Corps, courbes et surfaces

Fabien Priziac

Licence 3 Spécialité Mathématiques, année universitaire 2021-2022

Table des matières

Chapitre 1

Extensions de corps et algébricité

Dans ce document, un corps désigne un anneau commutatif unitaire dont tout élément non nul est inversible.

1.1 Extensions de corps

Soient K et L deux corps et soit $j : K \to L$ un morphisme de corps i.e. un morphisme d'anneaux unitaires entre les corps K et L.

Lemme 1.1.1. *Le morphisme $j : K \to L$ est injectif et l'image $j(K)$ de K par j est un sous-corps de L isomorphe à K.*

Démonstration. Soit $x \in K$ tel que $j(x) = 0_L$, supposons par l'absurde que $x \neq 0_K$. Alors x est inversible dans K et $j(x)j\left(x^{-1}\right) = j\left(xx^{-1}\right) = j(1_K) = 1_L$. En particulier, $j(x)$ est inversible dans L, ce qui est impossible car $j(x) = 0_L$. Ainsi, $x = 0_K$ et j est donc inversible.

L'image $j(K)$ de K par j est un sous-anneau unitaire de L et, si $x \in K$ tel que $j(x) \neq 0_L$, i.e. $x \neq 0_K$ d'après ce que nous venons de démontrer, alors $j(x)j\left(x^{-1}\right) = 1_L$ et donc $j(x)$ est inversible dans $j(K)$: $j(K)$ est donc bien un sous-corps de L.

Enfin, l'application restreinte $K \to j(K)$; $x \to j(x)$ est un morphisme de corps surjectif et injectif : il s'agit donc d'un isomorphisme de corps. □

On pourra donc identifier K et le sous-corps $j(K)$ de L, et on appelle un tel morphisme de corps $j : K \to L$ une extension du corps K.

Remarque 1.1.2. Si K est un sous-corps de L, le morphisme d'inclusion $K \to L$; $x \mapsto x$ est un morphisme de corps et donc une extension de K.

Par abus de terminologie, on dira également que L est une extension du corps K.

Exemple 1.1.3.

1. Via l'inclusion, le corps $\mathbb{R}$ des nombres réels est une extension du corps $\mathbb{Q}$ des nombres rationnels. De façon analogue, le corps $\mathbb{C}$ des nombres complexes est une extension du corps $\mathbb{R}$ des nombres réels. Le corps $\mathbb{C}$ est également une extension du corps $\mathbb{Q}$.

2. Comme la composition de morphismes d'anneaux unitaires est un morphisme d'anneaux unitaires, si $\widetilde{j} : L \to M$ est une extension du corps L, alors $\widetilde{j} \circ j : K \to M$ est une extension du corps K.

3. Via l'injection $i : K \to K(X)\ ;\ x \to \frac{x}{1_K}$, le corps $K(X)$ des fractions rationnelles en une variable sur K est une extension de K.

4. Si on note $\mathbb{Q}[\sqrt{2}]$ le sous-ensemble $\left\{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\right\}$ de $\mathbb{R}$, $\mathbb{Q}[\sqrt{2}]$ est un sous-corps de $(\mathbb{R}, +, \times)$ contenant $\mathbb{Q}$:

   - si $a \in \mathbb{Q}$, $a = a + 0 \cdot \sqrt{2} \in \mathbb{Q}[\sqrt{2}]$, en particulier $1 \in \mathbb{Q}[\sqrt{2}]$,
   - si $a, b, a', b' \in \mathbb{Q}$, on a

     $$(a + b\sqrt{2}) - (a' + b'\sqrt{2}) = (a - a') + (b - b')\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$$

     et

     $$(a + b\sqrt{2})(a' + b'\sqrt{2}) = aa' + 2bb' + (ab' + a'b)\sqrt{2} \in \mathbb{Q}[\sqrt{2}],$$

   - si $a, b \in \mathbb{Q}$, $a + b\sqrt{2} = 0$ ssi $a = b = 0$ (si $a + b\sqrt{2} = 0$ et si $b = 0$, alors $a = 0$ et, si $b \neq 0$, alors $\sqrt{2} = \frac{-a}{b} \in \mathbb{Q}$, ce qui est impossible) et, si $(a, b) \neq (0, 0)$,

     $$(a + b\sqrt{2})(a - b\sqrt{2}) = a^2 - 2b^2$$

     et $a^2 - 2b^2 \neq 0$ (car sinon $a^2 - 2b^2 = 0$ et donc, si $b = 0$, alors $a = 0$ ce qui est impossible et, si $b \neq 0$, alors $\sqrt{2} = \frac{|a|}{|b|} \in \mathbb{Q}$ ce qui est impossible) donc

     $$(a + b\sqrt{2}) \left(\frac{a}{a^2 - 2b^2} + \frac{-b}{a^2 - 2b^2}\sqrt{2} \right) = 1$$

     et $\frac{a}{a^2-2b^2} + \frac{-b}{a^2-2b^2}\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$, donc $a + b\sqrt{2}$ est inversible dans $\mathbb{Q}[\sqrt{2}]$.

   Le corps $\mathbb{Q}[\sqrt{2}]$ est donc une extension du corps $\mathbb{Q}$.

Le morphisme $j : K \to L$ permet de plus de munir L d'une structure d'espace vectoriel sur K :

Proposition 1.1.4. *Le groupe abélien $(L, +)$ muni de la loi de composition externe*

$$\begin{array}{ccc} K \times L & \to & L \\ (\lambda, x) & \mapsto & \lambda \cdot x := j(\lambda)x \end{array}$$

est un K-espace vectoriel.

Démonstration. Si $\lambda, \mu \in K$ et $x, y \in L$, on a

$$\lambda \cdot (x + y) = j(\lambda)(x + y) = j(\lambda)x + j(\lambda)y = \lambda \cdot x + \lambda \cdot y,$$

ainsi que

$$(\lambda + \mu) \cdot x = j(\lambda + \mu)x = \big(j(\lambda) + j(\mu)\big)x = j(\lambda)x + j(\mu)x = \lambda \cdot x + \mu \cdot x,$$

et

$$(\lambda\mu)\cdot x = j(\lambda\mu)x = j(\lambda)j(\mu)x = j(\lambda)\big(\mu\cdot x\big) = \lambda\cdot(\mu\cdot x),$$

et enfin

$$1_K\cdot x = j(1_K)x = 1_L x = x.$$

□

Remarque 1.1.5. Etant de plus un anneau commutatif, le K-espace vectoriel L est même une algèbre sur le corps K (pour $\lambda\in K$, $x,y\in L$, on a

$$\begin{aligned}\lambda\cdot(xy) = j(\lambda)xy &= \big(j(\lambda)x\big)y = (\lambda\cdot x)y\\ &= x\big(j(\lambda)y\big) = x(\lambda\cdot y)\ ).\end{aligned}$$

On appelle degré de l'extension L sur K la dimension du K-espace vectoriel L. On note $[L:K]$ cette quantité, et on dit que l'extension L est de degré fini sur K si le degré $[L:K]$ est fini, de degré infini sur K sinon. Si $[L:K]=2$, on dira que L est une extension quadratique de K.

Exemple 1.1.6. Reprenons les exemples de l'exemple 1.1.3.

1. $\mathbb{C}$ est une extension quadratique de $\mathbb{R}$: $\{1,i\}$ est une base du $\mathbb{R}$-espace vectoriel $\mathbb{C}$.
2. $\mathbb{Q}[\sqrt{2}]$ est une extension quadratique de $\mathbb{Q}$: $\{1,\sqrt{2}\}$ est une base du $\mathbb{Q}$-espace vectoriel $\mathbb{Q}[\sqrt{2}]$.
3. $\mathbb{R}$ est une extension de degré infini sur $\mathbb{Q}$: si $[\mathbb{R}:\mathbb{Q}]$ était de degré fini $d\in\mathbb{N}\backslash\{0\}$, $\mathbb{R}$ serait isomorphe au produit $\mathbb{Q}^d$ et, en tant que produit d'ensembles dénombrables, serait dénombrable, ce qui n'est pas le cas. De façon analogue, $\mathbb{C}$ est une extension de degré infini sur $\mathbb{Q}$.
4. $K(X)$ est une extension de degré infini sur $\mathbb{Q}$: le K-espace vectoriel $K[X]$ des polynômes en une variable sur K est un sous-espace vectoriel de $K(X)$ et est de dimension infinie.

Remarque 1.1.7. On a $[L:K]=1$ ssi $L=j(K)$ (car $j(K)$ est un K-sous-espace vectoriel de dimension 1 de L). En particulier, si K est un sous-corps de L et j est le morphisme d'inclusion de L dans K, $[L:K]=1$ ssi $L=K$.

Soit $\widetilde{j}: L\to M$ une extension de L. Nous avons énoncé dans l'exemple 1.1.3 2. que la composition $\widetilde{j}\circ j: K\to M$ était une extension de K. Nous allons énoncer ci-dessous le lien qui existe entre les degrés $[M:K]$, $[L:K]$ et $[M:L]$:

Théorème 1.1.8. *L'extension M est de degré fini sur K si et seulement si l'extension M est de degré fini sur L et l'extension L est de degré fini sur K, et, dans ce cas,*

$$[M:K] = [M:L][L:K]$$

(en particulier, dans ce cas, $[L:K]$ et $[M:L]$ divisent $[M:K]$).

Démonstration. Supposons que les degrés $[M : L]$ et $[L : K]$ soient finis et notons $n := [L : K]$ et $p := [M : L]$. Soient donc $\{l_1, \ldots, l_n\}$ une base de L sur K et $\{m_1, \ldots, m_p\}$ une base de M sur L, et considérons la famille $\mathcal{B} := \left\{\widetilde{j}(l_r)m_s,\ r \in \{1, \ldots, n\},\ s \in \{1, \ldots, p\}\right\}$ de M. Nous allons montrer que $\mathcal{B}$ est une base de M sur K.

Montrons tout d'abord que $\mathcal{B}$ est une famille libre du K-espace vectoriel M : soit $(\lambda_{r,s})_{\substack{1\leqslant r\leqslant n\\ 1\leqslant s\leqslant p}} \in K^{np}$ tel que

$$\sum_{\substack{1\leqslant r\leqslant n\\ 1\leqslant s\leqslant p}} \lambda_{r,s} \cdot \left(\widetilde{j}(l_r)m_s\right) = 0_M$$

i.e.

$$0_M = \sum_{\substack{1\leqslant r\leqslant n\\ 1\leqslant s\leqslant p}} \widetilde{j}\big(j(\lambda_{r,s})\big)\widetilde{j}(l_r)m_s = \sum_{1\leqslant s\leqslant p}\left(\sum_{1\leqslant r\leqslant n} \widetilde{j}\big(j(\lambda_{r,s})l_r\big)\right)m_s = \sum_{1\leqslant s\leqslant p} \widetilde{j}\left(\sum_{1\leqslant r\leqslant n} j(\lambda_{r,s})l_r\right)m_s$$

($\widetilde{j}$ est un morphisme de corps). Comme la famille $\{m_1, \ldots, m_p\}$ est une famille libre du L-espace vectoriel M, pour tout $s \in \{1, \ldots, p\}$, $\sum_{1\leqslant r\leqslant n} j(\lambda_{r,s})l_r = 0_L$ et donc, comme $\{l_1, \ldots, l_n\}$ est une famille libre du K-espace vectoriel L, pour tout $s \in \{1, \ldots, p\}$, pour tout $r \in \{1, \ldots, n\}$, $\lambda_{r,s} = 0_K$.

Montrons ensuite que $\mathcal{B}$ est une famille génératrice du K-espace vectoriel M : soit $x \in M$, alors, comme $\{m_1, \ldots, m_p\}$ est une base de M sur L, il existe $\lambda_1, \ldots, \lambda_p \in L$ tels que

$$x = \sum_{s=1}^{p} \lambda_s \cdot m_s = \sum_{s=1}^{p} \widetilde{j}\left(\lambda_s\right) m_s,$$

et, comme $\{l_1, \ldots, l_n\}$ est une base de L sur K, pour tout $s \in \{1, \ldots, p\}$, il existe $\mu_{s,1}, \ldots, \mu_{s,n}$ tels que

$$\lambda_s = \sum_{r=1}^{n} \mu_{s,r} \cdot l_r = \sum_{r=1}^{n} j\left(\mu_{s,r}\right) l_r,$$

et donc

$$\begin{aligned} x &= \sum_{s=1}^{p} \widetilde{j}\left(\lambda_s\right) m_s \\ &= \sum_{s=1}^{p} \widetilde{j}\left(\sum_{r=1}^{n} j\left(\mu_{s,r}\right) l_r\right) m_s \\ &= \sum_{\substack{1\leqslant r\leqslant n\\ 1\leqslant s\leqslant p}} \widetilde{j} \circ j\left(\mu_{s,r}\right) \widetilde{j}(l_r)m_s \\ &= \sum_{\substack{1\leqslant r\leqslant n\\ 1\leqslant s\leqslant p}} \mu_{s,r} \cdot \left(\widetilde{j}(l_r)m_s\right). \end{aligned}$$

Ainsi, la famille finie $\mathcal{B}$ de cardinal pn est bien une base M sur K : le K-espace vectoriel M est donc de dimension finie et

$$[M : K] = \dim_K M = pn = [M : L][L : K].$$

Réciproquement, supposons que l'extension M soit de degré fini sur K et montrons que les degrés $[M : L]$ et $[L : K]$ sont également finis. Pour cela, considérons une famille libre $\{l_1, \ldots, l_n\}$ du K-espace vectoriel L et une famille libre $\{m_1, \ldots, m_p\}$ du L-espace vectoriel M. Nous avons montré plus haut que la famille $\left\{\widetilde{j}(l_r)m_s,\ r \in \{1, \ldots, n\},\ s \in \{1, \ldots, p\}\right\}$ du K-espace vectoriel M était alors libre. En tant que telle et comme $[M : K] = \dim_K M$ est finie, le cardinal np de cette famille vérifie $np \leqslant [M : K]$. En particulier, $n \leqslant [M : K]$ et $p \leqslant [M : K]$. Autrement dit, toute famille d'au moins $[M : K] + 1$ éléments de L, resp. M, est K-liée, resp. L-liée.

Mais, si L était un K-espace vectoriel de dimension infinie, toute sous-famille finie de tout cardinal d'une base infinie de L serait libre. Le degré de L sur K est donc bien fini. De même, M est un L-espace vectoriel de dimension finie. □

1.2 Extensions engendrées

Soient K et L deux corps tels que K est un sous-corps de L : L est donc une extension de K. Soit A un sous-ensemble de L. On note $K(A)$ l'intersection de tous les sous-corps de L contenant K et A. Alors :

Proposition 1.2.1. *$K(A)$ est le plus petit (pour l'inclusion) sous-corps de L contenant K et A.*

Démonstration. Tout d'abord, $K(A)$ est bien un sous-corps de L, car l'intersection (quelconque) de sous-corps de L est un sous-corps de L. Ensuite, $K(A)$ contient bien K et A, car K et A sont contenus dans tous les sous-corps de L contenant K et A, donc dans $K(A)$.

Montrons enfin qu'il s'agit du plus petit sous-corps de L contenant K et A. Considérons pour cela un sous-corps M de L contenant K et A, alors $K(A) \subset M$ car $K(A)$ est l'intersection de tous les sous-corps de L contenant K et A. □

Le sous-corps $K(A)$ de L est appelé sous-corps de L engendré par K et A. Il s'agit en particulier d'une extension du corps K et on l'appelle également extension de K engendrée par A.

Si $A = \{a_1, \ldots, a_p\}$ est fini, on note habituellement $K(a_1, \ldots, a_p) := K(\{a_1, \ldots, a_p\})$.

Exemple 1.2.2.

1. On a $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}[\sqrt{2}]$. En effet, $\mathbb{Q}[\sqrt{2}]$ est un sous-corps de $\mathbb{R}$ contenant $\mathbb{Q}$ et $\sqrt{2}$, ce qui montre que $\mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}[\sqrt{2}]$. Réciproquement, comme $\mathbb{Q}(\sqrt{2})$ est un corps contenant $\mathbb{Q}$ et $\sqrt{2}$, $\mathbb{Q}(\sqrt{2})$ contient tous les nombres réels de la forme $a + b\sqrt{2}$, $a, b \in \mathbb{Q}$, donc $\mathbb{Q}(\sqrt{2})$ contient $\mathbb{Q}[\sqrt{2}]$.
2. On a $\mathbb{R}(i) = \mathbb{C}$. En effet, $\mathbb{R}(i) \subset \mathbb{C}$ et, comme $\mathbb{R}(i)$ est un corps contenant $\mathbb{R}$ et i, $\mathbb{R}(i)$ contient tous les éléments de la forme $a + bi$, $a, b \in \mathbb{R}$, autrement dit $\mathbb{R}(i)$ contient $\mathbb{C}$.

Proposition 1.2.3. *Soit B un sous-ensemble de L. Alors $K(A \cup B) = \big(K(A)\big)(B)$.*

Démonstration. On a $A \cup B \subset K(A) \cup B$ (car $K(A)$ contient A) et $K(A) \cup B \subset \big(K(A)\big)(B)$ (car $\big(K(A)\big)(B)$ contient $K(A)$ et B), donc $A \cup B \subset \big(K(A)\big)(B)$. De plus, $\big(K(A)\big)(B)$ est un sous-corps de L contenant $K(A)$ donc K. Ainsi, comme $\big(K(A)\big)(B)$ est un sous-corps de L contenant K et $A \cup B$, $K(A \cup B) \subset \big(K(A)\big)(B)$.

Réciproquement, $K(A \cup B)$ est un sous-corps de L contenant $K(A)$ (car $K(A \cup B)$ est un sous-corps de L contenant K et $A \cup B$ donc A, et donc $K(A) \subset K(A \cup B)$) ainsi que B, et donc $\big(K(A)\big)(B) \subset K(A \cup B)$. □

Remarque 1.2.4.

1. On écrira $K(A)(B) := \big(K(A)\big)(B)$.
2. On a $K(A)(B) = \big(K(A)\big)(B) = K(A \cup B) = K(B \cup A) = \big(K(B)\big)(A) = K(B)(A)$.
3. Si $a, b \in L$, on a $K(a, b) = K(a)(b) = K(b)(a)$.

On termine cette section par une description des éléments de $K(A)$:

Proposition 1.2.5. *On a*

$$K(A) = \left\{ \frac{S(a_1, \ldots, a_k)}{T(a_1, \ldots, a_k)} \;\middle|\; k \in \mathbb{N},\ a_1, \ldots, a_k \in A,\ \frac{S}{T} \in K(X_1, \ldots, X_k) \text{ tels que } T(a_1, \ldots, a_k) \neq 0 \right\}.$$

Démonstration. Notons M l'ensemble de droite. Alors

- M contient en particulier K,
- M contient également A : tout élément a de A peut s'écrire $a = X(a)$ et $X \in K(X)$,
- M est contenu dans L : si $\frac{S(a_1,\ldots,a_k)}{T(a_1,\ldots,a_k)}$ est un élément de M avec les notations ci-dessus, $S(a_1, \ldots, a_k), T(a_1, \ldots, a_k) \in L$, car L est stable par sommes et produits, et $\frac{S(a_1,\ldots,a_k)}{T(a_1,\ldots,a_k)} \in L$ car L est stable par inverses (d'éléments non nuls) et produits.
- M est un sous-corps de L : si $k, l \in \mathbb{N}$, $a_1, \ldots, a_k, b_1, \ldots, b_l \in A$, $\frac{S}{T} \in K(X_1, \ldots, X_k)$, $\frac{U}{V} \in K(Y_1, \ldots, Y_l)$ tels que $T(a_1, \ldots, a_k) \neq 0$ et $V(b_1, \ldots, b_l) \neq 0$, alors
  1. $\frac{S}{T} - \frac{U}{V} = \frac{SV - UT}{TV} \in K(X_1, \ldots, X_k, Y_1, \ldots, Y_l)$ et
  $$\frac{S(a_1, \ldots, a_k)}{T(a_1, \ldots, a_k)} - \frac{U(b_1, \ldots, b_l)}{V(b_1, \ldots, b_l)} = \left(\frac{SV - UT}{TV}\right)(a_1, \ldots, a_k, b_1, \ldots, b_l) \in M,$$
  2. $\frac{S}{T}\frac{U}{V} = \frac{SU}{TV} \in K(X_1, \ldots, X_k, Y_1, \ldots, Y_l)$ et
  $$\frac{S(a_1, \ldots, a_k)}{T(a_1, \ldots, a_k)} \frac{U(b_1, \ldots, b_l)}{V(b_1, \ldots, b_l)} = \left(\frac{SU}{TV}\right)(a_1, \ldots, a_k, b_1, \ldots, b_l) \in M,$$
  3. $\frac{S(a_1,\ldots,a_k)}{T(a_1,\ldots,a_k)} \neq 0$ ssi $S(a_1, \ldots, a_k) \neq 0$ et, dans ce cas, l'inverse de $\frac{S(a_1,\ldots,a_k)}{T(a_1,\ldots,a_k)}$ dans L est
  $$\frac{T(a_1, \ldots, a_k)}{S(a_1, \ldots, a_k)} = \left(\frac{T}{S}\right)(a_1, \ldots, a_k) \in M.$$

Au total, M est donc un sous-corps de L contenant K et A. On a donc $K(A) \subset M$. Réciproquement, si N est un sous-corps de L contenant K et A, alors N contient tout élément de la forme $\frac{S(a_1,\dots,a_k)}{T(a_1,\dots,a_k)}$ avec $k \in \mathbb{N}$, $a_1, \dots, a_k \in A$, $\frac{S}{T} \in K(X_1, \dots, X_k)$ tels que $T(a_1, \dots, a_k) \neq 0$, car N contient K et A et est stable par sommes, produits et inverses d'éléments non nuls. Ainsi, $M \subset N$, et donc $M \subset K(A)$. □

1.3 Eléments algébriques

Soient K et L deux corps tels que K est un sous-corps de L. Soit $a \in L$.

Définition 1.3.1. *On dit que a est algébrique sur K s'il existe un polynôme non nul P de $K[X]$ tel que $P(a) = 0$, transcendant sur K sinon.*

Exemple 1.3.2.

1. Si $a \in K$, alors a est algébrique sur K car a est racine du polynôme $X - a$ de $K[X]$.
2. Le nombre $\sqrt{2}$ de $\mathbb{R}$ est algébrique sur $\mathbb{Q}$ car il est racine du polynôme $X^2 - 2$ de $\mathbb{Q}[X]$.
3. Le nombre i de $\mathbb{C}$ est algébrique sur $\mathbb{Q}$ car il est racine du polynôme $X^2 + 1$ de $\mathbb{Q}[X]$ (i est donc également algébrique sur $\mathbb{R}$).
4. Tout nombre complexe $\alpha + i\beta$, $\alpha, \beta \in \mathbb{R}$, est algébrique sur $\mathbb{R}$: $\alpha + i\beta$ est en effet racine du polynôme $(X - \alpha)^2 + \beta^2$ de $\mathbb{R}[X]$.
5. Les nombres e et π sont transcendants sur $\mathbb{Q}$.

Remarque 1.3.3.

- Soit M un corps contenant $\mathbb{Q}$ et soit $x \in M$. Alors x est algébrique sur $\mathbb{Q}$ si et seulement s'il existe un polynôme non nul P de $\mathbb{Z}[X]$ tels que $P(x) = 0$. En effet, $\mathbb{Z}[X] \subset \mathbb{Q}[X]$, et si $Q \in \mathbb{Q}[X]\backslash\{0\}$ vérifie $Q(x) = 0$ alors, en notant α le PPCM des dénominateurs des coefficients du polynôme Q, $\alpha Q \in \mathbb{Z}[X]$ et $\big(\alpha Q\big)(x) = \alpha Q(x) = 0$.
- Si M désigne maintenant un sous-corps de L contenant K et si a est algébrique sur K alors a est algébrique sur M (car $K[X] \subset M[X]$).

Notons $I_a := \{P \in K[X] \mid P(a) = 0\}$. Alors $I_a \neq \{0\}$ ssi a est algébrique sur K (de manière équivalente, $I_a = \{0\}$ ssi a est transcendant sur K).

De plus, I_a est un idéal de l'anneau $K[X]$:

- le polynôme nul annule a,
- si $P, Q \in I_a$, $(P - Q)(a) = P(a) - Q(a) = 0 - 0 = 0$,
- si $P \in I_a$ et $Q \in K[X]$, alors $(PQ)(a) = P(a)Q(a) = 0 \cdot Q(a) = 0$.

Comme l'anneau $K[X]$ est principal, il existe un polynôme $P_0 \in I_a$ tel que I_a est engendré par le polynôme P_0 i.e. $I_a = (P_0) = \{P_0 Q \mid Q \in K[X]\}$.

On suppose dans la suite de cette section que a est algébrique sur K. Alors $I_a \neq (0)$ et :

Proposition et Définition 1.3.4. *Il existe un unique polynôme $\mu_{a,K}$ unitaire tel que $I_a = (\mu_{a,K})$ (en particulier, comme a est algébrique sur K i.e. $I_a \neq (0)$, $\mu_{a,K}$ est nécessairement non nul). Le polynôme $\mu_{a,K}$ est appelé polynôme minimal de a sur K.*

Démonstration. Soient $P_1, P_2 \in I_a$ unitaires tels que $I_a = (P_1) = (P_2)$ alors, en particulier, P_1 divise P_2 et P_2 divise P_1 : il existe donc $\alpha \in K^*$ tel que $P_1 = \alpha P_2$. Mais, comme les polynômes P_1 et P_2 sont tous deux unitaires, $\alpha = 1$ et donc $P_1 = P_2$. □

Remarque 1.3.5.
- Une autre façon d'exprimer le fait que $\mu_{a,K}$ engendre l'idéal I_a est de dire que l'ensemble des polynômes de $K[X]$ annulant a est l'ensemble des multiples de $\mu_{a,K}$.
- Le polynôme $\mu_{a,K}$ est nécessairement non constant : un polynôme constant non nul de $K[X]$ n'annule aucun élément de L.

L'assertion suivante nous donne un moyen de déterminer concrètement le polynôme minimal de a sur K :

Proposition 1.3.6. *Soit P un polynôme de $K[X]$. Alors $P = \mu_{a,K}$ ssi P est unitaire et irréductible dans $K[X]$ (en particulier non constant) et vérifie $P(a) = 0$.*

Démonstration. Supposons donc que P est un polynôme non nul unitaire et irréductible de $K[X]$ tel que $P(a) = 0$. Alors $P \in I_a$ et $\mu_{a,K}$ divise donc P : il existe $Q \in \mathbb{K}[X]$ tel que $P = Q\mu_{a,K}$. Mais P est irréductible dans $K[X]$ et $\mu_{a,K}$ est non constant donc, nécessairement, $Q \in K$, et P est unitaire comme $\mu_{a,K}$ donc $Q = 1$ et $P = \mu_{a,K}$.

Réciproquement, $\mu_{a,K}$ est irréductible dans $K[X]$: supposons par l'absurde qu'il existe des polynômes non constants $Q_1, Q_2 \in K[X]$ tels que $\mu_{a,K} = Q_1Q_2$ (en particulier, les degrés de Q_1 et Q_2 sont strictement plus petits que le degré de $\mu_{a,K}$), alors

$$0 = \mu_{a,K}(a) = Q_1(a)Q_2(a)$$

et donc, par intégrité de $K[X]$, $Q_1(a) = 0$ ou $Q_2(a) = 0$ i.e. $Q_1 \in I_a$ ou $Q_2 \in I_a$. Supposons sans perdre de généralité que $Q_1 \in I_a$, alors $\mu_{a,K}$ divise Q_1. Comme par hypothèse Q_1 divise également $\mu_{a,K}$, il existe $\alpha \in K^*$ tel que $Q_1 = \alpha\mu_{a,K}$. Mais $\deg Q_1 \neq \deg \mu_{a,K}$, d'où une contradiction. □

Utilisons ce lemme pour déterminer quelques polynômes minimaux.

Exemple 1.3.7.
1. Si $a \in K$, le polynôme minimal de a sur K est $X - a$: $X - a$ est unitaire, irréductible dans $K[X]$ et annule a.
2. Le polynôme minimal de $\sqrt{2}$ sur $\mathbb{Q}$ est $X^2 - 2$: $X^2 - 2$ est unitaire, irréductible dans $\mathbb{Q}[X]$ et annule $\sqrt{2}$.
3. Le polynôme minimal de i sur $\mathbb{Q}$ est $X^2 + 1$: $X^2 + 1$ est unitaire, irréductible dans $\mathbb{Q}[X]$ et annule i.
4. Le polynôme minimal du nombre réel $\sqrt[4]{2}$ sur $\mathbb{Q}$ est $X^4 - 2$: $X^4 - 2 \in \mathbb{Q}[X]$ est unitaire, annule $\sqrt[4]{2}$ et est irréductible dans $\mathbb{Q}[X]$ par le critère d'Eisenstein (le nombre premier 2 ne divise pas 1, divise 2 et $2^2 = 4$ ne divise pas 2).

5. Le polynôme minimal de $\sqrt[4]{2}$ sur $\mathbb{Q}[\sqrt{2}]$ est $X^2-\sqrt{2}$: le polynôme unitaire $X^2-\sqrt{2}$ de $(\mathbb{Q}[\sqrt{2}])[X]$ annule $\sqrt[4]{2}$ donc $\mu_{\sqrt[4]{2},\mathbb{Q}[\sqrt{2}]}$ divise $X^2-\sqrt{2}$ dans $(\mathbb{Q}[\sqrt{2}])[X]$, et $\mu_{\sqrt[4]{2},\mathbb{Q}[\sqrt{2}]}$ ne peut être de degré 1 sinon, par le deuxième point de la remarque suivante, $\sqrt[4]{2}$ appartiendrait à $\mathbb{Q}[\sqrt{2}]$ (ce qui n'est pas le cas : s'il existait $a,b\in\mathbb{Q}$ tels que $\sqrt[4]{2}=a+b\sqrt{2}$, alors on aurait
$$\sqrt{2}=\left(\sqrt[4]{2}\right)^2=(a+b\sqrt{2})^2=a^2+2\sqrt{2}ab+2b^2$$
et donc $\sqrt{2}(1-2ab)=a^2+2b^2$, et
   - si $1-2ab=0$, alors $a^2+2b^2=0$ donc $a=b=0$ et $\sqrt[4]{2}=0$, ce qui n'est pas le cas,
   - si $1-2ab\neq 0$, alors $\sqrt{2}=\frac{a^2+2b^2}{1-2ab}\in\mathbb{Q}$, ce qui n'est pas le cas).

Remarque 1.3.8.
- Comme on peut notamment le constater avec les deux derniers exemples ci-dessus, le polynôme minimal de a sur K dépend bien du corps K : on a $\mu_{\sqrt[4]{2},\mathbb{Q}}=X^4-2$ et $\mu_{\sqrt[4]{2},\mathbb{Q}[\sqrt{2}]}=X^2-\sqrt{2}$.

- On a $\deg\mu_{a,K}=1$ ssi $\mu_{a,K}=X-a$ ssi $a\in K$. En effet, on a montré plus haut que si $a\in K$, alors $\mu_{a,K}=X-a$. De plus, si $\mu_{a,K}=X-a$ alors $\deg\mu_{a,K}=1$. Enfin, si $\deg\mu_{a,K}=1$, alors $\mu_{a,K}=X-\alpha$ avec $\alpha\in K$ et, comme $0=\mu_{a,K}(a)=a-\alpha$, on a $a=\alpha\in\mathbb{K}$.

- Soit $b\in L$ tel que $\mu_{a,K}(b)=0$, alors $\mu_{b,K}=\mu_{a,K}$: en effet, $\mu_{a,K}$ est alors un polynôme unitaire et irréductible dans $K[X]$ qui annule b.

Soit $d\in\mathbb{N}\backslash\{0\}$. Si $d=\deg\mu_{a,K}$, on dit que a est algébrique de degré d sur K.

Exemple 1.3.9.
1. D'après la remarque précédente, a est algébrique de degré 1 sur K ssi $a\in K$.

2. $\sqrt{2}$ et i sont algébriques de degré 2 sur $\mathbb{Q}$.

3. $\sqrt[4]{2}$ est algébrique de degré 4 sur $\mathbb{Q}$ et est algébrique de degré 2 sur $\mathbb{Q}[\sqrt{2}]$.

Soit $b\in L$, notons $K[b]$ le sous-ensemble $\{P(b)\mid P\in K[X]\}$ de L : il s'agit de l'image du morphisme d'anneaux (unitaires) $\varphi_b : K[X]\to L\ ;\ P\mapsto P(b)$, en particulier $K[b]$ est un sous-anneau de L.

Lemme 1.3.10. *$K[b]$ est le plus petit sous-anneau de L contenant K et b.*

Démonstration. Tout d'abord, remarquons que $K[b]$ contient bien b et K : on peut écrire $b=\varphi_b(X)$ et, si $x\in K$, $x=\varphi_b(x)$.

Ensuite, soit R un sous-anneau de L contenant K et b alors, par stabilité de R par sommes et produits et comme R contient K et b, R contient tout élément de la forme $P(b)$ avec $P\in K[X]$, et donc $K[b]\subset R$. □

Remarque 1.3.11.
- $K[b]$ est l'intersection de tous les sous-anneaux de L contenant K et b.

- Remarquons également que $K[b]$ est un espace vectoriel sur K : l'application φ_b est une application linéaire entre les K-espaces vectoriels $K[X]$ et L, et son image $K[b]$ est donc un sous-espace vectoriel de L. Une famille génératrice du K-espace vectoriel $K[b]$ est $\{b^s, s \in \mathbb{N}\}$.
- On a $K[b] \subset K(b)$ car $K(b)$ est un sous-anneau (car sous-corps) de L contenant K et b.

Nous allons montrer que, comme a est algébrique sur K, $K[a] = K(a)$, en particulier $K[a]$ est un corps. Plus précisément :

Proposition 1.3.12. *Les propriétés suivantes sont équivalentes :*

1. *b est algébrique sur K,*
2. *la dimension du K-espace vectoriel $K[b]$ est finie,*
3. *$K[b]$ est un corps,*
4. *$K[b] = K(b)$.*

Démonstration. Prouvons cette proposition par démonstration circulaire :

1. $\Rightarrow$ 2. : Si b est algébrique sur K, il existe $P \in K[X]$ non nul tel que $P(b) = 0$. Si on écrit $P = \sum_{r=0}^{d} a_r X^r$ avec $a_d \neq 0$, on a donc $0 = \sum_{r=0}^{d} a_r b^r$ i.e. $b^d = -\sum_{r=0}^{d-1} \left(a_d^{-1} a_r\right) b^r$, et donc $\{b^s, s \in \mathbb{N}\} \subset \mathrm{Vect}_K\{1, \ldots, b^{d-1}\}$. Ainsi, la famille $\{1, \ldots, b^{d-1}\}$ engendre $K[b]$, en particulier, $K[b]$ est de dimension finie sur K.

2. $\Rightarrow$ 3. : Supposons que $\dim_K K[b]$ soit finie, et soit y un élément non nul de $K[b]$. Considérons l'application $\psi : K[b] \to K[b]$; $x \mapsto yx$: il s'agit d'un endomorphisme linéaire du K-espace vectoriel $K[b]$. ψ est de plus injective : si $x \in K[b]$ vérifie $\psi(x) = 0$ i.e. $yx = 0$ alors, comme $y \neq 0$ et $K[b]$ est un anneau intègre (en tant que sous-anneau du corps L), nécessairement $x = 0$. Mais, comme $K[b]$ est, par hypothèse, un K-espace vectoriel de dimension finie, ψ est alors également surjective : il existe donc $x \in K[b]$ tel que $1 = \psi(x)$ i.e. $1 = yx$, et donc en particulier y est inversible dans $K[b]$. $K[b]$ est donc bien un corps.

3. $\Rightarrow$ 4. : Si $K[b]$ est un corps, alors, comme $K[b]$ contient K et b, on a $K(b) \subset K[b]$. Mais $K(b)$ est un sous-anneau de L contenant K et b donc $K[b] \subset K(b)$.

4. $\Rightarrow$ 1. : Supposons que $K[b] = K(b)$. Si $b = 0$, alors $b \in K$ donc b est algébrique sur K. Si $b \neq 0$, comme $K(b)$ est un corps, $b^{-1} \in K(b) = K[b]$: il existe donc $P = \sum_{r=0}^{d} a_r X^r \in K[X]$ tel que

$$b^{-1} = P(b) = \sum_{r=0}^{d} a_r b^r$$

donc

$$1 = \sum_{r=0}^{d} a_r b^{r+1} \text{ i.e. } 1 - \sum_{r=0}^{d} a_r b^{r+1} = 0 \text{ i.e. } \left(1 - \sum_{r=0}^{d} a_r X^{r+1}\right)(b) = 0,$$

et b est donc algébrique sur K (le polynôme P est non nul car sinon $b^{-1} = P(b)$ serait nul). □

Remarque 1.3.13. En particulier, si b est algébrique sur K, l'extension $K(b)$ de K est de degré fini.

Complétons la propriété précédente. On rappelle que a est algébrique sur K. Notons alors d le degré du polynôme minimal $\mu_{a,K}$ de a sur K.

Proposition 1.3.14. *La famille* $\{a^s, s \in \{0, \dots, d-1\}\}$ *est une base du* K*-espace vectoriel* $K(a) = K[a]$. *En particulier,* $[K(a) : K] = d$.

Démonstration. Notons $\mathcal{B} := \{a^s, s \in \{0, \dots, d-1\}\}$ et montrons tout d'abord que $\mathcal{B}$ est une famille libre de $K[a]$: soient donc $\lambda_0, \dots, \lambda_{d-1} \in K$ tels que

$$\sum_{s=0}^{d-1} \lambda_s a^s = 0$$

i.e. $P(a) = 0$ où $P := \sum_{s=0}^{d-1} \lambda_s X^s \in K[X]$. Ainsi $P \in I_a$ donc $\mu_{a,K}$ divise P. Mais $\deg P \leqslant d-1$ et $\deg \mu_{a,K} = d$ donc, nécessairement, $P = 0$ i.e. pour tout $s \in \{0, \dots, d-1\}$, $\lambda_s = 0$.

Montrons ensuite que $\mathcal{B}$ engendre le K-espace vectoriel $K[a]$. Soit $P \in K[X]$ et considérons la division euclidienne de P par $\mu_{a,K}$: il existe $Q, R \in K[X]$ tels que $P = Q\mu_{a,K} + R$ et $\deg R < \deg \mu_{a,K}$. On a alors

$$P(a) = Q(a)\mu_{a,K}(a) + R(a) = R(a)$$

et donc, si l'on écrit $R := \sum_{s=0}^{N} \mu_s X^s$ avec $N \leqslant d-1$, $P(a) = R(a) = \sum_{s=0}^{N} \mu_s a^s \in \mathrm{Vect}_K(\mathcal{B})$. □

Exemple 1.3.15. Utilisons la proposition précédente pour déterminer le degré de l'extension $\mathbb{Q}(\sqrt{2}, i)$ de $\mathbb{Q}$. On a $\mathbb{Q}(\sqrt{2}, i) = \mathbb{Q}(\sqrt{2})(i)$ et considérons la suite d'inclusions $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt{2})(i)$ de sous-corps de $\mathbb{R}$. D'après le théorème 1.1.8,

$$[\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2})(i) : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}].$$

Nous avions déterminé dès l'exemple 1.1.6 que l'extension $\mathbb{Q}(\sqrt{2})$ de $\mathbb{Q}$ était de degré 2.

Ensuite, le polynôme minimal de i sur $\sqrt{2}$ est X^2+1 (car X^2+1 annule i, est unitaire et est irréductible sur $\mathbb{R}$ donc sur $\mathbb{Q}(\sqrt{2}) \subset \mathbb{R}$) donc, d'après la proposition précédente, $[\mathbb{Q}(\sqrt{2})(i) : \mathbb{Q}(\sqrt{2})] = 2$ et donc

$$[\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2})(i) : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2 \times 2 = 4.$$

Remarque 1.3.16. Reprenons notre élément b quelconque de L. Le morphisme d'anneaux (unitaires) $\varphi_b : K[X] \to K[b]$ est surjectif (par définition) et induit l'isomorphisme d'anneaux (unitaires)

$$\overline{\varphi_b} : \begin{array}{ccc} K[X]/I_b & \to & K[b] \\ \overline{P} & \mapsto & P(b) \end{array}$$

par la propriété universelle du quotient (Ker $\varphi_b = \{P \in K[X] \mid P(b) = 0\} = I_b$).

Ainsi,

- si b est transcendant sur K, $\overline{\varphi_b}$ est un isomorphisme de $K[X]$ sur $K[b]$,
- si b est algébrique sur K, $\overline{\varphi_b}$ est un isomorphisme de $K[X]/(\mu_{b,K})$ sur $K[b] = K(b)$.

1.4 Extensions algébriques

Soient K et L deux corps tels que K est un sous-corps de L.

Définition 1.4.1. *L'extension L de K est dite algébrique sur K si tout élément de L est algébrique sur K.*

Exemple 1.4.2.
1. L'extension $\mathbb{C}$ de $\mathbb{R}$ est algébrique sur $\mathbb{R}$: nous avons montré dans l'exemple 1.3.2 4. que tout nombre complexe était racine d'un polynôme de degré 2 à coefficients réels.
2. L'extension $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}[\sqrt{2}]$ de $\mathbb{Q}$ est algébrique sur $\mathbb{Q}$: si $a, b \in \mathbb{Q}$, le nombre $a + b\sqrt{2}$ est racine du polynôme $(X - a)^2 - 2b^2$ de $\mathbb{Q}[X]$.

Plus généralement, toute extension de degré fini est algébrique :

Proposition 1.4.3. *On suppose que L est de degré fini sur K. Alors L est algébrique sur K. De plus, si on note $n := [L : K]$, tout élément de L est algébrique sur K de degré au plus égal à n.*

Démonstration. Soit $a \in L$ et considérons la famille $\{a^s \mid s \in \{0, \dots, n\}\}$ de L.

S'il existe $s_1, s_2 \in \{0, \dots, n\}$ avec $s_1 \neq s_2$ tels que $a^{s_1} = a^{s_2}$, alors le polynôme non nul $X^{s_1} - X^{s_2}$ de $K[X]$ annule a donc a est algébrique sur K.

Supposons maintenant que les éléments a^s, $s \in \{0, \dots, n\}$ sont deux à deux distincts. Alors, la famille $\{a^s \mid s \in \{0, \dots, n\}\}$ étant de cardinal $n + 1$ et L étant de dimension n, cette famille ne peut être libre et il existe donc $\lambda_0, \dots, \lambda_n \in K$ non tous nuls tels que

$$\sum_{s=0}^{n} \lambda_s a^s = 0 \text{ i.e. } \left(\sum_{s=0}^{n} \lambda_s X^s \right)(a) = 0.$$

Le polynôme $P := \sum_{s=0}^{n} \lambda_s X^s$ de $K[X]$ étant non nul (car les scalaires $\lambda_0, \dots, \lambda_n \in K$ sont non tous nuls), a est algébrique sur K et, de plus, $\deg \mu_{a,K} \leqslant \deg P$ (car $\mu_{a,K}$ divise P) donc $\deg \mu_{a,K} \leqslant n$. □

Soient maintenant a et b deux éléments algébriques de L (l'extension L de K n'est ici pas supposée algébrique ou de degré fini). Alors :

Proposition 1.4.4. *L'extension $K(a, b)$ de K est de degré fini.*

Démonstration. Considérons la suite d'inclusions $K \subset K(a) \subset K(a, b)$ de sous-corps de L. Comme a est algébrique sur K, l'extension $K(a)$ de K de degré fini par la proposition 1.3.12 (voir aussi la remarque 1.3.13). De plus, b est algébrique sur K donc sur $K(a)$, et l'extension $K(a, b) = K(a)(b)$ de $K(a)$ est donc de degré fini.

D'après le théorème 1.1.8, l'extension $K(a, b)$ est donc de degré fini sur K. □

En conséquence :

Corollaire 1.4.5. *L'extension $K(a,b)$ de K est algébrique. En particulier, $a+b$ et ab sont algébriques sur K, ainsi que, si $b \neq 0$, le quotient $\frac{a}{b}$.*

Démonstration. L'extension $K(a,b)$ de K est de degré fini par la proposition précédente, et est donc algébrique par la proposition 1.4.3. Comme $a+b, ab \in K(a,b)$, $a+b$ et ab sont algébriques sur K. Si $b \neq 0$, $\frac{a}{b}$ appartient également à $K(a,b)$ et est donc algébrique sur K. □

Remarque 1.4.6.

- Les éléments algébriques $a+b$, ab et, si $b \neq 0$, $\frac{a}{b}$ sont tous de degré au plus égal à $[K(a,b) : K]$ d'après la proposition 1.4.3. Par ailleurs, si n est le degré de a sur K et p est le degré de b sur K alors $[K(a,b) : K(a)] \leqslant p$ (car $\mu_{b,K(a)}$ divise $\mu_{b,K}$) et donc $[K(a,b) : K] = [K(a,b) : K(a)][K(a) : K] \leqslant pn$.

- Si $a_1, \ldots, a_m$ sont des éléments de L algébriques sur K, on peut également montrer, par récurrence sur m, que l'extension $K(a_1, \ldots, a_m)$ de K est de degré fini, et donc algébrique sur K. Il s'ensuit que tout élément de L de la forme $\frac{S(a_1,\ldots,a_m)}{T(a_1,\ldots,a_m)}$, où $a_1, \ldots, a_m$ sont des éléments algébriques sur K et $\frac{S}{T}$ est une fraction rationnelle de $K(X_1, \ldots, X_m)$ tels que $T(a_1, \ldots, a_m) \neq 0$, est algébrique sur K.

- Le corollaire montre que le sous-ensemble $\widehat{K}$ de L formé des éléments algébriques sur K est un sous-corps de L (contenant K) : si $a, b \in \widehat{K}$, alors $a-b$ et ab sont également dans $\widehat{K}$ car $a-b$ et ab sont dans l'extension algébrique $K(a,b)$, et, si $a \neq 0$, $a^{-1} \in \widehat{K}$ car a^{-1} est dans $K(a,b)$ et est donc également algébrique.

Exemple 1.4.7. En appliquant les résultats précédents, nous pouvons affirmer que $\sqrt{2}+i$ est un élément algébrique sur $\mathbb{Q}$ de degré au plus égal à 4. De plus, comme

- $\sqrt{2}+i \notin \mathbb{Q}$,
- $\mathbb{Q}(\sqrt{2}+i) \subset \mathbb{Q}(\sqrt{2}, i)$ donc $[\mathbb{Q}(\sqrt{2}+i) : \mathbb{Q}]$ divise $[\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}]$,
- $[\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}] = 4$ (d'après l'exemple 1.3.15),

nous savons que le degré de $\sqrt{2}+i$ sur $\mathbb{Q}$ est 2 ou 4. Supposons qu'il existe un polynôme P de la forme $P = X^2 + \beta X + \gamma$, $\beta, \gamma \in \mathbb{Q}$ tel que

$$\begin{aligned} P(\sqrt{2}+i) = 0 &\Leftrightarrow (\sqrt{2}+i)^2 + \beta(\sqrt{2}+i) + \gamma = 0 \\ &\Leftrightarrow 1 + 2\sqrt{2}i + \beta(\sqrt{2}+i) + \gamma = 0 \\ &\Leftrightarrow 1 + \beta\sqrt{2} + \gamma + \big(2\sqrt{2} + \beta\big)i = 0 \\ &\Rightarrow 2\sqrt{2} + \beta = 0 \\ &\Rightarrow \sqrt{2} = -\frac{\beta}{2}, \end{aligned}$$

ce qui est impossible : $\sqrt{2}+i$ est donc algébrique de degré 4 sur $\mathbb{Q}$.

En particulier, $[\mathbb{Q}(\sqrt{2}+i) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}]$ et donc, comme $\mathbb{Q}(\sqrt{2}+i) \subset \mathbb{Q}(\sqrt{2}, i)$, $\mathbb{Q}(\sqrt{2}+i) = \mathbb{Q}(\sqrt{2}, i)$.

Pour terminer cette section, restreignons-nous à l'étude de l'extension $\mathbb{Q} \subset \mathbb{C}$ et montrons le résultat suivant :

Lemme 1.4.8. *Soit α un élément de $[0; +\infty[$ algébrique sur $\mathbb{Q}$ et soit $n \in \mathbb{N}\backslash\{0\}$. Alors $\sqrt[n]{\alpha}$ est également algébrique sur $\mathbb{Q}$.*

Démonstration. Considérons d'une part la suite d'inclusions

$$\mathbb{Q} \subset \mathbb{Q}(\alpha) \subset \mathbb{Q}(\alpha, \sqrt[n]{\alpha})$$

de sous-corps de $\mathbb{R}$:

- le polynôme $X^n - \alpha$ de $\mathbb{Q}(\alpha)[X]$ annule $\sqrt[n]{\alpha}$ donc $\sqrt[n]{\alpha}$ est algébrique sur $\mathbb{Q}(\alpha)$ et l'extension $\mathbb{Q}(\alpha, \sqrt[n]{\alpha}) = \mathbb{Q}(\alpha)(\sqrt[n]{\alpha})$ de $\mathbb{Q}(\alpha)$ est de degré fini,
- α est algébrique sur $\mathbb{Q}$ par hypothèse donc le degré $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ est également fini.

L'extension $\mathbb{Q}(\alpha, \sqrt[n]{\alpha})$ de $\mathbb{Q}$ est donc de degré fini.

Considérons d'autre part la suite d'inclusions

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt[n]{\alpha}) \subset \mathbb{Q}(\sqrt[n]{\alpha}, \alpha) = \mathbb{Q}(\alpha, \sqrt[n]{\alpha}).$$

L'extension $\mathbb{Q}(\alpha, \sqrt[n]{\alpha})$ de $\mathbb{Q}$ étant de degré fini, d'après le théorème 1.1.8, l'extension $\mathbb{Q}(\sqrt[n]{\alpha})$ de $\mathbb{Q}$ est également de degré fini : elle est donc algébrique sur $\mathbb{Q}$ et $\sqrt[n]{\alpha} \in \mathbb{Q}(\sqrt[n]{\alpha})$ est donc algébrique sur $\mathbb{Q}$. □

Ce lemme, combiné avec le corollaire 1.4.5, nous montre que tout nombre réel exprimé à l'aide de sommes, différences, produits, quotients, racines n-ièmes, $n \in \mathbb{N}\backslash\{0\}$, de nombres rationnels est algébrique sur $\mathbb{Q}$.

Par exemple, le nombre réel $\frac{\sqrt{11}}{\sqrt[4]{3}} - \sqrt[186]{\frac{3-\sqrt[3]{5}}{2+4\sqrt{7}}}$ est algébrique sur $\mathbb{Q}$.

Chapitre 2

Constructibilité à la règle et au compas

2.1 Points constructibles du plan

Soit $(\mathcal{P})$ un plan et soient A, B et C sont trois points de $(\mathcal{P})$ tels que $A \neq B$. On note

- (AB) l'unique droite de $(\mathcal{P})$ passant par A et B,
- $[AB]$ le segment reliant les points A et B,
- $\mathcal{C}(C, [AB])$ le cercle de centre C et de rayon $[AB]$.

Soit maintenant $\mathcal{E}$ un ensemble de points du plan $(\mathcal{P})$. On note

- $\mathcal{D}_\mathcal{E}$ l'ensemble des droites passant par deux points (distincts) de $\mathcal{E}$,
- $\mathcal{C}_\mathcal{E}$ l'ensemble des cercles de centre un point de $\mathcal{E}$ et de rayon un segment reliant deux points (distincts) de $\mathcal{E}$:

$$\mathcal{D}_\mathcal{E} = \{(AB) \mid A, B \in \mathcal{E},\ A \neq B\} \text{ et } \mathcal{C}_\mathcal{E} = \{\mathcal{C}(C, [AB]) \mid A, B, C \in \mathcal{E},\ A \neq B\}.$$

Soit P un point de $(\mathcal{P})$.

Définition 2.1.1. *On dit que P est constructible en une étape à partir de $\mathcal{E}$ si P est à l'intersection de deux éléments distincts de $\mathcal{D}_\mathcal{E} \cup \mathcal{C}_\mathcal{E}$ i.e. s'il est inclus dans l'intersection*

- *de deux droites distinctes de $\mathcal{D}_\mathcal{E}$,*
- *d'une droite de $\mathcal{D}_\mathcal{E}$ et d'un cercle de $\mathcal{C}_\mathcal{E}$,*
- *ou de deux cercles distincts de $\mathcal{C}_\mathcal{E}$.*

Si $n \in \mathbb{N}\backslash\{0; 1\}$, on dira qu'un point P est constructible en n étapes à partir de $\mathcal{E}$ s'il existe une suite finie $P_1, \ldots, P_n$ de points de plan tels que

1. *P_1 est constructible en une étape à partir de $\mathcal{E}$,*

2. *pour tout* $i \in \{2, \dots, n\}$, P_i *est constructible en une étape à partir de* $\mathcal{E} \cup \{P_j,\ j \in \{1, \dots, i-1\}$,

3. $P_n = P$.

On dira également que P est constructible en zéro étape à partir de $\mathcal{E}$ si $P \in \mathcal{E}$, et finalement que P est constructible à partir de $\mathcal{E}$ (ou des points de $\mathcal{E}$) s'il existe $n \in \mathbb{N}$ tel que P est constructible en n étapes à partir de $\mathcal{E}$.

Les points du plan $(\mathcal{P})$ constructibles à partir de $\mathcal{E}$ sont exactement les points de $\mathcal{E}$ et les points que l'on peut construire à partir des points de $\mathcal{E}$ à l'aide d'une règle (non graduée) et d'un compas.

Exemple 2.1.2. Le milieu M du segment $[AB]$ est constructible à partir des points A et B. En effet,

1. soient $\mathcal{C}$ le cercle de centre A et de rayon $[AB]$ et $\mathcal{C}'$ le cercle de centre B et de rayon $[AB]$, et construisons les deux points d'intersection D et D' de $\mathcal{C}$ et $\mathcal{C}'$: comme $\mathcal{C}, \mathcal{C}' \in \mathcal{C}_{\{A,B\}}$, les points D et D' sont constructibles (en une étape) à partir de $\{A, B\}$,

2. le point M est alors le point d'intersection de la droite (AB) et de la droite (DD') : M est donc constructible (en trois étapes) à partir de $\{A, B\}$: D est constructible à partir de $\{A, B\}$, D' est constructible à partir de $\{A, B, D\}$ et enfin M est constructible à partir de $\{A, B, D, D'\}$.

Remarque 2.1.3. Si $\mathcal{E}_1$ et $\mathcal{E}_2$ sont deux ensembles de points de $(\mathcal{P})$ tels que $\mathcal{E}_1 \subset \mathcal{E}_2$, alors tout point constructible à partir de $\mathcal{E}_1$ est constructible à partir de $\mathcal{E}_2$.

Notons $\mathcal{K}(\mathcal{E})$ les points du plan constructibles à partir de $\mathcal{E}$. Il est à remarquer qu'un point constructible à partir de $\mathcal{K}(\mathcal{E})$ i.e. un point constructible à partir de points constructibles à partir de $\mathcal{E}$ est constructible à partir de $\mathcal{E}$ (i.e $\mathcal{K}\big(\mathcal{K}(\mathcal{E})\big) = \mathcal{K}(\mathcal{E})$.)

Une droite passant par deux points constructibles à partir de $\mathcal{E}$ (i.e. une droite de $\mathcal{D}_{\mathcal{K}(\mathcal{E})}$) sera également dite constructible à partir de $\mathcal{E}$. Une cercle de centre un point constructible à partir de E et de rayon un segment reliant deux points constructibles à partir de $\mathcal{E}$ (i.e. un cercle de $\mathcal{C}_{\mathcal{K}(\mathcal{E})}$), sera dit constructible à partir de $\mathcal{E}$. Il est à noter qu'un point à l'intersection de deux constructions distinctes de $\mathcal{D}_{\mathcal{K}(\mathcal{E})} \cup \mathcal{C}_{\mathcal{K}(\mathcal{E})}$ est constructible à partir de $\mathcal{E}$.

Exemple 2.1.4.

1. Reprenons le premier exemple de l'exemple 2.1.2 : la droite (DD') que nous avons construite est la médiatrice du segment $[AB]$. Comme les points D et D' sont constructibles à partir de $\{A, B\}$, la médiatrice du segment $[AB]$ est constructible à partir de $\{A, B\}$.

2. La droite perpendiculaire à (AB) passant par A est constructible à partir de A et B. En effet,

   (a) soit $\mathcal{C}$ le cercle de centre A et de rayon $[AB]$ et notons B' l'autre point d'intersection de $\mathcal{C}$ avec la droite (AB) : comme $\mathcal{C} \in \mathcal{C}_{\{A,B\}}$ et $(AB) \in \mathcal{D}_{\{A,B\}}$, le point B' est constructible (en une étape) à partir de $\{A, B\}$,

   (b) la droite perpendiculaire à (AB) passant par A est alors la médiatrice du segment $[BB']$ et est donc constructible à partir de $\{A, B\}$ puisque B et B' le sont.

3. Supposons que $C \notin (AB)$. La droite parallèle à (AB) passant par C est constructible à partir de $\{A, B, C\}$. En effet,

   (a) notons $\mathcal{C}$ le cercle de centre A et de rayon $[AC]$ et soit D l'un des deux points d'intersection de $\mathcal{C}$ avec la droite (AB) : comme $\mathcal{C} \in \mathcal{C}_{\{A,B,C\}}$ et $(AB) \in \mathcal{D}_{\{A,B,C\}}$, le point D est constructible à partir de $\{A, B, C\}$,

   (b) soit $\mathcal{C}'$ le cercle de centre D et de rayon $[AC]$ et soit $\mathcal{C}''$ le cercle de centre C et de rayon $[AC]$: $A \in \mathcal{C}' \cap \mathcal{C}''$ et comme D, A et C ne sont pas alignés, $\mathcal{C}'$ et $\mathcal{C}''$ possèdent un autre point d'intersection que l'on note E et qui est constructible à partir de $\{A, B, C\}$,

   (c) la droite (EC) passant par C est alors parallèle à la droite (AB) (car le quadrilatère de sommets A, D, E, C a ses quatre côtés de longueurs égales donc est un losange) et est constructible à partir de $\{A, B, C\}$.

4. Supposons à nouveau que les points A, B et C ne sont pas alignés. La bissectrice de l'angle $\widehat{ABC}$ est constructible à partir de $\{A, B, C\}$. En effet,

   (a) soit $\mathcal{C}$ le centre de centre B et de rayon $[BA]$ et notons D le point d'intersection de $\mathcal{C}$ et (BC) situé sur la demi-droite $[BC)$: comme $\mathcal{C} \in \mathcal{C}_{\{A,B,C\}}$ et $(BC) \in \mathcal{D}_{\{A,B,C\}}$, le point D est constructible à partir de $\{A, B, C\}$,

   (b) la bissectrice de l'angle $\widehat{ABC}$ est alors la médiatrice du segment $[AD]$, qui est constructible à partir de $\{A, D\}$ d'après l'exemple 1 et est donc constructible à partir de $\{A, B, C\}$ puisque le point D est constructible à partir de $\{A, B, C\}$.

2.2 Constructibilité et extensions de corps

Reprenons notre plan $(\mathcal{P})$ et soit $\mathcal{E}$ un ensemble de points de $(\mathcal{P})$ contenant au moins deux points distincts O et A.

Considérons ensuite un point B du plan tel que B est à l'intersection de la droite perpendiculaire à (OA) passant par O et du cercle de centre O et de rayon $[OA]$: d'une part, le point B est constructible à partir de $\{O, A\}$ (cf. exemple 2.1.4 2) et, d'autre part, le triplet (O, A, B) forme un repère orthonormal du plan $(\mathcal{P})$. Notons (x, y) les coordonnées (réelles) dans le repère (O, A, B) (dans ce repère, O, A et B ont pour coordonnées respectives $(0, 0)$, $(1, 0)$ et $(0, 1)$).

Notons ensuite $\mathbb{Q}(\mathcal{E})$ l'extension de $\mathbb{Q}$ engendrée dans $\mathbb{R}$ par les coordonnées des points de E. Précisément, si $\mathcal{E} = \{P_i,\ i \in I\}$ et si, pour $i \in I$, le point P_i a pour coordonnées (x_i, y_i) dans le repère (O, A, B), on définit

$$\mathbb{Q}(\mathcal{E}) := \mathbb{Q}\left(\bigcup_{i\in I}\{x_i, y_i\}\right).$$

Exemple 2.2.1. 1. On a

$$\mathbb{Q}\big(\{O, A\}\big) = \mathbb{Q}(0, 0, 1, 0) = \mathbb{Q}.$$

2. Soit C le point du plan $(\mathcal{P})$ tel que le quadrilatère $OACB$ est un carré. Soient ensuite D et E les deux points d'intersection du cercle de centre O et de rayon $[OC]$ et de la

droite (OB) (il est à remarquer que C, D et E sont constructibles à partir de $\{O, A\}$). On a $\mathbb{Q}\big(\{O, A, D, E\}\big) = \mathbb{Q}(\sqrt{2})$.

En effet, les coordonnées de D et E dans le repère (O, A, B) sont $(0, \sqrt{2})$ et $(0, -\sqrt{2})$ et on a donc

$$\mathbb{Q}\big(\{O, A, D, D'\}\big) = \mathbb{Q}(0, 0, 1, 0, 0, \sqrt{2}, 0, -\sqrt{2}) = \mathbb{Q}(\sqrt{2}).$$

Remarque 2.2.2. Si $\mathcal{E}_1$ et $\mathcal{E}_2$ sont deux ensembles de points de $(\mathcal{P})$ tels que $\mathcal{E}_1 \subset \mathcal{E}_2$, alors $\mathbb{Q}(\mathcal{E}_1) \subset \mathbb{Q}(\mathcal{E}_2)$ i.e. $\mathbb{Q}(\mathcal{E}_2)$ est une extension de $\mathbb{Q}(\mathcal{E}_1)$.

Nous allons établir un lien entre la constructibilité à partir de $\mathcal{E}$ et l'existence d'extensions particulières du corps $\mathbb{Q}(\mathcal{E})$.

Dans la suite, lorsque le contexte sera clair, nous dirons simplement qu'un point, une droite ou un cercle de $(\mathcal{P})$ est constructible si l'objet en question est constructible à partir de $\mathcal{E}$.

Par ailleurs, nous prendrons la liberté de désigner un point par ses coordonnées dans le repère (O, A, B).

Soit P un point de $(\mathcal{P})$ de coordonnées (x_0, y_0) dans le repère (O, A, B). Remarquons que $\mathbb{Q}\big(\mathcal{E} \cup \{P\}\big) = Q(\mathcal{E})(x_0, y_0)$ est une extension de $\mathbb{Q}(\mathcal{E})$ (cf. remarque 2.2.2).

Nous allons ci-dessous établir un critère nécessaire de constructibilité de P en une étape :

Proposition 2.2.3. *On suppose que P est constructible en une étape à partir de $\mathcal{E}$. Alors l'extension $\mathbb{Q}\big(\mathcal{E} \cup \{P\}\big)$ sur $\mathbb{Q}(\mathcal{E})$ est de degré fini et on a*

$$[\mathbb{Q}\big(\mathcal{E} \cup \{P\}\big) : \mathbb{Q}(\mathcal{E})] \in \{1; 2\},$$

autrement soit $\mathbb{Q}\big(\mathcal{E} \cup \{P\}\big) = \mathbb{Q}(E)$, soit $\mathbb{Q}\big(\mathcal{E} \cup \{P\}\big)$ est une extension quadratique de $\mathbb{Q}(\mathcal{E})$.

Démonstration. P étant constructible en une étape, P est à l'intersection

- de deux droites de $\mathcal{D}_{\mathcal{E}}$,
- d'une droite de $\mathcal{D}_{\mathcal{E}}$ et d'un cercle de $\mathcal{C}_{\mathcal{E}}$,
- ou de deux cercles de $\mathcal{C}_{\mathcal{E}}$.

Nous allons montrer la conclusion de la proposition dans chacun de ces trois cas. Pour cela, nous utilisons le lemme 2.2.4 ci-dessous qui donne la forme des équations, dans les coordonnées (x, y), d'une droite de $\mathcal{D}_{\mathcal{E}}$ et d'un cercle de $\mathcal{C}_{\mathcal{E}}$.

Supposons tout d'abord que P est l'unique point d'intersection de deux droites distinctes $\mathcal{D}$ et $\mathcal{D}'$ de $\mathcal{D}_{\mathcal{E}}$ d'équations respectives $ax+by+c = 0$ et $a'x+b'y+c' = 0$ dans les coordonnées (x, y), avec $a, a', b, b', c, c' \in \mathbb{Q}(\mathcal{E})$, $(a, b) \neq (0, 0)$, $(a', b') \neq (0, 0)$ (lemme 2.2.4 1). Les coordonnées (x_0, y_0) de P constituent ainsi l'unique solution du système

$$\begin{cases} ax + by &= -c \\ a'x + b'y &= -c' \end{cases}$$

qui est alors un système dit de Cramer, dont le couple solution (x_0, y_0) est donné par des quotients de déterminants en les nombres $a, a', b, b', c, c' \in \mathbb{Q}(\mathcal{E})$, donc par des fractions rationnelles en les nombres $a, a', b, b', c, c' \in \mathbb{Q}(\mathcal{E})$: par la proposition 1.2.5, $x_0, y_0 \in \mathbb{Q}(\mathcal{E})$. Ainsi, $\mathbb{Q}\big(\mathcal{E} \cup \{P\}\big) = \mathbb{Q}(\mathcal{E})(x_0, y_0) = \mathbb{Q}(\mathcal{E})$.

Supposons maintenant que P est à l'intersection d'une droite $\mathcal{D}$ d'équation $ax + by + c = 0$ et d'un cercle $\mathcal{C}$ d'équation $x^2 + y^2 + a'x + b'y + c' = 0$, avec $a, a', b, b', c, c' \in \mathbb{Q}(\mathcal{E})$, $(a, b) \neq (0, 0)$, $(a', b', c') \neq (0, 0, 0)$ (lemme 2.2.4 1 et 2). On a ainsi

$$\begin{cases} ax_0 + by_0 + c & = 0 \\ x_0^2 + y_0^2 + a'x_0 + b'y_0 + c' & = 0 \end{cases}$$

Supposons sans perdre de généralité que $b \neq 0$ (si $a \neq 0$, on permute les rôles de x_0 et y_0) et écrivons alors

$$y_0 = -\frac{ax_0 + c}{b} \in \mathbb{Q}(\mathcal{E})(x_0).$$

En particulier, $\mathbb{Q}\big(\mathcal{E} \cup \{P\}\big) = \mathbb{Q}(\mathcal{E})(x_0, y_0) = \mathbb{Q}(\mathcal{E})(x_0)$, puis

$$0 = x_0^2 + y_0^2 + a'x_0 + b'y_0 + c' = x_0^2 + \left(\frac{ax_0 + c}{b}\right)^2 + a'x_0 - b'\frac{ax_0 + c}{b} + c' :$$

le nombre x_0 est donc racine d'un polynôme de $\mathbb{Q}(\mathcal{E})[X]$ de degré 2. Ainsi, x_0 est algébrique de degré au plus 2 sur $\mathbb{Q}(E)$ et donc

$$[\mathbb{Q}\big(\mathcal{E} \cup \{P\}\big) : \mathbb{Q}(\mathcal{E})] = [\mathbb{Q}(\mathcal{E})(x_0) : \mathbb{Q}(\mathcal{E})] \leqslant 2.$$

Supposons enfin que P est à l'intersection de deux cercles distincts $\mathcal{C}$ et $\mathcal{C}'$ de $\mathcal{C}_\mathcal{E}$ d'équations respectives $x^2 + y^2 + ax + by + c = 0$ et $x^2 + y^2 + a'x + b'y + c' = 0$, avec $a, a', b, b', c, c' \in \mathbb{Q}(\mathcal{E})$, $(a, b, c) \neq (0, 0, 0)$, $(a', b', c') \neq (0, 0, 0)$ (lemme 2.2.4 2). Ainsi, les coordonnées (x_0, y_0) de P sont solution du système

$$\begin{cases} x^2 + y^2 + ax + by + c & = 0 \\ x^2 + y^2 + a'x + b'y + c' & = 0 \end{cases}$$

et donc du système

$$\begin{cases} x^2 + y^2 + ax + by + c & = 0 \\ (a' - a)x + (b' - b)y + c' - c & = 0 \end{cases}$$

(on retranche la première équation du système à la seconde). De plus, $(a' - a, b' - b) \neq (0, 0)$ car sinon on aurait $c' = c$ et les cercles $\mathcal{C}$ et $\mathcal{C}'$ seraient alors confondus : P est donc à l'intersection du cercle $\mathcal{C}$ et de la droite d'équation $(a' - a)x + (b' - b)y + c' - c = 0$ avec $a' - a, b' - b, c \in \mathbb{Q}(\mathcal{E})$ et on se ramène ainsi au système du cas précédent (attention : la droite d'équation $(a' - a)x + (b' - b)y + c' - c = 0$ n'est pas nécessairement une droite de $\mathcal{D}_\mathcal{E}$). □

Lemme 2.2.4. *1. Soit $\mathcal{D}$ une droite de $\mathcal{D}_\mathcal{E}$. Alors il existe $a, b, c \in \mathbb{Q}(\mathcal{E})$ tels que $(a, b) \neq 0$ et, pour tous $x, y \in \mathbb{R}$, le point de coordonnées (x, y) appartient à $\mathcal{D}_\mathcal{E}$ ssi*

$$ax + by + c = 0.$$

2. *Soit $\mathcal{C}$ un cercle de $\mathcal{C}_\mathcal{E}$. Alors il existe $a, b, c \in \mathbb{Q}(\mathcal{E})$ tels que $(a, b, c) \neq (0, 0, 0)$ et, pour tous $x, y \in \mathbb{R}$, le point de coordonnées (x, y) appartient à $\mathcal{C}_\mathcal{E}$ ssi*

$$x^2 + y^2 + ax + by + c = 0.$$

Démonstration. 1. La droite $\mathcal{D}$ passe, par définition, par deux points distincts M et N de $\mathcal{E}$ et, si (x_1, y_1) et (x_2, y_2) sont les coordonnées respectives de M et N, l'équation de la droite $\mathcal{D}$ en les coordonnées (x, y) est alors

$$(x-x_1)(y_2-y_1)-(y-y_1)(x_2-x_1) = 0 \text{ i.e. } (y_2-y_1)x+(x_1-x_2)y+\big(y_1(x_2-x_1)-x_1(y_2-y_1)\big) = 0$$

qui est bien de la forme voulue car $y_2 - y_1$, $x_1 - x_2$, $\big(y_1(x_2 - x_1) - x_1(y_2 - y_1)\big) \in \mathbb{Q}(\mathcal{E})$ (car $x_1, y_1, x_2, y_2 \in \mathbb{Q}(\mathcal{E})$ car $M, N \in \mathcal{E}$).

2. Soient $C, M, N \in \mathcal{E}$ tels que $M \neq N$ et $\mathcal{C} = \mathcal{C}(C, [MN])$. Alors, si (x', y'), (x_1, y_1), (x_2, y_2) désignent les coordonnées respectives des points C, M et N dans le repère (O, A, B), le segment $[MN]$ est de longueur $\sqrt{(x_2 - x_1)^2 + (y_2 - y_1)^2}$ et l'équation du cercle $\mathcal{C}$ en les coordonnées (x, y) est alors

$$(x - x')^2 + (y - y')^2 - \big((x_2 - x_1)^2 + (y_2 - y_1)^2\big) = 0$$

i.e.

$$x^2 + y^2 + (-2x')x + (-2y')y + \Big(x'^2 + y'^2 - (x_2 - x_1)^2 - (y_2 - y_1)^2\Big) = 0$$

qui est bien de la forme voulue $(-2x', -2y', x'^2 + y'^2 - (x_2 - x_1)^2 - (y_2 - y_1)^2 \in \mathbb{Q}(\mathcal{E})$ car $C, M, N \in \mathcal{E}$).

□

Remarque 2.2.5. Les réciproques respectives des assertions 1 et 2 du lemme 2.2.4 ne sont pas vraies : la droite d'équation $x + y + 1 = 0$ n'appartient pas à $\mathcal{D}_{\{O,A\}}$ bien que $1 \in \mathbb{Q}\big(\{O, A\}\big)$ et le cercle d'équation $x^2 + y^2 - 2 = 0$ n'appartient pas à $\mathcal{C}_{\{O,A\}}$ bien que $\{1; 2\} \subset \mathbb{Q}\big\{O, A\}\big)$.

On utilise ensuite la proposition 2.2.3 pour montrer le critère nécessaire de constructibilité générale suivant :

Corollaire 2.2.6. *Soit $n \in \mathbb{N}$ et supposons que le point P soit constructible en n étapes à partir de $\mathcal{E}$. Alors il existe une suite finie croissante*

$$K_0 \subset \cdots \subset K_n,$$

de sous-corps de $\mathbb{R}$ telle que

- $K_0 = \mathbb{Q}(\mathcal{E})$,
- $x_0, y_0 \in K_n$,
- *si $n \geqslant 1$, pour tout $i \in \{1, \ldots, n\}$, $[K_i : K_{i-1}] \in \{1; 2\}$.*

Démonstration. Si $n = 0$ alors $P \in \mathcal{E}$ et $x_0, y_0 \in \mathbb{Q}(\mathcal{E})$ par définition.

Si maintenant $n \in \mathbb{N}\backslash\{0\}$, il existe une suite finie $P_1, \ldots, P_n$ de points du plan tels que

- P_1 est constructible en une étape à partir de $\mathcal{E}$,
- si $n > 1$, pour tout $i \in \{2, \dots, n\}$, P_i est constructible en une étape à partir de $\mathcal{E} \cup \{P_j,\ j \in \{1, \dots, i-1\}$,
- $P_n = P$.

Notons alors $K_0 := \mathbb{Q}(\mathcal{E})$ et, pour $i \in \{1, \dots, n\}$, $K_i := \mathbb{Q}\big(\mathcal{E} \cup \{P_j,\ j \in \{1, \dots, i\}\}\big)$.

Le point P_1 étant constructible à partir de $\mathcal{E}$, d'après la proposition 2.2.3, le corps $K_1 = \mathbb{Q}\big(\mathcal{E} \cup \{P_1\}\big)$ est une extension de degré fini inférieur ou égal à deux de $K_0 = \mathbb{Q}(\mathcal{E})$.

Si $n > 1$, pour tout $i \in \{2, \dots, n\}$, le point P_i est constructible en une étape à partir de $\mathcal{E} \cup \{P_j,\ j \in \{1, \dots, i-1\}\}$: d'après la proposition 2.2.3, le corps

$$K_i = \mathbb{Q}\big(\mathcal{E} \cup \{P_j,\ j \in \{1, \dots, i-1\}\} \cup \{P_i\}\big)$$

est une extension de degré fini inférieur ou égal à deux de

$$K_{i-1} = \mathbb{Q}\big(\mathcal{E} \cup \{P_j,\ j \in \{1, \dots, i-1\}\big).$$

Enfin, $x_0, y_0 \in K_n = \mathbb{Q}\big(\mathcal{E} \cup \{P_j,\ j \in \{1, \dots, n\}\}\big)$ car $P = P_n \in \mathcal{E} \cup \{P_j,\ j \in \{1, \dots, n\}\}$. □

Nous établirons plus loin une réciproque du corollaire 2.2.6 : le théorème 2.4.1.

On déduit du corollaire 2.2.6 un autre critère nécessaire de constructibilité. Attention cependant : ce critère n'est pas suffisant.

Corollaire 2.2.7 (Critère de Wantzel)**.** *Si P est constructible à partir de $\mathcal{E}$ alors ses coordonnées x_0, y_0 sont des nombres réels algébriques sur $\mathbb{Q}(\mathcal{E})$ de degré des puissances de 2.*

Démonstration. Supposons donc que P est constructible en n étapes à partir de $\mathcal{E}$ avec $n \in \mathbb{N}$. Appliquons alors le corollaire 2.2.6 et reprenons ses notations.

Si $n = 0$, $x_0, y_0 \in K_0 = \mathcal{Q}(\mathcal{E})$ et les nombres x_0 et y_0 sont donc algébriques de degré 1 sur $\mathcal{Q}(\mathcal{E})$.

Si $n = 1$, $x_0, y_0 \in K_1$ et $[K_1 : K_0] \leqslant 2$: en particulier, l'extension K_1 sur $K_0 = \mathcal{Q}(\mathcal{E})$ est algébrique et les nombres x_0 et y_0 sont donc algébriques de degrés respectifs 1 ou 2 sur $\mathcal{Q}(\mathcal{E})$.

Si $n > 1$, on a, d'après le théorème de multiplicativité des degrés (théorème 1.1.8),

$$[K_n : K_0] = [K_n : K_{n-1}] \cdots [K_1 : K_0]$$

et $[K_n : K_0]$ est donc une puissance de deux (car chaque terme du produit est soit 1 soit 2).

En particulier, K_n est une extension de degré fini de $K_0 = \mathbb{Q}(\mathcal{E})$: elle est donc algébrique sur $\mathbb{Q}(\mathcal{E})$ par la proposition 1.4.3. Les nombres $x_0, y_0 \in K_n$ sont donc algébriques sur $\mathbb{Q}(\mathcal{E})$ de degrés respectifs divisant $[K_n : \mathbb{Q}(\mathcal{E})]$ qui est une puissance de deux. □

Remarque 2.2.8.

- La démonstration ci-dessus nous permet en fait de montrer une propriété plus forte. En effet, avec les notations du corollaire 2.2.6, comme $x_0, y_0 \in K_n$, toute fraction rationnelle α en les nombres x_0 et y_0 appartient à K_n (car K_n est un corps) et est donc également algébrique sur $\mathbb{Q}(\mathcal{E})$ de degré une puissance de deux car, d'après la preuve précédente, K_n est une extension algébrique sur $\mathbb{Q}(\mathcal{E})$ de degré une puissance de deux.

  De plus, si $\alpha \geqslant 0$, alors $[K_n(\sqrt{\alpha}) : K_n] \leqslant 2$ (car le polynôme $X^2 - \alpha \in K_n[X]$ annule $\sqrt{\alpha}$) donc
  $$[K_n(\sqrt{\alpha}) : \mathbb{Q}(\mathcal{E})] = [K_n(\sqrt{\alpha}) : K_n][K_n : \mathbb{Q}(\mathcal{E})]$$
  est également une extension algébrique sur $\mathbb{Q}(\mathcal{E})$ de degré une puissance de deux : comme $\sqrt{\alpha} \in K_n(\sqrt{\alpha})$, le nombre $\sqrt{\alpha}$ est également algébrique sur $\mathbb{Q}(\mathcal{E})$ de degré une puissance de deux.

- La réciproque du corollaire 2.2.7 n'est pas vraie (cf. feuille de TD 2).

2.3 Application à des problèmes de constructibilité à la règle et au compas

On utilise le critère nécessaire de constructibilité du corollaire 2.2.7 pour montrer la non-constructibilité à la règle et au compas de deux constructions géométriques.

On reprend les notations de la section précédente.

2.3.1 La quadrature du cercle

Etant fixée la longueur-unité OA (dans le repère orthonormal (O, A, B) construit à partir de $\{O, A\}$, $OA = 1$), peut-on construire à la règle et au compas à partir des points O et A un carré dont l'aire soit la même que celle du cercle de centre O et de rayon $[OA]$ i.e. un carré de côté $\sqrt{\pi}$?

Le corollaire 2.2.7 nous permet d'apporter une réponse négative à cette question. En effet, supposons par l'absurde que les sommets d'un tel carré soient constructibles à partir de $\{O, A\}$. Soient (x_1, y_1) et (x_2, y_2) les coordonnées respectives de deux sommets consécutifs M et N de ce carré. D'après le corollaire 2.2.7, les nombres réels x_1, x_2, y_1, y_2 sont algébriques sur $\mathbb{Q}\big(\{O, A\}\big) = \mathbb{Q}$, et d'après le corollaire 1.4.5 et la remarque 1.4.6 (cf. également la remarque 2.2.8), la quantité
$$(x_2 - x_1)^2 + (y_2 - y_1)^2 = MN^2$$
est alors également algébrique sur $\mathbb{Q}$.

Or $MN^2 = \sqrt{\pi}^2 = \pi$, qui est transcendant sur $\mathbb{Q}$.

2.3.2 La duplication du cube

Soit $C \in (\mathcal{P})$ tel que le quadrilatère $OACB$ soit un carré (C est constructible à partir de $\{O, A\}$), et notons $\mathcal{U}$ le cube construit à partir du carré $OACB$. La longueur-unité étant la longueur du segment $[OA]$, le cube $\mathcal{U}$ est de volume 1.

Est-il alors possible de construire à la règle et au compas à partir des points O et A un carré dont le cube associé est de volume le double du volume de $\mathcal{U}$?

Supposons qu'un tel carré soit constructible à partir de $\{O, A\}$. Si M et N sont deux sommets consécutifs de ce carré de coordonnées respectives (x_1, y_1) et (x_2, y_2), on a $MN^3 = 2$ i.e. $MN = \sqrt[3]{2}$.

Or, comme M et N sont constructibles à partir de $\{O, A\}$, d'après la remarque 2.2.8, la quantité

$$MN = \sqrt{(x_2 - x_1)^2 + (y_2 - y_1)^2}$$

est algébrique de degré une puissance de deux sur $\mathbb{Q}\big(\{O, A\}\big) = \mathbb{Q}$.

Mais $\sqrt[3]{2}$ est algébrique de degré 3 sur $\mathbb{Q}$: la duplication du cube n'est donc pas réalisable à la règle et au compas.

2.4 Critère suffisant de constructibilité

Reprenons les notations des sections précédentes et établissons la réciproque suivante du corollaire 2.2.6 :

Théorème 2.4.1. *Supposons qu'il existe une suite finie croissante*

$$K_0 \subset \cdots \subset K_m,$$

$m \in \mathbb{N}$, de sous-corps de $\mathbb{R}$ telle que

- $K_0 = \mathbb{Q}(\mathcal{E})$,
- $x_0, y_0 \in K_m$,
- *si $m \geqslant 1$, pour tout $i \in \{1, \ldots, m\}$, $[K_i : K_{i-1}] \in \{1; 2\}$.*

Alors P est constructible à partir de $\mathcal{E}$.

La preuve de ce résultat repose sur les considérations géométriques rassemblées dans le lemme ci-dessous, où "constructible" signifie "constructible à partir de $\mathcal{E}$:

Lemme 2.4.2. *Soient $x, y \in \mathbb{R}$.*

1. *Le point (x, y) est constructible ssi les points $(x, 0)$ et $(0, y)$.*
2. *Le point $(x, 0)$ est constructible ssi le point $(0, x)$ est constructible.*
3. *Supposons que les points $(x, 0)$ et $(y, 0)$ soient constructibles, alors :*
   (a) *le point $(-x, 0)$ est constructible,*
   (b) *le point $(x + y, 0)$ est constructible,*
   (c) *le point $(xy, 0)$ est constructible,*
   (d) *si $x \neq 0$, le point $\left(\frac{1}{x}, 0\right)$ est constructible.*

Démonstration. On note S le point de coordonnées (x, y), M le point de coordonnées $(x, 0)$, N le point de coordonnées $(0, y)$ et Q le point de coordonnées $(y, 0)$.

On rappelle que le point B est constructible à partir de O et A donc à partir de $\mathcal{E}$.

1. Supposons que le point S soit constructible. Alors la droite parallèle à la droite (OB) passant par S est constructible (exemple 2.1.4 3) ainsi que la droite (OA) : leur point d'intersection M est donc constructible. De façon analogue, la droite parallèle à la droite (OA) passant par S étant constructible, le point d'intersection N de cette droite avec la droite (OB) est également constructible.

   Réciproquement, supposons que les points M et N soient constructibles. Le point S est l'intersection de la droite parallèle à la droite (OB) passant par M et de la droite parallèle à la droite (OA) passant par N : comme M et N sont constructibles, ces deux droites sont constructibles et leur point d'intersection S est donc constructible.

2. Notons R le point de coordonnées $(0, x)$. R est à l'intersection du cercle $\mathcal{C}$ de centre O et de rayon $[OM]$ et de la droite (OB). Ainsi, si M est constructible, R est constructible. Réciproquement, comme M est à l'intersection du cercle $\mathcal{C}$ de centre O et de rayon $[OR]$ et de la droite (OA), si R est constructible, alors M est constructible.

3. (a) Le point de coordonnées $(-x, 0)$ est l'autre point d'intersection de la droite (OA) et du cercle de centre O et de rayon $[OM]$.

   (b) Le point de coordonnée $(x + y, 0)$ est à l'intersection du cercle de centre M et de rayon OQ (à droite ou à gauche de M suivant le signe de y).

   (c) Notons $\mathcal{D}$ la droite parallèle à (BM) passant par N : $\mathcal{D}$ est constructible. Notons ensuite T le point d'intersection des droites $\mathcal{D}$ et (OA) : T est constructible de coordonnées $(z, 0)$ avec $z \in \mathbb{R}$ et, d'après le théorème de Thalès appliqué aux triangles semblables TON et MOB, on a

   $$\frac{OT}{OM} = \frac{ON}{OB} \text{ i.e. } \frac{|z|}{|x|} = \frac{|y|}{1} \text{ i.e. } |z| = |x||y|.$$

   De plus, le signe de l'abscisse z de T est le produit des signes de x et y. On a donc $z = xy$ et le point de coordonnées $(xy, 0)$ est bien constructible.

   (d) Comme le point M est constructible, il en est de même pour R par 2. On considère alors la droite $\mathcal{D}'$ parallèle à (RA) passant par B : $\mathcal{D}'$ est constructible et on note U son point d'intersection avec la droite (OA) ($\mathcal{D}'$ n'est pas parallèle à (OA) car $x \neq 0$). Le point constructible U a pour coordonnées $(w, 0)$ avec $w \in \mathbb{R}$ et, d'après le théorème de Thalès appliqué aux triangles semblables UOB et AOR, on a

   $$\frac{OU}{OA} = \frac{OB}{OR} \text{ i.e. } \frac{|w|}{1} = \frac{1}{|x|} \text{ i.e. } |w| = \frac{1}{|x|}.$$

   De plus le signe de l'abscisse w de U est le même que le signe de x : on a donc $w = \frac{1}{x}$ et le point de coordonnées $\left(\frac{1}{x}, 0\right)$ est bien constructible.

□

Démonstration du théorème 2.4.1. D'après les points 1 et 2 du lemme 2.4.2, le point P est constructible ssi les points $(x_0, 0)$ et $(y_0, 0)$ sont constructibles. Pour montrer que P est constructible, il suffit donc de montrer que si $a \in K_m$, alors le point $(a, 0)$ est constructible.

On montre ce résultat par récurrence sur $m \in \mathbb{N}$.

Commençons donc par montrer que si $a \in \mathbb{Q}(\mathcal{E})$, alors le point $(a, 0)$ est constructible. Soit donc a un élément de $\mathbb{Q}(\mathcal{E})$. D'après la proposition 1.2.5, il existe $k \in \mathbb{N}$, des abscisses et/ou des ordonnées $a_1, \ldots, a_k \in \mathbb{R}$ de points de $\mathcal{E}$, une fraction rationnelle $\frac{S}{T} \in K(X_1, \ldots, X_k)$ tels que $T(a_1, \ldots, a_k) \neq 0$ et

$$a = \frac{S(a_1, \ldots, a_k)}{T(a_1, \ldots, a_k)}.$$

Or, d'après les points 1 et 2 du lemme 2.4.2, les points de coordonnées $(a_1, 0)$, $\ldots$, $(a_k, 0)$ sont constructibles. Donc, d'après le point 3 du lemme 2.4.2, le point de coordonnées $(a, 0) = \left(\frac{S(a_1,\ldots,a_k)}{T(a_1,\ldots,a_k)}, 0\right)$.

Supposons ensuite que $m \in \mathbb{N}\backslash\{0\}$ et que la propriété est vérifiée au rang $m-1$, et reprenons la suite d'extensions

$$K_0 \subset \cdots \subset K_m$$

de $K_0 = \mathbb{Q}(\mathcal{E})$ de l'énoncé.

Soit $a \in K_m$. Si $a \in K_{m-1}$ alors, en appliquant l'hypothèse de récurrence à a et la suite d'extensions $K_0 \subset \cdots \subset K_{m-1}$, on obtient la constructibilité du point $(a, 0)$. Si $a \in K_m\backslash K_{m-1}$ alors nécessairement $K_m \neq K_{m-1}$, $[K_m : K_{m-1}] = 2$, et a est algébrique de degré 2 sur K_{m-1} : le polynôme minimal de a sur K_{m-1} est de la forme

$$X^2 + bX + c$$

avec $b, c \in K_{m-1}$.

Remarquons tout d'abord que, comme $b, c, 0 \in K_{m-1}$, par hypothèse de récurrence, les points de coordonnées $(b, 0)$ et $(c, 0)$ sont constructibles à partir de $\mathcal{E}$. Ensuite, a étant une racine réelle du polynôme à coefficients réels $X^2 + bX + c$, on a $b^2 - 4c \geqslant 0$ et

$$a = \frac{-b \pm \sqrt{b^2 - 4c}}{2}.$$

Par le lemme 2.4.2, les points de coordonnées $(-b, 0), \left(\frac{1}{2}, 0\right)$ et $\left(b^2 - 4c, 0\right)$ sont constructibles et, pour montrer que le point de coordonnées $(a, 0)$ est constructible, il nous suffit donc de montrer que, si $z \in [0, +\infty[$ et si le point de coordonnées $(z, 0)$ est constructible, alors le point de coordonnées $(\sqrt{z}, 0)$ est constructible.

Soit donc $z \in [0, +\infty[$ tel que le point $(z, 0)$ est constructible. D'après le lemme 2.4.2, le point de coordonnées $(\sqrt{z}, 0)$ est constructible ssi le point de coordonnées $(1, \sqrt{z})$ est constructible. Nous allons montrer que le point D de coordonnées $(1, \sqrt{z})$ est constructible.

Notons C le point de coordonnées $(z + 1, 0)$: C est constructible par le lemme 2.4.2 car le point A, de coordonnées $(1, 0)$, et le point $(z, 0)$ sont constructibles. Le milieu M du segment

$[OC]$, de coordonnées $\big(\frac{z+1}{2}, 0\big)$, est donc également constructible (cf. l'exemple 1 de l'exemple 2.1.2).

On note ensuite $\mathcal{C}$ le cercle de centre M est de rayon $[OM]$, i.e. le cercle d'équation

$$\left(x - \frac{z+1}{2}\right)^2 + (y-0)^2 = \left(\frac{z+1}{2}\right)^2.$$

Le point D est à l'intersection du cercle $\mathcal{C}$ et de la droite parallèle à la droite (OB) passant par A, i.e. la droite d'équation $x = 1$: les coordonnées $(1, \sqrt{z})$ de D vérifient les deux équations).

Comme le cercle $\mathcal{C}$ et la droite $\mathcal{D}$ sont constructibles à partir de $\mathcal{E}$, le point D est constructible à partir de $\mathcal{E}$. □

Synthétisons le corollaire 2.2.6 et le théorème 2.4.1 en un seul énoncé :

Théorème 2.4.3. *Le point P est constructible à partir de $\mathcal{E}$ si et seulement s'il existe une suite finie croissante*

$$K_0 \subset \cdots \subset K_m,$$

$m \in \mathbb{N}$, de sous-corps de $\mathbb{R}$ telle que

- $K_0 = \mathbb{Q}(\mathcal{E})$,
- $x_0, y_0 \in K_m$,
- *si $m \geqslant 1$, pour tout $i \in \{1, \ldots, m\}$, $[K_i : K_{i-1}] \in \{1; 2\}$.*

Remarque 2.4.4. En particulier, les points constructibles à partir de $\{O, A\}$ sont exactement les points dont les coordonnées peuvent s'exprimer à l'aide de nombres rationnels, de sommes, de différences, de produits, de quotients et de racines carrées.

2.5 Application au problème de la trisection de l'angle

On applique maintenant le théorème 2.4.3 au problème de la trisection de l'angle. Soit C un point du plan $(\mathcal{P})$ n'appartenant pas à la demi-droite $[OA)$, et notons θ la mesure, en radians, de l'angle orienté délimité par les demi-droites $[OA)$ et $[OC)$. Notons également D le point de coordonnées $\big(\cos(\theta), \sin(\theta)\big)$ dans le repère orthonormal (O, A, B).

On dit alors que l'angle $\widehat{AOC}$ est trisectable à la règle et au compas s'il est possible de construire à la règle et au compas à partir de $\{O, A, D\}$ deux droites $\mathcal{D}$ et $\mathcal{D}'$ telles que les trois angles délimités, entre les demi-droites $[OA)$ et $[OC)$, par les droites (OA), $\mathcal{D}$, $\mathcal{D}'$ et (OC) (dans cet ordre) sont de mesure $\frac{\theta}{3}$.

Grâce au théorème 2.4.3, on obtient le critère nécessaire et suffisant de trisectabilité suivant :

Proposition 2.5.1. *L'angle $\widehat{AOC}$ est trisectable à la règle et au compas ssi le polynôme*

$$4X^3 - 3X - \cos(\theta)$$

possède une racine dans $\mathbb{Q}\big(\cos(\theta)\big)$.

Démonstration. Commençons par remarquer que l'angle $\widehat{AOC}$ est trisectable à la règle et au compas ssi le point S de coordonnées $\big(\cos\left(\frac{\theta}{3}\right), \sin\left(\frac{\theta}{3}\right)\big)$ est constructible à partir de $\{A, O, D\}$.

En effet, si l'angle $\widehat{AOC}$ est trisectable à la règle et au compas et si l'on reprend les notations ci-dessus, alors le point S est l'intersection de la droite $\mathcal{D}$ et du cercle de centre O et de rayon $[OA]$, tous deux constructibles à partir de $\{A, O, D\}$. Réciproquement, si le point S est constructible à partir de $\{A, O, D\}$, on construit ensuite le point S' de coordonnées $\big(\cos\left(\frac{2\theta}{3}\right), \sin\left(\frac{2\theta}{3}\right)\big)$ comme intersection du cercle de centre O et de rayon $[OA]$ et le cercle de centre S et de rayon $[SA]$, et les droites (OS) et (OS') coupent $\widehat{AOC}$ en trois angles de mesures égales.

Montrons donc que le point S est constructible à partir de $\{A, O, D\}$. Soit T le point de coordonnées $\big(\cos\left(\frac{\theta}{3}\right), 0\big)$: S est constructible à partir de $\{A, O, D\}$ ssi T est constructible à partir de $\{A, O, D\}$, car T est l'intersection de la droite (OA) et de la droite perpendiculaire à (OA) passant par S, et S est l'intersection de la droite perpendiculaire à (OA) passant par T et du cercle de centre O et de rayon $[OA]$.

Notons enfin E le point de coordonnées $\big(\cos(\theta), 0\big)$. Par des arguments tout à fait analogues à ci-dessus, E est constructible à partir de $\{O, A, D\}$ et D est constructible à partir de $\{O, A, E\}$. Ainsi, T est constructible à partir de $\{A, O, D\}$ ssi T est constructible à partir de $\{A, O, E\}$.

Nous allons maintenant appliquer le critère du théorème 2.4.3. Nous avons tout d'abord

$$\mathbb{Q}\big(\{A, O, E\}\big) = \mathbb{Q}(0, 1, \cos(\theta)) = \mathbb{Q}(\cos(\theta)).$$

Ensuite,

$$\cos(\theta) = \cos\left(3 \times \frac{\theta}{3}\right) = 4\cos\left(\frac{\theta}{3}\right)^3 - 3\cos\left(\frac{\theta}{3}\right)$$

i.e. le réel $\alpha := \cos\left(\frac{\theta}{3}\right)$ annule le polynôme

$$P := 4X^3 - 3X - \cos(\theta)$$

à coefficients dans $\mathbb{Q}(\cos(\theta))$ i.e. $\mu_{\alpha,\mathbb{Q}(\cos(\theta))}$ divise P.

Deux cas se présentent alors :

- Si P possède une racine dans $\mathbb{Q}(\cos(\theta))$, alors P n'est pas irréductible sur $\mathbb{Q}(\cos(\theta))$: α annule donc un facteur de degré 1 ou 2 de P dans $\mathbb{Q}(\cos(\theta))[X]$, et le degré de $\mu_{\alpha,\mathbb{Q}(\cos(\theta))}$ est donc 1 ou 2. L'extension $\mathbb{Q}(\cos(\theta))(\alpha)$ de $\mathbb{Q}(\cos(\theta))$ vérifie alors $[\mathbb{Q}\big(\cos(\theta)\big)(\alpha) : \mathbb{Q}(\cos(\theta))] \leqslant 2$ et on a une suite d'extensions

  $$\mathbb{Q}(\{A, O, E\}) = \mathbb{Q}(\cos(\theta)) \subset \mathbb{Q}\big(\cos(\theta)\big)(\alpha)$$

  avec $[\mathbb{Q}\big(\cos(\theta)\big)(\alpha) : \mathbb{Q}(\cos(\theta))] \leqslant 2$: comme $\alpha \in \mathbb{Q}\big(\cos(\theta)\big)(\alpha)$, d'après le théorème 2.4.3, le point T de coordonnées $(\alpha, 0) = \big(\cos\left(\frac{\theta}{3}\right), 0\big)$ est constructible à partir de $\{A, O, E\}$, et l'angle $\widehat{AOC}$ est trisectable à la règle et au compas.

- Si P ne possède pas de racine dans $\mathbb{Q}(\cos(\theta))$ alors, comme P est de degré 3, P est irréductible sur $\mathbb{Q}(\cos(\theta))$ et donc $\mu_{\alpha,\mathbb{Q}(\cos(\theta))} = \frac{1}{4}P$. En particulier α est algébrique

de degré 3 sur $\mathbb{Q}(\cos(\theta)) = \mathbb{Q}(\{A, O, E\})$: d'après le corollaire 2.2.7, le point T de coordonnées $(\alpha, 0) = \left(\cos\left(\frac{\theta}{3}\right), 0\right)$ n'est donc pas constructible à partir de $\{A, O, E\}$, et l'angle $\widehat{AOC}$ n'est donc trisectable à la règle et au compas.

□

Chapitre 3

Constructibilité à la règle et au compas des polygones réguliers

3.1 Introduction

Reprenons les notations du chapitre précédent : on considère un plan $(\mathcal{P})$ et $\mathcal{E}$ un ensemble de points de $(\mathcal{P})$ contenant au moins deux points distincts O et A. Soit ensuite un point B de $(\mathcal{P})$ tel que le triplet (O, A, B) forme un repère orthonormal du plan $(\mathcal{P})$ et notons (x, y) les coordonnées (réelles) dans le repère (O, A, B).

Soit $n \in \mathbb{N}\backslash\{0; 1; 2\}$ Nous allons dans ce chapitre établir une condition nécessaire et suffisante de constructibilité à partir de $\{O, A\}$ du polygone régulier à n côtés dont le centre est en O et un sommet est en A, que l'on note $\mathcal{R}_n$. Précisément, nous allons démontrer le résultat ci-dessous.

Introduisons tout d'abord la notation suivante : si $m \in \mathbb{N}$, on note $F_m := 1 + 2^{2^m}$ et l'entier F_m est appelé $\underline{\text{m}^{\text{ème}} \text{ nombre de Fermat}}$.

Théorème 3.1.1 (Théorème de Gauss-Wantzel)**.** *Le polygone régulier $\mathcal{R}_n$ est constructible à partir de $\{O, A\}$ si et seulement si n est le produit d'une puissance de deux et de nombres de Fermat $\underline{\text{premiers}}$ et $\underline{\text{deux à deux distincts}}$.*

Pour prouver ce théorème, nous allons utiliser le plan complexe $\mathbb{C}$ et la notion de *nombre complexe constructible à partir de $\mathcal{E}$.*

3.2 Nombres complexes constructibles

Soit $z = a + ib \in \mathbb{C}$.

Définition 3.2.1. *On dit que z est $\underline{\text{constructible à partir de } \mathcal{E}}$ si le point d'affixe z, i.e. le point de coordonnées (a, b), est constructible à partir de $\mathcal{E}$.*

Notons $\mathcal{F}_\mathcal{E}$ l'ensemble des nombres complexes constructibles à partir de $\mathcal{E}$. Le lemme 2.4.2 nous permet alors de montrer la proposition suivante :

Proposition 3.2.2. *L'ensemble $\mathcal{F}_\mathcal{E}$ des nombres complexes constructibles à partir de $\mathcal{E}$ est un sous-corps de $\mathbb{C}$ contenant $\mathbb{Q}(\mathcal{E})$.*

Démonstration. Le nombre complexe 1 est constructible car le point A de coordonnées $(1,0)$ appartient à $\mathcal{E}$. Supposons maintenant que z est constructible à partir de $\mathcal{E}$ et soit $z' = a' + ib' \in \mathcal{F}_\mathcal{E}$. Alors

- $z - z' = (a-a') + i(b-b') \in \mathcal{F}_\mathcal{E}$ car le point de coordonnées $(a-a', b-b')$ est constructible à partir de $\mathcal{E}$ par le lemme 2.4.2,
- $zz' = (aa' - bb') + i(ab' + a'b) \in \mathcal{F}_\mathcal{E}$ car le point de coordonnées $(aa' - bb', ab' + a'b)$ est constructible à partir de $\mathcal{E}$ par le lemme 2.4.2,
- $\frac{1}{z} = \frac{a}{a^2+b^2} - i\frac{b}{a^2+b^2} \in \mathcal{F}_\mathcal{E}$ car le point de coordonnées $\left(\frac{a}{a^2+b^2}, -\frac{b}{a^2+b^2}\right)$ est constructible à partir de $\mathcal{E}$ par le lemme 2.4.2.

Montrons enfin que $\mathcal{F}_\mathcal{E}$ contient $\mathbb{Q}(\mathcal{E})$. Soit $x \in \mathbb{Q}(\mathcal{E})$. D'après le théorème 2.4.1, le point de coordonnées $(x,0)$ est constructible à partir de $\mathcal{E}$ et le nombre "complexe" x est donc constructible à partir de $\mathcal{E}$. □

Si le nombre complexe z est constructible à partir de $\mathcal{E}$, il en est également de même pour ses racines carrées :

Proposition 3.2.3. *Supposons que $z \in \mathcal{F}_\mathcal{E}$ et soit $\omega \in \mathbb{C}$ tel que $\omega^2 = z$. Alors $\omega \in \mathcal{F}_\mathcal{E}$.*

Démonstration. Si $z = 0$, alors $\omega = 0 \in \mathcal{F}_\mathcal{E}$.

Supposons maintenant que $z \neq 0$ et écrivons $z = re^{i\theta}$ avec $r \in]0; +\infty[$ et $\theta \in [0; 2\pi[$. Alors $\omega = \pm\sqrt{r}e^{i\frac{\theta}{2}}$.

Notons P le point du plan $(\mathcal{P})$ d'affixe z : P est constructible à partir de $\mathcal{E}$ par hypothèse sur z. Le point de coordonnées $(r,0)$, intersection de la demi-droite $[OA)$ et du cercle de centre O et de rayon $[OP]$ est alors également constructible à partir de $\mathcal{E}$, ainsi que le point de coordonnées $(\sqrt{r},0)$ d'après la preuve du théorème 2.4.1, et donc $\sqrt{r} \in \mathcal{F}_\mathcal{E}$.

Par ailleurs, le point d'affixe $e^{i\frac{\theta}{2}}$ est à l'intersection de la bissectrice de l'angle $\widehat{AOP}$ et du cercle de centre O et de rayon $[OA]$ et est donc constructible à partir de $\mathcal{E}$.

Ainsi $e^{i\frac{\theta}{2}} \in \mathcal{F}_\mathcal{E}$ et donc, comme $\mathcal{F}_\mathcal{E}$ est un corps, le nombre complexe $\omega = \pm\sqrt{r}e^{i\frac{\theta}{2}}$ est constructible à partir de $\mathcal{E}$. □

De ces deux propositions 3.2.2 et 3.2.3, on déduit l'adaptation suivante du corollaire 2.2.6 et du théorème 2.4.1 :

Théorème 3.2.4. *Le nombre complexe z est constructible à partir de $\mathcal{E}$ si et seulement s'il existe une suite finie croissante*

$$K_0 \subset \cdots \subset K_N,$$

$N \in \mathbb{N}$, de sous-corps de $\mathbb{C}$ telle que

- $K_0 = \mathbb{Q}(\mathcal{E})$,
- $z \in K_N$,
- *si $N \geqslant 1$, pour tout $i \in \{1, \ldots, N\}$, $[K_i : K_{i-1}] \in \{1; 2\}$.*

Démonstration. Supposons tout d'abord que $z = a + ib$ soit constructible à partir de $\mathcal{E}$ i.e. que le point P de coordonnées (a, b) soit constructible à partir de $\mathcal{E}$: d'après le corollaire 2.2.6, il existe alors une suite finie croissante

$$K_0 \subset \cdots \subset K_m,$$

$m \in \mathbb{N}$, de sous-corps de $\mathbb{R}$ telle que

- $K_0 = \mathbb{Q}(\mathcal{E})$,
- $a, b \in K_m$,
- si $m \geqslant 1$, pour tout $i \in \{1, \ldots, m\}$, $[K_i : K_{i-1}] \in \{1; 2\}$.

Posons ensuite $K_{m+1} := K_m(i)$: on a $[K_{m+1} : K_m] = 2$ (car $\mu_{i,K_m} = X^2 + 1$) et $z = a + ib \in K_{m+1}$ (car $a, b, i \in K_{m+1}$).

Montrons la réciproque par récurrence sur $N \in \mathbb{N}$.

Si $z \in \mathbb{Q}(\mathcal{E}) \subset \mathbb{R}$, le point P d'affixe z a pour coordonnées $(z, 0)$ et est constructible à partir de $\mathcal{E}$ d'après le théorème 2.4.1, i.e. $z \in \mathcal{F}_\mathcal{E}$.

Supposons maintenant la propriété vérifiée au rang $N-1$ pour $N \in \mathbb{N}\backslash\{0\}$ fixé et supposons qu'il existe une suite finie croissante

$$K_0 \subset \cdots \subset K_N,$$

$N \in \mathbb{N}$, de sous-corps de $\mathbb{C}$ telle que

- $K_0 = \mathbb{Q}(\mathcal{E})$,
- $z \in K_N$,
- si $N \geqslant 1$, pour tout $i \in \{1, \ldots, N\}$, $[K_i : K_{i-1}] \in \{1; 2\}$.

Si $z \in K_{N-1}$, on peut directement appliquer l'hypothèse de récurrence. Si maintenant $z \notin K_{N-1}$, $[K_N : K_{N-1}] = 2$ ($z \in K_N$) et le polynôme minimal $\mu_{z,K_{N-1}}$ de z sur K_{N-1} est de degré 2, de la forme $X^2 + uX + v$ avec $u, v \in K_{N-1}$. Le nombre z est alors de la forme

$$z = \frac{-u \pm \omega}{2}$$

où ω est l'un des deux nombres complexes vérifiant $\omega^2 = u^2 - 4v^2$.

Or, par hypothèse de récurrence, les nombres complexes u et v, étant des éléments de K_{N-1}, sont constructibles à partir de $\mathcal{E}$: on a alors, par la proposition 3.2.2, $u^2 - 4v^2 \in \mathcal{F}_\mathcal{E}$ donc, par la proposition 3.2.3, $\omega \in \mathcal{F}_\mathcal{E}$, et finalement $z \in \dfrac{-u \pm \omega}{2} \in \mathcal{F}_\mathcal{E}$.

□

Par une démonstration tout à fait analogue à celle du corollaire 2.2.7, on montre le critère nécessaire de constructibilité pour les nombres complexes suivant :

Corollaire 3.2.5 (Critère de Wantzel)**.** *Tout nombre complexe constructible à partir de $\mathcal{E}$ est algébrique sur $\mathbb{Q}(\mathcal{E})$ de degré une puissance de deux.*

3.3 Constructibilité du polygone régulier $\mathcal{R}_n$: première étude

Revenons à la question de la constructibilité à partir de $\{O, A\}$ du polygone régulier à n côtés $\mathcal{R}_n$, i.e. de la constructibilité à partir de $\{O, A\}$ de tous les sommets de $\mathcal{R}_n$. Pour simplifier les énoncés, dans la suite, nous dirons *constructible* pour *constructible à partir de* $\{O, A\}$ (pour *constructible à la règle et au compas*).

Une première remarque est la suivante :

Lemme 3.3.1. *Le polygone $\mathcal{R}_n$ est constructible ssi le nombre complexe $\zeta_n := e^{\frac{2i\pi}{n}}$ est constructible.*

Démonstration. Pour $k \in \{0, \dots, n-1\}$, notons P_k le point d'affixe $\zeta_n^k := e^{\frac{2ik\pi}{n}}$ i.e. le point de coordonnées $\left(\cos\left(\frac{2k\pi}{n}\right), \sin\left(\frac{2k\pi}{n}\right)\right)$: $P_0 = A$ et les points $P_0, \dots, P_{n-1}$ sont les n sommets du polygone $\mathcal{R}_n$.

Si $\mathcal{R}_n$ est constructible, en particulier le sommet P_1 est constructible i.e. ζ_n est constructible.

Réciproquement, si ζ_n est constructible i.e. si le point P_1 est constructible, alors on peut construire tous les sommets de $\mathcal{R}_n$ par récurrence : si $k \in \{1, \dots, n-1\}$, le point P_k est à l'intersection du cercle de centre O et de rayon $[OA]$ et du cercle de centre P_{k-1} et de rayon $[AP_1]$. □

Nous sommes ainsi ramenés à étudier la constructibilité du nombre complexe $\zeta_n = e^{\frac{2i\pi}{n}}$. En tant que racine de l'unité, ζ_n est algébrique sur $\mathbb{Q} = \mathbb{Q}(\{O, A\})$. Plus précisément, nous avons la propriété ci-dessous.

Dans cet énoncé, on note

$$\Phi_n := \prod_{\substack{1 \leqslant k \leqslant n \\ \text{pgcd}(k,n)=1}} \left(X - \zeta_n^k\right) = \prod_{\substack{1 \leqslant k \leqslant n \\ \text{pgcd}(k,n)=1}} \left(X - e^{\frac{2ik\pi}{n}}\right) \in \mathbb{C}[X]$$

le $n^{ème}$ *polynôme cyclotomique*. On rappelle que $\Phi_n \in \mathbb{Z}[X]$ et que Φ_n est irréductible dans $\mathbb{Q}[X]$.

Proposition 3.3.2. *Le polynôme minimal de ζ_n sur $\mathbb{Q}$ est Φ_n. En particulier, ζ_n est algébrique de degré $\varphi(n)$ sur $\mathbb{Q}$, où*

$$\varphi : \begin{array}{ccc} \mathbb{N}\backslash\{0\} & \mapsto & \mathbb{N}\backslash\{0\} \\ m & \mapsto & \text{Card}\left(\{k \in \{1, \dots, m\} \mid \text{pgcd}(k, n) = 1\}\right) \end{array}$$

est la fonction indicatrice d'Euler.

Démonstration. On a $\Phi_n \in \mathbb{Z}[X] \subset \mathbb{Q}[X]$ et, par définition ζ_n est une racine de Φ_n. De plus Φ_n est unitaire et irréductible dans $\mathbb{Q}[X]$. On a donc bien $\mu_{\zeta_n,\mathbb{Q}} = \Phi_n$.

En particulier, ζ_n est algébrique de degré $\deg(\Phi_n) = \varphi(n)$ sur $\mathbb{Q}$. □

Remarque 3.3.3.

- Les propriétés précédentes sont également vraies si $n \in \{1; 2\}$.
- Si n est un nombre premier, on a $\Phi_p = 1 + X + \cdots + X^{p-1}$.

3.4 Démonstration du théorème de Gauss-Wantzel : sens direct

Nous allons commencer par montrer que si le polygone régulier $\mathcal{R}_n$ est constructible i.e. si le nombre complexe ζ_n est constructible, alors n est nécessairement le produit d'une puissance de deux et de nombres de Fermat premiers et deux à deux distincts.

Supposons donc que ζ_n est constructible à partir de $\{O, A\}$ et considérons la décomposition

$$n = \prod_{r=1}^{N} p_r^{\nu_r}$$

de n en facteurs premiers, où, pour tout $r \in \{1, \dots, N\}$, $\nu_r \in \mathbb{N}\backslash\{0\}$. D'après la proposition 3.3.2, ζ_n est algébrique sur $\mathbb{Q}$ de degré

$$\varphi(n) = \prod_{r=1}^{N} p_r^{\nu_r - 1}(p_r - 1),$$

mais, puisque $\zeta_n \in \mathcal{F}_{\{O,A\}}$, d'après le corollaire 3.2.5, ζ_n est algébrique sur $\mathbb{Q}(\{O, A\}) = \mathbb{Q}$ de degré une puissance de deux.

Il existe donc $m \in \mathbb{N}\backslash\{0\}$ tel que

$$\prod_{r=1}^{N} p_r^{\nu_r - 1}(p_r - 1) = \varphi(n) = 2^m.$$

Ainsi, pour tout $r \in \{1, \dots, N\}$ tel que p_r est impair, ν_r est nécessairement égal à 1 et $p_r - 1$ est nécessairement une puissance de deux i.e. $p_r = 1 + 2^{k_r}$ avec $k_r \in \mathbb{N}\backslash\{0\}$. L'entier n est donc de la forme

$$n = 2^d \prod_{s=1}^{M} \left(1 + 2^{d_s}\right)$$

où $d \in \mathbb{N}$, $M \in \mathbb{N}$, pour $s \in \{1, \dots, M\}$, $d_s \in \mathbb{N}\backslash\{0\}$ et $1 + 2^{d_s}$ est un nombre premier (impair), et les entiers $1 + 2^{d_s}$, $s \in \{1, \dots, M\}$, sont deux à deux distincts.

De plus :

Lemme 3.4.1. *Soit $k \in \mathbb{N}\backslash\{0\}$ tel que l'entier $1 + 2^k$ soit premier. Alors k est une puissance de 2 et $1 + 2^k$ est donc un nombre de Fermat.*

Démonstration. Supposons par l'absurde k soit divisible par un nombre impair l au moins égal à trois et soit q le quotient de la division euclidienne de k par l. On a alors

$$1 + 2^k = 1 + (2^q)^l = 1^l - (-2^q)^l$$

et l'entier $1 - (-2^q) = 1 + 2^q$ divise donc $1 + 2^k$. Or $1 < q < k$ et $1 + 2^k$ est premier, d'où une contradiction. □

Ainsi, pour tout $s \in \{1, \dots, M\}$, il existe $m_s \in \mathbb{N}$ tel que

$$n = 2^d \prod_{s=1}^{M} F_{m_s},$$

les entiers $m_1, \dots, m_M$ sont deux à deux distincts et les nombres $F_{m_1}, \dots, F_{m_s}$ sont premiers.

Nous avons ainsi montré le sens direct du théorème 3.1.1 :

Proposition 3.4.2. *Si le polygone régulier $\mathcal{R}_n$ est constructible, alors n est le produit d'une puissance de deux et de nombres de Fermat premiers deux à deux distincts.*

Nous allons maintenant montrer la réciproque. Nous allons tout d'abord commencer par une réduction au cas où n lui-même un nombre de Fermat premier.

3.5 Sens réciproque du théorème de Gauss-Wantzel : réduction

Supposons donc maintenant que n est de la forme

$$n = 2^d \prod_{s=1}^{M} F_{m_s},$$

avec $d \in \mathbb{N}$, $m_1, \dots, m_s \in \mathbb{N}$ deux à deux distincts et, pour tout $s \in \{1, \dots, M\}$, F_{m_s} premier, et nous allons montrer que le polygone régulier $\mathcal{R}_n$ est constructible i.e. que ζ_n est constructible.

On peut supposer que n est soit une puissance de deux, soit un entier de Fermat premier, en vertu du lemme suivant :

Lemme 3.5.1. *Soient k_1 et k_2 deux entiers naturels non nuls premiers entre eux. Alors le nombre $\zeta_{k_1 k_2}$ est constructible si et seulement si les nombres ζ_{k_1} et ζ_{k_2} sont constructibles.*

Démonstration. Si $\zeta_{k_1 k_2} \in \mathcal{F}_{\{O,A\}}$, alors

$$\zeta_{k_1} = e^{\frac{2i\pi}{k_1}} = e^{\frac{2i\pi k_2}{k_1 k_2}} = (\zeta_{k_1 k_2})^{k_2} \in \mathcal{F}_{\{O,A\}}$$

(car $\mathcal{F}_{\{O,A\}}$ est un corps). De façon analogue, ζ_{k_2} est également constructible.

Supposons maintenant que ζ_{k_1} et ζ_{k_2} sont constructibles. Comme $\text{pgcd}(k_1, k_2) = 1$, il existe $u, v \in \mathbb{Z}$ tel que $uk_1 + vk_2 = 1$, et alors

$$\zeta_{k_1 k_2} = e^{\frac{2i(uk_1 + vk_2)\pi}{k_1 k_2}} = e^{\frac{2iuk_1\pi}{k_1 k_2}} e^{\frac{2ivk_2\pi}{k_1 k_2}} = e^{\frac{2iu\pi}{k_2}} e^{\frac{2iv\pi}{k_1}} = (\zeta_{k_2})^u (\zeta_{k_1})^v \in \mathcal{F}_{\{O,A\}}.$$

□

Ainsi, pour montrer que ζ_n est constructible, il suffit de montrer que les nombres ζ_{2^d} et $\zeta_{F_{m_s}}$, $s \in \{1, \dots, M\}$, sont constructibles.

Tout d'abord :

Lemme 3.5.2. *Soit $m \in \mathbb{N}$. Le nombre complexe ζ_{2^m} est constructible.*

Démonstration. On montre ce lemme par récurrence sur $m \in \mathbb{N}$: le nombre $\zeta_{2^0} = \zeta_1 = e^{2i\pi} = 1$ est constructible à partir de $\{O, A\}$ (le point d'affixe 1 est A) et si l'on suppose, pour $m \in \mathbb{N}\backslash\{0\}$ fixé, que le point Q d'affixe $\zeta_{2^{m-1}} = e^{\frac{2i\pi}{2^{m-1}}}$ est constructible, alors le point d'affixe $\zeta_{2^m} = e^{\frac{2i\pi}{2^m}}$ est constructible en tant que point à l'intersection du cercle de centre O et de rayon $[OA]$ et de la bissectrice de l'angle $\widehat{AOQ}$.

□

Pour montrer que ζ_n est constructible i.e. que $\mathcal{R}_n$ est constructible, il nous suffit donc de montrer que si p est un entier de Fermat premier, alors ζ_p est constructible.

C'est ce que nous allons prouver dans la suite de ce chapitre et, pour cela, nous allons emprunter quelques outils à la théorie de Galois.

3.6 Groupe de Galois d'une extension

Pour terminer notre démonstration du théorème de Gauss-Wantzel 3.1.1, nous allons utiliser la notion de *groupe de Galois d'une extension* et quelques-unes de ses propriétés.

Soient L un corps et K un sous-corps de L. Soit également $\psi : L \to L$ une application.

Définition 3.6.1. *On dit que ψ est un endomorphisme de L sur K si*

- *$\psi : L \to L$ est un (endo)morphisme de corps (i.e. un endomorphisme d'anneau unitaire),*
- *$\psi : L \to L$ est un endomorphisme de K-espace vectoriel L.*

On dit ensuite que ψ est un automorphisme de L sur K si ψ est un endomorphisme de L sur K bijectif, et on note

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

l'ensemble des automorphismes de L sur K.

Remarque 3.6.2.
- Si ψ est un automorphisme de L sur K, alors ψ^{-1} est également un endomorphisme de L sur K (et donc un automorphisme de L sur K).
- Tout morphisme de corps étant injectif (cf. lemme 1.1.1), un endomorphisme de L sur K est nécessairement injectif : si l'extension L est de degré fini sur K, tout endomorphisme de L sur K est un automorphisme de L sur K.
- L'application ψ est un endomorphisme, resp. automorphisme, de L sur K si et seulement si ψ est un endomorphisme, resp. automorphisme, de K-algèbres.

Un endomorphisme de L sur K est caractérisé par le fait qu'il préserve les fractions rationnelles à coefficients dans K :

Lemme 3.6.3. *L'application $\psi : L \to L$ est un endomorphisme de L sur K si et seulement si pour tout $k \in \mathbb{N}$, pour tous $a_1, \ldots, a_k \in L$, pour toute fraction fractionnelle $\frac{S}{T} \in K(X_1, \ldots, X_k)$ tels que $T(a_1, \ldots, a_k) \neq 0$,*

$$\psi\left(\frac{S(a_1, \ldots, a_k)}{T(a_1, \ldots, a_k)}\right) = \frac{S\big(\psi(a_1), \ldots, \psi(a_k)\big)}{T\left(\psi(a_1), \ldots, \psi(a_k)\right)}.$$

Démonstration. Supposons que ψ soit un endomorphisme de L sur K. Tout d'abord, si $x \in K$, on a

$$\begin{aligned}
\psi(x) &= \psi(x \cdot 1) \\
&= x\psi(1) \text{ (car } \psi \text{ est une application } K\text{-linéaire)} \\
&= x \cdot 1 \text{ (car } \psi \text{ est un morphisme d'anneaux unitaires)} \\
&= x
\end{aligned}$$

Soient maintenant $k \in \mathbb{N}\backslash\{0\}$, $a_1, \ldots, a_k \in L$ et $P = \sum_{\substack{r_1,\ldots,r_k \in \mathbb{N} \\ 0 \leqslant r_1 + \cdots + r_k \leqslant d}} \lambda_{r_1,\ldots,r_k} X_1^{r_1} \cdots X_k^{r_k} \in K[X_1, \ldots, X_k]$.

On a

$$\begin{aligned}
\psi\big(P(a_1, \ldots, a_k)\big) &= \psi\left(\sum_{\substack{r_1,\ldots,r_k \in \mathbb{N} \\ 0 \leqslant r_1 + \cdots + r_k \leqslant d}} \lambda_{r_1,\ldots,r_k} a_1^{r_1} \cdots a_k^{r_k}\right) \\
&= \sum_{\substack{r_1,\ldots,r_k \in \mathbb{N} \\ 0 \leqslant r_1 + \cdots + r_k \leqslant d}} \lambda_{r_1,\ldots,r_k} \psi\left(a_1^{r_1} \cdots a_k^{r_k}\right) \text{ (car } \psi \text{ est une application } K\text{-linéaire)} \\
&= \sum_{\substack{r_1,\ldots,r_k \in \mathbb{N} \\ 0 \leqslant r_1 + \cdots + r_k \leqslant d}} \lambda_{r_1,\ldots,r_k} \big(\psi(a_1)\big)^{r_1} \cdots \big(\psi(a_k)\big)^{r_k} \text{ (ψ est un morphisme d'anneau unitaire)} \\
&= P\big(\psi(a_1), \ldots, \psi(a_k)\big)
\end{aligned}$$

Enfin, soit $\frac{S}{T} \in K(X_1, \ldots, X_k)$ tels que $T(a_1, \ldots, a_k) \neq 0$. On a alors

$$\begin{aligned}
\psi\left(\frac{S(a_1, \ldots, a_k)}{T(a_1, \ldots, a_k)}\right) &= \frac{\psi\big(S(a_1, \ldots, a_k)\big)}{\psi\big(T(a_1, \ldots, a_k)\big)} \text{ (car } \psi \text{ est un morphisme de corps)} \\
&= \frac{S\big(\psi(a_1), \ldots, \psi(a_k)\big)}{T\big(\psi(a_1), \ldots, \psi(a_k)\big)} \text{ (par ce que l'on vient de démontrer).}
\end{aligned}$$

Réciproquement, supposons que l'application ψ préserve toute fraction rationnelle à coefficients dans K et montrons que ψ est un endomorphisme de L sur K : si $a, b \in L$ et $\lambda, \mu \in K$, on a $\psi(1) = 1$,

$$\psi(a + b) = \psi\big((X_1 + X_2)(a, b)\big) = (X_1 + X_2)\big(\psi(a), \psi(b)\big) = \psi(a) + \psi(b),$$

$$\psi(ab) = \psi\big((X_1X_2)(a,b)\big) = (X_1X_2)\big(\psi(a),\psi(b)\big) = \psi(a)\psi(b)$$

et

$$\psi(\lambda a + \mu b) = \psi\big((\lambda X_1 + \mu X_2)(a,b)\big) = (\lambda X_1 + \mu X_2)\big(\psi(a),\psi(b)\big) = \lambda\psi(a) + \mu\psi(b).$$

□

Remarque 3.6.4. Supposons que ψ soit un endomorphisme de L sur K.

- Si un élément x de L est une racine d'un polynôme P de $K[X]$, alors $\psi(x)$ est également une racine de P dans L. En effet, on a
$$P\big(\psi(x)\big) = \psi\big(P(x)\big) = \psi(0) = 0.$$
- S'il existe $a_1, \ldots, a_l \in L$ tels que $L = K(a_1, \ldots, a_l)$, alors ψ est déterminé par les images respectives de $a_1, \ldots, a_l$ par ψ (d'après la proposition 1.2.5, tout élément de L est alors une fraction rationnelle à coefficients dans K évaluée en les éléments $a_1, \ldots, a_l$).

Exemple 3.6.5. Soit $\phi : \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{2})$ un endomorphisme de $\mathbb{Q}(\sqrt{2})$ sur $\mathbb{Q}$. Tout d'abord, comme l'extension $\mathbb{Q}(\sqrt{2})$ est de degré fini sur $\mathbb{Q}$, ϕ est un automorphisme de $\mathbb{Q}(\sqrt{2})$ sur $\mathbb{Q}$ (i.e. $\phi \in \mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$).

Ensuite, ϕ est déterminé par l'image de $\sqrt{2}$. Or, comme $\sqrt{2}$ est racine du polynôme $X^2 - 2 \in \mathbb{Q}[X]$, $\phi(\sqrt{2})$ est également une racine de $X^2 - 2$ dans $\mathbb{Q}(\sqrt{2})$: on a donc $\phi(\sqrt{2}) = \sqrt{2}$ ou $\phi(\sqrt{2}) = -\sqrt{2}$. L'application ϕ est donc soit l'application

$$\begin{array}{ccc} \mathbb{Q}(\sqrt{2}) & \to & \mathbb{Q}(\sqrt{2}) \\ a + b\sqrt{2} & \mapsto & a + b\sqrt{2} \end{array}$$

i.e. l'identité de $\mathbb{Q}(\sqrt{2})$ soit l'application

$$\rho : \begin{array}{ccc} \mathbb{Q}(\sqrt{2}) & \to & \mathbb{Q}(\sqrt{2}) \\ a + b\sqrt{2} & \mapsto & a - b\sqrt{2} \end{array}$$

Réciproquement, ces deux applications sont des automorphismes de $\mathbb{Q}(\sqrt{2})$ sur $\mathbb{Q}$. On a donc

$$\mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) = \Big\{\mathrm{id}_{\mathbb{Q}(\sqrt{2})}, \rho\Big\}$$

(remarquons que $\rho^2 = \mathrm{id}_{\mathbb{Q}(\sqrt{2})}$).

Intéressons-nous maintenant plus précisément à l'ensemble $\mathrm{Gal}(L/K)$ des automorphismes de L sur K. Muni de la composition, il s'agit d'un groupe, appelé groupe de Galois de L sur K :

Proposition 3.6.6. $\mathrm{Gal}(L/K)$ *est un sous-groupe du groupe des bijections de* L *dans* L.

Démonstration. L'identité de L est tout d'abord un automorphisme de L sur K. Nous avons par ailleurs déjà remarqué (cf. remarque 3.6.2) que l'inverse d'un automorphisme de L sur K était un automorphisme de L sur K. Enfin la composition d'applications linéaires, resp. de morphismes d'anneaux unitaires, d'applications bijectives est une application linéaire, resp. un morphisme d'anneaux unitaires, resp. une application bijective. □

Exemple 3.6.7. Nous avons montré dans l'exemple 3.6.5 que le groupe de Galois $\mathrm{Gal}\left(\mathbb{Q}(\sqrt{2})/\mathbb{Q}\right)$ était un groupe à deux éléments, (nécessairement isomorphe) à $\mathbb{Z}/2\mathbb{Z}$.

En lien avec notre problème initial, déterminons le groupe de Galois de $\mathbb{Q}(\zeta_n)$ sur $\mathbb{Q}$ pour tout $n \in \mathbb{N}\backslash\{0\}$:

Théorème 3.6.8. *Soit $n \in \mathbb{N}\backslash\{0\}$. Il existe un isomorphisme de groupes*

$$(\mathbb{Z}/n\mathbb{Z})^\times \to \mathrm{Gal}\left(\mathbb{Q}(\zeta_n)/\mathbb{Q}\right),$$

où $(\mathbb{Z}/n\mathbb{Z})^\times$ désigne le groupe des éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$.

Démonstration. Soit $m \in \mathbb{Z}$ un entier premier avec n. On commence par définir l'application ψ_m qui à tout élément $P(\zeta_n)$, $P \in \mathbb{Q}[X]$, de $\mathbb{Q}(\zeta_n) = \mathbb{Q}[\zeta_n]$ associe $P\left(\zeta_n^m\right)$ (en particulier, $\psi_m(\zeta_n) = \zeta_n^m$). L'application ψ_m est alors un automorphisme de $\mathbb{Q}(\zeta_n)$ sur $\mathbb{Q}$ i.e. un élément de $\mathrm{Gal}\left(\mathbb{Q}(\zeta_n)/\mathbb{Q}\right)$.

En effet, ψ_m est un endomorphisme de $\mathbb{Q}(\zeta_n)$ sur $\mathbb{Q}$ car, si $P_1, P_2 \in \mathbb{Q}[X]$ et $\lambda_1, \lambda_2 \in \mathbb{Q}$, on a

$$\begin{aligned}
\psi_m\big(\lambda_1 P_1(\zeta_n) + \lambda_2 P_2(\zeta_n)\big) &= \psi_m\big((\lambda_1 P_1 + \lambda_2 P_2)(\zeta_n)\big) \\
&= \left(\lambda_1 P_1 + \lambda_2 P_2\right)\left(\zeta_n^m\right) \\
&= \lambda_1 P_1\left(\zeta_n^m\right) + \lambda_2 P_2\left(\zeta_n^m\right) \\
&= \lambda_1 \psi_m\big(P_1(\zeta_n)\big) + \lambda_2 \psi_m\big(P_2(\zeta_n)\big)
\end{aligned}$$

et

$$\begin{aligned}
\psi_m\big(P_1(\zeta_n) P_2(\zeta_n)\big) &= \psi_m\big((P_1 P_2)(\zeta_n)\big) \\
&= \left(P_1 P_2\right)\left(\zeta_n^m\right) \\
&= P_1\left(\zeta_n^m\right) P_2\left(\zeta_n^m\right) \\
&= \psi_m\big(P_1(\zeta_n)\big)\psi_m\big(P_2(\zeta_n)\big)
\end{aligned}$$

Comme de plus l'extension $\mathbb{Q}(\zeta_n)$ est de degré fini sur $\mathbb{Q}$, ψ_m est un automorphisme de $\mathbb{Q}(\zeta_n)$ sur $\mathbb{Q}$.

Remarquons maintenant que si $m' \in \mathbb{Z}$ est un entier premier avec n et congru à m modulo n, il existe $k \in \mathbb{Z}$ tel que $m' = m + kn$ et donc

$$\zeta_n^{m'} = \zeta_n^{m+kn} = \zeta_n^m \left(\zeta_n^n\right)^k = \zeta_n^m,$$

ce qui montre que $\psi_{m'} = \psi_m$, et justifie que l'application

$$\begin{array}{rccc}
\Psi : & (\mathbb{Z}/n\mathbb{Z})^\times & \to & \mathrm{Gal}\left(\mathbb{Q}(\zeta_n)/\mathbb{Q}\right) \\
& \overline{m} & \mapsto & \psi_m
\end{array}$$

est bien définie.

Nous allons à présent montrer que l'application Ψ est un isomorphisme de groupes.

Il s'agit tout d'abord d'un morphisme de groupes car, si $\overline{m_1}, \overline{m_2} \in (\mathbb{Z}/n\mathbb{Z})^\times$, on a

$$\Psi\left(\overline{m_1}\ \overline{m_2}\right) = \Psi\left(\overline{m_1 m_2}\right) = \psi_{m_1 m_2}$$

et

$$\begin{aligned}
\psi_{m_1 m_2}(\zeta_n) &= \zeta_n^{m_1 m_2} \\
&= \left(\zeta_n^{m_1}\right)^{m_2} \\
&= X^{m_2}\left(\zeta_n^{m_1}\right) \\
&= \psi_{m_1}\left(X^{m_2}(\zeta_n)\right) \\
&= \psi_{m_1}\left(\zeta_n^{m_2}\right) \\
&= \psi_{m_1}\left(\psi_{m_2}(\zeta_n)\right) \\
&= \psi_{m_1} \circ \psi_{m_2}(\zeta_n),
\end{aligned}$$

donc $\psi_{m_1 m_2} = \psi_{m_1} \circ \psi_{m_2}$ (un endomorphisme de $\mathbb{Q}(\zeta_n)$ sur $\mathbb{Q}$ est déterminé par l'image de η_n) i.e. $\Psi\left(\overline{m_1}\ \overline{m_2}\right) = \Psi\left(\overline{m_1}\right) \circ \Psi\left(\overline{m_2}\right)$.

Le morphisme de groupes Ψ est ensuite injectif : soit $\overline{m} \in (\mathbb{Z}/n\mathbb{Z})^\times$ tel que $\psi_m = id_L$ alors, en particulier, $\zeta_n^m = \zeta_n$ et donc $\zeta_n^{m-1} = 1$. Comme ζ_n est d'ordre n dans le groupe des racines de l'unité, n divise $m-1$ et donc $\overline{m-1} = \overline{0}$ i.e. $\overline{m} = \overline{1}$.

Montrons enfin que Ψ est surjectif. Soit $\psi \in \mathrm{Gal}\left(\mathbb{Q}(\zeta_n)/\mathbb{Q}\right)$. Alors, comme ζ_n est une racine du polynôme cyclotomique Φ_n, il en est de même pour $\psi(\zeta_n)$: il existe donc $m \in \{1, \ldots, n\}$ premier avec n tel que $\psi(\zeta_n) = \zeta_n^m$ et donc $\psi = \psi_m = \Psi(\overline{m})$. □

En particulier, si $p = 1 + 2^{2^m}$ est un nombre de Fermat premier, $m \in \mathbb{N}$, le groupe de Galois $\mathrm{Gal}\left(\mathbb{Q}(\zeta_p)/\mathbb{Q}\right)$ est cyclique (car alors $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique d'ordre $p-1$ car $\mathbb{Z}/p\mathbb{Z}$ est un corps fini car p est premier).

Soit alors ρ un générateur de $\mathrm{Gal}\left(\mathbb{Q}(\zeta_p)/\mathbb{Q}\right)$. Pour tout $k \in \{0, \ldots, 2^m\}$, notons ensuite G_k le sous-groupe de $\mathrm{Gal}\left(\mathbb{Q}(\zeta_p)/\mathbb{Q}\right)$ engendré par ρ^{2^k}. Remarquons que $G_0 = \mathrm{Gal}\left(\mathbb{Q}(\zeta_p)/\mathbb{Q}\right)$, que $G_{2^m} = \left\{\mathrm{id}_{\mathbb{Q}(\zeta_p)}\right\}$ (car $\rho^{2^{2^m}} = \rho^{p-1} = \mathrm{id}_{\mathbb{Q}(\zeta_p)}$) et que l'on a une suite d'inclusions

$$\left\{\mathrm{id}_{\mathbb{Q}(\zeta_p)}\right\} = G_{2^m} \subset G_{2^m - 1} \subset \cdots \subset G_1 \subset G_0 = \mathrm{Gal}\left(\mathbb{Q}(\zeta_p)/\mathbb{Q}\right)$$

(pour tout $k \in \{0, \ldots, 2^m - 1\}$, $\rho^{2^{k+1}} = \left(\rho^{2^k}\right)^2 \in G_k$).

Nous allons appliquer à cette suite d'inclusions la propriété suivante, issue de la théorie de Galois, pour obtenir une suite d'extensions qui nous permettra, via le théorème 3.2.4, de montrer que le nombre complexe ζ_p est constructible.

Proposition 3.6.9. *Soit S un sous-ensemble de $\mathrm{Gal}(L/K)$ et notons*

$$L^S := \{x \in L \mid \forall \psi \in S, \psi(x) = x\}.$$

L'ensemble L^S est un sous-corps de L contenant K.

Démonstration. Pour tout $\psi \in S$, $\psi(1) = 1$ (car tout élément de S est en particulier un automorphisme de L sur K donc un morphisme d'anneau unitaire) donc $1 \in L^S$.

Soient maintenant $x, y \in L^S$. Pour tout $\psi \in S$, on a

$$\psi(x - y) = \psi(x) - \psi(y) = x - y,$$

$$\psi(xy) = \psi(x)\psi(y) = xy$$

et, si $x \neq 0$,

$$\psi\left(x^{-1}\right) = \psi(x)^{-1} = x^{-1}$$

donc $x - y$, $xy \in L^S$ et, si $x \neq 0$, $x^{-1} \in L^S$: L^S est donc un sous-corps de L.

Enfin, si $a \in K$, on a, pour tout $\psi \in S$, $\psi(a) = a$ (car toute application de S est en particulier un automorphisme de L sur K donc laisse fixe tous les éléments de K) : L^S contient donc K. □

Remarquons également que si S_1 et S_2 sont deux sous-ensembles de $\mathrm{Gal}(L/K)$ tels que $S_1 \subset S_2$, alors $L^{S_2} \subset L^{S_1}$: si $x \in L^{S_2}$, on a, pour tout $\psi \in S_1 \subset S_2$, $\psi(x) = x$.

Nous allons appliquer cette remarque et la proposition 3.6.9 à la suite d'inclusions de sous-groupes de $\mathrm{Gal}\left(\mathbb{Q}(\zeta_p)/\mathbb{Q}\right)$ définie plus haut pour terminer la preuve du sens réciproque du théorème de Gauss-Wantzel 3.1.1.

3.7 Sens réciproque du théorème de Gauss-Wantzel : fin de la preuve

Reprenons notre nombre de Fermat premier $p = 1 + 2^{2^m}$ avec $m \in \mathbb{N}$. Nous avions justifié que si nous parvenions à montrer la constructibilité du nombre complexe ζ_p, cela montrerait le sens réciproque du théorème de Gauss-Wantzel.

Reprenons la suite d'inclusions

$$\left\{\mathrm{id}_{\mathbb{Q}(\zeta_p)}\right\} = G_{2^m} \subset G_{2^m-1} \subset \cdots \subset G_1 \subset G_0 = \mathrm{Gal}\left(\mathbb{Q}(\zeta_p)/\mathbb{Q}\right)$$

de sous-groupes du groupe de Galois $\mathrm{Gal}\left(\mathbb{Q}(\zeta_p)/\mathbb{Q}\right)$ définie plus haut, et appliquons-lui la proposition 3.6.9 : si, pour tout $i \in \{0, \ldots, 2^m\}$, on note $L_i := \mathbb{Q}(\zeta_p)^{G_i}$, obtient une suite

$$L_0 \subset L_1 \subset \cdots \subset L_{2^m-1} \subset L_{2^m}$$

de sous-corps de $\mathbb{Q}(\zeta_p)$ contenant $\mathbb{Q}$ avec $L_{2^m} = \mathbb{Q}(\zeta_p)^{G_{2^m}} = \mathbb{Q}(\zeta_p)^{\left\{\mathrm{id}_{\mathbb{Q}(\zeta_p)}\right\}} = \mathbb{Q}(\zeta_p)$.

Nous allons maintenant montrer que cette suite d'extensions et ζ_p vérifient le critère suffisant de constructibilité du théorème 3.2.4 :

Théorème 3.7.1. *On a*

- $L_0 = \mathbb{Q}$ $(= \mathbb{Q}(\{O, A\}))$,

- $\zeta_p \in L_{2^m} = \mathbb{Q}(\zeta_p)$,
- *pour tout* $i \in \{1, \dots, 2^m\}$, $[L_i : L_{i-1}] = 2$,

et le nombre complexe ζ_p *est donc constructible à partir de* $\{O, A\}$ *par le théorème 3.2.4.*

Démonstration. Rappelons que nous avions considéré un générateur ρ du groupe cyclique $\mathrm{Gal}\left(\mathbb{Q}(\zeta_p)/\mathbb{Q}\right)$ d'ordre $p-1$: on a donc

$$\mathrm{Gal}\left(\mathbb{Q}(\zeta_p)/\mathbb{Q}\right) = \left\{\mathrm{id}_{\mathbb{Q}(\zeta_p)}, \rho, \dots, \rho^{p-2}\right\}.$$

Par ailleurs, comme ζ_p est une racine de $\Phi_p \in \mathbb{Q}[X]$, pour tout $l \in \{0, \dots, p-2\}$, $\rho^l(\zeta_p)$ est également une racine de Φ_p dans $\mathbb{Q}(\zeta_p)$: il existe donc $r \in \{1, \dots, p-1\}$ tel que $\rho^l(\zeta_p) = \zeta_p^r$ (p est premier). De plus, si $\rho^{l_1}(\zeta_p) = \rho^{l_2}(\zeta_p)$ avec $l_1, l_2 \in \{0, \dots, p-2\}$, alors $\rho^{l_1} = \rho^{l_2}$ (un automorphisme de $\mathbb{Q}(\zeta_p)$ sur $\mathbb{Q}$ est déterminé par sa valeur en ζ_p) et donc $l_1 = l_2$ (ρ engendre $\mathrm{Gal}\left(\mathbb{Q}(\zeta_p)/\mathbb{Q}\right)$).

On déduit des considérations précédentes que

$$\left\{\zeta_p, \rho(\zeta_p), \dots, \rho^{p-2}(\zeta_p)\right\} = \left\{\zeta_p, \zeta_p^2, \dots, \zeta_p^{p-1}\right\}.$$

Or la famille $\left\{\zeta_p, \zeta_p^2, \dots, \zeta_p^{p-1}\right\}$ est libre sur $\mathbb{Q}$. En effet, si $\lambda_1, \dots, \lambda_{p-1}$ sont des scalaires de $\mathbb{Q}$ tels que $0 = \sum_{s=1}^{p-1} \lambda_s \zeta_p^s = \left(\sum_{s=1}^{p-1} \lambda_s X^s\right)(\zeta_p)$ alors le polynôme $\sum_{s=1}^{p-1} \lambda_s X^s$, de degré au plus $p-1$, annule ζ_p et est donc un multiple de $\mu_{\zeta_p,\mathbb{Q}} = \Phi_p = 1 + X + \cdots + X^{p-1}$: il existe donc $a \in \mathbb{Q}$ tel que

$$\lambda_1 X + \cdots + \lambda_{p-1} X^{p-1} = a + aX + \cdots + aX^{p-1}$$

et donc nécessairement $a = 0$ i.e. $\sum_{s=1}^{p-1} \lambda_s X^s = 0$ i.e. $\lambda_1 = \cdots = \lambda_{p-1} = 0$.

La famille à $p-1$ éléments $\left\{\zeta_p, \rho(\zeta_p), \dots, \rho^{p-2}(\zeta_p)\right\} = \left\{\zeta_p, \zeta_p^2, \dots, \zeta_p^{p-1}\right\}$ est ainsi une $\mathbb{Q}$-base de $\mathbb{Q}(\zeta_p)$ ($[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p-1$).

On utilise cette propriété pour montrer tout d'abord que $L_0 = \mathbb{Q}(\zeta_p)^{\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})} = \mathbb{Q}$.

Soit $x \in L_0 \subset \mathbb{Q}(\zeta_p)$. D'après ce que l'on vient de démontrer, il existe $a_0, \dots, a_{p-2} \in \mathbb{Q}$ tels que

$$x = a_0\zeta_p + \cdots + a_{p-2}\rho^{p-2}(\zeta_p)$$

Comme $x \in L_0 = \mathbb{Q}(\zeta_p)^{\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})}$, $\rho \in \mathrm{Gal}\left(\mathbb{Q}(\zeta_p)/\mathbb{Q}\right)$ et $\rho^{p-1} = id_{\mathbb{Q}(\zeta_p)}$, on a ensuite

$$x = \rho(x) = a_0\rho(\zeta_p) + \cdots + a_{p-1}\rho^{p-2}(\zeta_p) + a_{p-2}\zeta_p = a_{p-2}\zeta_p + a_0\rho(\zeta_p) + \cdots + a_{p-1}\rho^{p-2}(\zeta_p).$$

Par indépendance linéaire de la famille $\left\{\zeta_p, \rho(\zeta_p), \dots, \rho^{p-2}(\zeta_p)\right\}$, on obtient alors que $a_{p-2} = a_0$ et, pour tout $l \in \{1, \dots, p-2\}$, $a_l = a_{l-1}$.

Ainsi,

$$x = a_0\zeta_p + \cdots + a_0\rho^{p-2}(\zeta_p) = a_0\left(\zeta_p + \cdots + \rho^{p-2}(\zeta_p)\right) = a_0\left(\zeta_p + \cdots + \zeta_p^{p-1}\right) = a_0\left(\Phi_p(\zeta_p) - 1\right) = -a_0 \in \mathbb{Q}$$

et donc $L_0 = \mathbb{Q}$.

Nous allons à présent montrer que pour tout $i \in \{1, \ldots, 2^m\}$, $[L_i : L_{i-1}] = 2$. Afin de simplifier, notons tout d'abord $d := 2^m$. Soit ensuite $i \in \{1, \ldots, d\}$ et notons

$$\alpha_i := \sum_{k=0}^{2^{d-i}-1} \rho^{2^i k}(\zeta_p) \in \mathbb{C}.$$

Rappelons que $\left\{\zeta_p, \rho(\zeta_p), \ldots, \rho^{p-2}(\zeta_p)\right\} = \left\{\zeta_p, \zeta_p^2, \ldots, \zeta_p^{p-1}\right\}$ et que ρ engendre le groupe cyclique $\mathrm{Gal}\left(\mathbb{Q}(\zeta_p)/\mathbb{Q}\right)$: en particulier, $\alpha_i \in \mathbb{Q}(\zeta_p)$. Remarquons ensuite que si $k \in \{0, \ldots, 2^{d-i}-1\}$, $2^i k \in \{0, \ldots, p-2\}$, car alors

$$0 \leqslant 2^i k \leqslant 2^i \left(2^{d-i} - 1\right) = 2^d - 2^i \leqslant 2^d - 1 = p - 2$$

$(p = 1 + 2^d)$.

Nous allons prouver que $\alpha_i \in L_i \backslash L_{i-1}$: ceci montrera en particulier que $[L_i : L_{i-1}] \geqslant 2$.

Prouvons tout d'abord que $\alpha_i \in L_i = \mathbb{Q}(\zeta_p)^{G_i} = \mathbb{Q}(\zeta_p)^{G_i}$ où G_i est le sous-groupe de $\mathrm{Gal}\left(\mathbb{Q}(\zeta_p)/\mathbb{Q}\right)$ engendré par ρ^{2^i}, autrement dit prouvons que $\rho^{2^i}(\alpha_i) = \alpha_i$: on a

$$\begin{aligned}
\rho^{2^i}(\alpha_i) &= \rho^{2^i}\left(\sum_{k=0}^{2^{d-i}-1} \rho^{2^i k}(\zeta_p)\right) \\
&= \sum_{k=0}^{2^{d-i}-1} \rho^{2^i}\left(\rho^{2^i k}(\zeta_p)\right) \\
&= \sum_{k=0}^{2^{d-i}-1} \rho^{2^i + 2^i k}(\zeta_p) \\
&= \sum_{k=0}^{2^{d-i}-1} \rho^{2^i (k+1)}(\zeta_p) \\
&= \sum_{k=1}^{2^{d-i}} \rho^{2^i k}(\zeta_p) \\
&= \sum_{k=0}^{2^{d-i}-1} \rho^{2^i k}(\zeta_p) = \alpha_i
\end{aligned}$$

car

$$\rho^{2^i \times 2^{d-i}}(\zeta_p) = \rho^{2^d}(\zeta_p) = \rho^{p-1}(\zeta_p) = \mathrm{id}_{\mathbb{Q}(\zeta_p)}(\zeta_p) = \zeta_p = \rho^{2^i \times 0}(\zeta_p).$$

Prouvons maintenant que $\alpha_i \notin L_{i-1}$ i.e. $\rho^{2^{i-1}}(\alpha_i) \notin \alpha_i$. On a

$$\begin{aligned}\rho^{2^{i-1}}(\alpha_i) &= \rho^{2^{i-1}}\left(\sum_{k=0}^{2^{d-i}-1}\rho^{2^i k}(\zeta_p)\right)\\ &= \sum_{k=0}^{2^{d-i}-1}\rho^{2^{i-1}}\left(\rho^{2^i k}(\zeta_p)\right)\\ &= \sum_{k=0}^{2^{d-i}-1}\rho^{2^i k+2^{i-1}}(\zeta_p).\end{aligned}$$

Comme

$$\begin{aligned}1 \leqslant 2^i k + 2^{i-1} &\leqslant 2^i\left(2^{d-i}-1\right)+2^{i-1}\\ &= 2^d - 2^i + 2^{i-1}\\ &= 2^d - 2^{i-1} \text{ (car } 2^{i-1}-2^i = 2^{i-1}(1-2) = -2^{i-1})\\ &= p-1-2^{i-1}\\ &\leqslant p-2,\end{aligned}$$

L'écriture $\rho^{2^{i-1}}(\alpha_i) = \sum_{k=0}^{2^{d-i}-1}\rho^{2^i k+2^{i-1}}(\zeta_p)$ est la décomposition de $\rho^{2^{i-1}}(\alpha_i)$ dans la $\mathbb{Q}$-base $\left\{\zeta_p, \rho(\zeta_p), \ldots, \rho^{p-2}(\zeta_p)\right\}$ de $\mathbb{Q}(\zeta_p)$, décomposition différente de la décomposition $\alpha_i = \sum_{k=0}^{2^{d-i}-1}\rho^{2^i k}(\zeta_p)$ de α_i car, par exemple, le terme ζ_p apparaît dans la seconde somme mais pas dans la première : les éléments α_i et $\rho^{2^{i-1}}(\alpha_i)$ de $\mathbb{Q}(\zeta_p)$ sont donc différents, et $\alpha_i \notin L_{i-1}$.

En particulier, comme L_i contient un élément qui n'est pas dans L_{i-1}, le degré de L_i sur L_{i-1} est au moins 2.

Montrons enfin que pour tout $j \in \{1, \ldots, d\}$, $[L_j : L_{j-1}]$ est égal à 2. D'après le théorème 1.1.8 de multiplicativité des degrés, on a, puisque $L_0 = \mathbb{Q}$ et $L_d = \mathbb{Q}(\zeta_p)$,

$$2^d = p-1 = [\mathbb{Q}(\zeta_p) : \mathbb{Q}] = [L_d : L_0] = [L_d : L_{d-1}]\cdots[L_1 : L_0].$$

Or, pour tout $j \in \{1, \ldots, d\}$, $[L_j : L_{j-1}] \geqslant 2$ et s'il existait un indice $j_0 \in \{1, \ldots, n\}$ tel que $[L_{j_0} : L_{j_0-1}] > 2$, le produit $[L_d : L_{d-1}]\cdots[L_1 : L_0]$ serait alors strictement plus grand que 2^d, ce qui n'est pas le cas : on a donc bien, pour tout $j \in \{1, \ldots, d\}$, $[L_j : L_{j-1}] = 2$. □

Remarque 3.7.2. Avec les notations de la preuve ci-dessus, pour tout $i \in \{1, \ldots, d\}$, $L_i = L_{i-1}(\alpha_i)$.

Nous avons ainsi terminé la démonstration du théorème de Gauss-Wantzel dont nous rappelons ci-dessous l'énoncé :

Théorème 3.7.3 (Théorème de Gauss-Wantzel)**.** *Soit $n \in \mathbb{N}\backslash\{0;1;2\}$. Le polygone régulier à n côtés $\mathcal{R}_n$ est constructible à partir de $\{O, A\}$ si et seulement si n est le produit d'une puissance de deux et de nombres de Fermat premiers et deux à deux distincts.*

Exemple 3.7.4.

- Le triangle équilatéral est constructible à la règle et au compas.
- Le carré est constructible à la règle et au compas.
- Le pentagone régulier est constructible à la règle et au compas.
- L'hexagone régulier est constructible à la règle et au compas.
- L'heptagone régulier n'est pas constructible à la règle et au compas.
- L'octogone régulier est constructible à la règle et au compas.
- Le nonagone (ou ennéagone) régulier n'est pas constructible à la règle et au compas.
- Le décagone régulier est constructible à la règle et au compas.
- Le hendécagone régulier n'est pas constructible à la règle et au compas.
- Le dodécagone régulier est constructible à la règle et au compas.
- Le tridécagone régulier n'est pas constructible à la règle et au compas.
- Le tétradécagone régulier n'est pas constructible à la règle et au compas.
- Le pentadécagone régulier est constructible à la règle et au compas.
- L'hexadécagone régulier est constructible à la règle et au compas.
- L'heptadécagone régulier est constructible à la règle et au compas.
- L'octadécagone régulier n'est pas constructible à la règle et au compas.
- L'ennéadécagone régulier n'est pas constructible à la règle et au compas.
- L'icosagone régulier est constructible à la règle et au compas.

Chapitre 4

Courbes paramétrées

4.1 Introduction

Soit $d \in \mathbb{N}\backslash\{0\}$. Dans tout ce chapitre, on se place dans l'espace vectoriel $\mathbb{R}^d$ muni de la norme euclidienne

$$\|\cdot\| : \begin{array}{ccc} \mathbb{R}^d & \to & [0;+\infty[\\ (x_1,\dots,x_d) & \mapsto & \sqrt{\sum_{i=1}^{d} x_i^2} \end{array}$$

Dans ce contexte, on rappelle que si I est un intervalle de $\mathbb{R}$, si

$$f : \begin{array}{ccc} I & \to & \mathbb{R}^d \\ t & \mapsto & f(t) = (f_1(t),\dots,f_d(t)) \end{array}$$

est une *fonction vectorielle* et si $k \in \mathbb{N} \cup \{\infty\}$, f est dite *dérivable* sur I, resp. *de classe* $\mathcal{C}^k$ sur I, si toutes les fonctions $f_1,\dots,f_d$ sont dérivables sur I, resp. de classe $\mathcal{C}^k$ sur I. Si f est dérivable sur I, on note f' la fonction vectorielle

$$\begin{array}{ccc} I & \to & \mathbb{R}^d \\ t & \mapsto & (f_1'(t),\dots,f_d'(t)) \end{array}$$

et, pour tout $t \in I$, si $h \in \mathbb{R}$ est tel que $t+h \in I$, on a

$$\frac{f(t+h)-f(t)}{h} \xrightarrow[h\to 0]{} f'(t).$$

Si I est un segment $[a,b]$ avec $a,b \in \mathbb{R}$ tels que $a < b$, on dit que la fonction vectorielle f est *intégrable au sens de Riemann* (ou *Riemann-intégrable*) sur $[a,b]$ si toutes les fonctions $f_1,\dots,f_n$ sont intégrables au sens de Riemann sur $[a,b]$, et on note alors $\displaystyle\int_a^b f(t)\mathrm{d}t$ le vecteur

$$\left(\int_a^b f_1(t)\mathrm{d}t,\dots,\int_a^b f_d(t)\mathrm{d}t\right)$$

de $\mathbb{R}^d$. Si f est Riemann-intégrable sur $[a,b]$, on a l'inégalité

$$\left\| \int_a^b f(t)\mathrm{d}t \right\| \leqslant \int_a^b \|f(t)\| \,\mathrm{d}t.$$

4.2 Notion de courbe paramétrée

Soit $k \in \mathbb{N} \cup \{\infty\}$. Une courbe paramétrée (ou arc paramétré) de classe $\mathcal{C}^k$ dans $\mathbb{R}^d$ désigne toute fonction vectorielle de classe $\mathcal{C}^k$

$$\gamma : I \to \mathbb{R}^d$$

où I est un intervalle de $\mathbb{R}$. Une courbe paramétrée dans $\mathbb{R}^2$ est appelée une courbe paramétrée plane.

Commençons par donner quelques exemples de courbes paramétrées :

Exemple 4.2.1.
1. L'application $\mathbb{R} \to \mathbb{R}^2$; $t \mapsto (t,t)$ est une courbe paramétrée de classe $\mathcal{C}^\infty$.
2. L'application $\mathbb{R} \to \mathbb{R}^2$; $t \mapsto (t^2,t^3)$ est une courbe paramétrée de classe $\mathcal{C}^\infty$.
3. L'application $[0,2\pi[\to \mathbb{R}^2$; $t \mapsto (\cos(t),\sin(t))$ est une courbe paramétrée de classe $\mathcal{C}^\infty$.
4. L'application $\mathbb{R} \to \mathbb{R}^3$; $t \mapsto (\cos(t),\sin(t),t)$ est une courbe paramétrée de classe $\mathcal{C}^\infty$ (dans $\mathbb{R}^3$).

Remarque 4.2.2. Par définition, une courbe paramétrée est une fonction vectorielle (au moins) continue.

Soit $k \in \mathbb{N} \cup \{\infty\}$ et soit $\gamma : I \to \mathbb{R}^d$ une courbe paramétrée de classe $\mathcal{C}^k$. On prendra bien garde de ne pas confondre la courbe paramétrée γ avec son *support* :

Définition 4.2.3. *Le support de la courbe paramétrée γ est l'image*

$$\mathcal{C}_\gamma := \{\gamma(t) \mid t \in I\}$$

de γ et on dit alors que γ est une paramétrisation de $\mathcal{C}_\gamma$. Le support d'une courbe paramétrée sera simplement appelé courbe.

Exemple 4.2.4. Reprenons les exemples de l'exemple 4.2.1.

1. Le support de la courbe paramétrée n° 1 est la droite d'équation $y = x$ dans $\mathbb{R}^2$.
2. Le support de la courbe paramétrée n° 2 est la courbe *cuspidale* d'équation $y^2 = x^3$ dans $\mathbb{R}^2$.
3. Le support de la courbe paramétrée n° 3 est le cercle unité dans $\mathbb{R}^2$ d'équation $x^2+y^2 = 1$.
4. Le support de la courbe paramétrée n° 4 est une courbe *hélicoïdale* dans $\mathbb{R}^3$.

Remarque 4.2.5. Deux courbes paramétrées différentes peuvent avoir le même support. Par exemple, le support de la courbe paramétrée $\mathbb{R} \to \mathbb{R}^2$; $t \mapsto (t^3, t^3)$ est, comme dans l'exemple 1 ci-dessus, la droite d'équation $y = x$ dans $\mathbb{R}^2$, et le support de la courbe paramétrée $\mathbb{R} \to \mathbb{R}^2$; $t \mapsto (\cos(t), \sin(t))$ est, comme dans l'exemple 3 ci-dessus, le cercle unité dans $\mathbb{R}^2$. Une même courbe peut ainsi posséder plusieurs paramétrisations.

La courbe paramétrée γ contient plus d'informations géométriques que son support C_γ : la fonction vectorielle γ correspond à une "façon de parcourir" la courbe C_γ. Deux paramétrisations de C_γ seront considérées comme *équivalentes* si l'on peut passer de l'une à l'autre par composition avec un difféomorphisme :

Définition 4.2.6. *Soit $\eta : J \to \mathbb{R}^d$ une courbe paramétrée de classe $\mathcal{C}^k$. On dit que la courbe paramétrée γ est $\mathcal{C}^k$-équivalente à la courbe paramétrée η s'il existe un $\mathcal{C}^k$-difféomorphisme $\sigma : J \to I$ tel que $\gamma \circ \sigma = \eta$, et on dira alors que η est une reparamétrisation de classe $\mathcal{C}^k$ de C_γ.*

Remarque 4.2.7. Si $\eta : J \to \mathbb{R}^d$ est une courbe paramétrée $\mathcal{C}^0$-équivalente à γ, on a bien $C_\eta = C_\gamma$: si $\sigma : J \to I$ est un homéomorphisme tel que $\gamma \circ \sigma = \eta$, alors

$$C_\eta = \{\eta(s) \mid s \in J\} = \big\{\gamma\big(\sigma(s)\big) \mid s \in J\big\} = \{\gamma(t) \mid t \in I\}\,.$$

Exemple 4.2.8.

1. La courbe paramétrée $\mathbb{R} \to \mathbb{R}^2$; $t \mapsto (t^3, t^3)$ est $\mathcal{C}^0$-équivalente à $\mathbb{R} \to \mathbb{R}^2$; $t \mapsto (t, t)$, via l'homéomorphisme $\mathbb{R} \mapsto \mathbb{R}$; $t \mapsto t^{\frac{1}{3}}$.

2. La courbe paramétrée
$$\eta : \begin{array}{ccc} \mathbb{R} & \to & \mathbb{R}^2 \\ t & \mapsto & \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right) \end{array}$$
est une reparamétrisation de classe $\mathcal{C}^\infty$ de la courbe C_ρ où
$$\rho : \begin{array}{ccc}]-\pi, \pi[& \to & \mathbb{R}^2 \\ \theta & \mapsto & (\cos(\theta), \sin(\theta)) \end{array}$$
(la courbe C_ρ est constituée du cercle unité de $\mathbb{R}^2$ privé du point de coordonnées $(-1, 0)$). En effet, si $\theta \in]-\pi, \pi[$,
$$\begin{aligned} \cos(\theta) &= \cos\left(2 \times \frac{\theta}{2}\right) \\ &= \cos^2\left(\frac{\theta}{2}\right) - \sin^2\left(\frac{\theta}{2}\right) \\ &= \frac{\cos^2\left(\frac{\theta}{2}\right) - \sin^2\left(\frac{\theta}{2}\right)}{\cos^2\left(\frac{\theta}{2}\right) + \sin^2\left(\frac{\theta}{2}\right)} \\ &= \frac{\cos^2\left(\frac{\theta}{2}\right)\left(1 - \tan^2\left(\frac{\theta}{2}\right)\right)}{\cos^2\left(\frac{\theta}{2}\right)\left(1 + \tan^2\left(\frac{\theta}{2}\right)\right)} \\ &= \frac{1 - \tan^2\left(\frac{\theta}{2}\right)}{1 + \tan^2\left(\frac{\theta}{2}\right)} \end{aligned}$$

et

$$\begin{aligned}\sin(\theta) &= \sin\left(2\times\frac{\theta}{2}\right)\\ &= 2\sin\left(\frac{\theta}{2}\right)\cos\left(\frac{\theta}{2}\right)\\ &= \frac{2\sin\left(\frac{\theta}{2}\right)\cos\left(\frac{\theta}{2}\right)}{\cos^2\left(\frac{\theta}{2}\right)+\sin^2\left(\frac{\theta}{2}\right)}\\ &= \frac{\cos^2\left(\frac{\theta}{2}\right)\left(2\tan\left(\frac{\theta}{2}\right)\right)}{\cos^2\left(\frac{\theta}{2}\right)\left(1+\tan^2\left(\frac{\theta}{2}\right)\right)}\\ &= \frac{2\tan\left(\frac{\theta}{2}\right)}{1+\tan^2\left(\frac{\theta}{2}\right)},\end{aligned}$$

donc, si l'on note σ le $\mathcal{C}^\infty$-difféomorphisme

$$\begin{array}{ccc}\mathbb{R} & \to &]-\pi,\pi[\\ t & \mapsto & 2\arctan(t)\end{array}$$

d'inverse

$$\begin{array}{ccc}]-\pi,\pi[& \to & \mathbb{R}\\ \theta & \mapsto & \tan\left(\frac{\theta}{2}\right)\end{array},$$

on a

$$\eta\circ\sigma^{-1}=\rho \quad \text{i.e.} \quad \rho\circ\sigma=\eta.$$

Remarquons que, si $k\in\mathbb{N}$, la $\mathcal{C}^k$-équivalence est bien une relation d'équivalence.

Lemme 4.2.9. *Soit $k\in\mathbb{N}$ et notons $\gamma_1\sim_k\gamma_2$ si γ_1 et γ_2 sont deux courbes paramétrées de classe $\mathcal{C}^k$ telles que γ_1 est $\mathcal{C}^k$-équivalente à γ_2. La relation $\sim_k$ est une relation d'équivalence.*

Démonstration. La relation $\sim_k$ est tout d'abord réflexive : si la courbe paramétrée γ de classe $\mathcal{C}^k$, alors $\gamma\sim_k\gamma$ car $\gamma\circ\mathrm{id}_I=\gamma$ et l'identité id_I est une fonction de classe $\mathcal{C}^\infty$ (et donc en particulier de classe $\mathcal{C}^k$) sur I.

La relation $\sim_k$ est ensuite symétrique. En effet, si $\gamma_1:I_1\to\mathbb{R}^d$ et $\gamma_2:I_2\to\mathbb{R}^d$ sont deux courbes paramétrées de classe $\mathcal{C}^k$ et $\sigma:I_2\to I_1$ est un $\mathcal{C}^k$-difféomorphisme tels que $\gamma_1\circ\sigma=\gamma_2$, alors $\gamma_2\circ\sigma^{-1}=\gamma_1$ et $\sigma^{-1}:I_1\to I_2$ est également un $\mathcal{C}^k$-difféomorphisme donc $\gamma_2\sim_k\gamma_1$.

La relation $\sim_k$ est enfin transitive : soient $\gamma_1:I_1\to\mathbb{R}^d$, $\gamma_2:I_2\to\mathbb{R}^d$, $\gamma_3:I_3\to\mathbb{R}^d$ trois courbes paramétrées de classe $\mathcal{C}^k$ et deux $\mathcal{C}^k$-difféomorphismes $\sigma:I_2\to I_1$, $\tau:I_3\to I_2$ tels que

$$\gamma_1\circ\sigma=\gamma_2 \quad \text{et} \quad \gamma_2\circ\tau=\gamma_3.$$

Alors on a

$$\gamma_1\circ(\sigma\circ\tau)=(\gamma_1\circ\sigma)\circ\tau=\gamma_2\circ\tau=\gamma_3.$$

L'application composée $\sigma\circ\tau:I_3\to I_1$ étant également un $\mathcal{C}^k$-difféomorphisme, la courbe paramétrée γ_1 est bien $\mathcal{C}^k$-équivalente à γ_1. □

Dans la suite de ce chapitre, nous allons introduire et étudier différentes notions générales des courbes paramétrées.

4.3 Multiplicité et simplicité

Soit $\gamma : I \to \mathbb{R}^d$ et soit $t_0 \in I$.

Définition 4.3.1. *Soit $m \in \mathbb{N}\backslash\{0\}$. On dit que le point $\gamma(t_0)$ de la courbe C_γ* paramétrée par *γ est de multiplicité m si l'ensemble $\{t \in I \mid \gamma(t) = \gamma(t_0)\}$ des antécédents de $\gamma(t_0)$ par γ est fini de cardinal m. Si l'ensemble $\{t \in I \mid \gamma(t) = \gamma(t_0)\}$ est infini, on dit que $\gamma(t_0)$ est un point de multiplicité infinie de C_γ.*

Un point de multiplicité 1, resp. 2, resp. 3, sera également dit simple, resp. double, resp. triple.

Exemple 4.3.2.

1. Le point $(0,0)$ du *lemniscate de Bernoulli* paramétré par la courbe paramétrée (de classe $\mathcal{C}^\infty$)
$$\begin{array}{rccc} \rho : & [0,2\pi[& \to & \mathbb{R} \\ & \theta & \mapsto & \left(\frac{\cos(\theta)}{1+\sin^2(\theta)}, \frac{\sin(\theta)\cos(\theta)}{1+\sin^2(\theta)}\right) \end{array}$$
est un point double ($(0,0) = \rho\left(\frac{\pi}{2}\right) = \rho\left(\frac{3\pi}{2}\right)$).

2. Tout point du cercle unité de $\mathbb{R}^2$ paramétré par la courbe paramétrée $[0,2\pi[\to \mathbb{R}^2$; $t \mapsto (\cos(t), \sin(t))$ est simple.

3. Tout point du cercle unité de $\mathbb{R}^2$ paramétré par la courbe paramétrée $\mathbb{R} \to \mathbb{R}^2$; $t \mapsto (\cos(t), \sin(t))$ est de multiplicité infinie.

4. On considère la courbe paramétrée (de classe $\mathcal{C}^0$)
$$\begin{array}{rccc} \eta : & [0;2[& \to & \mathbb{R}^1 \\ & t & \mapsto & \begin{cases} t & \text{si } t \in [0;1[, \\ 2-t & \text{si } t \in [1;2[, \end{cases} \end{array}$$
de support le segment $[0;1]$: le point 0 est l'unique point simple de la courbe C_η paramétrée par η et tous les autres points de C_η sont doubles.

Remarque 4.3.3.

- Si $\gamma(t_0)$ n'est pas un point simple de la courbe C_γ (paramétrée par γ), C_γ possède une "auto-intersection" en $\gamma(t_0)$.

- Si $\eta : J \to \mathbb{R}^d$ est une reparamétrisation de C_γ donnée par un homéomorphisme $\sigma : J \to I$, la multiplicité du point $\gamma(t_0) = \eta\left(\sigma^{-1}(t_0)\right)$ de $C_\gamma = C_\eta$ paramétrée par η est la même que la multiplicité du point $\gamma(t_0)$ de C_γ paramétrée par γ : on a
$$\begin{array}{rcl} \left\{s \in J \mid \eta(s) = \eta\left(\sigma^{-1}(t_0)\right)\right\} & = & \left\{s \in \sigma^{-1}(I) \mid \eta(s) = \eta\left(\sigma^{-1}(t_0)\right)\right\} \\ & = & \sigma^{-1}\left(\left\{t \in I \mid \eta\left(\sigma^{-1}(t)\right) = \eta\left(\sigma^{-1}(t_0)\right)\right\}\right) \\ & = & \sigma^{-1}\left(\{t \in I \mid \gamma(t) = \gamma(t_0)\}\right) \end{array}$$
et σ^{-1} est une bijection de I sur J.

La courbe paramétrée γ sera dite simple si pour tout $t \in I$, $\gamma(t)$ est un point simple de la courbe C_γ paramétrée par γ, i.e. si γ est une application injective, et dans ce cas, par la remarque précédente, toute reparamétrisation de C_γ est également simple.

Remarque 4.3.4. Si $f : I \to \mathbb{R}$ est une fonction de classe $\mathcal{C}^k$ sur l'intervalle I, l'application

$$\begin{array}{ccc} I & \to & \mathbb{R} \\ t & \mapsto & (t, f(t)) \end{array}$$

est une courbe paramétrée plane de classe $\mathcal{C}^k$ simple, dont le support est le *graphe* de la fonction f.

4.4 Tangence

Reprenons les notations de la section précédente. Nous allons considérer des notions de *vecteur tangent* et de *droite tangente* à la courbe paramétrée γ en t_0. Nous ne définirons ces notions qu'en des points "localement simples" :

Définition 4.4.1. *On suppose qu'il existe un intervalle ouvert J de $\mathbb{R}$ contenant t_0 tel que pour tout $t \in (I \cap J)\backslash\{t_0\}$, $\gamma(t) \neq \gamma(t_0)$ (i.e. tel que le point $\gamma(t_0)$ est un point simple de la courbe $C_{\gamma_{|I\cap J}}$). Soit ensuite v un vecteur non nul de $\mathbb{R}^d$. On dit que le vecteur v est tangent à la courbe paramétrée γ en t_0 si le vecteur unitaire $\frac{v}{\|v\|}$ est à la limite, quand $t \in (I \cap J)\backslash\{t_0\}$ tend vers t_0, de la suite des vecteurs directeurs unitaires des droites passant par les points $\gamma(t_0)$ et $\gamma(t)$, précisément si*

$$\frac{\gamma(t)-\gamma(t_0)}{\|\gamma(t)-\gamma(t_0)\|} \xrightarrow[t\in I\cap J\cap]-\infty,t_0[,\ t\to t_0} \pm\frac{v}{\|v\|} \quad \text{et} \quad \frac{\gamma(t)-\gamma(t_0)}{\|\gamma(t)-\gamma(t_0)\|} \xrightarrow[t\in I\cap J\cap]t_0,+\infty[,\ t\to t_0} \pm\frac{v}{\|v\|}.$$

Remarque 4.4.2. Un vecteur tangent à une courbe paramétrée est, par définition, non nul.

Supposons donc qu'il existe un intervalle ouvert J de $\mathbb{R}$ contenant t_0 tel que le point $\gamma(t_0)$ est un point simple de la courbe $C_{\gamma_{|I\cap J}}$. Commençons par remarquer que si u et v sont deux vecteurs tangents à γ en t_0, alors u et v sont nécessairement colinéaires : on a $\frac{v}{\|v\|} = \pm\frac{u}{\|u\|}$.

Si γ possède un vecteur tangent v en t_0, on définit ainsi *la* droite tangente à γ en t_0 comme étant la droite affine de direction v passant par $\gamma(t_0)$.

Exemple 4.4.3. 1. Si γ est la courbe paramétrée plane $\mathbb{R} \to \mathbb{R}^2$; $t \mapsto (t, t^2)$ (de support la parabole d'équation $y = x^2$ dans $\mathbb{R}^2$), on a, si $t \in \mathbb{R}^*$,

$$\frac{\gamma(t)-\gamma(0)}{\|\gamma(t)-\gamma(0)\|} = \frac{1}{\sqrt{t^2+t^4}}(t,t^2) = \frac{1}{|t|\sqrt{1+t^2}}(t,t^2) = \frac{1}{\sqrt{1+t^2}}(\mathrm{sgn}(t),|t|),$$

où $\mathrm{sgn}(t) := \begin{cases} 1 & \text{si } t > 0, \\ -1 & \text{si } t < 0, \end{cases}$ et donc

$$\frac{\gamma(t)-\gamma(0)}{\|\gamma(t)-\gamma(0)\|} \xrightarrow[t\to 0,\ t>0]{} (1,0) \quad \text{et} \quad \frac{\gamma(t)-\gamma(0)}{\|\gamma(t)-\gamma(0)\|} \xrightarrow[t\to 0,\ t<0]{} (-1,0).$$

Ainsi, le vecteur $(1, 0)$ est tangent à la courbe paramétrée γ en 0 et la droite tangente à γ en 0 est la droite d'équation $y = 0$ ($\gamma(0) = (0, 0)$).

2. Si maintenant γ est la courbe paramétrée $\mathbb{R} \to \mathbb{R}^2$; $t \mapsto (t^2, t^3)$ (de support la courbe cuspidale d'équation $y^2 = x^3$ dans $\mathbb{R}^2$), on a, si $t \in \mathbb{R}^*$,
$$\frac{\gamma(t)-\gamma(0)}{\|\gamma(t)-\gamma(0)\|} = \frac{1}{\sqrt{t^4+t^6}}(t^2,t^3) = \frac{1}{t^2\sqrt{1+t^2}}(t^2,t^3) = \frac{1}{\sqrt{1+t^2}}(1,t) \xrightarrow[t\to 0,\ t\neq 0]{} (1,0)$$
et le vecteur tangent $(1,0)$ est donc tangent γ en 0.

3. Si γ est la courbe paramétrée $\mathbb{R} \to \mathbb{R}^2$; $t \mapsto (t, |t|)$, γ ne possède pas de vecteur tangent en 0 : en effet, si $t \neq 0$, on a
$$\frac{\gamma(t)-\gamma(0)}{\|\gamma(t)-\gamma(0)\|} = \frac{1}{\sqrt{t^2+t^2}}(t,|t|) = \frac{1}{|t|\sqrt{2}}(t,|t|) = \frac{1}{\sqrt{2}}(\mathrm{sgn}(t),1)$$
et donc
$$\frac{\gamma(t)-\gamma(0)}{\|\gamma(t)-\gamma(0)\|} \xrightarrow[t\to 0,\ t>0]{} \frac{1}{\sqrt{2}}(1,1) \quad \text{et} \quad \frac{\gamma(t)-\gamma(0)}{\|\gamma(t)-\gamma(0)\|} \xrightarrow[t\to 0,\ t<0]{} \frac{1}{\sqrt{2}}(-1,1),$$
mais les vecteurs $\frac{1}{\sqrt{2}}(1,1)$ et $\frac{1}{\sqrt{2}}(-1,1)$ ne sont pas colinéaires.

4. Si enfin γ est la courbe paramétrée
$$\begin{array}{ccc} \mathbb{R} & \to & \mathbb{R}^2 \\ t & \mapsto & \begin{cases} \left(t^4\cos\left(\frac{1}{t}\right), t^4\sin\left(\frac{1}{t}\right)\right) & \text{si } t \neq 0, \\ (0,0) & \text{si } t = 0, \end{cases} \end{array}$$
γ est de classe $\mathcal{C}^1$ et γ ne possède pas de vecteur tangent en 0 (cf. feuille de TD 4).

Par définition, la courbe paramétrée γ possède un vecteur tangent en t_0 si et seulement si la quantité $\dfrac{\gamma(t)-\gamma(t_0)}{\|\gamma(t)-\gamma(t_0)\|}$, $t \in (I \cap J)\backslash\{t_0\}$, possède des limites à gauche et à droite en t_0 qui ne diffèrent que d'un scalaire ± 1. Si γ est dérivable en t_0, on a une condition *suffisante* d'existence d'un vecteur tangent (et donc d'une droite tangente) en t_0 plus "simple" :

Proposition 4.4.4. *On suppose que γ est dérivable en t_0. Si $\gamma'(t_0) \neq \overrightarrow{0}$ (où $\overrightarrow{0}$ désigne le vecteur nul de $\mathbb{R}^d$), alors $\gamma'(t_0)$ est un vecteur tangent à γ en t_0.*

Démonstration. Comme γ est dérivable en t_0, d'après le théorème de Taylor-Young, il existe une fonction $\epsilon : I \cap J \to \mathbb{R}^d$ telle que $\epsilon(t) \xrightarrow[t\to t_0]{} \overrightarrow{0}$ et, pour tout $t \in I \cap J$,
$$\gamma(t) = \gamma(t_0) + \gamma'(t_0)(t-t_0) + (t-t_0)\epsilon(t).$$
Soit $t \in I \cap J$, on a donc $\gamma(t) - \gamma(t_0) = (t-t_0)\big(\gamma'(t_0) + \epsilon(t)\big)$ et, si $t > t_0$,
$$\frac{\gamma(t)-\gamma(t_0)}{\|\gamma(t)-\gamma(t_0)\|} = \frac{(t-t_0)(\gamma'(t_0)+\epsilon(t))}{|t-t_0|\,\|\gamma'(t_0)+\epsilon(t)\|} = \frac{\gamma'(t_0)+\epsilon(t)}{\|\gamma'(t_0)+\epsilon(t)\|} \xrightarrow[t\in I\cap J\cap]t_0,+\infty[,\ t\to t_0]{} \frac{\gamma'(t_0)}{\|\gamma'(t_0)\|},$$
et, si $t < t_0$,
$$\frac{\gamma(t)-\gamma(t_0)}{\|\gamma(t)-\gamma(t_0)\|} = \frac{(t-t_0)(\gamma'(t_0)+\epsilon(t))}{|t-t_0|\,\|\gamma'(t_0)+\epsilon(t)\|} = -\frac{\gamma'(t_0)+\epsilon(t)}{\|\gamma'(t_0)+\epsilon(t)\|} \xrightarrow[t\in I\cap J\cap]-\infty,t_0[,\ t\to t_0]{} -\frac{\gamma'(t_0)}{\|\gamma'(t_0)\|}.$$
□

Exemple 4.4.5. 1. Si γ est la paramétrisation $[0,2\pi[\to \mathbb{R}^2$; $\theta \mapsto (\cos(\theta),\sin(\theta))$ du cercle unité de $\mathbb{R}^2$ et si $\theta \in [0,2\pi[$, on a

$$\gamma'(\theta) = (-\sin(\theta),\cos(\theta)) \neq \overrightarrow{0}$$

et $(-\sin(\theta),\cos(\theta))$ est donc un vecteur tangent à γ en θ. La droite tangente à γ en θ est la droite d'équation de direction le vecteur $(-\sin(\theta),\cos(\theta))$ et passant par le point $(\cos(\theta),\sin(\theta))$ i.e. la droite d'équation

$$-\sin(\theta)(y-\sin(\theta)) - \cos(\theta)(x-\cos(\theta)) = 0 \iff \sin(\theta)y + \cos(\theta)x = 1$$

dans $\mathbb{R}^2$.

2. Si γ est la paramétrisation

$$\begin{array}{ccc} [0,2\pi[& \to & \mathbb{R} \\ \theta & \mapsto & \left(\frac{\cos(\theta)}{1+\sin^2(\theta)}, \frac{\sin(\theta)\cos(\theta)}{1+\sin^2(\theta)}\right) \end{array}$$

du lemniscate de Bernoulli, on a, si $\theta \in [0,2\pi[$,

$$\gamma'(\theta) = \left(\frac{-\sin(\theta)(1+\sin^2(\theta)) - \cos(\theta)(2\cos(\theta)\sin(\theta))}{(1+\sin^2(\theta))^2}, \frac{(\cos^2(\theta)-\sin^2(\theta))(1+\sin^2(\theta)) - \sin(\theta)\cos(\theta)(2\cos(\theta)\sin(\theta))}{(1+\sin^2(\theta))^2}\right)$$

et donc $\gamma'\left(\frac{\pi}{2}\right) = \left(-\frac{1}{2},-\frac{1}{2}\right)$ et $\gamma'\left(\frac{3\pi}{2}\right) = \left(\frac{1}{2},-\frac{1}{2}\right)$.

La droite tangente à γ en $\frac{\pi}{2}$ est donc la droite d'équation $y = x$ dans $\mathbb{R}^2$ et la droite tangente à γ en $\frac{3\pi}{2}$ est donc la droite d'équation $y = -x$ dans $\mathbb{R}^2$ ($\gamma\left(\frac{\pi}{2}\right) = \gamma\left(\frac{3\pi}{2}\right) = (0,0)$).

Remarque 4.4.6. Si γ est dérivable en t_0 et $\gamma'(t_0) \neq \overrightarrow{0}$, le vecteur unitaire $\frac{\gamma'(t_0)}{\|\gamma'(t_0)\|}$ correspond à la "direction instantanée" en t_0 du parcours de C_γ par γ, et la quantité $\|\gamma'(t_0)\|$ correspond à la "vitesse instantanée" (absolue) en t_0.

On suppose dans la suite de la section que γ est dérivable en 0.

Définition 4.4.7. *Si $\gamma'(t_0) \neq \overrightarrow{0}$, on dit que la courbe paramétrée γ est régulière en t_0. Si $\gamma'(t_0) = \overrightarrow{0}$, on dit que γ est singulière en t_0. Si γ est régulière en tout point de I, on dit que γ est une courbe paramétrée régulière.*

Exemple 4.4.8. Les deux courbes paramétrées de l'exemple 4.4.5 sont régulières.

Remarque 4.4.9.
- D'après la proposition 4.4.4, si γ est régulière en t_0, alors γ possède un vecteur tangent (et donc une droite tangente) en t_0. La réciproque de cette assertion est cependant fausse : par exemple, dans le deuxième exemple de l'exemple 4.4.3, γ possède un vecteur tangent en 0 alors que $\gamma'(0) = (0,0)$.
- Si $\eta : \widetilde{I} \to \mathbb{R}^d$ est une courbe $\mathcal{C}^1$-équivalente à γ et si γ est régulière, alors η est également régulière. En effet, si $\sigma : \widetilde{I} \to I$ est un difféomorphisme tel que $\gamma \circ \sigma = \eta$ alors, pour $s \in \widetilde{I}$,

$$\eta'(s) = (\gamma\circ\sigma)'(s) = \sigma'(s)\cdot\gamma'(\sigma(s)) \neq \overrightarrow{0}$$

(car pour tout $t \in I$, $\gamma'(t) \neq \overrightarrow{0}$ par hypothèse, et pour tout $s \in \widetilde{I}$, $\sigma'(s) \neq 0$ car σ est un difféomorphisme). Remarquons également que la reparamétrisation η de C_γ modifie, du scalaire multiplicatif $|\sigma'(s)|$, la "vitesse instantanée" en $\gamma(\sigma(s))$ et, si $\sigma'(s)$ est négatif, renverse la "direction instantanée" en $\gamma(\sigma(s))$.

Plus "généralement", si l'une des dérivées de γ ne s'annule pas en t_0, γ possède un vecteur tangent en t_0 :

Proposition 4.4.10. *Soit $k \in \mathbb{N}\backslash\{0\}$ tel que γ est de classe $\mathcal{C}^k$ sur $I \cap J$ et tel que pour tout $i \in \{0, \ldots, k-1\}$, $\gamma^{(i)}(t_0) = \overrightarrow{0}$ et $\gamma^{(k)}(t_0) \neq \overrightarrow{0}$. Alors $\gamma^{(k)}(t_0)$ est un vecteur tangent à γ en t_0.*

Démonstration. Comme γ est de classe $\mathcal{C}^k$ sur $I \cap J$, par le théorème de Taylor-Young, il existe une fonction $\epsilon : I \cap J \to \mathbb{R}^d$ telle que $\epsilon(t) \xrightarrow[t \to t_0]{} \overrightarrow{0}$ et telle que, pour tout $t \in I \cap J$,

$$\gamma(t) = \gamma(t_0) + \gamma'(t_0)(t-t_0) + \cdots + \frac{\gamma^{(k)}(t_0)}{k!}(t-t_0)^k + (t-t_0)^k\epsilon(t) = \gamma(t_0) + \frac{\gamma^{(k)}(t_0)}{k!}(t-t_0)^k + (t-t_0)^k\epsilon(t)$$

(car pour tout $i \in \{0, \ldots, k-1\}$, $\gamma^{(i)}(t_0) = 0$). Ainsi,

$$\begin{aligned}\frac{\gamma(t)-\gamma(t_0)}{\|\gamma(t)-\gamma(t_0)\|} &= \frac{\frac{\gamma^{(k)}(t_0)}{k!}(t-t_0)^k + (t-t_0)^k\epsilon(t)}{\left\|\frac{\gamma^{(k)}(t_0)}{k!}(t-t_0)^k + (t-t_0)^k\epsilon(t)\right\|} \\ &= \operatorname{sgn}(t-t_0)^k \frac{\gamma^{(k)}(t_0) + k!\epsilon(t)}{\left\|\gamma^{(k)}(t_0) + k!\epsilon(t)\right\|}\end{aligned}$$

et donc, si $t > t_0$,

$$\frac{\gamma(t)-\gamma(t_0)}{\|\gamma(t)-\gamma(t_0)\|} \xrightarrow[t \in I \cap J \cap]t_0, +\infty[,\ t \to t_0]{} \frac{\gamma^{(k)}(t_0)}{\left\|\gamma^{(k)}(t_0)\right\|},$$

et si $t < t_0$,

$$\frac{\gamma(t)-\gamma(t_0)}{\|\gamma(t)-\gamma(t_0)\|} \xrightarrow[t \in I \cap J \cap]-\infty, t_0[,\ t \to t_0]{} (-1)^k \frac{\gamma^{(k)}(t_0)}{\left\|\gamma^{(k)}(t_0)\right\|}.$$

□

Remarque 4.4.11. Même si γ est de classe $\mathcal{C}^\infty$ et si pour tout $k \in \mathbb{N}$, $\gamma^{(k)}(t_0) = \overrightarrow{0}$, γ peut posséder une droite tangente en x_0 : la courbe paramétrée

$$\eta : \begin{array}{ccc} [0, +\infty[& \to & \mathbb{R} \\ t & \mapsto & \begin{cases} e^{-\frac{1}{t}} & \text{si } t > 0, \\ 0 & \text{si } t = 0, \end{cases} \end{array}$$

dans $\mathbb{R}$ est de classe $\mathcal{C}^\infty$ et pour tout $k \in \mathbb{N}$, $\eta^{(k)}(0) = 0$, bien que, si $t \in]0, +\infty[$,

$$\frac{\eta(t)-\eta(0)}{|\eta(t)-\eta(0)|} = \frac{e^{-\frac{1}{t}}}{e^{-\frac{1}{t}}} = 1.$$

On fait un petit aparté sur une étude du comportement local des courbes planes par rapport à leurs droites tangentes.

4.5 Une étude du comportement local des courbes planes

Soit donc $\gamma : I \to \mathbb{R}^2$ une courbe paramétrée plane. Soit ensuite $t_0 \in I$ tel qu'il existe un intervalle ouvert J de $\mathbb{R}$ contenant t_0 tel que le point $\gamma(t_0)$ soit un point simple de la courbe $C_{\gamma_{|I\cap J}}$.

On suppose de plus que

- γ est de classe $\mathcal{C}^N$, $N \in \mathbb{N}\backslash\{0\}$,
- il existe $q \in \{1, \ldots, N-1\}$ tel que $\gamma^{(q)}(t_0) \neq \overrightarrow{0}$ et pour tout $i \in \{1, \ldots, q-1\}$, $\gamma^{(i)}(t_0) = \overrightarrow{0}$ ($\gamma^{(q)}(t_0)$ est donc un vecteur tangent à γ en t_0 d'après la proposition 4.4.10),
- il existe $r \in \{q+1, \ldots, N\}$ tel que $\gamma^{(r)}(t_0) \notin \text{Vect}\left\{\gamma^{(q)}(t_0)\right\}$ et pour tout $i \in \{q+1, \ldots, r-1\}$, $\gamma^{(i)}(t_0) \in \text{Vect}\left\{\gamma^{(q)}(t_0)\right\}$.

D'après le théorème de Taylor-Young, il existe une fonction $\epsilon : I \cap J \to \mathbb{R}^2$ telle que $\epsilon(t) \xrightarrow[t\to t_0]{} \overrightarrow{0}$ et telle que, pour tout $t \in I \cap J$,

$$\gamma(t) = \gamma(t_0)+\gamma^{(q)}(t_0)\frac{(t-t_0)^q}{q!}+\gamma^{(q+1)}(t_0)\frac{(t-t_0)^{q+1}}{(q+1)!}+\cdots+\gamma^{(r-1)}(t_0)\frac{(t-t_0)^{r-1}}{(r-1)!}+\gamma^{(r)}(t_0)\frac{(t-t_0)^r}{r!}+(t-t_0)^r\epsilon(t)$$

Or, pour tout $i \in \{q+1, \ldots, r-1\}$, $\gamma^{(i)}(t_0) \in \text{Vect}\left\{\gamma^{(q)}(t_0)\right\}$. Ainsi, pour tout $i \in \{q+1, \ldots, r-1\}$, il existe $\mu_i \in \mathbb{R}$ tel que, pour tout $t \in I \cap J$,

$$\gamma(t)-\gamma(t_0) = \gamma^{(q)}(t_0)\frac{(t-t_0)^q}{q!}\left(1+\mu_{q+1}(t-t_0)+\ldots+\mu_{r-1}(t-t_0)^{r-1-q}\right)+\gamma^{(r)}(t_0)\frac{(t-t_0)^r}{r!}+(t-t_0)^r\epsilon(t).$$

Si, pour $t \in I \cap J$, $\begin{pmatrix}\epsilon_1(t)\\ \epsilon_2(t)\end{pmatrix}$ désigne le vecteur des coordonnées de $\epsilon(t)$ dans la base $\left\{\gamma^{(q)}(t_0), \gamma^{(r)}(t_0)\right\}$ de $\mathbb{R}^2$, on a alors, dans la base $\left\{\gamma^{(q)}(t_0), \gamma^{(r)}(t_0)\right\}$ de $\mathbb{R}^2$,

$$\begin{aligned}\overrightarrow{\gamma(t_0)\gamma(t)} &= \begin{pmatrix}\frac{(t-t_0)^q}{q!}\left(1+\mu_{q+1}(t-t_0)+\ldots+\mu_{r-1}(t-t_0)^{r-1-q}\right)+(t-t_0)^r\epsilon_1(t)\\ \frac{(t-t_0)^r}{r!}+(t-t_0)^r\epsilon_2(t)\end{pmatrix}\\ &\underset{t\to t_0}{\sim} \begin{pmatrix}\frac{(t-t_0)^q}{q!}\\ \frac{(t-t_0)^r}{r!}\end{pmatrix}\end{aligned}$$

Au voisinage de t_0, quatre types de comportements se présentent alors :

- si q est impair et r est pair, la quantité $(t-t_0)^q$ est négative "à gauche" de t_0, positive "à droite" de t_0, et la quantité $(t-t_0)^r$ est positive : au voisinage de t_0 (ou plutôt de $\gamma(t_0)$), la courbe $C_{\gamma_{|I\cap J}}$ "traverse" donc le vecteur $\gamma^{(r)}(t_0)$ (ou plutôt la droite de direction $\gamma^{(r)}(t_0)$ passant par $\gamma(t_0)$) mais pas le vecteur tangent $\gamma^{(q)}(t_0)$ (ou plutôt la droite de direction $\gamma^{(q)}(t_0)$ passant par $\gamma(t_0)$), et on dit que t_0 est un point ordinaire de γ,
- si q est impair et r est impair, les deux quantités $(t-t_0)^q$ et $(t-t_0)^r$ sont négatives à gauche de t_0 et positives à droite : au voisinage de $\gamma(t_0)$, la courbe $C_{\gamma_{|I\cap J}}$ traverse donc les deux vecteurs $\gamma^{(q)}(t_0)$ et $\gamma^{(r)}(t_0)$, et on dit que t_0 est un point d'inflexion de γ,

- si q est pair et r est impair, la courbe $C_{\gamma_{|I\cap J}}$ traverse le vecteur tangent $\gamma^{(q)}(t_0)$ au voisinage de $\gamma(t_0)$ mais pas $\gamma^{(r)}(t_0)$, et on dit que t_0 est un point de rebroussement de première espèce de γ,

- si q est pair et r est pair, la courbe $C_{\gamma_{|I\cap J}}$ ne traverse aucun des vecteurs $\gamma^{(q)}(t_0)$ et $\gamma^{(r)}(t_0)$, et on dit que t_0 est un point de rebroussement de deuxième espèce de γ.

Exemple 4.5.1.
- La courbe paramétrée plane $\eta : \mathbb{R} \to \mathbb{R}^2 \ ; \ t \mapsto (t, t^2)$ possède un point ordinaire en 0 (on a ici $q = 1$, $r = 2$ et $\eta'(0) = (1, 0)$, $\eta^{(2)}(0) = (0, 2)$).

- La courbe paramétrée plane $\eta : \mathbb{R} \to \mathbb{R}^2 \ ; \ t \mapsto (t, t^3)$ possède un point d'inflexion en 0 (on a ici $q = 1$, $r = 3$ et $\eta'(0) = (1, 0)$, $\eta^{(3)}(0) = (0, 6)$).

- La courbe paramétrée plane $\eta : \mathbb{R} \to \mathbb{R}^2 \ ; \ t \mapsto (t^2, t^3)$ possède un point de rebroussement de première espèce en 0 (on a ici $q = 2$, $r = 3$ et $\eta^{(2)}(0) = (2, 0)$, $\eta^{(3)}(0) = (0, 6)$).

- La courbe paramétrée plane $\eta : \mathbb{R} \to \mathbb{R}^2 \ ; \ t \mapsto (t^2, t^4)$ possède un point de rebroussement de deuxième espèce en 0 (on a ici $q = 2$, $r = 4$ et $\eta^{(2)}(0) = (2, 0)$, $\eta^{(4)}(0) = (0, 24)$).

4.6 Longueur d'une courbe paramétrée

Soit $\gamma : I \to \mathbb{R}^d$ une courbe paramétrée de $\mathbb{R}^d$. Nous allons définir une notion de *longueur* de la courbe paramétrée γ. Une idée naturelle est de chercher à approcher la courbe C_γ, support de γ, par des segments, et la "longueur" de C_γ par la somme des longueurs de ces segments. Cela nous mène à la définition qui suit, qui utilise la notion de *subdivision* de l'intervalle I : une subdivision de I est un uplet $(t_0, \dots, t_n)$, $n \in \mathbb{N}\backslash\{0\}$, de points de I tels que $t_0 < t_1 < \cdots < t_n$. On note Σ_I l'ensemble des subdivisions de I.

Définition 4.6.1. *On dit que la courbe paramétrée γ est rectifiable si le supremum*

$$\sup_{(t_0,\dots,t_n)\in\Sigma_I,\ n\in\mathbb{N}\backslash\{0\}} \sum_{i=0}^{n-1} \|\gamma(t_{i+1}) - \gamma(t_i)\|$$

est fini, et, dans ce cas, on note $L(\gamma)$ cette quantité que l'on appelle longueur de la courbe paramétrée γ.

Remarque 4.6.2.
- Si $(t_0, \dots, t_n)$, $n \in \mathbb{N}\backslash\{0\}$, est une subdivision de I, la quantité $\sum_{i=0}^{n-1} \|\gamma(t_{i+1}) - \gamma(t_i)\|$ est la longueur de la ligne brisée reliant les points $\gamma(t_0), \dots, \gamma(t_n)$ de C_γ.

- Si γ est rectifiable, la longueur $L(\gamma)$ est positive ou nulle.

- Si I est réduit à un point, γ est rectifiable et $L(\gamma) = 0$.

Avant de donner une condition suffisante de rectifiabilité dans le cas où I est un segment, exhibons quelques propriétés à partir de la seule définition ci-dessus :

Lemme 4.6.3. *On suppose que la courbe paramétrée γ est rectifiable. Alors :*

1. *si J est un intervalle de $\mathbb{R}$ contenu dans I, la courbe paramétrée restreinte $\gamma_{|J} : J \to \mathbb{R}^d$ est rectifiable et $L(\gamma) \geqslant L\left(\gamma_{|J}\right)$,*
2. *si $c \in I$, $L(\gamma) = L\left(\gamma_{|I\cap]-\infty;c]}\right) + L\left(\gamma_{|I\cap[c;+\infty[}\right)$,*
3. *si $a, b \in I$, $L(\gamma) \geqslant \|\gamma(b) - \gamma(a)\|$.*

Démonstration. 1. Soit J un intervalle de $\mathbb{R}$ contenu dans I et soit $(s_0, \ldots, s_m)$, $m \in \mathbb{N}\backslash\{0\}$, une subdivision de J. Alors $(s_0, \ldots, s_m)$ est également une subdivsion de I car $J \subset I$. Ainsi

$$\begin{aligned}\sum_{j=0}^{m-1} \left\|\gamma_{|J}(s_{j+1}) - \gamma_{|J}(s_j)\right\| &= \sum_{j=0}^{m-1} \|\gamma(s_{j+1}) - \gamma(s_j)\| \\ &\leqslant \sup_{(t_0,\ldots,t_n)\in\Sigma_I,\ n\in\mathbb{N}\backslash\{0\}} \sum_{i=0}^{n-1} \|\gamma(t_{i+1}) - \gamma(t_i)\| \\ &= L(\gamma)\end{aligned}$$

et donc

$$\sup_{(s_0,\ldots,s_m)\in\Sigma_J,\ m\in\mathbb{N}\backslash\{0\}} \sum_{j=0}^{m-1} \|\gamma(s_{j+1}) - \gamma(s_j)\| \leqslant L(\gamma) :$$

en particulier, la courbe paramétrée $\gamma_{|J} : J \to \mathbb{R}^d$ est rectifiable et

$$L\left(\gamma_{|J}\right) = \sup_{(s_0,\ldots,s_m)\in\Sigma_J,\ m\in\mathbb{N}\backslash\{0\}} \sum_{j=0}^{m-1} \|\gamma(s_{j+1}) - \gamma(s_j)\| \leqslant L(\gamma).$$

2. Remarquons tout d'abord que, par ce que nous venons de démontrer, les courbes paramétrées $\gamma_{|I\cap]-\infty;c]}$ et $\gamma_{|I\cap[c;+\infty[}$ sont rectifiables.

   Nous allons tout d'abord montrer que $L(\gamma) \leqslant L\left(\gamma_{|I\cap]-\infty;c]}\right) + L\left(\gamma_{|I\cap[c;+\infty[}\right)$. Soit donc $(t_0, \ldots, t_n)$, $n \in \mathbb{N}\backslash\{0\}$, une subdivision de I. On suppose tout d'abord qu'il existe $i \in \{0, \ldots, n-1\}$ tel que $c \in [t_i, t_{i+1}]$:

   - si $c = t_i$, alors $(t_0, \ldots, t_{i-1}, c)$ est une subdivision de $I\cap]-\infty; c]$ et $(c, t_{i+1}, \ldots, t_n)$ est une subdivision de $I \cap [c; +\infty[$, et

   $$\begin{aligned}\sum_{i=0}^{n-1} \|\gamma(t_{i+1}) - \gamma(t_i)\| &= \sum_{k=0}^{i-1} \|\gamma(t_{k+1}) - \gamma(t_k)\| + \|\gamma(t_{i+1}) - \gamma(c)\| + \sum_{j=i+1}^{n-1} \|\gamma(t_{j+1}) - \gamma(t_j)\| \\ &\leqslant L\left(\gamma_{|I\cap]-\infty;c]}\right) + L\left(\gamma_{|I\cap[c;+\infty[}\right),\end{aligned}$$

   - si $c = t_{i+1}$, alors $(t_0, \ldots, t_i, c)$ est une subdivision de $I\cap]-\infty; c]$ et $(c, t_{i+2}, \ldots, t_n)$ est une subdivision de $I \cap [c; +\infty[$, et

   $$\begin{aligned}\sum_{i=0}^{n-1} \|\gamma(t_{i+1}) - \gamma(t_i)\| &= \sum_{k=0}^{i-1} \|\gamma(t_{k+1}) - \gamma(t_k)\| + \|\gamma(c) - \gamma(t_i)\| + \sum_{j=i+1}^{n-1} \|\gamma(t_{j+1}) - \gamma(t_j)\| \\ &\leqslant L\left(\gamma_{|I\cap]-\infty;c]}\right) + L\left(\gamma_{|I\cap[c;+\infty[}\right),\end{aligned}$$

- si $c \in]t_i, t_{i+1}[$, alors $(t_0, \dots, t_i, c)$ est une subdivision de $I \cap]-\infty; c]$ et $(c, t_{i+1}, \dots, t_n)$ est une subdivision de $I \cap [c; +\infty[$, et

$$\begin{aligned}\sum_{i=0}^{n-1} \|\gamma(t_{i+1}) - \gamma(t_i)\| &= \sum_{k=0}^{i-1} \|\gamma(t_{k+1}) - \gamma(t_k)\| + \|\gamma(c) - \gamma(t_i)\| + \|\gamma(t_{i+1}) - \gamma(c)\| + \sum_{j=i+1}^{n-1} \|\gamma(t_{j+1}) - \gamma(t_j)\| \\ &\leqslant L\left(\gamma_{|I\cap]-\infty;c]}\right) + L\left(\gamma_{|I\cap[c;+\infty[}\right),\end{aligned}$$

Si maintenant $c < t_0$, alors $(t_0, \dots, t_n)$ est une subdivision de $I \cap [c; +\infty[$ et

$$\sum_{i=0}^{n-1} \|\gamma(t_{i+1}) - \gamma(t_i)\| \leqslant L\left(\gamma_{|I\cap[c;+\infty[}\right) \leqslant L\left(\gamma_{|I\cap]-\infty;c]}\right) + L\left(\gamma_{|I\cap[c;+\infty[}\right),$$

et si $c > t_n$, $(t_0, \dots, t_n)$ est une subdivision de $I \cap]-\infty; c]$ et

$$\sum_{i=0}^{n-1} \|\gamma(t_{i+1}) - \gamma(t_i)\| \leqslant L\left(\gamma_{|I\cap]-\infty;c]}\right) \leqslant L\left(\gamma_{|I\cap]-\infty;c]}\right) + L\left(\gamma_{|I\cap[c;+\infty[}\right).$$

Ainsi, dans tous les cas,

$$\sum_{i=0}^{n-1} \|\gamma(t_{i+1}) - \gamma(t_i)\| \leqslant L\left(\gamma_{|I\cap]-\infty;c]}\right) + L\left(\gamma_{|I\cap[c;+\infty[}\right)$$

et donc

$$L(\gamma) = \sup_{(t_0,\dots,t_n)\in\Sigma_I,\ n\in\mathbb{N}\setminus\{0\}} \sum_{i=0}^{n-1} \|\gamma(t_{i+1}) - \gamma(t_i)\| \leqslant L\left(\gamma_{|I\cap]-\infty;c]}\right) + L\left(\gamma_{|I\cap[c;+\infty[}\right).$$

Réciproquement, montrons que $L(\gamma) \geqslant L\left(\gamma_{|I\cap]-\infty;c]}\right) + L\left(\gamma_{|I\cap[c;+\infty[}\right)$. Soient $(s_0, \dots, s_m)$, $m \in \mathbb{N}\setminus\{0\}$, une subdivision de $I \cap]-\infty; c]$ et $(r_0, \dots, r_l)$, $l \in \mathbb{N}\setminus\{0\}$, une subdivision de $I \cap [c; +\infty[$.

- Si $s_m = r_0 = c$, l'uplet $(s_0, \dots, s_m, r_1, \dots, r_l)$ est une subdivision de I et on a donc

$$\sum_{k=0}^{m-1} \|\gamma(s_{k+1}) - \gamma(s_k)\| + \sum_{j=0}^{l-1} \|\gamma(r_{j+1}) - \gamma(r_j)\| \leqslant \sup_{(t_0,\dots,t_n)\in\Sigma_I,\ n\in\mathbb{N}\setminus\{0\}} \sum_{i=0}^{n-1} \|\gamma(t_{i+1}) - \gamma(t_i)\| = L(\gamma).$$

- Si $s_m < r_0$, l'uplet $(s_0, \dots, s_m, r_0, \dots, r_l)$ est une subdivision de I et on a

$$\begin{aligned}\sum_{k=0}^{m-1} \|\gamma(s_{k+1}) - \gamma(s_k)\| + \sum_{j=0}^{l-1} \|\gamma(r_{j+1}) - \gamma(r_j)\| &\leqslant \sum_{k=0}^{m-1} \|\gamma(s_{k+1}) - \gamma(s_k)\| + \|\gamma(r_0) - \gamma(s_m)\| + \sum_{j=0}^{l-1} \|\gamma(r_{j+1}) - \gamma(r_j)\| \\ &\leqslant \sup_{(t_0,\dots,t_n)\in\Sigma_I,\ n\in\mathbb{N}\setminus\{0\}} \sum_{i=0}^{n-1} \|\gamma(t_{i+1}) - \gamma(t_i)\| \\ &= L(\gamma)\end{aligned}$$

Ainsi, dans tous les cas, on a

$$\sum_{k=0}^{m-1} \|\gamma(s_{k+1}) - \gamma(s_k)\| + \sum_{j=0}^{l-1} \|\gamma(r_{j+1}) - \gamma(r_j)\| \leqslant L(\gamma)$$

et donc

$$\sum_{k=0}^{m-1} \|\gamma(s_{k+1}) - \gamma(s_k)\| + \sup_{(r_0,\dots,r_l)\in\Sigma_{I\cap[c;+\infty[},\ l\in\mathbb{N}\setminus\{0\}} \sum_{j=0}^{l-1} \|\gamma(r_{j+1}) - \gamma(r_j)\| \leqslant L(\gamma)$$

i.e.

$$\sum_{k=0}^{m-1} \|\gamma(s_{k+1}) - \gamma(s_k)\| + L\left(\gamma_{|I\cap[c;+\infty[}\right) \leqslant L(\gamma),$$

puis

$$\sup_{(s_0,\dots,s_m)\in\Sigma_{I\cap]+\infty;c]},\ m\in\mathbb{N}\setminus\{0\}} \sum_{k=0}^{m-1} \|\gamma(s_{k+1}) - \gamma(s_k)\| + L\left(\gamma_{|I\cap[c;+\infty[}\right) \leqslant L(\gamma)$$

i.e.

$$L\left(\gamma_{|I\cap]-\infty;c]}\right) + L\left(\gamma_{|I\cap[c;+\infty[}\right) \leqslant L(\gamma).$$

3. Soient $a, b \in I$ et supposons sans perdre de généralité que $a < b$. Alors (a, b) est une subdivision de I et donc

$$\|\gamma(b) - \gamma(a)\| \leqslant \sup_{(t_0,\dots,t_n)\in\Sigma_I,\ n\in\mathbb{N}\setminus\{0\}} \sum_{i=0}^{n-1} \|\gamma(t_{i+1}) - \gamma(t_i)\| = L(\gamma).$$

□

Remarque 4.6.4. D'après la démonstration du point 2 du lemme précédent, si $c \in I$ est tel que les courbes paramétrées restreintes $\gamma_{|I\cap]-\infty;c]}$ et $\gamma_{|I\cap[c;+\infty[}$ sont rectifiables, alors γ est rectifiable.

Remarquons également que les notions de *rectifiabilité* et de *longueur* d'une courbe paramétrée est invariante par $\mathcal{C}^0$-équivalence :

Proposition 4.6.5. *Soit $\eta : J \to \mathbb{R}^d$ une courbe paramétrée $\mathcal{C}^0$-équivalente à γ. Alors γ est rectifiable si et seulement si η est rectifiable, et, dans ce cas, $L(\gamma) = L(\eta)$.*

Démonstration. Soit $\sigma : J \to I$ un homéomorphisme tel que $\gamma \circ \sigma = \eta$. En particulier, σ est une fonction strictement monotone.

Supposons alors que γ est rectifiable et soit $(s_0, \dots, s_m)$, $m \in \mathbb{N}\setminus\{0\}$, une subdivision de J. Si σ est une fonction strictement croissante, l'uplet $\big(\sigma(s_0), \dots, \sigma(s_m)\big)$ est une subdivision de

I et, si σ est strictement décroissante, $\big(\sigma(s_m),\dots,\sigma(s_0)\big)$ est une subdivision de I : dans tous les cas, on a

$$\begin{aligned}\sum_{j=0}^{m-1}\|\eta(s_{j+1})-\eta(s_j)\| &= \sum_{j=0}^{m-1}\big\|\gamma\big(\sigma(s_{j+1})\big)-\gamma\big(\sigma(s_j)\big)\big\| \\ &\leqslant \sup_{(t_0,\dots,t_n)\in\Sigma_I,\ n\in\mathbb{N}\setminus\{0\}}\sum_{i=0}^{n-1}\|\gamma(t_{i+1})-\gamma(t_i)\| \\ &\leqslant L(\gamma).\end{aligned}$$

Ainsi,

$$\sup_{(s_0,\dots,s_m)\in\Sigma_J,\ m\in\mathbb{N}\setminus\{0\}}\sum_{j=0}^{m-1}\|\eta(s_{j+1})-\eta(s_j)\|\leqslant L(\gamma):$$

la courbe paramétrée $\eta : J\to\mathbb{R}^d$ est donc rectifiable et $L(\eta)\leqslant L(\gamma)$.

En échangeant les rôles de γ et η (la relation de $\mathcal{C}^0$-équivalence est symétrique), on obtient que γ est rectifiable si η est rectifiable, qu'alors $L(\gamma)\leqslant L(\eta)$, et donc $L(\gamma)=L(\eta)$. □

Si I est un segment et γ est de classe $\mathcal{C}^1$, la courbe paramétrée γ est rectifiable et sa longueur est donnée par sa dérivée :

Théorème 4.6.6. *On suppose que I est un segment $[a,b]$ avec $a,b\in\mathbb{R}$ tels que $a<b$. Si γ est de classe $\mathcal{C}^1$ sur $I=[a,b]$, alors γ est rectifiable et*

$$L(\gamma)=\int_a^b\|\gamma'(t)\|\mathrm{d}t.$$

Démonstration. Soit $(t_0,\dots,t_n)$, $n\in\mathbb{N}\setminus\{0\}$, une subdivision de I. Si $i\in\{0,\dots,n-1\}$, on a $\displaystyle\int_{t_i}^{t_{i+1}}\gamma'(t)\mathrm{d}t=\gamma(t_{i+1})-\gamma(t_i)$ et donc

$$\|\gamma(t_{i+1})-\gamma(t_i)\|=\left\|\int_{t_i}^{t_{i+1}}\gamma'(t)\mathrm{d}t\right\|\leqslant\int_{t_i}^{t_{i+1}}\big\|\gamma'(t)\big\|\,\mathrm{d}t.$$

Ainsi

$$\sum_{i=0}^{n-1}\|\gamma(t_{i+1})-\gamma(t_i)\|\leqslant\sum_{i=0}^{n-1}\int_{t_i}^{t_{i+1}}\big\|\gamma'(t)\big\|\,\mathrm{d}t=\int_{t_0}^{t_n}\big\|\gamma'(t)\big\|\,\mathrm{d}t\leqslant\int_a^b\big\|\gamma'(t)\big\|\,\mathrm{d}t$$

et donc

$$\sup_{(t_0,\dots,t_n)\in\Sigma_I,\ n\in\mathbb{N}\setminus\{0\}}\sum_{i=0}^{n-1}\|\gamma(t_{i+1})-\gamma(t_i)\|\leqslant\int_a^b\big\|\gamma'(t)\big\|\,\mathrm{d}t:$$

la courbe paramétrée γ est donc rectifiable et $L(\gamma)\leqslant\displaystyle\int_a^b\big\|\gamma'(t)\big\|\,\mathrm{d}t$.

Nous allons ensuite montrer l'égalité $L(\gamma) = \displaystyle\int_a^b \left\|\gamma'(t)\right\| \mathrm{d}t$. Pour cela, nous allons considérer la fonction

$$\phi : \begin{array}{ccc} [a,b] & \to & [0;+\infty[\\ t & \mapsto & L(\gamma_{|[a,t]}) \end{array}$$

(par le lemme 4.6.3 1., pour tout $t \in [a,b]$, la courbe restreinte $\gamma_{|[a,t]}$ est rectifiable) et montrer que, pour tout $t \in [a,b]$, $\phi(t) = \displaystyle\int_a^t \left\|\gamma'(u)\right\| \mathrm{d}u$: en particulier, $L(\gamma) = \phi(b) = \displaystyle\int_a^b \left\|\gamma'(u)\right\| \mathrm{d}u$.

La preuve va en grande partie consister à montrer que la fonction ϕ est dérivable et que, pour tout $t \in [a,b]$, $\phi'(t) = \|\gamma'(t)\|$.

Soit donc $t \in [a,b]$ et soit $h \in \mathbb{R}\backslash\{0\}$ tel que $t+h \in [a,b]$. Si $h > 0$, on a

$$\begin{array}{rcl} \phi(t+h) - \phi(t) & = & L(\gamma_{|[a,t+h]}) - L(\gamma_{|[a,t]}) \\ & = & L(\gamma_{|[t,t+h]}) \text{ (par le lemme 4.6.3 2.)} \\ & \leqslant & \displaystyle\int_t^{t+h} \left\|\gamma'(u)\right\| \mathrm{d}u \text{ (par ce que l'on a montré plus haut)} \end{array}$$

et donc

$$\frac{\phi(t+h) - \phi(t)}{h} \leqslant \frac{1}{h} \int_t^{t+h} \left\|\gamma'(u)\right\| \mathrm{d}u.$$

Si $h < 0$, on obtient, de façon analogue, $\phi(t) - \phi(t+h) \leqslant \displaystyle\int_{t+h}^t \left\|\gamma'(u)\right\| \mathrm{d}u$ et donc

$$\frac{\phi(t) - \phi(t+h)}{-h} \leqslant \frac{1}{-h} \int_{t+h}^t \left\|\gamma'(u)\right\| \mathrm{d}u \quad \text{i.e.} \quad \frac{\phi(t+h) - \phi(t)}{h} \leqslant \frac{1}{h} \int_t^{t+h} \left\|\gamma'(u)\right\| \mathrm{d}u.$$

Par ailleurs, si $h > 0$,

$$\phi(t+h) - \phi(t) = L(\gamma_{|[t,t+h]}) \geqslant \|\gamma(t+h) - \gamma(t)\|$$

(par le lemme 4.6.3 3.) et donc

$$\frac{\phi(t+h) - \phi(t)}{h} \geqslant \frac{\|\gamma(t+h) - \gamma(t)\|}{h} = \left\|\frac{\gamma(t+h) - \gamma(t)}{h}\right\|.$$

Si $h < 0$, on a

$$\phi(t) - \phi(t+h) \geqslant \|\gamma(t) - \gamma(t+h)\|$$

donc

$$\frac{\phi(t+h) - \phi(t)}{h} = \frac{\phi(t) - \phi(t+h)}{-h} \geqslant \frac{\|\gamma(t) - \gamma(t+h)\|}{-h} = \left\|\frac{\gamma(t) - \gamma(t+h)}{-h}\right| = \left\|\frac{\gamma(t+h) - \gamma(t)}{h}\right\|.$$

Ainsi, dans tous les cas, on a l'encadrement

$$\left\|\frac{\gamma(t+h) - \gamma(t)}{h}\right\| \leqslant \frac{\phi(t+h) - \phi(t)}{h} \leqslant \frac{1}{h} \int_t^{t+h} \left\|\gamma'(u)\right\| \mathrm{d}u.$$

Or

$$\left\| \frac{\gamma(t+h)-\gamma(t)}{h} \right\| \xrightarrow[h\to 0]{} \|\gamma'(t)\|$$

(la fonction $\gamma : I \to \mathbb{R}^d$ est de classe $\mathcal{C}^1$ en particulier dérivable en t, et la norme $\|\cdot\| : \mathbb{R}^d \to [0;+\infty[$ est continue) et

$$\frac{1}{h}\int_t^{t+h} \|\gamma'(u)\| \,\mathrm{d}u = \frac{\displaystyle\int_a^{t+h} \|\gamma'(u)\| \,\mathrm{d}u - \int_a^t \|\gamma'(u)\| \,\mathrm{d}u}{h} \xrightarrow[h\to 0]{} \|\gamma'(t)\|$$

(par le théorème fondamental du calcul intégral) donc, par théorème d'encadrement,

$$\frac{\phi(t+h)-\phi(t)}{h} \xrightarrow[h\to 0]{} \|\gamma'(t)\|$$

i.e. ϕ est dérivable en t et $\phi'(t) = \|\gamma'(t)\|$.

Enfin,

$$\phi(t) - \phi(a) = \int_a^t \phi'(u)\mathrm{d}u = \int_a^t \|\gamma'(u)\|\mathrm{d}u$$

et $\phi(a) = L(\gamma_{|[a,a]}) = 0$, d'où

$$L(\gamma_{|[a,t]}) = \phi(t) = \int_a^t \|\gamma'(u)\|\mathrm{d}u.$$

En particulier,

$$L(\gamma) = L(\gamma_{|[a,b]}) = \int_a^b \|\gamma'(u)\|\mathrm{d}u.$$

□

Remarque 4.6.7. Il existe des courbes paramétrées continues sur des segments qui ne sont pas rectifiables.

Exemple 4.6.8. 1. Si γ est la courbe paramétrée $[-1;1] \to \mathbb{R}^2$; $t \mapsto (t^2, t^3)$, γ est de classe

$\mathcal{C}^1$ sur le segment $[-1;1]$ et

$$\begin{aligned}
L(\gamma) &= \int_{-1}^{1} \|\gamma'(t)\| \mathrm{d}t \\
&= \int_{-1}^{1} \sqrt{(2t)^2 + (3t^2)^2} \mathrm{d}t \\
&= \int_{-1}^{1} \sqrt{4t^2 + 9t^4} \mathrm{d}t \\
&= \int_{-1}^{1} |t| \sqrt{4 + 9t^2} \mathrm{d}t \\
&= \int_{0}^{1} t\sqrt{4 + 9t^2} \mathrm{d}t - \int_{-1}^{0} t\sqrt{4 + 9t^2} \mathrm{d}t \\
&= \int_{0}^{1} \frac{\sqrt{4 + 9u}}{2} \mathrm{d}u - \int_{1}^{0} \frac{\sqrt{4 + 9u}}{2} \mathrm{d}u \text{ (par le changement de variable } u = t^2) \\
&= 2\left[\frac{1}{18}(4 + 9u)^{\frac{3}{2}}\right]_0^1 \\
&= \frac{1}{9}\left(13^{\frac{3}{2}} - 8\right).
\end{aligned}$$

2. Si γ est la courbe paramétrée $[0; 2\pi] \to \mathbb{R}^2$; $t \mapsto (\cos(t), \sin(t))$, γ est de classe $\mathcal{C}^1$ sur le segment $[0, 2\pi]$ et

$$\begin{aligned}
L(\gamma) &= \int_{0}^{2\pi} \|\gamma'(t)\| \mathrm{d}t \\
&= \int_{0}^{2\pi} \sqrt{\cos^2(t) + \sin^2(t)} \mathrm{d}t \\
&= \int_{0}^{2\pi} \sqrt{1} \mathrm{d}t \\
&= 2\pi.
\end{aligned}$$

3. Si maintenant γ est la courbe paramétrée $[0; 3\pi] \to \mathbb{R}^2$; $t \mapsto (\cos(t), \sin(t))$, γ est de classe $\mathcal{C}^1$ sur le segment $[0, 3\pi]$ et

$$L(\gamma) = \int_{0}^{3\pi} \|\gamma'(t)\| \mathrm{d}t = \int_{0}^{3\pi} \mathrm{d}t = 3\pi.$$

Remarque 4.6.9. Les deux derniers exemples précédents montrent que la longueur d'une courbe paramétrée ne dépend pas seulement de son support.

4.7 Paramétrisation normale et abscisse curviligne

Dans cette dernière section, on s'intéresse aux paramétrisations des courbes qui paramètrent la position d'un point par sa distance au "point de départ", des paramétrisations dites *normales* :

Définition 4.7.1. *On dit qu'une courbe paramétrée rectifiable $\eta : J \to \mathbb{R}^d$ est <u>normale</u> si pour tous $l_1, l_2 \in J$ tels que $l_1 \leqslant l_2$,*

$$L(\eta_{|[l_1,l_2]}) = l_2 - l_1.$$

Soit $\eta : J \to \mathbb{R}^d$ une courbe paramétrée rectifiable et soit $l_0 \in J$. La "normalité" de η peut être caractérisée par une "normalité" par rapport à l_0 :

Lemme 4.7.2. *La courbe paramétrée η est normale si et seulement si pour tout $l \in I$,*

- $L(\eta_{|[l_0,l]}) = l - l_0$ *si* $l \geqslant l_0$,
- $L(\eta_{|[l,l_0]}) = l_0 - l$ *si* $l \leqslant l_0$.

Démonstration. Supposons tout d'abord que la courbe paramétrée η soit normale, alors

- si $l \in I$ vérifie $l_0 \leqslant l$, on a $L(\eta_{|[l_0,l]}) = l - l_0$,
- si $l \in I$ vérifie $l \leqslant l_0$, on a $L(\eta_{|[l,l_0]}) = l_0 - l$.

Réciproquement, si η vérifie l'hypothèse de l'énoncé alors, pour tout $l_1, l_2 \in I$ tels que $l_1 \leqslant l_2$,

- si $l_0 \leqslant l_1$,

$$L(\eta_{|[l_1,l_2]}) = L(\eta_{|[l_0,l_2]}) - L(\eta_{|[l_0,l_1]}) = l_2 - l_0 - (l_1 - l_0) = l_2 - l_1,$$

- si $l_1 \leqslant l_0 \leqslant l_2$,

$$L(\eta_{|[l_1,l_2]}) = L(\eta_{|[l_1,l_0]}) + L(\eta_{|[l_0,l_2]}) = l_0 - l_1 + l_2 - l_0 = l_2 - l_1,$$

- si $l_1 \leqslant l_2 \leqslant l_0$,

$$L(\eta_{|[l_1,l_2]}) = L(\eta_{|[l_1,l_0]}) - L(\eta_{|[l_2,l_0]}) = l_0 - l_1 - (l_0 - l_2) = l_2 - l_1.$$

□

Si l'intervalle J est fermé borné, on peut considérer un "point de départ" pour la courbe paramétrée η et relier le caractère "normal" à la distance à ce "point de départ".

Lemme 4.7.3. *On suppose que $J = [\alpha, \beta]$ avec $\alpha, \beta \in \mathbb{R}$ tels que $\alpha < \beta$, ainsi que le $\mathcal{C}^\infty$-difféomorphisme $\sigma : [0, \beta - \alpha] \to [\alpha, \beta]$; $t \mapsto t - \alpha$. Alors η est normale si et seulement si la reparamétrisation $\widetilde{\eta} := \eta \circ \sigma : [0, \beta - \alpha] \to \mathbb{R}^d$ est normale, et on a alors, pour tout $s \in [0, \alpha - \beta]$,*

$$L(\widetilde{\eta}_{|[0,s]})) = s$$

(le point $\widetilde{\eta}(s)$ est à une "longueur d'arc paramétré" s du point de départ $\widetilde{\eta}(0)$).

Démonstration. Supposons que η soit normale et soit $s \in [0, \alpha-\beta]$, alors les courbes paramétrées $\widetilde{\eta}_{|[0,s]}$ et $\eta_{|[\alpha,s+\alpha]}$ sont $\mathcal{C}^0$-équivalentes (via la restriction de σ à $[0,s]$) et donc, par la proposition 4.6.5,

$$L(\widetilde{\eta}_{|[0,s]}) = L(\eta_{|[\alpha,s+\alpha]}) = s + \alpha - \alpha = s :$$

la courbe paramétrée $\widetilde{\eta}$ est donc normale par le lemme 4.7.2.

Réciproquement, si $\widetilde{\eta}$ est normale et $l \in [\alpha, \beta]$, les courbes paramétrées $\eta_{|[\alpha,l]}$ et $\widetilde{\eta}_{|[0,l-\alpha]}$ sont $\mathcal{C}^0$-équivalentes (via la restriction de σ^{-1} à $[\alpha, l]$) et donc

$$L(\eta_{|[\alpha,l]}) = L(\widetilde{\eta}_{|[0,l-\alpha]}) = l - \alpha.$$

□

Avec les notations ci-dessus, on dit, lorsque η est normale, que la courbe paramétrée $\widetilde{\eta}$ est une *paramétrisation de C_η par longueurs d'arc.*

La terminologie "normale" est motivée par la proposition suivante, qui nécessite de supposer une régularité de classe $\mathcal{C}^1$:

Proposition 4.7.4. *On suppose que la courbe paramétrée η est de classe $\mathcal{C}^1$. Alors η est normale si et seulement si pour tout $l \in J$, $\|\eta'(l)\| = 1$.*

Démonstration. Supposons que η soit normale. Soit alors $l_0 \in J$ et considérons la fonction

$$s_{l_0} : \begin{array}{ccc} J & \to & \mathbb{R} \\ l & \mapsto & \displaystyle\int_{l_0}^{l} \|\eta'(u)\| \mathrm{d}u \end{array}$$

Comme η est de classe $\mathcal{C}^1$ sur J, la fonction s_{l_0} est de classe $\mathcal{C}^1$ sur J et, pour tout $l \in J$,

$$s'_{l_0}(l) = \|\eta'(l)\|$$

(par le théorème fondamental du calcul intégral).

D'autre part, si $l \in J$, on a, si $l \geqslant l_0$,

$$s_{l_0}(l) = \int_{l_0}^{l} \|\eta'(u)\| \mathrm{d}u = L(\eta_{|[l_0,l]}) = l - l_0$$

et, si $l \leqslant l_0$,

$$s_{l_0}(l) = \int_{l_0}^{l} \|\eta'(u)\| \mathrm{d}u = -\int_{l}^{l_0} \|\eta'(u)\| \mathrm{d}u = -L(\eta_{|[l,l_0]}) = -(l_0 - l) = l - l_0.$$

Ainsi, pour tout $l \in J$, $s_{l_0}(l) = l - l_0$. En particulier, pour tout $l \in J$, $s'_{l_0}(l) = 1$ et donc, pour tout $l \in J$, $s'_{l_0}(l) = \|\eta'(l)\| = 1$.

Réciproquement, supposons que pour tout $l \in J$, $\|\eta'(l)\| = 1$, et soient $l_1, l_2 \in J$ tels que $l_1 \leqslant l_2$,

$$L(\eta_{|[l_1,l_2]}) = \int_{l_1}^{l_2} \|\eta'(u)\| \mathrm{d}u = \int_{l_1}^{l_2} \mathrm{d}u = l_2 - l_1$$

et donc la courbe paramétrée η est normale. □

Remarque 4.7.5. Si la courbe paramétrée η est de classe $\mathcal{C}^1$ et normale, η est régulière et pour tout $l \in J$, le vecteur tangent $\eta'(l)$ est unitaire, en particulier la "vitesse instantanée" est constante égale à 1 sur J.

Exemple 4.7.6. La courbe paramétrée $\gamma : \mathbb{R} \to \mathbb{R}^2$; $t \mapsto (\cos(t), \sin(t))$ de classe $\mathcal{C}^1$ est normale : pour tout $t \in \mathbb{R}$,

$$\|\gamma'(t)\| = \sqrt{\cos^2(t) + \sin^2(t)} = \sqrt{1} = 1.$$

Soit maintenant $\gamma : I \to \mathbb{R}^d$ une courbe paramétrée de classe $\mathcal{C}^1$. Sous une hypothèse de régularité, nous allons déterminer une paramétrisation normale de C_γ à l'aide de la fonction auxiliaire s_{t_0} définie dans la preuve ci-dessus, où $t_0 \in I$:

Définition 4.7.7. *On fixe $t_0 \in I$ et on note s_{t_0} la fonction*

$$\begin{array}{ccc} I & \to & \mathbb{R} \\ t & \mapsto & \displaystyle\int_{t_0}^{t} \|\gamma'(u)\| \mathrm{d}u \end{array}$$

appelée abscisse curviligne de γ à partir de t_0.

Remarque 4.7.8. D'après la preuve de la proposition 4.7.4, on a, pour tout $t \in I$,

$$s_{t_0}(t) = \begin{cases} L(\gamma_{|[t_0,t]}) & \text{si } t \geqslant t_0, \\ L(\gamma_{|[t,t_0]}) & \text{si } t \leqslant t_0. \end{cases}$$

De plus, comme γ est de classe $\mathcal{C}^1$, il en est de même pour la fonction s_{t_0} et, pour tout $t \in I$, $s'_{t_0}(t) = \|\gamma'(t)\|$. Remarquons également que la fonction s_{t_0} est donc croissante.

Soit donc $t_0 \in I$. L'abscisse curviligne de γ à partir de t_0 permet de définir une reparamétrisation normale de C_γ, lorsque γ est régulière :

Théorème 4.7.9. *On suppose que la courbe paramétrée γ est régulière (i.e. pour tout $t \in I$, $\gamma'(t) \neq \overrightarrow{0}$: cf. définition 4.4.7). Alors $s_{t_0} : I \to s_{t_0}(I)$ est un $\mathcal{C}^1$-difféomorphisme et l'application*

$$\gamma \circ s_{t_0}^{-1} : s_{t_0}(I) \to \mathbb{R}^d$$

est une courbe paramétrée normale ($\mathcal{C}^1$-équivalente à γ).

Démonstration. On a, pour tout $t \in I$, $s'_{t_0}(t) = \|\gamma'(t)\| > 0$ car γ est régulière. La fonction s_{t_0} est donc strictement croissante et est donc une bijection de I sur $s_{t_0}(I)$. De plus, comme s_{t_0} est également de classe $\mathcal{C}^1$ et, pour tout $t \in I$, $s'_{t_0}(t) \neq 0$, la réciproque $s_{t_0}^{-1} : s_{t_0}(I) \to I$ de $s_{t_0} : I \to s_{t_0}(I)$ est également de classe $\mathcal{C}^1$ et, pour tout $l \in s_{t_0}(I)$,

$$\left(s_{t_0}^{-1}\right)'(l) = \frac{1}{s'_{t_0}(s_{t_0}^{-1}(l))}.$$

Ainsi, la fonction $s_{t_0} : I \to s_{t_0}(I)$ est bien un $\mathcal{C}^1$-difféomorphisme et, si $l \in s_{t_0}(I)$, on a

$$\begin{aligned}
\left\|\left(\gamma \circ s_{t_0}^{-1}\right)'(l)\right\| &= \left\|\left(s_{t_0}^{-1}\right)'(l) \cdot \gamma'\left(\left(s_{t_0}^{-1}\right)(l)\right)\right\| \\
&= \left\|\frac{1}{s'_{t_0}(s_{t_0}^{-1}(l))} \cdot \gamma'\left(\left(s_{t_0}^{-1}\right)(l)\right)\right\| \\
&= \frac{1}{s'_{t_0}\left(s_{t_0}^{-1}(l)\right)}\left\|\gamma'\left(\left(s_{t_0}^{-1}\right)(l)\right)\right\| \\
&= \frac{1}{\left\|\gamma'\left(s_{t_0}^{-1}(l)\right)\right\|}\left\|\gamma'\left(\left(s_{t_0}^{-1}\right)(l)\right)\right\| \\
&= 1.
\end{aligned}$$

La reparamétrisation $\gamma \circ s_{t_0}^{-1} : s_{t_0}(I) \to \mathbb{R}^d$ est donc normale par la proposition 4.7.4.

□

Si de plus l'intervalle I est fermé borné, on peut construire, grâce au théorème précédent, une paramétrisation de C_γ par longueurs d'arc :

Corollaire 4.7.10. *On suppose que $I = [a, b]$ avec $a, b \in \mathbb{R}$ tels que $a < b$ et que γ est régulière. Alors l'application*

$$\gamma \circ s_a^{-1} : [0, L(\gamma)] \to \mathbb{R}^d$$

est une paramétrisation normale de C_γ par longueurs d'arc.

Démonstration. En reprenant la preuve du théorème 4.7.9, on a

$$s_a(I) = s_a([a, b]) = [s_a(a), s_a(b)]$$

et $s_a(a) = L(\gamma_{|[a,a]}) = 0$, $s_a(b) = L(\gamma_{|[a,b]}) = L(\gamma)$. □

Remarque 4.7.11. Avec les notations et hypothèses ci-dessus, on peut voir la courbe paramétrée $\gamma \circ s_a^{-1} : [0, L(\gamma)] \to \mathbb{R}^d$ comme l'"enroulement" du segment $[0, L(\gamma)]$ sur la courbe C_γ.

Exemple 4.7.12. On suppose que γ est la courbe paramétrée de classe $\mathcal{C}^1$

$$\begin{array}{ccc}
\left[0; \frac{1}{2}\right] & \to & \mathbb{R}^2 \\
t & \mapsto & (t, \sqrt{1 - t^2})
\end{array}$$

alors, pour tout $t \in \left[0; \frac{1}{2}\right]$,

$$\gamma'(t) = \left(1, \frac{-2t}{2\sqrt{1 - t^2}}\right) = \left(1, \frac{-t}{\sqrt{1 - t^2}}\right).$$

En particulier, γ est régulière et l'abscisse curviligne de γ à partir de 0 est donnée par, si $t \in \left[0; \frac{1}{2}\right]$,

$$\begin{aligned}
s_0(t) &= L(\gamma_{|[0,t]}) \\
&= \int_0^t \|\gamma'(u)\| \mathrm{d}u \\
&= \int_0^t \sqrt{1^2 + \left(\frac{-u}{\sqrt{1-u^2}}\right)^2} \mathrm{d}u \\
&= \int_0^t \sqrt{1 + \frac{u^2}{1-u^2}} \mathrm{d}u \\
&= \int_0^t \sqrt{\frac{1}{1-u^2}} \mathrm{d}u \\
&= \int_0^t \frac{1}{\sqrt{1-u^2}} \mathrm{d}u \\
&= [\arcsin(u)]_0^t \\
&= \arcsin(t).
\end{aligned}$$

Ainsi, $s_0\left(\left[0; \frac{1}{2}\right]\right) = \left[\arcsin(0), \arcsin\left(\frac{1}{2}\right)\right] = \left[0, \frac{\pi}{6}\right]$ et la fonction réciproque de $s_0 : \left[0; \frac{1}{2}\right] \to \left[0, \frac{\pi}{6}\right]$ est

$$s_0^{-1} : \begin{array}{ccc} \left[0, \frac{\pi}{6}\right] & \to & \left[0; \frac{1}{2}\right] \\ \theta & \mapsto & \sin(\theta) \end{array}$$

La courbe paramétrée

$$\gamma \circ s_0^{-1} : \begin{array}{ccc} \left[0, \frac{\pi}{6}\right] & \to & \mathbb{R}^2 \\ \theta & \mapsto & \left(\sin(\theta), \sqrt{1-\sin^2(\theta)}\right) = (\sin(\theta), \cos(\theta)) \end{array}$$

est alors une paramétrisation normale de C_γ par longueurs d'arc.