**Troisième fascicule : 04/03/2008**

## 1.2 Critère d'irrationalité (suite et fin)

Si $\alpha$ est racine d'un polynôme quadratique $P(X) = aX^2 + bX + c$, alors $P'(\alpha) = 2a\alpha + b$ est une racine carrée du discriminant de $P$. D'après le lemme 1.9, le lemme de Hurwitz 1.5 est optimal pour toutes les racines de polynômes quadratiques de discriminant 5. En passant, cela montre que 5 est le plus petit discriminant d'un polynôme quadratique irréductible de $\mathbf{Z}[X]$ (évidemment on vérifie de façon élémentaire que si $a$, $b$, $c$ sont trois entiers rationnels satisfaisant $a > 0$ et $b^2 - 4ac$ positif sans être un carré parfait dans $\mathbf{Z}$, alors $b^2 - 4ac \geq 5$).

Soit $x$ un nombre réel irrationnel. Désignons par $\gamma(x) \in [\sqrt{5}, +\infty]$ la borne supérieure des nombres réels $\gamma > 0$ tels qu'il existe une infinité de $p/q \in \mathbf{Q}$ satisfaisant

$$\left|x - \frac{p}{q}\right| \leq \frac{1}{\gamma q^2}.$$

La minoration $\gamma \geq \sqrt{5}$ n'est autre que le lemme 1.5 de Hurwitz. Les lemmes 1.5 et 1.9 montrent que $\gamma(\Phi) = \sqrt{5}$.

En écrivant

$$\left|x + 1 - \frac{p}{q}\right| = \left|x - \frac{p+q}{q}\right| \quad \text{et} \quad \left|-x - \frac{p}{q}\right| = \left|x + \frac{p}{q}\right|,$$

on obtient $\gamma(x+1) = \gamma(-x) = \gamma(x)$. On montre aussi que $\gamma(1/x) = \gamma(x)$. Il en résulte que si $x$ et $y$ sont deux nombres réels que l'on déduit l'un de l'autre en itérant ces trois opérations $x \mapsto x+1$, $x \mapsto -x$ et $x \mapsto 1/x$, alors $\gamma(x) = \gamma(y)$. Un résultat classique ([6] Chap. VII § 1.2) est que le groupe multiplicatif engendré par les trois matrices

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

est le groupe des matrices $2 \times 2$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

à coefficients dans $\mathbf{Z}$ de déterminant $\pm 1$. Nous n'allons pas utiliser cet énoncé mais nous démontrons directement :

**Lemme 1.11.** *Soit $x \in \mathbf{R} \setminus \mathbf{Q}$ et soient $a$, $b$, $c$, $d$ des entiers rationnels satisfaisant $ad - bc = \pm 1$. On pose*

$$y = \frac{ax + b}{cx + d}.$$

*Alors $\gamma(x) = \gamma(y)$.*

*Démonstration.* Soit $\epsilon > 0$ et soit $\gamma = \gamma(x) - \epsilon$. Par définition de $\gamma(x)$, existe une infinité de $p/q \in \mathbf{Q}$ tels que

$$\left| x - \frac{p}{q} \right| \leq \frac{1}{\gamma q^2}.$$

Comme $c$ et $d$ ne sont pas tous deux nuls, au plus un d'entre eux satisfait $cp+dq = 0$. On s'intéresse aux autres. Posons

$$r = ap + bq, \quad s = cp + dq.$$

Quitte à changer les signes de $a$, $b$, $c$ et $d$ on peut supposer $s > 0$. On écrit

$$y - \frac{r}{s} = \frac{ax+b}{cx+d} - \frac{ap+bq}{cp+dq} = \frac{(ad-bc)(qx-p)}{(cx+d)(cp+dq)} = \pm \frac{qx-p}{(cx+d)(cp+dq)}$$

et

$$\left| y - \frac{r}{s} \right| \leq \frac{1}{\gamma q} \cdot \left| \frac{1}{(cx+d)(cp+dq)} \right| = \frac{1}{\gamma s^2} \cdot \frac{cp+dq}{q|cx+d|}.$$

Pour $q$ suffisamment grand on a

$$|c| \cdot \left| x - \frac{p}{q} \right| \leq \frac{|c|}{\gamma q^2} \leq \epsilon |cx+d|,$$

donc

$$\left| \frac{cp+dq}{q(cx+d)} - 1 \right| \leq \epsilon$$

et

$$\left| y - \frac{r}{s} \right| \leq \frac{1+\epsilon}{\gamma s^2}.$$

Comme il y a une infinité de $r/s \in \mathbf{Q}$ satisfaisant cette inégalité on en déduit

$$\gamma(y) \geq \frac{\gamma}{1+\epsilon} = \frac{\gamma(x) - \epsilon}{1+\epsilon}.$$

Cette inégalité est vraie pour tout $\epsilon > 0$, par conséquent $\gamma(y) \geq \gamma(x)$. Comme

$$x = \frac{-dy+b}{cy-a},$$

en permutant $x$ et $y$ on obtient l'égalité annoncée $\gamma(y) = \gamma(x)$. □

Des lemmes 1.5, 1.9 et 1.11 on déduit que tous les nombres réels $x$ de la forme $(a\Phi+b)/(c\Phi+d)$ avec $a$, $b$, $c$, $d$ dans $\mathbf{Z}$ et $ad-bc = \pm 1$ satisfont $\gamma(x) = \sqrt{5}$. Hurwitz a aussi montré que pour tous les autres nombres réels irrationnels $y$, on a $\gamma(y) \geq 2\sqrt{2}$. Cette inégalité est optimale, comme on le voit en prenant $y = \sqrt{2}$ (voir l'exercice ci-dessous). Le lemme 1.11 implique alors $\gamma(y) = 2\sqrt{2}$ pour tout $y$ de la forme $(a\sqrt{2}+b)/(c\sqrt{2}+d)$ avec $ad-bc = \pm 1$, et une fois de plus la minoration peut être améliorée pour tous les autres nombres réels irrationnels. Ce processus donne lieu à une suite d'exposants

$$\sqrt{5}, \sqrt{8}, \sqrt{221}/5, \sqrt{1517}/13, \ldots$$

convergeant vers $1/3$, qui est à l'origine de l'équation de Markoff (cf § 0.2 et [1] Chap. 7).

**Exercice.** On pose $G_0 = 0$, $G_1 = 1$, et par récurrence on définit $G_n = 2G_{n-1} + G_{n-2}$ pour $n \geq 2$.
a) Vérifier, pour tout $n \geq 1$,

$$G_n^2 - 2G_nG_{n-1} - G_{n-1}^2 = (-1)^{n-1}.$$

b) Montrer que la suite $(G_n/G_{n-1})_{n\geq 2}$ converge quand $n \to \infty$. Quelle est la limite ?
c) Montrer qu'il existe une suite $(p_n/q_n)_{n\geq 1}$ de nombre rationnels telle que

$$\lim_{n\to\infty} q_n \left| q_n\sqrt{2} - p_n \right| = \frac{1}{2\sqrt{2}}.$$

d) Montrer que pour tout $\kappa > 2\sqrt{2}$, il n'y a qu'un nombre fini de nombres rationnels $p/q \in \mathbf{Q}$ satisfaisant

$$\left| \sqrt{2} - \frac{p}{q} \right| \leq \frac{1}{\kappa q^2}.$$

## 1.3 Nombres : algébriques, transcendants

Un nombre complexe qui est racine d'un polynôme non nul à coefficients rationnels est appelé *algébrique*. Ainsi les nombres rationnels (racines d'un polynôme de degré 1 ) sont algébriques, $\sqrt{2}$ et $i$, racines des polynômes $X^2-2$ et $X^2+1$ sont algébriques irrationnels – on les appelle *quadratiques* car ils sont racines de polynômes de degré 2. Un nombre *cubique* est une racine d'un polynôme de degré 3 ; un exemple est $\sqrt[3]{2}$.

Étant donné un nombre algébrique $\alpha$, l'ensemble des polynômes à coefficients rationnels qui s'annulent en $\alpha$ forme un idéal premier de $\mathbf{Q}[X]$, cet idéal est principal, chacun de ses générateurs est un polynôme irréductible de $\mathbf{Q}[X]$ dont le degré est le *degré de* $\alpha$. Il y a un unique générateur unitaire, qui est appelé **le** *polynôme irréductible* de $\alpha$. Quand on multiplie ce polynôme par le ppcm des dénominateurs de ses coefficients, on obtient le *polynôme minimal* de $\alpha$, qui est l'unique polynôme irréductible dans l'anneau *factoriel* $\mathbf{Z}[X]$ s'annulant au point $\alpha$ et ayant un coefficient directeur positif. Voir par exemple [3] Chap. 2 § 5 pour les prérequis concernant notamment les anneaux factoriels.

Les nombres algébriques complexes forment un corps. L'exercice suivant en fournit une démonstration.

**Exercice.** a) Soient $x$ un nombre complexe et $n$ un entier positif. Montrer que les conditions suivantes sont équivalentes.
(i) Le nombre $x$ est racine d'un polynôme non nul de $\mathbf{Q}[X]$ de degré $\leq n$.
(ii) Les nombres $1, x, x^2, \ldots, x^n$ sont linéairement indépendants sur $\mathbf{Q}$.
(iii) Le $\mathbf{Q}$–espace vectoriel engendré par les nombres $x^i$, $(i \geq 1)$ est de dimension $\leq n$.
b) Montrer que l'inverse $1/x$ d'un nombre algébrique non nul $x$ est un nombre algébrique.
c) Soient $x$ et $y$ deux nombres algébriques. Montrer que le $\mathbf{Q}$–espace vectoriel engendré par $x^iy^j$, $(i \geq 0,\ j \geq 0)$ est de dimension finie. En déduire que le produit de deux nombres algébriques est un nombre algébrique.
d) Soient $x$ et $y$ deux nombres algébriques. Montrer que le $\mathbf{Q}$–espace vectoriel engendré par $x^i+y^j$, $(i \geq 0,\ j \geq 0)$ est de dimension finie. En déduire que la somme de deux nombres algébriques est un nombre algébrique.

Un nombre complexe est dit *transcendant* s'il n'est pas algébrique. L'ensemble des nombres transcendants ne jouit pas de bonnes propriétés algébriques : la somme de nombres transcendants peut être un nombre rationnel, ou algébrique irrationnel, ou encore transcendant. De même pour le produit de deux nombres transcendants. La somme d'un nombre algébrique et d'un nombre transcendant est un nombre transcendant. Le produit d'un nombre algébrique *non nul* et d'un nombre est un nombre transcendant. La racine carrée (et plus généralement la racine $k$-ième, pour $k \geq 1$) d'un nombre transcendant est un nombre transcendant. Toute puissance entière $\geq 1$ d'un nombre transcendant est encore un nombre transcendant.

L'existence de nombres transcendants a été établie en 1844 par J. Liouville. Son idée consiste à établir une propriété satisfaite par tous les nombres algébriques, puis à exhiber des nombres qui ne satisfont pas cette propriété. Ce que montre Liouville est que les nombres algébriques irrationnels sont relativement mal approchés par des nombres rationnels.

Le lemme suivant ([5] p. 6 Lemma 2E) est une des nombreuses variantes de l'inégalité de Liouville. On peut le voir comme un généralisation du lemme 1.10 : au lieu de $X^2 - X - 1$ on prend n'importe quel polynôme irréductible de degré $\geq 2$, ce qui revient à remplacer le nombre d'or par n'importe quel nombre algébrique irrationnel.

**Lemme 1.12.** *Soit $\alpha$ un nombre algébrique racine de degré $d \geq 2$ et soit $P \in \mathbf{Z}[X]$ son polynôme minimal. On pose $c = |P'(\alpha)|$. Soit $\epsilon > 0$. Alors il existe un entier $q_0$ tel que, pour tout $p/q \in \mathbf{Q}$ avec $q \geq q_0$, on ait*

$$\left|\alpha - \frac{p}{q}\right| \geq \frac{1}{(c+\epsilon)q^d}.$$

*Démonstration.* Soit $q$ un entier suffisamment grand et soit $p$ l'entier le plus proche de $q\alpha$. En particulier on a

$$|q\alpha - p| \leq \frac{1}{2}.$$

On désigne par $a_0$ le coefficient directeur de $P$ (quitte à remplacer s'il le faut $P$ par $-P$, on supposera $a_0 > 0$) et par $\alpha_1, \ldots, \alpha_d$ ses racines, avec $\alpha_1 = \alpha$. Ainsi

$$P(X) = a_0(X - \alpha_1)(X - \alpha_2)\cdots(X - \alpha_d)$$

et

$$q^d P(p/q) = a_0 q^d \prod_{i=1}^{d} \left(\frac{p}{q} - \alpha_i\right). \tag{1.13}$$

On a aussi

$$P'(\alpha) = a_0 \prod_{i=2}^{d} (\alpha - \alpha_i).$$

Le membre de gauche de (1.13) est un entier rationnel car $P$ est de degré $d$ à coefficients entiers. Il n'est pas nul parce que $P$ est irréductible de degré $\geq 2$. Pour $i \geq 2$ on a

$$\left|\alpha_i - \frac{p}{q}\right| \leq |\alpha_i - \alpha| + \frac{1}{2q}.$$

On déduit de (1.13)

$$1 \leq q^d a_0 \left|\alpha - \frac{p}{q}\right| \prod_{i=2}^{d} (|\alpha_i - \alpha| + \frac{1}{2q}).$$

Pour $q$ suffisamment grand le membre de droite est majoré par

$$q^d \left|\alpha - \frac{p}{q}\right| (|P'(\alpha)| + \epsilon).$$

□

Le corollaire suivant du lemme 1.12 est le résultat principal de J. Liouville en 1844 : c'est l'outil qui lui a permis, non seulement de montrer l'existence de nombres transcendants, mais aussi d'en exhiber. Ses premiers exemples utilisaient des fractions continues. Ensuite il a utilisé des séries rapidement convergentes comme

$$\vartheta = \sum_{n\geq 0} g^{-n!}$$

pour tout entier $g \geq 2$.

**Lemme 1.14.** *Pour tout nombre algébrique $\alpha$, il existe une constante $\kappa > 0$ telle que, pour tout nombre rationnel $p/q \neq \alpha$,*

$$\left|\alpha - \frac{p}{q}\right| \geq \frac{1}{\kappa q^d},$$

*où $d$ est le degré de $\alpha$*

*Démonstration.* Quand $d = 1$ ce résultat est vrai en prenant pour $\kappa$ le dénominateur de $\alpha$. Supposons maintenant $d \geq 2$. Le lemme 1.12 avec $\epsilon = 1$ montre que l'inégalité est vraie avec $\kappa = c+1$ pour $q$ suffisamment grand, disons $q \geq q_0$. Pour avoir un résultat uniforme (pour tout $p/q$) il suffit de prendre

$$\kappa = \max\left\{c+1, \max_{1\leq q<q_0} \frac{1}{q^{d-1}|q\alpha - p|}\right\}.$$

□

**Exercice.** Le lemme 1.14 est trivial si $\alpha$ n'est pas réel. Dire pourquoi.

**Exercice.** On désigne par $P \in \mathbf{Z}[X]$ le polynôme minimal de $\alpha$, par $a_0$ son coefficient directeur et par $\alpha_1, \ldots, \alpha_d$ ses racines, avec $\alpha_1 = \alpha$ :

$$P(X) = a_0(X - \alpha_1)(X - \alpha_2)\cdots(X - \alpha_d).$$

a) Démontrer le lemme 1.14 avec

$$\kappa = \max\{1\,;\ \max_{|t-\alpha|\leq 1} |P'(t)|\}.$$

b) Démontrer le lemme 1.14 avec

$$\kappa = a_0 \prod_{i=2}^{d} (|\alpha_j - \alpha| + 1).$$

`Indication` *Pour les deux parties de l'exercice, on pourra distinguer deux cas selon que $|\alpha - (p/q)|$ est $\geq 1$ ou $< 1$.*

**Définition.** Un nombre réel $\vartheta$ est un *nombre de Liouville* si, pour tout $\kappa > 0$, il existe $p/q \in \mathbf{Q}$ avec $q \geq 2$ tel que

$$0 < \left|\alpha - \frac{p}{q}\right| \leq \frac{1}{q^\kappa}.$$

Le lemme 1.14 implique que les nombres de Liouville sont transcendants [2]. Dans la théorie des systèmes dynamiques, on dit qu'un nombre réel *satisfait une condition Diophantienne* si ce n'est pas un nombre de Liouville : cela signifie qu'il existe une constante $\kappa > 0$ telle que, pour tout $p/q \in \mathbf{Q}$ avec $q$ suffisamment grand,

$$\left|\alpha - \frac{p}{q}\right| > \frac{1}{q^\kappa}.$$

`Exemple.` Soit $g \geq 2$ un entier rationnel et soit $(a_n)_{n\geq 0}$ une suite bornée d'entiers rationnels. On suppose qu'une infinité d'entre eux ne sont pas nuls. Montrons que *le nombre*

$$\vartheta = \sum_{n\geq 0} a_n g^{-n!}$$

*est un nombre de Liouville.*

Soit $A = \max_{n\geq 0} |a_n|$ et soit $\kappa > 0$ un nombre réel. Prenons pour $N$ un entier suffisamment grand avec $a_{N+1} \neq 0$ et posons

$$q = g^{N!}, \quad p = \sum_{n=0}^{N} a_n g^{N!-n!}.$$

On a $p \in \mathbf{Z}$, $q \in \mathbf{Z}$, $q > 0$ et

$$\vartheta - \frac{p}{q} = \frac{a_{N+1}}{g^{(N+1)!}} + \sum_{k\geq 2} \frac{a_{N+k}}{g^{(N+k)!}}.$$

Pour $k \geq 2$ on utilise l'estimation grossière

$$(N+k)! - (N+1)! \geq N + k$$

qui donne, pour $N$ suffisamment grand,

$$\sum_{k\geq 2} \frac{|a_{N+k}|}{g^{(N+k)!}} \leq \frac{A}{g^{(N+1)!}} \sum_{k\geq 2} \frac{1}{g^{N+k}} < \frac{1}{g^{(N+1)!}} \leq \frac{|a_{N+1}|}{g^{(N+1)!}},$$

donc $\vartheta \neq p/q$ et

$$0 < \left|\vartheta - \frac{p}{q}\right| \leq \frac{2|a_{N+1}|}{g^{(N+1)!}}.$$

On utilise enfin $|a_{N+1}| \leq A$ et $g^{(N+1)!} = q^{N+1}$, d'où

$$0 < \left|\vartheta - \frac{p}{q}\right| \leq \frac{2A}{q^{N+1}}.$$

Il en résulte que $\vartheta$ est un nombre de Liouville.

[2] `Exercice : rédiger la démonstration de cette affirmation.`

Après que Liouville ait construit les premiers exemples de nombres transcendants, G. Cantor a donné un autre argument qui montre non seulement qu'il existe des nombres transcendants, mais aussi qu'il y en a *beaucoup*. La première étape consiste à montrer que les nombres algébriques forment un ensemble dénombrable. Pour cela il remarque que pour chaque couple $(d, H)$ d'entiers positifs, il n'y a qu'un nombre fini de polynômes à coefficients entiers de degré $\leq d$ dont tous les coefficients ont une valeur absolue $\leq H$, et chacun de ces polynômes n'a qu'un nombre fini de racines. La réunion de l'ensemble de ces racines, quand $d$ et $H$ varient, est une réunion dénombrable d'ensembles dénombrables, donc est dénombrable, et c'est l'ensemble des nombres algébriques.

Pour obtenir l'existence de nombres transcendants, Cantor introduit son *argument diagonal* : si on numérote les nombres algébriques de l'intervalle $(0, 1)$ et qu'on écrit chacun d'eux avec son développement en base 2 (en prenant soin d'écrire les deux développements pour les quotients d'un entier par une puissance de 2, l'un qui termine par des 0, l'autre qui termine par des 1), disons

$$\begin{aligned} x_1 &= 0, a_{11}\, a_{12}\, a_{13} \cdots a_{1n} \cdots \\ x_2 &= 0, a_{21}\, a_{22}\, a_{33} \cdots a_{2n} \cdots \\ x_3 &= 0, a_{31}\, a_{32}\, a_{33} \cdots a_{3n} \cdots \\ &\vdots \\ x_m &= 0, a_{m1}\, a_{m2}\, a_{m3} \cdots a_{mn} \cdots \\ &\vdots \end{aligned}$$

et si on pose $b_n = 1 - a_{nn}$, alors le nombre réel

$$y = 0, b_1 b_2 b_3 \cdots b_n \cdots$$

n'est pas dans la liste, puisqu'il diffère de $x_n$ au moins par le $n$-ième chiffre ; il est donc transcendant.

Cette construction donne aussi la transcendance du nombre

$$z = 0, a_{11} a_{22} a_{33} \cdots a_{nn} \cdots ,$$

puisque $y + z = 1$.

On sait (voir par exemple l'appendice 1 de [3] ou bien le chapitre 12 de [2]) que le nombre $e$ est transcendant (Hermite, 1873), que le nombre $\pi$ est transcendant (Lindemann, 1882). Plus généralement le théorème de Hermite–Lindemann s'énonce sous les deux formes équivalentes suivantes.

**Théorème 1.15** (Hermite–Lindemann)**.** *a) Soit $\alpha$ un nombre algébrique non nul et soit $\log \alpha$ un logarithme non nul de $\alpha$ (c'est-à-dire un nombre complexe tel que $\exp(\log \alpha) = \alpha$). Alors $\log \alpha$ est un nombre transcendant.*
*b) Soit $\beta$ un nombre algébrique non nul. Alors le nombre $e^\beta$ est transcendant.*

En 1934, A.O. Gel'fond et Th. Schneider ont résolu le 7ème des 23 problèmes posés par D. Hilbert en 1900. On peut de nouveau énoncer ce résultat sous deux formes équivalentes.

**Théorème 1.16** (Gel'fond–Schneider)**.** *a) Soient $\alpha$ un nombre algébrique non nul, $\beta$ un nombre algébrique irrationnel et $\log \alpha$ un logarithme non nul de $\alpha$. Alors le nombre $\alpha^\beta$, qui est défini comme $\exp(\beta \log \alpha)$, est transcendant.*
*b) Soient $\alpha_1$ et $\alpha_2$ deux nombres algébriques non nuls, $\log \alpha$ et $\log \alpha_2$ des logarithmes non nuls de $\alpha_1$ et $\alpha_2$ respectivement. On suppose que le quotient $\log \alpha_1 / \log \alpha_2$ est irrationnel. Alors $\log \alpha_1 / \log \alpha_2$ est transcendant.*

Le théorème 1.16 contient la transcendance des nombres

$$2^{\sqrt{2}}, \quad 2^i, \quad e^\pi, \quad \frac{\log 3}{\log 2}, \quad \frac{\pi}{\log 2}.$$

**Exercice.** On considère un nombre complexe non nul $a$, un nombre complexe irrationnel $b$, et une détermination non nulle $\log a$ du logarithme de $a$. Chacun des trois nombres $a$, $b$ et $a^b = e^{b \log a}$ peut être algébrique ou transcendant, ce qui fait a priori 8 possibilités, mais le théorème de Gel'fond–Schneider montre que l'une de ces possibilités est exclue : les trois nombres en question ne peuvent pas tous être algébriques. Donner un exemple de chacune des 7 autres situations (on pourra utiliser les théorèmes de Hermite–Lindemann et Gel'fond–Schneider).

# 2 Extensions Algébriques

## Quelques rappels

Consulter [3] (Chap. 2), [4] (§ 1.1) et [2] (notamment le chapitre 5) pour revoir les notions de base sur la divisibilité dans les anneaux (on les suppose toujours commutatifs unitaires et, sauf mention explicite du contraire, intègres), sur les corps (ils sont toujours supposés commutatifs), sur les *unités* d'un anneau (= éléments inversibles), les éléments *irréductibles*, les éléments *premiers* (dans un anneau intègre tout premier est irréductible), les idéaux, ainsi que les notions d'anneau principal, factoriel et euclidien.

Dans un anneau, l'élément neutre pour la multiplication (noté 1) est différent de l'élément neutre pour l'addition (noté 0). Un anneau a donc au moins deux éléments. L'homomorphisme canonique de $\mathbf{Z}$ dans un anneau $A$ a pour noyau un idéal premier de $\mathbf{Z}$ (car $A$ est supposé intègre), donc de la forme $\{0\}$ ou $p\mathbf{Z}$ avec $p$ premier. Dans le premier cas, l'anneau $A$ est de *caractéristique nulle* et on identifie $\mathbf{Z}$ à un sous-anneau de $A$, dans le second $A$ est de *caractéristique* $p$ et on identifie le corps fini $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$ à un sous-anneau de $A$.

Une intersection de sous–anneaux est un sous-anneau, ce qui permet de définir le *sous-anneau de $A$ engendré par une partie $E$ de $A$* : c'est l'intersection de tous les sous-anneaux de $A$ contenant $E$, qui est le plus petit sous-anneau de $A$ contenant $E$. Par exemple, quand $E$ est l'ensemble vide, on obtient ainsi le plus petit sous-anneau de $A$, qui est $\mathbf{Z}$ en caractéristique nulle et $\mathbf{F}_p$ en caractéristique $p$. Quand $B$ est un sous-anneau de $A$ et $E$ une partie de $A$, on désigne par $B[E]$ le sous-anneau de $A$ engendré par $B \cup E$. Si $E$ est un ensemble fini $\{x_1, \ldots, x_n\}$, on écrit $B[x_1, \ldots, x_n]$ au lieu de $B[\{x_1, \ldots, x_n\}]$ : c'est l'image de l'unique homomorphisme de $B$–algèbres de l'anneau des polynômes $B[X_1, \ldots, X_n]$ dans $A$ qui envoie $X_i$ sur $x_i$.

De même une intersection de sous-corps d'un corps $K$ est un sous-corps de $K$. Si $k$ est un sous-corps de $K$ et $E$ une partie de $K$, on désigne par $k(E)$ le sous corps de $K$ engendré par $k \cup E$ : c'est le corps des fractions de $k[E]$. Ainsi $k(E)$ est l'ensemble des éléments de $K$ de la forme $R(\alpha_1, \ldots, \alpha_n)$ quand $\{\alpha_1, \ldots, \alpha_n\}$ décrit les familles finies d'éléments de $E$ et $R$ l'ensemble des fractions rationnelles dans $k(X_1, \ldots, X_n)$ dont le dénominateur ne s'annule pas au point $(\alpha_1, \ldots, \alpha_n)$.

On écrit encore $k(E, E')$ au lieu de $k(E \cup E')$ et $k(\alpha)$ au lieu de $k(\{\alpha\})$.

## 2.1 Extensions de corps

Soient $L$ un corps et $K$ un sous-corps de $L$. On dit alors que $L$ est une *extension* de $K$. On écrit aussi une telle extension $L/K$. Dans ces conditions $L$ est un $K$-espace vectoriel. On dit que l'extension est *finie* si le $K$-espace vectoriel $L$ est de dimension finie sur $K$. Cette dimension est notée $[L : K]$ et appelée le *degré* de l'extension $L/K$. On a $[L : K] = 1$ si et seulement si $L = K$.

Une extension $L/K$ est *de type fini* s'il existe un ensemble fini $E$ tel que $L = K(E)$. Elle est *monogène* s'il existe $\alpha \in L$ tel que $L = K(\alpha)$ ; dans ce cas $\alpha$ est un *générateur* de l'extension $L/K$.

**Lemme 2.1.** *Soient $K \subset L \subset F$ trois corps. L'extension $F/K$ est finie si et seulement si les deux extensions $L/K$ et $F/L$ sont finies. Dans ce cas*

$$[F : K] = [F : L][L : K].$$

$$\begin{matrix} & F & \\ [F : L] & | & \\ & L & \end{matrix} \quad \begin{matrix} \\ \Big) [F : K] \\ \\ \end{matrix}$$
$$[L : K] \begin{pmatrix} | \\ K \end{pmatrix}$$

*Démonstration.* Si $\{\alpha_i \ ; \ i \in I\}$ est une base de $L/K$ et $\{\beta_j \ ; \ j \in J\}$ est une base de $F/L$, alors $\{\alpha_i\beta_j \ ; \ (i, j) \in I \times J\}$ est une base de $F/K$. □

Avec les notations du lemme 2.1, on a les équivalences

$$[L : K] = 1 \Longleftrightarrow [F : L] = [F : K] \Longleftrightarrow L = K$$

et

$$[F : L] = 1 \Longleftrightarrow [L : K] = [F : K] \Longleftrightarrow L = F.$$

## 2.2 Extensions algébriques et extensions transcendantes

Soient $A$ un anneau, $K$ un sous-corps de $A$ et $\alpha$ un élément de $A$. Considérons l'homomorphisme de $K$-algèbres $\Phi : K[X] \to A$ qui envoie $X$ sur $\alpha$. Son image $K[\alpha]$ est le sous anneau de $A$ engendré par $K \cup \{\alpha\}$, son noyau $\ker \Phi$ est un idéal de $K[X]$. Les deux anneaux $K[X]/\ker \Phi$ et $K[\alpha]$ sont isomorphes.

Si $\ker \Phi = \{0\}$, c'est-à-dire si $\Phi$ est injectif, on dit que $\alpha$ est *transcendant* sur $K$. Alors les anneaux $K[X]$ et $K[\alpha]$ sont isomorphes et le corps des fractions $K(\alpha)$ de $K[\alpha]$ est isomorphe au corps des fractions rationnelles $K(X)$.

Supposons $\ker \Phi \neq \{0\}$. On dit alors que $\alpha$ est *algébrique* sur $K$. L'anneau $K[X]$ est principal, donc il existe un unique polynôme unitaire $f \in K[X]$ qui engendre l'idéal $\ker \Phi$. C'est le polynôme de degré *minimal* qui s'annule en $\alpha$. Comme $A$ est intègre, ce polynôme est irréductible dans l'anneau $K[X]$ ; on dit que $f$ est *le polynôme irréductible* [3] *de $\alpha$ sur $K$*. L'idéal $\ker \Phi$ est maximal, le quotient $K[X]/\ker \Phi$ est un corps, donc $K[\alpha] = K(\alpha)$. L'extension $K(\alpha)/K$ est finie, de degré $[K(\alpha) : K]$ le degré du polynôme $f$, qu'on appelle encore le *degré* de $\alpha$ sur $K$. Une base de $K(\alpha)$ comme $K$-espace vectoriel est $\{1, \alpha, \alpha^2, \ldots, \alpha^{d-1}\}$.

[3] Dans certains ouvrages ce que nous appelons polynôme irréductible est appelé *polynôme minimal de $\alpha$ sur $K$*. Nous garderons l'appellation *polynôme minimal* pour le polynôme irréductible sur $\mathbf{Z}[X]$ d'un nombre algébrique.

Une extension $L/K$ est dite *algébrique* si tout élément de $L$ est algébrique sur $K$. Dans le cas contraire on dit qu'elle est *transcendante*. Comme nous l'avons vu, quand le corps de base $K$ est celui des rationnels, on dit seulement qu'un nombre est *algébrique* ou *transcendant*, en sous-entendant *sur* $\mathbf{Q}$.

**Lemme 2.2.** *Si $L/K$ est une extension finie, alors c'est une extension algébrique et, pour tout $\alpha \in L$, le degré $[K(\alpha) : K]$ de $\alpha$ sur $K$ divise le degré $[L : K]$ de $L$ sur $K$.*

*Démonstration.* L'extension $L/K$ étant finie, pour tout $\alpha \in L$ les éléments

$$1, \alpha, \alpha^2, \ldots, \alpha^n, \ldots$$

sont liés dans le $K$-espace vectoriel $L$, donc $\alpha$ est algébrique sur $K$. Comme $K(\alpha)$ est un sous-corps de $L$ contenant $K$, son degré $[K(\alpha) : K]$ sur $K$ divise $[L : K]$, d'après le lemme 2.1. □

$L$

|

$K(\alpha)$

|

$K$

Par exemple quand $\alpha$ est algébrique sur $K$, pour tout $\beta \in K(\alpha)$ le degré de $\beta$ sur $K$ divise le degré de $\alpha$ sur $K$.

Il résulte aussi du lemme 2.2 que si $L$ est une extension finie de $K$ de degré premier $p$, alors pour tout élément $\alpha$ de $L$ qui n'est pas dans $K$ on a $L = K(\alpha)$.

**Lemme 2.3.** *Soit $L/K$ une extension et soient $\alpha_1, \ldots, \alpha_m$ des éléments de $L$ qui sont algébriques sur $K$. Alors $K(\alpha_1, \ldots, \alpha_m)$ est une extension finie de $K$.*

*Démonstration.* On peut démontrer ce résultat par récurrence sur $m$. Pour $m = 1$ l'extension $K(\alpha_1)/K$ est finie car $\alpha_1$ est algébrique sur $K$. Comme $\alpha_m$ est algébrique sur $K$, il l'est sur le corps $K(\alpha_1, \ldots, \alpha_{m-1})$ et le lemme 2.1 joint à l'hypothèse de récurence permet de conclure. □

Il est évident qu'une extension finie est de type fini et, d'après le lemme 2.2, elle est aussi algébrique ; le lemme 2.3 montre que, réciproquement, une extension algébrique de type fini est finie.

**Lemme 2.4.** *Soient $K \subset L \subset E$ trois corps. L'extension $E/K$ est algébrique si et seulement si les deux extensions $L/K$ et $E/L$ sont algébriques.*

*Démonstration.* Si l'extension $E/K$ algébrique, il est clair sur la définition que chacune des deux extensions $L/K$ et $E/L$ est algébrique. Inversement, supposons les deux extensions $L/K$ et $E/L$ algébriques. Soit $\alpha \in E$. Comme $E$ est algébrique sur $L$, il existe un polynôme non nul de $L[X]$ qui s'annule en $\alpha$. Soient $a_0, \ldots, a_m$ ses cœfficients ; chacun d'eux est un élément de $L$, donc est algébrique sur $K$. Maintenant $\alpha$ est algébrique sur $K(a_0, \ldots, a_m)$. Le lemme 2.1 montre que l'extension $K(a_0, \ldots, a_m, \alpha)/K$ est finie, donc (lemme 2.2) algébrique et ainsi $\alpha$ est algébrique sur $K$.

□

**Lemme 2.5.** *Soit $L/K$ une extension et soit $A$ une partie de $L$. On suppose que tous les éléments de $A$ sont algébriques sur $K$. Alors $K(A)$ est une extension algébrique de $K$ et on a $K[A] = K(A)$.*

*Démonstration.* Soit $\beta \in K(A)$. Il existe une partie finie $\{\alpha_1, \ldots, \alpha_m\}$ de $A$ telle que $\beta \in K(\alpha_1, \ldots, \alpha_m)$. Le lemme 2.4 montre que $\beta$ est algébrique sur $K$. Il reste à vérifier que $K[A]$ est un corps. Soit $\gamma \in K[A]$, $\gamma \neq 0$. Alors $K[\gamma] \subset K[A]$ et comme $\gamma$ est algébrique sur $K$ on a $K(\gamma) = K[\gamma]$, d'où $\gamma^{-1} \in K[A]$.

□

**Exercice.** Soient $L/K$ une extension, $\alpha \in L$ un élément algébrique sur $K$ de degré $d$ et soit

$$\gamma = a_0 + a_1\alpha + \cdots + a_{d-1}\alpha^{d-1}$$

un élément non nul de $K(\alpha)$ avec $a_i \in K$ $(0 \leq i \leq d-1)$. On note $P$ le polynôme irréductible de $\alpha$ sur $K$. En utilisant l'algorithme d'Euclide pour calculer un pgcd, dire comment on peut écrire $1/\gamma$ sous la forme

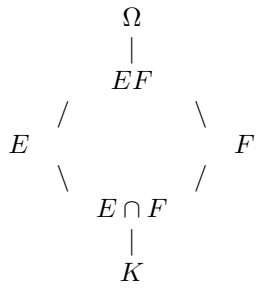
$$\frac{1}{\gamma} = b_0 + b_1\alpha + \cdots + b_{d-1}\alpha^{d-1}$$

avec $b_i \in K$ $(0 \leq i \leq d-1)$.

Soient $E$ et $F$ deux sous-corps d'un corps $\Omega$. L'intersection de tous les sous-corps de $\Omega$ qui contiennent $E \cup F$ est le plus petit sous-corps de $\Omega$ qui contienne $E$ et $F$, c'est à la fois $E(F)$ et $F(E)$. On le note $EF$ et on l'appelle *le composé* (ou *compositum*) de $E$ et $F$.

Quand $K$ est un sous corps de $E \cap F$, on a $EF = K(E, F)$ ; de plus l'extension $EF/K$ est finie (resp. algébrique) si et seulement si les deux extensions $E/K$ et $F/K$ sont finies (resp. algébriques).

**Lemme 2.6.** *Soient $\Omega/K$ une extension de corps, $E$ et $F$ deux sous-corps de $\Omega$ qui contiennent $K$. Si l'extension $F/K$ est algébrique, alors l'extension $EF/E$ est aussi algébrique et $EF = E[F]$.*




*Démonstration.* Soit $\alpha \in F$. Par hypothèse $\alpha$ est algébrique sur $K$, donc sur $E$. Le lemme 2.5 avec $A = F$ et $L = EF$ montre que $E[F] = E(F)$ et que l'extension $E(F)/E$ est algébrique. □

Soit $\Omega/K$ une extension de corps. On dit que $K$ est *algébriquement fermé* dans $\Omega$ si tout élément de $\Omega$ algébrique sur $K$ appartient à $K$.

**Exemple.** On montre dans le cours d'analyse complexe que le corps $\mathbf{C}(z)$ des fractions rationnelles est algébriquement fermé dans le corps des fonctions méromorphes sur $\mathbf{C}$.

**Lemme 2.7.** *Soit $\Omega/K$ une extension. L'ensemble $E$ des éléments de $\Omega$ algébriques sur $K$ est un corps, algébriquement fermé dans $\Omega$.*

*Démonstration.* Soient $\alpha$ et $\beta$ deux éléments de $E$. Les lemmes 2.2 et 2.3 entraînent que l'extension $K(\alpha, \beta)$ est algébrique, donc $\alpha + \beta \in E$ et $\alpha\beta \in E$ ; de plus $\alpha^{-1} \in E$ si $\alpha \neq 0$.

Soit $\gamma$ un élément de $\Omega$ algébrique sur $E$. L'extension $E(\gamma)/E$ est finie (lemme 2.3), donc algébrique (lemme 2.2), par conséquent $E(\gamma)$ est une extension algébrique de $K$ (lemme 2.4). Il s'ensuit que $\gamma$ est algébrique sur $K$, et par définition de $E$ cela veut dire que $\gamma$ est dans $E$.

□

Ce corps $E$, qui est la plus grande extension algébrique de $K$ contenue dans $\Omega$, est la *fermeture algébrique de $K$ dans $\Omega$*. C'est aussi la plus petite extension de $K$ contenue dans $\Omega$ qui soit algébriquement fermée dans $\Omega$.

On désignera par $\overline{\mathbf{Q}}$ l'ensemble des nombres complexes algébriques sur $\mathbf{Q}$ ; c'est le *corps des nombres algébriques*. La fermeture algébrique de $\mathbf{Q}$ dans $\mathbf{R}$ est le corps $\overline{\mathbf{Q}} \cap \mathbf{R}$ des nombres algébriques réels.

**Exercice.** Montrer que $\overline{\mathbf{Q}}$ est une extension algébrique de $\mathbf{Q}$ qui n'est pas finie.

Un corps $\Omega$ est dit *algébriquement clos* s'il vérifie les propriétés équivalentes suivantes :
(i) tout polynôme non constant de $\Omega[X]$ a au moins une racine dans $\Omega$
(ii) tout polynôme non constant de $\Omega[X]$ se décompose complètement dans $\Omega[X]$
(iii) les éléments irréductibles de l'anneau $\Omega[X]$ sont les polynômes de degré 1.

Un corps algébriquement clos est algébriquement fermé dans toute extension.

Si $K$ est un corps, une extension $\Omega$ de $K$ est appelée *clôture algébrique de $K$* si $\Omega$ est un corps algébriquement clos et $\Omega/K$ est une extension algébrique.

Quand $\Omega$ est un corps algébriquement clos et $K$ un sous-corps de $\Omega$, la fermeture algébrique de $K$ dans $\Omega$ est une clôture algébrique de $K$.

**Exemple.** Le corps $\mathbf{C}$ est algébriquement clos et $\overline{\mathbf{Q}}$ est une clôture algébrique de $\mathbf{Q}$ (voir par exemple [4] § 2.3 et appendice du Chap. 2, [3] Chap. V § 2).

Nous admettrons l'existence, pour tout corps $K$, d'un corps $\Omega$ algébriquement clos contenant $K$ (voir par exemple [3] Chap. V § 2 Theorem 2.5).

**Théorème 2.8.** *Tout corps $K$ admet une clôture algébrique.*

*Démonstration.* Soit $\Omega$ un corps algébriquement clos contenant $K$. Soit $\overline{K}$ la fermeture algébrique de $K$ dans $\Omega$. Alors $\overline{K}$ est une clôture algébrique de $K$. □

**Remarque.** On peut aussi montrer que si $\overline{K}_1$ et $\overline{K}_2$ sont deux clôtures algébriques de $K$, alors il existe un isomorphisme de $\overline{K}_1$ sur $\overline{K}_2$ dont la restriction à $K$ est l'identité. Il n'y a pas unicité d'un tel isomorphisme : le groupe des automorphismes d'une clôture algébrique de $K$ dont la restriction à $K$ est l'identité est le *groupe de Galois absolu de $K$*.

Étant donné que tout homomorphisme d'un corps dans un anneau est injectif, se donner une extension revient à se donner un homomorphisme d'un corps dans un autre. Plus précisément, si $\sigma : K \to L$ est un homomorphisme de corps, alors le corps $\sigma(K)$ est isomorphe à $K$ et $L$ est une extension de $\sigma(K)$. Dans ces conditions on dit que $\sigma$ est un isomorphisme de $K$ *dans* $L$. On étend $\sigma$ en l'unique homomorphisme (encore noté $\sigma$) de $K[X]$ dans $L[X]$ qui envoie $X$ sur $X$ et coïncide avec $\sigma$ sur $K$ :

$$\sigma\big(a_0 + a_1X + \cdots + a_nX^n\big) = \sigma(a_0) + \sigma(a_1)X + \cdots + \sigma(a_n)X^n.$$

Soient $E$ et $L$ deux extensions d'un même corps $K$ et soit $\sigma : E \to L$ un isomorphisme de $E$ dans $L$. On dit que $\sigma$ est un *$K$-isomorphisme* si la restriction de $\sigma$ à $K$ est l'identité.

Si $E_1$ et $E_2$ sont deux corps entre lesquels il existe un homomorphisme de corps $\sigma : E_1 \to E_2$, alors $E_1$ et $E_2$ ont la même caractéristique et le même sous-corps premier $F$ (plus précisément il

y a un isomorphisme unique entre leurs sous-corps premiers, ce qui nous autorise à les identifier). Dans ce cas $\sigma$ est un $F$-isomorphisme de $E_1$ dans $E_2$.

Soit $L/K$ une extension. Deux éléments $\alpha$ et $\beta$ de $L$ sont dits *conjugués* sur $K$ s'il existe un $K$-isomorphisme $\sigma$ de $K(\alpha)$ dans $K(\beta)$ tel que $\sigma(\alpha) = \beta$. Dans ce cas $\sigma$ est unique et surjectif. La conjugaison définit une relation d'équivalence sur $L$.

**Lemme 2.9.** *Soient $L/K$ une extension et $\alpha$, $\beta$ deux éléments de $L$. Si $\alpha$ est transcendant sur $K$, alors $\beta$ est conjugué de $\alpha$ sur $K$ si et seulement si $\beta$ est aussi transcendant. Si $\alpha$ est algébrique sur $K$, alors $\beta$ est conjugué de $\alpha$ si et seulement si $\beta$ est algébrique sur $K$ avec le même polynôme irréductible que $\alpha$ sur $K$.*

*Démonstration.* Si $\alpha$ est transcendant sur $K$, alors $K(\alpha)$ est isomorphe au corps $K(X)$ des fractions rationnelles sur $X$, donc à tout $K(\beta)$ avec $\beta$ transcendant sur $K$. Dans ces conditions, comme $K(\alpha)$ n'est pas de degré fini sur $K$, il ne peut pas être isomorphe à $K(\beta)$ quand $\beta$ est algébrique sur $K$.

Supposons maintenant $\alpha$ et $\beta$ algébriques sur $K$ et conjugués. Soit $\sigma : K(\alpha) \to K(\beta)$ un $K$-isomorphisme tel que $\sigma(\alpha) = \beta$. Notons $f \in K[X]$ le polynôme irréductible de $\alpha$ sur $K$. On a $f(\alpha) = 0$, donc $\sigma\big(f(\alpha)\big) = 0$. Mais, comme la restriction à $K$ de $\sigma$ est l'identité et que les coefficients de $f$ sont dans $K$, on a

$$\sigma\big(f(\alpha)\big) = f\big(\sigma(\alpha)\big) = f(\beta).$$

Donc $\beta$ est racine de $f$.

Enfin si $\alpha$ et $\beta$ sont algébriques racines du même polynôme irréductible $f \in K[X]$, alors $K(\alpha)$ et $K(\beta)$ sont tous deux isomorphes au corps $K[X]/(f)$. En effet le morphisme d'anneaux $K[X] \to K[\alpha]$ qui envoie $X$ sur $\alpha$ et laisse fixe les éléments de $K$ a pour image $K[\alpha] = K(\alpha)$ et pour noyau l'idéal $(f)$ de $K[X]$. L'isomorphisme de corps de de $K(\alpha)$ sur $K(\beta)$ qui rend commutatif le diagramme

$$\begin{array}{ccc} K[X] & \to & K[\beta] \\ \downarrow & \nearrow_{\sigma} & \\ K[\alpha] & & \end{array}$$

n'est autre que l'application $K$-linéaire $\sigma$ de $K(\alpha)$ dans $K(\beta)$ définie sur la base $\{1, \alpha, \ldots, \alpha^{n-1}\}$ (où $n$ désigne le degré de $\alpha$) par $\sigma(\alpha^i) = \beta^i$ $(0 \leq i \leq n-1)$. □

## 2.3 Corps de rupture d'un polynôme

Soient $K$ un corps et $f \in K[X]$ un polynôme irréductible. Une extension $L/K$ est un *corps de rupture de $f$ sur $K$* s'il existe une racine $\alpha$ de $f$ dans $L$ telle que $L = K(\alpha)$.

**Exemple.** Si 1, $j$ et $j^2$ désignent les trois racines cubiques de l'unité dans $\mathbf{C}$, chacun des trois corps $\mathbf{Q}(\sqrt[3]{2})$, $\mathbf{Q}(j\sqrt[3]{2})$ et $\mathbf{Q}(j^2\sqrt[3]{2})$ est un corps de rupture sur $\mathbf{Q}$ du polynôme $X^3 - 2$.

L'existence d'un corps de rupture est donnée par le lemme suivant :

**Lemme 2.10.** *Soient $K$ un corps et $f$ un polynôme irréductible de $K[X]$. L'idéal principal $(f)$ de $K[X]$ est maximal, le quotient $L = K[X]/(f)$ contient (un sous-corps isomorphe à) $K$ et $L$ est un corps de rupture de $f$ sur $K$.*

*Démonstration.* Soit $j$ l'injection naturelle de $K$ dans $K[X]$ et soit $s : K[X] \to K/(f)$ la surjection canonique de noyau l'idéal $(f)$ engendré par $f$. Alors $\sigma = s \circ j$ est un isomorphisme de $K$ dans $L$. Soit $\alpha \in L$ la classe de $X$ modulo $f$ et soit $g = \sigma(f) \in \sigma(K)[X]$. On a

$$g(\alpha) = s(f) = 0.$$

Ainsi on voit que $L$ est un corps de rupture sur $\sigma(K)$ du polynôme $g = \sigma(f)$. Comme $\sigma(K)$ est un corps isomorphe à $K$ on peut l'identifier avec $K$ et alors $g = f$. □

Un corps de rupture est unique à isomorphisme près :

**Lemme 2.11.** *Soient $K$ un corps, $f$ un polynôme irréductible de $K[X]$, $\varphi : K \to K'$ un isomorphisme de $K$ sur un corps $K'$, $L$ un corps de rupture de $f$ sur $K$, $\alpha$ une racine de $f$ dans $L$, $L'$ un corps de rupture de $\varphi f$ sur $K'$ et $\alpha'$ une racine de $\varphi f$ dans $L'$. Alors il existe un unique isomorphisme $\psi$ de $L$ sur $L'$ dont la restriction à $K$ soit $\varphi$ et tel que $\psi(\alpha) = \alpha'$.*

*Démonstration.* Comme $L = K(\alpha)$ et $L' = K(\alpha')$, l'unicité de $\psi$ est claire. Pour l'existence, on reprend l'argument de la démonstration du lemme 2.9.

□

**Exercice.** Soit $L/K$ une extension finie de degré $d$ et soit $P \in K[X]$ un polynôme irréductible sur $K$ de degré $m$. On suppose que $m$ et $d$ sont premiers entre eux. Montrer que $P$ est irréductible sur $L$.

## 2.4 Corps de décomposition d'un polynôme

Comme nous venons de le voir dans le §2.3, un corps de rupture d'un polynôme $f$ irréductible sur un corps $K$ est une extension de $K$ qui contient au moins une racine de $f$ (et qui est minimale pour cette propriété). Nous recherchons maintenant une extension qui contienne toutes les racines de $f$ - il n'est alors plus nécessaire de supposer $f$ irréductible pour étudier la question.

Soient $K$ un corps et $f$ un polynôme non constant de $K[X]$. Quand $L$ est une extension de $K$, on dit que le polynôme $f$ est *complètement décomposé* dans $L$ si $f$ est produit de facteurs linéaires de $L[X]$. On dit que $L$ est un *corps de décomposition de $f$ sur $K$* si $f$ est complètement décomposé dans $L$ et s'il existe des racines $\alpha_1, \ldots, \alpha_m$ de $f$ dans $L$ telles que $L = K(\alpha_1, \ldots, \alpha_m)$. Ainsi, $f$ est complètement décomposé dans une extension $L$ de $K$ si et seulement si on peut écrire

$$f(X) = a_0(X - \alpha_1) \cdots (X - \alpha_d)$$

avec $\alpha_1, \ldots, \alpha_d$ dans $L$ (ici $d$ est le degré de $f$ et $a_0 \in K$ est le coefficient directeur de $f$). Alors *le* corps de décomposition de $f$ dans $L$ est $K(\alpha_1, \ldots, \alpha_d)$.

L'énoncé suivant assure l'existence d'un corps de décomposition.

**Lemme 2.12.** *Soient $K$ un corps et $f$ un polynôme non constant de $K[X]$. Alors il existe un corps de décomposition $L$ de $f$ sur $K$.*

*Démonstration.* On démontre le résultat par récurrence sur le degré $d$ de $f$. Si $d = 1$ on prend $L = K$. Supposons le résultat vrai pour tous les corps et pour les polynômes de degré $< d$. Soit $g$ un facteur irréductible de $f$, soit $E$ un corps de rupture sur $K$ de $g$ et soit $\alpha \in E$ une racine de $g$ dans $E$ telle que $E = K(\alpha)$. Alors dans $E[X]$ on a $f(X) = (X - \alpha)h(X)$ avec $h$ de degré $d-1$. Il suffit maintenant de prendre pour $L$ un corps de décomposition de $h(X)$ sur $E$ en utilisant l'hypothèse de récurrence. □

Voici maintenant l'unicité :

**Lemme 2.13.** *Soient $K$ un corps, $f$ un polynôme non constant de $K[X]$, $\varphi : K \to K'$ un isomorphisme de $K$ sur un corps $K'$, $L$ un corps de décomposition de $f$ sur $K$ et $L'$ un corps de décomposition de $\varphi f$ sur $K'$. Alors il existe un isomorphisme $\psi$ de $L$ sur $L'$ dont la restriction à $K$ soit $\varphi$.*

*Démonstration.* On va démontrer le résultat par récurrence sur le degré $d$ de $f$, le cas $d = 1$ étant banal. Supposons le résultat vrai pour tous les corps et tous les polynômes de degré $< d$. Soient $g$ un facteur irréductible de $f$ dans $K[X]$, $\alpha$ une racine de $g$ dans $L$, $\alpha'$ une racine de $\varphi \circ g$ dans $L'$. Le lemme 2.11 montre qu'il existe un isomorphisme $\theta$ de $K(\alpha)$ sur $K(\alpha')$ qui envoie $\alpha$ sur $\alpha'$ et dont la restriction à $K$ soit $\varphi$. On remarque que $L$ est un corps de décomposition sur $K(\alpha)$ du polynôme $h(X) = f(X)/(X - \alpha)$ et $L'$ est un corps de décomposition sur $K'(\alpha')$ du polynôme $\theta\big(h(X)\big) = \varphi\big(f(X)\big)/(X - \alpha')$. L'hypothèse de récurrence permet de conclure.

□

L'isomorphisme $\psi$ qui étend $\varphi$ n'est en général pas unique. Si on en choisit un, on obtient tous les autres en le composant avec un $K$-automorphisme de $L$. Un tel automorphisme est déterminé par son action sur les racines de $f$, qui est une permutation. La théorie de Galois a pour but d'étudier ces permutations.

Nous allons voir maintenant qu'un corps de décomposition contenu dans une extension $E$ de $K$ est stable sous tout $K$-automorphisme de $E$ :

**Lemme 2.14.** *Soit $L$ un corps de décomposition d'un polynôme de $K[X]$, soit $E$ une extension de $L$ et soit $\sigma$ un $K$-isomorphisme de $L$ dans $E$. Alors $\sigma(L) = L$.*

*Démonstration.* Soient $\alpha_1, \ldots, \alpha_d$ les racines dans $L$ du polynôme considéré. On a $L = K(\alpha_1, \ldots, \alpha_d)$ et $\sigma$ permute les $\alpha_i$, donc $\sigma(L) = K(\alpha_1, \ldots, \alpha_d) = L$.

□

# Références


[1] J.H. Conway & R.K. Guy – *The book of numbers*, Copernicus Books, Springer Science + Business Media, 2006.

[2] D. Duverney – *Théorie des nombres : cours et exercices corrigés*, Paris : Dunod. viii, 244 p., 1998.

[3] S. Lang – *Algèbre*, Dunod, 2004.

[4] P. Samuel – *Théorie algébrique des nombres*, Hermann, Paris, 1967.

[5] W. M. Schmidt – *Diophantine approximation*, Lecture Notes in Mathematics, vol. 785, Springer-Verlag, Berlin, 1980.

[6] J-P. Serre – *Cours d'arithmétique*, Coll. SUP, Presses Universitaires de France, Paris, 1970.