N° d'ordre : 14 / 2005-M / MT

MINISTERE DE L'ENSEIGNEMENT SUPERIEURE ET DE LA RECHERCHE SCIENTIFIQUE

Université des Sciences et de la Technologie HOUARI Boumediène

Faculté de Mathématiques

Mémoire présenté pour l'obtention du diplôme de Magister
EN MATHEMATIQUES

Spécialité : Algèbre et Théorie des Nombres

Par : Mr. Toufik MEKERRI

SUJET

Courbes elliptiques et hyperelliptiques sur le corps des nombres complexes $\mathbb{C}$

Soutenu publiquement le :10/10/2005, devant le jury composé de :

Mr ZITOUNI	**Mohamed**	**Professeur**	**USTHB**	**Président**
Mr BETINA	**Kamel**	**Professeur**	**USTHB**	**Directeur de Thèse**
Mr AROUCHE	**Abdelouahab**	**Maître de Conférences**	**USTHB**	**Examinateur**
Mr BEHLOUL	**Djilali**	**Chargé de Recherche**	**USTHB**	**Examinateur**

Remerciements

Je tient à remercier profondément Monsieur Kamel BETINA mon directeur de thèse pour m’avoir proposé ce sujet, pour ces orientations et des remarques fructueuses. Qu’il trouve ici ma profonde gratitude.

Mes remerciements s’adressent également à Monsieur Mohamed ZITOUNI pour m’avoir fait l’honneur d’être président du jury.

Mes remerciements vont aussi à Messieurs Abdelouahab AROUCHE et Djilali BEHLOUL qui ont voulus faire partie du jury.

SOMMAIRE

Introduction

La théorie des surfaces de Riemann fait partie du domaine de l'analyse complexe. Dans ce mémoire, nous nous intéressons à l'étude des surfaces de Riemann X compactes

Pour un polynôme $\mathrm{P} \in \mathbb{C}[x, y]$, où f est une fonction méromorphe sur X, une surface X_f de Riemann associée à f est compacte si la fonction f est algébrique : $\mathrm{P}(f) = 0$.

Une surface de Riemann compacte admet des structures de surface topologique, de corps de degré de transcendance 1 sur $\mathbb{C}$, de variété analytique.

Nous allons nous intéresser ici à l'étude des surfaces de Riemann compactes munies de structures de variétés analytiques ; deux types de courbes remarquables serons traités dans cette théorie : les courbes elliptiques et les courbes hyperelliptiques.

Une grande part de la théorie des surfaces de Riemann compactes concerne l'étude des fonctions méromorphes, qui sont moins nombreuses que dans le cas des surfaces de Riemann non compactes.

Dans le premier chapitre, nous introduisons la notion de surface de Riemann et quelques définition et résultats nécessaires qui nous seront utiles par la suite.

Dans le deuxième chapitre, nous abordons l'étude des courbes elliptiques.

Le troisième chapitre est consacré à quelques propriétés des courbes hyperelliptiques et aux points de Weierstrass.

Chapitre I
Surfaces de Riemann et définitions de base.

Les surfaces de Riemann sont traitées par plusieurs auteurs : Farkas-Kra [7], Gunning [12], Forster [8] et Reyssat [16].
Nous commençons par les variétés analytiques, les fonctions holomorphes et méromorphes, les morphismes.

I-1/ Variété analytique complexe de dimension 1

Définition 1.1
Une fonction analytique sur un ouvert U de $\mathbb{C}$ est une fonction développable en série entière pour tout point de U.

Définition 1.2
Un homéomorphisme est une fonction bijective continue $f : X \longrightarrow Y$ *d'espaces topologiques X et Y telle que la fonction réciproque* f^{-1} *est continue.*

Définition 1.3
Une carte de X est une paire formée d'un ouvert U_α *et d'un homéomorphisme* $f_\alpha : U_\alpha \longrightarrow f_\alpha(U_\alpha) = V_\alpha \subset \mathbb{C}$.

Définition 1.4
Un atlas de X est une famille de cartes $(C_\alpha)_{\alpha\in I}$ *où chaque carte* $C_\alpha = (U_\alpha, f_\alpha)$ *et les ouverts* U_α *sont tels que* $X = \bigcup_{\alpha\in I} U_\alpha$

Pour tout $\alpha, \beta \in I$ $\quad f_\alpha \circ f_\beta^{-1} : f_\beta(U_\alpha \cap U_\beta) \longrightarrow f_\alpha(U_\alpha \cap U_\beta)$ *est analytique.*

Définition 1.5

a) *Une variété analytique complexe est un espace topologique X séparé connexe muni d'une structure analytique formée d'un atlas* $(C_\alpha)_{\alpha\in I} = \{(U_\alpha, f_\alpha)\}_{\alpha\in I}$ *et d'un recouvrement ouvert* $X = \bigcup_{\alpha\in I} U_\alpha$ *tels que les fonctions*

$$f_\alpha \circ f_\beta^{-1} : f_\beta(U_\alpha \cap U_\beta) \longrightarrow f_\alpha(U_\alpha \cap U_\beta)$$

soient analytiques.

b) *Les fonctions* $f_\alpha \circ f_\beta^{-1}$ *sont des fonctions de transitions sur X.*

Deux atlas $\mathcal{A} = \{ (U_\alpha, f_\alpha) \}$ et $\mathcal{B} = \{ (W_\beta, g_\beta) \}$ sont équivalents si leur réunion en est un.
La dimension d'une variété est la dimension de $\mathbb{C}$ comme $\mathbb{C}$-espace vectoriel.

L'espace $\mathbb{C}$ est un espace vectoriel de dimension 1 sur lui-même.

Définition 1.6

Une variété analytique complexe de dimension 1 est une surface de Riemann.

Exemples de surfaces de Riemann

Exemple 1 : Le plan complexe $\mathbb{C}$ muni d'un atlas $\{(\mathbb{C}, Id_{\mathbb{C}})\}$.
Exemple 2 : Tout ouvert U de $\mathbb{C}$ muni d'un atlas $\{(U, Id_U)$.
Exemple 3 : La droite projective complexe.
L'espace topologique $\mathbb{P}^1(\mathbb{C})$ est l'espace quotient de l'espace complexe $\mathbb{C}^2 \backslash \{0\}$ par la relation d'équivalence $\mathcal{R}$

$\xi_1, \xi_2 \in \mathbb{C}^2 \backslash \{0\}$; $\xi_1 \; \mathcal{R} \; \xi_2$ si et seulement s'il existe $\lambda \in \mathbb{C}^*$ tel que $\xi_2 = \lambda \, \xi_1$.

L'espace topologique $\mathbb{P}^1(\mathbb{C})$ est un espace compact et connexe, donc une surface de Riemann.

I-1.1 Fonctions méromorphes dans un ouvert de $\mathbb{C}$

Définition 1.7

Une fonction méromorphe sur un ouvert U de $\mathbb{C}$*, toute fonction holomorphe f sur un ouvert* U' *de U tel que* $U \backslash U'$ *est discret et possédant la propriété suivante : tout point* $z_0 \in U$ *a un voisinage ouvert connexe* U_{z_0} *dans U tel que*

$$f|_{U_{Z_0}} \in \mathcal{F}(U_{z_0}).$$

Soit U un ouvert connexe de $\mathbb{C}$ et $f, h \in \mathcal{O}(U)$ des fonctions holomorphes sur U ; les zéros de h constituent un ensemble discret $Z(h)$ de U.

La fonction $f.\, h^{-1} : z \longrightarrow f(z)\, h^{-1}(z)$ est holomorphe sur la différence $U \setminus Z(h)$.

Soient $z_0 \in Z(h)$ et les développements en séries entières au voisinage de z_0 :

$f(z) = (z - z_0)^m f_1(z)$, $h(z) = (z - z_0)^n h_1(z)$, $m \geq 0, n \rangle\, 0$, f_1 et h_1 holomorphes au voisinage de z_0.

Supposons que $m \langle\, n$, alors $f(z)h^{-1}(z) = (z - z_0)^{m-n} h_2(z)$, h_2 est une fonction holomorphe au voisinage de z_0 et $h_2(z_0) \neq 0$. Le point z_0 est le pôle de $f\, h^{-1}$.

L'anneau des fonctions holomorphes $\mathcal{O}(U)$ sur U est un anneau intègre, on note $\mathcal{F}(U)$ son corps des fractions.

L'ensemble $\mathcal{M}(U)$ des fonctions méromorphes sur un ouvert connexe U de $\mathbb{C}$ a une structure de corps.

Théorème 1.1 (de prolongement de Riemann)

Soit f une fonction $f : \mathcal{O}(B^*(0,\ell)) \longrightarrow \mathbb{C}$, où $B^*(0,\ell) = B(0,\ell) - \{0\}$ est *le disque épointé de rayon* ℓ, *alors les deux conditions suivantes sont équivalentes* :

1) *f se prolonge en une fonction holomorphe sur* $B(0,\ell)$.
2) *f est bornée au voisinage de* 0.

I-2/Morphismes de surfaces de Riemann

Il y a des morphismes de groupes, des morphismes d'anneaux, des morphismes de corps et des morphismes de surfaces de Riemann.

Définition 2.1

Une application $f : X \longrightarrow Y$ *de surfaces de Riemann est holomorphe* (*ou morphisme de X dans Y*) *si elle est continue et si elle possède la propriété suivante* :

pour tout couple (U, h) *une carte de X,* (V, k) *une carte de Y tel que* $f(U) \subset V$ *, alors la fonction* :

$$k \circ (f|_U) \circ h^{-1} : h(U) \longrightarrow k(V),$$

est holomorphe.

En particulier, si $Y = \mathbb{C}$ muni d'un atlas $\mathcal{A} = \{(\mathbb{C}, Id_{\mathbb{C}})\}$, $f : X \longrightarrow \mathbb{C}$ est une fonction holomorphe sur X.

Définition 2.2

1) Une fonction $f : X \longrightarrow \mathbb{C}$ *est holomorphe si les composés*

$$f \circ f_\alpha^{-1},$$

sont holomorphes pour tout indice α ..

2) Une fonction $f : X \longrightarrow \mathbb{C}$ *est méromorphe si les composés*

$$f \circ f_\alpha^{-1},$$

sont méromorphes pour tout indice α .

Soit $\mathcal{M}(X)$ le corps des fonctions méromorphes sur X.

Théorème 2.1

Soient X et *Y deux surfaces de Riemann, et*

$$f_1,\ f_2 : X \longrightarrow \mathbb{P}^1(\mathbb{C})$$

deux morphismes qui coïncident au voisinage d'un point x_0 *de X, alors* f_1 et f_2 *coïncident sur* X.

Théorème 2.2

Soit un morphisme non constant de surfaces de Riemann

$$f : X \longrightarrow Y.$$

Pour tout $a \in X$, *il existe une carte* (U, h) *de X centrée* en a, *une carte* (V, k) *de Y centrée en* $b = f(a)$, *avec* $f(U) \subset V$ *et un entier* $n \geq 1$ *tel que l'application*

$$\mathrm{F} = k \circ f \circ h^{-1} : h(U) \longrightarrow k(V)$$

soit donnée par $$z \longrightarrow \mathrm{F}(z) = z^n.$$

Preuve

Soit un morphisme non constant

$$f : X \longrightarrow Y,$$

et soient (h', U'), (k, V) deux cartes centrées en a et b respectivement telles que $f(U') \subset V$.

Soit ζ la coordonnée dans la carte h', la fonction définie comme suit

$$G = k \circ f \circ h'^{-1} : h'(U') \longrightarrow k(V),$$

vérifie $G(0) = 0$ (car $h'(a) = 0$, $k(b) = 0$).

G est une fonction holomorphe sur l'ouvert $h'(U')$ de $\mathbb{C}$ et à valeurs dans un ouvert $k(V)$ de $\mathbb{C}$, à l'aide du développement de Taylor de G en 0, on obtient :

$$G(z) = \sum_{i=1}^{\infty} a_i z^i = z^n c\, g(z), \tag{1}$$

où g est holomorphe au voisinage de $z = 0$; $g(0) = 1$ avec $n = \mathrm{Inf}\{ i \in \mathbb{N}^* / a_i \neq 0 \}$, $a_n = c \neq 0$.

On écrit g sous la forme

$$g(z) = 1 + g_1(z)\,;\, g_1(z) = 0\,.$$

Pour $|z|$ assez petit, le logarithme de $g(z)$

$$\log(1 + g_1(z)),$$

a un sens ; i.e dans un voisinage W' de 0 à valeurs dans $h'(U')$, donc de même pour la fonction

$$\zeta(z) = c^{1/n}\, e^{1/n \log(g(z))}. \tag{2}$$

En élevant les deux côtés de l'égalité à la puissance n, on déduit que

$$c\ g(z) = \zeta^n(z).$$

En comparant les formules (1) et (2), on trouve

$$\begin{aligned} G(z) &= z^n\, c\, g(z) = z^n\, \zeta^n(z) \\ &= (z\, \zeta(z))^n = k \circ f \circ h'^{-1}\,. \end{aligned}$$

L'application suivante :

$$\begin{aligned} \lambda :\ W' &\longrightarrow W = \lambda(W') \\ z &\longrightarrow \lambda(z) = z\ \zeta(z), \end{aligned}$$

est un isomorphisme.

On pose

$$U = h'^{-1}\ (\ W')$$

et

$$h = \lambda \circ h'\ :\ h'^{-1}(W') \longrightarrow \lambda(W') = W\,,$$

alors la fonction composée

$$\begin{aligned} F = k \circ f \circ h^{-1} = k \circ f \circ h'^{-1} \circ \lambda^{-1} : h(U) &\longrightarrow k(V) \\ z &\longrightarrow z^n, \end{aligned}$$

convient ■.

I-3/ Morphismes de surfaces de Riemann compactes :

Un morphisme de surfaces de Riemann compactes introduit un nouvel entier n ; n est le degré de morphisme. Nous utilisons ce degré pour définir certains types de courbes par la suite, et il intervient aussi dans la formule de Hurwitz.

Définition 3.1

Une application d'espaces topologiques

$$f : X \longrightarrow Y$$

est un homéomorphisme local si, pour tout $x \in X$*, il existe un voisinage ouvert* U_x *de x dans X tel que* $f|_{U_x}$ *soit un homéomorphisme de* U_x *sur l'ouvert* $f(U_x)$.

On applique la définition d'une application ouverte pour prouver que tout homéomorphisme local f est une application ouverte.

Définition3.2

Une application $f : X \longrightarrow Y$ *d'espaces topologiques est propre si l'image réciproque par f de tout compact de Y est un compact de X.*

Définition 3.3

Une application continue $f : X \longrightarrow Y$ *d'espaces topologiques est un revêtement topologique si la condition suivante est réalisée : pour tout* $y \in Y$*, il existe un voisinage ouvert V de* y *tel que* $f^{-1}(V) = \bigcup_{i \in I} U_i$ *où les* U_i *sont des ouverts disjoints de X tels que, pour tout* $i \in I$ *, la restriction de* f *à* U_i

$$f|_{U_i} : U_i \longrightarrow V ,$$

est un homéomorphisme.

Proposition 3.1

Un revêtement topologique $f : X \longrightarrow Y$ *est un homéomorphisme local.*

Définition 3.4

Une fibre au point $y \in Y$ d'une application continue $f : X \longrightarrow Y$ est l'image réciproque $f^{-1}(y)$

Définition 3.5

Une application continue

$$f : X \longrightarrow Y$$

est discrète si sa fibre $f^{-1}(y)$ est discrète pour tout $y \in Y$.

Théorème 3.2

Soit $f : X \longrightarrow Y$ un homéomorphisme local propre. Alors f est un revêtement topologique.

I-3.1 Revêtement ramifié :

Soit $f : X \longrightarrow Y$ un morphisme non constant de surfaces de Riemann. Soient $x_0 \in X$, $y_0 = f(x_0)$, h une carte en x_0 sur X, et k une carte en y_0 sur Y. Puisque f est holomorphe au voisinage de x_0, alors la composée prend la valeur

$$k \circ f \circ h^{-1}(z) = \sum_{n=0}^{\infty} a_n z^n .$$

Les cartes sont centrées en x_0 et y_0.

Comme f n'est pas constant, nous trouvons :

$$k \circ f = \sum_{n=n_0}^{\infty} a_n h^n ,$$

où $a_{n_0} \neq 0$, $n_0 \geq 1$.

Proposition 3.3

L'entier n_0 est indépendant des cartes h et k.

Définition 3.6

L'indice ou degré de ramification de f *en* x_0 *est l'entier* $e_{x_0}(f)=n_0$.

f est ramifié en x_0 ou x_0 point de ramification de f si $e_{x_0}(f)\rangle 1$.

D'après le théorème 2.2, si on se donne $f: X \longrightarrow Y$ et une carte k en $y_0=f(x_0)$, il existe une carte h en x_0 telle que $k \circ f = h^n$ où $n = e_{x_0}(f)$.

Théorème 3.4

Soit $f: X \longrightarrow Y$ *un morphisme non constant entre deux surfaces de Riemann compactes. Alors* :

1) f *n'a qu'un nombre fini de points de ramification* $x_1, \ldots, x_k$.
2) *Hors des fibres* $f^{-1}(f(x_i))$, f *définit un revêtement topologique* (*étale*) *à fibres finies* *de cardinal constant, soit* n .
3) *Pour tout point* y *de* Y,

$$\sum_{f(x)=y} e_x(f) = n .$$

Preuve

Preuve de 1 : D'après la remarque précédente, au voisinage d'un point x, la fonction f est de la forme $z \mapsto z^e$. Les point de ramification sont ceux où la dérivée s'annule (e>1 est l'ordre du zéro) donc au plus en $z = 0$; donc l'ensemble des points de ramification sur X est discret, il est aussi fini car X compact.

preuve de 2 : f définit un isomorphisme local hors des points de ramification $x_1, \ldots, x_k$, en particulier hors des mauvaises fibres $f^{-1}(f(x_i))$.

Comme X est compact, f est propre, donc aussi sa restriction hors des mauvaises fibres.

Or d'après le théorème 3.1, l'homéomorphisme local propre

$$f: M = X \setminus \bigcup_i f^{-1}(f(x_i)) \longrightarrow N = Y \setminus \bigcup_i f(x_i),$$

est un revêtement, à fibres finies (un homéomorphisme local est discret donc $f^{-1}(x_i)$ est discret et $f^{-1}(x_i)$ compact).

f est un revêtement à fibres finies, donc de cardinal localement constant, même constant puisque Y est connexe, donc aussi constant sur Y moins un nombre fini de points.

Preuve de 3 Soit $x \in X$, $y = f(x)$ et U un voisinage de x ne contenant pas d'autre point de la fibre $f^{-1}(y)$. On suppose que $f(z) = z^{e_x(f)}$ sur U, donc il existe un voisinage V de y tel que pour tout $c \in V \setminus \{y\}$ le cardinal de $\left(f^{-1}(c) \cap U\right)$ soit égal à $e_x(f)$; les point de $f^{-1}(c) \cap U$ sont tous non ramifiés, donc la fonction

$$g(y) = \sum_{f(x)=y} e_x(x),$$

est localement constante sur Y, donc constante (car Y connexe) . ■

Ainsi, en comptant les multiplicités, toutes les fibres ont n éléments :

Définition 3.7

La fonction f est un revêtement ramifié de degré n.

Proposition 3.5

Soit f une fonction méromorphe sur une surface de Riemann compacte X, alors f a autant de zéros que de pôles, comptés avec leurs multiplicités ;

$$\sum_{x \in X} ord_x f = 0.$$

Preuve

On considère f comme morphisme $X \longrightarrow \mathbb{P}^1(\mathbb{C})$ (remarque du paragraphe 1.2), d'après le théorème précédent pour $y = 0$ et $y = \infty$, on obtient :

$$\sum_{f(x)=0} e_x(f) = \sum_{f(x)=\infty} e_x(f) .$$

Le genre d'une surface de Riemann compacte

Nous définissons un invariant sur une surface de Riemann compacte en utilisant le langage des revêtements.

Soit $f : X \longrightarrow \mathbb{C}$ une fonction méromorphe sur X, donc elle définit un morphisme $X \longrightarrow \mathbb{P}^1(\mathbb{C})$. D'après le théorème 3.2, le morphisme f fait de X un revêtement ramifié de la droite projective $\mathbb{P}^1(\mathbb{C})$. Soit n le degré de ce revêtement ; alors le nombre de points dans une fibre (la fibre qui ne contient pas de points de ramification). Pour chaque point x de X, soit $e_x(f)$ l'indice de ramification de f en x ; alors on a la définition suivante :

Définition 3.8

Le genre g d'une surface de Riemann compacte est le nombre

$$g = 1 - n + \frac{1}{2} \sum_{x \in X} (e_x(f) - 1).$$

I-4 / Courbes elliptiques et hyperelliptiques

Dans ce paragraphe, nous rappelons les définitions des courbes elliptiques et des courbes hyperelliptiques.

Définition 4.1 [16]

Une courbe elliptique X a une structure analytique de surface de Riemann compacte X de genre 1.

Définition 4.2 [16]

Une surface de Riemann compacte X est hyperelliptique si existe une fonction méromorphe f sur X ayant 2 pôles, en comptant la multiplicité.

D'après le corollaire précédent le nombre de pôles de f est égal au degré de f comme revêtement ramifié de $\mathbb{P}^1(\mathbb{C})$ (un morphisme $f : X \longrightarrow \mathbb{P}^1(\mathbb{C})$).

Donc $f : X \longrightarrow \mathbb{P}^1(\mathbb{C})$ étant un revêtement double de $\mathbb{P}^1(\mathbb{C})$, les degrés de ramification ne peuvent valoir que 1 (point non ramifié) ou 2 (point ramifié)

$$\sum_{f(x)=y} e_x(f) = 2 \quad \text{et} \quad e_x(f) \geq 1.$$

La formule de Hurwitz relie les genres de deux surfaces de Riemann compactes X et Y.

Soient g_X et g_Y les genres de X et Y respectivement, et $f : X \longrightarrow Y$ un revêtement ramifié de degré n ; alors la formule de Hurwitz s'obtient sous cette forme

$$2g_X - 2 = n(2g_Y - 2) + \sum_{x \in X} (e_x(f) - 1).$$

Sur un revêtement ramifié double X de la droite projective $\mathbb{P}^1(\mathbb{C})$, la formule de Hurwitz nous permet de calculer le nombre k de points de ramification sur X :

$$k = \sum_{x \in X} (e_x(f) - 1) = 2g + 2,$$

où g est le genre de X.

CHAPITRE II
LA STRUCTURE DE GROUPE SUR LA JACOBIENNE

L'équation des courbes elliptiques a été déterminée par Weierstrass sous la forme

$y^2 + a_1 x y + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6 \in K[x, y]$ où les 5 coefficients $a_1, \ldots, a_6$ sont des éléments d'un corps commutatif K global, local ou fini.

La théorie des diviseurs s'applique aux courbes algébriques et aux surfaces algébriques.

II-1 Diviseurs sur une surface de Riemann

Les diviseurs sont construits sur les points d'une surface X. Prenons la définition d'un diviseur de Farkas [7].

Soit X une surface de Riemann compacte. Un diviseur de X est une somme formelle D

$$D = \sum_{P \in X} n_P \langle P \rangle,$$

où $n_P \in \mathbb{Z}$, pour tout point P de X et les n_P sont presque tous nuls.

Avec l'addition sur l'ensemble $Div\,(X)$ des diviseurs,

$$\text{pour } D_1 = \sum_{P \in X} n_P \langle P \rangle \;,\; D_2 = \sum_{P \in X} m_P \langle P \rangle \;\text{ et }\; D_0 = \sum_{P \in X} 0 \langle P \rangle$$

$$D = D_1 + D_2 = \sum_{P \in X} (n_P + m_P) \langle P \rangle,\; D_1 + D_0 = D_0 + D_1 = D_1$$

nous obtenons le groupe $Div\,(X)$ des diviseurs de X.

La relation $n_P + m_P = m_P + n_P$ dans l'anneau $\mathbb{Z}$ implique que le groupe des diviseurs $Div\,(X)$ sur X est un groupe abélien.

Le diviseur $0=\sum_{P\in X} n_P\langle P\rangle$; $n_P=0$ pour tout $P\in X$, est un élément neutre du groupe $Div(X)$.

Le diviseur $D'=\sum_{P\in X} n'_P\langle P\rangle$ avec $n'_P=-n_P$ pour tout $P\in X$, est le symétrique de $D=\sum_{P\in X} n_P\langle P\rangle$.

Définition 1.1

1) *Le groupe $Div(X)$ est le groupe des diviseurs de X.*

2) *Un diviseur D* est *positif si tous les n_P sont positifs ou nuls*.

Un diviseur positif est un diviseur effectif.

II-2 Différentielle d'ordre 1

L'existence de fonctions méromorphes sur une surface de Riemann compacte X est l'une des questions posées dans l'étude de ces surfaces. Une démonstration de ce problème est basée sur l'existence de fonctions harmoniques sur X, est donnée dans [7], ce qui nous donne l'existence des différentielles méromorphes sur une surface de Riemann compacte X.

Définition 2.1

Une différentielle d'ordre 1 (ou 1-forme) ω sur une surface de Riemann compacte X est la donnée pour chaque carte locale $z=x+iy : U \longrightarrow \mathbb{C}$ (pour toute carte (U, h) de X est définie comme suit : à tout élément z de U, sa valeur par h est notée aussi par z ; c'est-à-dire $z=h(z)=x+iy$) de deux fonctions continues $f, g : U \longrightarrow \mathbb{C}$ telles que si les fonctions f_1, g_1 sont associées à la carte

$$z_1=x_1+iy_1 : U \longrightarrow \mathbb{C},$$

alors ces fonctions satisfaient la relation

$$\begin{pmatrix} f_1 \\ g_1 \end{pmatrix} = \mathrm{J} \begin{pmatrix} f \\ g \end{pmatrix},$$

où $\mathrm{J} = \begin{pmatrix} \dfrac{\partial x}{\partial x_1} & \dfrac{\partial y}{\partial x_1} \\ \dfrac{\partial x}{\partial x_2} & \dfrac{\partial y}{\partial x_2} \end{pmatrix}$ est la jacobienne de $z_1 \longrightarrow z$.

La différentielle ω est représentée par f, g dans la carte z.

Définition 2.2

ω est de classe C^1 si f et g le sont,

$$\omega = f \ dx + g \ dy.$$

Lorsque ω est de classe C^r, $r \rangle 1$, alors

$$\omega = f \ dx + g \ dy$$

ω est de classe C^∞ si f et g le sont,

$$\omega = f \ dx + g \ dy.$$

Si z est une carte, la fonction z et sa conjuguée $\bar{z}$ ont localement les différentielles

$$dz = dx + i \ dy \quad et \quad d\,\bar{z} = dx - i\,dy \ ;$$

donc toute différentielle $\omega = f \ dx + g \ dy$ est de la forme

$$\omega = f'(z)\,dz + g'(z)\,d\bar{z}\,,$$

où $f' = \dfrac{1}{2}(f - ig),\ g' = \dfrac{1}{2}(f + ig).$

Définition 2.3

1) *Une différentielle*

$$\omega = f(z) \ dz + g(z) \ d \ \bar{z}\,,$$

est méromorphe si g = 0 et si f est méromorphe

2) *La différentielle ω est holomorphe si g = 0 et si f est holomorphe.*

3) *Si $\omega = f(z)\,dz$ au voisinage de P, l'ordre de la différentielle ω en P est égal à*

$$ord_P\,\omega \ = \ ord_P f.$$

Ces définitions précédentes ne dépendent pas de la carte choisie.

Définition 2.4

1) *Soit f une fonction sur une surface de Riemann compacte X, alors son diviseur est égal à*

$$\left(f\right)=\sum_{P\in X} ord_P(f)\left\langle P\right\rangle.$$

2) *Soit une forme différentielle* $\omega = f\ \ dx + g\ \ dy$, alors son diviseur est égal à

$$\left(\omega\right)=\sum_{P\in X} ord_P(\omega)\left\langle P\right\rangle.$$

Le diviseur du produit de deux fonctions f_1 et f_2 est égal à la somme de deux diviseurs :

$$\left(f_1 . f_2\right)=\left(f_1\right)+\left(f_2\right).$$

Définition 2.5

La fonction degré est l'homomorphisme de groupes

$$deg : Div\,(X) \longrightarrow \mathbb{Z}$$

$$D=\sum_{P\in X} n_P\left\langle P\right\rangle \longrightarrow deg\,(\,D\,)=\sum_{P\in X} n_P\ .$$

Exemple

Une fonction méromorphe f sur X possède autant de zéros que de pôles, comptés avec leurs multiplicités, donc $deg\big((f)\big) = 0$, on écrit :

$$deg(f) = 0\ .$$

Le degré d'une différentielle, sur une surface de Riemann compacte X, s'exprime seulement par le genre de X, il est donné explicitement dans la proposition suivante.

Proposition 2.1

Si ω *est une différentielle méromorphe non identiquement nulle sur une surface de Riemann compacte* X *de genre* g*, alors son degré est égal à*

$$deg\,(\,\omega\,) = 2g - 2\ .$$

Preuve

Le quotient de deux différentielles méromorphes non nulles $\omega_1 = f_1(\,z)\ dz$ et $\omega_2 = f_2(z)\ dz$

est une fonction méromorphe $\dfrac{\omega_1}{\omega_2} = \dfrac{f_1}{f_2}$, donc le degré

$$deg\left(\frac{\omega_1}{\omega_2}\right) = deg(\,\omega_1\,) - deg(\,\omega_2\,),$$

et d'après l'exemple précédent, le degré d'une fonction méromorphe est nul, nous obtenons

$$deg(\omega_1) = deg(\omega_2).$$

Il suffit donc de prouver le résultat pour une différentielle ω. Soit $\omega = df$ où f est une fonction méromorphe non constante sur X.

On choisit f non ramifiée au-dessus de ∞, sinon on compose f par une bijection de $\mathbb{P}^1(\mathbb{C})$ de la forme :

$$z \mapsto \frac{a\,z+b}{c\,z+d}.$$

Localement, la différentielle ω est égal à

$$\omega = f'(z)\,d\,z, \tag{1}$$

Il en résulte l'égalité

$$ord_P(\omega) = ord_P(f').$$

Deux cas se présentent pour calculer l'ordre de la différentielle ω.

1) Si P n'est pas un pôle ; alors $f(P) \neq \infty$, cela implique

$$(f \circ h^{-1})(z) = (f \circ h^{-1})(0) + (f \circ h^{-1})'(0)\,z + \frac{(f \circ h^{-1})''(0)}{2!}\,z^2 + \dots$$

$$= \frac{(f \circ h^{-1})^{(e)}(0)}{e!}\,z^e \tag{2}$$

où $e = e_P(f) = ord_P(f)$, et h est une carte de X centrée en P ; donc $h(P) = 0$.

La dérivée de (2) implique

$$(f \circ h^{-1})'(z) = \frac{e\,(f \circ h^{-1})^{(e)}(0)}{e!}\,z^{e-1}, \tag{3}$$

On en déduit les égalités

$$ord_P(f') = ord_P(f) = e_P(f) - 1.$$

2) Si P est un pôle, alors $f(P) = \infty$, on pose

$$\tilde{f} = \frac{1}{f},$$

donc $\tilde{f}(P) = 0$ et $e_P(\tilde{f})$ est l'indice de ramification de $\tilde{f}$ en P ; On en déduit l'égalité

$$ord_P(\tilde{f}) = e_P(\tilde{f}), \tag{4}$$

cela nous montre que P est un pôle de f d'ordre $e_P(\tilde{f})$, ce qui implique l'ordre de f au point P

$$ord_P(f) = -e_P(f) = -e_P(\widetilde{f}). \qquad (5)$$

Les formules (4) et (5) impliquent que

$$ord_P(f') = ord_P(f) - 1 = -e_P(\widetilde{f}) - 1 = -e_P(f) - 1,$$

mais on a choisit f non ramifiée à l'∞ ; $e_P(f) = 1$, donc on obtient

$$ord_P(f') = -2. \qquad (6)$$

Les formules (1), (3) et (6) entraînent la valeur du degré

$$deg(\omega) = \sum_{P \in X} (e_P(f) - 1) = \sum_{P \in X \setminus \text{pôles}} (e_P(f) - 1) + \sum_{P \text{ est un pôle}} (-2). \qquad (7)$$

Comme f est un revêtement ramifié de $\mathbb{P}^1(\mathbb{C})$,de degré n, alors le cardinal de la fibre au point ∞ est égal

$$\# f^{-1}(\infty) = n. \qquad (8)$$

Les formules (7) et (8) impliquent la valeur

$$deg(\omega) = \sum_{P \in X \setminus \text{pôles}} (e_P(f) - 1) - 2n. \qquad (9)$$

D'après la formule de Hurwitz appliquée au morphisme $f : X \longrightarrow \mathbb{P}^1(\mathbb{C})$, les genre g_X et $g_{\mathbb{P}_1}$ satisfont l'égalité

$$2g_X - 2 = n(2g_{\mathbb{P}^1} - 2) + \sum_{P \in X} (e_P(f) - 1),$$

On en déduit la relation

$$2g - 2 = -2n + \sum_{P \in X} (e_P(f) - 1). \qquad (10)$$

Mais dans la formule (9) on peut prendre la somme sur X, car l'indice de ramification est égal à 1 aux pôles ($e_P(f) = 1$), donc

$$deg(\omega) = \sum_{P \in X} (e_P(f) - 1) - 2n. \qquad (11)$$

Les formules (10) et (11) impliquent que :

$$deg(\omega) = 2g - 2. \qquad \blacksquare$$

II-3 Théorème de Riemann-Roch

Le théorème de Riemann-Roch est le point central de la théorie des surfaces de Riemann, il précise l'existence de fonctions méromorphes ayant des singularités données, que l'on prescrit sous la forme d'un diviseur.

Soit X une surface de Riemann compacte de genre g.

Définition 3.1

Soit un diviseur $D \in Div(X)$, $\mathcal{L}(D)$ est le $\mathbb{C}$-espace vectoriel

$$\mathcal{L}(D) = \{0\} \cup \{f \text{ méromorphe} \neq 0 \,;\, (f) + D \geq 0\}.$$

On note par l sa dimension

$$l = l(D) = \dim_{\mathbb{C}} \mathcal{L}(D).$$

Exemples

1/ Si $D = 0$, $\mathcal{L}(D)$ est l'espace vectoriel des fonctions holomorphes sur X, or toute fonction holomorphe sur une surface de Riemann compacte est constante, alors

$$l(D) = 1.$$

2/ Si $deg(D) < 0$, alors $l(D) = 0$, soit $f \in \mathcal{L}(D)$; f non constante. Alors le diviseur $(f) + D \geq 0$, donc de la relation suivante

$$(f) \geq -D,$$

on obtient l'inégalité sur les degrés

$$deg(f) \geq deg(-D) = -deg(D),$$

et comme le degré d'une fonction méromorphe est nul, on aura

$$deg(D) \geq 0.$$

Contradiction avec le fait que $deg(D) < 0$.

Proposition 3.1

Une surface de Riemann compacte X est hyperelliptique si et seulement s'il existe un diviseur D effectif de degré 2, tel que $l(D) \geq 2$.

Preuve

La 1re implication

● Si $D = (f)_\infty$ est le diviseur des pôles de f ; les deux fonctions $1, f \in \mathcal{L}(D)$. Donc la dimension $l(D) \geq 2$.

La 2ème implication

● Soit une fonction $f \in \mathcal{L}(D)$ non constante ; donc elle a au plus deux pôles. Si elle n'a qu'un seul pôle, alors la fonction f^2 convient. ■

Théorème 3.2 (Riemann-Roch)

Soit $\omega \neq 0$ une différentielle méromorphe sur X et $K = (\omega)$ son diviseur. Alors pour tout diviseur D, les dimensions $l(D)$ et $l(K-D)$ satisfont :

$$l(D) < +\infty \quad et \quad l(D) - l(K-D) = deg(D) + 1 - g.$$

On applique le théorème de Riemann-Roch à quelques cas.

Proposition 3.3

L'espace vectoriel $\Omega(X)$ des différentielles holomorphes sur X est de dimension g sur $\mathbb{C}$.

Preuve

On fixe une différentielle méromorphe non nulle ω. A toute différentielle $\omega' \in \Omega(X)$ on associe la fonction $\frac{\omega'}{\omega}$; ω' est holomorphe sur *X*, donc $(\omega') \geq 0$, cela implique que

$$\left(\frac{\omega'}{\omega}\right) = (\omega') - (\omega) \geq -(\omega) = -K,$$

avec $(\omega) = K$.

C'est-à-dire $\left(\frac{\omega'}{\omega}\right) + K \geq 0$, ce qui signifie que $\frac{\omega'}{\omega} \in \mathcal{L}(K)$.

On définit donc un isomorphisme :

$$\begin{aligned} \Omega(X) &\longrightarrow \mathcal{L}(K) \\ \omega' &\longrightarrow \frac{\omega'}{\omega}. \end{aligned} \tag{1}$$

En effet, si $\frac{\omega'}{\omega} = \frac{\omega''}{\omega}$, alors $\omega' = \omega''$. D'où l'injectivité.

Soit $f \in \mathcal{L}(K)$, on pose

$$\omega' = f.\omega.$$

Le diviseur de cette différentielle et égal à

$$(\omega') = (f) + (\omega) = (f) + K,$$

et il est effectif, car f appartient à $\mathcal{L}(K)$; on conclue que la différentielle ω' est holomorphe sur *X*, il existe alors ω' dont $f = \dfrac{\omega'}{\omega}$ est son image ; d'où la surjectivité.

On applique le théorème de Riemann-Roch à $D = K$, on obtient

$$l(K) - l(0) = deg(K) + 1 - g, \tag{2}$$

la relation (2) et la bijection de l'application (1) impliquent que

$$\begin{aligned} \dim_{\mathbb{C}} \Omega(X) &= l(K) = l(0) + deg(K) + 1 - g \\ &= 1 + (2g - 2) + 1 - g \\ &= g, \end{aligned}$$

d'où

$$\dim_{\mathbb{C}} \Omega(X) = g . \qquad \blacksquare$$

Proposition 3.4

Si $P \in X$ et n entier $\geq 2g$, il existe une fonction méromorphe sur X ayant en P un pôle d'ordre exact n, et holomorphe ailleurs.

Preuve

D'après la proposition 1.2.3, le degré de diviseur $(K - (n-1)\langle P\rangle)$ est égal à

$$\begin{aligned} deg(K - (n-1)\langle P\rangle) &= (2g - 2) - (n - 1) \\ &= 2g - n - 1 < 0. \end{aligned} \tag{1}$$

Le numéro 2 de l'exemple précédent et (1) impliquent que

$$l(K - (n-1)\langle P\rangle) = 0. \tag{2}$$

La relation (2) et l'application du théorème de Riemann-Roch pour $D = (n-1)\langle P\rangle$, nous donnent

$$l((n-1)\langle P\rangle) = n - g. \tag{3}$$

De même pour $l((n\langle P\rangle)$, on a :

$$\begin{aligned} deg(K - n\langle P\rangle) &= (2g - 2) - n \\ &= 2g - n - 2 < 0, \end{aligned}$$

cela implique que

$$l(K - n\langle P\rangle) = 0, \tag{4}$$

La relation (4) et l'application du théorème de Riemann-Roch pour $D = n\langle P\rangle$, impliquent que

$$l((n\langle P\rangle) = n + 1 - g. \qquad (5)$$

Les formules (3) et (5) entraînent que

$$l((n\langle P\rangle) > l((n-1)\langle P\rangle),$$

il existe donc une fonction f dans $\mathcal{L}((n\langle P\rangle) \setminus \mathcal{L}((n-1)\langle P\rangle)$, si une fonction $f \in \mathcal{L}((n\langle P\rangle)$, alors d'après la définition de l'espace $\mathcal{L}$, on obtient une suite de valeurs possibles des ordres de f en P

$$ord_P(f) = -n, -(n-1), -(n-2), \ldots$$

De même pour une fonction $f \in \mathcal{L}((n-1)\langle P\rangle)$, nous avons

$$ord_P(f) = -(n-1), -(n-2), \ldots$$

Donc il reste une seule possibilité pour une fonction $f \in \mathcal{L}((n\langle P\rangle) \setminus \mathcal{L}((n-1)\langle P\rangle)$

$$ord_P(f) = -n, \text{ et } ord_Q(f) \geq 0 \text{ avec } Q \neq P.$$

Ce qui montre l'existence d'une fonction f avec un pôle d'ordre exact n, et holomorphe ailleurs. ■

II-4 Plongement projectif d'une courbe elliptique

Une courbe elliptique X admet un plongement projectif dans l'espace $\mathbb{P}^2(\mathbb{C})$.

Définition 4.1

Un plongement de X dans l'espace $\mathbb{P}^N(\mathbb{C})$ *est une application holomorphe injective*

$$U \longrightarrow \mathbb{P}^N(\mathbb{C})$$

$$P \longrightarrow (\varphi_0(P),\dots,\varphi_N(P)),$$

où les φ_i *sont des fonctions holomorphes* $U \longrightarrow \mathbb{C}$, *telles que* :

$$\text{pour tout } P \text{ de } X,\quad (\varphi_0(P),\dots,\varphi_N(P)) \neq (0,\dots,0)$$
$$\text{et } (d\varphi_0(P),\dots,d\varphi_N(P)) \neq (0,\dots,0).$$

On construit un plongement d'une surface de Riemann compacte *X*, en choisissant un diviseur *D* sur *X* et une base de l'espace $\mathcal{L}(D)$.

Théorème 4.1

Soit D un diviseur sur X de degré $deg \geq 2g+1$, et $(f_0,\dots,f_N)$ *une base de* $\mathcal{L}(D)$. *Alors l'application*

$$\varphi : P \longrightarrow (f_0(P),\dots,f_N(P)) \in \mathbb{P}^N(\mathbb{C}),$$

est bien définie hors des zéros et pôles des f_i, *et se prolonge en un plongement*

$$\varphi : X \longrightarrow \mathbb{P}^N(\mathbb{C}).$$

Preuve

Pour $P \in X$, soit z_P une carte en *P*, nous définissons les fonctions

$$h_{i,P} = z_P^{-k_P} f_i ,$$

où $k_P = \min_i ord_P(f_i)$.

Donc au voisinage U de P, on aura pour $Q \in U - \{P\}$

$$\varphi(Q) = \left(h_{0,P}(Q), \ldots, h_{N,P}(Q) \right) ;$$

et par définition de k_P, les fonctions $h_{i,P}$ ne s'annulent pas simultanément en P, donc on définit encore la valeur de φ en P par

$$\varphi(P) = \left(h_{0,P}(P), \ldots, h_{N,P}(P) \right).$$

D'où une fonction holomorphe φ :

$$\varphi : X \longrightarrow \mathbb{P}^N(\mathbb{C})$$

$$Q \longrightarrow \varphi(Q) = \left(h_{0,P}(Q), \ldots, h_{N,P}(Q) \right).$$

Montrons que φ est injective :

Soit D un diviseur de degré $deg\, D \geq 2g$, et un point $Q \in X$. On applique le théorème de Riemann-Roch à ce diviseur D, et on obtient la dimension

$$l(D) = deg\, D + 1 - g , \tag{1}$$

Le diviseur $D - \langle Q \rangle$, a pour dimension

$$l(D - \langle Q \rangle) = deg\, D - g . \tag{2}$$

(1) et (2) impliquent que la différence des dimension est égal à

$$l(D) - l(D - \langle Q \rangle) = 1 , \tag{3}$$

cela implique l'existence d'une fonction f telle que :

$$f \in \mathcal{L}(D) \setminus \mathcal{L}(D - \langle Q \rangle),$$

cela nous confirme que la fonction f est d'ordre exact n_Q en Q

$$ord_Q f = n_Q \,. \tag{4}$$

Appliquant le raisonnement précédent au diviseur $D = \sum_{P \in X} n_P \langle P \rangle$.

La formule (3) implique que f est parmi les éléments de la base de $\mathcal{L}(D)$, alors le minimum des $ord_P f_i$ est égal à

$$\min_i ord_P\, f_i = \min\{ ord_P\, f \;, f \in \mathcal{L}(D)\}, \tag{5}$$

comme la fonction f est dans $\mathcal{L}(D)$, ce qui signifie que $ord_P f_i \geq -n_P$.

Les formules (4) et (5) entraînent que

$$\min_i ord_P\, f_i = -n_P \,,$$

d'où le minimum k_P des ordre des f_i en P

$$k_P = -n_P \,. \tag{6}$$

Pour montrer que φ est injective nous montrons que les deux images $\varphi(P_1)$ et $\varphi(P_2)$ ne sont pas sur le même plan.

D'après le raisonnement précédent pour $D' = D - \langle P_2 \rangle$, il existe une fonction f dans $\mathcal{L}(D - \langle P_2 \rangle) \setminus \mathcal{L}\,(D - \langle P_1 \rangle - \langle P_2 \rangle)$, alors

$$ord_{P_1}\, f = -n_{P_1} \,, \tag{7}$$

$$\text{et } ord_{P_2}\, f \geq -n_{P_2} + 1 \rangle - n_{P_2} \,, \tag{8}$$

Décomposons f dans la base $\{ f_i \}_i$ de $\mathcal{L}(D)$, donc

$$f = \sum_{i=0}^{N} \lambda_i\, f_i \,.$$

Nous calculons la valeur de $\sum_{i=0}^{N} \lambda_i \, h_{i,P_1}$ en P_1, nous obtenons

$$\left(\sum_{i=0}^{N} \lambda_i \, h_{\,i,P_1}\right)(P_1) = \left(\sum_{i=0}^{N} \lambda_i \, z_{P_1}^{-k_{P_1}} \, f_i\right)(P_1)$$

$$= z_{P_1}^{-k_{P_1}} \left(\sum_{i=0}^{N} \lambda_i \, f_i\right)(P_1)$$

$$= \left(z_{P_1}^{-k_{P_1}} \, f\right)(P_1). \tag{9}$$

Les formules (6), (7), (8) et (9) impliquent que

$$\left(\sum_{i=0}^{N} \lambda_i \, h_{\,i,P_1}\right)(P_1) = \left(z_{P_1}^{-k_{P_1}} \, f\right)(P_1) \neq 0,$$

la valeur de la fonction $z_{P_1}^{-k_{P_1}} \, f$ est nulle en P_1, car $ord_{P_1} f = -n_{P_1}$.

Donc $\varphi(P_1)$ n'appartient pas à l'hyperplan $\mathrm{H} : \sum_{i=0}^{N} \lambda_i \, X_i = 0$,

$$\varphi(P_1) \notin \mathrm{H}. \tag{10}$$

De même pour le point P_2

$$\left(\sum_{i=0}^{N} \lambda_i \, h_{\,i,P_2}\right)(P_2) = \left(z_{P_2}^{-k_{P_2}} \, f\right)(P_2).$$

La formule (8) implique

$$\left(\sum_{i=0}^{N} \lambda_i \, h_{\,i,P_2}\right)(P_2) = \left(z_{P_2}^{-k_{P_2}} \, f\right)(P_2) = 0,$$

donc $\varphi(P_2)$ est dans l'hyperplan H

$$\varphi(P_2) \in \mathrm{H}, \tag{11}$$

(10) et (11) entraînant la relation

$$\varphi(P_1) \neq \varphi(P_2).$$

D'où l'injectivité de φ.

On achève la preuve du théorème en démontrant que $(dh_{0,P}(P),\ldots,dh_{N,P}(P)) \neq (0,\ldots,0)$.

D'après le raisonnement précédent pour $D' = D - \langle P \rangle$ avec $P \in X$, il existe une fonction f dans $\mathcal{L}(D - \langle P \rangle) \setminus \mathcal{L}(D - 2\langle P \rangle)$, ce qui implique l'ordre de f :

$$ord_P(f) = -n_P + 1. \tag{12}$$

La décomposition de f

$$f = \sum_{i=0}^{N} \lambda_i f_i ,$$

implique l'ordre de f

$$ord_P\left(\sum_{i=0}^{N} \lambda_i h_{i,P}\right) = ord_P\left(z_P^{n_P} f\right). \tag{13}$$

De (12) et (13), on déduit l'ordre :

$$ord_P\left(\sum_{i=0}^{N} \lambda_i h_{i,P}\right) = 1,$$

donc l'une au moins des $dh_{i,P}$ est non nulle en *P*.

L'entier *N* se déduit du théorème de Riemann-Roch. Par la formule de Riemann-Roch pour le diviseur *D* et un diviseur *K* d'une différentielle

$$l(D) - l(K - D) = deg(D) + 1 - g.$$

L'hypothèse $deg(D) \geq 2g + 1$ implique que $deg(K - D) = 0$, et par suite $l(K - D) = 0$. On remplace la valeur de la dimension $l(D)$ dans la formule de Riemann-Roch, on obtient

$$N+1=deg(D)+1-g,$$

d'où l'entier *N* égal à $deg(D)-g$. ■

Théorème 4.2

Soit f une fonction méromorphe non constante sur X, de degré n,.alors le corps $\mathcal{M}(X)$ des fonctions méromorphes sur X est une extension algébrique de degré n sur $\mathbb{C}(f)$:

$$[\mathcal{M}(X):\mathbb{C}(f)]=n.$$

Preuve

Soit $h\in\mathcal{M}(X)$, alors on construit un polynôme P de $\mathbb{C}(f)[X]$ tel que $\mathrm{P}(h)\equiv 0$.

On choisit un ouvert *U* de $\mathbb{P}^1(\mathbb{C})$ tel que f ne soit pas ramifiée sur $f^{-1}(U)$ et f, $h\neq\infty$ sur leurs domaines de définition, de plus *U* peut être choisi de façon que h soit holomorphe sur $V=f^{-1}(U)$.

D'après la remarque de la définition 3.3 du chapitre I, la fonction f est un isomorphisme local sur *V*, alors les n fonctions symétriques élémentaires suivantes

$$s_1(y)=\sum_{f(x)=y}h(x)\ ,\dots,\quad s_n(y)=\prod_{f(x)=y}h(y),$$

sont holomorphes sur *U*. Elle sont même méromorphes sur $\mathbb{P}^1(\mathbb{C})$ (voir Reyssat [16] pour plus de détail). Comme toute fonction méromorphe sur $\mathbb{P}^1(\mathbb{C})$ est une fraction rationnelle, ainsi on définit le polynôme suivant à coefficients dans $\mathbb{C}(f)$

$$\mathrm{P}(\mathrm{X})=X^n-(s_1\circ f)X^{n-1}+\cdots+(-1)^n(s_n\circ f).$$

La construction de ce polynôme nous donne pour chaque point $x \in V$, $\mathrm{P}(\mathrm{h})(x) = 0$, et donc $\mathrm{P}(h) \equiv 0$. Par suite, le polynôme minimal de h sur $\mathbb{C}(f)$ divise P, ce qui montre que $[\mathbb{C}(f, h) : \mathbb{C}(f)] \leq n$.

D'où
$$[\mathcal{M}(X) : \mathbb{C}(f)] \leq n. \qquad (1)$$

En choisissant un point $y \in U$ de telle sorte que h n'ait ni zéro ni pôle aux points de la fibre $f^{-1}(y) = \{x_1, \cdots, x_n\}$, alors pour tout polynôme $Q \in \mathbb{C}(f)[X]$ nul sur h est de degré $\geq n$, car Q a au moins n racines $h(x_1), \ldots, h(x_n)$; donc le polynôme minimal de h est de degré $\geq n$, on écrit $[\mathbb{C}(f, h) : \mathbb{C}(f)] \geq n$.

D'où
$$[\mathcal{M}(X) : \mathbb{C}(f)] \geq n. \qquad (2)$$

De (1) et (2), on obtient
$$[\mathcal{M}(X) : \mathbb{C}(f)] = n.$$

On va préciser le plongement projectif donné par une base de $\mathcal{L}(3\langle\theta\rangle)$. Pour le diviseur $D = 3\langle\theta\rangle$, son degré $deg(3\langle\theta\rangle) = 3 \geq 2g + 1$; $g = 1$, alors le théorème 4.1 nous donne un plongement. ■

Proposition 4.3

Soit X une courbe elliptique sur $\mathbb{C}$, *il existe un isomorphisme de X vers la cubique projective de* $\mathbb{P}^2(\mathbb{C})$ *d'équation affine* :
$$y^2 + a_1 x y + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6 ;$$
avec $a_i \in \mathbb{C}$.

Preuve

Soit θ un point de *X*, *n* un entier positif, *K* un diviseur d'une différentielle méromorphe sur *X* et $l(D)$ la dimension de l'espace vectoriel $\mathcal{L}(D)$ pour un diviseur *D* de *X*.
Le degré de diviseur $(K - n\langle\theta\rangle)$ est négatif
$$deg(K - n\langle\theta\rangle) = 2g - 2 - n = -n,$$
alors la dimension de l'espace vectoriel $\mathcal{L}(K - n\langle\theta\rangle)$ est égal à
$$l(K - n\langle\theta\rangle) = 0. \qquad (1)$$
D'après le théorème de Riemann-Roch pour $D = n\langle\theta\rangle$ et (1)

$$\begin{aligned} l((n\langle\theta\rangle) &= deg((n\langle\theta\rangle) + 1 - g \\ &= deg((n\langle\theta\rangle) \\ &= n, \end{aligned} \qquad (2)$$

D'après la proposition 3.4, il existe des fonctions x et y telles que

$$x \in \mathcal{L}(2\langle\theta\rangle) \setminus \mathcal{L}(\langle\theta\rangle) \text{ et } y \in \mathcal{L}(3\langle\theta\rangle) \setminus \mathcal{L}(2\langle\theta\rangle),$$

θ est l'unique pôle double de x, alors d'après le théorème 3.2 de chapitre I, x est un revêtement ramifié de $\mathbb{P}^1(\mathbb{C})$ de degré 2.

θ est l'unique pôle triple de y, alors d'après le théorème 3.2 de chapitre I, y est un revêtement ramifié de $\mathbb{P}^1(\mathbb{C})$ de degré 3. Le théorème 4.2 implique que le degré de l'extension $\mathcal{M}(X)$ de $\mathbb{C}(x)$ est égal au degré de x

$$[\mathcal{M}(X) : \mathbb{C}(x)] = 2, \qquad (3)$$

Pour tout élément du corps $\mathbb{C}(x)$ a θ comme pôle d'ordre pair, et puisque y admet un pôle d'ordre 3 impair en θ, cela implique que

$$y \notin \mathbb{C}(x). \qquad (4)$$

Les formules (3) et (4) donnent

$$\mathcal{M}(X) = \mathbb{C}(x, y).$$

La formule (2) implique que la dimension de $\mathcal{L}(6\langle\theta\rangle)$ est égale à 6. Les fonctions $1, x, x^2, x^3, y, y^2, xy$ sont dans $\mathcal{L}(6\langle\theta\rangle)$, donc ces fonctions sont dépendantes ; alors il existe des coefficients $\alpha'_0, \alpha_i \in \mathbb{C}$ tels que :

$$\alpha_0 y^2 + \alpha_1 xy + \alpha_3 y = \alpha'_0 x^3 + \alpha_2 x^2 + \alpha_4 x + \alpha_6 . \qquad (5)$$

Les relations $ord_{\mathrm{p}}(\alpha_1 xy + \alpha_3 y) \neq ord_{\mathrm{p}}(\alpha'_0 x^3 + \alpha_2 x^2 + \alpha_4 x + \alpha_6)$.

$$ord_{\mathrm{p}}(\alpha_0 y^2 + \alpha_1 xy + \alpha_3 y) \neq ord_{\mathrm{p}}(\alpha_2 x^2 + \alpha_4 x + \alpha_6)$$

impliquent que le produit $\alpha_0 \alpha'_0 \neq 0$ donc $\alpha_0 \neq 0$ et $\alpha'_0 \neq 0$.

On multiplie l'équation (5) par élément $\alpha_0{}^{-1}$, on obtient

$$y^2 + \alpha_0{}^{-1}\alpha_1 xy + \alpha_0{}^{-1}\alpha_3 y = \alpha_0{}^{-1}\alpha'_0 x^3 + \alpha_0{}^{-1}\alpha_2 x^2 + \alpha_0{}^{-1}\alpha_4 x + \alpha_0{}^{-1}\alpha_6 \qquad (6)$$

En changeant x par $\left(\alpha_0{}^{-1}\alpha'_0\right)^{-1/3} x$ dans l'équation (6), on obtient

$$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6 , \qquad (7)$$

où $a_1 = \alpha_0{}^{-1}\alpha_1 \left(\alpha_0{}^{-1}\alpha'_0\right)^{-1/3}$, $a_2 = \alpha_0{}^{-1}\alpha_2 \left(\alpha_0{}^{-1}\alpha'_0\right)^{-2/3}$, $a_3 = \alpha_0{}^{-1}\alpha_3$,

$a_4 = \alpha_0{}^{-1}\alpha_4 \left(\alpha_0{}^{-1}\alpha'_0\right)^{-1/3}$, $a_6 = \alpha_0{}^{-1}\alpha_6$

en changeant y en $y+\frac{1}{2}(a_1 x+a_3)$, on enlève les termes en xy et y de la formule (7), et ensuite en changeant $2y$ par y, on obtient

$$y^2=4x^3+b_2x^2+2b_4x+b_6 \quad . \tag{8}$$

Où $b_2=4a_2+a_1^2$, $b_4=2a_4+a_1a_3$ et $b_6=4a_6+a_3^2$

Puis les termes en x^2 en changeant x en $x-b_2/12$ dans l'équation 8, on obtient

$$y^2=4x^3-g_2x-g_3\ ,g_i\in\mathbb{C}. \tag{9}$$

La proposition suivante donne les équivalences entre les singularités.

Proposition 4.4

Soit une courbe C d'équation $\mathrm{P}(x,y)=y^2-4x^3+g_2x+g_3=0$, *alors les trois propositions suivantes sont équivalentes*

1) *C est non singulière, les équations* $\mathrm{P}(x,y)=0$, $\mathrm{P}'_x(x,y)=0$ et $\mathrm{P}'_y(x,y)=0$ *n'ont pas de solutions communes.*

2) *Les zéros du polynôme* $4x^3-g_2x-g_3$ *sont simples.*

3) *Le nombre* $g_2^3+27g_3^2$ *est non nulle.*

La cubique (5) est non singulière, s'il existe un point singulier *P* de valeur α par x, alors la relation (5) s'écrit

$$y^2=4(x-\alpha)^2(x-\beta)\,,$$

et donc

$$\left(\frac{y}{x-\alpha}\right)^2=4(x-\beta)\,.$$

La fonction $x-\beta$ a un pôle double en θ, cela implique que la fonction

$$\frac{y}{x-\alpha},$$

a un pôle simple en θ.

Donc la fonction $\frac{y}{x-\alpha}$ est un revêtement de $\mathbb{P}^1(X)$ de degré 1, donc un isomorphisme

$X \cong \mathbb{P}^1(X)$, ce qui est absurde car le genre de X est non nul. On en déduit que le discriminant de la cubique

$$\Delta = g_2^3 + 27 g_3^2,$$

est non nul.

On a donc un plongement de X comme cubique plane lisse (non singulière) :

$$\begin{aligned} X &\longrightarrow \mathbb{P}^2(\mathbb{C}) \\ P &\longrightarrow (0, 1, 0). \qquad (6) \\ Q &\longrightarrow (x(Q), y(Q), 1). \end{aligned}$$

■

II-5/ Structure de groupe sur les diviseurs

Dans le groupe *Div* (X) il y a une relation d'équivalence.

.

Définition 5.1

a *) Deux diviseurs D et D' sont linéairement équivalents si la différence $D-D'$ est un diviseur principal*

b) *Le groupe quotient . Div* (X) / $\mathcal{R}$ = *Pic* (X) est le groupe de Picard.

c) *La norme d'un diviseur D est l'entier*

$$|D| = \sum_{P \in X - \{\theta\}} |n_P| \geq 0.$$

Définition 5.2

Une droite L a une équation de la forme :

$$L = \alpha x + \beta y + \gamma \in \mathbb{C}[x, y].$$

Les diviseurs d'une droite L sont de l'une des formes suivant le nombre de points d'intersection de la droite et de la courbe X cubique

1) $\langle P \rangle + \langle Q \rangle + \langle R \rangle - 3\langle \theta \rangle$.

2) $2\langle P \rangle + \langle Q \rangle - 3\langle \theta \rangle$.

3) $3\langle P \rangle - 3\langle \theta \rangle$.

4) $\langle P \rangle + \langle Q \rangle - 2\langle \theta \rangle$.

5) $2\langle P \rangle - 2\langle \theta \rangle$.

Pour tout diviseur D ayant l'une des 5 formes précédentes, alors il existe une droite L telle que $D = div(L)$.

Théorème 5.1 **(réduction linéaire)**

Soit un diviseur $D \in Div(X)$, alors il existe un diviseur $\overline{D} \in Div(X)$ tel que :

$$D \sim \overline{D},\ deg\, D = deg\, \overline{D} \text{ et } \left|\overline{D}\right| \leq 1.$$

Preuve

Soit un diviseur $D = \sum_{P \in X} n_P \langle P \rangle \in Div(X)$. On suppose qu'il existe deux points P et Q distincts de X tels que n_P et n_Q soient de même signe et non nuls.

Soit D' un diviseur d'une droite L passant par P et Q, alors

$$D' = \langle P \rangle + \langle Q \rangle + \langle R \rangle - 3\langle \theta \rangle = div(L),$$

où R est le 3ème point de la droite L.

Nous avons alors deux cas à traiter.

1er cas :

Si n_P et n_Q sont strictement positifs, on obtient

$$|D-D'| \langle |D|.$$

Et comme D' est un diviseur d'une droite, alors

$$deg\,(D) = deg\,(D-D')$$
$$\text{et } D \sim (D-D'),$$

d'où le diviseur $D_1 = D-D'$ convient.

2ème cas :

Si n_P et n_Q sont strictement négatifs, on aura

$$|D+D'| \langle |D|.$$

Et D' est un diviseur d'une droite, on obtient

$$deg\,(D) = deg\,(D+D')$$
$$\text{et } D \sim (D+D'),$$

d'où le diviseur $D_1 = D+D'$ convient.

On continue la réduction prescrite dans le 1er cas et le 2ème cas jusqu'à ce que nous obtenons un diviseur de la forme :

$$D = n_P\langle P\rangle - n_Q\langle Q\rangle + s\langle\theta\rangle,$$

avec $n_P \geq 0$, $n_Q \geq 0$ et $s \in \mathbb{Z}$.

Nous utilisons le diviseur D'' d'une droite L

$$D'' = 2\langle P\rangle + \langle Q\rangle - 3\langle\theta\rangle,$$

nous obtenons la norme de $D_2 = D - D''$

$$|D_2| \langle |D|.$$

Comme D'' est un diviseur d'une droite, on a alors

$$deg\ D = deg\ D_2$$
$$\text{et } D \sim D_2.$$

A la fin, nous obtenons un diviseur $\overline{D} \in Div(X)$ tel que :

$$D \sim \overline{D},\ deg\,D = deg\,\overline{D} \text{ et } |\overline{D}| \leq 1. \qquad \blacksquare$$

Corollaire 5.2

Pour tout diviseur $D \in Div^0(X)$*, il existe un point unique* $P \in X$ *tel que*

$$D \sim \langle P \rangle - \langle \theta \rangle .$$

Preuve

Existence

Soit un diviseur $D \in Div^0(X)$, alors d'après le théorème de la réduction linéaire, il existe un diviseur $\overline{D} \in Div^0(X)$ tel que :

$$D \sim \overline{D} \text{ et } \left| \overline{D} \right| \leq 1 .$$

Puisque $deg\,\overline{D} = 0$, le diviseur $\overline{D}$ a l'une des deux formes suivantes

$$\overline{D} = \langle P \rangle - \langle \theta \rangle \text{ ou } \overline{D} = -\langle P \rangle + \langle \theta \rangle .$$

On va traiter ces deux cas du diviseur $\overline{D}$.

1) Si $\overline{D} = \langle P \rangle - \langle \theta \rangle$, donc on a le résultat du corollaire.

2) Si $\overline{D} = -\langle P \rangle + \langle \theta \rangle$, on considère le diviseur d'une droite L

$$(L) = 2\langle P \rangle - 2\langle \theta \rangle ,$$

on a alors

$$\overline{\overline{D}} = \overline{D} + (L) \sim \overline{D} .$$

D'où le résultat

$$\overline{D} \sim \overline{\overline{D}} = \langle P \rangle - \langle \theta \rangle .$$

L'unicité :

Supposons qu'il existe un autre point Q tel que

$$D \sim \langle Q \rangle - \langle \theta \rangle .$$

Il en résulte alors, l'équivalence de ces diviseurs

$$\langle P \rangle - \langle \theta \rangle \sim \langle Q \rangle - \langle \theta \rangle ,$$

cela signifie que le diviseur $\langle P \rangle - \langle Q \rangle$ est principal

$$(f) = \langle P \rangle - \langle Q \rangle .$$

Donc la fonction f admet un unique pôle Q, et on en déduit que f est un revêtement ramifié de $\mathbb{P}^1(\mathbb{C})$ de degré 1, alors

$$X \simeq \mathbb{P}^1(\mathbb{C}),$$

or le genre de X est égal à 1.

Il en résulte l'unicité du point P. ■

Proposition 5.3

Si P_1 , $P_2 \in X$, *il existe un unique point* $P_3 \in X$ *tel que le diviseur*

$$\langle P_1 \rangle + \langle P_2 \rangle + \langle P_3 \rangle - 3\langle \theta \rangle,$$

soit principal.

On note alors $\theta = 0$ et $P_1 + P_2 + P_3 = 0$, *ce qui définit une structure de groupe sur X, telle que l'application :*

$$\Phi : X \longrightarrow Pic^0(X)$$

$$Q \longrightarrow \Phi(Q) = \langle Q \rangle - \langle \theta \rangle,$$

soit un isomorphisme de groupes.

Preuve

Unicité

Si le diviseur $(f) = \langle P_1 \rangle + \langle P_2 \rangle + \langle P_3 \rangle - 3\langle \theta \rangle$, et P_4 un autre point de X tel que le diviseur $\langle P_1 \rangle + \langle P_2 \rangle + \langle P_4 \rangle - 3\langle \theta \rangle$ est principal

$$(f') = \langle P_1 \rangle + \langle P_2 \rangle + \langle P_4 \rangle - 3\langle \theta \rangle,$$

alors

$$\left(\frac{f'}{g} \right) = \langle P_3 \rangle - \langle P_4 \rangle .$$

Supposons que $P_3 \neq P_4$, et donc la fonction $\frac{f'}{g}$ est un revêtement ramifié de degré 1, ainsi un isomorphisme de X sur $\mathbb{P}^1(\mathbb{C})$, ce qui est absurde car $\mathbb{P}^1(\mathbb{C})$ est de genre 0.

Existence

Soient x , y les fonctions donnant le plongement de X dans $\mathbb{P}^2(\mathbb{C})$ par

$$Q \longrightarrow (x(Q), y(Q), 1).$$

Soit L la droite de $\mathbb{P}^2(\mathbb{C})$ passant par P_1 et $P_2 \in X \subset \mathbb{P}^2(\mathbb{C})$ d'équation $L : aU + bV + cW = 0$, c'est la tangente à X en P_1 si $P_1 = P_2$, et soit $f = ax + by + c$, alors f s'annule en P_1 et P_2 car $P_1 \in X \subset \mathbb{P}^2(\mathbb{C})$; $P_1 = (x(P_1), y(P_1), 1)$, on a :

$$f(P_1) = a\,x(P_1) + b\,y(P_1) + c.1,$$

comme $P_1 \in L$, on aura

$$f(P_1) = 0.$$

De même pour P_2

$$f(P_2) = 0.$$

Si $b \neq 0$, alors f est de degré 3 (unique pôle, triple, en θ) donc f a un troisième zéro P_3 sur la droite L, qui convient.

Si b=0, alors la fonction

$$f = a\,x + c$$

est de degré 2, car θ est l'unique pôle double de x donc de f, alors f n'a plus que les deux zéros P_1 et P_2 , et on prend $P_3 = \theta$ qui est sur la droite

$$aU + cW = 0,$$

avec($\theta = (0, 1, 0)$) dans le plan projectif $\mathbb{P}^2(\mathbb{C})$.

D'où le diviseur de f

$$\begin{aligned}(f) &= \langle P_1\rangle + \langle P_2\rangle - 2\langle\theta\rangle \\ &= \langle P_1\rangle + \langle P_2\rangle + \langle\theta\rangle - 3\langle\theta\rangle\ .\end{aligned}$$

Montrons que Φ est bijective :

Φ est surjective : soit $D \in Pic^0(X) = Div^0(X)/\sim$, d'après le lemme il existe un point $Q \in X$ tel que

$$D \sim \langle Q\rangle - \langle\theta\rangle,$$

cela signifie qu'il existe un point Q de X tel que

$$\Phi(Q) = D,$$

d'où la surjectivité de Φ.

Le point Q est unique :

Supposons qu'il existe un autre point $R \neq Q$ tel que

$$\langle Q\rangle - \langle\theta\rangle \sim \langle R\rangle - \langle\theta\rangle,$$

cela signifie que le diviseur

$$\langle Q\rangle - \langle\theta\rangle - \langle R\rangle + \langle\theta\rangle,$$

est un diviseur principal, et on pose

$$(f) = \langle Q\rangle - \langle\theta\rangle - \langle R\rangle + \langle\theta\rangle = \langle Q\rangle - \langle R\rangle .$$

ainsi f admet un seul pôle simple, donc f est un revêtement ramifié de degré 1 ce qui signifie que $X \cong \mathbb{P}^1(\mathbb{C})$, contradiction avec le fait que le genre de X est égal à 1, cela implique que Φ est bijective .

Montrons que Φ est un morphisme :

1/ Si $P_1 = -P_2$ (P_1 est l'inverse de P_2), d'une part, on a

$$\Phi\left(P_1 + P_2\right) = \Phi(0) = 0 .$$

D'autre part

$$\begin{aligned}\Phi\left(P_1\right) + \Phi\left(P_2\right) &= classe\left(\langle P_1\rangle - \langle\theta\rangle\right) + classe\left(\langle P_2\rangle - \langle\theta\rangle\right)\\ &= classe\left(\langle P_1\rangle + \langle P_2\rangle - 2\langle\theta\rangle\right),\end{aligned}$$

mais le diviseur

$$\langle P_1\rangle + \langle P_2\rangle - 2\langle\theta\rangle ,$$

est principal, donc sa classe est nulle

$$classe\left(\langle P_1\rangle + \langle P_2\rangle - 2\langle\theta\rangle\right) = 0.$$

2/ Si $P_1 \neq P_2$, soit P_3 le 3ième point de la droite L tel que

$$P_1 + P_2 + P_3 = 0 ,$$

qui s'écrit

$$P_1 + P_2 = -P_3 .$$

Soit L' la droite passant par P_3 et $-P_3$, alors les diviseurs de L' et L sont respectivement

$$div\,(L') = \langle P_3\rangle + \langle -P_3\rangle - 2\langle\theta\rangle$$

$$\text{et}\ \ div\,(L) = \langle P_1\rangle + \langle P_2\rangle + \langle P_3\rangle - 3\langle\theta\rangle .$$

Donc, on écrit $div(L)$ sous une autre forme

$$\langle P_1\rangle + \langle P_2\rangle + \langle P_3\rangle - 3\langle\theta\rangle = \left(\langle P_1\rangle - \langle\theta\rangle\right) + \left(\langle P_2\rangle - \langle\theta\rangle\right) + \left(\langle P_3\rangle - \langle\theta\rangle\right) \sim 0,$$

car c'est un diviseur d'une fonction méromorphe (de la droite L), donc

$$classe\left(\left(\langle P_1\rangle - \langle\theta\rangle\right) + \left(\langle P_2\rangle - \langle\theta\rangle\right) + \left(\langle P_3\rangle - \langle\theta\rangle\right)\right) = 0.$$

La structure du groupe de Picard de degré zéro nous permet d'écrire

$$classe\left(\langle P_1\rangle - \langle\theta\rangle\right) + classe\left(\langle P_2\rangle - \langle\theta\rangle\right) + classe\left(\langle P_3\rangle - \langle\theta\rangle\right) = 0,$$

et en ajoutant la classe du diviseur $(\langle -P_3\rangle - \langle\theta\rangle)$ dans chaque côté de l'égalité, on obtient

$$classe(\langle P_1\rangle - \langle\theta\rangle) + classe(\langle P_2\rangle - \langle\theta\rangle) + classe(\langle P_3\rangle - \langle\theta\rangle) + classe(\langle -P_3\rangle - \langle\theta\rangle) =$$
$$classe(\langle -P_3\rangle - \langle\theta\rangle).$$

La loi du groupe de $Pic^0(X)$ induite par celle du groupe $Div^0(X)$, nous donne

$classe(\langle P_1\rangle - \langle\theta\rangle) + classe(\langle P_2\rangle - \langle\theta\rangle) + classe(\langle P_3\rangle + \langle -P_3\rangle - 2\langle\theta\rangle) = classe(\langle -P_3\rangle - \langle\theta\rangle)$,

or l'élément $classe(\langle P_3\rangle + \langle -P_3\rangle - 2\langle\theta\rangle)$ est nul, car le diviseur $\langle P_3\rangle + \langle -P_3\rangle - 2\langle\theta\rangle$ est un diviseur de la droite L'.

Par conséquent

$$classe(\langle P_1\rangle - \langle\theta\rangle) + classe(\langle P_2\rangle - \langle\theta\rangle) = classe(\langle -P_3\rangle - \langle\theta\rangle),$$

il en résulte que

$$classe(\langle P_1 + P_2\rangle - \langle\theta\rangle) = classe(\langle P_1\rangle - \langle\theta\rangle) + classe(\langle P_2\rangle - \langle\theta\rangle),$$

avec $P_1 + P_2 = -P_3$.

D'où Φ vérifie l'axiome de morphisme de groupes

$$\Phi(P_1 + P_2) = \Phi(P_1) + \Phi(P_2). \qquad \blacksquare$$

Corollaire 5.4

Soient P_1, P_2 et P_3 *trois points de X, alors dans le plongement de X sur* $\mathbb{P}^2(\mathbb{C})$ *défini précédemment, on a :*

$$P_1 + P_2 + P_3 = 0 \textit{ si et seulement si } P_1,\ P_2 \text{ et } P_3 \textit{ sont alignés}.$$

Preuve

Si $P_1 + P_2 + P_3 = 0$, alors P_1 , P_2 , P_3 sont des zéros de la fonction f d'équation

$$f = ax + by + c,$$

qui est par définition une équation d'une droite, donc P_1 , P_2 , P_3 sont alignés.

Si P_1 , P_2 , P_3 sont alignés, alors P_1 , P_2 , P_3 sont des zéros de la droite L d'équation

$$L = ax + by + c,$$

son diviseur est égal à $\qquad (L) = \langle P_1\rangle + \langle P_2\rangle + \langle P_3\rangle - 3\langle\theta\rangle$.

Alors, on prend $\theta = 0$ et $P_1 + P_2 + P_3 = 0$. $\qquad \blacksquare$

II-6/ La jacobienne

Dans ce paragraphe on va démontrer que toute courbe elliptique X sur $\mathbb{C}$ est isomorphe à un tore $\mathbb{C}/\Lambda$. Pour cela on définit une intégration sur un chemin dans X d'une 1-forme différentielle sur X.

Définition 6.1

Soit $\omega = f\ dx + g\ dy$ *une 1-forme différentielle sur X, et*

$$\gamma \ : \ [0,1] \longrightarrow X$$
$$t \longrightarrow \gamma(t)$$

un chemin dans X, l'intégrale de la différentielle ω *sur* γ *est égal à*

$$\int_\gamma \omega = \int_0^1 \left(f(\gamma(t))\frac{dx}{dt} + g(\gamma(t))\frac{dy}{dt} \right) dt\,.$$

Cette intégrale est bien définie grâce à la matrice jacobienne par changement de carte, en effet, soit $h' = x_1 + iy_1$ une autre carte de X, alors :

$$\int_\gamma \omega = \int_0^1 \left(f_1(\gamma(t))\frac{dx_1}{dt} + g_1(\gamma(t))\frac{dy_1}{dt} \right) dt$$

$$= \int_0^1 \left(f_1(\gamma(t))\frac{dx}{dt} + g_1(\gamma(t))\frac{dy}{dt} \right) \ \mathrm{J}\left(h' \circ h^{-1}\right) dt$$

$$= \int_0^1 \left(f(\gamma(t))\frac{dx}{dt} + g(\gamma(t))\frac{dy}{dt} \right) dt \cdot$$

On a $\dim_{\mathbb{C}} \Omega(X) = g = 1$, alors il existe une différentielle holomorphe ω non identiquement nulle (unique à $\mathbb{C}^*$ près), et sans zéro car $deg(\omega) = 2g - 2 = 0$.

Du point de vue courbe algébrique, si on voit X comme cubique lisse de $\mathbb{P}^2(\mathbb{C})$ (proposition 4.3), d'équation

$$y^2 = 4x^3 - g_2 x - g_3 \ ;$$

On a la proposition suivante :

Proposition 6.1

Soient $\mathrm{P}\,(x, y) = y^2 - 4x^3 + g_2 x + g_3 \in \mathbb{C}[x, y]$, $C_{\mathrm{P}} = \{(x, y) \in \mathbb{C}^2 \text{ tel que } \mathrm{P}(x, y) = 0\}$ *et* $X = X_{\mathrm{P}}$ *est une surface de Riemann associée à la courbe algébrique* C_{P} *; Alors la différentielle* $\omega = \dfrac{2dx}{\mathrm{P}'_y(x, y)} = \dfrac{dx}{y}$ *forme une base des différentielles holomorphes* $\Omega(X)$ *sur* X.(voir [10], [16])

On note θ le point choisit de X dans le plongement sur $\mathbb{P}^2(\mathbb{C})$, $\theta = (0, 1, 0)$. Soit γ un chemin de θ à Q sur X, autrement dit l'application

$$\gamma : [0,1] \longrightarrow X,$$

est continue, telle que $\gamma(0) = \theta$ et $\gamma(1) = Q$, on définit :

$$I(\gamma) = \int_\gamma \omega \in \mathbb{C}.$$

Pour définir un isomorphisme de X dans $\mathbb{C}/\Lambda$, nous avons besoin de définir le premier groupe d'homologie sur X.

Définition 6.2

Un 2-simplexe d'une surface X est une injection continue T $\longrightarrow$ *X, où T est le triangle de sommets 0, 1,* $e^{i\pi/3}$ *dans* $\mathbb{C}$*. L'image est appelée un triangle dans X.*

On dit que la surface X est triangulable s'il existe des 2-simplexes

$$f_i : T \longrightarrow X,$$

dont les images recouvrent X, tels que pour tout point $P \in X$*,*

1) *si P n'est pas sur une arête, il appartient à un unique triangle* $f_i(T)$*, qui est alors un voisinage de P.*
2) *si P est sur une arête "a", mais n'est pas sur un sommet, il appartient exactement à deux triangles* $t_i = f_i(T)$ *et* $t_j = f_j(T)$*, tels que* $t_i \cap t_j = a$ *et* $t_i \cup t_j$ *est un voisinage de P.*
3) *si P est un sommet, il appartient à un nombre fini de triangles* t_i*, ...,* t_k *; ceux-ci ont P pour sommet, leur réunion* $\bigcup_{i=1}^{k} t_i$ *est un voisinage de P, avec* t_i *et* t_{i+1} $(1 \le i \le t-1)$ *ont exactement une arête commune.*

Théorème 6.2

Toute surface de Riemann compacte est orientable et triangulable.(voir [2])

On fixe une triangulation sur *X*, un 0-simplexe est un sommet d'un triangle t_i de *X*, un 1-simplexe est une arête d'un triangle t_i de *X* et un 2-simplexe est une face orientée d'un triangle de *X*.

L'ensemble

$$C_n = C_n(X) = \{ \sum m_i\, a_i,\ m_i \in \mathbb{Z},\ a_i = n - simplexe \},$$

$n = 0, 1, 2$, est un groupe abélien libre sur les *n*-simplexes.

Un élément de $C_n(X)$ est appelé n-chaîne.

On définit un opérateur bord $\partial : C_n \longrightarrow C_{n-1}$, pour un o-simplexe $\langle P_1 \rangle$, on a $\partial \langle P_1 \rangle = 0$.

L'image d'un 1-simplexe $\langle P_1, P_2 \rangle$ par ∂ est égale à

$$\partial \langle P_1, P_2 \rangle = \langle P_1 \rangle - \langle P_2 \rangle,$$

et l'image d'un 2-simplexe $\langle P_1, P_2, P_3 \rangle$ par l'opérateur ∂ est égale à

$$\partial \langle P_1, P_2, P_3 \rangle = \langle P_1, P_2 \rangle + \langle P_2, P_3 \rangle + \langle P_3, P_1 \rangle .$$

Par linéarité de ∂, on définit le bord d'une *n*-chaîne.

L'image $\mathcal{B}_1(X)$ de C_2 par $\partial : C_2 \longrightarrow C_1$ constitue les bords, le noyau $\mathcal{Z}_1(X)$ de $\partial : C_1 \longrightarrow C_0$ les cycles, on vérifie que $\partial^2 = 0$, donc tout bord est un cycle ; d'où l'inclusion $\mathcal{B}_1(X) \subset \mathcal{Z}_1(X)$.

Définition 6.3

Le groupe quotient $\mathcal{H}_1(X) = \mathcal{Z}_1(X) / \mathcal{B}_1(X)$ *est le premier groupe d'homologie de X.*

Ce groupe ne dépend pas de la triangulation choisie.(voir [10])

Proposition 6.3

Le groupe $\mathcal{H}_1(X)$ *est isomorphe à* $\mathbb{Z}^2$.

Dans la définition de l'intégrale $I(\gamma)$, si on change γ par un autre chemin γ' de *P* à *Q* sur *X*, alors :

$$\int_{\gamma}\omega+\int_{-\gamma'}\omega=\int_{\gamma-\gamma'}\omega \quad ,$$

où $-\gamma'$ est le chemin inverse de γ'.

$\gamma-\gamma'$ forme un cycle, $\gamma-\gamma' \in \mathcal{H}_1(X)$, donc :

$$\int_{\gamma-\gamma'}\omega \in \Lambda ,$$

avec Λ est l'ensemble

$$\Lambda=\left\{\int_{\gamma}\omega ,\gamma \in \mathcal{H}_1(X)\simeq \mathbb{Z}^2\right\}.$$

On a donc une application bien définie :

$$I : X \longrightarrow \mathbb{C}/\Lambda$$

$$Q \longrightarrow I(Q)=\int_{P}^{Q}\omega.$$

I est analytique ; donc pour γ_0 un chemin fixé de *P* à Q_0, et *U* un voisinage simplement connexe de Q_0, alors :

$$I : U \longrightarrow \mathbb{C}$$

$$Q \longrightarrow \int_{\gamma_0}\omega+\int_{Q_0}^{Q}\omega ,$$

est bien définie, si γ_1 et γ_2 deux chemins de Q_0 à *Q*, alors :

$$\int_{\gamma_1}\omega-\int_{\gamma_2}\omega=\int_{\gamma_1-\gamma_2}\omega \in \Lambda ,$$

Lemme 6.4

Le groupe Λ est un réseau de $\mathbb{C}$.

Preuve

Le premier groupe d'homologie $\mathcal{H}_1(X)$ est isomorphe à $\mathbb{Z}^2$, cela implique que Λ est engendré par les deux périodes :

$$\Sigma_i=\int_{\gamma_i}\omega ,\ i=1,2$$

où γ_1, γ_2 est une base du groupe d'homologie $\mathcal{H}_1(X)$.

On raisonne par l'absurde, supposons qu'elles sont $\mathbb{R}$-linéairement dépendantes, alors ils existent $\lambda_1, \lambda_2 \in \mathbb{C}^*$ tels que :

$$\Sigma_1 = \int_{\gamma_1} \lambda_1 \omega \text{ et } \Sigma_2 = \int_{\gamma_2} \lambda_2 \omega,$$

sont imaginaires ; $\Sigma_1, \Sigma_2 \in i\mathbb{R}$.

Comme I est analytique, alors la fonction

$$I' : X \longrightarrow \mathbb{R}$$

$$Q \longrightarrow I'(Q) = \mathcal{R}e\left(\int_P^Q \omega\right),$$

est harmonique.

cette fonction est constante par le principe du maximum, le maximum est atteint sur la frontière de l'adhérence $\overline{U}$.

Donc sur un ouvert simplement connexe, $I(Q)$ est analytique de partie réelle constante, il en résulte que $I(Q)$ est constante modulo

$$\Lambda = \mathbb{Z}\Sigma_1 + \mathbb{Z}\Sigma_2 \subset i\,\mathbb{R},$$

d'où ω est identiquement nulle, ce qui est absurde. Donc le quotient $\mathbb{C}/\Lambda$ est un tore.

On peut définir sur le tore $\mathbb{C}/\Lambda$ une structure analytique complexe de dimension 1, et on obtient par suite une surface de Riemann compacte $\mathbb{C}/\Lambda$. ■

Finalement, nous avons démontrer que l'application I est bien définie dans $\mathbb{C}$ modulo Λ.

Proposition 6.5

L'application

$$I : X \longrightarrow \mathbb{C}/\Lambda$$

$$Q \longrightarrow I(Q) = \int_P^Q \omega,$$

est un isomorphisme de surfaces de Riemann.

Preuve

L'application I est un morphisme de surfaces de Riemann, non constant car ω est non nulle.

D'une part on a $I(X)$ est fermé car $I(X)$ est un compact ; l'image d'un compact par une application continue.

D'autre part $I(X)$ est ouvert car I est une application ouverte, comme $\mathbb{C}/\Lambda$ est connexe, alors $I(X) = \mathbb{C}/\Lambda$; d'où la surjectivité de I.

Montrons que I est injective :

l'application I est un revêtement étale de $\mathbb{C}/\Lambda$ grâce à la formule de Hurwitz qui s'écrit :

$$0 = 0 + \sum_{x \in X} \left(e_x(I) - 1\right) \ ;$$

donc $e_x(I) = 1$ pour tout $x \in X$.

On a encore l'application

$$\pi : \mathbb{C} \longrightarrow \mathbb{C}/\Lambda,$$

est un revêtement universel de $\mathbb{C}/\Lambda$, donc on peut voir X comme quotient de $\mathbb{C}$ par un sous groupe Λ' de Λ.

Montrons que $\Lambda \subset \Lambda'$:

Soit $\lambda = \int_\gamma \omega \in \Lambda$ où γ est un cycle, alors $\gamma = \gamma_1 - \gamma_2$ avec γ_1 et γ_2 deux chemins de P au même point $Q \in X$, donc modulo Λ', la valeur

$$I(\gamma_1) = I(\gamma_2) = r \in \mathbb{C}/\Lambda',$$

cela implique que

$$\lambda = \int_\gamma \omega = I(\gamma_1) - I(\gamma_2) \in \Lambda',$$

d'où $\Lambda \subset \Lambda'$.

Il en résulte que I est un isomorphisme de surfaces de Riemann. Cet isomorphisme induit donc une structure de groupe sur $\mathbb{C}/\Lambda$. ■

6.1/ Les fonctions méromorphes sur $\mathbb{C}/\Lambda$

D'après la proposition précédente, une courbe elliptique est isomorphe à un tore $\mathbb{C}/\Lambda$. Par définition : les fonctions méromorphes sur le tore $\mathbb{C}/\Lambda$ sont les fonctions méromorphes sur $\mathbb{C}$ qui sont Λ-périodiques.

La fonction $\wp$ de Weierstrass

Définition 6.4

La fonction $\wp$ de Weierstrass relative à un réseau Λ est la fonction :

$\wp : \mathbb{C} \longrightarrow \mathbb{C}$ *de valeur* $\wp(z) = \dfrac{1}{z^2} + \displaystyle\sum_{\theta \in \Lambda - \{0\}} \left(\dfrac{1}{(z-\theta)^2} - \dfrac{1}{\theta^2} \right)$.

Proposition 6.6

$\wp$ est méromorphe sur $\mathbb{C}$ et dérivable. La $\wp$ (z) converge absolument et uniformément sur tout compact du tore $\mathbb{C}/\Lambda$

Proposition 6.7

La fonction $\wp$ est périodique de périodes θ_1 et θ_2 la base du tore Λ. La fonction $\wp$ *(z)* est paire.

Preuve

Calculons $\wp$ *(-z)*

$$\wp(z) = \frac{1}{z^2} + \sum_{\theta \in \Lambda - \{0\}} \left(\frac{1}{(z-\theta)^2} - \frac{1}{\theta^2} \right)$$

$$= \frac{1}{z^2} + \sum_{\theta \in \Lambda - \{0\}} \left(\frac{1}{(z+\theta)^2} - \frac{1}{\theta^2} \right). \qquad (1)$$

On remplace l'élément $-z$ dans la formule (1), on obtient

$$\wp(-z) = \frac{1}{(-z)^2} + \sum_{\theta \in \Lambda - \{0\}} \left(\frac{1}{(-z+\theta)^2} - \frac{1}{\theta^2} \right)$$

$$= \frac{1}{z^2} + \sum_{\theta \in \Lambda - \{0\}} \left(\frac{1}{(z-\theta)^2} - \frac{1}{\theta^2} \right),$$

d'où $\wp(-z) = \wp(z)$, donc $\wp$ est paire.

La fonction dérivée de $\wp$ est égale à

$$\wp'(z) = \sum_{\theta \in \Lambda} \frac{-2}{(z-\theta)^3},$$

Nous allons vérifier que pour tout élément $z \in \mathbb{C}$, les valeurs de $\wp'$ en $z+\theta_1$, $z+\theta_2$ et z sont égales

$$\wp'(z+\theta_1) = \wp'(z+\theta_2) = \wp'(z),$$

ce qui signifiera que $\wp'$ est périodique sur Λ.

On considère la fonction

$$f(z) = \wp(z+\theta_1) - \wp(z).$$

On dérive la fonction *f*, on obtient

$$f'(z) = \wp'(z+\theta_1) - \wp'(z),$$

et comme $\wp'$ est périodique, alors cette dérivée est nulle, donc on aura

$$f(z) = \wp(z+\theta_1) - \wp(z) = c, \tag{2}$$

c est une constante.

On remplace la valeur $z = -\dfrac{\theta_1}{2}$ dans la formule (2), on obtient

$$c = \wp\left(\frac{\theta_1}{2}\right) - \wp\left(-\frac{\theta_1}{2}\right) = 0,$$

car $\wp$ est paire.

Il en résulte que

$$\wp(z+\theta_1) = \wp(z).$$

On fait la même chose pour θ_2, on trouve

$$\wp(z+\theta_1) = \wp(z+\theta_2) = \wp(z).$$

La fonction $\wp$ est donc périodique de période θ_1 et θ_2, et méromorphe, les pôles de $\wp$ sont les éléments de Λ, ils sont tous d'ordre 2. Ainsi la fonction $\wp$ est méromorphe sur $\mathbb{C}/\Lambda$, dont 0 est le seul pôle double modulo Λ. ■

Proposition 6.8

Le corps des fonctions méromorphes sur X= $\mathbb{C}/\Lambda$ *est* $\mathcal{M}(X) = \mathbb{C}(\wp, \wp')$.

Preuve

Comme $\wp$ est un revêtement ramifie de degré 2, on a

$$[\mathcal{M}(X) : \mathbb{C}(\wp)] = 2,$$

et puisque $\wp' \notin \mathbb{C}(\wp)$, car $\wp'$ a l'élément 0 comme pôle d'ordre 3 impair ; il en résulte que le corps des fonctions méromorphes sur *X* est engendré sur $\mathbb{C}$ par deux éléments $\wp$ et $\wp'$

$$\mathcal{M}(X) = \mathbb{C}(\wp, \wp'). \quad ■$$

CHAPITRE III
POINTS DE WEIERSTRASS

Une courbe hyperelliptique *X* de genre g possède un ensemble de points canoniques : ses points de Weierstrass. Dans le cas où $g=1$, la suite des trous de *X* est réduite 1. Nous déterminons l'équation plane d'une courbe hyperelliptique de genre $g \geq 2$. Nous étudions les points de Weierstrass de *X* et nous déterminons le groupe engendré par ces points dans la jacobienne de *X*.

III-1/ Équation plane des courbes hyperelliptiques

Une courbe elliptique admet un plongement comme cubique plane lisse dans le plan projectif $\mathbb{P}^2(\mathbb{C})$. Dans la suite nous cherchons la forme de l'équation d'une courbe hyperelliptique.

Théorème 1.1

Soient X une courbe hyperelliptique et f *un revêtement ramifié*

$$f : X \longrightarrow \mathbb{P}^1(\mathbb{C}),$$

de degré 2, *et* $z_1, ..., z_{2g+2}$ *les points de ramification de* f *sur* $\mathbb{P}^1(\mathbb{C})$*, alors X est la surface de Riemann associée à la courbe d'équation*

$$h^2 = \prod_{i=1}^{2g+2} (f - z_i).$$

Preuve

Le degré de l'extension $\mathcal{M}(X)$ de $\mathbb{C}(f)$ et égal au degré de ramification de f

$$[\mathcal{M}(X) : \mathbb{C}(f)] = 2, \qquad (1)$$

soit une fonction $h \in \mathcal{M}(X) \setminus \mathbb{C}(f)$, la formule (1) implique que

$$\mathcal{M}(X) = \mathbb{C}(f, h),$$

il en résulte qu'une équation de *X* est donnée par un polynôme de la forme

$$h^2 - 2\,a\,h + c = 0, \qquad (2)$$

avec $a, c \in \mathbb{C}(f)$.

L'équation (2) s'écrit

$$(h-a)^2 + c - a^2 = 0,$$

par le changement de variable suivant

$$\begin{cases} h_1 = h - a \\ f_1 = f \end{cases},$$

on obtient

$$h_1^2 = a^2 - c,$$

où $a^2 - c = \Phi(f) \in \mathbb{C}(f)$, et $h_1 \in \mathcal{M}(\mathrm{X}) \setminus \mathbb{C}(f)$; c'est-à-dire $\mathcal{M}(X) = \mathbb{C}(f, h_1)$.

La fraction rationnelle $\Phi(f)$ en f se décompose complètement dans $\mathbb{C}(f)$, on a alors

$$h_1^2 = k \prod_{i=1}^{s} (f - c_i)^{r_i}, \qquad (3)$$

avec $0 \neq k \in \mathbb{C}$, $c_i \in \mathbb{C}$ et $r_i \in \mathbb{Z}$.

Soit $r_i = 2s_i + l_i, s_i \in \mathbb{Z}$, et $l_i \in \{0,1\}$, on définit

$$h_2 = h_1 \prod_{i=1}^{i=s} (f - c_i)^{-s_i}, \qquad (4)$$

alors $\mathcal{M}(X) = \mathbb{C}(f, h_2)$, et les formules (3) et (4) impliquent que

$$h_2^2 = \Phi'(f) = \prod_{i=1}^{r} (f - c_i),$$

on remarque que $\Phi'(f) \in \mathbb{C}[f]$, c_i sont des nombres complexes distincts.

Nous démontrons que $r = 2g + 2$ ou $2g + 1$ et $z_i = c_i$, soient Q_i un zéro de $f - c_i$; $f(Q_i) = c_i$ et r le degré de $\Phi'(f)$.

Supposons que Q_∞ est un pôle simple de f, alors

$$ord_{Q_i}(\Phi'(f)) = 1 \text{ et } ord_{Q_i}(\Phi'(f)) = -r.$$

Nous définissons l'entier

$$\tau_P = \mathrm{p\,gcd}(2, ord_P(\Phi'(f))),$$

donc, nous déduisons τ_Q sur chaque point Q de X

$$\tau_{Q_i} = 1 \text{ pour } i = 1, \ldots, r.$$

$$\tau_{Q_\infty} = \begin{cases} 1 & \text{si } r \equiv 1 \bmod 2 \\ 2 & \text{si } r \equiv 0 \bmod 2 \end{cases}$$

$$\tau_Q = 2 \text{ pour tout autre points de } X.$$

Comme l'indice de ramification de f en un point P est donné en fonction de τ_P

$$e_P(f) = \frac{2}{\tau_P},$$

où $P \in X$.

Cela implique que Q_i pour $i = 1,...,r$ sont des points de ramification. On applique la formule de Hurwitz sur *f*, on obtient

$$2g - 2 = (2 \times 0 - 2)2 + \sum_{Q \in X} (e_Q(f) - 1) ,$$

$$= \begin{cases} -4 + r + 1 & si \ r \equiv 1 \bmod 2 \\ -4 + r & si \ r \equiv 0 \bmod 2 \end{cases}$$

$$= \begin{cases} r - 3 & si \ r \equiv 1 \bmod 2 \\ r - 4 & si \ r \equiv 0 \bmod 2 \end{cases},$$

il en résulte que

1) $r = 2g + 1$ si Q_∞ est un point de ramification.

2) ou $r = 2g + 2$ si Q_∞ n'est pas un point de ramification.

D'où X admet une équation plane de la forme

$$h^2 = \prod_{i=1}^{r} (f - z_i) \text{ avec } r = 2g + 2 \text{ ou } 2g + 1. \qquad \blacksquare$$

La réciproque de ce théorème est : à toute courbe donnée par l'équation ci-dessus est hyperelliptisue, donc elle est paramétrée par ses $2g + 2$ points de ramification, on détermine son genre à l'aide de la formule de Hurwitz, ainsi le genre est égal à la partie entière de $\frac{r-1}{2}$.

En particulier, il existe des courbes hyperelliptiques de chaque genre. (voir [10])

Voici quelques exemples de courbes pour g donné. On peut les décrire assez explicitement. (voir [14], [10]) :

Pour $g = 0$, X est la droite projective $\mathbb{P}^1(\mathbb{C})$.

Pour $g = 1$, X est une cubique projective non singulière de $\mathbb{P}^2(\mathbb{C})$, c'est une cubique.

Pour $g = 2$, X est un revêtement ramifié de $\mathbb{P}^1(\mathbb{C})$ à deux feuillets, avec 6 points de ramification ; c'est une courbe hyperelliptique qui a un modèle affine plan d'équation $y^2 = \mathrm{P}(x)$ de degré 5 ou 6.

Pour $g = 3$: Il y a deux types de courbes hyperelliptiques

a) Les courbes hyperelliptiques qui sont revêtements doubles de $\mathbb{P}^1(\mathbb{C})$ à 8 points de ramification. Elles ont un modèle plan d'équation $y^2 = \mathrm{P}(x)$ de degré 7 ou 8.

b) Les quartiques planes non singulières dans $\mathbb{P}^2(\mathbb{C})$.

Pour $g = 4$: Il y a deux types de courbes hyperelliptiques

a) Courbes hyperelliptiques qui sont revêtements doubles de $\mathbb{P}^1(\mathbb{C})$ à 10 points de ramification. Elles ont un modèle plan d'équation $y^2 = \mathrm{P}(x)$ de degré 9 ou 10.

b) Sextiques lisses X de $\mathbb{P}^3(\mathbb{C})$, X est l'intersection complète d'une quadrique et d'une cubique.

Pour $g = 5$:

a) Courbes hyperelliptiques qui sont revêtements doubles de $\mathbb{P}^1(\mathbb{C})$ à 12 points de ramification. Elles ont un modèle plan d'équation $y^2 = \mathrm{P}(x)$ de degré 11 ou 12.

b) Courbes lisses de degré 8 dans $\mathbb{P}^4(\mathbb{C})$.

Pour $g = 6$:

a) Courbes hyperelliptiques qui sont revêtements doubles de $\mathbb{P}^1(\mathbb{C})$ à 14 points de ramification. Elles ont un modèle plan d'équation $y^2 = \mathrm{P}(x)$ de degré 13 ou 14.

b) Les courbes lisses de degré 10 dans $\mathbb{P}^5(\mathbb{C})$.

III-2/ Involution hyperelliptique

Une condition nécessaire et suffisante pour qu'une surface X de Riemann compacte soit hyperelliptique, est l'existence d'un automorphisme de X d'ordre 2.

Théorème 2.1

Une surface de Riemann X est hyperelliptique si et seulement s'il existe un automorphisme J

sur X d’ordre 2 fixant $2g+2$ points exactement.

Preuve

Supposons que X est une courbe hyperelliptique, alors soit un morphisme de degré 2

$$f : X \longrightarrow \mathbb{P}^1(\mathbb{C}).$$

Soit un automorphisme $J : X \longrightarrow X$

par $J = f^{-1} \circ f$.

L’ensemble quotient $X/(J)$ possède une structure de surface de Riemann.

Soit $\tilde{g}$ le genre de $X/(J)$. La formule de Hurwitz implique l’égalité

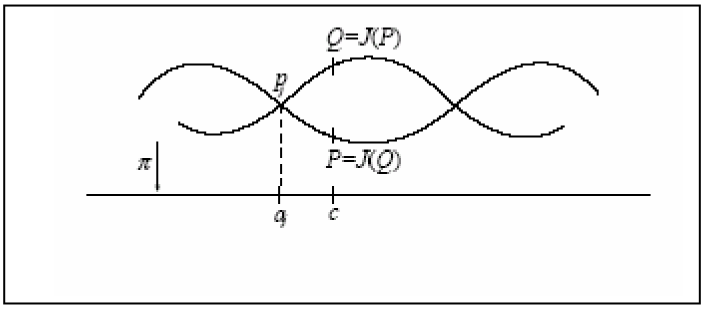
$$2g-2 = 2\left(2\tilde{g}-2\right)+2g+2,$$

Il en résulte que la surface $X/(J)$ est isomorphe à $\mathbb{P}^1(\mathbb{C})$.

Définition 2.1

L’automorphisme J est l’involution hyperelliptique de la surface X.

La figure ci-dessous est un exemple d'une involution hyperelliptique.



Surface hyperelliptique et involution hyperelliptique.

III-3/ La loi de groupe sur une courbe hyperelliptique

Dans ce paragraphe, nous nous proposons de définir une structure de groupe sur une courbe hyperelliptique.

Contrairement aux courbes elliptiques, il n'y pas de loi de groupe définissable directement sur l'ensemble des points de la courbe hyperelliptique *X*, c'est pour cela, on étudie la jacobienne de *X*.

Il y a deux types de construction de la loi de groupe sur la jacobienne de *X*, l'un à partir des diviseurs, et l'autre par intégration de formes différentielles.

Le théorème d'Abel-Jacobi montre qu'il existe un isomorphisme entre ces groupes.

Définition 3.1

Le groupe de Picard d'une courbe hyperelliptique X est l'ensemble quotient :

$$Pic^0(X) = \{diviseurs\ de\ \deg ré\ 0\} / \{diviseurs\ de\ \ fonctions\},$$

Soit *X* une courbe hyperelliptique de genre *g*, alors *X* s'obtient topologiquement en recollant les 4*g* côtés d'un polygone $\mathcal{P}$. (voir [16])

Proposition 3.1

Soit ω différentielle méromorphe sur X, et $\mathcal{P}$ une représentation polygonale de X dont le bord évite les pôles. Soit $O \in \overset{\circ}{\mathcal{P}}$ (l'intérieur de $\mathcal{P}$) ; pour $\phi \in \Omega(X)$, soit $f(P) = \int_O^P \phi$ elle est bien définie dans $\overset{\circ}{\mathcal{L}}$. Alors

$$2i\pi \sum_{P\in X} res_P(f\omega) = -\sum_{i=1}^{2g} \alpha_i\, \beta_i\ ,$$

où $\alpha_i = \int_{a_i} \omega\, , \beta_i = \int_{b_i} \phi.$

Nous appliquerons ce résultat à toute une base $\phi_1, \ldots, \phi_g$ de $\Omega(X)$; il est commode d'introduire une notation vectorielle :

$$\Phi = (\phi_1, \ldots, \phi_g), \quad F(P) = \int_O^P \Phi = \left(\int_O^P \phi_k\right)_{k=1,\ldots,g},$$

$$A_i = \int_{a_i} \Phi \in \mathbb{C}^g, \text{ et } B_i = \int_{b_i} \Phi \in \mathbb{C}^g \;;$$

avec a_i, b_i sont des éléments du polygone $\mathcal{P}$.

Les A_i et $B_i, i = 1, \ldots, 2g$ sont les mêmes à permutation et au signe près, d'où le résultat :

$$2i\pi \sum_{P \in X} res_P(F\omega) = -\sum_{i=1}^{2g} \alpha_i B_i \in \mathbb{C}. \qquad (1)$$

Les côtés a_i, b_i forment des cycles sur la surface *X*. (voir [2], [16])

Définition 3.2

Soit $\phi_1, \ldots, \phi_g$ une base de l'espace vectoriel des 1-formes différentielles holomorphes $\Omega(X)$, le groupe Λ de leurs périodes est l'ensemble :

$$\Lambda = \left\{\left(\int_\gamma \phi_1, \ldots, \int_\gamma \phi_g\right); \gamma \in \mathcal{H}_1(X) \simeq \mathbb{Z}^2\right\} \subset \mathbb{C}^g.$$

Ce groupe est engendré par les A_i ou par les B_i, $i = 1, \ldots, 2g$.

Définition 3.3

Le groupe quotient $J(X) = \mathbb{C}^g / \Lambda$ est la jacobienne de la surface X.

Proposition 3.2

Si $(x_i)_i \in \mathbb{C}^{2g}$, alors $\sum_{i=1}^{2g} x_i B_i = 0$ si et seulement s'il existe $B \in \mathbb{C}^g$, tel que $x_i = B A_i$, pour tout i=1,…,2g. (voir [16])

Théorème 3.3 (Abel-Jacobi)

L'application

$$\Psi : \quad Div^0(X) \longrightarrow \mathbb{C}^g$$
$$D = \sum_{P \in X} n_P \langle P \rangle \longrightarrow \Psi(D) = \sum_{P \in X} n_P F(P) = \left(\sum_{P \in X} n_P \int_O^P \phi_k \right)_{k=1,\dots,g},$$

induit un isomorphisme

$$\Psi : Pic^0 \longrightarrow J(X),$$

il est indépendant du choix de O à l'intérieur du polygone $\mathcal{P}$.

Preuve

La preuve de ce théorème se répartie en trois étapes.

1) Montrons que Ψ est bien définie, et indépendante du choix de O :

Soit un diviseur $D = \sum_{P \in X} n_P = (f)$ principal. Montrons que $\Psi(D) \in \Lambda$, soit $\omega = \frac{df}{f}$ une différentielle méromorphe sur X, alors son résidu est égal à

$$res_P \omega = ord_P f = n_P. \tag{2}$$

Les formules (1) et (2) impliquent que

$$\sum_{P \in X} n_P F(P) = \sum_{P \in X} res_P F\omega = -\frac{1}{2i\pi} \sum_{i=1}^{2g} B_i \int_{a_i} \frac{df}{f} \in \sum_{i=1}^{2g} B_i \mathbb{Z} = \Lambda,$$

$\log(f)$ est bien définie modulo $2i\pi$, et localement (au voisinage de P), on obtient

$$\int_P^Q \frac{df}{f} = \log(f(Q)) - \log(f(P)).$$

Donc nous intégrons sur les cycles a_i, nous trouvons

$$\int_{a_i} \frac{df}{f} \in 2i\pi\,\mathbb{Z},$$

d'où Ψ est bien définie.

L'intégrale entre O' et P se décompose

$$\sum_{P \in X} n_P \int_{O'}^P \phi_k = \sum_{P \in X} n_P \left(\int_{O'}^O \phi_k + \int_O^P \phi_k \right)$$

$$= \left(\sum_{P \in X} n_P \right) \int_{O'}^{O} \phi_k + \sum_{P \in X} n_P \int_{O}^{P} \phi_k \ ,$$

puisque le diviseur *D* est de degré 0

$$\sum_{P \in X} n_P \int_{O'}^{P} \phi_k = \sum_{P \in X} n_P \int_{O}^{P} \phi_k \ ,$$

il en résulte que Ψ est indépendante du point *O*.

2) Montrons que Ψ est injective (théorème d'Abel)

Soit un diviseur $D = \sum_{P \in X} n_P \in Div_0(X)$ tel que $\Psi(D) \in \Lambda$, nous montrons que $D = (f)$, pour une fonction f ; donc *D* est un diviseur principal.

Soit ω une différentielle méromorphe n'ayant que des pôles simples, et de résidus n_P en *P*, une telle différentielle existe. (voir [9])

La formule (1) implique que

$$\begin{aligned} -\frac{1}{2i\pi} \sum_{j=1}^{2g} \omega_j B_j &= \sum_{P \in X} res_P F\omega \\ &= \sum_{P \in X} n_P F(P) \qquad (3) \\ &= \Psi(D). \end{aligned}$$

L'image $\Psi(D)$ est dans le groupe Λ ; elle est de la forme

$$\Psi(D) = \sum_{j=1}^{2g} m_j B_j \ , \qquad (4)$$

où $m_j \in \mathbb{Z}$.

Les formules (3) et (4) impliquent que

$$\sum_{j=1}^{2g} \left(\omega_j + 2i\pi\, m_j \right) B_j = 0 \ ,$$

d'après la proposition 3.2, on obtient

$$\omega_j + 2i\pi\, m_j = B A_j \ , \qquad (5)$$

pour un $B \in \mathbb{C}^g$, et j=1,…, g.

Supposons que $\int\limits_{a_j} \omega \in 2i\pi\mathbb{Z}$, sinon nous allons définir une différentielle ω' qui satisfera $\int\limits_{a_j} \omega' \in 2i\pi\mathbb{Z}$, et qui a les même pôles et résidus que ω. Soit la différentielle suivante

$$\omega' = \omega - B\Phi .$$

Cette différentielle a les mêmes pôles et résidus que ω, car Φ est une forme différentielle holomorphe sur X ; on intègre ω' sur a_j, on aura

$$\int\limits_{a_j} \omega' = \int\limits_{a_j} \omega - \int\limits_{a_j} B\Phi = \omega_j - B\int\limits_{a_j} \Phi = \omega_j - BA_j . \qquad (6)$$

Les formules (5) et (6) impliquent que

$$\int\limits_{a_j} \omega' \in 2i\pi\mathbb{Z} .$$

Alors la fonction suivante

$$f(P) = \exp\left(\int\limits_{O}^{P} \omega'\right),$$

est bien définie et holomorphe hors des pôles de ω', donc de ω, et que l'ordre de f en P est le résidu de ω au même point P

$$res_P\omega = ord_P f = n_P ,$$

d'où la fonction f convient, et elle a le diviseur

$$D = (f) = \sum_{P\in X} n_P \langle P\rangle .$$

3) Montrons que Ψ est surjective (théorème de Jacobi)

Le problème est local, si Ψ est surjective dans un voisinage U de $\mathbb{C}^g$, soit $\chi \in \mathbb{C}^g$, et pour n assez grand, on trouve

$$\chi' = \frac{1}{n}\chi \in U \subset \operatorname{Im}\Psi \text{, donc } \chi' = \Psi(D), D \in Div^0(X).$$

Comme Ψ est un morphisme de groupes, alors

$$\chi = n\chi' = n\Psi(D) = \Psi(nD) = \Psi(D') \text{ avec } D' \in Div^0(X),$$

cela implique que

$$\chi \in \operatorname{Im}\Psi .$$

On fixe provisoirement les points $M_1,\dots,M_g \in X$, si un point P_i est dans un voisinage V_i de M_i , on considère Ψ (D) avec D égal à

$$D = \sum_{i=1}^{g} \left(\langle P_i \rangle - \langle M_i \rangle \right).$$

Alors Ψ définit une application

$$\begin{aligned} \Psi : \prod_{i=1}^{g} V_i &\longrightarrow \mathbb{C}^g \\ (P_i)_i &\longrightarrow \Psi(D) = \left(\sum_{i=1}^{g} \int_{M_i}^{P_i} \phi_k \right)_{k=1,\dots,g} \end{aligned}.$$

Si on écrit localement

$$\phi_k = f_{ik}(z_i)\, dz_i ,$$

où z_i est une carte en M_i , alors le jacobien de cette application est égal à

$$\delta = \det\left(f_{ik}(0) \right).$$

Pour montrer que Ψ est surjective, par le théorème des fonctions implicites, il suffit d'établir que $\delta \neq 0$.

Il s'agit donc de montrer que l'application

$$\begin{aligned} \xi :\ \Omega(X) &\longrightarrow \mathbb{C}^g \\ \phi = f_i\, dz_i &\longrightarrow \left(f_1(0),\dots, f_g(0) \right) \end{aligned},$$

est un isomorphisme.

Le noyau de cette application ξ est égal à

$$\ker \xi = \left\{ \phi \in \Omega(X) ; \phi \text{ nulle en } M_1,\dots,M_g \right\},$$

on a le choix des points M_i , et on peut les choisir de telle manière que le noyau de ξ soit nul (voir [10] ou [16]), et donc ξ est injective. Et par suite, l'application ξ est surjective, car les espaces $\Omega(X)$ et $\mathbb{C}^g$ ont même dimension

$$\dim_{\mathbb{C}} \Omega(X) = \dim_{\mathbb{C}} \mathbb{C}^g = g .$$

Il en résulte que ξ est un isomorphisme, cela implique que le jacobien est non nul

$$\delta = \det\left(f_{ik}(0) \right) \neq 0 ,$$

on en déduit que l'application Ψ est injective. Finalement, on conclue que le groupe $Pic^0(X)$ est isomorphe au groupe $J = \mathbb{C}^g / \Lambda$. ■

Proposition 3.4

Pour tout point $O \in X$ fixé, Ψ définit une injection

$$P \mapsto \Psi\left(\langle P\rangle - \langle O\rangle\right),$$

de X dans sa jacobienne si $g \geq 1$.

Preuve

Supposons que pour $P_1 \neq P_2$, on a

$$\Psi\left(\langle P_1\rangle - \langle O\rangle\right) = \Psi\left(\langle P_2\rangle - \langle O\rangle\right),$$

ce qui implique que

$$\Psi\left(\langle P_1\rangle - \langle P_2\rangle\right) = 0,$$

donc il existe une fonction f sur X telle que le diviseur de f est

$$(f) = \langle P_1\rangle - \langle P_2\rangle,$$

il en résulte que f est un revêtement de degré 1 de $\mathbb{P}^1(\mathbb{C})$. Ce qui est absurde pour $g \geq 1$. ■

Proposition 3.5

L'application φ sur l'espace X^g :

$$\begin{aligned} \varphi : \quad X^g \quad &\xrightarrow{\Sigma} \quad Pic_0(X) \quad \xrightarrow{\Psi} \mathbb{C}^g / \Lambda \\ \left(P_1, \ldots, P_g\right) \mapsto \quad &\sum_{i=1}^{g}\left(\langle P_i\rangle - \langle O\rangle\right) \mapsto \sum_{i=1}^{g} \int_{O}^{P_i} \Phi \end{aligned},$$

est surjective.

Preuve

Ψ est surjective (théorème de Jacobi).

Soit $D \in Div^0(X)$, alors d'après le théorème de Riemann-Roch, on a

$$l\left(g\langle O\rangle + D\right) \geq g + 1 - g = 1,$$

donc il existe une fonction $f \in \mathcal{L}\left(g\langle O\rangle + D\right)$, ce qui signifie

$$(f) + g\langle O\rangle + D = D' \geq 0, \qquad (8)$$

par suite on aura

$$\deg D' = g\,, \tag{9}$$

car $\deg(f) = \deg D = 0$.

Les formules (8) et (9) impliquent que

$$D' = \sum_{i=1}^{g} \langle P_i \rangle = (f) + g\langle O \rangle + D\,,$$

nous extrayons le diviseur de f

$$(f) = \sum_{i=1}^{g} \langle P_i \rangle - g\langle O \rangle - D\,,$$

il en résulte que

$$D \sim \left(\sum_{i=1}^{g} \langle P_i \rangle - g\langle O \rangle \right) = \sum_{i=1}^{g} \left(\langle P_i \rangle - \langle O \rangle \right).$$

Alors modulo l'ensemble des fonctions méromorphes sur *X*, la classe de *D* dans $Pic^0(X)$ est

$$D = \sum_{i=1}^{g} \left(\langle P_i \rangle - \langle O \rangle \right), \tag{10}$$

donc on peut choisir $x = (P_1, \ldots, P_g) \in X^g$, avec les points P_i de diviseur D' tel que

$$\Sigma(x) = D\,.$$

D'où Σ est surjective.

L'application Ψ est surjective (théorème 3.3), il en résulte que la composée $\varphi = \Psi \circ \Sigma$ est surjective. ■

Soit *O* le point choisi de *X*. Tout diviseur *D* se ramène à un diviseur de degré 0.

$D = \sum_{P \in X} n_P \langle P \rangle$, implique que le diviseur $D' = D - (\deg D)\langle O \rangle = \sum_{P \in X} n_P \left(\langle P \rangle - \langle O \rangle \right)$.

Corollaire 3.6

Tout élément de la jacobienne $\mathbb{C}^g / \Lambda$ est l'image d'un diviseur effectif de degré g.de Div(X).

Preuve

La restriction de l'application φ à l'ensemble $X^{(g)}$ des diviseurs effectifs de degré g est surjective, après identification de $X^{(g)}$ à X^g, soit $a \in \mathbb{C}^g / \Lambda$, donc $a = \Psi(D)$ où

D est de degré zéro, car Ψ est surjective ; or tout diviseur D de degré zéro se ramène à un diviseur de la forme indiquée dans la formule (10), on écrit

$$a = \Psi\left(\sum_{i=1}^{g}\left(\langle P_i\rangle - \langle O\rangle\right)\right).$$

L'application Σ est surjective, cela nous donne

$$a = \left(\Psi \circ \Sigma\right)\left(\sum_{i=1}^{g}\langle P_i\rangle\right)$$

$$= \varphi\left(\sum_{i=1}^{g}\langle P_i\rangle\right),$$

d'où le diviseur $\Delta = \sum_{i=1}^{g}\langle P_i\rangle$ convient. ■

III-4/ Points de Weierstrass

Soit X une courbe hyperelliptique de genre g.

Pour un point $P \in X$ et un entier $n \geq 2$, il existe une différentielle ω ayant un pôle d'ordre n en P et holomorphe ailleurs.

La position de notre problème se situe dans la même voie, étant donnés un entier naturel n, un point P de X ; existe-elle une fonction f sur X ayant un pôle d'ordre n en P et holomorphe ailleurs ? C'est dans ce sens que se dirige notre étude sur les fonctions.

Pour $n = 1$:

Soit P un point de X, nous cherchons une fonction

$$f : X \longrightarrow \mathbb{P}^1(\mathbb{C}),$$

avec un unique pôle simple, c'est donc un revêtement de degré 1, ce qui implique que $X \simeq \mathbb{P}^1(\mathbb{C})$. Il en résulte que cette fonction n'existe pas sur une courbe hyperelliptique, car le genre de X est non nul.

Pour $n = 2$:

nous cherchons une fonction

$$f : X \longrightarrow \mathbb{P}^1(\mathbb{C}),$$

avec un unique pôle double, et donc X est une courbe hyperelliptique.

Définition 4.1

Soit un point $P \in X$, le semi-groupe associé à P est l'ensemble des ordres des pôles en P de fonctions holomorphes hors de P

$$\Gamma_P = \left\{ n \in \mathbb{N}^* \ ; \ \text{il existe } f \in \mathcal{L}\left(n\langle P\rangle\right) \setminus \mathcal{L}\left(\left(n-1\right)\langle P\rangle\right)\right\}.$$

Cet ensemble est stable par addition, si $n_1, n_2 \in \Gamma_P$ alors il existe des fonctions f_1, f_2 telles que

$$f_1 \in \mathcal{L}\left(n_1\langle P\rangle\right) \setminus \mathcal{L}\left(\left(n_1 - 1\right)\langle P\rangle\right) \ ;$$

$$\text{et } \ f_2 \in \mathcal{L}\left(n_2\langle P\rangle\right) \setminus \mathcal{L}\left(\left(n_2 - 1\right)\langle P\rangle\right).$$

Le produit de ces deux fonctions $f_1 . f_2$ est un élément de l'espace vectoriel

$$\mathcal{L}\left(\left(n_1 + n_2\right)\langle P\rangle\right) \setminus \mathcal{L}\left(\left(n_1 + n_2 - 1\right)\langle P\rangle\right),$$

l'ordre du produit de f_1 et f_2 est égal à la somme des ordres

$$ord_P\left(f_1 . f_2\right) = ord_P\left(f_1\right) + ord_P\left(f_2\right).$$

D'où $n_1 + n_2 \in \Gamma_P$.

Lemme 4.1

Pour tout entier $n \in \mathbb{N}^*$, les dimensions $l\left(n\langle P\rangle\right)$ et $l\left(\left(n-1\right)\langle P\rangle\right)$ satisfont les inégalités

$$0 \leq l\left(n\langle P\rangle\right) - l\left(\left(n-1\right)\langle P\rangle\right) \leq 1 .$$

Preuve

1) $l\left(n\langle P\rangle\right) - l\left(\left(n-1\right)\langle P\rangle\right) \geq 0$, car $\mathcal{L}\left(\left(n-1\right)\langle P\rangle\right) \subset \mathcal{L}\left(n\langle P\rangle\right)$.

2) Soit $f \in \mathcal{L}\left(n\langle P\rangle\right)$, et $f = \sum_i a_i z^i$ est le développement en série de Laurent de f, avec

$a_i \in \mathbb{C}$ et z une carte centrée en P.

On considère l'application linéaire

$$\begin{aligned} T : \mathcal{L}(n\langle P\rangle) &\longrightarrow \mathbb{C} \\ f = \sum_i a_i z^i &\longrightarrow a_{-n} \end{aligned}.$$

Le noyau de cette application est égal à

$$Ker\mathrm{T} = \left\{ f \in \mathcal{L}\left(n\langle P\rangle\right) \ ; \ a_{-n} = 0\right\} = \mathcal{L}\left((n-1)\langle P\rangle\right),$$

il en résulte que

$$l\left(n\langle P\rangle\right) - l\left((n-1)\langle P\rangle\right) \leq 1. \qquad \blacksquare$$

Proposition 4.2

Soit n *un entier non nul,* Γ_P *le semi-groupe associé à un point* $P \in X$ *,* $l\left(n\langle P\rangle\right)$ *la dimension de* $\mathcal{L}\left(n\langle P\rangle\right)$ et $l\left((n-1)\langle P\rangle\right)$ *la dimension de* $\mathcal{L}\left((n-1)\langle P\rangle\right)$*, alors les deux propositions suivantes sont équivalentes :*

1) $n \in \Gamma_P$.

2) $l\left(n\langle P\rangle\right) = l\left((n-1)\langle P\rangle\right) + 1$.

Preuve

1) Si $n \in \Gamma_P$, alors il existe une fonction f qui a un pôle d'ordre n en P et holomorphe ailleurs, donc l'inclusion suivante est stricte

$$\mathcal{L}\left((n-1)\langle P\rangle\right) \subset \mathcal{L}\left(n\langle P\rangle\right),$$

cela implique que la différence des dimensions de ces espaces est non nulle

$$l\left(n\langle P\rangle\right) - l\left((n-1)\langle P\rangle\right) \neq 0. \qquad (1)$$

La formule (1) et le lemme précédent entraînent que

$$l\left(n\langle P\rangle\right) - l\left((n-1)\langle P\rangle\right) = 1.$$

2) Si la dimension $l\left(n\langle P\rangle\right) = l\left((n-1)\langle P\rangle\right) + 1$, alors l'inclusion $\mathcal{L}\left((n-1)\langle P\rangle\right) \subset \mathcal{L}\left(n\langle P\rangle\right)$ est stricte, ce qui donne l'existence d'une fonction f dans $\mathcal{L}\left(n\langle P\rangle\right) \setminus \mathcal{L}\left((n-1)\langle P\rangle\right)$, par suite $n \in \Gamma_P$. $\blacksquare$

Définition 4.2

Les éléments de $\mathbb{N}^* \setminus \Gamma_P$ *sont les trous ou lacunes de Weierstrass au point* P.

Proposition 4.3

Soit P *un point de X ; il existe exactement g trous en* P*, soit* $n_1, \ldots, n_g$ *; ils vérifient*

$$1 = n_1 \langle\, n_2 \,\langle \ldots \langle\, n_g \le 2g - 1.$$

Preuve

On a $l(0) = l(\langle P \rangle) = 1$, alors le premier trous $n_1 = 1$.

Nous appliquons le théorème de Riemann-Roch au diviseur K d'une différentielle méromorphe sur *X*, et au diviseur $D = n\langle P \rangle$. Pour cela remarquons d'abord que *K* est de degré

$$deg(K) = 2g - 2\,,$$

et pour $n \ge 2g - 1$, alors $deg(K - n\langle P \rangle) \,\langle\, 0$, cela implique que

$$l(K - n\langle P \rangle) = 0\,.$$

Ainsi, la formule de Riemann-Roch nous donne

$$l(n\langle P \rangle) = n + 1 - g \quad ; n \ge 2g - 1, \qquad (1)$$

On conclue alors que $n \in \Gamma_P$, pour tout $n \rangle\, 2g - 1$.

Il reste à traiter les entiers $n \le 2g - 1$:

On remplace $n = 2g - 1$ dans la formule (1), on obtient

$$l((2g - 1)\langle P \rangle) = g\,.$$

Puisque la suite $l_n = l(n\langle P \rangle)$ croît de 0 ou 1 à chaque pas, on aura

$$g = \sum_{n=1}^{2g-1} (l_n - l_{n-1}) + 1,$$

cela implique que

$$\sum_{n=1}^{2g-1} (l_n - l_{n-1}) = g - 1,$$

donc il y aura nécessairement $g - 1$ entiers, tels que

$$l_n - l_{n-1} = 1 \quad ; n = 1, \ldots, 2g - 1.$$

Il reste alors $(2g - 1) - (g - 1) = g$ entiers, tels que

$$l_n - l_{n-1} = 0\,,$$

d'où g trous en *P*, qui vérifient

$$1 = n_1 \langle\, n_2 \,\langle \ldots \langle\, n_g \le 2g - 1. \qquad \blacksquare$$

III-4-1/ Points de Weierstrass

Les points de Weierstrass d'une courbe hyperelliptique *X* sont les points de ramification de cette courbe.

Définition 4.3

Un point de Weierstrass sur une courbe hyperelliptique X est un point $P \in X$ tel qu'il existe une fonction f sur X avec un unique pôle en P, d'ordre inférieur où égal au genre g de X.

Définition 4.4

P est un point de Weierstrass hyperelliptique si $2 \in \Gamma_P$.

Si $2 \in \Gamma_P$, alors il existe une fonction avec un unique pôle double, par suite *X* est une courbe hyperelliptique ; Γ_P est un semi-groupe, donc les multiples de 2 sont dans Γ_P, finalement on obtient tout les trous de Weierstrass au point *P* de la courbe hyperelliptique *X*

$$\mathbb{N}^* \setminus \Gamma_P = \{1, 3, 5, \ldots, 2g-1\}.$$

Définition 4.5

Le poids d'un point $P \in X$ est le nombre

$$\Theta(P) = \sum_{i=1}^{g} (n_i - i), \tag{1}$$

où $n_1, \ldots, n_g$ sont les trous au point P.

Le poids $\Theta(P)$ est positif ou nul, car la suite des trous est strictement croissante ; et les points de Weierstrass sont les points de poids strictement positifs, en effet, pour un point *P* de Weierstrass, les entiers $1, 2, \ldots, g$ ne sont pas tous des trous, alors la formule (1) de la définition 4.5 donne le poids d'un point de Weierstrass hyperelliptique

$$\Theta(P) = \sum_{i=1}^{g} (n_i - i) = \sum_{i=1}^{g} ((2i-1) - i) = \sum_{i=1}^{g} (i-1) = \frac{g(g-1)}{2}. \tag{2}$$

Nous étudions maintenant les points de Weierstrass sur une courbe hyperelliptique.

Proposition 4.4

Soit X une courbe hyperelliptique de genre $g \geq 2$ d'équation plane

$$h^2 = \prod_{i=1}^{2g+2} \left(f - f\left(P_i\right)\right) ,$$

avec $f\left(P_i\right) \neq \infty \,; i = 1, \ldots, 2\,g + 2$*, f est une fonction de degré* 2 *et* P_i *les points de ramification de f. Alors le diviseur de la fonction h est égal à*

$$\left(h\right) = 1\left\langle P_1\right\rangle + \cdots + 1\left\langle P_{2g+2}\right\rangle - \left(g+1\right)\left\langle Q_1\right\rangle - \left(g+1\right)\left\langle Q_2\right\rangle ,$$

avec Q_1, Q_2 *pôles de f.* (voir [7]).

Proposition 4.5

Si $f : X \longrightarrow \mathbb{P}^1(\mathbb{C})$ *est une fonction de degré* 2*, et X de genre* $g \geq 2$*, alors les points de Weierstrass sur X sont les* 2 *g* + 2 *points de ramification de f ; il sont tous hyperelliptiques.*

Preuve

Nous considérons la fonction

$$\frac{1}{f - f\left(P_i\right)} = \frac{\prod_{j=1,\, j\neq i}^{2g+2}\left(f - f\left(P_j\right)\right)}{h^2} ,$$

elle admet un unique pôle double en P_i, cela entraîne que $2 \in \Gamma_{P_i}$; et on a $1 \leq 2 \leq g$.

Il en résulte que P_i est un point de Weierstrass, et même un point de Weierstrass hyperelliptique.

D'après la formule (2), nous obtenons la somme des poids sur les points P_i

$$\sum_{i=1}^{2g+2} \Theta\left(P_i\right) = \left(2g+2\right)\frac{g\left(g-1\right)}{2} = g\left(g^2 - 1\right).$$

Le théorème suivant nous confirme que les P_i sont les seuls points de Weierstrass sur *X*.

Théorème 4.6

Les poids des points sur une courbe hyperelliptique sont liés par la relation

$$\sum_{P \in X} \Theta\left(P\right) = g\left(g^2 - 1\right).$$ (voir [16]).

■

Le résultat suivant permet de démontrer l'unicité de la fonction *f*.

Corollaire 4.7

Soit X une courbe hyperelliptiqur de genre $g \geq 2$ *, alors le morphisme*

$$f : X \longrightarrow \mathbb{P}^1(\mathbb{C}),$$

de degré 2 *est unique à Aut*($\mathbb{P}^1(\mathbb{C})$) *près.*

Preuve

Soit f' un autre morphisme

$$f' : X \longrightarrow \mathbb{P}^1(\mathbb{C}),$$

de degré 2, et P un point de Weierstrass sur *X*, donc d'après la proposition 4.5, *P* est un point de ramification pour *f* et f', alors les fonctions

$$1, \frac{1}{f - f(P)} \in \mathcal{L}\big(2\langle P\rangle\big) \text{ (resp. } 1, \frac{1}{f' - f'(P)} \in \mathcal{L}\big(2\langle P\rangle\big)). \qquad (3)$$

Comme la dimension de $\mathcal{L}\big(2\langle P\rangle\big)$ est égale à

$$l\big(2\langle P\rangle\big) \leq 2\,, \qquad (4)$$

les formules (3) et (4) impliquent que

$$\frac{1}{f' - f'(P)} = a.1 + b\,\frac{1}{f - f(P)} \quad ;\, a, b \in \mathbb{C}.$$

Nous faisons les calculs, et nous obtenons

$$f' = \frac{\alpha\, f + \beta}{\gamma\, f + \delta} = h \circ f\,,$$

où $\alpha, \beta, \gamma, \delta \in \mathbb{C}$ et $h : z \longrightarrow \dfrac{\alpha\, z + \beta}{\gamma\, z + \delta}$ est une homographie. ■

Corollaire 4.8

Sur une courbe hyperelliptique de genre $g \geq 2$ *, il existe un unique automorphisme* φ *différent de l'identité* $(\varphi \neq Id)$ *fixant au moins 5 points de la courbe.*

Preuve

Existence

L'involution hyperelliptique $J \neq Id$, fixe 2*g* + 2 points, et le nombre $2g + 2 \geq 6$.

L'unicité

Soit φ un autre automorphisme qui fixe au moins 5 points, avec $\varphi \neq Id$, et $f : X \longrightarrow \mathbb{P}^1(\mathbb{C})$

un morphisme de degré 2, alors la composée $f\circ\varphi$ est un morphisme de degré 2. D'après le corollaire 4.7, on a

$$f\circ\varphi = A\circ f\ , \tag{5}$$

où A est une homographie.

A fixe les $f(P_j)$, où P_j étant les points fixes de φ, comme on peut avoir une répétition des $f(P_j)$, donc les points fixes par A sont en nombre

$$n \geq \frac{5}{\deg(f)} \rangle\, 2\,, \tag{6}$$

d'une autre manière, si $n \leq 2$ on aura au moins trois points parmi les $f(P_j)$ qui ont même valeur c,donc # $f^{-1}(c) \geq 3$; or le morphisme f est de degré 2, alors # $f^{-1}(c) = 2$.

Donc la formule (6) implique que

$$A=Id, \tag{7}$$

les formules (5) et (7) entraînent que

$$f\circ\varphi = f\ ,$$

par suite, φ ne peut être que l'échange de feuillets associé à f.

D'où $\varphi = J$ est l'involution hyperelliptique. ■

III-4-2/ Automorphismes de courbes hyperelliptiques

Nous allons démontrer que le groupe des automorphismes sur une courbe hyperelliptique est fini.

Proposition 4.9

Tout automorphisme ϕ de X différent de l'identité a au plus $2g + 2$ points fixes.

Preuve

Soit P un point de X, tel que P n'est pas un point de Weierstrass, donc $P \in \mathbb{N}^{*}\setminus\Gamma_P$, alors il existe une fonction f

$$f \in \mathcal{L}\big((g+1)\langle P\rangle\big)\setminus\mathcal{L}\big(g\langle P\rangle\big).$$

Nous considérons la fonction

$$h = f - (f\circ\phi),$$

le diviseur des pôles de h est de la forme

$$(h)_\infty = (g+1)\langle P\rangle + (g+1)\left\langle \phi^{-1}(P)\right\rangle,$$

donc la fonction h a $2(g+1)$ zéros ; or tout point fixe de ϕ est un zéro de h, cela entraîne que ϕ fixe au plus $2(g+1)$ points de *X*. ■

Proposition 4.10

Le groupe $Aut(X)$ des automorphismes de X est fini.

Preuve

Un automorphisme de *X* conserve les ordres des pôles, donc il agit sur les points de Weierstrass, alors nous avons un morphisme de groupes

$$\varphi : Aut(X) \longrightarrow S_W ,$$

où S_W est le groupe des permutations des points de Weierstrass.

Le noyau de φ est un sous groupe de $Aut(X)$, qui fixe 2g + 2 points, donc d'après le corollaire 4.8, on a

$$Ker\,\varphi = \langle J\rangle ,$$

c'est le groupe engendré par l'involution hyperelliptique.

Par conséquent, φ induit un isomorphisme de groupes

$$Aut(X)/\langle J\rangle \simeq S_W , \qquad (1)$$

l'ordre de sous groupe $\langle J\rangle$ est fini et (1) impliquent que chaque classe de $Aut(X)/\langle J\rangle$ contient un nombre fini d'éléments, ainsi le groupe $Aut(X)$ est aussi fini. ■

III-4-3/ Le groupe W engendré par les points de Weierstrass

Les points de Weierstrass d'une courbe hyperelliptique X, vus sur la jacobienne par l'injection : $j : X \hookrightarrow \mathbb{C}^g / \Lambda \simeq Pic^0(X)$ engendre un groupe W dans $\mathbb{C}^g / \Lambda$. La proposition suivante précise le groupe W engendré par ces points.

Proposition 4.11

Soit X une courbe hyperelliptique de genre g, le groupe W engendré par les points de Weierstrass dans la jacobienne de X est $(\mathbb{Z}/2\mathbb{Z})^{2g}$.

Preuve

Supposons que l'un des points de ramification P_i de f est un pôle double de f. Une courbe hyperelliptique a une équation plane de la forme

$$h^2 = \prod_{i=1}^{2g+1} (f - z_i),$$

avec z_i des nombres complexes distincts.

Les points de Weierstrass sont les points $P_i = (z_i, 0)$ et ∞ sur le plan projectif $\mathbb{P}^1(\mathbb{C})$; sont encore les points de ramification de la courbe.

La suite de lacunes d'un point de Weierstrass P_i est $G(P_i) = \mathbb{N}^* \setminus \Gamma_{P_i} = \{1, 3, 5, \ldots, 2g-1\}$ et le poids d'un point de Weierstrass est $\Theta(P_i) = \dfrac{g(g-1)}{2}$.

La proposition 4.4 nous donne les diviseurs

$$(f - z_i) = 2\langle P_i \rangle - 2\langle \infty \rangle$$

$$\text{et} \qquad (h) = \langle P_1 \rangle + \cdots + \langle P_{2g+1} \rangle - (2g+1)\langle \infty \rangle.$$

Si l'on note x_i l'élément $\langle P_i \rangle - \langle \infty \rangle$ de la jacobienne, on obtient les relations suivantes :

1) $2x_i = 0$ pour $1 \leq i \leq 2g+1$;

2) $x_1 + \cdots + x_{2g+1} = 0$.

Cela nous permet de dire que W est l'ensemble $\left\{ \sum_{i \in I} x_i \, , \, I \subset \{1, \cdots, 2g\} \right\}$ et est un sous groupe du groupe $(\mathbb{Z}/2\mathbb{Z})^{2g}$.

Nous allons montrer que W est égal à $(\mathbb{Z}/2\mathbb{Z})^{2g}$. Donc il suffit de voir que : $\sum_{i\in I} x_i = 0$ entraîne que $I = \varnothing$ ou $I = \{1,\cdots,2g+1\}$.

Supposons qu'on a une relation entre les points de la jacobienne du type $\sum_{i\in I} x_i = 0$, avec *I* de cardinal m ; cela implique qu'il existe une fonction méromorphe y sur *X* dont le diviseur satisfait

$$(y) = \sum_{i\in I} \langle P_i \rangle - m\langle \infty \rangle \ ;$$

et y est un élément du corps des fonctions méromorphes sur *X*

$$y \in \mathcal{M}(X) = \mathbb{C}(f,h),$$

les deux fonctions f et h sont reliées par l'équation plane, on aura donc

$$y \in \mathbb{C}(f) + h\,\mathbb{C}(f),$$

et comme y n'a pas de pôle qu'en ∞, cela entraîne que y est de la forme

$$y = \mathrm{P}(f) + h\,\mathrm{Q}(f),$$

avec P et Q des polynômes. On a :

$$ord_\infty \mathrm{P}(f) = -2\deg \mathrm{P} \qquad (1)$$

$$\text{et } ord_\infty\left(h\,\mathrm{Q}(f)\right) = -2\deg \mathrm{Q} - 2g - 1. \qquad (2)$$

1) Si $\mathrm{Q} = 0,$ alors $y = \mathrm{P}(f)$ et donc $\mathrm{P} = \prod (f - z_i)$, et par suite la relation (1) nous montre que pour chaque point dans le diviseur de y intervient avec une multiplicité paire, donc ce cas est exclu.

2) Si $\mathrm{Q} \neq 0,$ et comme $m \leq 2g+1$, la relation (2) montre que Q est nécessairement constant. La fonction méromorphe y est alors de la forme $y = \mathrm{P}(f) + h,$ avec $\deg \mathrm{P} \leq g$ car $m \leq 2g+1$, delà on déduit que $m = 2g+1$ et alors $I = \{1,\cdots,2g+1\}$.

De plus, pour $i \in I$, on a $y(P_i) = \mathrm{P}(z_i) = 0$, ce qui entraîne que $\prod_{1\leq i\leq 2g+1} (f - z_i)$ divise P. Le polynôme P est nécessairement nul, et on aura $y = h$; comme $I = \{1,\cdots,2g+1\}$, on obtient alors la relation que nous avions déjà. ■

Dans le cas où les points de ramification P_i ne sont pas des pôles doubles de f, on reprend la preuve de la proposition avec l'équation plane $h^2 = \prod_{i=1}^{2g+2}(f - z_i)$ et le diviseur $(h) = \langle P_1 \rangle + \cdots + \langle P_{2g+2} \rangle - 2(g+1)\langle \infty \rangle$.

Conclusion

Dans ce mémoire, nous avons étudier deux types de courbes : les courbes elliptiques et hyperelliptiques ; qui peuvent être regarder comme des courbes algébriques sur le corps de base $\mathbb{C}$. Au cours des trois chapitres que nous avons traités, on a constaté certaines différences qui apparaissent sur ces deux courbes selon la valeur du genre g : pour $g=1$, la courbe est réalisée comme cubique non singulière de $\mathbb{P}^2(\mathbb{C})$; le cas où $g\rangle 1$, la courbe s'obtient sous la forme d'une courbe algébrique de degré $2g+2$ ou $2g+1$, et elle admet un plongement dans $\mathbb{P}^N(\mathbb{C})$; ainsi le calcul dans la jacobienne d'une courbe, munie d'une structure du groupe : pour $g=1$ et moins facile que dans le cas des courbes de genre $g\rangle 1$. Le long de ce travail, on a fait plusieurs applications du théorème de Riemann-Roch, et il intervient souvent dans les preuves des théorèmes.

BIBLIOGRAPHIE

[1] **V.Ahlford**. *Complex analysis, Second edition,* (1966).

[2] **Ahlford-Sario**. *Riemann Surfaces ; Princeton Univ. Press* (1960).

[3] **Arbarello-Cornalba-Griffiths-Harris**. *Geometry of algebraic curves, Vol* 1 *; Springer Grundlehren* 267 (1987).

[4] **H Cartan**. *Théorie élémentaire des fonctions analytiques d'une ou plusieurs variables complexes, Hermann, Paris.* (1961).

[5] **Conway**. *Functions of one complex variable ; Springer GTM* 11 (1978).

[6] **F.Cukieman and L-Y.Fong**. *On higher Weierstrass points. Duke Math. J,* 62, n°1 (1991), 179-203.

[7] **Farkas-Kra**. *Riemann Surfaces, Deuxième édition, Springer-Verlag,* (1992).

[8] **Forster**. *Lectures on Riemann surfaces ; Springer Verlag GTM* 81 (1981).

[9] **W.Fulton**. *Algebraic curves, Benjamin, New York*, (1969).

[10] **P.Griffiths, J.Harris**. *Principles of Algebraic Geometry, Wiley*, (1978).

[11] **A.Grothendieck-SGA1**. *Revêtement étales et groupe fondamental, Lecture Notes in Mathemataics, Springer,* (1970)

[12] **R.C.Gunning**. *Lectures on Riemann Surfaces, Princeton Univ. Press* (1966)

[13] **D.Laksov and A.Thorup**. *Weierstrass points and gap sequences for families of curves. Ark. Mat*, 32, n°2 (1994), 393-422.

[14] **Mumford**. *Curves and their Jacobians, Michigan university Press*, (1975).

[15] **D.Mumford**. *Tata lectures on theta. II, Birkhaïser Boston Inc., boston, MA*, (1984).

[16] **E.Reyssat**. *Quelques Aspects des Surfaces de Riemann, Birkhäuser,* (1989).

[17] **Shafarevich**. *Basic algebraic geometry, Springer Grundlehren* 213 (1974).

[18] **J.H.Silverman**. *The Arithmetic of Elliptic Curves, G.T.M* 106, *Springer-Verlag*, (1986).

[19] **J.H. Silverman**. *Some arithmetic properties of Weierstrass points : hyperelliptic curves. Bol. Soc. Brasil. Mat.* (*N.S.*), 21, n°1 (1990), 11-50.

[20] **K. Yany**. *Compact Riemann Surfaces and Algebraic Curves, World scientific*, (1988).

Quelques notations utilisées

$\mathbb{N}$: L'ensemble des entiers naturels.
$\mathbb{Z}$: L'anneau des entiers relatifs.
$\mathbb{C}$: Le corps des nombres complexes.
$Aut(X)$: Le groupe des automorphismes de X.
$Div(X)$: Le groupe des diviseurs sur X.
$\sim$: La relation d'équivalence sur X.
$Div^0(X)$: Le groupe des diviseurs de degré 0 sur X.
$Pic(X)$: Le groupe de Picard de X.
$Pic^0(X)$: Le groupe de Picard de degré 0.
$|D|$: La norme du diviseur D.
$classe(D)$: La classe du diviseur D dans $Pic^0(X)$.
C^1, C^∞ : La classe de différentielles ou de fonctions d'ordre 1 (resp. infini)
g : Le genre d'une surface de Riemann.
$e_x(f)$: L'indice de ramification de f en x.
$\mathcal{O}(U)$: L'anneau des fonctions holomorphes sur U.
$\mathcal{F}(U)$: Le corps des fractions de $\mathcal{O}(U)$.
$\mathcal{M}(X)$: Le corps des fonctions méromorphes sur X.
(f) : Le diviseur d'une fonction (ou différentielle).
$deg(D)$: Le degré du diviseur D.
$\# f^{-1}(y)$: Le cardinal d'une fibre en y.
C_n : Le groupe abélien libre sur les n-simplexes.
∂ : L'opérateur bord défini sur C_n.
$\mathcal{B}_1(X)$: L'ensemble des bords de C_1.
$\mathcal{Z}_1(X)$: L'ensemble des cycles de C_1.
$\mathcal{H}_1(X)$: Le premier groupe d'homologie de X.
J : L'involution hyperelliptique.
$J(X)$: La jacobienne d'une surface de Riemann.
$\mathcal{L}(D)$: Le $\mathbb{C}$-espace vectoriel pour un diviseur D.
$l(D)$: La dimension de $\mathcal{L}(D)$.
$\wp$: La fonction de Weierstrass.
$\mathcal{P}$: Une représentation polygonale d'une surface de Riemann.
$\overset{\circ}{\mathcal{P}}$: L'intérieur de $\mathcal{P}$.
$\mathbb{P}^N(\mathbb{C})$: L'espace projectif.
$ord_P(f)$: L'ordre d'une fonction (ou différentielle) au point P.
$res_P(f)$: Le résidu d'une fonction (ou différentielle) au point P.
$\Omega(X)$: Le $\mathbb{C}$-espace vectoriel des différentielles holomorphes sur X.
Γ_P : Le semi-groupe associé à P.
$\mathbb{N}^* \setminus \Gamma_P$: L'ensemble des trous (ou lacunes) de Weierstrass au point P.
$\Theta(P)$: Le poids d'un point P.
S_W : Le groupe des permutations des points de Weierstrass.
W : Le groupe engendré par les points de Weierstrass.