf{Q}(\sqrt[3]{2}) \longrightarrow \mathbf{C}, \qquad \tau_j(a+b\sqrt[3]{2}+c\sqrt[3]{4}) = a + b\rho^j\sqrt[3]{2} + c\rho^{2j}\sqrt[3]{4} \qquad\qquad (a, b, c \in \mathbf{Q}).$$

Leurs images $\tau_j(\mathbf{Q}(\sqrt[3]{2}))$ dans $\mathbf{C}$ sont distinctes.

(6.1.2) Lemme-Définition. *Soit L/K une extension de degré fini. Les propriétés suivantes sont équivalents; si elles sont vérifiées, on dit que l'extension L/K est* **normale**.
(i) *Si $f \in K[X]$ est un polynôme irréductible (sur K) ayant une racine $\alpha_1 \in L$, alors f se décompose dans $L[X]$: $f(X) = c(X-\alpha_1)\cdots(X-\alpha_n)$ ($c \in K^*$, $\alpha_i \in L$); c'est-à-dire que si L contient une racine de f, il les contient toutes.*
(ii) *Si M/K est une extension de corps et $\sigma, \tau \in \mathrm{Hom}_{K-\mathrm{Alg}}(L, M)$, alors on a $\sigma(L) = \tau(L)$.*

Preuve. (i) $\Longrightarrow$ (ii): Soient M/K, σ, τ comme en (ii). Il suffit de démontrer que, pour tout $\alpha_1 \in L$, on a $\sigma(\alpha_1) \subseteq \tau(L)$. Soit $f \in K[X]$ le polynôme minimal de α_1 sur K; on a $f(X) = c(X-\alpha_1)\cdots(X-\alpha_n)$ dans $L[X]$ grâce à l'hypothèse (i). On obtient d'ici l'égalité

$$c\prod_{j=1}^{n}(X-\sigma(\alpha_j)) = {}^{\sigma}f(X) = f(X) = {}^{\tau}f(X) = c\prod_{j=1}^{n}(X-\tau(\alpha_j)) \tag{6.1.2.1}$$

de polynômes dans $M[X]$, ce qui entraîne qu'il existe $j = 1, \ldots, n$ tel que $\sigma(\alpha_1) = \tau(\alpha_j) \in \tau(L)$.
(ii) $\Longrightarrow$ (i): Soit f comme en (i). On note $K' \supset L$ un corps de décomposition de f sur L; on a alors $f(X) = c(X-\alpha_1)\cdots(X-\alpha_n)$ dans $K'[X]$. Il faut démontrer que toute racine $\alpha_j \in K'$ de f appartient à L. D'après 5.1.5(i) il existe un homomorphisme $\sigma_j \in \mathrm{Hom}_{K-\mathrm{Alg}}(K(\alpha_1), K')$ tel que $\sigma_j(\alpha_1) = \alpha_j$. D'après 5.2.4(iii) il existe une extension M/K' et un homomorphisme $\tau_j \in \mathrm{Hom}_{K-\mathrm{Alg}}(L, M)$ prolongeant σ_j. L'hypothèse (ii) alors montre que $\tau_j(L) = L$ (comme sous-corps de M), donc $\alpha_j = \sigma_j(\alpha_1) = \tau_j(\alpha_1) \in L$.

(6.1.3) Exemples : (i) L'extension $\mathbf{Q}(\sqrt{2})/\mathbf{Q}$ (resp., $\mathbf{Q}(\sqrt[3]{2})/\mathbf{Q}$) est (resp., n'est pas) normale.
(ii) Si L/K est normale et $K \subset F \subset L$, alors l'extension L/F est aussi normale.
(iii) Une extension de degré $[L:K] = 2$ est normale (exercise !).
(iv) Les extensions $\mathbf{Q}(\sqrt{2})/\mathbf{Q}$ et $\mathbf{Q}(\sqrt[4]{2})/\mathbf{Q}(\sqrt{2})$ sont normales, mais l'extension $\mathbf{Q}(\sqrt[4]{2})/\mathbf{Q}$ ne l'est pas.

(6.1.4) Proposition. *Soit L un corps de décomposition d'un polynôme $f \in K[X]$ de degré $n \geq 1$. Alors l'extension L/K est normale et $[L:K]$ divise $n!$.*

Preuve. On a $L = K(\alpha_1, \ldots, \alpha_n)$, où $f(X) = c(X-\alpha_1)\cdots(X-\alpha_n)$ dans $L[X]$. Soient M/K une extension et $\sigma, \tau \in \mathrm{Hom}_{K-\mathrm{Alg}}(L, M)$. Le même argument que plus haut montre l'égalité (6.1.2.1), d'où $\sigma(L) = K(\sigma(\alpha_1), \ldots, \sigma(\alpha_n)) = K(\tau(\alpha_1), \ldots, \tau(\alpha_n)) = \tau(L)$; l'extension L/K est donc normale.
On va établir la divisibilité $[L:K] \,|\, n!$ par récurrence; on peut supposer que $n > 1$. Si f est irréductible sur K, soit $\alpha \in L$ une racine de f. Alors $[K(\alpha):K] = n$ et L est un corps de décomposition du polynôme $f(X)/(X-\alpha)$ sur $K(\alpha)$. Comme $[L:K(\alpha)] \,|\, (n-1)!$ par l'hypothèse de récurrence, $[L:K]$ divise $n\cdot(n-1)! = n!$. Si $f = gh$ est réductible sur K ($g, h \in K[X]$, $1 \leq \deg(g) = d < n$), soit F un corps de décomposition de g sur K; alors L est un corps de décomposition de h sur F, donc $[F:K] \,|\, d!$ et $[L:F] \,|\, (n-d)!$, d'où $[L:K] \,|\, d!(n-d)! \,|\, n!$.

(6.1.5) Exemples (de corps de décomposition) : (i) Si $K \subset \mathbf{C}$, alors on a $L = K(\text{racines complexes de } f)$.∎
(ii) Si $K = \mathbf{Q}$ et $f(X) = X^3 - 2$, alors $L = \mathbf{Q}(\sqrt[3]{2}, \rho\sqrt[3]{2}, \rho^2\sqrt[3]{2}) = \mathbf{Q}(\sqrt[3]{2}, \rho)$ et $[L:K] = 6 = 3!$.
(iii) Si $K = \mathbf{Q}$ et $f(X) = X^4 - 2$, alors $L = \mathbf{Q}(\sqrt[4]{2}, i\sqrt[4]{2}, -\sqrt[4]{2}, -i\sqrt[4]{2}) = \mathbf{Q}(\sqrt[4]{2}, i)$ et $[L:K] = 8 | 24 = 4!$.

(6.2) Extensions galoisiennes

(6.2.1) Lemme-Définition. *Soit L/K une extension de corps.*
(i) *L'ensemble* $\mathrm{Aut}(L/K) = \mathrm{Isom}_{K-\mathrm{Alg}}(L,L)$ *est un groupe (par rapport à l'opération* $\sigma\tau = \sigma\circ\tau$*). On l'appelle le* **groupe d'automorphismes de l'extension** L/K.
(ii) *Pour tout sous-groupe* $G \subset \mathrm{Aut}(L/K)$*, l'ensemble* $L^G = \{\alpha \in L \,|\, (\forall g \in G) \quad g(\alpha) = \alpha\}$ *est un sous-corps de L contenant K; on l'appelle le* **corps fixe de** G.
(iii) *Si* $[L:K] < \infty$*, alors on a* $\mathrm{Aut}(L/K) = \mathrm{Hom}_{K-\mathrm{Alg}}(L,L)$.

Preuve. (ii) On a $K \subset L^G$ par définition. Si $\alpha, \beta \in L^G$ et $g \in G$, alors on a $g(\alpha \pm \beta) = g(\alpha) \pm g(\beta) = \alpha \pm \beta$, $g(\alpha\beta) = g(\alpha)g(\beta) = \alpha\beta$, $g(\alpha/\beta) = g(\alpha)/g(\beta)$ (si $\beta \neq 0$), donc $\alpha \pm \beta$, $\alpha\beta$ (et α/β si $\beta \neq 0$) appartiennent tous à L^G, ce qui démontre que L^G est un sous-corps de L.
(iii) Tout élément $\sigma \in \mathrm{Hom}_{K-\mathrm{Alg}}(L,L)$ est une application K-linéaire injective $\sigma : L \longrightarrow L$; comme $\dim_K(L) < \infty$, σ est surjective (donc bijective).

(6.2.2) Proposition-Définition. *Soit L/K une extension de corps de degré fini.*
(i) *On a* $|\mathrm{Aut}(L/K)| \leq [L:K]$.
(ii) $|\mathrm{Aut}(L/K)| = [L:K] \iff$ *l'extension L/K est normale et séparable. Si c'est le cas, on dit que l'extension L/K est* **galoisienne** *et on appelle* $\mathrm{Gal}(L/K) := \mathrm{Aut}(L/K)$ *le* **groupe de Galois** *de L/K (donc* $|\mathrm{Gal}(L/K)| = [L:K]$*). On dit que l'extension L/K est* **abélienne** *(resp.,* **cyclique***) si le groupe* $\mathrm{Gal}(L/K)$ *est abélien (resp., cyclique).*

Preuve. (i) On a $|\mathrm{Aut}(L/K)| \leq |\mathrm{Hom}_{K-\mathrm{Alg}}(L,L)| \leq [L:K]$, d'après 5.2.4(i).
(ii) Si $|\mathrm{Aut}(L/K)| = [L:K] = n$, alors L/K est séparable, d'après 5.2.4(ii). Soient M/K une extension et $\sigma, \tau \in \mathrm{Hom}_{K-\mathrm{Alg}}(L,M)$. Si l'on note $g_1, \ldots, g_n$ les éléments de $\mathrm{Aut}(L/K)$, alors $\sigma\circ g_1, \ldots, \sigma\circ g_n$ (resp., $\tau\circ g_1, \ldots, \tau\circ g_n$) sont des éléments distincts (puisque σ (resp., τ) est injectif) de $\mathrm{Hom}_{K-\mathrm{Alg}}(L,M)$. L'inégalité $|\mathrm{Hom}_{K-\mathrm{Alg}}(L,M)| \leq n$ de 5.2.4(i) montre qu'il existe $j \in \{1,\ldots,n\}$ tel que $\sigma\circ g_1 = \tau\circ g_j$, d'où $\tau(L) = \tau(g_j(L)) = \sigma(g_1(L)) = L$; l'extension L/K est donc normale. Réciproquement, si l'extension L/K est normale et séparable, alors il existe une extension M/K tel que $\mathrm{Hom}_{K-\mathrm{Alg}}(L,M) = \{\sigma_1, \ldots, \sigma_n\}$ ($n = [L:K]$); comme $\sigma_1(L) = \cdots = \sigma_n(L) \subset M$, on obtient n éléments distincts $g_i = \sigma_1^{-1}\circ\sigma_i \in \mathrm{Aut}(L/K)$. Il résulte de (i) que l'on a $|\mathrm{Aut}(L/K)| = n$.

(6.2.3) Corollaire-Définition. *Soit K un corps.*
(i) *Si $f \in K[X]$ est un polynôme séparable de degré $n \geq 1$ et L son corps de décomposition sur K, alors L/K est une extension galoisienne (de degré $[L:K] \,|\, n!$). On note* $\mathrm{Gal}(f) = \mathrm{Gal}(L/K)$.
(ii) *Si L/K est une extension galoisienne (de degré fini), alors L est un corps de décomposition sur K d'un polynôme séparable $f \in K[X]$ (ni f, ni son degré n'étant pas unique; cf. 6.2.5 ci-dessous).*

Preuve. (i) Ceci est une conséquence de 6.1.4 et 6.2.2(ii).
(ii) Il existe $\alpha \in L$ tel que $L = K(\alpha)$; on prend pour f le polynôme minimal de α sur K.

(6.2.4) Lemme (Groupes de Galois et groupes de permutations). *Soient K un corps, $f \in K[X]$ un polynôme séparable de degré $n \geq 1$ et L son corps de décomposition sur K; alors on a $f(X) = c(X-\alpha_1)\cdots(X-\alpha_n)$ dans $L[X]$ et $L = K(\alpha_1,\ldots,\alpha_n)$ (on a choisi une numérotation des racines de f).*
(i) *Pour tout $g \in \mathrm{Gal}(f) = \mathrm{Gal}(L/K)$, on a $f(g(\alpha_i)) = g(f(\alpha_i)) = 0$, donc g induit une permutation $\sigma_g \in S_n$ des racines de f: $g(\alpha_i) = \alpha_{\sigma_g(i)}$ $(1 \leq i \leq n)$.*
(ii) *L'application $g \mapsto \sigma_g$ est un homomorphisme injectif de groupes $\mathrm{Gal}(f) \longrightarrow S_n$; on peut donc identifier $\mathrm{Gal}(f)$ à un sous-groupe de S_n.*
(iii) *Si l'on change la numérotation des racines, $\mathrm{Gal}(f)$ sera remplacé par un sous-groupe conjugué.*
(iv) *Le polynôme f est irréductible sur $K \iff \mathrm{Gal}(f)$ agit transitivement sur les racines de f.*

Preuve. (i), (ii) Ceci est clair (si $(\forall i)\ \sigma_g(i) = i$, alors on a $(\forall i)\ g(\alpha_i) = \alpha_i$, donc $g(x) = x$ pour tout $x \in K(\alpha_1,\ldots,\alpha_n) = L$).
(iii) Après un changement de numérotation des racines $\alpha_i = \alpha'_{\tau(i)}$ (où $\tau \in S_n$) on a

$$\alpha'_{\sigma'_g(j)} = g(\alpha'_j) = g(\alpha_{\tau^{-1}(j)}) = \alpha_{\sigma_g\tau^{-1}(j)} = \alpha'_{\tau\sigma_g\tau^{-1}(j)} \Longrightarrow \sigma'_g = \tau\sigma_g\tau^{-1}\ (\forall g \in \mathrm{Gal}(f)).$$

(iv) L'ensemble des racines de chaque facteur irréductible de f (dans $K[X]$) est stable par l'action de $\mathrm{Gal}(f)$, ce qui démontre l'implication "$\Longleftarrow$". Si f est irréductible sur K et $\alpha_i, \alpha_j \in L$ sont deux racines de f, alors il existe in isomorphisme $\sigma \in \mathrm{Isom}_{K-\mathrm{Alg}}(K(\alpha_i), K(\alpha_j))$ tel que $\sigma(\alpha_i) = \alpha_j$ (d'après 3.5.4(vi)), une extension M/L et un homomorphisme $\tau \in \mathrm{Hom}_{K-\mathrm{Alg}}(L, M)$ prolongeant $\sigma : K(\alpha_i) \longrightarrow K(\alpha_j) \subset L$ (d'après 5.2.4(iii)). L'extension L/K étant normale, on a $\tau(L) = L$, donc $\tau \in \mathrm{Hom}_{K-\mathrm{Alg}}(L, L) = \mathrm{Aut}(L/K)$ (d'après 6.2.1(iii)) et $\tau(\alpha_i) = \sigma(\alpha_i) = \alpha_j$, d'où la transitivité.

(6.2.5) Exemples : (i) $K = \mathbf{Q}$, $f = X^3 - 2$, $n = 3$. Fixons une racine complexe $\alpha_1 = \sqrt[3]{2} \in \mathbf{C}$ de f et posons $\alpha_2 = \rho\alpha_1 = \rho\sqrt[3]{2}$, $\alpha_3 = \rho^2\alpha_1 = \rho^2\sqrt[3]{2}$. Alors $L = \mathbf{Q}(\alpha_1, \alpha_2, \alpha_3) = \mathbf{Q}(\alpha_1, \rho) = \mathbf{Q}(\sqrt[3]{2}, \rho)$. L'ordre du groupe de Galois $\mathrm{Gal}(L/\mathbf{Q}) \subset S_3$ est égal à $[L : \mathbf{Q}] = 6$ (cf. 3.2.7), donc $\mathrm{Gal}(L/\mathbf{Q}) = S_3$. On va noter

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \qquad \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \qquad \sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

les éléments d'ordre 2 dans S_3 et $H_j = \{1, \sigma_j\} \subset S_3$ $(j = 1, 2, 3)$ les sous-groupes d'ordre 2 engendrés par les σ_i. Pour chaque $j = 1, 2, 3$, on a $H_j \subset \mathrm{Aut}(L/\mathbf{Q}(\alpha_j))$ et $2 = |H_j| \leq |\mathrm{Aut}(L/\mathbf{Q}(\alpha_j))| \leq [L : \mathbf{Q}(\alpha_j)] = 2$, donc l'extension $L/\mathbf{Q}(\alpha_j)$ est galoisienne et $\mathrm{Gal}(L/\mathbf{Q}(\alpha_j)) = H_j$. Comme

$$\sigma_1(\rho) = \sigma_1(\alpha_2)/\sigma_1(\alpha_1) = \alpha_3/\alpha_1 = \rho^2, \qquad \sigma_2(\rho) = \sigma_2(\alpha_2)/\sigma_2(\alpha_1) = \alpha_2/\alpha_3 = \rho^2 \implies \sigma_1\sigma_2(\rho) = \rho,$$

le sous-groupe $H = \{1, \tau, \tau^2\} = A_3 \subset S_3$, où

$$\tau = \sigma_1\sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \qquad \tau^2 = \sigma_2\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix},$$

est contenu dans $\mathrm{Aut}(L/\mathbf{Q}(\rho))$. On a $3 = |H| \leq |\mathrm{Aut}(L/\mathbf{Q}(\rho))| \leq [L : \mathbf{Q}(\rho)] = 3$, donc l'extension $L/\mathbf{Q}(\rho)$ est aussi galoisienne et $H = \mathrm{Gal}(L/\mathbf{Q}(\rho))$. Par contre, les extensions $\mathbf{Q}(\alpha_j)/\mathbf{Q}$ ne sont pas galoisiennes (d'après 6.1.3(i)), mais $\mathbf{Q}(\rho)/\mathbf{Q} = \mathbf{Q}(\sqrt{-3})/\mathbf{Q}$ l'est.

(ii) Sous les hypothèses de (i), posons $\beta_1 = \sqrt[3]{2} + \rho$. Les images

$$\{g(\beta_1) \in L \,|\, g \in S_3\} = \{\sqrt[3]{2} + \rho,\, \sqrt[3]{2} + \rho^2,\, \rho\sqrt[3]{2} + \rho,\, \rho\sqrt[3]{2} + \rho^2,\, \rho^2\sqrt[3]{2} + \rho,\, \rho^2\sqrt[3]{2} + \rho^2\} = \{\beta_1, \ldots, \beta_6\}$$

sont distinctes, donc β_1 a au moins $6 = [L : \mathbf{Q}]$ conjugués, d'où $L = \mathbf{Q}(\beta_1)$. Il en résulte que $F(X) = (X - \beta_1) \cdots (X - \beta_6)$ est le polynôme minimal de β_j $(j = 1, \ldots, 6)$ sur $\mathbf{Q}$ et L est son corps de décomposition (sur $\mathbf{Q}$). L'action du groupe $G = \mathrm{Gal}(L/\mathbf{Q})$ sur les racines de $F(X)$ permet de réaliser G comme un sous-groupe de S_6; bien sûr, G est isomorphe à S_3, d'après (i).

(iii) $K = \mathbf{Q}$, $f = (X^2 - 2)(X^2 - 3)$, $n = 4$. Les racines complexes de f sont $\alpha_1 = \sqrt{2}, \alpha_2 = -\sqrt{2}, \alpha_3 = \sqrt{3}, \alpha_4 = -\sqrt{3}$, $L = \mathbf{Q}(\alpha_1, \alpha_2, \alpha_3, \alpha_4) = \mathbf{Q}(\sqrt{2}, \sqrt{3})$. On a $[L : \mathbf{Q}] = 4$ (d'après 3.2.8(iv)), donc $|\mathrm{Gal}(L/\mathbf{Q})| = 4$. L'action de tout élément $g \in \mathrm{Gal}(L/\mathbf{Q})$ étant déterminée par les valeurs $g(\sqrt{2}) = \pm\sqrt{2}$ et $g(\sqrt{3}) = \pm\sqrt{3}$, on obtient que

$$\mathrm{Gal}(L/\mathbf{Q}) = \{g_{ab}, \,|\, a, b \in \mathbf{Z}/2\mathbf{Z}\}, \qquad g_{ab}(\sqrt{2}) = (-1)^a\sqrt{2}, \qquad g_{ab}(\sqrt{3}) = (-1)^b\sqrt{3}.$$

Comme $g_{ab}^2 = 1$ et $g_{ab}g_{cd} = g_{a+c,b+d}$, l'application

$$\mathrm{Gal}(L/\mathbf{Q}) \xrightarrow{\sim} \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}, \qquad g_{ab} \mapsto (a, b)$$

est un isomorphisme de groupes. Pour la numérotation des racines ci-dessus, on a $\mathrm{Gal}(L/\mathbf{Q}) \subset S_4$, où

$$g_{00} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \qquad g_{10} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}, \qquad g_{01} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix}, \qquad g_{11} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}.$$

(iv) Le même corps $L = \mathbf{Q}(\sqrt{2}, \sqrt{3})$ est un corps de décomposition (sur $\mathbf{Q}$) du polynôme minimal $F(X) = X^4 - 10X^2 + 1$ (sur $\mathbf{Q}$) de $\beta_1 = \sqrt{2} + \sqrt{3} \in L$; on a $F(X) = (X - \beta_1) \cdots (X - \beta_4)$, où $\beta_2 = -\sqrt{2} + \sqrt{3} = 1/\beta_1$, $\beta_3 = -\sqrt{2} - \sqrt{3} = -\beta_1$, $\beta_4 = \sqrt{2} - \sqrt{3} = -\beta_2 = -1/\beta_1$. Les formules

$$g_{10} : \beta_1 \longleftrightarrow \beta_2, \qquad g_{10} : \beta_3 \longleftrightarrow \beta_4, \qquad g_{10} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$$

$$g_{01} : \beta_1 \longleftrightarrow \beta_4, \qquad g_{01} : \beta_2 \longleftrightarrow \beta_3, \qquad g_{01} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$$

$$g_{11} : \beta_1 \longleftrightarrow \beta_3, \qquad g_{11} : \beta_2 \longleftrightarrow \beta_4, \qquad g_{11} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$$

donnent une autre réalisation du groupe $\mathrm{Gal}(L/\mathbf{Q})$ comme un sous-groupe de S_4. Les deux sous-groupes de S_4 ainsi construits sont isomorphes à $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$, mais ils ne sont pas conjugués. En effet, le sous-groupe en (iii) n'est pas transitif mais celui en (iv) l'est (grâce à 6.2.4(iv)).

(6.3) La correspondence de Galois

(6.3.1) Rappel : sous-groupes distingués. Soit G un groupe. Un sous-groupe $H \subset G$ est dit **distingué** (notation: $H \lhd G$) si l'on a

$$(\forall g \in G) \quad gHg^{-1} = H \iff (\forall g \in G) \quad gH = Hg,$$

où l'on a noté

$$gHg^{-1} = \{ghg^{-1} \,|\, h \in H\}, \qquad gH = \{gh \,|\, h \in H\}, \qquad Hg = \{hg \,|\, h \in H\}.$$

En particulier, tout sous-groupe d'un groupe abélien est distingué. Si $f : G \longrightarrow K$ est un homomorphisme de groupes, alors son noyau $H = \mathrm{Ker}(f) = \{g \in G \,|\, f(g) = e_K\}$ est un sous-groupe distingué de G. Réciproquement, si $H \lhd G$, alors l'ensemble $G/H = \{gH \,|\, g \in G\}$ est un groupe par rapport à l'opération $gH \cdot g'H = gg'H$, l'application $\pi(g) = gH$ est un homomorphisme surjectif de groupes $\pi : G \longrightarrow G/H$ et $\mathrm{Ker}(\pi) = H$.

Pour tout homomorphisme de groupes $f : G \longrightarrow K$, posons $H = \mathrm{Ker}(f)$. L'application $\overline{f} : G/H \longrightarrow K$, $\overline{f}(gH) = f(g)$, alors induit un isomorphisme de groupes $\overline{f} : G/\mathrm{Ker}(f) \xrightarrow{\sim} \mathrm{Im}(f) = \{f(g) \,|\, g \in G\}$.

(6.3.2) Théorème (E. Artin). *Soient L/K une extension de corps et $G \subset \mathrm{Aut}(L/K)$ un groupe fini d'automorphismes de L sur K. Alors $[L : L^G] = |G|$, l'extension L/L^G est galoisienne et $G = \mathrm{Gal}(L/L^G)$.*

Preuve. Fixons $a \in L$ et posons $A = \{g(a) \,|\, g \in G\}$, $f_a(X) = \prod_{b \in A}(X - b) \in L[X]$. Pour tout $g \in G$, l'action de g induit une permutation de A, donc ${}^g f_a = f_a$; on en déduit que $f_a \in L^G[X]$. Le polynôme f étant séparable et $f(a) = 0$, l'extension L/K est algébrique et séparable. Comme $\deg(f_a) \leq |G|$ pour tout $a \in L$, il résulte de 5.2.10 que $[L : L^G] \leq |G|$. D'autre part, $K \subset L^G$, donc $G \subset \mathrm{Aut}(L/L^G) \subset \mathrm{Aut}(L/K)$. Comme $[L : L^G] < \infty$, on a $|G| \leq |\mathrm{Aut}(L/L^G)| \leq [L : L^G]$ (d'après 5.2.4(i)), d'où $|G| = |\mathrm{Aut}(L/L^G)| = [L : L^G]$ et $G = \mathrm{Aut}(L/L^G)$.

(6.3.3) Corollaire. *Si L/K est une extension galoisienne (de degré fini) et $G = \mathrm{Gal}(L/K)$, alors on a $K = L^G$.*

Preuve. On a $K \subset L^G$, mais $[L : K] = |G| = [L : L^G]$ (d'après 6.2.2(ii) et 6.3.2).

(6.3.4) Exemple : Soit K un corps, $L = K(x_1, \ldots, x_n)$ le corps de fonctions rationnelles en n variables sur K et $G = S_n \subset \mathrm{Aut}(L/K)$ agissant sur L (à gauche) comme en 1.7.2. D'après 1.7.9, $L^G = K(\sigma_1, \ldots, \sigma_n)$. On déduit de 6.3.2 que l'extension $K(x_1, \ldots, x_n)/K(\sigma_1, \ldots, \sigma_n)$ est galoisienne de degré $|S_n| = n!$ et que son groupe de Galois est égal à S_n.

(6.3.5) Théorème Fondamental de Théorie de Galois. *Soit L/K une extension galoisienne (de degré fini); posons $G = \mathrm{Gal}(L/K)$.*
(i) *Les formules $F \mapsto H = \mathrm{Gal}(L/F)$, $H \mapsto F = L^H$ définissent des bijections inverses l'une de l'autre entre les ensembles*

$$\{F \text{ corps} \,|\, K \subset F \subset L\} \longleftrightarrow \{\text{sous} - \text{groupes } H \subset G\}$$

("correspondence de Galois"). En particulier, toutes les extensions L/F sont galoisiennes.
(ii) *Si F correspond à H, alors on a* $[L : F] = |H|$, $[F : K] = |G|/|H| = (G : H)$.
(iii) *Si F_1 (resp., F_2) correspond à H_1 (resp., H_2), alors on a*

$$F_1 \subset F_2 \iff H_1 \supset H_2.$$

(iv) *Si F correspond à H, alors* $(\forall g \in G)$ $g(F)$ *correspond à* gHg^{-1}.
(v) *Si F correspond à H, alors*

$$\text{l'extension } F/K \text{ est galoisienne} \iff H \text{ est un sous} - \text{groupe distingué de } G.$$

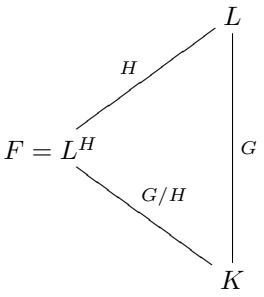
Si c'est le cas, l'application "restriction à F" définit un homomorphisme surjectif de groupes

$$G = \mathrm{Gal}(L/K) \longrightarrow \mathrm{Gal}(F/K), \qquad g \mapsto g_{|F},$$

à noyau $H = \mathrm{Gal}(L/F)$, donc un isomorphisme de groupes

$$G/H = \mathrm{Gal}(L/K)/\mathrm{Gal}(L/F) \xrightarrow{\sim} \mathrm{Gal}(F/K).$$

On peut résumer cet énoncé dans le diagramme suivant:



Preuve. (i) Soit $H \subset G$ un sous-groupe de G; posons $F = L^H$. On a $K = L^G \subset L^H = F \subset L$. D'après 6.3.2, l'extension L/F est galoisienne, $H = \mathrm{Gal}(L/F)$ et $[L : F] = |H|$. Réciproquement, si F est un corps, $K \subset F \subset L$, alors l'extension L/F est séparable et normale, d'après 5.2.2(iii) et 6.1.3(ii), respectivement; elle est donc galoisienne. Posons $H = \mathrm{Aut}(L/F) = \mathrm{Gal}(L/F)$; alors on a $L^H = F$ (d'après 6.3.3) et $[L : F] = |H|$.
(ii) On vient de démontrer que $[L : F] = |H|$, donc $[F : K] = [L : K]/[L : F] = |G|/|H| = (G : H)$.
(iii) Ceci est clair.
(iv) Soient $g, h \in G$. Un élément $x \in L$ est fixé par $h \iff g(x)$ est fixé par ghg^{-1}, car $ghg^{-1}g(x) = gh(x)$; il en résulte que

$$L^{gHg^{-1}} = g(L^H).$$

(v) Si l'extension $F/K = L^H/K$ est galoisienne, alors elle est normale, donc $(\forall g \in G)$ $g(F) = \mathrm{id}(F) = F$; on déduit de (iv) que $(\forall g \in G)$ $gHg^{-1} = H$. Réciproquement, si $H \lhd G$ et $F = L^H$, alors pour tout $g \in G$ la restriction $g_{|F} : F \longrightarrow g(F) \overset{(iv)}{=} F$ est un élément de $\mathrm{Aut}(F/K)$. L'application $g \mapsto g_{|F}$ est un homomorphisme de groupes $r : G \longrightarrow \mathrm{Aut}(F/K)$ avec noyau $\mathrm{Ker}(r) = \mathrm{Aut}(L/F) = H$. Il en résulte que

$$[F : K] \geq |\mathrm{Aut}(F/K)| \geq |\mathrm{Im}(r)| = |G|/|\mathrm{Ker}(r)| = |G|/|H| = [F : K],$$

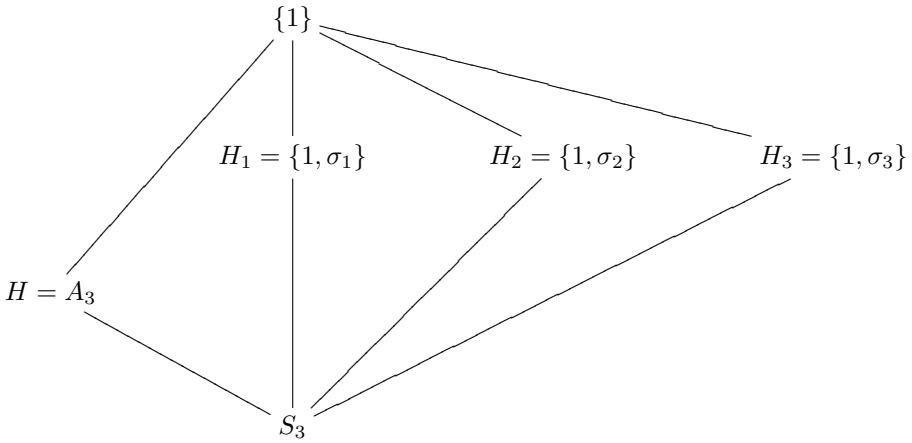
donc $[F : K] = |\mathrm{Aut}(F/K)| = |\mathrm{Im}(r)|$, ce qui démontre (v).

(6.3.6) Corollaire. *Si $F = L^H$, fixons $g_1, \ldots, g_m \in G$ ($m = (G : H) = |G|/|H| = [F : K]$) tels que $G = g_1 H \cup \cdots \cup g_m H$; alors on a*

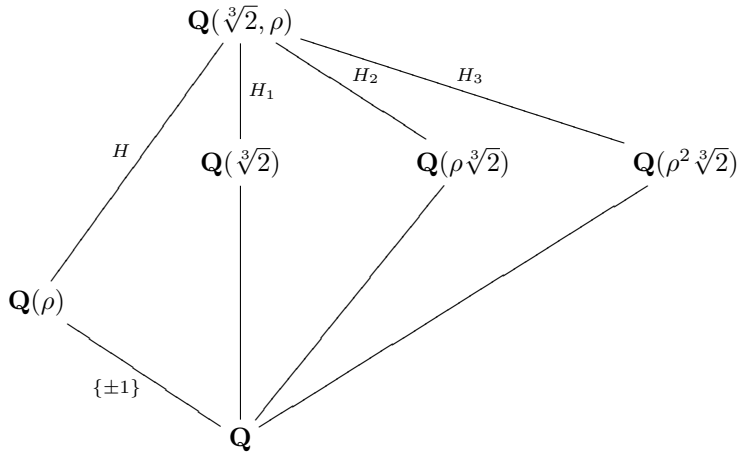
$$(\forall \beta \in L) \qquad Tr_{L/F}(\beta) = \sum_{h \in H} h(\beta), \qquad N_{L/F}(\beta) = \prod_{h \in H} h(\beta)$$
$$(\forall \alpha \in F) \qquad Tr_{F/K}(\alpha) = \sum_{i=1}^{m} g_i(\alpha), \qquad N_{F/K}(\alpha) = \prod_{i=1}^{m} g_i(\alpha).$$

Preuve. Proposition 5.3.2 s'applique, avec $\mathrm{Hom}_{F-\mathrm{Alg}}(L, L) = H$ et $\mathrm{Hom}_{K-\mathrm{Alg}}(F, L) = \{g_1, \ldots, g_m\}$; c'est-à-dire que l'ensemble des conjugués de β sur F (resp., de α sur K) est égal à $\{h(\beta) \,|\, h \in H\}$ (resp., $\{g_1(\alpha), \ldots, g_m(\alpha)\}$).

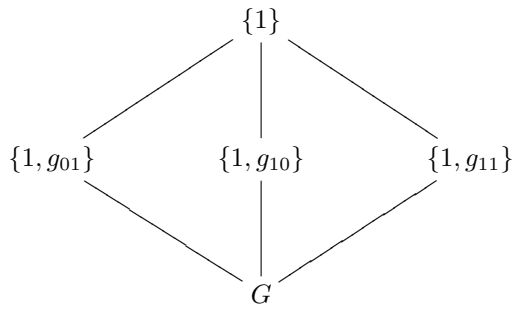
(6.3.7) Exemples : (i) D'après 6.2.5(i), les sous-groupes de S_3

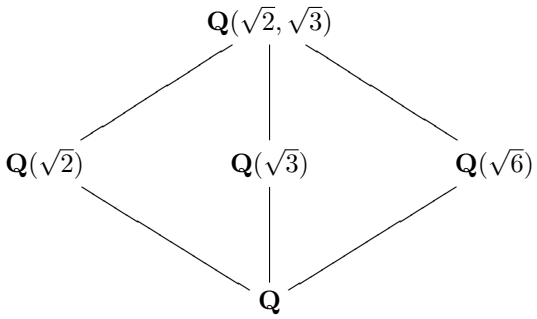


correspondent aux sous-corps $\mathbf{Q} \subset F \subset \mathbf{Q}(\sqrt[3]{2}, \rho)$:



On a $H = A_3 \lhd S_3$, mais $H_j \not\lhd S_3$ ($j = 1, 2, 3$); l'application sgn : $S_3 \longrightarrow \{\pm 1\}$ induit un isomorphisme de groupes $\mathrm{Gal}(\mathbf{Q}(\rho)/\mathbf{Q}) = S_3/H = S_3/A_3 \xrightarrow{\sim} \{\pm 1\}$.
(ii) Soit $L/K = \mathbf{Q}(\sqrt{2}, \sqrt{3})/\mathbf{Q}$. Les sous-groupes de $G = \mathrm{Gal}(\mathbf{Q}(\sqrt{2}, \sqrt{3})/\mathbf{Q}) = \{g_{00}, g_{01}, g_{10}, g_{11}\} \xrightarrow{\sim} \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ (cf. 6.2.5(iii)) correspondent aux sous-corps $\mathbf{Q} \subset F \subset \mathbf{Q}(\sqrt{2}, \sqrt{3})$:





(6.4) Exemples de groupes de Galois

(6.4.1) Proposition. *Si K est un corps et $f \in K[X]$ un polynôme séparable unitaire de degré $n \geq 1$, alors on a:*

$$\mathrm{Gal}(f) \subset A_n \iff \mathrm{disc}(f) \in K^{*2}.$$

Preuve. Soient L un corps de décomposition de f sur K et $\alpha_1, \ldots, \alpha_n \in L$ les racines de f. On a

$$\mathrm{disc}(f) = d^2, \qquad d = \prod_{i<j}(\alpha_i - \alpha_j) \in L^*, \qquad (\forall g \in \mathrm{Gal}(f)) \quad g(d) = \mathrm{sgn}(g)d,$$

donc

$$\mathrm{disc}(f) \in K^{*2} \iff d \in K^* \iff d \in (L^{\mathrm{Gal}(f)})^* \iff (\forall g \in \mathrm{Gal}(f)) \quad \mathrm{sgn}(g) = 1 \iff \mathrm{Gal}(f) \subset A_n.$$

(6.4.2) Corollaire. *Soient K un corps et $f \in K[X]$ un polynôme unitaire irréductible de degré* $\deg(f) = 3$. *Si* $\mathrm{disc}(f) \neq 0$ *(ce qui est automatique si* $\mathrm{car}(K) \neq 3$, *d'après 5.2.3(i)), alors on a*

$$\mathrm{Gal}(f) = \begin{cases} A_3, & \mathrm{disc}(f) \in K^{*2} \\ S_3, & \mathrm{disc}(f) \notin K^{*2} \end{cases}$$

Plus précisement, on a la tour d'extensions

$$K \subset K(\sqrt{\mathrm{disc}(f)}) \subset L, \qquad \mathrm{Gal}(L/K(\sqrt{\mathrm{disc}(f)})) = A_3.$$

Preuve. L'ordre de $\mathrm{Gal}(f) \subset S_3$ est divisible par $[K(\alpha_1) : K] = 3$, donc $\mathrm{Gal}(f) = A_3$ ou S_3. On applique 6.4.1 et le fait que $d = \sqrt{\mathrm{disc}(f)}$ appartient à L^{A_3}.

(6.4.3) Lemme. *Soient p un nombre premier et $G \subset S_p$ un sous-groupe de S_p.*
(i) *Si l'action de G sur $\{1, \ldots, p\}$ est transitive, alors G contient un p-cycle (= un cycle de longeur p).*
(ii) *Si G contient un p-cycle et un 2-cycle, alors on a $G = S_p$.*

Preuve. On va utiliser trois résultats de la théorie des groupes finis:
(A) Soient G un groupe fini agissant sur un ensemble X et $x \in X$; posons $G_x = \{g \in G \,|\, g(x) = x\}$ ("le fixateur de x") et $O(x) = \{g(x) \,|\, g \in G\}$ ("l'orbite de x"). Alors $|G| = |G_x| \cdot |O(x)|$; en particulier, $|O(x)|$ divise $|G|$.
(B) Si G est un groupe fini et p un nombre premier qui divise $|G|$, alors G possède un élément d'ordre p ("Théorème de Cauchy").
(C) Le groupe S_n ($n \geq 2$) est engendré par les 2-cycles $(12), (23), \ldots, (n-1\,n)$.
(i) L'action de G sur $\{1, \ldots, p\}$ étant transitive, $\{1, \ldots, p\}$ est la seule orbite; il résulte de (A) que p divise $|G|$, donc G possède un élément d'ordre p. Mais les seules éléments d'ordre p dans S_p sont les p-cycles.
(ii) On peut supposer que G contient $c = (12 \cdots p)$ et $s = (ij)$ $(i < j)$. On va idéntifier $\{1, \ldots, p\}$ avec $\mathbf{F}_p$; pour tout $k \in \mathbf{Z}$, on a $c^{(j-i)k} s c^{(i-j)k} = (j_k j_{k+1}) \in G$, où l'on a noté $j_k = i + (j-i)k \in \mathbf{F}_p$. Comme $\mathbf{F}_p = \{j_1, \ldots, j_p\}$, les 2-cycles $(j_1 j_2), \ldots (j_{p-1} j_p)$ engendrent S_p.

(6.4.4) Corollaire. *Soient p un nombre premier, K un sous-corps de $\mathbf{R}$ et $f \in K[X]$ un polynôme irréductible de degré p. Posons $L = K(\alpha_1, \ldots, \alpha_p)$, où $\alpha_1, \ldots, \alpha_p \in \mathbf{C}$ sont les racines complexes de f. Si $\alpha_1, \alpha_2 \notin \mathbf{R}$ et $\alpha_3, \ldots, \alpha_p \in \mathbf{R}$, alors on a $\mathrm{Gal}(f) = \mathrm{Gal}(L/K) = S_p$.*

Preuve. L'action de $\mathrm{Gal}(f)$ sur $\{1, \ldots, p\}$ est transitive, puisque f est irréductible; le groupe $\mathrm{Gal}(f) \subset S_p$ donc contient un p-cycle, d'après 6.4.3(i). Comme $K \subset \mathbf{R}$, la conjugaison complexe $c(a+bi) = a-bi$ $(a, b \in \mathbf{R})$ définit un élément de $c \in \mathrm{Hom}_{K-\mathrm{Alg}}(L, c(L)) = \mathrm{Hom}_{K-\mathrm{Alg}}(L, L) = \mathrm{Gal}(L/K) = \mathrm{Gal}(f)$ (l'extension L/K étant normale, on a $c(L) = L$). Les hypothèses sur les racines de f entraînent que c agit sur $\{1, \ldots, p\}$ comme un 2-cycle; on peut donc appliquer 6.4.3(ii).

(6.4.5) Exemple : Le polynôme $f(X) = X^5 - 6X + 2 \in \mathbf{Q}[X]$ est irréductible sur $\mathbf{Q}$, d'après le critère d'Eisenstein. Comme f a 3 racines réelles, son groupe de Galois (sur $\mathbf{Q}$) est égal à $\mathrm{Gal}(f) = S_5$.

(6.4.6) Théorème. *Soit $f \in \mathbf{Z}[X]$ un polynôme unitaire de degré $n \geq 1$. Soit p un nombre premier; on note $\overline{f} = f \pmod p \in \mathbf{F}_p[X]$ la réduction de f modulo p. On suppose que $\overline{f}$ est séparable ($\iff p \nmid \mathrm{disc}(f)$) et on écrit $\overline{f} = \overline{f}_1 \cdots \overline{f}_r$, où chaque $\overline{f}_i \in \mathbf{F}_p[X]$ est un polynôme irréductible (sur $\mathbf{F}_p$) de degré n_i $(n_1 + \cdots + n_r = n)$. Alors le polynôme f est séparable et $\mathrm{Gal}(f) \subset S_n$ contient un élément $c_1 \cdots c_r$, où $c_1, \ldots, c_r$ sont des cycles à supports disjoints, de longeurs $n_1, \ldots, n_r$.*

"Preuve". Si'l y a assez de temps, on va démontrer un résultat plus général dans la deuxième partie du cours.

(6.4.7) Exemple : Soit $f(X) = X^5 - X + 1 \in \mathbf{Q}[X]$; posons $G = \mathrm{Gal}(f)$ (sur $\mathbf{Q}$). La factorisation $f \pmod 2 = (X^2 + X + 1)(X^3 + X^2 + 1)$ (voir 4.1.3(iii)) montre que $G \subset S_5$ contient un élément de la forme $g = (ab)(cde)$, donc aussi le 2-cycle $g^3 = (ab)$. On peut vérifier que le polynôme $f \pmod 3 \in \mathbf{F}_3[X]$ est irréductible sur $\mathbf{F}_3$ (par exemple, l'algorithme de division montre que $\mathrm{pgcd}(f(X), X^9 - X) = 1$, donc f n'a aucun facteur irréductible de degré 1 ou 2, d'après 4.1.2(ii)). Il résulte de 6.4.6 que G aussi contient un 5-cycle, donc $G = S_5$, d'après 6.4.3(ii). On peut également vérifier que $f \pmod 5 \in \mathbf{F}_5[X]$ est irréductible sur $\mathbf{F}_5$:

(6.4.8) Exercice. *Si p est un nombre premier et $a \in \mathbf{F}_p^*$, alors le polynôme $f(X) = X^p - X + a$ est irréductible dans $\mathbf{F}_p[X]$. [Indication: $f(X+1) = f(X)$.]*

(6.4.9) Exemples de groupes finis : (i) Le groupe cyclique d'ordre $n \geq 1$: $C_n = \{\sigma, \sigma^2, \ldots, \sigma^n = 1\}$.
(ii) Le groupe diédral d'ordre $2n \geq 4$: $D_{2n} = C_n \cup \tau C_n$, où $\tau^2 = 1, \tau\sigma\tau^{-1} = \sigma^{-1}$. Le groupe D_{2n} est le groupe des isométries d'un polygone régulier à n côtés. L'action de D_{2n} sur les sommets du polygone définit un homomorphisme injectif de groupes $D_{2n} \hookrightarrow S_n$. Par exemple, $D_8 \subset S_4$ contient un 4-cycle σ et un 2-cycle τ, mais $D_8 \neq S_4$.
(iii) Le groupe $GL_n(R)$ des matrices inversibles $(n \times n)$ sur un anneau (commutatif, unitaire) fini R.
(iv) Son sous-groupe $SL_n(R) = \{g \in GL_n(R) \,|\, \det(g) = 1\}$.
(v) Le groupe d'isomorphismes affines $R^n \xrightarrow{\sim} R^n$ sur un anneau fini R:

$$GA_n(R) = \{x \mapsto Ux + a \ (x \in R^n) \,|\, U \in GL_n(R),\, a \in R^n\}.$$

La formule $f(x \mapsto Ux + a) = U$ définit un homomorphisme surjectif de groupes

$$f : GA_n(R) \longrightarrow GL_n(R),$$

dont le noyau est égal au groupe des translations $x \mapsto x + a$, isomorphe à $(R^n, +)$. Comme

$$U(Vx + b) + a = UVx + (Ub + a), \qquad \begin{pmatrix} U & a \\ 0 & 1 \end{pmatrix} \begin{pmatrix} V & b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} UV & Ub + a \\ 0 & 1 \end{pmatrix},$$

on peut aussi considérer $GA_n(R)$ comme le sous-groupe

$$\left\{ \begin{pmatrix} U & a \\ 0 & 1 \end{pmatrix} \,\middle|\, U \in GL_n(R),\, a \in R^n \right\} \subset GL_{n+1}(R).$$

(vi) En particulier, l'action naturelle du groupe

$$GA_1(R) = \{x \mapsto ux + a \ (x \in R) \,|\, u \in R^*,\, a \in R\} \xrightarrow{\sim} \left\{ \begin{pmatrix} u & a \\ 0 & 1 \end{pmatrix} \,\middle|\, u \in R^*,\, a \in R \right\} \subset GL_2(R)$$

sur R définit un homomorphisme injectif de groupes $GA_1(R) \hookrightarrow S_{|R|}$ (dès que l'on choisit une numérotation des éléments de R).

Par exemple, si p est un nombre premier et $R = \mathbf{F}_p$, on obtient ainsi un sous-groupe $GA_1(\mathbf{F}_p) \subset S_p$ d'ordre $|\mathbf{F}_p^*| \cdot |\mathbf{F}_p| = p(p-1)$.

Un autre exemple : pour tout entier $n \geq 2$, le sous-groupe

$$\{x \mapsto \pm x + a \ (x \in \mathbf{Z}/n\mathbf{Z}) \,|\, a \in \mathbf{Z}/n\mathbf{Z}\} \xrightarrow{\sim} \left\{ \begin{pmatrix} \pm 1 & a \\ 0 & 1 \end{pmatrix} \,\middle|\, a \in R \right\} \subset GA_1(\mathbf{Z}/n\mathbf{Z})$$

est isomorphe à D_{2n}. En particulier, $GA_1(\mathbf{Z}/n\mathbf{Z}) \xrightarrow{\sim} D_{2n}$ pour $n = 3, 4, 6$.

(6.4.10) Exercice. *Montrer qu'un sous-groupe G transitif de S_4 (resp., de S_5) est isomorphe à $C_2 \times C_2, C_4, D_8, A_4$ ou S_4 (resp., à $C_5, D_{10}, GA_1(\mathbf{F}_5), A_5$ ou S_5). La réciproque est vrai, si $G \neq C_2 \times C_2$ (cf. 6.2.5(iii)).*

(6.4.11) Exercice. *Soient K un corps et $f \in K[X]$ un polynôme irréductible séparable de degré $\deg(f) = 4$; posons $F = K[X]/(f)$ (donc $[F : K] = 4$). Montrer que:*

$$\text{il existe un corps } K \subset E \subset F \text{ tel que } [E : K] = 2 \iff \mathrm{Gal}(f) = C_2 \times C_2, C_4 \text{ ou } D_8.$$

(6.5) Corps finis

(6.5.1) Théorème. *Soient p un nombre premier et $n \geq 1$ un entier.*
(i) *L'extension $\mathbf{F}_{p^n}/\mathbf{F}_p$ est galoisienne. Son groupe de Galois est cyclique d'ordre n, engendré par l'application de Frobenius $\varphi(x) = x^p$, $\mathrm{Gal}(\mathbf{F}_{p^n}/\mathbf{F}_p) = \{\varphi, \varphi^2, \ldots, \varphi^n = 1\}$.*
(ii) *Tout sous-groupe de $\mathrm{Gal}(\mathbf{F}_{p^n}/\mathbf{F}_p)$ est cyclique d'ordre n/m (où m est un diviseur de n), engendré par φ^m. Son corps fixe est égal à $\mathbf{F}_{p^m}$ et on a $\mathrm{Gal}(\mathbf{F}_{p^n}/\mathbf{F}_{p^m}) = \{\varphi^m, \varphi^{2m}, \ldots, \varphi^{\frac{n}{m} \cdot m} = 1\}$.*

Preuve. (i) Pour tous $m = 1, \ldots, n-1$, on a

$$|\{x \in \mathbf{F}_{p^n} \,|\, \varphi^m(x) = x\}| = |\{\text{racines de } X^{p^m} - X \text{ dans } \mathbf{F}_{p^n}\}| \leq \deg(X^{p^m} - X) = p^m < p^n,$$

donc $\varphi, \varphi^2, \ldots, \varphi^{n-1} \neq 1 \in \mathrm{Aut}(\mathbf{F}_{p^n}/\mathbf{F}_p)$. On en déduit que

$$n = |\{\varphi, \varphi^2, \ldots, \varphi^n = 1\}| \leq |\mathrm{Aut}(\mathbf{F}_{p^n}/\mathbf{F}_p)| \leq [\mathbf{F}_{p^n} : \mathbf{F}_p)] = n,$$

d'où les égalité $\{\varphi, \varphi^2, \ldots, \varphi^n = 1\} = \mathrm{Aut}(\mathbf{F}_{p^n}/\mathbf{F}_p) = \mathrm{Gal}(\mathbf{F}_{p^n}/\mathbf{F}_p)$.
(ii) Il est bien connu que tout sous-groupe H du groupe cyclique d'ordre n engendré par φ est aussi cyclique, engendré par φ^m (où $m|n$). D'après 4.3.1(ii), le corps fixe de H est égal à

$$\mathbf{F}_{p^n}^H = \{x \in \mathbf{F}_{p^n} \,|\, x^{p^m} = x\} = \mathbf{F}_{p^m},$$

donc $\mathrm{Gal}(\mathbf{F}_{p^n}/\mathbf{F}_{p^m}) = H$ d'après 6.3.2.

(6.5.2) Corollaire. *Sous les hypothèses de 6.5.1, soient $q = p^m$ une puissance de p et $d \geq 1$ un entier. Alors:* (i) *Le groupe* $\mathrm{Gal}(\mathbf{F}_{q^d}/\mathbf{F}_q)$ *est cyclique d'ordre d, engendré par $\varphi_q(x) = \varphi^m(x) = x^q$.*
(ii) $(\forall x \in \mathbf{F}_{q^d}^*) \quad N_{\mathbf{F}_{q^d}/\mathbf{F}_q}(x) = x^{1+q+\cdots+q^{d-1}} = x^{(q^d-1)/(q-1)}$.
(iii) *Si x engendre $\mathbf{F}_{q^d}^*$, alors sa norme $N_{\mathbf{F}_{q^d}/\mathbf{F}_q}(x)$ engendre $\mathbf{F}_q^*$. En particulier, l'homomorphisme $N_{\mathbf{F}_{q^d}/\mathbf{F}_q} : \mathbf{F}_{q^d}^* \longrightarrow \mathbf{F}_q^*$ est surjectif.*

Preuve. (i) Ceci est une réformulation de 6.5.1. (ii) On applique 6.3.6. (iii) L'ordre de x étant égal à $q^d - 1$, celui de $x^{(q^d-1)/(q-1)}$ est égal à $q - 1$.

(6.6) Racines de l'unité

(6.6.1) Fixons un corps K. Pour tout entier $n \geq 1$, on va noter

$$\mu_n(K) = \{a \in K \mid a^n = 1\}$$

l'ensemble de racines n-ièmes de l'unité appartenant à K. Si $\mathrm{car}(K) = p > 0$ et $n = p^k \cdot m$, $p \nmid m$, alors la formule $X^n - 1 = (X^m - 1)^{p^k} \in K[X]$ montre que $\mu_n(K) = \mu_m(K)$.

On va considérer les polynomes $\Phi_n(X) \in \mathbf{Z}[X]$ (voir 1.6.4 ci-dessus) comme des éléments de $K[X]$; la formule de factorisation 1.6.4(i)

$$(\forall n \geq 1) \qquad \prod_{d|n} \Phi_d(X) = X^n - 1 \in K[X] \tag{6.6.1.1}$$

est valable dans $K[X]$. Fixons un corps de décomposition $K(\mu_n)$ du polynôme $X^n - 1$ sur K et posons $\mu_n = \mu_n(K(\mu_n))$.

(6.6.2) Proposition. *Soient K un corps et $n \geq 1$ un entier tel que* $\mathrm{car}(K) \nmid n$.
(i) *Le polynôme $f(X) = X^n - 1 \in K[X]$ est séparable.*
(ii) *Pour tout corps $F \supset K(\mu_n)$, le groupe $\mu_n(F)$ est cyclique d'ordre n; soit $\mu_n^0(F)$ l'ensemble de générateurs de $\mu_n(F)$. Fixons $\zeta_n \in \mu_n^0(F)$; alors on a*

$$\mu_n^0(F) = \{\zeta_n^a \mid 1 \leq a \leq n,\ \mathrm{pgcd}(a, n) = 1\} = \{\text{racines de } \Phi_n(X) \text{ dans } F\}.$$

(iii) *Soit ζ_n un générateur de μ_n; alors on a $K(\mu_n) = K(\zeta_n) =$ un corps de décomposition du polynôme $\Phi_n(X)$ sur K.*
(iv) *L'extension $K(\mu_n)/K$ est galoisienne. Il existe un homomorphisme injectif de groupes*

$$\chi_n : \mathrm{Gal}(K(\mu_n)/K) \longrightarrow (\mathbf{Z}/n\mathbf{Z})^* = GL_1(\mathbf{Z}/n\mathbf{Z})$$

tel que

$$(\forall \zeta \in \mu_n)\ (\forall g \in \mathrm{Gal}(K(\mu_n)/K)) \quad g(\zeta) = \zeta^{\chi_n(g)}.$$

(v) *L'extension $K(\mu_n)/K$ est abélienne.*

Preuve. (i) D'après 3.5.11, il suffit de vérifier que $1 = X^n - (X^n - 1) = n^{-1}Xf'(X) - f(X) \in (f, f')$ (l'entier n étant inversible dans K).
(ii) D'après 4.2.2, le groupe $\mu_n(F)$ est cyclique. Il résulte de (i) que les racines de f sont distinctes, donc $|\mu_n(F)| = \deg(f) = n$. Si $\zeta_n \in \mu_n^0(F)$, alors on déduit de (6.6.1.1) que

$$(\forall m = 1, \ldots, n-1) \quad \zeta_n^m - 1 \neq 0 \implies (\forall m = 1, \ldots, n-1) \quad \Phi_m(\zeta_n) \neq 0,$$

donc $\Phi_n(\zeta_n) = 0$. On vient de démontrer que $\mu_n^0(F) = \{\zeta_n^a \mid 1 \leq a \leq n,\ \mathrm{pgcd}(a, n) = 1\}$ est contenu dans l'ensemble des racines de $\Phi_n(X)$ dans F; les deux ensembles ayant la même cardinalité $|\mu_n^0(F)| = \varphi(n) = \deg(\Phi_n)$, il sont égaux.
(iii) Comme $\mu_n = \{\zeta_n, \zeta_n^2, \ldots, \zeta_n^n = 1\}$, on a $K(\mu_n) = K(\zeta_n) = K(\mu_n^0)$, le dernier corps étant un corps de décomposition de $\Phi_n(X)$ sur K, d'après (ii).

(iv) L'extension $K(\mu_n)/K$ est galoisienne, puisque $K(\mu_n)$ est un corps de décomposition (sur K) du polynôme séparable $X^n - 1 \in K[X]$ (voir 6.2.3(i)). Fixons $\zeta_n \in \mu_n^0$ (= une racine de $\Phi_n(X)$ dans $K(\mu_n)$). Pour tout $g \in \mathrm{Gal}(K(\mu_n)/K)$, on a

$$\Phi_n(g(\zeta_n)) = g(\Phi_n(\zeta_n)) = g(0) = 0,$$

donc il existe un élément (unique) $a \in (\mathbf{Z}/n\mathbf{Z})^*$ tel que $g(\zeta_n) = \zeta_n^a$. Tout élément $\zeta \in \mu_n$ s'écrit comme $\zeta = \zeta_n^b$ $(1 \leq b \leq n)$; il en résulte que

$$g(\zeta) = g(\zeta_n^b) = g(\zeta_n)^b = \zeta_n^{ab} = \zeta^a.$$

En particulier, l'exposant

$$\chi_n(g) := a \in (\mathbf{Z}/n\mathbf{Z})^*$$

ne dépend pas du choix de $\zeta_n \in \mu_n^0$. L'application

$$\chi_n : \mathrm{Gal}(K(\mu_n)/K) \longrightarrow (\mathbf{Z}/n\mathbf{Z})^*$$

ainsi obtenue est un homomorphisme de groupes, puisque si $g, g' \in \mathrm{Gal}(K(\mu_n)/K)$ et $\zeta \in \mu_n$, alors on a

$$(gg')(\zeta) = g(g'(\zeta)) = g(\zeta^{\chi_n(g')}) = g(\zeta)^{\chi_n(g')} = (\zeta^{\chi_n(g)})^{\chi_n(g')} = \zeta^{\chi_n(g)\chi_n(g')} \implies \chi_n(gg') = \chi_n(g)\chi_n(g').$$

Si $g \in \mathrm{Ker}(\chi_n)$, alors on a $g(\zeta_n) = \zeta_n$, donc $g(\alpha) = \alpha$ pour tout élément $\alpha \in K(\zeta_n) = K(\mu_n)$, d'où $g = 1$.
(v) $\mathrm{Gal}(K(\mu_n)/K)$ est isomorphe au sous-groupe $\chi_n(\mathrm{Gal}(K(\mu_n)/K))$ du groupe abélien $(\mathbf{Z}/n\mathbf{Z})^*$.

(6.6.3) Proposition. *Si $K = \mathbf{Q}$ et $n \geq 1$, alors on a:*
(i) *Le polynôme $\Phi_n(X)$ est irréductible sur $\mathbf{Q}$.*
(ii) *L'homomorphisme $\chi_n : \mathrm{Gal}(\mathbf{Q}(\mu_n)/\mathbf{Q}) \longrightarrow (\mathbf{Z}/n\mathbf{Z})^*$ est un isomorphisme.*
(iii) *Si $m|n$, alors χ_n induit un isomorphisme de groupes*

$$\mathrm{Gal}(\mathbf{Q}(\mu_n)/\mathbf{Q}(\mu_m)) \xrightarrow{\sim} \{a \in (\mathbf{Z}/n\mathbf{Z})^* \mid a \equiv 1 \pmod m\}.$$

Preuve. (i) Si $n = p^k$ (p premier), voir 3.1.5. En général, supposons que $f(X) \in \mathbf{Z}[X]$ soit un facteur irréductible unitaire de $\Phi_n(X) = f(X)g(X)$ $(\deg(f) \geq 1)$; fixons une racine $\zeta \in \mathbf{Q}(\mu_n)$ de $f(X)$. Soit $p \nmid n$ un nombre premier; on va montrer que $f(\zeta^p) = 0$. Sinon, on a $g(\zeta^p) = 0$ (car $\Phi_n(\zeta^p) = 0$). Posons $h(X) = g(X^p) \in \mathbf{Z}[X]$; alors f divise h dans $\mathbf{Q}(X)$, puisque $h(\zeta) = 0$ et f est le polynôme minimal de ζ sur $\mathbf{Q}$. Le polynôme $f \in \mathbf{Z}[X]$ étant unitaire, l'algorithme de division montre que f divise h dans $\mathbf{Z}[X]$. Il en résulte que la réduction modulo p $\overline{f} = f \pmod p \in \mathbf{F}_p[X]$ divise $\overline{h}(X) = \overline{g}(X^p) = \overline{g}(X)^p$ dans $\mathbf{F}_p[X]$; en particulier, si $r \in \mathbf{F}_p[X]$ est un facteur irréductible non constant de $\overline{f}$, alors on a $r^2|\overline{f}\overline{g} = \overline{\Phi}_n \in \mathbf{F}_p[X]$, ce qui est impossible, puisque $\overline{\Phi}_n \in \mathbf{F}_p[X]$ est séparable, d'après 6.6.2(i).

Si $a \geq 1$ est un entier, $\mathrm{pgcd}(a, n) = 1$, alors $a = p_1 \cdots p_k$ est un produit de nombres premiers $p_j \nmid n$, donc $f(\zeta^a) = 0$, par récurrence sur k. On vient de démontrer que tout élément de μ_n^0 est une racine de f, donc $f = \Phi_n$.
(ii) D'après (i), le polynôme minimal de ζ_n sur $\mathbf{Q}$ est égal à $\Phi_n(X)$, d'où

$$|(\mathbf{Z}/n\mathbf{Z})^*| = \varphi(n) = \deg(\Phi_n) = [\mathbf{Q}(\zeta_n) : \mathbf{Q}] = [\mathbf{Q}(\mu_n) : \mathbf{Q}] = |\mathrm{Gal}(\mathbf{Q}(\mu_n)/\mathbf{Q})|.$$

L'homomorphisme χ_n étant injectif, il est donc surjectif.
(iii) Ceci est une conséquence de (ii).

(6.6.4) En particulier, si $n = p$ est un nombre premier, le groupe $\mathrm{Gal}(\mathbf{Q}(\mu_p)/\mathbf{Q}) \xrightarrow{\sim} (\mathbf{Z}/p\mathbf{Z})^*$ est cyclique d'ordre $p - 1$. Par exemple, le groupe $(\mathbf{Z}/7\mathbf{Z})^*$ est engendré par $3 \pmod 7$, donc $\mathrm{Gal}(\mathbf{Q}(\mu_7)/\mathbf{Q}) = \{\sigma, \sigma^2, \ldots \sigma^6 = 1\}$, où $\sigma(\zeta) = \zeta^3$ $(\zeta \in \mu_7)$; cf. 1.6.7.

(6.6.5) Exemple (Sommes de Gauss) : Fixons un nombre premier $p > 2$. Le groupe $G = \mathrm{Gal}(\mathbf{Q}(\mu_p)/\mathbf{Q})$ étant cyclique d'ordre $p - 1 = 2\frac{p-1}{2}$, il existe un seul sous-groupe $H \subset G$ d'ordre $\frac{p-1}{2}$, donc il existe une

unique sous-extension $\mathbf{Q} \subset F \subset \mathbf{Q}(\mu_p)$ de degré $[F : \mathbf{Q}] = 2$, à savoir $F = \mathbf{Q}(\mu_p)^H$. Fixons un générateur $g \in G$; alors H est engendré par g^2. Posons $\zeta_p = e^{2\pi i/p}$ et

$$\tau_p = \sum_{j=1}^{p-1} (-1)^j \, g^j(\zeta_p) = \sum_{j=1}^{p-1} (-1)^j \, \zeta_p^{(a^j)} \in \mathbf{Q}(\mu_p) \qquad\qquad (a = \chi_p(g) \in (\mathbf{Z}/p\mathbf{Z})^*)$$

(il est facile de voir que τ_p ne dépend pas du choix de g). Comme

$$g(\tau_p) = \sum_{j=1}^{p-1} (-1)^j \, g^{j+1}(\zeta_p) = -\sum_{k=2}^{p} (-1)^k \, g^k(\zeta_p) = -\tau_p,$$

on a

$$\begin{aligned} g^2(\tau_p) = \tau_p &\implies \tau_p \in \mathbf{Q}(\mu_p)^H = F \\ g(\tau_p^2) = \tau_p^2 &\implies \tau_p^2 \in \mathbf{Q}(\mu_p)^G = \mathbf{Q}. \end{aligned}$$

Par exemple, on a calculé en 1.6.6-7 les valeurs

$$\tau_3 = \zeta_3 - \zeta_3^2 = i\sqrt{3}, \qquad \tau_5 = \zeta_5 - \zeta_5^2 - \zeta_5^3 + \zeta_5^4 = \sqrt{5}, \qquad \tau_7 = \zeta_7 + \zeta_7^2 - \zeta_7^3 + \zeta_7^4 - \zeta_7^5 - \zeta_7^6 = i\sqrt{7}.$$

En général, on peut montrer que l'on a $\tau_p^2 = (-1)^{(p-1)/2} p$ et

$$\tau_p = \begin{cases} +\sqrt{p} & p \equiv 1 \pmod 4 \\ +i\sqrt{p} & p \equiv 3 \pmod 4. \end{cases}$$

Plus généralement, si $r|(p-1)$ et $\alpha \in \mu_r^0$, on peut considérer la somme

$$\tau_p(\alpha, g) = \sum_{j=1}^{p-1} \alpha^j \, g^j(\zeta_p) \in \mathbf{Q}(\mu_p, \mu_r) = \mathbf{Q}(\mu_{pr})$$

Le même calcul que plus haut montre que l'on a (cf. 1.6.7)

$$\tau_p(\alpha, g)^r \in \mathbf{Q}(\mu_r).$$

(6.6.6) Exemple (Gauss) : Le groupe $G = \mathrm{Gal}(\mathbf{Q}(\mu_{17})/\mathbf{Q}) \xrightarrow{\sim} (\mathbf{Z}/17\mathbf{Z})^*$ est cyclique d'ordre $16 = 2^4$, engendré par $g : \zeta \mapsto \zeta^3$ ($\zeta \in \mu_{17}$). Les sous-groupes de G

$$G = H_0 \supset H_1 \supset H_2 \supset H_3 \supset H_4 = \{1\},$$

où $H_j = \{g_j, g_j^2, \ldots, g_j^{2^{4-j}} = 1\}$ est engendré par $g_j = g^{2^j}$, correspondent aux sous-corps $K_j = \mathbf{Q}(\mu_{17})^{H_j}$ de $\mathbf{Q}(\mu_{17})/\mathbf{Q}$:

$$\mathbf{Q} = K_0 \subset K_1 \subset K_2 \subset K_3 \subset K_4 = \mathbf{Q}(\mu_{17}).$$

Posons $\zeta = \zeta_{17} = e^{2\pi i/17}$ et

$$a_j = \mathrm{Tr}_{K_4/K_j}(\zeta) = \sum_{\sigma \in H_j} \sigma(\zeta) = \sum_{k=1}^{2^{4-j}} \zeta^{\left(3^{(k \cdot 2^j)}\right)}.$$

On a $K_j = \mathbf{Q}(a_j)$ et $[K_j : K_{j-1}] = 2$. Les conjugués de a_j sur K_{j-1} sont a_j et $a_j' = g_{j-1}(a_j)$, puisque $H_{j-1} = H_j \cup g_{j-1} H_j$. Explicitement, on a

$$
\begin{aligned}
a_0 &= -1 & a'_0 &= -1\\
a_1 &= \zeta+\zeta^9+\zeta^{-4}+\zeta^{-2}+\zeta^{-1}+\zeta^{-9}+\zeta^4+\zeta^2 & a'_1 &= \zeta^3+\zeta^{-7}+\zeta^5+\zeta^{-6}+\zeta^{-3}+\zeta^7+\zeta^{-5}+\zeta^6\\
a_2 &= \zeta+\zeta^4+\zeta^{-4}+\zeta^{-1} & a'_2 &= \zeta^9+\zeta^2+\zeta^{-2}+\zeta^{-9}\\
a_3 &= \zeta+\zeta^{-1}=2\cos\tfrac{2\pi}{17} & a'_3 &= \zeta^{-4}+\zeta^4\\
a_4 &= \zeta & a'_4 &= \zeta^{-1}
\end{aligned}
$$

En particulier, $a_j + a'_j = a_{j-1}$; on peut calculer explicitement les produit $b_{j-1} = a_j a'_j \in K_{j-1}$, donc obtenir le polynôme minimal $(X-a_j)(X-a'_j) = X^2 - a_{j-1}X + b_{j-1}$ de a_j sur K_{j-1} (cf. [Es], p.149-150). Le résultat final

$$16\cos\tfrac{2\pi}{17} = -1+\sqrt{17}+\sqrt{34-2\sqrt{17}}+\sqrt{68+12\sqrt{17}-4\sqrt{34-2\sqrt{17}}-8\sqrt{34+2\sqrt{17}}}$$

permet de construir le polygone régulier à 17 côtés à la règle et au compas.

7. Résolubilité des équations par radicaux

(7.1) Extensions de Kummer

(7.1.1) Proposition. *Soient K un corps, $n \geq 1$ un entier tel que $\mathrm{car}(K) \nmid n$ et $a \in K^*$. Soit L un corps de décomposition du polynôme $X^n - a$ sur K. Alors on a:*
(i) *L'extension L/K est galoisienne.*
(ii) *Le groupe $\mu_n(L)$ est cyclique d'ordre n; fixons un générateur $\zeta_n \in \mu_n(L)$.*
(iii) *Fixons une racine $\alpha = \sqrt[n]{a} \in L$ de $X^n - a$; alors on a $X^n - a = \prod_{j=1}^{n}(X - \zeta_n^j \alpha)$ et $L = K(\zeta_n, \alpha) = K(\zeta_n, \sqrt[n]{a}) = K(\mu_n, \sqrt[n]{a})$.*
(iv) *Si $g \in \mathrm{Gal}(L/K)$, alors on a*

$$g(\zeta_n) = \zeta_n^{\chi(g)}, \qquad g(\alpha) = \zeta_n^{c(g)}\alpha, \qquad \chi(g) = \chi_n(g) \in (\mathbf{Z}/n\mathbf{Z})^*, \qquad c(g) \in \mathbf{Z}/n\mathbf{Z}$$

et l'application

$$\lambda : g \mapsto \begin{pmatrix} \chi(g) & c(g) \\ 0 & 1 \end{pmatrix}$$

est un homomorphisme injectif de groupes

$$\lambda : \mathrm{Gal}(K(\mu_n, \sqrt[n]{a})/K) \hookrightarrow GA_1(\mathbf{Z}/n\mathbf{Z}).$$

(v) *Si $K = K(\mu_n)$ ($\iff$ K contient n racines n-ièmes de l'unité), alors on a $L = K(\sqrt[n]{a})$ et l'application $c : g \mapsto c(g)$ est un homomorphisme injectif de groupes*

$$c : \mathrm{Gal}(K(\sqrt[n]{a})/K) \hookrightarrow \mathbf{Z}/n\mathbf{Z}$$

et le groupe $\mathrm{Gal}(K(\sqrt[n]{a})/K)$ est cyclique, d'ordre un diviseur de n.
(vi) *En général, on a un diagramme commutatif*

$$\begin{array}{ccccccccc}
\{1\} & \longrightarrow & \mathrm{Gal}(K(\mu_n, \sqrt[n]{a})/K(\mu_n)) & \longrightarrow & \mathrm{Gal}(K(\mu_n, \sqrt[n]{a})/K) & \longrightarrow & \mathrm{Gal}(K(\mu_n)/K) & \longrightarrow & \{1\} \\
 & & \downarrow c & & \downarrow \lambda & & \downarrow \chi & & \\
\{1\} & \longrightarrow & \mathbf{Z}/n\mathbf{Z} & \longrightarrow & GA_1(\mathbf{Z}/n\mathbf{Z}) & \longrightarrow & (\mathbf{Z}/n\mathbf{Z})^* & \longrightarrow & \{1\}.
\end{array}$$

Preuve. (i) Le même argument qu'en 6.6.2(i) montre que le polynôme $X^n - a$ est séparable, donc 6.2.3(i) s'applique.
(ii), (iii) Soient $\alpha_1 = \alpha, \ldots, \alpha_n \in L$ les racines (distinctes) de $X^n - a$ dans L; alors on a $\{\alpha_j/\alpha \,|\, 1 \leq j \leq n\} = \mu_n(L)$, ce qui démontre (ii) et (iii).
(iv) D'après 6.6.2(iv), on a $g(\zeta_n) = \zeta_n^{\chi(g)}$ ($\chi(g) \in (\mathbf{Z}/n\mathbf{Z})^*$). Comme $g(\alpha)$ est une racine de $X^n - a$, on a $g(\alpha) = \zeta_n^{c(g)}\alpha$, $c(g) \in \mathbf{Z}/n\mathbf{Z}$. Soient $g, g' \in \mathrm{Gal}(L/K)$; alors on a $\chi(gg') = \chi(g)\chi(g')$ (d'après 6.6.2(iv)) et

$$\zeta_n^{c(gg')}\alpha = (gg')(\alpha) = g(g'(\alpha)) = g(\zeta_n^{c(g')}\alpha) = g(\zeta_n)^{c(g')}g(\alpha) = \zeta_n^{\chi(g)c(g')+c(g)}\alpha \implies c(gg') = \chi(g)c(g') + c(g),$$

donc

$$\lambda(gg') = \begin{pmatrix} \chi(gg') & c(gg') \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} \chi(g) & c(g) \\ 0 & 1 \end{pmatrix}\begin{pmatrix} \chi(g') & c(g') \\ 0 & 1 \end{pmatrix} = \lambda(g)\lambda(g').$$

Si $g \in \mathrm{Ker}(\lambda)$, alors on a $g(\zeta_n) = \zeta_n$ et $g(\alpha) = \alpha$, d'où $g(x) = x$ pour tout $x \in K(\zeta_n, \alpha) = L$, ce qui démontre l'injectivité de λ.

(v) Si $\mu_n \subset K$, alors on a $L = K(\sqrt[n]{a})$ et $\chi(g) = 1$ pour tout $g \in \mathrm{Gal}(L/K)$, ce qui entraîne que c est un homomorphisme de groupes (injectif, d'après (iv)): $c(gg') = c(g') + c(g)$ $(g, g' \in \mathrm{Gal}(L/K))$. Il en résulte que $\mathrm{Gal}(L/K)$, étant isomorphe à un sous-groupe de $\mathbf{Z}/n\mathbf{Z}$, est cyclique d'ordre un diviseur de n.
(vi) Ceci est une conséquence de (iv), (v) et 6.6.2(iv).

(7.1.2) Exemple : Soit p un nombre premier. Le corps de décomposition du polynôme (irréductible) $f(X) = X^p - 2 \in \mathbf{Q}[X]$ sur $\mathbf{Q}$ est égal à $L = \mathbf{Q}(\zeta_p, \sqrt[p]{2}) \subset \mathbf{C}$. Les degrés $[\mathbf{Q}(\zeta_p) : \mathbf{Q}] = p - 1$ et $[\mathbf{Q}(\sqrt[p]{2}) : \mathbf{Q}] = p$ étant premiers entre eux, on a $[\mathbf{Q}(\zeta_p, \sqrt[p]{2}) : \mathbf{Q}] = p(p-1) = |GA_1(\mathbf{F}_p)|$. Il en résulte que l'homomorphisme injectif

$$\mathrm{Gal}(f) = \mathrm{Gal}(\mathbf{Q}(\zeta_p, \sqrt[p]{2})/\mathbf{Q}) \xrightarrow{\sim} GA_1(\mathbf{F}_p)$$

est un isomorphisme.

(7.1.3) Proposition. *Soient K un corps, $n \geq 1$ un entier tel que $\mathrm{car}(K) \nmid n$ et $\mu_n \subset K$. Si L/K est une extension cyclique d'ordre n, alors il existe $a \in K^*$ tel que $L = K(\sqrt[n]{a})$.*

Preuve. Fixons un générateur σ (resp., ζ_n) du groupe cyclique $G = \mathrm{Gal}(L/K)$ (resp., de $\mu_n = \mu_n(K)$). Soit $\omega_1, \ldots, \omega_n$ une base de L/K; comme le discriminant $D(\omega_1, \ldots, \omega_n) = \det(B)^2 \neq 0$ (d'après 5.3.9(i)), la matrice $B = (\sigma^i(\omega_j))_{1 \leq i,j \leq n} \in M_n(L)$ est inversible. On en déduit qu'il existe un élément de la base $x \in \{\omega_1, \ldots, \omega_n\}$ dont la *résolvante de Lagrange*

$$\alpha = \sum_{i=0}^{n-1} \zeta_n^{-i}\, \sigma^i(x) = x + \zeta_n^{-1}\, \sigma(x) + \cdots + \zeta_n^{1-n}\, \sigma^{n-1}(x) \in L$$

ne soit pas nul. Comme

$$\sigma(\alpha) = \sigma(x) + \zeta_n^{-1}\, \sigma^2(x) + \cdots + \zeta_n^{1-n}\, x = \zeta_n \alpha,$$

on a $a := \alpha^n \in L^G = K$. Les éléments conjugués $\{\alpha, \sigma(\alpha), \ldots, \sigma^{n-1}(\alpha)\} = \{\alpha, \zeta_n\alpha, \ldots, \zeta_n^{n-1}(\alpha)\}$ à α étant distincts, on a $[K(\alpha) : K] \geq n = [L : K]$, donc $L = K(\alpha)$.

(7.1.4) Proposition. *Soient K un corps, $n \geq 1$ un entier tel que $\mathrm{car}(K) \nmid n$ et L/K une extension galoisienne (de degré fini). Alors le groupe $\mathrm{Gal}(L(\mu_n)/K(\mu_n))$ est isomorphe à un sous-groupe de $\mathrm{Gal}(L/K)$.*

Preuve. D'après 6.2.3(ii), L est un corps de décomposition (sur K) d'un polynôme séparable $f \in K[X]$; alors $L(\mu_n)$ est un corps de décomposition de f sur $K(\mu_n)$. La restriction d'un élément $g \in \mathrm{Gal}(L(\mu_n)/K(\mu_n))$ à L est un élément de $\mathrm{Gal}(L/K)$; ceci définit un homomorphisme de groupes $f : \mathrm{Gal}(L(\mu_n)/K(\mu_n)) \longrightarrow \mathrm{Gal}(L/K)$. Soient $\alpha_1, \ldots, \alpha_r \in L(\mu_n)$ les racines de f dans $L(\mu_n)$; alors on a $L = K(\alpha_1, \ldots, \alpha_r)$ et $L(\mu_n) = K(\mu_n)(\alpha_1, \ldots, \alpha_r)$. Si $g \in \mathrm{Ker}(f)$, alors on a $g(\alpha_j) = \alpha_j$ $(j = 1, \ldots, r)$, donc $g = 1$. L'homomorphisme f est donc injectif, d'où le résultat.

(7.1.5) Exercice. *Soit p un nombre premier. Montrer que le corps de décomposition du polynôme $f(X) = X^4 - p \in \mathbf{Q}[X]$ sur $\mathbf{Q}$ est égal à $L = \mathbf{Q}(i, \sqrt[4]{p}) \subset \mathbf{C}$ et que $\mathrm{Gal}(L/\mathbf{Q}) \xrightarrow{\sim} GA_1(\mathbf{Z}/4\mathbf{Z}) \xrightarrow{\sim} D_8$. Expliciter l'action de D_8 sur L.*

(7.2) Groupes résolubles

(7.2.1) Définition. *Un groupe G est* **résoluble** *s'il existe une suite finie de sous-groupes $G = G_0 \supset G_1 \supset \cdots \supset G_k = \{1\}$ $(k < \infty)$ telle que $G_{i+1} \lhd G_i$ et G_i/G_{i+1} soit abélien pour tous $i = 0, \ldots, k-1$.*

(7.2.2) Exemples : (i) Un groupe abélien G est résoluble: $G \supset \{1\}$.
(ii) $G = GA_1(R)$ est résoluble: $G \supset G_1 = (R, +) \supset \{1\}$, $G/G_1 \xrightarrow{\sim} R^*$.
(iii) $G = S_3$ est résoluble: $S_3 \supset A_3 \supset \{1\}$.
(iv) $G = S_4$ est résoluble: l'action de S_4 sur les polynômes y_1, y_2, y_3 que l'on a défini en 1.4.1 donne un homomorphisme surjectif de groupes $\pi : S_4 \longrightarrow S_3$, dont le noyau est isomorphe à $C_2 \times C_2$. On obtient donc une suite de sous-groupes $S_4 \supset A_4 \supset C_2 \times C_2 \supset \{1\}$ (voir [Es], 10.8).

(v) Un groupe simple non abélien n'est pas résoluble (rappel : un groupe G est **simple** si G ne possède aucun sous-groupe distingué $H \neq G, \{1\}$).
(vi) Tout sous-groupe $H \subset G$ d'un groupe résoluble G est résoluble (on prend $H_i = H \cap G_i$).
(vii) L'image d'un groupe résoluble G par tout homomorphisme de groupes $f : G \longrightarrow K$ est résoluble (on prend $f(G)_i = f(G_i)$).
(viii) Pour tout $n \geq 5$ le groupe A_n est simple. Il résulte de (v) (resp., de (vi)) que A_n (resp., S_n) n'est pas résoluble pour $n \geq 5$.
(ix) Tout groupe d'ordre p^n (où p est un nombre premier) est résoluble.

(7.2.3) Lemme. *Un groupe fini G est résoluble $\iff$ il existe une suite de sous-groupes $G = H_0 \supset \cdots \supset H_l = \{1\}$ telle que $H_{j+1} \lhd H_j$ et H_j/H_{j+1} soit cyclique d'ordre premier pour tous $j = 0, \ldots, l-1$.*

Preuve. Il suffit de démontrer "$\Longrightarrow$": si G_i est une suite de sous-groupes de G comme en 7.2.1, on construit pour tout i une suite de sous-groupes intermédiaires $G_i = K_0^i \supset K_1^i \supset \cdots \supset K_{r_i}^i = G_{i+1}$: on choisit K_{j+1}^i un sous-groupe distingué maximal de K_j^i contenant G_{i+1}. Le quotient K_j^i/K_{j+1}^i est un groupe simple abélien, donc cyclique d'ordre premier. On obtient la suite $H_0 = K_0^0 \supset H_1 = K_1^0 \supset \cdots \supset K_{r_0}^0 \supset K_0^1 \supset \cdots \supset \{1\}$ recherchée.

(7.3) Extensions radicales

(7.3.1) Définition. *Soit K un corps.*
(i) *Une extension L/K de degré fini est une* **extension radicale** *s'il existe des extensions*

$$K = K_0 \subset \cdots \subset K_j = K(\alpha_1, \ldots, \alpha_j) = K_{j-1}(\alpha_j) \subset \cdots \subset K_m = L$$

telles que pour tous $j = 1, \ldots, m$ il existe un entier $n_j \geq 1$, $\mathrm{car}(K) \nmid n_j$, tel que $a_j := \alpha_j^{n_j} \in K_{j-1}$ ($\iff K_j = K_{j-1}(\sqrt[n_j]{a_j})$).
(ii) *Soit $f \in K[X]$ un polynôme séparable. On dit que l'équation $f(X) = 0$ est* **résoluble par radicaux sur** *K s'il existe une extension radicale L de K contenant un corps de décomposition de f ($\iff$ contenant toutes les racines de f).*

(7.3.2) Lemme. *Toute extension radicale de K est contenue dans une extension radicale L/K ayant les propriétés suivantes:*
(i) *L'extension L/K est galoisienne.*
(ii) *$K_1 = K(\mu_n)$, où $\mathrm{car}(K) \nmid n$.*
(iii) *Pour tous $j = 1, \ldots, m$, $K_j = K_{j-1}(\sqrt[n]{a_j})$ ($a_j \in K_{j-1}$).*

Preuve. On remplace, d'abord, chaque corps K_{j+1} par $K_j(\mu_n)$, où $n = \mathrm{ppcm}(n_1, \ldots, n_m)$. Le (nouveau) corps $K_2 = K_1(\sqrt[n_1]{a_1}) = K_1(\sqrt[n]{a_1^{n/n_1}})$ est une extension galoisienne de $K_1 = K(\mu_n)$. Ensuite, on ajoute toutes les racines n-ièmes des éléments $\sigma(a_2)^{n/n_2}$, où $\sigma \in \mathrm{Gal}(K_2/K_1)$, etc. [Par exemple, l'extension $\mathbf{Q}(\sqrt[3]{2+\sqrt[4]{5}})/\mathbf{Q}$ est contenue dans $L = \mathbf{Q}(\mu_{12}, \rho^j \sqrt[3]{2 + i^k \sqrt[4]{5}};\ j = 0, 1, 2,\ k = 0, 1, 2, 3)$.]

(7.3.3) Théorème. *Soient K un corps et $f \in K[X]$ un polynôme séparable.*
(i) *Si l'équation $f = 0$ est résoluble par radicaux sur K, alors le groupe de Galois $\mathrm{Gal}(f)$ (sur K) est résoluble.*
(ii) *Si $\mathrm{Gal}(f)$ est résoluble est son ordre n'est pas divisible par $\mathrm{car}(K)$, alors l'équation $f = 0$ est résoluble par radicaux.*

Preuve. (i) Soit F un corps de décomposition de f sur K. D'après 7.3.2, il existe une extension radicale L/K contenant F ayant les propriétés (i)–(iii). Posons $G = \mathrm{Gal}(L/K)$ et $G_j = \mathrm{Gal}(L/K_j)$ ($j = 0, \ldots, m$). Pour tous $j = 0, \ldots, m-1$, l'extension $K_{j+1} = K_j(\sqrt[n]{a_{j+1}})$ est galoisienne (donc $G_{j+1} \lhd G_j$) et le groupe $\mathrm{Gal}(K_{j+1}/K_j) = G_j/G_{j+1}$ est abélien, d'après 7.1.1(v) (resp., 6.6.2(v)). Il en résulte que G est résoluble, donc son quotient $\mathrm{Gal}(f) = \mathrm{Gal}(F/K) = G/\mathrm{Gal}(L/F)$ est aussi résoluble, d'après 7.2.2(vii).
(ii) Posons $n = |\mathrm{Gal}(f)|$. Soit F un corps de décomposition de f sur K; alors $F(\mu_n)$ est un corps de décomposition de f sur $K(\mu_n)$ et $\mathrm{Gal}(f(\mu_n)/K(\mu_n))$ est un sous-groupe de $\mathrm{Gal}(f) = \mathrm{Gal}(F/K)$ (d'après

7.1.4), donc résoluble. L'extension $K(\mu_n)/K$ étant radicale, on peut remplacer K par $K(\mu_n)$ et supposer que $\mu_n \subset K$. Il résulte de 7.2.3 qu'il existe une suite de sous-groupes $\mathrm{Gal}(f) = G = H_0 \supset \cdots \supset H_l = \{1\}$ telle que $(\forall j = 0, \ldots, l-1) \quad H_{j+1} \lhd H_j$ et $H_j/H_{j+1} \xrightarrow{\sim} \mathbf{Z}/p_j\mathbf{Z}$, où p_j est un nombre premier. Posons $K_j = F^{H_j}$; on a alors $K_0 = K \subset K_1 \subset \cdots \subset K_l = F$ et $\mathrm{Gal}(K_{j+1}/K_j) = H_j/H_{j+1} \xrightarrow{\sim} \mathbf{Z}/p_j\mathbf{Z}$. Comme p_j divise $|G|$, on déduit de 7.1.3 que $K_{j+1} = K_j(\sqrt[p_j]{a_{j+1}})$ $(a_{j+1} \in K_j)$, donc F/K est une extension radicale.

(7.3.4) Exemple : L'équation $f(X) = X^5 - X + 1 = 0$ n'est pas résoluble sur $\mathbf{Q}$ par radicaux, puisque le groupe $\mathrm{Gal}(f) = S_5$ (voir 6.4.7) n'est pas résoluble.

(7.3.5) Équation générale de degré n. Soient F un corps, $L = F(x_1, \ldots, x_n)$ le corps de fonctions rationnelles en les variables $x_1, \ldots, x_n$ et $K = L^{S_n} = F(\sigma_1, \ldots, \sigma_n)$ le sous-corps de fonctions rationnelles symétriques. On sait (voir 6.3.4) que l'extension L/K est galoisienne et $\mathrm{Gal}(L/K) = S_n$. Plus précisement, $L = K(x_1, \ldots, x_n)$ est un corps de décomposition (sur K) du polynôme séparable

$$f(X) = (X - x_1) \cdots (X - x_n) = X^n - \sigma_1 X^{n-1} + \sigma_2 X^{n-2} - \cdots + (-1)^n \sigma_n \in K[X].$$

Comme S_n n'est pas résoluble pour $n \geq 5$, il résulte de 7.3.3(i) que "l'équation générale"

$$X^n - \sigma_1 X^{n-1} + \sigma_2 X^{n-2} - \cdots + (-1)^n \sigma_n = 0$$

sur $K = F(\sigma_1, \ldots, \sigma_n)$ n'est pas résoluble par radicaux pour $n \geq 5$.

VERSION 30/09/2009

Bibliographie

[Ar] E. Artin, *Galois Theory*, Dover, 1998.

[Es] J.-P. Escofier, *Théorie de Galois*, Dunod, 2000.

[Ga] D.J.H. Garling : *Galois Theory*, Cambridge University Press, 1986.

[Sa] P. Samuel : *Théorie algébrique des Nombres*, Hermann, 1967.

[Ti 1] J.-P. Tignol, *Leçons sur la théorie des équations*, Université Catholique de Louvain, 1980.

[Ti 2] J.-P. Tignol, *Galois Theory of Algebraic Equations*, World Scientific, 2001.