Les courbes elliptiques en géométrie complexe

Aziz El Kacimi
Professeur émérite
Université Polytechnique Hauts-de-France

First International Conference on Algebraic Topology and its Applications in Robotics (ICATAR)

Meknès 17 et 18 mars 2023

On retrouve les courbes elliptiques dans diverses branches des mathématiques :

- *algèbre, théorie des nombres,*
- *analyse,*
- *géométrie algébrique,*
- *géométrie complexe,*
- *...*

Nous les regarderons en géométrie complexe.

Nous montrons d'abord comment une courbe elliptique est construite géométriquement.

Nous donnons sa structure complexe et ce qui régit sa variation.

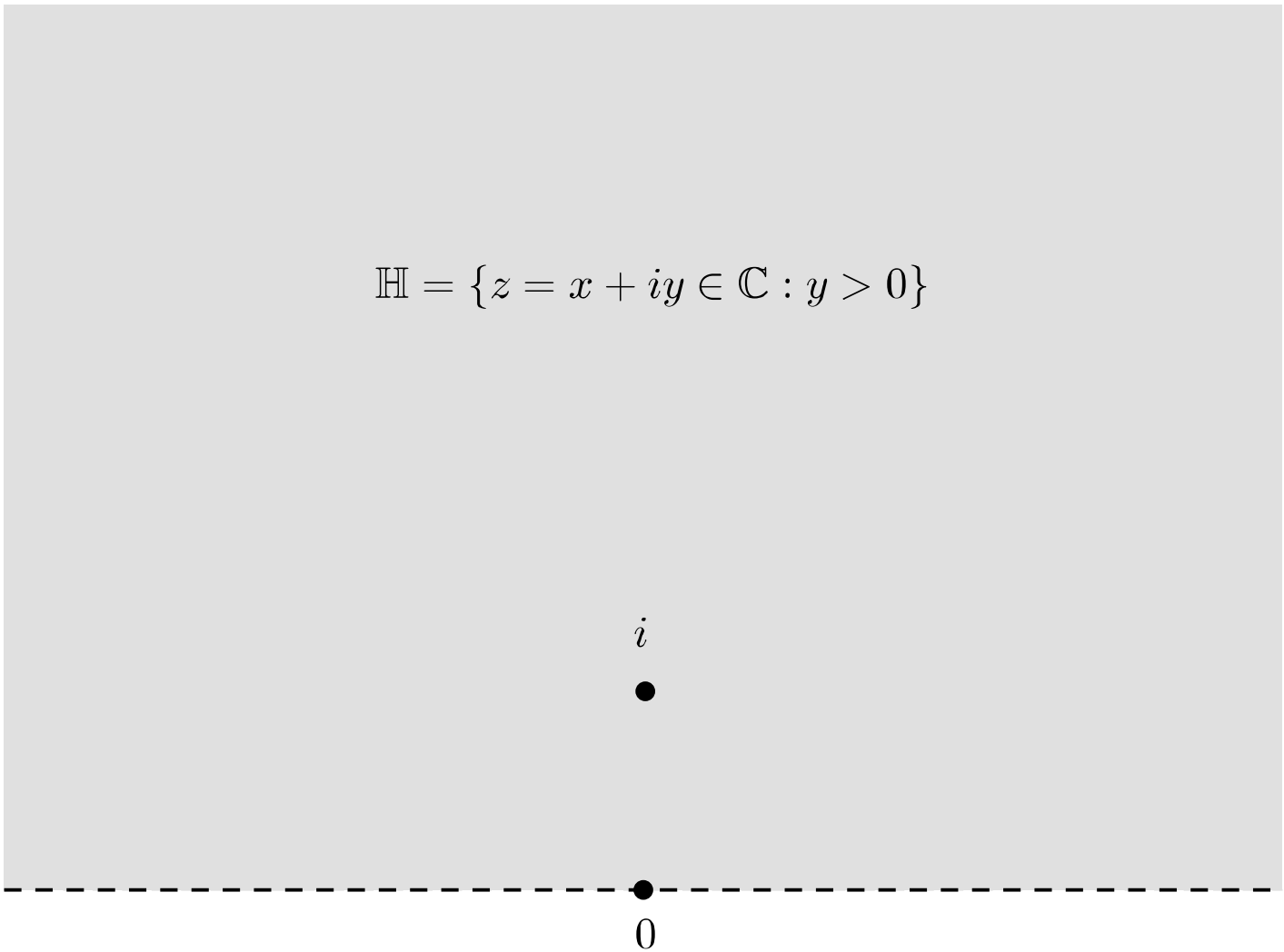
Nous introduisons les fonctions elliptiques.

Exemple fondamental : la fonction de Weierstrass $\wp$.

Nous indiquons comment $\wp$ est utilisée pour plonger une courbe elliptique dans le plan projectif complexe $P^2(\mathbb{C})$.

Demi-plan de Poincaré $\mathbb{H}$

$$\mathbb{H} = \{z = x + iy \in \mathbb{C} : y > 0\}$$



Les homographies de $\mathbb{H}$

On s'intéresse aux transformations $h : z \in \mathbb{H} \longmapsto h(z) \in \mathbb{H}$ *de la forme :*

$$h(z) = \frac{az + b}{cz + d}$$

où a, b, c, d *sont des réels. On peut bien entendu supposer que* a, b, c, d *vérifient la relation* $ad - bc = 1$.

Elles forment un groupe qu'on notera $\mathcal{H}$ *: groupe des homographies.*

Le groupe SL(2,R)

C'est le groupe des matrices réelles :
$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ *de déterminant* $ad - bc = 1$.

Le meilleur de ses sous-groupes : SL(2,Z)

Les mêmes matrices mais à coefficients des entiers relatifs.

1. Courbes elliptiques

1.1. Réseaux dans $\mathbb{C}$

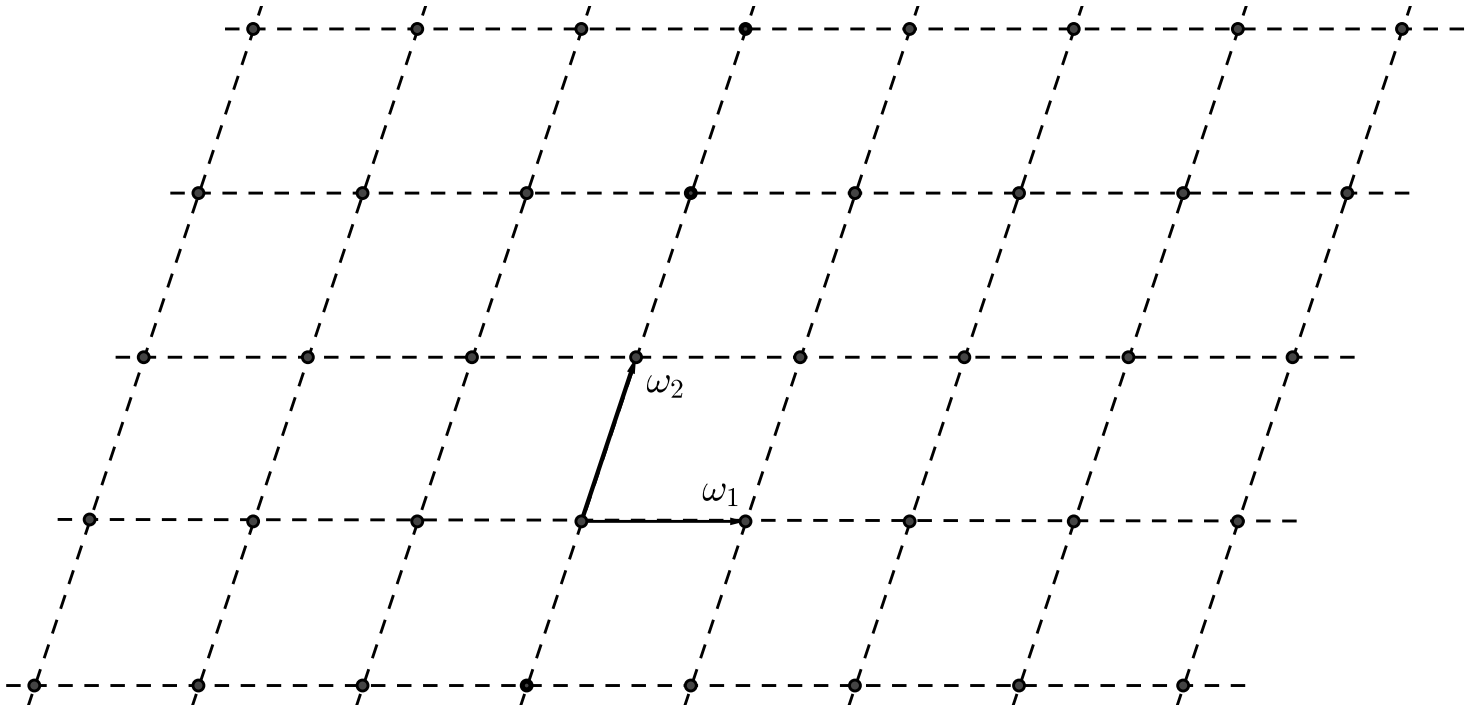
Definition

Un ***réseau*** *de* $\mathbb{C}$ *est un sous-groupe discret* Γ *du groupe additif* $(\mathbb{C}, +)$ *isomorphe à* $\mathbb{Z}^2 \simeq \mathbb{Z} \oplus \mathbb{Z}$.

Soit $\omega_1 \in \Gamma$ tel que $|\omega_1| = \inf\{|\omega| : \omega \in \Gamma \backslash \{0\}\}$. Un tel élément existe puisque Γ est une partie discrète de $\mathbb{C}$. De même, on peut trouver $\omega_2 \in \Gamma$ non nul de module minimal dans $\Gamma \backslash \{0, \omega_1\}$ et tel que le rapport $\frac{\omega_2}{\omega_1}$ ne soit pas réel. On peut alors montrer (voir par exemple [1] page 265) que Γ coïncide avec le réseau :

$$\{m_1\omega_1 + m_2\omega_2 : m_1, m_2 \in \mathbb{Z}\}$$

c'est-à-dire, qu'en tant que $\mathbb{Z}$-module, Γ admet le couple (ω_1, ω_2) comme base.



Le parallélogramme Δ du plan formé par les deux vecteurs ω_1 et ω_2 est appelé ***domaine fondamental*** du réseau Γ. On en distingue 5 types en fonction de leur « forme » :

a) ***Oblique :*** $|\omega_1| < |\omega_2| < |\omega_1 - \omega_2| < |\omega_1 + \omega_2|$

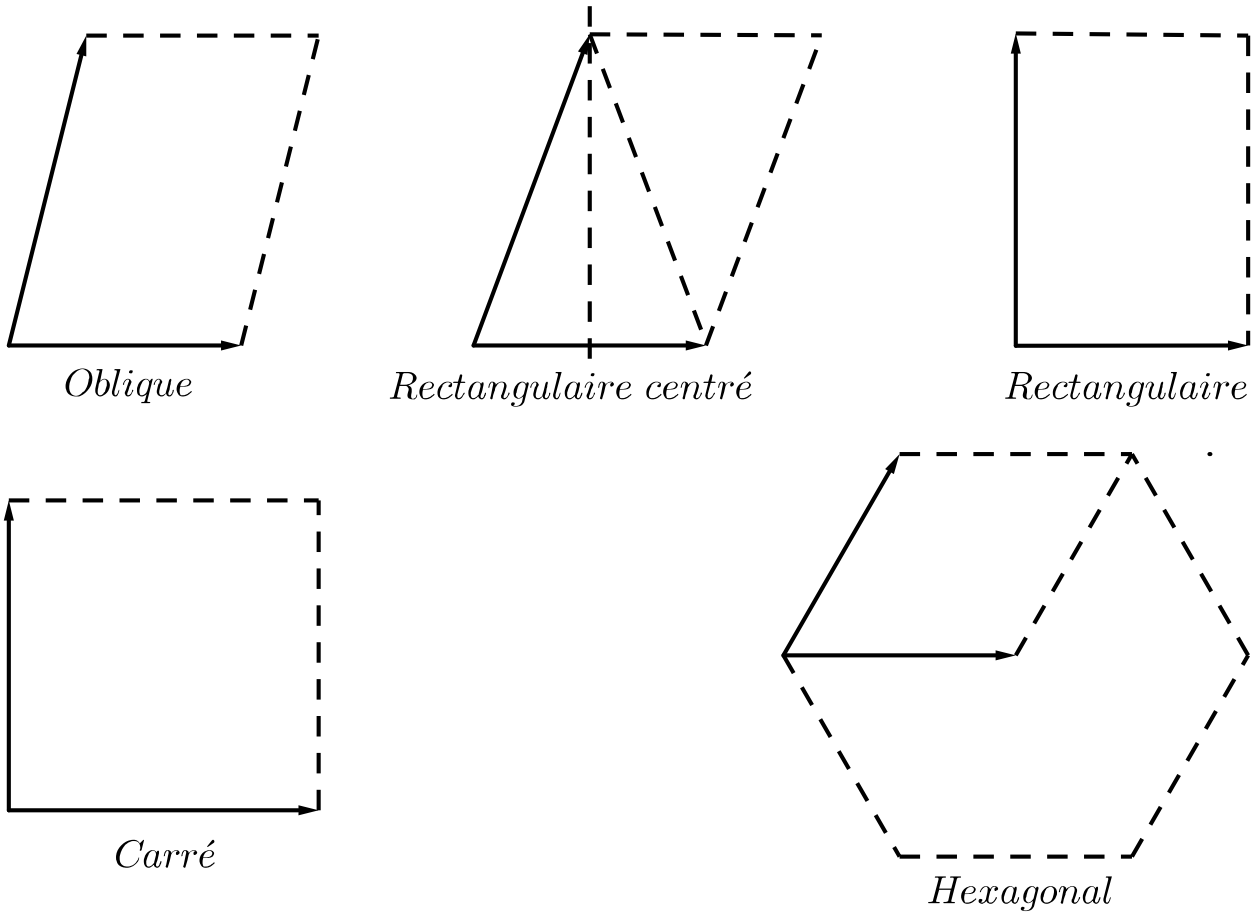
b) ***Rectangulaire centré :*** $|\omega_1| < |\omega_2| = |\omega_1 - \omega_2| < |\omega_1 + \omega_2|$

c) ***Rectangulaire :*** $|\omega_1| < |\omega_2| < |\omega_1 - \omega_2| = |\omega_1 + \omega_2|$

d) ***Carré :*** $|\omega_1| = |\omega_2| < |\omega_1 - \omega_2| = |\omega_1 + \omega_2|$

e) ***Hexagonal :*** $|\omega_1| = |\omega_2| = |\omega_1 - \omega_2| < |\omega_1 + \omega_2|$

Voici les différents dessins qui leur correspondent. Ils ne nous serviront pas ici, ils apparaissent plutôt dans l'étude des pavages du plan.



Notons $\mathrm{GL}(2,\mathbb{Z})$ le groupe des matrices carrées d'ordre 2 à coefficients dans $\mathbb{Z}$ et de déterminant $+1$ ou -1 ; celles de déterminant 1 en constituent le sous-groupe $\mathrm{SL}(2,\mathbb{Z})$.

Proposition

Soient (ω_1, ω_2) ***et*** (ω_1', ω_2') ***deux bases de*** Γ***. Alors il existe une matrice*** $A \in \boldsymbol{GL}(2, \mathbb{Z})$ ***telle que*** $\begin{pmatrix} \omega_1' \\ \omega_2' \end{pmatrix} = A \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix}$***.***

Preuve. Comme $\omega_1', \omega_2' \in \Gamma$, il existe $a, b, c, d \in \mathbb{Z}$ tels que l'on ait $\omega_1' = a\omega_1 + b\omega_2$ et $\omega_2' = c\omega_1 + d\omega_2$ qu'on peut écrire sous forme matricielle $\begin{pmatrix} \omega_1' \\ \omega_2' \end{pmatrix} = A \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix}$ où A est la matrice $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$. De même, il existe une matrice à coefficients entiers $A' = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}$ telle que $\begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} = A' \begin{pmatrix} \omega_1' \\ \omega_2' \end{pmatrix}$. Ceci donne : $\begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} = A' \begin{pmatrix} \omega_1' \\ \omega_2' \end{pmatrix} = A'A \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix}$. La matrice $A'A$ fixe la base (ω_1, ω_2) ; c'est donc la matrice identité $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

Par suite $\det A \cdot \det A' = 1$. Comme ces déterminants sont des entiers, on a $\det A = 1$ ou $\det A = -1$ i.e. la matrice A est un élément de $\mathrm{GL}(2, \mathbb{Z})$. □

Le groupe (multiplicatif) $\mathbb{C}^*$ agit sur l'ensemble $\mathfrak{R}$ des réseaux de $\mathbb{C}$: à $(\alpha, \Gamma) \in \mathbb{C}^* \times \mathfrak{R}$ où Γ est engendré par (ω_1, ω_2), on associe le réseau $\alpha\Gamma$ engendré par $(\alpha\omega_1, \alpha\omega_2)$. Chaque orbite de cette action contient le réseau donné par la base $(1, \tau)$ où $\tau = \frac{\omega_2}{\omega_1}$. Quitte à appliquer à ce dernier la matrice $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \in \mathrm{GL}(2, \mathbb{Z})$, on peut toujours se ramener au cas où $\Im(\tau) > 0$, c'est-à-dire τ est un élément du demi-plan hyperbolique $\mathbb{H}$. Les couples $(1, \tau)$ de ce type permettent, comme on le verra, de mieux décrire l'équivalence entre courbes elliptiques du point de vue complexe.

1.2. Le tore différentiable

Commençons d'abord par introduire la nature topologique (et aussi différentiable) de l'objet. Nous verrons ensuite comment ça se passe du point de vue complexe.

Soit Γ_ω le réseau engendré par une base $\omega = (\omega_1, \omega_2)$. On fait agir Γ_ω sur $\mathbb{C}$ de la façon suivante : à $m_1\omega_1 + m_2\omega_2$ dans Γ_ω et $z \in \mathbb{C}$ on associe le complexe $z + m_1\omega_1 + m_2\omega_2$. Cette action est différentiable, libre et propre. Le quotient $\mathbb{C}/\Gamma_\omega$ est donc une surface différentiable. Regardons comment elle se fabrique géométriquement.

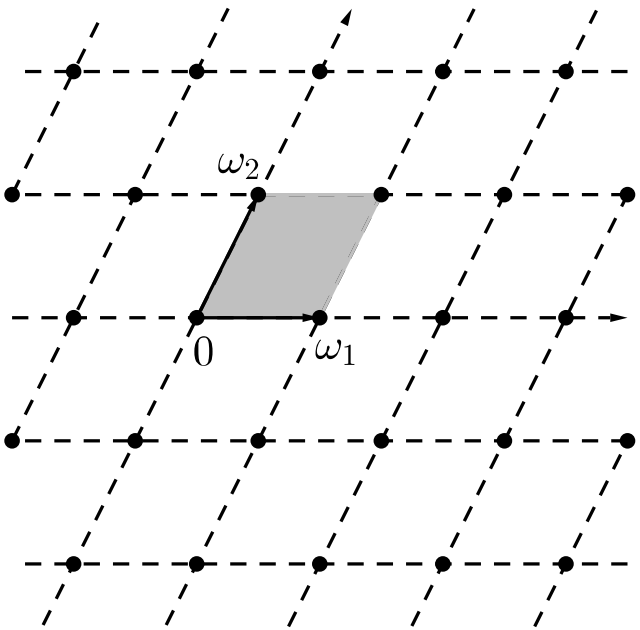
L'orbite de 0 est le sous-groupe Γ_ω de $\mathbb{C}$; il y définit un ***grillage*** $\mathcal{G}$: l'ensemble des droites parallèles aux vecteurs ω_1 et ω_2 et passant par les points de Γ_ω (voir dessin ci-dessous).

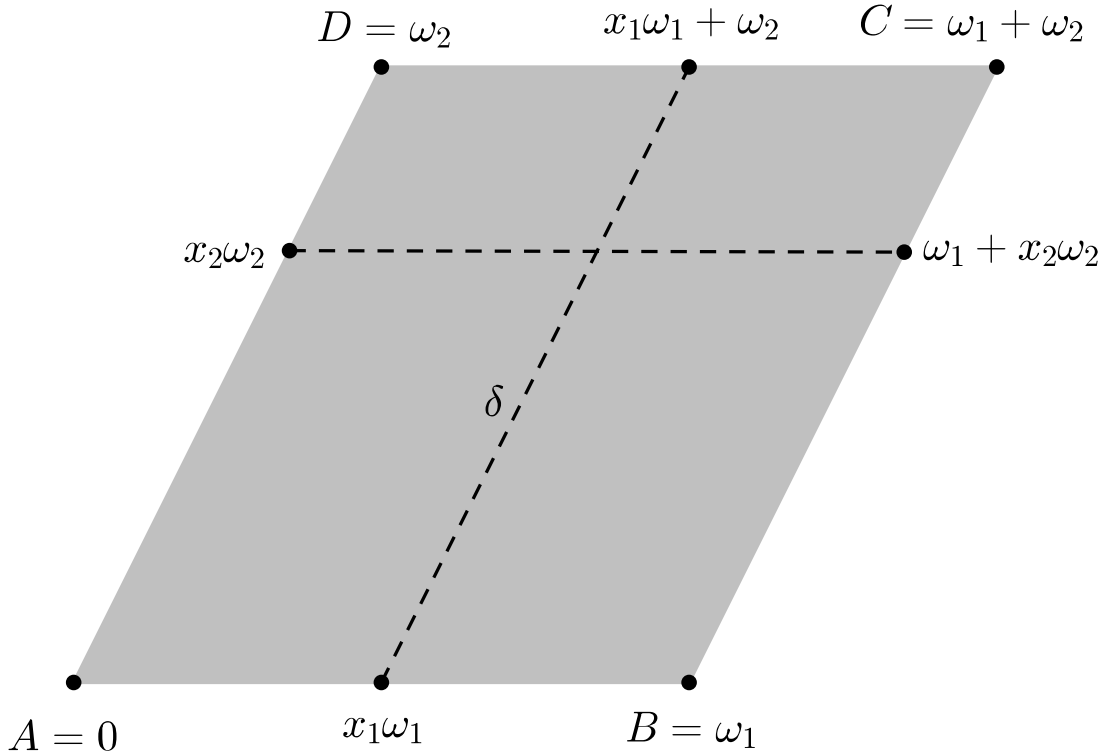
• Si $w \in \mathbb{C}\backslash\mathcal{G}$, il est équivalent à un unique point de l'intérieur du carré $\mathcal{C}$.

• Si $w \in \Gamma_\omega$, il est équivalent aux quatre sommets A, B, C et D du carré $\mathcal{C}$.

• Si $w \in \mathcal{G}\backslash\Gamma_\omega$, il est équivalent aux deux points $x_1\omega_1$ et $x_1\omega_1 + \omega_2$ ou aux deux points $x_2\omega_2$ et $\omega_1 + x_2\omega_2$ (qu'on voit sur le desin de droite) où $x_1 = y_1 - E(y_1)$ et $x_2 = y_2 - E(y_2)$ (ici $E(z)$ désigne le plus grand entier relatif inférieur ou égal au réel z).

Dans tous les cas considérés, le carré $\mathcal{C}$ contient au moins un élément de chaque classe d'équivalence. C'est un ***domaine fondamental*** pour la relation $\mathcal{R}$ associée à l'action. Il va permettre d'obtenir l'espace quotient $\mathbb{C}/\mathcal{R}$.


ω_2
0
ω_1


$D = \omega_2$
$x_1\omega_1 + \omega_2$
$C = \omega_1 + \omega_2$
$x_2\omega_2$
$\omega_1 + x_2\omega_2$
δ
$A = 0$
$x_1\omega_1$
$B = \omega_1$

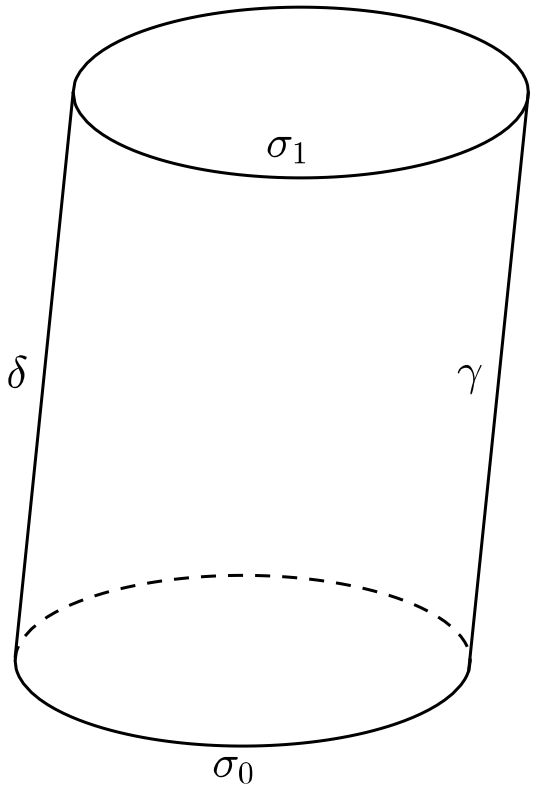
Il s'agit d'identifier les points équivalents. Il suffit donc de le faire sur $\mathcal{C}$ puisque toute classe d'équivalence y a un représentant.

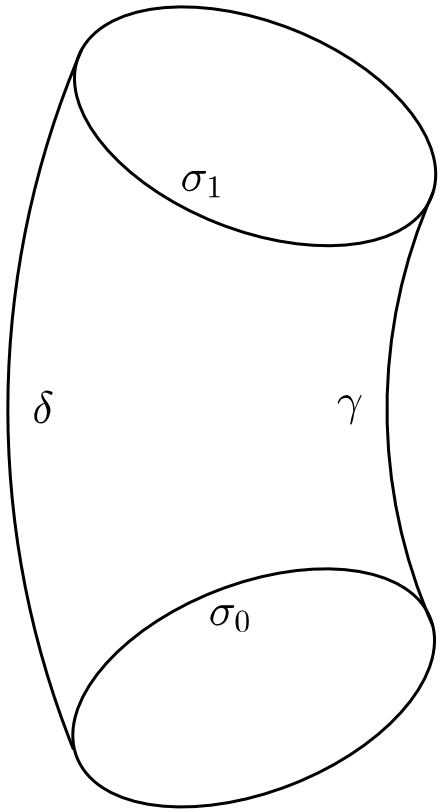
Sur le carré grisé, on colle le vecteur $\overrightarrow{AD}$ sur le vecteur $\overrightarrow{BC}$; on obtient un cylindre dans lequel ces deux vecteurs donnent le segment γ (voir dessin ci-dessous).

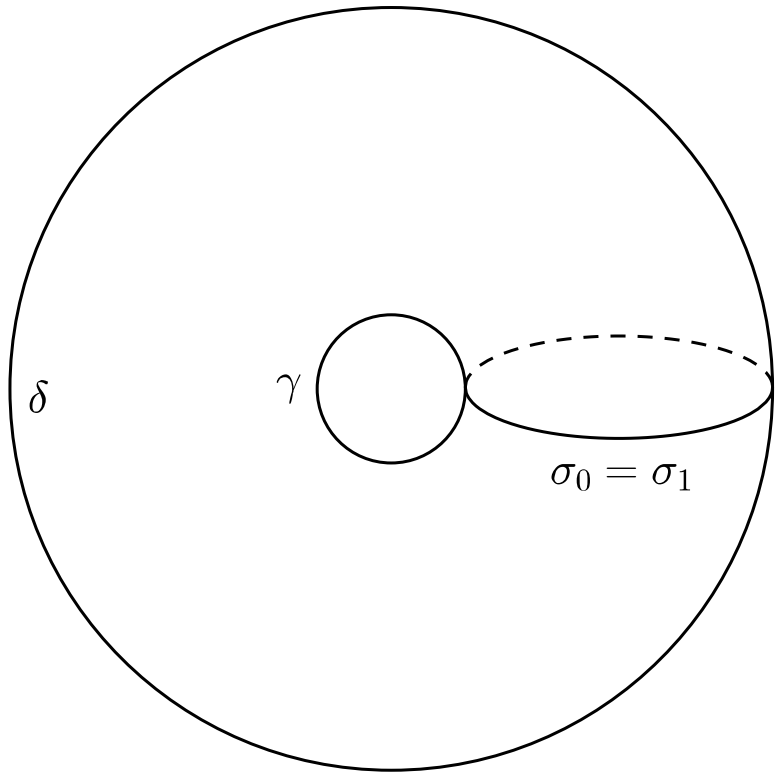
Les segments AB et DC deviennent respectivement les deux cercles σ_0 et σ_1.

Ensuite, on tord le cylindre en poussant le haut et le bas (vers la droite par exemple) jusqu'à superposer le cercle σ_0 sur le cercle σ_1.

La surface fermée ainsi obtenue (penser à une chambre à air gonflée) s'appelle ***tore*** et se note $\mathbb{T}^2_\omega$.


σ_1
δ
γ
σ_0


σ_1
δ
γ
σ_0


δ
γ
$\sigma_0 = \sigma_1$

A priori la structure différentiable sur $\mathbb{T}^2_\omega$ dépend de la base $\omega = (\omega_1, \omega_2)$. En fait, il n'en est rien comme le précise la :

Proposition

Soient Γ_ω et $\Gamma_{\omega'}$ deux réseaux de $\mathbb{C}$ définis respectivement par les bases $\omega = (\omega_1, \omega_2)$ et $\omega' = (\omega'_1, \omega'_2)$. Alors il existe un difféomorphisme f envoyant $\mathbb{T}^2_\omega$ sur $\mathbb{T}^2_{\omega'}$.

Preuve. Elle est immédiate. Il existe un automorphisme linéaire réel $\widetilde{f}$ de $\mathbb{C}$ tel que $\widetilde{f}(\omega_1) = \omega'_1$ et $\widetilde{f}(\omega_2) = \omega'_2$. Cet automorphisme induit un ismorphisme du réseau Γ_ω sur le réseau $\Gamma_{\omega'}$ et donne donc un difféomorphisme $f : \mathbb{C}/\Gamma_\omega = \mathbb{T}^2_\omega \longrightarrow \mathbb{T}^2_{\omega'} = \mathbb{C}/\Gamma_{\omega'}$. □

1.3. Courbes elliptiques

Nous avons vu que, pour tout réseau Γ_ω de $\mathbb{C}$, le quotient $\mathbb{T}^2_\omega = \mathbb{C}/\Gamma_\omega$ est une surface compacte dont la structure différentiable ne dépend pas de la base $\omega = (\omega_1, \omega_2)$. C'est la raison pour laquelle, vue sous cet angle, on la note communément $\mathbb{T}^2$ en la considérant comme le quotient de $\mathbb{C}$ par le réseau standard $\{m_1 + im_2 : m_1, m_2 \in \mathbb{Z}\} \simeq \mathbb{Z}^2$. Il n'en sera rien de tout cela lorsqu'on regardera le quotient $\mathbb{T}^2_\omega$ sous l'aspect complexe.

L'action par translations de Γ_ω sur $\mathbb{C}$ est par biholomorphismes. Comme elle est en plus libre et propre, la surface quotient $\mathbb{T}^2_\omega$ est une courbe complexe. C'est ce qu'on appelle la ***courbe elliptique*** associée au réseau Γ_ω.

Soient maintenant $\omega = (\omega_1, \omega_2)$, $\alpha \in \mathbb{C}^*$ et $\omega' = (\alpha\omega_1, \alpha\omega_2)$. Alors les deux courbes elliptiques $\mathbb{T}^2_\omega$ et $\mathbb{T}^2_{\omega'}$ sont (biholomorphiquement) équivalentes.

En effet, l'application $z \in \mathbb{C} \longmapsto \alpha z \in \mathbb{C}$ est un biholomorphisme qui envoie le réseau Γ_ω sur le réseau $\Gamma_{\omega'}$; il induit alors un biholomorphisme de $\mathbb{T}^2_\omega$ sur $\Gamma_{\omega'}$.

On se contentera donc de travailler avec les réseaux du type Γ_τ où $\tau = (1, \tau)$ avec $\tau \in \mathbb{H}$.

Proposition

Soient $\mathbb{T}^2_\tau$ *et* $\mathbb{T}^2_{\tau'}$ *deux courbes elliptiques associées respectivement aux réseaux* Γ_τ *et* $\Gamma_{\tau'}$ *avec* $\tau = (1, \tau)$ *et* $\tau' = (1, \tau')$. *Alors* $\mathbb{T}^2_\tau$ *et* $\mathbb{T}^2_{\tau'}$ *sont équivalentes si, et seulement si, il existe une matrice* $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \boldsymbol{SL}(2, \mathbb{Z})$ *telle que* $\tau' = \frac{a\tau + b}{c\tau + d}$.

Preuve. L'égalité $\tau' = \frac{a\tau+b}{c\tau+d}$ est équivalente à $\frac{\tau'}{a\tau+b} = \frac{1}{c\tau+d} = \alpha$ où α est un nombre complexe non nul. On a alors $1 = \alpha(c\tau + d)$ et $\tau' = \alpha(a\tau + b)$, ce qu'on peut écrire matriciellement :

$$\begin{pmatrix} 1 \\ \tau' \end{pmatrix} = \begin{pmatrix} d & c \\ b & a \end{pmatrix} \begin{pmatrix} \alpha \\ \alpha\tau \end{pmatrix}.$$

Comme $\begin{pmatrix} d & c \\ b & a \end{pmatrix}$ est encore une matrice de $\mathrm{SL}(2,\mathbb{Z})$, ceci dit que $(\alpha, \alpha\tau)$ est aussi une base du réseau $\Gamma_{\tau'}$; donc les courbes elliptiques $\mathbb{T}^2_{\tau'}$ et celle associée à la base $(\alpha, \alpha\tau)$ sont équivalentes. Mais la dernière est équivalente à $\mathbb{T}^2_{\tau}$. Par suite $\mathbb{T}^2_{\tau}$ est équivalente à $\mathbb{T}^2_{\tau'}$.

Inversement, supposons $\mathbb{T}^2_\tau$ et $\mathbb{T}^2_{\tau'}$ équivalentes, i.e. il existe un biholomorphisme $\Phi : \mathbb{T}^2_\tau \longrightarrow \mathbb{T}^2_{\tau'}$. Celui-ci se relève en un automorphisme $\widetilde{\Phi}(z) = \alpha z + \beta$ de $\mathbb{C}$. Le couple $(\alpha, \alpha\tau)$ est alors une base de $\Gamma_{\tau'}$; on doit donc avoir $1 = a_0\alpha + b_0\alpha\tau$ et $\tau' = c_0\alpha + d_0\alpha\tau$ avec $\begin{pmatrix} a_0 & b_0 \\ c_0 & d_0 \end{pmatrix} \in \mathrm{GL}(2, \mathbb{Z})$. Par suite :

$$\tau' = \frac{\tau'}{1} = \frac{\alpha(c_0 + d_0\tau)}{\alpha(a_0 + b_0\tau)} = \frac{d_0\tau + c_0}{b_0\tau + a_0} = \frac{a\tau + b}{c\tau + d}$$

où on a posé $a = d_0$, $b = c_0$, $c = b_0$ et $d = a_0$.

Comme la partie imaginaire de $\frac{a\tau+b}{c\tau+d}$ est $(ad - bc)\frac{\Im(\tau)}{|c\tau+d|^2}$ et que celles de τ et τ' sont positives, on a $ad - bc > 0$ c'est-à-dire $ad - bc = 1$, ce qui implique que la matrice $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ est en fait dans $\mathrm{SL}(2, \mathbb{Z})$.

□

À toute matrice $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2,\mathbb{R})$ on associe l'homographie du plan complexe $h(z) = \frac{az+b}{cz+d}$. Le groupe $\mathrm{SL}(2,\mathbb{R})$ agit donc sur $\mathbb{H}$; il y induit alors une action de son sous-groupe $\mathrm{SL}(2,\mathbb{Z})$.

Soient $s = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ et $t = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ les deux éléments de $\mathrm{SL}(2,\mathbb{Z})$ définissant les homographies de$\mathbb{H}$: $s(t) = -\frac{1}{z}$ et $t(z) = z + 1$. Ils vérifient $s^2 = \mathbf{1}$ (identité) et $(st)^3 = \mathbf{1}$. Il est démontré (par exemple dans [14]) que :

• Les éléments s et t engendrent le groupe $\mathrm{PSL}(2,\mathbb{Z})$ (dit ***groupe modulaire***), quotient de $\mathrm{SL}(2,\mathbb{Z})$ par le sous-groupe $\{I, -I\}$ où I est la matrice identité. En fait, s engendre un groupe G_1 isomorphe à $\mathbb{Z}/2\mathbb{Z}$ et st engendre un groupe G_2 isomorphe à $\mathbb{Z}/3\mathbb{Z}$ et $\mathrm{PSL}(2,\mathbb{Z})$ est le produit libre $G_1 * G_2$.

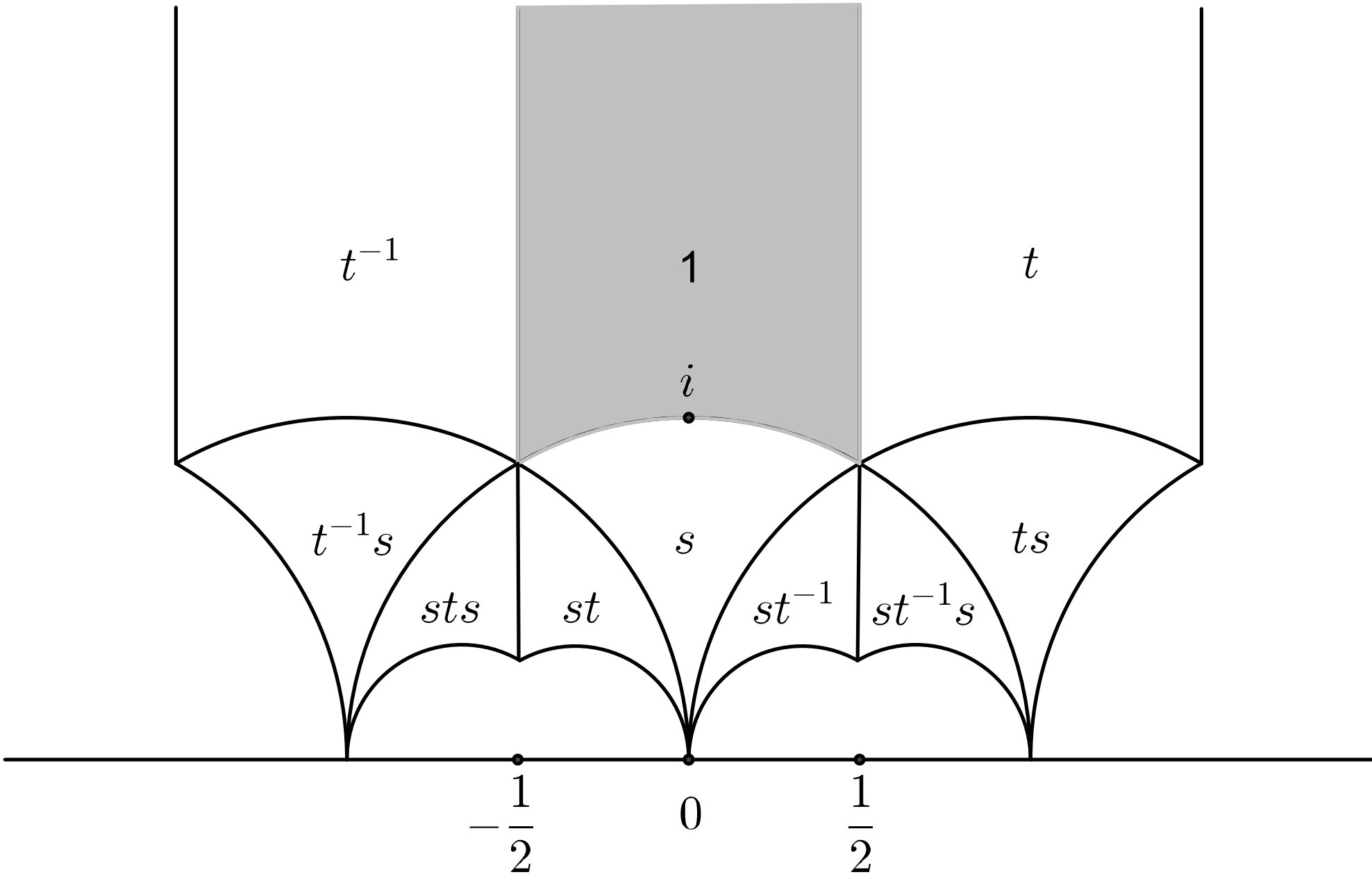
- La partie Δ (grisée sur le dessin qui suit) et définie par :

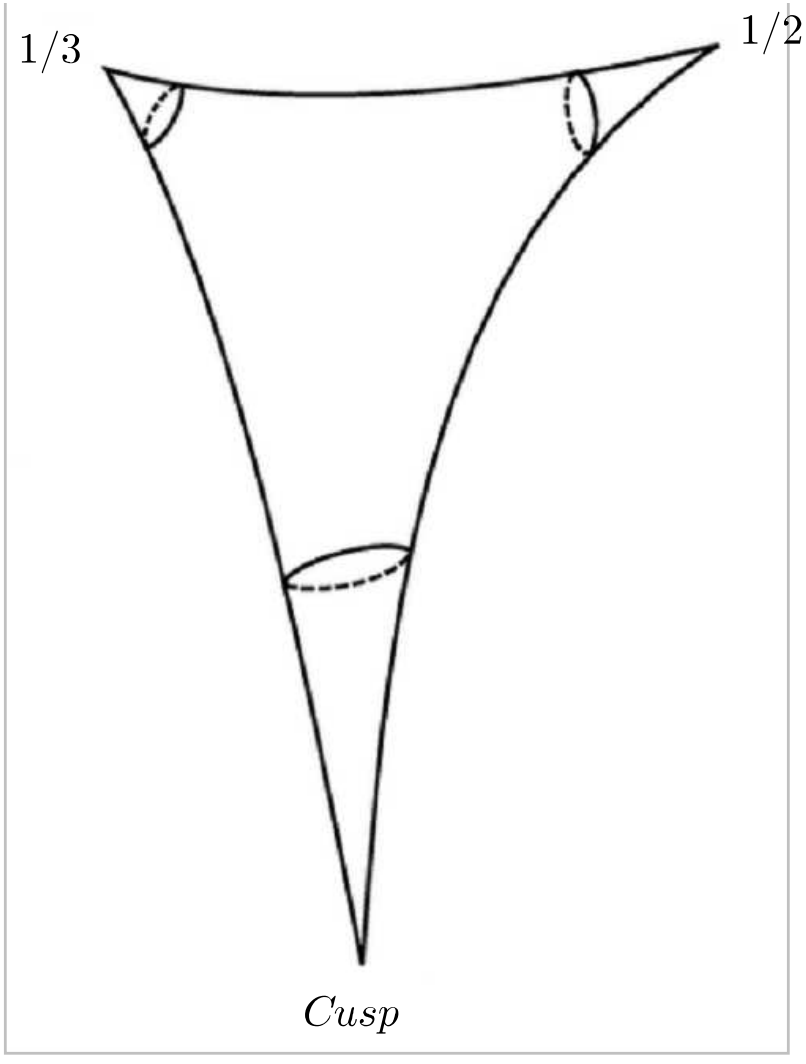
$$\Delta = \{z \in \mathbb{H} : |z| \geq 1 \text{ et } -\frac{1}{2} \leq \Re(z) \leq \frac{1}{2}\}$$

est un domaine fondamental de l'action de $\mathrm{PSL}(2,\mathbb{Z})$ sur $\mathbb{H}$.

La proposition qui précède dit que les classes d'équivalence de courbes elliptiques correspondent précisément aux orbites de l'action du groupe $\mathrm{PSL}(2,\mathbb{Z})$ sur le demi-plan $\mathbb{H}$ donc aux points du quotient $\mathcal{O} = \mathbb{H}/\mathrm{PSL}(2,\mathbb{Z})$ qu'on appelle ***orbifold modulaire***. Celle-ci est obtenue à partir du domaine fondamental Δ.

Tous ces éléments sont abondamment utilisés en arithmétique et en théorie des ***formes modulaires*** (voir [14] à cet effet).


t^{-1}
1
t
i
$t^{-1}s$
s
ts
sts
st
st^{-1}
$st^{-1}s$
$-\frac{1}{2}$
0
$\frac{1}{2}$



Orbifold modulaire : $\mathcal{O} = \mathbb{H}/PSL(2,\mathbb{Z})$

2.1. Les fonctions elliptiques

***Les fonctions elliptiques** sont importantes pour l'étude d'une courbe elliptique $\mathbb{T}_\tau$. L'une d'entre elles joue un rôle fondamental : elle permet de plonger $\mathbb{T}_\tau$ comme courbe lisse dans le plan projectif complexe $P^2(\mathbb{C})$ en la définissant dans celui-ci par une équation polynomiale explicite. C'est essentiellement ce dernier point qui motive le fait d'en parler (même sommairement) dans ce qui va suivre.*

Soit $\Gamma_\tau = \mathbb{Z} \oplus \tau\mathbb{Z}$ un réseau de $\mathbb{C}$ où $\tau = (1, \tau)$ avec $\tau \in \mathbb{H}$. On note $\mathbb{T}_\tau$ la courbe elliptique $\mathbb{C}/\Gamma_\tau$ et π la projection canonique $\mathbb{C} \longrightarrow \mathbb{T}_\tau$. L'action par translations de Γ_τ sur $\mathbb{C}$: $(\gamma, z) = (m + n\tau, z) \in \Gamma_\tau \times \mathbb{C} \longmapsto z + \gamma = z + m + n\tau \in \mathbb{C}$ induit une action sur toute fonction $\widetilde{f} : \mathbb{C} \longrightarrow \mathbb{C}$ donnée par $\widetilde{f}(z + \gamma) = \widetilde{f}(z + m + n\tau)$. On dira que $\widetilde{f}$ est Γ_τ-***invariante*** ou Γ_τ-***périodique*** si elle vérifie :

$$\widetilde{f}(z + \gamma) = \widetilde{f}(z) \quad \text{pour tout } z \in \mathbb{C} \text{ et tout } \gamma \in \Gamma_\tau.$$

Toute fonction Γ_τ-*invariante* $\widetilde{f}$ sur $\mathbb{C}$ induit donc une fonction f sur $\mathbb{T}_\tau$. Inversement, toute fonction f sur $\mathbb{T}_\tau$ définit une unique fonction $\widetilde{f} = f \circ \pi$ sur $\mathbb{C}$ invariante par l'action de Γ_τ. On a donc une identification naturelle entre l'espace des fonctions sur la courbe elliptique $\mathbb{T}_\tau$ et celui des fonctions Γ_τ-invariantes sur $\mathbb{C}$.

De façon évidente, on a les assertions suivantes :

(i) La fonction f est de classe C^k (avec $k \in \mathbb{N} \cup \{\infty\}$) si, et seulement si, $\widetilde{f}$ l'est.

(ii) Comme la projection $\mathbb{C} \xrightarrow{\pi} \mathbb{T}_\tau$ est holomorphe, f est holomorphe si, et seulement si, $\widetilde{f}$ l'est. Dans ce cas, $\widetilde{f}$ est bornée et par suite constante par le théorème de Liouville. La situation n'a alors pas beaucoup d'intérêt. Ce qui nous amène à demander un peu moins :

Definition

On appelle fonction elliptique sur $\mathbb{C}$ relativement au réseau Γ_τ toute fonction méromorphe Γ_τ-invariante ou, de façon équivalente, tout simplement une fonction méromorphe sur la courbe elliptique $\mathbb{T}_\tau$.

2.2. De telles fonctions existent bien sûr. Une manière de les construire consiste à utiliser des moyennes à l'aide de séries dont les termes sont indexés par les éléments du réseau. Par exemple en considérant, pour tout $z \in \mathbb{C}\backslash\Gamma_\tau$, la quantité formelle :

$$\wp(z) = \frac{1}{z^2} + \sum_{\gamma\in\Gamma_\tau\backslash\{0\}} \left(\frac{1}{(z-\gamma)^2} - \frac{1}{\gamma^2} \right).$$

On démontre que la famille $\{w_\gamma\}_{\gamma\in\Gamma_\tau\backslash\{0\}}$, avec $w_\gamma = \frac{1}{(z-\gamma)^2} - \frac{1}{\gamma^2}$, est uniformément sommable sur tout compact K de l'ouvert $\mathbb{C}\backslash\Gamma_\tau$.

Cela signifie qu'il existe une fonction $S : K \longrightarrow \mathbb{C}$ telle que, pour tout $\varepsilon > 0$, il existe une partie finie $J_0 \subset \Gamma_\tau \backslash \{0\}$ qui satisfait à la condition suivante : pour toute partie finie $J \subset \Gamma_\tau \backslash \{0\}$ vérifiant $J_0 \subset J$ on a :

$$\sup_{z \in K} \left| S(z) - \sum_{\gamma \in J} \left(\frac{1}{(z-\gamma)^2} - \frac{1}{\gamma^2} \right) \right| < \varepsilon.$$

Si on écrit chaque $\gamma \in \Gamma_\tau \backslash \{0\}$ sous la forme $\gamma = m + \tau n$ avec $(m, n) \in \mathbb{Z} \times \mathbb{Z} \backslash \{(0, 0)\}$, cela implique que la série double $\sum_{(m,n)\neq(0,0)} \left(\frac{1}{(z - m - \tau n)^2} - \frac{1}{(m + \tau n)^2} \right)$ est uniformément et absolument convergente sur K. Par suite la quantité $\wp(z)$ définit bien une fonction holomorphe sur l'ouvert $\mathbb{C} \setminus \Gamma_\tau$. Donc $\wp$ est une fonction méromorphe sur $\mathbb{C}$ ayant comme pôles les éléments du réseau Γ_τ ; tous ces pôles sont doubles. On peut aussi voir facilement que $\wp$ est une fonction paire *i.e.* elle vérifie $\wp(-z) = \wp(z)$ pour tout $z \in \mathbb{C} \setminus \Gamma_\tau$.

La série $\wp(z) = \frac{1}{z^2} + \sum_{\gamma \in \Gamma_\tau \setminus \{0\}} \left(\frac{1}{(z-\gamma)^2} - \frac{1}{\gamma^2} \right)$ étant uniformément convergente sur tout compact, on peut la dériver terme à terme. On obtient $\wp'(z) = -\sum_{\gamma \in \Gamma_\tau} \frac{2}{(z-\gamma)^3}$, expression qui montre que la fonction $\wp'$ est Γ_τ-invariante, i.e elle vérifie $\wp'(z+\gamma) = \wp'(z)$ pour tout $\gamma \in \Gamma_\tau$.

On en déduit que la fonction $z \longmapsto \wp(z+\gamma) - \wp(z)$ est constante. Ce sera en particulier le cas si on prend $\gamma = 1$ ou $\gamma = \tau$. Mais pour $z = -\frac{1}{2}$, on a $\wp(-\frac{1}{2}+1) - \wp(-\frac{1}{2}) = \wp(\frac{1}{2}) - \wp(\frac{1}{2}) = 0$ (on a utilisé la parité de $\wp$) ; la constante $\wp(z+1) - \wp(z)$ est donc nulle. En prenant cette fois-ci $z = -\frac{\tau}{2}$, on montre que la constante $\wp(z+\tau) - \wp(z)$ est nulle. Comme 1 et τ engendrent Γ_τ, on en déduit que, pour tout $\gamma \in \Gamma_\tau$, $\wp(z+\gamma) - \wp(z) = 0$ i.e. la fonction $\wp$ est Γ_τ-invariante. C'est donc une fonction elliptique relativement au réseau Γ_τ, et par suite une fonction elliptique sur $\mathbb{T}_\tau$. Sur cette courbe, $\wp$ a un seul pôle au point $\widehat{0}$ (image du réseau Γ_τ par la projection canonique $\pi : \mathbb{C} \longrightarrow \mathbb{T}_\tau$).

Definition

$\wp$ est appelée fonction de Weierstrass du réseau Γ_τ ou de la courbe elliptique $\mathbb{T}_\tau$.

2.3. Nous allons dire un mot de l'un des rôles fondamentaux de la fonction $\wp$: elle permet de réaliser une courbe elliptique comme ***courbe algébrique*** dans un espace projectif.

Une courbe complexe M dans $\mathbb{C}^2$ est la courbe de niveau d'une fonction holomorphe $f : \mathbb{C}^2 \longrightarrow \mathbb{C}$ dont la différentielle complexe $\partial_z f$ est non nulle en tout point $z \in M$. Sa particularité est que M est l'ensemble des points de $\mathbb{C}^2$ dont les coordonnées (z_1, z_2) vérifient une relation concrète, algébrique ou autre. On dira alors que M est ***plongée*** dans $\mathbb{C}^2$. Malheureusement, il n'est pas possible de faire cela pour une courbe complexe compacte et donc non plus pour une courbe elliptique.

(On dit que $f : M \longrightarrow \mathbb{C}^d$ (avec $d \geq 2$) est un ***plongement holomorphe*** si f est une application holomorphe, injective, à image fermée et si, pour tout point $z \in M$, la différentielle complexe $\partial_z f : T^{10}_z M \simeq \mathbb{C} \longrightarrow \mathbb{C}^d$ est injective.)

Mais on peut plonger une courbe elliptique dans le plan projectif $P^2(\mathbb{C})$. On va en expliquer les grandes étapes.

Le ***plan projectif complexe*** $P^2(\mathbb{C})$ est l'ensemble des classes pour la relation d'équivalence sur $\mathbb{C}^3\backslash\{0\}$: $w \sim w'$ s'il existe $\lambda \in \mathbb{C}^*$ tel que l'on ait $w' = \lambda w$. On notera $p : \mathbb{C}^3\backslash\{0\} \longrightarrow P^2(\mathbb{C})$ la projection canonique. Les ***coordonnées homogènes*** d'un point de $P^2(\mathbb{C})$ seront notées $[w_1, w_2, w_3]$ (avec $(w_1, w_2, w_3) \in \mathbb{C}^3\backslash\{0\}$) ; elles sont définies à un facteur multiplicatif non nul près.

Comme pour le cas réel, pour k variant dans $\{1, 2, 3\}$, les ensembles $U_k = p(\widetilde{U}_k)$ avec $\widetilde{U}_k = \{(w_1, w_2, w_3) \in \mathbb{C}^3 : w_k \neq 0\}$ forment un recouvrement ouvert de $P^2(\mathbb{C})$ et les applications $\varphi_k : \mathbb{C}^2 \longrightarrow U_k$ définies ci-dessous sont des cartes locales :

$$\begin{cases} \varphi_1(u, v) = [1, u, v] \\ \varphi_2(u, v) = [u, 1, v] \\ \varphi_3(u, v) = [u, v, 1]. \end{cases}$$

On peut montrer que la fonction $\wp$ vérifie l'équation différentielle :

$$\wp'(z)^2 - 4\wp(z)^3 + a\wp(z) + b = 0$$

où a et b sont les constantes complexes données (en fonction des éléments γ du réseau Γ_τ) par les séries :

$$a = 60 \sum_{\gamma \in \Gamma_\tau \setminus \{0\}} \frac{1}{\gamma^4} \quad \text{et} \quad b = 140 \sum_{\gamma \in \Gamma_\tau \setminus \{0\}} \frac{1}{\gamma^6}.$$

Soit $Q : \mathbb{C}^3 \setminus \{0\} \longrightarrow \mathbb{C}$ la fonction polynôme définie par :

$$Q(w_1, w_2, w_3) = w_1 w_2^2 - 4w_3^3 + a w_1^2 w_3 + b w_1^3.$$

L'ensemble $\{(w_1, w_2, w_3) \in \mathbb{C}^3 \setminus \{0\} : Q(w_1, w_2, w_3) = 0\}$ est une partie fermée non vide de $\mathbb{C}^3 \setminus \{0\}$. Elle est invariante par multiplication par une constante complexe non nulle et définit une partie fermée $\mathcal{C}$ dans $P^2(\mathbb{C})$.

(Sur le plan affine $H = \{w_1 = 1\}$ de $\mathbb{C}^3$, la trace de $\mathcal{C}$ est donnée par la formule $y^2 = 4x^3 - ax - b$ où $x = w_3$ et $y = w_2$, une relation qu'on utilise aussi pour étudier une courbe elliptique : c'est la ***forme de Weierstrass*** de l'équation de la courbe.) La différentielle (au sens complexe) $\partial_w Q$ de la fonction Q en un point $w = (w_1, w_2, w_3)$ est donnée par les dérivées partielles :

$$\begin{cases} \frac{\partial Q}{\partial w_1}(w) = w_2^2 + 2aw_1w_3 + 3bw_1^2 \\ \\ \frac{\partial Q}{\partial w_2}(w) = 2w_1w_2 \\ \\ \frac{\partial Q}{\partial w_3}(w) = aw_1^2 - 12w_3^2. \end{cases}$$

On voit alors clairement qu'en chaque point $w = (w_1, w_2, w_3) \neq (0, 0, 0)$, l'application linéaire $\partial_w Q : \mathbb{C}^3 \longrightarrow \mathbb{C}$ est de rans 1, et par suite surjective ; donc Q est de rang maximum. En fait, comme la quantité $a^3 - 27b^2$ est non nulle, $\mathcal{C}$ est une courbe algébrique lisse dans $P^2(\mathbb{C})$.

La fonction $\wp$ et sa dérivée $\wp'$ sont holomorphes sauf au point $\widehat{0}$ (image de Γ_τ par la projection canonique $\mathbb{C} \longrightarrow \mathbb{T}_\tau$) en lequel elles admettent un pôle double pour la première et d'ordre 3 pour la seconde. On a alors le :

Théorème

L'application Ψ *de* $\mathbb{T}_\tau$ *dans le plan projectif* $P^2(\mathbb{C})$ *définie par :*

$$\Psi(z) = \begin{cases} [1, \wp'(z), \wp(z)] & \text{si } z \neq \widehat{0} \\ [0, 1, 0] & \text{si } z = \widehat{0} \end{cases}$$

réalise un bihomorphisme de la courbe elliptique $\mathbb{T}_\tau$ *sur la courbe algébrique lisse* $\mathcal{C}$.

2.4. Le cas réel

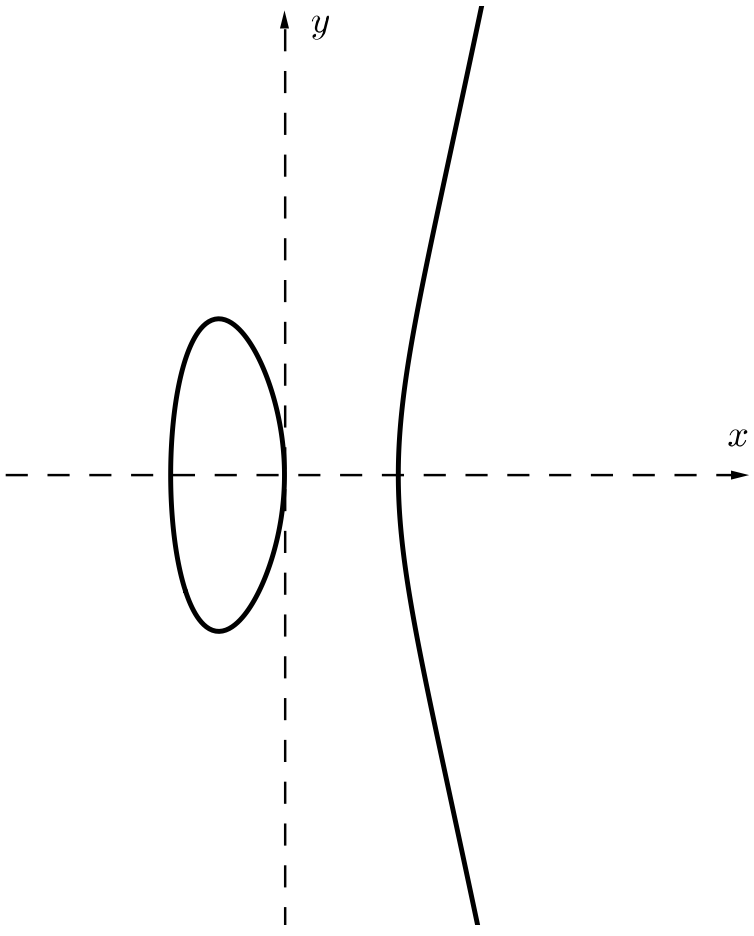
L'équation dans $\mathbb{R}^2$ d'une ***courbe elliptique réelle*** a la forme de Weierstrass qu'on a évoquée ci-dessus, c'est-à-dire :

$$y^2 = 4x^3 - ax - b$$

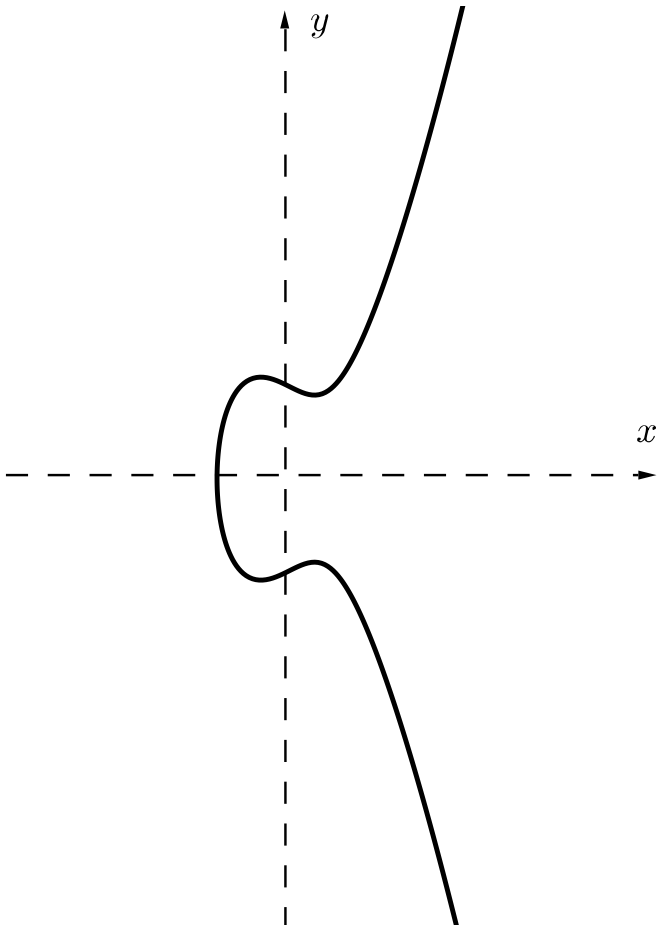
où a et b sont des réels tels que $a^3 - 27b^2 \neq 0$. Cette dernière condition dit que la courbe n'a aucun ***point singulier*** (un bon exercice de calcul différentiel).

Voici (dessins qui suivent) quatre exemples de courbes dans le plan euclidien dont deux sont des courbes elliptiques et les deux autres ne le sont pas.

Deux courbes elliptiques dans le plan $\mathbb{R}^2$.

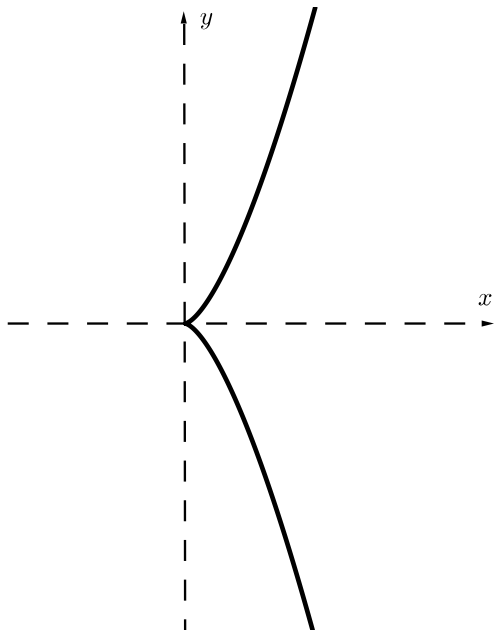


$y^2 = 4x^3 - 6x$

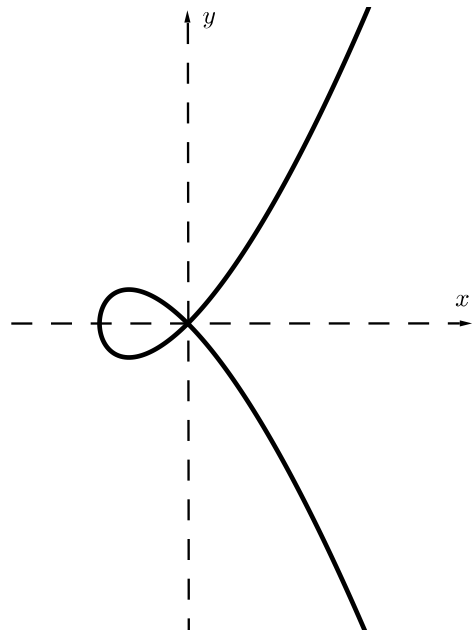


$y^2 = 4x^3 - x + 1$

Deux courbes non elliptiques. La première a son équation sous la forme de Weierstrass mais elle est singulière au point $(0,0)$; la deuxième est aussi singulière au même point (et son équation n'a pas la forme de Weierstrass).



$y^2 = 4x^3$



$y^2 = x^3 + x^2$

BIBLIOGRAPHIE

[1] Ahlfors, L.V. *Complex Analysis*. Collection *Mathematics Series*, McGraw-Hill (1979).

[2] Cartan, H. *Théorie élémentaire des fonctions analytiques d'une ou plusieurs variables complexes*. Collection *Enseignement des Sciences*, Hermann (1985).

[3] El Kacimi Alaoui, A. *Variable complexe et surfaces riemanniennes.* Références Sciences, Ellipses (2021).

[4] Farkas, H.M. & Kra, I. *Riemann Surfaces.* GTM 71 (1980), Springer-Verlag.

[5] Forster, O. *Lectures on Riemann Surfaces.* GTM 81 (1981), Springer-Verlag.

[6] Freitag, E. *Hilbert Modular Forms.* Springer-Verlag, (1990).

[7] Hörmander, L. *An Introduction to Complex Analysis in Several Variables*. D. Van Nostrand Compagny. Inc. (1966).

[8] Jones, G. & Singerman, D. *Complex Functions. An algebraic and geometric viewpoint.* Cambridge University Press, (1987).

[9] Krantz, S. G. *Geometric Function Theory*. Birkhäuser (2006).

[10] Lavrentiev, M. & Chabat, B. *Méthodes de la théorie des fonctions d'une variable complexe*. Éditions Mir, Moscou (1972).

[11] Maass, H. *Lectures on Modular Functions of one Complex Variable.* Tata Institute of Fundamental Research, (1964).

[12] Saint-Gervais, H. P. *Uniformisation des surfaces de Riemann*. ENS Éditions, Lyon (2010).

[13] Schlichenmaier, M. *An Introduction to Riemann Surfaces, Algebraic Curves and Moduli Spaces*. Lecture Notes in Physics 322, Springer-Verlag (1979).

[14] Serre, J.-P. *Cours d'arithmétique*. Collection Sup, PUF (1970).

[15] Vidonne, R. *Groupe circulaire, rotations et quaternions*. Collections CAPES et Agrégation, Ellipses (2001).