

le théorème de Riemann-Roch

Notre but est de comprendre l'essence du théorème suivant et comment il permet de relier la définition abstraite de courbe elliptique sur un corps aux courbes algébriques planes $y^2 = x^3 + ax + b$.

Théorème (Riemann-Roch)

Soit C une courbe projective lisse de genre g sur un corps algébriquement clos K . Soit $D \in \text{Div}(C)$ un diviseur. Alors on a l'égalité

$$l(D) - l(K_C - D) = \deg D - g + 1$$

En fait, comme on a vu de regarder des courbes elliptiques sur $\mathbb{Q}$, $\mathbb{F}_p$, ... dans ce cours, on va travailler sur :

K corps parfait	$\nwarrow$ tout polynôme irréductible est séparable $\Leftrightarrow$ car $\text{car } K = 0$ ou car $\text{car } K = p > 0$ et $x \mapsto x^p$ automorphisme
$\bar{K}$ une clôture algébrique	
$\text{Gal}(\bar{K}/K)$	

Soit C une courbe (projective) lisse,
c'est-à-dire une variété projective lisse
de dimension 1. On note

$$m_p \subset \mathcal{O}_p \subset \bar{K}(C)$$

le corps des fonctions rationnelles sur C ,
c'est-à-dire les classes d'équivalence
de paires (U, f) où $U \subset C$ est un ouvert
de Zariski et $f \in \mathcal{O}(U)$ (fonctions régulières)
modulo $(U, f) \sim (U', f') \iff f|_{U \cap U'} = f'|_{U \cap U'}$,

l'anneau local $\mathcal{O}_p$ formé des paires (U, f)
avec $p \in U$; et l'idéal maximal $m_p \subset \mathcal{O}_p$
des fonctions s'annulant en p . On
appelle que $\bar{K}(C) = \text{Frac}(\mathcal{O}_p)$. Être

$$\mathcal{O}_p / m_p \simeq \bar{K}$$

lisse en p signifie que la dimension
de Krull de $\mathcal{O}_p$ (longueur d'une chaîne
maximale d'idéaux premiers) est égale à

$$\dim_{\bar{K}} (m_p / m_p^2) \quad \curvearrowright \quad \begin{array}{l} \text{l'espace vectoriel} \\ \text{dual est l'espace} \\ \text{tangent en } p. \end{array}$$

DIVISEURS

Définition. Soit C une courbe lisse. Un diviseur sur C est une somme finie

$$D = \sum_{P \in C(\bar{K})} n_P \cdot [P]$$

avec $n_P \in \mathbb{Z}$ et $n_P = 0$ pour presque tout P .

On note $\text{Div}(C)$ le groupe abélien des diviseurs, c'est-à-dire le groupe abélien libre de base $C(\bar{K})$.

le degré d'un diviseur D est l'entier

$$\deg D = \sum_{P \in C(\bar{K})} n_P \in \mathbb{Z}.$$

Il sera parfois utile de considérer le sous-groupe $\text{Div}^0(C)$ des diviseurs de degré 0.

Si C est définie sur K , le groupe de Galois $\text{Gal}(\bar{K}/K)$ agit sur les diviseurs par la formule

$$\sigma(D) = \sum_{P \in C(\bar{K})} n_P \cdot [\sigma(P)]$$

et on dit que D est défini sur K large

$$\sigma(D) = D \text{ pour tout } \sigma \in \text{Gal}(\bar{K}/K).$$

(C'est le cas si les $P \in C(\bar{K})$ pour lesquels $n_P \neq 0$ sont dans $C(K)$, mais pas seulement: par exemple, sur $C = \mathbb{P}^1$ sur $K = \mathbb{Q}$, le diviseur $[\sqrt{2}] + [-\sqrt{2}]$ est défini sur $\mathbb{Q}$).

Un diviseur $D = \sum n_P [P]$ est effectif si $n_P \geq 0$ pour tout P . On écrit alors $D \geq 0$. Ceci définit une relation d'ordre partielle sur les diviseurs

$$D_1 \geq D_2 \iff D_1 - D_2 \geq 0 \text{ (i.e. effectif)}$$

le diviseur d'une fonction

Soit C une courbe lisse sur K et $P \in C(K)$ un point. On définit une valuation sur l'anneau local de C en P

$\nearrow$

$$\text{ord}_P : \mathcal{O}_P \longrightarrow \{0, 1, 2, \dots\} \cup \{\infty\}$$
$$f \longmapsto \max \{d \mid f \in \mathfrak{m}_P^d\}$$

$\text{ord}_P(fg) = \text{ord}_P(f) + \text{ord}_P(g)$
 $\text{ord}_P(f+g) \geq \min(\text{ord}_P(f), \text{ord}_P(g))$

et on l'étend à son corps de fractions

$\bar{K}(C) = \text{Frac}(\mathcal{O}_P)$ en utilisant la formule

$$\text{ord}_P\left(\frac{f}{g}\right) = \text{ord}_P(f) - \text{ord}_P(g)$$

on obtient alors :

$$\text{ord}_P : \bar{K}(C) \longrightarrow \mathbb{Z} \cup \{\infty\}$$

- Si $\text{ord}_P(f) \geq 0$, alors f est régulière en P et on peut évaluer $f(P) \in \bar{K}$.
- Si $\text{ord}_P(f) > 0$, f a un zéro en P .
- Si $\text{ord}_P(f) < 0$, f a un pôle en P et on écrit $f(P) = \infty$.

Si $f \in \bar{K}(C)^\times$, alors il n'y a qu'un nombre fini de points $P \in C(\bar{K})$ tels que $\text{ord}_P(f) \neq 0$. (Intuition: pour les zéros, $\{f=0\}$ est un fermé de zéro-dimension de C , donc de dimension 0; pour les pôles, on regarde $1/f$).

Définition: Soit $f \in \bar{K}(C)^\times$. le diviseur de f est donné par

$$\text{div}(f) = \sum_{P \in C(\bar{K})} \text{ord}_P(f) \cdot [P]$$

Proposition : $\deg(\operatorname{div}(f)) = 0$

Rappelons que $\operatorname{Gal}(\bar{k}/k)$ agit sur les fonctions régulières par $\sigma(\mathcal{O}(U)) \subset \mathcal{O}(\sigma^{-1}(U))$.

On a

$$\operatorname{div}(\sigma(f)) = \sigma(\operatorname{div}(f))$$

et donc si $f \in k(C)$ est définie sur k , alors son diviseur $\operatorname{div}(f)$ est défini sur k .

Les notations $\operatorname{div}(f)$ et la relation $\geq$ sur les diviseurs permettent d'exprimer de manière très concise des propriétés sur les pôles et les zéros d'une fonction,

e.g. $\operatorname{div}(f) \geq -n[P]$ signifie que f est régulière en dehors de P et en P a au plus un pôle d'ordre $\leq n$.

Définition: Soit D un diviseur sur C .
on définit le $\bar{k}$ -espace vectoriel

$$\mathcal{L}(D) = \{f \in \bar{k}(C)^{\times} \mid \operatorname{div}(f) \geq -D\} \cup \{0\}$$

lemme: Soit C une courbe projective lisse.

Alors $\mathcal{L}(D)$ est de dimension finie.

Preuve: Si $D_1 \leq D_2$, alors $\text{div}(f) \geq -D_1$ implique $\text{div}(f) \geq -D_2$, donc $\mathcal{L}(D_1) \subset \mathcal{L}(D_2)$.

On peut donc supposer $D \geq 0$. On a alors

$$\dim \mathcal{L}(D) \leq \deg D + 1$$

comme on le voit par récurrence sur le degré de D . En effet,

1) Si $D=0$, $\mathcal{L}(D)$ est réduit aux fonctions constantes $\bar{k}$

2) Si $D \neq 0$, il existe $P \in C(\bar{k})$ tel que $D - [P] \geq 0$. Si $\mathcal{L}(D) = \mathcal{L}(D - [P])$, c'est bon par récurrence. Sinon, soit t une infinitésimale en P , c'est-à-dire un générateur de m_P . Alors

$$\mathcal{L}(D) \longrightarrow \bar{k}$$

$$f \longmapsto (t^{n_P} f)(P)$$

est surjective (car il existe $f \in \mathcal{L}(D) \setminus \mathcal{L}(D - [P])$)

de noyau $\mathcal{L}(D-[P])$, d'où

$$\mathcal{L}(D) = \mathcal{L}(D-[P]) \oplus \bar{k}f,$$

ce qui finit la preuve par récurrence □

Définition: $\mathcal{L}(D) = \dim_{\bar{k}} \mathcal{L}(D)$

Remarque: si $\deg D < 0$, alors $\mathcal{L}(D) = 0$.

Pour tout $g \in \bar{k}(C)^\times$, il y a une bijection

$$\mathcal{L}(D + \operatorname{div}(g)) \xrightarrow{\sim} \mathcal{L}(D)$$

$$f \longmapsto fg$$

car $\operatorname{div}(fg) \geq -D - \operatorname{div}(g)$

$$\Leftrightarrow \operatorname{div}(fg) = \operatorname{div}(f) + \operatorname{div}(g) \geq -D$$

L'espace $\mathcal{L}(D)$ ne dépend donc que de l'image de D dans le groupe de Picard

$$\operatorname{Pic}(C) = \operatorname{coker}(\bar{k}(C)^\times \rightarrow \operatorname{Div}(C)).$$

Lemme: si $\cdot$ est définie sur k , alors

$\mathcal{L}(D)$ admet une base de fonctions dans $k(C)$,
i.e. définies sur k .

(5)

Comme $\sigma(f) \in \mathcal{L}(\sigma(D)) = \mathcal{L}(D)$ si D est défini sur K , le groupe de Galois $\text{Gal}(\bar{K}/K)$ agit sur $\mathcal{L}(D)$. Le lemme résulte alors de:

Lemme: Soit V un $\bar{K}$ -espace vectoriel muni d'une action continue semi-linéaire de $\text{Gal}(\bar{K}/K)$, i.e.

* pour tout $v \in V$,

$$\{\sigma \in \text{Gal}(\bar{K}/K) \mid \sigma(v) = v\}$$

est un sous-groupe d'indice fini de $\text{Gal}(\bar{K}/K)$

* $\sigma(\lambda v) = \sigma(\lambda) \sigma(v)$ pour tous $\lambda \in \bar{K}$
 $v \in V$

Soit $V^{\text{Gal}(\bar{K}/K)} = \{v \in V \mid \sigma(v) = v \text{ pour tout } \sigma\}$

$$\text{Alors } \begin{array}{ccc} V^{\text{Gal}(\bar{K}/K)} & \otimes_K \bar{K} & \xrightarrow{\sim} V \\ \otimes & \longmapsto & \lambda v \end{array}$$

est un isomorphisme de $\bar{K}$ -vecteurs.

Preuve: il suffit de noter que tout élément de V est une $\bar{K}$ -combinaison linéaire d'éléments de $V^{\text{Gal}(\bar{K}/K)}$.

Soit $v \in V$. Comme $\{\sigma \in \text{Gal}(\bar{K}/K) \mid \sigma(v) = v\} = H$

est d'indice fini, son corps fixe $\bar{K}$ est une extension finie de K . Soit L la clôture galoisienne de $\bar{K}^H$. Remarque

$\alpha_1, \dots, \alpha_n$ base de L sur K

$$\{\sigma_1, \dots, \sigma_n\} = \text{Gal}(L/K)$$

les éléments $w_i = \sum_{j=1}^n \sigma_j(\alpha_i) \sigma_j(v) = \sigma_j(\alpha_i) \sigma_j(v)$ satisfont

$$\sigma(w_i) = \sum_{j=1}^n (\sigma \sigma_j)(\alpha_i) \sigma_j(v) = \sum_{j=1}^n \sigma_j(\alpha_i) \sigma_j(v)$$

pour tout $\sigma \in \text{Gal}(\bar{K}/K)$, et donc $w_i \in V^{\text{Gal}(\bar{K}/K)}$.

Comme la matrice $(\sigma_j(\alpha_i))_{i,j=1,\dots,n}$ est

invertible, tout $\sigma_j(v)$ (en particulier v)

est combinaison linéaire d'éléments de $V^{\text{Gal}(\bar{K}/K)}$.

□

Fonctions différentielles

Soit $A \rightarrow B$ un morphisme d'anneaux.

Définition. on définit $\Omega_{B/A}$, le module des différentiels de Kähler, comme le quotient du B -module libre engendré par

les symboles db pour tout $b \in B$ par le $\mathcal{O}_B$ -module engendré par les éléments

$$a) \quad d(b+b') = db + db'$$

$$b) \quad d(bb') = b db' + b' db \quad (\text{leibniz})$$

$$c) \quad da \quad \text{pour tout } a \in A$$

(les éléments de A sont des "constants")

Il est muni d'une application A -linéaire

$$d: B \longrightarrow \Omega_{B/A}$$

$$b \longmapsto db$$

qui est universelle au sens suivant:

soit $D: B \rightarrow M$ une A -dérivation, alors

$$B \xrightarrow{d} \Omega_{B/A}$$

satisfait a),
b), c)

$$D \searrow M$$

↑ morphisme de B -modules

On verra au fur et à mesure les propriétés de $\Omega_{B/A}$. Pour d'instaurer un contexte:

Proposition: Soit P un point d'une courbe lisse et soit k une unifié en P . Alors $\Omega_{\mathcal{O}_P/k}$ est un $\mathcal{O}_P$ -module

libre de rang 1, engendré par dt .

Définition: Soit C une courbe lisse.
On appelle espace de formes différentielles

invariants sur C $\Omega_{B/A} \otimes_{B/A} \bar{S}^1 B = \bar{S}^1 \Omega_{B/A} = \Omega_{\bar{S}^1 B/A}$
pour toute partie multiplicative S de B (e.g.)

$$\Omega_C = \Omega_{\bar{K}(C)/K}$$

la proposition ci-dessus plus la compatibilité avec la localisation impliquent que Ω_C est un $\bar{K}(C)$ -espace vectoriel de dim 1.

Le diviseur d'une forme différentielle

Soient $w \in \Omega_C$ et $P \in C(\bar{K})$. Choisissons une uniformisante t en P . Il existe $g \in \bar{K}(C)$ telle que

$$w = g dt \quad (\text{parfois notée } g = \frac{w}{dt})$$

L'entier $\boxed{\text{ord}_P(w) \stackrel{\text{def}}{=} \text{ord}(g)}$ ne dépend pas du choix de l'uniformisante. En effet, si t' est une autre uniformisante

Les points $P_i = [e_i : 0 : 1]$ pour $i=1, 2, 3$ et $\infty = [0 : 1 : 0]$, le seul point dans le compacité de la courbe affine

$$y^2 = (x - e_1)(x - e_2)(x - e_3)$$

$$x = \frac{X}{Z} \quad y = \frac{Y}{Z}$$

Calculons les degrés des facteurs x et y .
Pour cela on utilise l'égalité

$$\text{ord}_{P_i}(y) = \dim_K (\mathcal{O}_{P_i} / (y))$$

$$\text{Comme } K[X, Y]^{(P_i)} / (y, y^2 = (x - e_1)(x - e_2)(x - e_3))$$

est isomorphe à K , on trouve

$$\text{ord}_{P_i}(y) = 1$$

À l'infini, la fonction y a un pôle d'ordre l'ordre d'annulation de $1/y = \frac{z}{y}$.

On a donc $|K_C = -2[\infty]|$

Soit $w \in \mathcal{L}_C$ non nulle. Alors $w = f dt$ avec $f \in \bar{K}(\mathbb{P}^1)$ et

$$\operatorname{div}(f dt) = \underbrace{\operatorname{div}(f)}_{\text{degré } 0} - 2[\infty]$$

Conclusion: Il n'y a pas de différentielles holomorphes sur $C = \mathbb{P}^1$, c'est-à-dire c'est une courbe de genre $g(C) = 0$.

Exemple: Soit K un corps de caractéristique différente de 2 et $e_1, e_2, e_3 \in \bar{K}$ distincts. Soit $C \subset \mathbb{P}^2$ la courbe

$$Y^2 Z = (X - e_1 Z)(X - e_2 Z)(X - e_3 Z)$$

c'est une courbe lisse qui passe par

⑨

qui est de dimension 3, d'où

$$\text{ord}_0(y) = -3$$

On en déduit que le diviseur de y est égal à

$$\text{div}(y) = [P_1] + [P_2] + [P_3] - 3[\infty]$$

(on arrive par lecture par multiplication de ∞ de l'information $\deg(\text{div}(y)) = 0$)

De même, on peut montrer que

$$\text{div}(x - e_i) = 2[P_i] - 2[\infty]$$

En effet, l'ordre d'annulation en P_i est la dimension de

$$K[x, y]_{P_i} / (x - e_i, y^2 - (x - e_1)(x - e_2)(x - e_3))$$

qui est de dimension 2, et l'ordre d'annulation en ∞ est de dimension 3.

uniformité, d'où

$$\text{ind}_P(dx) = d((x - x_0)) = 0$$

En P_i , on a m p.e. $\text{ind}_{P_i}(x - x_i) = 2$,

ce qui implique $\text{ind}_{P_i}(dx) = 1$. Finalement,

comme $\text{ind}_\infty(x) = -2$ on a

$$\text{ind}_\infty(dx) = \text{ind}_\infty(-x^2 d(\frac{1}{x}))$$

$$= \text{ind}_\infty(-2x^3 d(\frac{1}{x})) = 3$$

Si $1/t$ est une uniformisante en ∞ .

Conclusion:

$$\text{div}(dx) = [P_1] + [P_2] + [P_3] - 3[\infty]$$

$$= \text{div}(y)$$

C'est-à-dire $\frac{dx}{y}$ est une différentielle

10

holomorphe et sans zéros et le diviseur canonique K_C est trivial dans $\text{Pic}(C)$. Par conséquent, la courbe C a genre 1.

On a enfin tous les ingrédients pour retrouver la réponse du Théorème de Riemann-Roch:

$$\ell(D) - \ell(K_C - D) = \deg D + 1 - g$$

Quelques cas séparent intéressants:

* En faisant $D = K_C$,

$$\ell(K_C) - \ell(0) = \deg K_C + 1 - g$$

$$\Rightarrow \deg K_C = 2g - 2$$

comme on l'avait déjà vérifié dans le

cas de $C = \mathbb{P}^1$ et d'une courbe $C \subset \mathbb{P}^2$

$$C = \mathbb{P}^1 \quad \text{ou} \quad C = (x - e_1)(x - e_2)(x - e_3).$$

$$f \mapsto f \circ \varphi$$

qui fait de $K(C)$ un K -module
de $\varphi^* K(C')$. on définit:

$$\deg \varphi = \begin{cases} 0 & \text{si } \varphi \text{ est étale} \\ [K(C) : \varphi^* K(C')] & \text{si } \varphi \text{ n'est pas étale} \end{cases}$$

Si $\deg \varphi = 1$, alors φ est un isomorphisme.

Pour chaque $P \in C$ l'indice de ramification

de $\varphi: C \rightarrow C'$ en P est l'entier

$$e_{\varphi}(P) = \text{ord}_P(\varphi^* t_{\varphi(P)})$$

où $t_{\varphi(P)}$ est une uniformisante au point $\varphi(P)$. On a $e_{\varphi}(P) \geq 1$ et on dit que φ est ramifié en P si $e_{\varphi}(P) > 1$.

①

on a les relations: pour tout $Q \in C'$,

$$\deg \varphi = \sum_{P \in \varphi^{-1}(Q)} e_P(\varphi)$$

À $\varphi: C \rightarrow C'$ on associe les morphismes suivants entre groupes de diviseurs

$$\begin{aligned} \varphi_*: \text{Div}(C) &\longrightarrow \text{Div}(C') \\ [P] &\longmapsto [\varphi(P)] \end{aligned}$$

$$\begin{aligned} \varphi^*: \text{Div}(C') &\longrightarrow \text{Div}(C) \\ [Q] &\longmapsto \sum_{P \in \varphi^{-1}(Q)} e_P(\varphi) \cdot [P] \end{aligned}$$

Importance: Soit $\varphi: C \rightarrow C'$ un morphisme non constant entre courbes lisses. Alors:

$$(a) \deg(\varphi^* D) = (\deg \varphi) \deg D$$

$$\operatorname{div}(f) = \operatorname{div}(\varphi^* t) = \varphi^* \left(\underbrace{[\bar{0}] - [\bar{\infty}]}_{\deg=0} \right)$$

d'où le degré de $\operatorname{div}(f)$ est

$$\deg(\varphi^*([\bar{0}] - [\bar{\infty}])) = (\deg \varphi) \deg([\bar{0}] - [\bar{\infty}]) = 0$$

Une mesure $\varphi: C \rightarrow C^1$ induit aussi une mesure sur les modules des formes différentielles, donc simplement sur

$$\begin{aligned} \varphi^*: \Omega_{C^1} &\longrightarrow \Omega_C \\ \sum t_i dx_i &\longmapsto \sum (\varphi^* t_i) d(\varphi^* x_i). \end{aligned}$$