Table des matières

COURS I
VARIÉTÉS ABÉLIENNES : INTRODUCTION ET HISTOIRE

I.1. Genèse historiques des courbes elliptiques

I.1.a. Intégrales elliptiques. —

I.1.1. — La première courbe algébrique qui s'impose à l'esprit humain est le cercle :

$$x^2 + y^2 = 1.$$

Un problème qui a irrigué les commencements des mathématiques est de déterminer la longueur du cercle ou plus généralement d'un arc de cercle. En termes modernes, cela revient à calculer l'intégrale :

$$u = \int_0^t \frac{dx}{\sqrt{1-x^2}}, t \in]-1,1[$$

et on obtient la fonction $u = \arcsin(x)$. Or c'est plutôt la fonction inverse qui est intéressante, la fonction sinus.

La méthode dite de Jacobi permet ainsi de montrer abstraitement que la fonction :

$$t \mapsto u = \int_0^t \frac{dx}{\sqrt{1-x^2}},$$

admet une fonction réciproque $t(u) =: \sin(u)$ définie sur tout le plan complexe, périodique de péridode 2π, solution de l'équation différentielle :

$$\left(\frac{dt}{du}\right)^2 = 1 - u^2.$$

Remarque I.1.2. — Le problème est que la fonction $\sqrt{1-x^2}$ n'admet pas de détermination unique pour $x \in \mathbb{C} - \{-1, 1\}$. Une telle détermination existe si on se place dans l'ouvert (simplement connexe)

$$\mathbb{C} - \big(]-\infty, 1] \sqcup [1, \infty[\big).$$

On peut alors réaliser l'inversion de la fonction u bien déterminée sur cet ouvert, et obtenir la fonction sin par prolongement analytique.

I.1.3. — La généralisation naturelle du problème précédent, qui a été attaqué au cours des XVIIème et XVIIIème siècles, est de déterminer la longueur d'un arc d'ellipse, d'équation

$$\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1.$$

Si l'on pose $e = \sqrt{1 - (b/a)^2}$, appelé l'*excentricité* (1) de l'ellipse, on obtient facilement que cela revient à calculer l'intégrale :

$$u = \int_0^t \frac{\sqrt{1 - e^2.x^2}}{\sqrt{1 - x^2}} dx, t \in]-1, 1[.$$

La détermination de cette intégrale à l'aide d'une série convergente a été effectuée par Wallis, Newton puis Euler, toujours aux XVIIème et XVIIIème siècle. Les mathématiciens a cette époque cherchaient de plus à exprimer la fonction $u(t)$ en termes de fonctions élémentaires t^a, $\log(t)$, e^t. Liouville (1837) démontra que c'est impossible.

La solution qui s'impose est de considérer cette intégrale comme une fonction à part entière. (2) Mais comme dans le cas du cercle, la fonction la plus naturelle est sa réciproque.

Ainsi, Abel (1827) et indépendamment Jacobi (1829) (4) attaque la question de cette intégrale associée à une ellipse du point de vue des fonctions complexes, en considérant sa réciproque. Le cadre naturel de leur travail est le suivant :

Définition I.1.4. — Considérons $R(x, y)$ une fraction rationnelle des variables x et y, et $P(x)$ un polynôme en x de degré 3 ou 4 sans racine multiple. On appelle *intégrale elliptique* la fonction :

$$u = \int_0^t R\left(x, \sqrt{P(x)}\right) dx.$$

Exemple I.1.5. — L'intégrale introduite précédemment pour calculer la longueur d'un arc d'ellipse est bien de cette forme :

$$u(t) = \int_0^t \frac{1 - e^2.x^2}{\sqrt{(1 - x^2)(1 - e^2.x^2)}} dx.$$

Dans la classification de Legendre (voir remarque ci-dessous), c'est une intégrale elliptique de deuxième espèce.

Remarque I.1.6. —

1. La première étude systématique des intégrales dégagées dans la définition précédente est du à Lagrange (1784) (5).
2. L'usage de l'adjectif « elliptique » est du à Legendre (6) qui fait une étude monumentale de ces intégrales en tant que fonctions à part entières. Il montre notamment qu'on peut les classifier en « trois espèces ».

---

1. Plus e est proche de 0, plus l'ellipse ressemble à un cercle : ce qui justifie la terminologie.
2. Une fonction *transcendante* suivant une terminologie répandue par Newton, qui opposait ce genre de fonction, et plus exactement les courbes qu'elles définissent à celles acceptées par Descartes dans sa géométrie, qui s'était volontairement restreint aux courbes admettant une paramétrisation (implicite) rationnelle. D'après ses dires, il s'agissait, à l'époque d'une choix plus pragmatique que dogmatique :

> Et j'espère que nos neveux me sauront gré, non seulement des choses que j'ai ici expliquées, mais aussi de celles que j'ai omises volontairement, afin de leur laisser le plaisir de les inventer. (3)

4. Coïncidence : ces deux mathématiciens avaient 25 ans quand leurs travaux furent publiés.
5. Une nouvelle methode de calcul integral pour les differentielles affectees d'un radical carre sous lequel la variable ne passe pas le quatrieme degre. (sic) (Mémoires de l'Académie royale des Sciences de Turin, t. II, 1784-1785)
6. Traité des fonctions elliptiques et des intégrales eulériennes, 1925.

I.1.b. Fonctions elliptiques. — La méthode d'Abel et Jacobi dans l'étude des intégrales elliptiques peut-être résumée par le théorème suivant, qui prolonge l'exemple explicité dans le cas de la longueur d'un arc de cercle :

Théorème I.1.7. — *(Abel, Jacobi) Pour toute fonction $u(t)$ exprimée par une intégrale elliptique, il existe une fonction inverse $t(u)$ qui est méromorphe sur $\mathbb{C}$ doublement périodique : il existe $\omega_1, \omega_2 \in \mathbb{C}^*$ tels que :*

$$t(z+\omega_1) = t(z+\omega_2) = t(z)$$

et $(\omega_1/\omega_2) \notin \mathbb{R}$.

Exemple I.1.8. — La réciproque de l'intégrale elliptique (de première espèce, dépendant du paramètre k) :

$$u : t \mapsto \int_0^t \frac{dx}{\sqrt{(1-x^2)(1-k^2.x^2)}}$$

est notée $\mathrm{sn}(u,k)$ et appelée la *fonction elliptique de Jacobi.* Notons qu'elle généralise la fonction sinus dans le sens ou $\mathrm{sn}(u,0) = \sin(u)$.

Comme annoncé, l'idée géniale d'Abel et de Jacobi est de porter leur intérêt sur la fonction réciproque obtenue dans leur théorème. En termes modernes, on introduit la définition suivante :

Définition I.1.9. —
- Un *réseau* dans $\mathbb{C}$ est un sous-groupe $\Lambda \subset \mathbb{C}$, qui est libre de rang 2 sur $\mathbb{Z}$ et engendre $\mathbb{C}$ sur $\mathbb{R}$: $\Lambda \otimes_{\mathbb{Z}} \mathbb{R} = \mathbb{C}$.
- Une *fonction elliptique* f est une fonction méromorphe sur $\mathbb{C}$ à valeurs complexes telle qu'il existe un réseau Λ vérifiant :

$$\forall \omega \in \Lambda, f(z+\omega) = f(z).$$

On dit encore que f est Λ-*elliptique.*

Pour une fonction elliptique f donnée, il existe un unique réseau maximal Λ satisfaisant les conditions précédentes pour f. On l'appelle le réseau associé à f.

I.1.10. — Fixons un réseau $\Lambda \subset \mathbb{C}$.

A un entier $n > 0$ pair et au réseau Λ, on associe une série dite *série d'Eisenstein de poids n* :

$$G_n = \sum_{\omega \in \Lambda^*} \omega^{-n}.$$

Cette série est absolument convergente. [7]

On définit la fonction elliptique de Weiestrass, associée à Λ :

$$\mathfrak{p}(z) = \frac{1}{z^2} + \sum_{\omega \in \Lambda^*} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right).$$

Cette série est absolument convergente sur tout compact de $\mathbb{C} - \Lambda$. [8] Elle se prolonge donc en une fonction méromorphe sur $\mathbb{C}$ ayant un pôle (d'ordre 2) en tout point de Λ. Notons de plus que $\mathfrak{p}$ est paire.

La dérivée de $\mathfrak{p}$ s'exprime grâce à la série :

$$\mathfrak{p}'(z) = -2. \sum_{\omega \in \Lambda^*} \frac{1}{(z-\omega)^2}$$

---

7. Il suffit d'estimer le nombre de points de Λ dans un disque de rayon $r > 0$ arbitrairement grand, soit $a.\pi.r^2$.
8. Pour $|z|$ borné, le module de son terme général est équivalent à $2|z|/|\omega|^3$ et on peut alors utiliser la convergence absolue de G_2.

qui définit bien une fonction méromorphe sur $\mathbb{C}$.[9] De manière évidente, cette fonction est Λ-elliptique. On en déduit que pour $\omega \in \Lambda$ fixé, la fonction $\mathfrak{p}(z+\omega) - \mathfrak{p}(z)$ est constante. Du fait que $\mathfrak{p}$ est paire, et pour $z = \omega/2$, on déduit que cette constante est nulle : $\mathfrak{p}$ est donc une fonction Λ-elliptique.

On voisinage de 0, la fonction $\mathfrak{p}(z)$ admet un développement en série de Laurent de la forme :[10]

$$\mathfrak{p}(z) = z^{-2} + \sum_{k=1}^{\infty}(2k+1)G_{2k+2}.z^{2k}. \tag{I.1}$$

Pour simplifier les notations, on pose : $g_k = (2k+1).G_{2k+2}$.

On en déduit le résultat suivant :

Proposition I.1.11. — *Pour tout $z \in \mathbb{C} - \Lambda$, la relation suivante est vérifiée :*

$$\mathfrak{p}'(z)^2 = 4.\mathfrak{p}(z)^3 - g_2.\mathfrak{p}(z) - g_3.$$

Démonstration. — Il suffit d'utiliser le développement de Laurent (I.1) pour obtenir que la fonction

$$\mathfrak{p}'(z)^2 - 4.\mathfrak{p}(z)^3 - g_2.\mathfrak{p}(z) - g_3$$

est holomorphe sur $\mathbb{C}$. Or elle est Λ-elliptique, donc bornée sur $\mathbb{C}$: le théorème de Liouville assure qu'elle est constante. Il ne reste plus qu'à constater que cette fonction évaluée en 0 est nulle. □

Renversant le principe qu'on a déjà vu pour le cercle, on déduit de la proposition précédente que la fonction elliptique $\mathfrak{p}$ est la réciproque de l'intégrale elliptique :

$$u = \int_0^t \frac{dx}{\sqrt{4.x^3 - g_2.x - g_3}}. \tag{I.2}$$

Remarque I.1.12. — Weierstrass montre que toute fonction elliptique peut s'exprimer comme une fraction rationnelle en $\mathfrak{p}(z)$ et $\mathfrak{p}'(z)$ (voir [**Sil09**][VI.3.2]).

I.1.c. Courbes elliptiques complexes. —

I.1.13. — Reprenons les notations du paragraphe I.1.10. Il résulte de la proposition I.1.11 que la fonction,

$$\phi : \mathbb{C} - \Lambda \to \mathbb{P}^2(\mathbb{C}), z \mapsto (\mathfrak{p}(z) : \mathfrak{p}'(z) : 1) \tag{I.3}$$

a son image incluse dans l'ensemble algébrique projectif solution de l'équation homogène :

$$(E) : y^2.z = 4.x^3 - g_2.x.z^2 - g_3.z^3.$$

Définition I.1.14. — On appelle *courbe elliptique* associée à Λ la courbe E_Λ du plan projectif complexe $\mathbb{P}^2_{\mathbb{C}}$ d'équation homogène (E).

Une courbe algébrique complexe est dite *elliptique* si elle est isomorphe à une courbe elliptique associée à un réseau de $\mathbb{C}$.

Remarque I.1.15. —

- On peut voir que l'application ϕ est surjective sur l'ensemble algébrique (affine) $E_\Lambda(\mathbb{C}) - \{(0 : 1 : 0)\}$ (voir [**Sil09**, 3.6]). Ainsi, la courbe E_Λ admet pour paramétrisation $z \mapsto (\mathfrak{p}(z) : \mathfrak{p}'(z) : 1)$, donnée par des fonctions elliptiques, ce qui justifie la terminologie : une courbe complexe algébrique projective est elliptique si elle admet une paramétrisation par des fonctions elliptiques (*i.e.* de la forme (I.3).

---

9. En utilisant à nouveau le fait que G_2 est absolument covergente.
10. Il suffit d'utiliser l'égalité suivante, valable pour $|z| < |\omega|$:

$$\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} = \frac{1}{\omega^2}\left(\frac{1}{(z/\omega - 1)^2} - 1\right) = \sum_{k=1}^{\infty}(k+1).\frac{z^k}{\omega^{k+2}}.$$

– On peut montrer la relation : $g_2^3 - 27.g_3^2 \neq 0$. (voir [**Sil09**, 3.6], modulo une petite faute de frappe dans l'énoncé). Réciproquement, on peut montrer que pour tout couple de nombres complexes (a, b) vérifiant la relation

$$\Delta(a,b) := a^3 - 27b^2 \neq 0,$$

il existe un réseau $\Lambda \subset \mathbb{C}$ tel que $a = g_2(\Lambda)$, $b = g_3(\Lambda)$.

Autrement dit, les courbes elliptiques complexes sont exactement les courbes algébriques projectives d'équation :

$$(E) : y^2.z = 4.x^3 - a.x.z^2 - b.z^3$$

où (a, b) sont des couples de nombres complexes vérifiant $\Delta(a, b) \neq 0$. Le nombre $\Delta(a, b)$ est appelé le discriminant de la courbe. (11)

I.1.16. — *Application d'Abel-Jacobi.*– Considérons les notations de la définition précédente et revenons au travaux d'Abel et Jacobi.

On a déjà vu que l'image de ϕ est contenue dans l'ensemble $E_\Lambda(\mathbb{C})$ des points complexes de la courbe E_Λ. On peut de plus voir les propriétés suivantes (voir à nouveau [**Sil09**, 3.6]) :

– ϕ est surjective sur $E_\Lambda(\mathbb{C}) - \{(0 : 1 : 0)\}$.
– $\phi(z) = \phi(z')$ équivaut à $(z - z') \in \Lambda$.

On en déduit donc un isomorphisme :

$$\tilde{\phi} : \mathbb{C}/\Lambda \to E_\Lambda(\mathbb{C})$$

égal à ϕ sur $\mathbb{C} - \Lambda$ et envoyant 0 sur le point à l'infini $(0 : 1 : 0)$. Cet isomorphisme peut se traduire par l'interprétation suivante des intégrales elliptiques de la forme (I.2).

– On pose $y^2 = 4.x^3 - g_2 - g_3$. On note $O = (0 : 1 : 0)$ le point à l'infini de $E_\Lambda(\mathbb{C})$. L'intégrale

$$\int_\infty^t \frac{dx}{y}$$

peut être comprise comme une intégrale de la forme

$$\int_{\gamma(P)} \omega$$

où $\gamma(P)$ est un arc de la courbe $E_\Lambda(\mathbb{C})$ allant du point O au point $P = (\mathfrak{p}(t) : \mathfrak{p}(t) : 1)$ et $\omega = \frac{dx}{y}$ est une forme différentielle sur $E_\Lambda(\mathbb{C})$.

On aimerait donc la voir comme une fonction :

$$\psi : E_\Lambda(\mathbb{C}) \to \mathbb{C}, P \mapsto \int_{\gamma(P)} \omega.$$

– La fonction ψ n'est pas bien définie : l'intégrale qui apparaît ci-dessus dépend du choix d'un arc de la courbe $E_\Lambda(\mathbb{C})$ joignant O à P. Par contre, du fait que $\mathfrak{p}$ est la réciproque de l'intégrale (I.2), on obtient la relation : $\phi \circ \psi(P) = P$. Du fait que ϕ est un isomorphisme, on déduit que la fonction multi-valuée ψ est bien définie si l'on considère ses valeurs modulo Λ. Autrement dit, la fonction :

$$\tilde{\psi} : E_\Lambda(\mathbb{C}) \to \mathbb{C}/\Lambda, P \mapsto \int_{\gamma(P)} \omega \mod \Lambda$$

est bien définie. Elle est réciproque de $\tilde{\phi}$. On l'appelle l'*application d'Abel-Jacobi* associée à E_Λ.

L'ensemble $\mathbb{C}/\Lambda$ peut être muni d'une structure de variété analytique. On l'appelle la *variété jacobienne* associée à la courbe elliptique E_Λ.

11. Lorsque $\Delta(a, b) = 0$, la courbe algébrique d'équation (E) est singulière.

I.1.d. Théorèmes d'addition. —

I.1.17. — Le couple d'isomorphismes $(\tilde{\phi}, \tilde{\psi})$ montre que l'ensemble de points $E_\Lambda(\mathbb{C})$ admet une structure de groupe.[12] C'est un phénomène remarquable qui remonte bien avant les considérations de la géométrie algébrique moderne.

Revenons à l'intégrale circulaire : on a une relation d'addition évidente en termes de la fonction sinus :

$$\int_0^{\sin(u_1)} \frac{dx}{\sqrt{1-x^2}} + \int_0^{\sin(u_2)} \frac{dx}{\sqrt{1-x^2}} = \int_0^{\sin(u_1+u_2)} \frac{dx}{\sqrt{1-x^2}}.$$

On en déduit la formule suivante pour l'addition de l'intégrale "circulaire" :

$$\int_0^{t_1} \frac{dx}{\sqrt{1-x^2}} + \int_0^{t_2} \frac{dx}{\sqrt{1-x^2}} = \int_0^{F(t_1,t_2)} \frac{dx}{\sqrt{1-x^2}}.$$

où

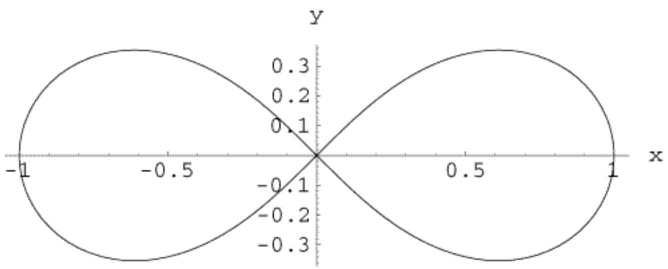
$$F(t_1,t_2) = t_1.\sqrt{1-t_2^2} + t_2.\sqrt{1-t_1^2}.$$

Il est remarquable que F est une fonction algébrique de t_1 et t_2.[13]

I.1.18. — L'étape suivante, historiquement, avant d'arriver aux cas des intégrales elliptiques générales, passe par une courbe algébrique dont je n'ai pas encore parlée : la *lemniscate.*[14] C'est encore l'ensemble algébrique défini par la relation

$$(x^2+y^2)^2 = x^2 - y^2$$

dont voici la représentation graphique :



L'intégrale permettant de calculer la longueur d'un arc de la lemniscate partant de l'origine est la suivante :

$$\int_0^t \frac{dx}{\sqrt{1-x^4}}, t \in [0,1[.$$

On reconnaît là une intégrale elliptique.[15] Fagnano, en 1718, découvre une formule de doublement d'un arc de la lemniscate :

$$2.\int_0^t \frac{dx}{\sqrt{1-x^4}} = \int_0^{G(t)} \frac{dx}{\sqrt{1-x^4}}$$

où l'on a posé :

$$G(t) = \frac{2.\sqrt{1-t^4}}{1+t^4}.$$

Il s'agit encore d'une expression algébrique.[16]

---

12. Notons au passage que le point à l'infini $O = (0:1:0)$ est par définition l'élément neutre de cette loi de groupe.

13. Utiliser les relations trigonométriques usuelles pour calculer $\sin(u+v)$.

14. Parfois appelée lemniscate de Benouilli, les frères Bernouilli ayant été les premiers a en introduire une définition différentielle et à l'utiliser dans le problème de l'isochrone paracentrique formulé par Leibniz.

15. Dans la classification de Legendre, il s'agit d'une intégrale elliptique de première espèce.

16. Pour obtenir cette formule, on fait le changement de variable : $x = 2y\sqrt{1-y^4}/(1+y^4)$.

I.1.19. — Euler rapporte le manuscrit de Fagnano en 1751 devant l'académie des sciences de Berlin. Fascina par la formule de Fagnano, Euler en obtient une généralisation s'appliquant aussi à l'addition des intégrales elliptiques de première espèce.

Reprenons un polynôme $P(x) = 4.x^3 - g_2.x - g_3$. Alors la *formule d'addition d'Euleur* s'écrit comme suit :

$$\int_0^{t_1} \frac{dx}{\sqrt{P(x)}} + \int_0^{t_2} \frac{dx}{\sqrt{P(x)}} = \int_0^{F(t_1,t_2)} \frac{dx}{\sqrt{P(x)}}$$

où l'on a posé :

$$F(t_1, t_2) = \frac{1}{4}.\left(\frac{\sqrt{P(t_1)} - \sqrt{P(t_2)}}{t_1 - t_2}\right)^2 - t_1 - t_2$$

Considérons maintenant un réseau Λ, $\mathfrak{p}$ la fonction elliptique de Weierstrass qui lui est associé et supposons : $g_2 = g_2(\Lambda)$, $g_3 = g_3(\Lambda)$. Compte tenu du fait que $\mathfrak{p}$ est la réciproque de l'intégrale elliptique ci-dessus, on peut réinterpréter la formule d'addition précédente comme suit :

$$\mathfrak{p}(z_1) + \mathfrak{p}(z_2) + \mathfrak{p}(z_1 + z_2) = \frac{1}{4}.\left(\frac{\mathfrak{p}'(z_1) - \mathfrak{p}'(z_2)}{\mathfrak{p}(z_1) - \mathfrak{p}(z_2)}\right)^2.$$

Cette forme de la formule d'Euler est encore appelée *formule de Weierstrass* car c'est Weierstrass qui l'a dégagée.

En utilisant par ailleurs la relation de la proposition I.1.11, on en déduit la relation suivante :

$$\begin{vmatrix} 1 & \mathfrak{p}(z_1) & \mathfrak{p}'(z_1) \\ 1 & \mathfrak{p}(z_2) & \mathfrak{p}'(z_2) \\ 1 & \mathfrak{p}(z_3) & \mathfrak{p}'(z_3) \end{vmatrix} = 0 \tag{I.4}$$

si $z_1 + z_2 + z_3 = 0$, modulo Λ.

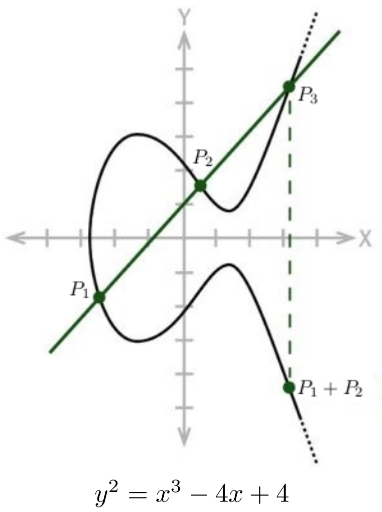
Notons que d'après la définition de la loi de groupe sur $E_\Lambda(\mathbb{C})$ via l'isomorphisme d'Abel-Jacobi, le point de E_Λ de paramétré z_3 est l'opposé de la somme des points paramétrés respectivement par z_1 et z_2. La relation précédente donne une relation algébrique entre les coordonnées de ces points : autrement dit la loi de groupe de $E_\Lambda(\mathbb{C})$ est algébrique. On obtient ainsi un morphisme de schémas

$$m : E_\Lambda \times E_\Lambda \to E_\Lambda$$

qui sur les points complexes redonne la multiplication considérée au début de cette section.

Notons que la relation (I.4) traduit en fait une relation de colinéarité des points P_1, P_2, P_3 de paramètres respectifs z_1, z_2, z_3.

On en déduit la traduction géométrique de la loi de groupe d'une courbe elliptique, traduisant la relation $P_1 + P_2 + P_3 = 0$ et exprimée dans la figure suivante :



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

I.2. Variétés abéliennes complexes

I.2.a. Intégrales abéliennes. — Abel et Jacobi ne se sont pas limités aux intégrales elliptiques.

Définition I.2.1. — On appelle *intégrale abéliennes* toute intégrale de la forme

$$u = \int R(x, y)dx$$

où R est une fraction rationnelle de x et y et ces deux variables sont liées par une relation algébriques $j(x, y) = 0$, j polynôme de degré arbitraire.

Exemple I.2.2. — Le cas où $j(x, y) = y2 - P(x)$ où $P(x)$ est sans racine multiple de degré 3 ou 4 correspond donc au cas des intégrales elliptiques.

Abel et Jacobi avait en particulier considéré le cas où le degré de $P(x)$ est arbitraire. L'intégrale ainsi obtenu est alors dite « hyper-elliptique ».

I.2.b. Jacobiennes (cas des courbes planes). —

I.2.3. — Considérons le cas d'une intégrale elliptique de la forme :

$$u = \int_{\infty}^{t} \frac{dx}{\sqrt{P(x)}} \tag{I.5}$$

où $P(x) = a_0 + a_1.x + ... + a_d.x^d$ est un polynôme sans racine multiple mais de degré d arbitraire.

On peut essayer de généraliser la définition de l'application d'Abel-Jacobi (Paragraphe I.1.16) au cas de cette intégrale.

On est donc conduit à considérer la courbe algébrique affine C_P définie dans le plan complexe par l'équation :

$$y^2 = a_0 + a_1.x + ... + a_d.x^d$$

et sa version projective $\bar{C}_P$ d'équation homogène :

$$y^2.z^{d-2} = a_0.z^d + a_1.x.z^{d-1} + ... + a_d.x^d.$$

Considérons à nouveau le point à l'infini $O := (0 : 1 : 0)$. Alors l'intégrale précédente peut-être remplacée par une intégrale calculée le long d'un chemin $\gamma(P)$ joigant O à un point P de la courbe $\bar{C}_P(\mathbb{C})$:

$$u = \int_{\gamma(P)} \frac{dx}{y}$$

où $\frac{dx}{y}$ est vue comme une forme différentielle sur $\bar{C}_P$. A nouveau cette intégrale dépend a priori du chemin choisi pour aller de O à P.

Dans le cas où $d > 4$, on ne peut plus procéder comme dans le cas des intégrales elliptiques pour lever cette indétermination. Jacobi découvre qu'il faut considérer ensembles plusieurs variation de cette intégrale. Posons : $g = \lfloor d + 1 \rfloor - 1$.[17] Jacobi introduit ainsi l'application suivante :[18]

$$\phi : C_P(\mathbb{C}) \to \mathbb{C}^g, P \mapsto \left(\int_{\gamma(P)} \frac{dx}{y}, \int_{\gamma(P)} \frac{x.dx}{y}, ..., \int_{\gamma(P)} \frac{x^{g-1}.dx}{y} \right).$$

Jacobi montre qu'il existe un sous-groupe abélien $\Lambda \subset \mathbb{C}^g$ qui est libre de rang g et engendre $\mathbb{C}^g$ telle que l'application

$$\tilde{\phi} : \bar{C}_P(\mathbb{C}) \to \mathbb{C}^g/\Lambda$$

est bien définie (*i.e.* indépendante du chemin $\gamma(P)$ choisi), égale à ϕ modulo Λ sur $C_P(\mathbb{C})$ et envoyant O sur 0.

17. On appelle cet entier le *genre* de la courbe C_P. On notera qu'il est égal à 1 dans le cas des intégrales elliptiques, *i.e.* $d = 3, 4$.
18. Pour être exact, Jacobi considère le cas $d = 6$.

De nos jours, on a introduit la terminologie suivante pour les concepts évoqués ci-dessus :

Définition I.2.4. — Considérons les notations du paragraphe précédent. On associe alors à la courbe algébriques projective $\bar{C}_P$ les données suivantes :

– sa *jacobienne* : l'espace $J(\bar{C}_P) := \mathbb{C}^g/\Lambda$.
– l'*application d'Abel-Jacobi* : $\tilde{\phi} : \bar{C}_P(\mathbb{C}) \to J(\bar{C}_P)$.

Tout élément de Λ est appelée une *période* (de la courbe $\bar{C}_P$).

I.2.5. — Pour comprendre la structure des jacobiennes, revenons au travail de Jacobi. Pour résoudre le problème de l'inversion des intégrales hyper-elliptiques (dans le cas $d = 6$), Jacobi (à la suite d'une idée d'Abel !) considère l'application suivante :

$$\mathcal{J} : \bar{C}_P(\mathbb{C})^g \to J(\bar{C}_P), (P_1, ..., P_g) \mapsto (\tilde{\phi}(P_1) + ... + \tilde{\phi}(P_g))$$

et montre qu'elle est surjective.

Elle n'est pas injective : du fait que la jacobienne est une groupe commutatif, pour toute permutation des coordonnées σ d'un point (P_i) on obtient la relation suivante : $\mathcal{J}(P_i) = \mathcal{J}(P_{\sigma(i)})$.

Si l'on note $\sim$ la relation d'équivalence sur l'ensemble algébrique $\bar{C}_P(\mathbb{C})^g$ identifiant deux points dont les coordonnées sont égales après permutation, on obtient donc un morphisme bien défini :

$$\mathcal{J} : \left(\bar{C}_P(\mathbb{C})^g/\sim\right) \to J(\bar{C}_P).$$

Ce morphisme est presque injectif : il l'est sur un ouvert de l'ensemble algébrique $(\bar{C}_P(\mathbb{C})^g/\sim)$. On peut traduire cette propriété en termes imagés : la jacobienne $J(\bar{C}_P)$ est birationnelle à une variété algébrique complexe.

Remarque I.2.6. — A la suite de Riemann, les mathématiciens ont cherché à donner une forme plus précise à ce résultat en montrant directement que la jacobienne d'une courbe est un ensemble algébrique à l'aide d'un plongement dans l'espace projectif complexe :

$$J(\bar{C}_P) \to \mathbb{P}^N_{\mathbb{C}}.$$

En général, grâce à la théorie des fonctions Θ de Riemann, on peut le faire quitte à se restreindre à un ouvert de $J(\bar{C}_P)$.

I.2.c. Les travaux de Weil. —

I.2.7. — A la suite de sa thèse, Weil s'intéressait essentiellement à l'arithmétique et notamment à l'étude des fonctions zêta associées à une courbe algébrique C sur un corps fini :

$$\zeta_C(s) = \prod_{x \in C_{(0)}} \frac{1}{1 - N(x)^{-s}}$$

où $C_{(0)}$ désigne l'ensemble des points fermés de la courbe C et pour un tel point x, $N(x)$ est le cardinal du corps résiduel de x.

Cette fonction est similaire à la fonction zêta de Riemann. [19] Dans le cas particulier d'une courbe elliptique, Hasse à la suite d'Artin avait démontré qu'elle satisfait une propriété analogue à l'hypothèse de Riemann (sur les zéros de la fonction zêta de Riemann).

Weil s'attaque à l'extension de ce résultat à toutes les courbes algébriques. Il en donne un principe de démonstration en 1940, mais pas une démonstration complète.

Son idée repose sur le fait suivant : comme on l'a vu, les courbes elliptiques sont égales à leur jacobienne. Weil entrevoit (comme Hasse et Schmidt) que dans la démonstration de Hasse, c'est la jacobienne qui est l'objet important (et plus concrètement, l'étude des diviseurs comme on le

19. C'est exactement la fonction zêta de Riemann si dans la définition précédente on remplace C par le schéma $\mathrm{Spec}(\mathbb{Z})$.

verra dans la suite de ce cours). Pour mener à bien son idée, il lui faut donner un sens algébrique à la jacobienne d'une courbe.

Malheureusement (à cette époque), personne n'est en mesure de trouver des plongements projectifs des jacobienne, c'est-à-dire de les écrire en termes de sous-ensembles algébriques d'un espace projectif complexe. Weil est donc contraint à introduire des variétés algébriques abstraites, qui ne sont plus nécessairement définie par des équations polynomiales, inaugurant ainsi la géométrie algébrique moderne (ou abstraite) qui mènera jusqu'à la théorie des schémas.

Weil montre ainsi que pour toute courbe algébrique C sur un corps algébriquement clos k, il existe à équivalence birationnelle près une unique variété algébrique propre munie d'une loi d'addition algébrique et dont les points fermés sont isomorphe (en tant que groupe) à la jacobienne de la courbe.

Pour les besoins de sa démonstration sur la fonction zêta, il porte son intérêt sur les propriétés de la jacobiennes : une *variété abélienne* est une variété algébrique (au sens de Weil) propre et munie d'une structure de groupe algébrique.

En termes modernes :

Définition I.2.8. — Soit S un schéma de base (un corps, corps algébriquement clos, anneau de valuation, ...).

Un S-schéma abélien X est un schéma $f : X \to S$ qui est propre et tel que X admet une structure de groupes dans la catégories des schémas : il existe des morphismes de schémas :

$$\underset{\text{multiplication}}{m : X \times_S X \to X}, \quad \underset{\text{opposé}}{s : X \to X}, \quad \underset{\text{unité}}{u : S \to X},$$

qui satisfont les propriétés formelles d'une loi de groupe abélien (associativité, commutativité, unité, existence d'un opposé).

I.3. Plan du cours

1. Théorème de Riemann-Roch et Courbes elliptiques.
2. Schémas abéliens et théorème du cube.
3. Variété abélienne duale et jacobiennes.

Références

[Sil09] J. H. Silverman – *The arithmetic of elliptic curves*, second éd., Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht, 2009.

---

premier semestre 2013

Frédéric Déglise, CNRS, UMPA (UMR 5669), E.N.S. Lyon, UMPA, 46, allée d'Italie, 69364 LYON Cedex 07 FRANCE, Tel. : +33 4 72 72 84 18 • *E-mail :* frederic.deglise@ens-lyon.fr
Url : http://perso.ens-lyon.fr/frederic.deglise/