Géométrie arithmétique, théorie de Galois-Grothendieck et chtoucas de Drinfeld inversibles

Notes de cours

par Laurent Lafforgue

Sommaire

I. Rappels sur les schémas

1 Anneaux

Définition I.1. –

(i) *Un anneau (commutatif) est un ensemble A muni de*
- *une loi d'addition $a, b \mapsto a + b$,*
- *un élément neutre de l'addition $0_A = 0$,*
- *un passage à l'opposé $a \mapsto -a$,*
- *une loi de multiplication $a, b \mapsto ab$,*
- *un élément neutre de la multiplication $1_A = 1$,*

vérifiant les propriétés habituelles (associativité, commutativité, distributivité) de l'addition et de la multiplication des entiers.

(ii) *Un morphisme d'un anneau A dans un anneau B est une application*

$$u : A \to B$$

compatible avec les structures de A et B, soit
- $\left.\begin{array}{rcl} u(a+b) & = & u(a)+u(b) \\ u(ab) & = & u(a)\,u(b) \end{array}\right\} \quad \forall\, a, b \in A\,,$
- $u(0_A) = 0_B\,, \quad u(1_A) = 1_B\,,$
- $u(-a) = -u(a)\,, \quad \forall\, a \in A\,.$

Exemples :

(i) L'unique anneau dans lequel $1 = 0$ est $\{0\}$.

(ii) $\mathbb{Z}$ est un anneau.

(iii) Tout anneau A possède un unique morphisme d'anneaux

$$\mathbb{Z} \to A\,.$$

□

Les principaux procédés de construction de nouveaux anneaux à partir d'un anneau A sont :
- la localisation A_f de A le long d'un élément $f \in A$ ou, ce qui revient au même, de $\{f^n \mid n \geq 1\}$, ou plus généralement la localisation A_S le long d'une partie S de A ou, ce qui revient au même, de

$$\overline{S} = \{f_1 \dots f_n \mid f_1, \dots, f_n \in S\}\,,$$

- le quotient A/I de A par un idéal I,

- la formation des anneaux de polynômes à coefficients dans A

$$A[X] \quad \text{ou} \quad A[X_1, \dots, X_d]$$

en une variable X ou en plusieurs variables $X_1, \dots, X_d$.

On rappelle ce que cela signifie :

Définition I.2. –

(i) *Si $\overline{S}$ désigne l'ensemble des produits d'éléments de S (y compris l'élément 1), $A_S = A_{\overline{S}}$ désigne le quotient de l'ensemble des couples (a, f), $a \in A$, $f \in \overline{S}$, par la relation d'équivalence*

$$(a, f) \sim (a', f') \Leftrightarrow \exists\, f'' \in \overline{S}\,, \quad af'f'' = a'ff''\,.$$

En notant $\frac{a}{f}$ la classe de tout couple (a, f), A_S est muni de l'addition et de la multiplication définies par

$$\frac{a}{f} + \frac{a'}{f'} = \frac{af' + fa'}{ff'}\,, \quad \frac{a}{f} \cdot \frac{a'}{f'} = \frac{aa'}{ff'}\,.$$

(ii) *Un idéal I de A est une partie non triviale telle que*

$$a, b \in I \Rightarrow a + b \in I\,,$$

$$a \in A \wedge b \in I \Rightarrow ab \in I\,.$$

La notation A/I désigne le quotient de A par la relation d'équivalence

$$a \sim b \Leftrightarrow a - b \in I\,.$$

En notant $\overline{a}$ la classe de tout $a \in A$, A/I est muni de l'addition et de la multiplication définies par

$$\overline{a} + \overline{b} = \overline{a + b}\,, \quad \overline{a} \cdot \overline{b} = \overline{a \cdot b}\,.$$

(iii) *Un polynôme $P \in A[X]$ [resp. $A[X_1, \dots, X_d]$] est une somme formelle*

$$P = \sum_{n \in \mathbb{N}} a_n\, X^n \qquad [\textit{resp.} \quad P = \sum_{n_1, \dots, n_d \in \mathbb{N}} a_{n_1, \dots, n_d}\, X_1^{n_1} \dots X_d^{n_d}]$$

dont les coefficients a_n [resp. $a_{n_1, \dots, n_d}$] sont dans A et "presque tous" nuls (c'est-à-dire tous nuls sauf un nombre fini).

Les constructions A_S, A/I, $A[X]$ ou $A[X_1, \dots, X_d]$ sont caractérisées par les "propriétés universelles" suivantes :

Lemme I.3. –

(i) *L'application $a \mapsto \frac{a}{1}$ définit un morphisme d'anneaux*

$$A \to A_S$$

qui envoie tout élément $f \in S$ sur un élément inversible $\frac{f}{1}$ d'inverse $\frac{1}{f}$.
De plus, un morphisme

$$A \xrightarrow{u} B$$

se factorise, de manière nécessairement unique, en

$$A \to A_S \to B$$

si et seulement si

$$u(f) \in B^\times\,, \quad \forall\, f \in S$$

(où $B^\times$ désigne le groupe multiplicatif des éléments inversibles de B).

(ii) *Pour tout morphisme d'anneaux*

$$A \xrightarrow{u} B\,,$$

son image $\mathrm{Im}\,(u)$ *est un sous-anneau de* B *et son noyau*

$$\mathrm{Ker}\,(u) = \{a \in A \mid u(a) = 0\}$$

est un idéal de A.

Le morphisme $u : A \to B$ *se factorise, de manière nécessairement unique, en*

$$A \twoheadrightarrow A/I \twoheadrightarrow \mathrm{Im}\,(u) \hookrightarrow B$$

si et seulement si l'idéal I *est contenu dans* $\mathrm{Ker}\,(u)$. *Dans ce cas, le morphisme surjectif*

$$A/I \twoheadrightarrow \mathrm{Im}\,(u)$$

est un isomorphisme si et seulement si

$$I = \mathrm{Ker}\,(u)\,.$$

(iii) *Pour tout morphisme d'anneaux*

$$u : A \to B$$

et tout élément $x \in B$ *[resp. tous éléments* $x_1, \ldots, x_d \in B$*], il existe un unique morphisme*

$$A[X] \to B \qquad [\textit{resp.} \quad A[X_1, \ldots, X_d] \to B]$$

qui prolonge u *et envoie* X *sur* x *[resp.* $X_1, \ldots, X_d$ *sur* $x_1, \ldots, x_d$*].*

Voici des cas particulièrement importants de localisation :

Définition I.4. –

(i) *Un anneau* A *est dit "intègre" si la partie* $A - \{0\}$ *est non vide et stable par multiplication.*
La localisation de A *le long de* $A - \{0\}$ *est alors un corps, appelé le corps des fractions de* A *et noté* $\mathrm{Frac}\,(A)$.
Le morphisme $A \to \mathrm{Frac}\,(A)$ *est injectif.*
Pour toute partie S *de* $A - \{0\}$*, le localisé* A_S *existe et s'identifie à un sous-anneau de* $\mathrm{Frac}\,(A)$ *qui contient* A.

(ii) *Un idéal* p *d'un anneau* A *est dit "premier" si la partie* $A - p$ *est non vide et stable par multiplication ou, ce qui revient au même, si le quotient* A/p *est intègre.*
La localisation de A *le long de* $A - p$ *est appelée l'anneau local de* A *en* p *et sera notée* A_p.

Exemples :

Les anneaux $\mathbb{Z}$ ou $K[X]$ (pour tout corps K) sont intègres. Leurs corps des fractions sont $\mathbb{Q}$ et $K(X)$.

Leurs idéaux sont engendrés par un seul élément $n \in \mathbb{N}$ ou $P \in K[X]$.

En dehors de l'idéal 0, leurs idéaux premiers sont ceux engendrés par les nombres premiers $n = p$ [resp. par les polynômes P irréductibles].

$\square$

On peut compléter cette définition par :

Lemme I.5. –

(i) *Tout idéal maximal d'un anneau A (c'est-à-dire qui n'est contenu dans aucun idéal non trivial) est premier.*

(ii) *Un idéal $\mathfrak{p}$ de A est maximal si et seulement si le quotient $A/\mathfrak{p}$ et un corps.*

(iii) *Pour tout idéal premier $\mathfrak{p}$ d'un anneau A, l'idéal engendré par $\mathfrak{p}$ dans $A_{\mathfrak{p}}$ contient tous les idéaux de $A_{\mathfrak{p}}$. En particulier, il est maximal et le corps quotient $\kappa_{\mathfrak{p}} = A_{\mathfrak{p}}/(\mathfrak{p})$, qui est appelé le corps résiduel de A en $\mathfrak{p}$, s'identifie au corps des fractions de l'anneau intègre $A/\mathfrak{p}$.*

Exemples :

Dans l'anneau $\mathbb{Z}$ [resp. $K[X]$], les idéaux maximaux sont ceux engendrés par les nombres premiers p [resp. par les polynômes irréductibles P]. Il en résulte que les quotients $\mathbb{Z}/p\,\mathbb{Z} = \mathbb{F}_p$ [resp. $K[X]/(P)$] sont des corps.

On remarque que chaque corps $\mathbb{F}_p$ est fini à p éléments et que chaque corps $K[X]/(P)$ est de dimension finie (égale au degré du polynôme P) en tant qu'espace vectoriel sur K.

$\square$

La notion d'espace vectoriel sur un corps se généralise en celle de module sur un anneau :

Définition I.6. –

(i) *Un module sur un anneau A est un groupe abélien $(M, +)$ muni d'une loi de multiplication par les éléments de A (que l'on peut appeler les scalaires)*

$$A \times M \to M\,, \qquad (a, m) \mapsto a \cdot m$$

telle que

- $\left.\begin{array}{rcl} a \cdot (a' \cdot m) & = & (a\,a') \cdot m \\ (a + a') \cdot m & = & a \cdot m + a' \cdot m \end{array}\right\} \quad \forall\, a, a' \in A\,, \quad \forall\, m \in M\,,$
- $a \cdot (m + m') = a \cdot m + a \cdot m'\,, \quad \forall\, a \in A\,, \quad \forall\, m, m' \in M$
- $1 \cdot m = m\,, \quad 0 \cdot m = 0\,, \quad \forall\, m \in M$
- $a \cdot 0 = 0\,, \quad \forall\, a \in A.$

(ii) *Un morphisme de A-modules*

$$M \xrightarrow{u} M'$$

est un morphisme de groupes abéliens tel que, de plus,

$$u(a \cdot m) = a \cdot u(m)\,, \quad \forall\, a \in A\,, \quad \forall\, m \in M\,.$$

Remarques :

(i) Tout groupe abélien est un module sur $\mathbb{Z}$.

(ii) Tout anneau A est un module sur lui-même.
Ses sous-modules ne sont autres que ses idéaux.

(iii) Tout morphisme d'anneaux $A \to B$ permet de voir les B-modules comme des A-modules. En particulier, il permet de voir B et ses idéaux comme des A-modules.

$\square$

Les principaux procédés de construction de modules sur un anneau A sont :

- la formation du A-module libre $A^{(I)}$ sur un ensemble I, défini comme l'ensemble des suites $(a_i)_{i\in I}$ d'éléments $a_i \in A$ "presque tous" nuls, c'est-à-dire nuls en dehors d'un ensemble fini d'indices,
- pour tout morphisme $M \xrightarrow{u} M'$ de A-modules, la formation de son noyau

$$\mathrm{Ker}\,(u) = \{m \in M \mid u(m) = 0\}\,,$$

de son image

$$\mathrm{Im}\,(u) = \{m' \in M' \mid \exists\, m \in M\,, \quad u(m) = m'\}\,,$$

et de son conoyau $\mathrm{Coker}\,(u)$ défini comme le quotient de M' par la relation d'équivalence

$$m_1' \sim m_2' \Leftrightarrow \exists\, m \in M\,, \quad m_1' - m_2' = u(m)\,,$$

- la formation du sous-module engendré par une famille d'éléments $(m_i)_{i\in I}$ d'un A-module M,
- la formation du produit tensoriel

$$M \otimes_A M'$$

de deux A-modules M et M', défini comme le quotient du A-module libre

$$A^{(M\times M')} = \left\{\sum a_{m,m'} \cdot m \otimes m'\right\}$$

par le sous-module engendré par les relations

$$(a \cdot m) \otimes m' = a \cdot m \otimes m' = m \otimes (a \cdot m')\,,$$

$$(m_1 + m_2) \otimes m' = m_1 \otimes m' + m_2 \otimes m'\,,$$
$$m \otimes (m_1' + m_2') = m \otimes m_1' + m \otimes m_2'\,.$$

Ces constructions sont caractérisées par les "propriétés universelles" suivantes :

Lemme I.7. –

(i) *Pour tout A-module M, se donner un morphisme*

$$A^{(I)} \to M$$

équivaut à se donner une famille $(m_i)_{i\in I}$ d'éléments de M. L'image du morphisme est alors le sous-module $\sum A \cdot m_i$ de M engendré par les m_i.

(ii) *Étant donné un morphisme $M \xrightarrow{u} M'$ et pour tout module N, un morphisme*

$$N \to M \qquad [\textit{resp.} \quad M' \to N\,, \quad \textit{resp.} \quad N \to M']$$

se factorise à travers $\mathrm{Ker}\,(u)$ *[resp.* $\mathrm{Coker}\,(u)$*, resp.* $\mathrm{Im}\,(u)$*] si et seulement si son composé*

$$\begin{array}{rccccc} & N & \longrightarrow & M & \xrightarrow{u} & M'\,, \\ [\textit{resp.} & M & \xrightarrow{u} & M' & \longrightarrow & N\,, \\ \textit{resp.} & N & \longrightarrow & M' & \longrightarrow & \mathrm{Coker}\,(u)\ ] \end{array}$$

est 0.

(iii) *Pour tout A-module, se donner un morphisme*

$$M \otimes_A M' \to N$$

équivaut à se donner une application A-bilinéaire

$$M \times M' \to N\,.$$

□

On déduit de la propriété universelle des produits tensoriels les deux corollaires suivants :

Corollaire I.8. –

Pour tout morphisme d'anneaux $A \to B$, on a :

(i) *Le foncteur*

$$M \mapsto B \otimes_A M$$

transforme les A-modules (et leurs morphismes) en B modules (et morphismes de B-modules).

(ii) *Pour tout A-module M et tout B-module N, se donner un morphisme de A-modules*

$$M \to N$$

équivaut à se donner un morphisme de B-modules

$$B \otimes_A M \to N\,.$$

□

Corollaire I.9. –

Pour tous morphismes d'anneaux

$$A \to B_1 \quad \textit{et} \quad A \to B_2\,,$$

le produit tensoriel

$$B_1 \otimes_A B_2$$

a une structure d'anneau.

De plus, pour tout anneau C, se donner un morphisme d'anneaux

$$B_1 \otimes_A B_2 \to C$$

équivaut à se donner deux morphismes

$$B_1 \to C \quad \textit{et} \quad B_2 \to C$$

rendant commutatif le carré :

$$\begin{tikzcd} A \arrow[r] \arrow[d] & B_1 \arrow[d] \\ B_2 \arrow[r] & C \end{tikzcd}$$

□

2 Schémas affines

A tout anneau A, on peut associer un espace topologique appelé son “spectre” :

Définition I.10. –

Le spectre Spec (A) *d'un anneau A est l'ensemble de ses idéaux* premiers.

Il est muni de la topologie “de Zariski” définie par la base d'ouverts constituée des

$$\mathrm{Spec}\,(A_f) = \{p \in \mathrm{Spec}\,(A) \mid f \notin p\}$$

associés aux éléments $f \in A$.

Remarques :

(i) Les ouverts de Spec (A) sont donc les réunions de parties de la forme Spec (A_f), $f \in A$.
Leur famille est stable par intersection finie car, pour tous éléments $f_1, \ldots, f_n \in A$, on a

$$\mathrm{Spec}\,(A_{f_1}) \cap \ldots \cap \mathrm{Spec}\,(A_{f_n}) = \mathrm{Spec}\,(A_{f_1 \cdots f_n})\,.$$

(ii) Pour tout idéal I de A, Spec (A/I) s'identifie à un fermé de Spec (A) qui est $\{p \in \mathrm{Spec}\,(A) \mid I \subseteq p\}$.
Réciproquement, tous les fermés de Spec (A) sont de cette forme.
En particulier, si p est un idéal premier, Spec (A/p) s'identifie à l'adhérence du point $p \in \mathrm{Spec}\,(A)$.
Les fermés de cette forme sont appelés “irréductibles”.

□

On peut définir la notion de dimension d'un anneau A. Elle ne dépend que de la topologie de Spec (A) :

Définition I.11. –

(i) *On dit qu'un anneau A est de dimension d si la longueur maximale de ses suites d'idéaux premiers emboîtés $p_1 \subsetneq \ldots \subsetneq p_k$ ou, ce qui revient au même, de fermés irréductibles emboîtés de* Spec (A)*, est égale à $d + 1$.*

(ii) *On appelle dimension de A en un point fermé $x \in \mathrm{Spec}\,(A)$, correspondant à un idéal maximal p de A, la dimension de l'anneau local A_p.*

Remarque :

Un anneau est de dimension d si d est le maximum de ses dimensions en ses points fermés. □

Cette définition de la dimension est justifiée par la proposition suivante :

Proposition I.12. –

Pour tout anneau A de dimension d, $A[X]$ est de dimension $d + 1$ et $A[X_1, \ldots, X_k]$ est de dimension $d + k$.

En particulier, pour tout corps K, $K[X]$ est de dimension 1 *et $K[X_1, \ldots, X_d]$ est de dimension d.*

Remarque :

L'anneau $\mathbb{Z}$ a la même dimension 1 que les $K[X]$. □

On a encore :

Lemme I.13. –

Pour tout morphisme d'anneaux $A \xrightarrow{u} B$, l'application

$$(p \subset B) \mapsto u^{-1}(p) = \operatorname{Ker}(A \to B \to B/p)$$

définit une application continue

$$\operatorname{Spec}(B) \to \operatorname{Spec}(A)\,.$$

Remarque :

En revanche, si p est un idéal maximal de B, $u^{-1}(p)$ n'est pas nécessairement un idéal maximal de A.

Démonstration :

Si $p \subset B$ est un idéal, le morphisme induit

$$A/u^{-1}(p) \to B/p$$

est injectif, si bien que $u^{-1}(p)$ est premier si p est premier.

De plus, pour tout $f \in A$, l'image réciproque de l'ouvert $\operatorname{Spec}(A_f)$ par $\operatorname{Spec}(B) \to \operatorname{Spec}(A)$ est l'ouvert $\operatorname{Spec}(B_{u(f)})$.

□

L'espace topologique $\operatorname{Spec}(A)$ exprime seulement une part de l'information contenue en A. Afin d'en tirer entièrement partie, on munit $\operatorname{Spec}(A)$ d'un faisceau d'anneaux induit par A. On rappelle d'abord :

Définition I.14. –

Soit X un espace topologique.

(i) *Un préfaisceau $\mathcal{F}$ [resp. un préfaisceau d'anneaux $\mathcal{O}$, resp. un préfaisceau de $\mathcal{O}$-modules $\mathcal{M}$] sur X consiste en une famille d'ensembles*

$$\mathcal{F}(U)$$

[resp. d'anneaux $\mathcal{O}(U)$, resp. de $\mathcal{O}(U)$-modules $\mathcal{M}(U)$] indexés par les ouverts U de X, et d'applications

$$\mathcal{F}(V) \to \mathcal{F}(U)$$

[resp. de morphismes $\mathcal{O}(V) \to \mathcal{O}(U)$, $\mathcal{M}(V) \to \mathcal{M}(U)$] associées à chaque inclusion d'un ouvert dans un autre

$$U \subset V\,,$$

et compatibles avec les inclusions composées

$$U \subset V \subset W\,.$$

(ii) *Un tel préfaisceau est appelé un faisceau si, pour toute famille d'ouverts $(U_i)_{i\in I}$ de réunion U, on a*

- *tout élément de $\mathcal{F}(U)$ [resp. $\mathcal{O}(U)$, resp. $\mathcal{M}(U)$], appelé une section de $\mathcal{F}$ sur U, est uniquement déterminé par ses images dans les $\mathcal{F}(U_i)$, appelées ses restrictions aux U_i,*
- *toute famille de sections dans les $\mathcal{F}(U_i)$, $i \in I$, qui ont les mêmes restrictions dans les $\mathcal{F}(U_i \cap U_j)$, $i, j \in I$, provient d'une unique section dans $\mathcal{F}(U)$.*

(iii) *Un morphisme de préfaisceaux (ou de faisceaux)*

$$\mathcal{F} \to \mathcal{F}' \qquad [\textit{resp. } \mathcal{O} \to \mathcal{O}' , \quad \textit{resp. } \mathcal{M} \to \mathcal{M}']$$

est une famille d'applications [resp. de morphismes]

$$\mathcal{F}(U) \to \mathcal{F}'(U) \qquad [\textit{resp. } \mathcal{O}(U) \to \mathcal{O}'(U) , \quad \textit{resp. } \mathcal{M}(U) \to \mathcal{M}'(U)]$$

qui commutent avec les applications [resp. les morphismes] de restriction :

$$\begin{array}{ccc} \mathcal{F}(V) & \longrightarrow & \mathcal{F}'(V) \\ \downarrow & & \downarrow \\ \mathcal{F}(U) & \longrightarrow & \mathcal{F}'(U) \end{array}$$

Remarques :

(i) Pour toute application continue entre espaces topologiques

$$X \xrightarrow{f} Y$$

et tout préfaisceau $\mathcal{F}$ sur X, la collection des $\mathcal{F}(f^{-1}(V))$ (associés aux ouverts V de Y) définit un préfaisceau sur Y, noté $f_*(\mathcal{F})$, qui est un faisceau si $\mathcal{F}$ est un faisceau.
Si $\mathcal{O}$ est un faisceau d'anneaux [resp. $\mathcal{M}$ un faisceau de $\mathcal{O}$-modules] sur X, $f_*(\mathcal{O})$ est un faisceau d'anneaux [resp. $f_*(\mathcal{M})$ est un faisceau de $f_*(\mathcal{O})$-modules] sur Y.

(ii) Un espace topologique X muni d'un faisceau d'anneaux $\mathcal{O}_X$ est appelé un espace annelé.
Un morphisme d'espaces annelés

$$(X, \mathcal{O}_X) \xrightarrow{f} (Y, \mathcal{O}_Y)$$

consiste en une application continue $f : X \to Y$ complétée par un morphisme de faisceaux d'anneaux sur Y

$$\mathcal{O}_Y \to f_*(\mathcal{O}_X) ,$$

c'est-à-dire, si l'on préfère, une collection de morphismes compatibles

$$\mathcal{O}_Y(U) \to \mathcal{O}_X(V)$$

pour tous ouverts $U \subset Y$, $V \subset X$ tels que $f(V) \subset U$.

(iii) Un faisceau $\mathcal{M}$ de $\mathcal{O}_X$-modules sur un espace annelé $(X, \mathcal{O}_X)$ peut aussi être appelé un $\mathcal{O}_X$-$\mathcal{M}$odule.
Son image $f_*(\mathcal{M})$ par un morphisme $(X, \mathcal{O}_X) \to (Y, \mathcal{O}_Y)$ d'espaces annelés est un $f_*(\mathcal{O}_X)$-$\mathcal{M}$odule et a fortiori un $\mathcal{O}_Y$-$\mathcal{M}$odule.

□

Ayant rappelé la définition des faisceaux, on a :

Lemme I.15. –

Soient A un anneau et $X = \mathrm{Spec}\,(A)$ son spectre.

(i) *Il existe un unique faisceau d'anneaux $\mathcal{O}_X$ sur X, appelé son faisceau de structure, tel que pour tout $f \in A$,*

$$\mathcal{O}_X(\mathrm{Spec}\,(A_f)) = A_f .$$

(ii) *Pour tout A-module M, il existe un unique $\mathcal{O}_X$-$\mathcal{M}$odule $\widetilde{M}$ sur $X = \mathrm{Spec}\,(A)$ tel que*

$$\widetilde{M}(\mathrm{Spec}\, A_f) = A_f \otimes_A M\,, \qquad \forall f \in A\,.$$

On peut donc poser :

Définition I.16. –

(i) *Un schéma affine $(X, \mathcal{O}_X)$ est un espace annelé isomorphe au spectre* $\mathrm{Spec}\,(A)$ *d'un anneau A, muni de son faisceau de structure.*

(ii) *Sur un schéma affine* $\mathrm{Spec}\,(A) = (X, \mathcal{O}_X)$*, un $\mathcal{O}_X$-$\mathcal{M}$odule est dit quasi-cohérent s'il est isomorphe à un $\mathcal{O}_X$-$\mathcal{M}$odule $\widetilde{M}$ associé à un A-module M.*

(iii) *On appelle morphismes d'un schéma affine dans un autre*

$$\mathrm{Spec}\,(A) \to \mathrm{Spec}\,(B)$$

leurs morphismes d'espaces annelés qui sont induits par les morphismes d'anneaux dans l'autre sens

$$B \to A\,.$$

$\square$

Si $X = \mathrm{Spec}\,(A) \xrightarrow{f} \mathrm{Spec}\,(B) = Y$ est un morphisme de schémas affines, le produit tensoriel

$$M \mapsto A \otimes_B M$$

définit un foncteur

$$\mathcal{M} = \widetilde{M} \mapsto \widetilde{A \otimes_B M} = f^*(\mathcal{M})$$

qui transforme les $\mathcal{O}_Y$-$\mathcal{M}$odules quasi-cohérents en $\mathcal{O}_X$-$\mathcal{M}$odules quasi-cohérents.

Les corollaires I.8 et I.9 se retraduisent en :

Corollaire I.17. –

(i) *Pour tout morphisme de schémas affines*

$$X = \mathrm{Spec}\,(A) \xrightarrow{f} \mathrm{Spec}\,(B) = Y\,,$$

tout $\mathcal{O}_X$-$\mathcal{M}$odules quasi-cohérent $\mathcal{M}$ et tout $\mathcal{O}_Y$-$\mathcal{M}$odule quasi-cohérent $\mathcal{N}$, se donner un morphisme de $\mathcal{O}_Y$-$\mathcal{M}$odules

$$\mathcal{N} \to f_*(\mathcal{M})$$

équivaut à se donner un morphisme de $\mathcal{O}_X$-$\mathcal{M}$odules

$$f^*(\mathcal{N}) \to \mathcal{M}\,.$$

(ii) *Pour tous schémas affines* $X_1 = \mathrm{Spec}\,(A_1)$, $X_2 = \mathrm{Spec}\,(A_2)$, $Y = \mathrm{Spec}\,(B)$ *reliés par deux morphismes $X_1, X_2 \to Y$, se donner deux morphismes d'un schéma affine Z dans X_1 et X_2 rendant commutatif le diagramme*

$$\begin{tikzcd} Z \arrow[r] \arrow[d] & X_1 \arrow[d] \\ X_2 \arrow[r] & Y \end{tikzcd}$$

équivaut à se donner un morphisme

$$Z \to X_1 \times_Y X_2 = \mathrm{Spec}\,(A_1 \otimes_B A_2)\,.$$

$\square$

3 Schémas

Nous pouvons maintenant donner la définition de la catégorie des schémas :

Définition I.18. –

(i) *Un schéma est un espace annelé* $(X, \mathcal{O}_X)$ *qui admet un recouvrement par des ouverts* $(U, \mathcal{O}_U = \mathcal{O}_{X|U})$ *qui sont des schémas affines.*

(ii) *Un morphisme de schémas est un morphisme d'espaces annelés*

$$f : (X, \mathcal{O}_X) \to (Y, \mathcal{O}_Y) \qquad \textit{(consistant en } X \xrightarrow{f} Y \textit{ et } \mathcal{O}_Y \to f_*(\mathcal{O}_X)\textit{)}$$

tel que, pour tout $x \in X$*, il existe un voisinage ouvert affine* U *de* x *et un voisinage ouvert affine* V *de* $f(x)$ *tels que le composé*

$$(U, \mathcal{O}_U) \to (X, \mathcal{O}_X) \to (Y, \mathcal{O}_Y)$$

se factorise en un morphisme de schémas affines

$$(U, \mathcal{O}_U) \to (V, \mathcal{O}_V)\,.$$

□

Se donner un faisceau $\mathcal{F}$ sur un espace topologique X écrit comme une réunion d'ouverts U_i équivaut à se donner un faisceau $\mathcal{F}_i$ sur chaque U_i et des isomorphismes

$$\mathcal{F}_{i|U_i \cap U_j} \cong \mathcal{F}_{j|U_i \cap U_j}$$

compatibles sur les intersections triples $U_i \cap U_j \cap U_k$.

Par conséquent, pour construire un schéma, il suffit de se donner des schémas affines $(U_i, \mathcal{O}_{U_i})$, $i \in I$, des ouverts affines $(U_{i,j}, \mathcal{O}_{U_{i,j}})$ des $(U_i, \mathcal{O}_{U_i})$, $i, j \in I$, et des isomorphismes de schémas affines

$$(U_{i,j}, \mathcal{O}_{U_{i,j}}) \xrightarrow{\sim} (U_{j,i}, \mathcal{O}_{U_{j,i}})\,, \qquad i, j \in I\,,$$

compatibles entre eux.

En particulier, on peut introduire :

Définition I.19. –

Soit A *un anneau.*

(i) *On appelle droite projective sur* A *le schéma* $\mathbb{P}^1_A$ *obtenu par recollement de deux droites affines*

$$\operatorname{Spec}(A[X]) \qquad \textit{et} \qquad \operatorname{Spec}(A[Y])$$

le long de leurs ouverts affines

$$\operatorname{Spec}(A[X, X^{-1}]) \qquad \textit{et} \qquad \operatorname{Spec}(A[Y, Y^{-1}])$$

identifiés par le changement de variable $Y = X^{-1}$.

(ii) *Plus généralement, on appelle espace projectif de dimension* d *sur* A *le schéma* $\mathbb{P}^d_A$ *obtenu par recollement des* $d+1$ *espaces affines*

$$\operatorname{Spec}\left(A\left[\frac{X_0}{X_i}, \frac{X_1}{X_i}, \ldots, \frac{X_d}{X_i}\right]\right), \qquad 0 \le i \le d\,,$$

le long de leurs ouverts affines

$$\mathrm{Spec}\left(A\left[\frac{X_0}{X_i}\,,\ \frac{X_1}{X_i}\,,\ \ldots\,,\ \frac{X_d}{X_i}\,,\ \frac{X_i}{X_j}\right]\right)\,, \qquad 0 \leq i,j \leq d\,,$$

identifiés par les changements de variables

$$\frac{X_k}{X_i} = \frac{X_k}{X_j}\cdot\frac{X_j}{X_i}\,, \qquad 0 \leq k \leq d\,, \quad 0 \leq i,j \leq d\,.$$

Un fermé d'un schéma X est dit irréductible s'il est l'adhérence d'un point de X.

Un schéma X est dit de dimension d si la plus grande longueur de chaînes de fermés irréductibles emboîtés de X

$$Z_1 \subsetneq \ldots \subsetneq Z_k$$

est égale à $d+1$. C'est le maximum des dimensions des ouverts de n'importe quel recouvrement de X par les ouverts affines.

On pose encore :

Définition I.20. –

Un faisceau quasi-cohérent $\mathcal{M}$ sur un schéma $(X, \mathcal{O}_X)$ est un faisceau de $\mathcal{O}_X$-$\mathcal{M}$odules dont la restriction à tout ouvert affine est quasi-cohérente au sens de la définition I.16(ii).

Remarque :

Si $(X, \mathcal{O}_X)$ est écrit comme la réunion d'ouverts affines $(U_i, \mathcal{O}_{U_i})$, se donner un faisceau quasi-cohérent sur X équivaut à se donner un faisceau quasi-cohérent $\mathcal{M}_i$ sur chaque U_i et des isomorphismes

$$\mathcal{M}_{i|U_i\cap U_j} \xrightarrow{\sim} \mathcal{M}_{j|U_i\cap U_j}$$

compatibles entre eux sur les intersections $U_i \cap U_j \cap U_k$. □

Pour tout point x d'un schéma X, l'anneau limite inductive filtrante

$$\mathcal{O}_x = \mathcal{O}_{x,X} = \varinjlim_{x\in U} \mathcal{O}_X(U)$$

est appelé l'anneau local de X en x. Si $U = \mathrm{Spec}\,(A)$ est n'importe quel ouvert affine qui contient x et p désigne l'idéal premier de A qui correspond à x, $\mathcal{O}_X$ s'identifie à l'anneau localisé A_p. Il possède pour plus grand ideal m_x l'idéal $p \cdot A_p$ engendré par p. Le quotient $\mathcal{O}_x/m_x = \kappa_x$ est appelé le corps résiduel de X en x.

Si $\mathcal{M}$ est un faisceau quasi-cohérent sur X, la limite inductive filtrante

$$\mathcal{M}_x = \varinjlim_{x\in U} \mathcal{M}(U)$$

est un $\mathcal{O}_x$-module appelé la fibre de $\mathcal{M}$ en x. Si la restriction de $\mathcal{M}$ à $U = \mathrm{Spec}\,(A)$ comme ci-dessus est de la forme $\widetilde{M}$ pour un A-module M, $\mathcal{M}_x$ s'identifie à $A_p \otimes_A M$. Le quotient $\mathcal{M}_x/m_x \cdot \mathcal{M}_x$ est un espace vectoriel sur κ_x qui peut être appelé la fibre résiduelle de $\mathcal{M}$ en x.

Pour construire un morphisme de schémas

$$(X, \mathcal{O}_X) \to (Y, \mathcal{O}_Y)\,,$$

il suffit d'un double recouvrement $(U_i)_{i\in I}$ et $(V_i)_{i\in I}$ de X et Y par des ouverts affines et d'une famille de morphismes de schémas affines

$$U_i \to V_i$$

telle que les composés $U_i \to V_i \to Y$ coïncident sur les intersections $U_i \cap U_j$. On en déduit en particulier :

Lemme I.21. –

Se donner un morphisme

$$(X, \mathcal{O}_X) \to \mathrm{Spec}\,(A)$$

d'un schéma arbitraire X dans un schéma affine $\mathrm{Spec}\,(A)$ *équivaut à se donner un morphisme d'anneaux*

$$A \to \mathcal{O}_X(X)\,.$$

Remarque :

On voit en particulier que tout schéma X est muni d'un unique morphisme

$$X \to \mathrm{Spec}\,(\mathbb{Z})\,,$$

autrement dit peut être vu comme un schéma sur $\mathrm{Spec}\,(\mathbb{Z})$.

S'il existe un nombre premier p tel que le morphisme

$$\mathbb{Z} \to \mathcal{O}_X(X)$$

se factorise à travers $\mathbb{Z}/p\,\mathbb{Z} = \mathbb{F}_p$, on dit que X est un schéma sur $\mathbb{F}_p$, ou encore un schéma de caractéristique p.

On déduit de ce lemme et du corollaire I.17(ii) la très importante construction suivante :

Proposition I.22. –

Pour tous schémas X_1, X_2 sur un même schéma Y (c'est-à-dire munis chacun d'un morphisme vers Y), il existe un schéma $X_1 \times_Y X_2$, nécessairement unique à unique isomorphisme près, tel que se donner un morphisme

$$Z \to X_1 \times_Y X_2$$

équivale à se donner une paire de morphismes $Z \to X_1$ et $Z \to X_2$ rendant commutatif le diagramme :

$$\begin{tikzcd}
Z \arrow[r] \arrow[d] & X_1 \arrow[d] \\
X_2 \arrow[r] & Y
\end{tikzcd}$$

Démonstration :

Si $Y = \mathrm{Spec}\,(A)$, $X_1 = \mathrm{Spec}\,(B_1)$ et $X_2 = \mathrm{Spec}\,(B_2)$ sont tous trois affines, il suffit d'après le lemme I.21 ci-dessus et le corollaire I.9 (ou le corollaire I.17(ii)) de prendre $X_1 \times_Y X_2 = \mathrm{Spec}\,(B_1 \otimes_A B_2)$.

Sinon, choisissons pour Y, X_1 et X_2 un triple recouvrement par des ouverts affines U_i, V_i et W_i, $i \in I$, tels que $X_1 \to Y$ envoie chaque V_i dans U_i et $X_2 \to Y$ envoie chaque W_i dans U_i.

Alors les $V_i \times_{U_i} W_i$ sont déjà construits et sont des schémas affines. Pour tous indices i, j,

$$(V_i \cap V_j) \times_{U_i} (W_i \cap W_j) = (V_i \cap V_j) \times_{U_j} (W_i \cap W_j)$$

est bien défini comme un ouvert à la fois de $V_i \times_{U_i} W_i$ et de $V_j \times_{U_j} W_j$. Les isomorphismes de recollement ainsi définis sont compatibles et définissent un schéma $X_1 \times_Y X_2$ qui répond à la question posée.

□

Si $X \to Y$ est un schéma au-dessus d'un schéma de base Y et $Y' \to Y$ est un morphisme de schémas, le produit fibré $X \times_Y Y'$ est appelé le schéma sur Y' déduit de X par le changement de base $Y' \to Y$.

En particulier, si y est un point de Y de corps résiduel κ_y, $X \times_Y \operatorname{Spec}(\kappa_y) = X_y$ est appelé la fibre de X au-dessus de Y. Lorsque y est un point générique de Y, c'est-à-dire $Y = \overline{\{y\}}$, X_y est appelée la fibre générique de X. Par exemple, pour tout schéma X vu comme un schéma sur $\mathbb{Z}$, on dispose de sa fibre générique $X_{\mathbb{Q}} = X \times_{\operatorname{Spec}(\mathbb{Z})} \operatorname{Spec}(\mathbb{Q})$ et de ses fibres résiduelles $X_p = X \times_{\operatorname{Spec}(\mathbb{Z})} \operatorname{Spec}(\mathbb{F}_p)$ en tous les nombres premiers p.

Enfin, si $X \to \operatorname{Spec}(K)$ est un schéma sur un corps K, et $\overline{K}$ est une clôture algébrique de K, on dispose du schéma “géométrique” associé $X \times_{\operatorname{Spec}(K)} \operatorname{Spec}(\overline{K}) = \overline{X}$.

Il existe aussi un changement de base pour les faisceaux quasi-cohérents :

Lemme I.23. –

Soit $X \xrightarrow{f} Y$ un morphisme de schémas. Alors :

(i) *Pour tout $\mathcal{O}_X$-$\mathcal{M}$odule quasi-cohérent $\mathcal{M}$ sur X, le $\mathcal{O}_Y$-$\mathcal{M}$odule $f_*(\mathcal{M})$ sur Y est quasi-cohérent.*

(ii) *Pour tout $\mathcal{O}_Y$-$\mathcal{M}$odule quasi-cohérent $\mathcal{N}$ sur Y, il existe un $\mathcal{O}_X$-$\mathcal{M}$odule quasi-cohérent $f^*(\mathcal{N})$ sur X, unique à unique isomorphisme près, tel que se donner un morphisme de $\mathcal{O}_X$-$\mathcal{M}$odules*

$$f^*(\mathcal{N}) \to \mathcal{M}$$

équivale à se donner un morphisme de $\mathcal{O}_Y$-$\mathcal{M}$odules

$$\mathcal{N} \to f_*(\mathcal{M}) .$$

Démonstration :

(i) La propriété est locale sur Y donc on peut supposer que Y est affine. Si X est écrit comme la réunion d'ouverts affines U_i, $\mathcal{M}(X)$ s'identifie au module des familles d'éléments des $\mathcal{M}(U_i)$, $i \in I$, qui ont mêmes images dans les $\mathcal{M}(U_i \cap U_j)$, $i, j \in I$. On se ramène ainsi au cas où X aussi est affine, qui est évident.

(ii) La propriété “universelle” qui caractérise $f^*(\mathcal{N})$ indique que, s'il existe, il est nécessairement unique à unique isomorphisme près. Or, d'après le corollaire I.17(i), $f^*(\mathcal{N})$ existe si Y et X sont affines et sa formation commute aux localisations. Cela permet de construire $f^*(\mathcal{N})$ par recollement dans le cas où X et Y sont des schémas arbitraires.

□

On voit en particulier que si X est un schéma sur une base Y et $Y' \to Y$ un morphisme de changement de base, tout $\mathcal{M}$odule quasi-cohérent $\mathcal{M}$ sur X induit un $\mathcal{M}$odule quasi-cohérent sur $X \times_Y Y'$. Ainsi, pour tout point $y \in Y$, $\mathcal{M}$ induit un $\mathcal{M}$odule quasi-cohérent $\mathcal{M}_y$ sur $X_y = X \times_{\operatorname{Spec}(Y)} \kappa_y$.

Parmi les propriétés possibles des morphismes de schémas, on distingue en premier :

Définition I.24. –

Un morphisme de schémas $X \xrightarrow{f} Y$ est dit

(1) *une immersion ouverte s'il identifie X à un ouvert de Y muni du faisceau de structure induit,*

(2) *une immersion fermée si, pour tout ouvert affine* $U = \mathrm{Spec}\,(A)$ *de* Y, $f^{-1}(U)$ *s'identifie à* $\mathrm{Spec}\,(A/I)$ *pour un certain idéal* I *de* A,

(3) *une immersion localement fermée s'il est le composé d'une immersion fermée et d'une immersion ouverte,*

(4) *affine si, pour tout ouvert affine* $U = \mathrm{Spec}\,(A)$ *de* Y, $f^{-1}(U)$ *s'identifie au spectre* $\mathrm{Spec}\,(B)$ *d'une* A*-algèbre* B *(c'est-à-dire d'un anneau* B *muni d'un morphisme* $A \to B$*),*

(5) *de type fini si, pour tout ouvert affine* $U = \mathrm{Spec}\,(A)$ *de* Y, $f^{-1}(U)$ *est réunion finie d'ouverts affines* $V_i = \mathrm{Spec}\,(B_i)$ *associés à des* A*-algèbres* B_i *de type fini (c'est-à-dire engendrées sur* A *par un nombre fini d'éléments),*

(6) *séparé si le morphisme diagonal*

$$X \to X \times_Y X$$

est une immersion fermée,

(7) *propre s'il est de type fini, séparé et universellement fermé au sens que pour tout morphisme de changement de base* $Y' \to Y$, *le morphisme*

$$X \times_Y Y' \to Y'$$

transforme tout fermé de $X \times_Y Y'$ *en un fermé de* Y'.

Remarque :

Lorsque l'on parle de schéma affine, de type fini, séparé ou propre, c'est toujours par rapport à un schéma de base implicite. La base par défaut est le schéma $\mathrm{Spec}\,(\mathbb{Z})$.

□

On a :

Lemme I.25. –

(i) *Chacune des propriétés* (1) *à* (7) *ci-dessus des morphismes de schémas* $X \to Y$ *est respectée par composition ainsi que par tout changement de base* $Y' \to Y$.

(ii) *Tout morphisme affine est séparé, donc aussi toute immersion localement fermée.*

(iii) *Tout morphisme diagonal* $X \to X \times_Y X$ *est localement fermé.*

(iv) *Si un composé* $X \to Y \to Z$ *est séparé, il en est de même de* $X \to Y$.

(v) *Si un composé* $X \to Y \to Z$ *est de type fini [resp. propre] et que* $Y \to Z$ *est séparé, alors* $X \to Y$ *est de type fini [resp. propre].*

Démonstration :

(i) est évident.

(ii) résulte de ce que, pour toute A-algèbre B, le morphisme $B \otimes_A B \to B$ est surjectif.

(iii) résulte de (ii).

(iv) et (v) se montrent en utilisant

- la factorisation de $X \to Y$ en $X \to X \times_Z Y \to Y$,
- le fait que $X \to X \times_Z Y$ se déduit de $Y \to Y \times_Z Y$ par le changement de base $X \to Y$,
- le fait que $X \times_Z Y \to Y$ se déduit de $X \to Z$ par le changement de base $Y \to Z$. □

On a le résultat important :

Proposition I.26. –

Pour tout anneau A, les espaces projectifs $\mathbb{P}_A^n = \mathbb{P}_{\mathbb{Z}}^n \times_{\mathrm{Spec}(\mathbb{Z})} \mathrm{Spec}\,(A)$ sont propres sur $\mathrm{Spec}\,(A)$, donc aussi tous leurs sous-schémas fermés appelés "schémas projectifs" sur A.

□

Parmi les propriétés globales des schémas, on distingue :

Définition I.27. –

(i) *Un anneau A est dit nœthérien s'il vérifie les propriétés équivalentes suivantes :*
- *toute suite croissante d'idéaux de A est stationnaire,*
- *tout idéal de A est engendré par un nombre fini d'éléments,*
- *pour tout A-module M qui est de type fini (c'est-à-dire engendré par un nombre fini d'éléments), les sous-modules de M sont de type fini.*

(ii) *Un schéma X est dit nœthérien si*
- *il est localement nœthérien au sens qu'il est réunion d'ouverts affines $U = \mathrm{Spec}\,(A)$ associés à des anneaux nœthériens,*
- *il est quasi-compact au sens que tout recouvrement de X par des ouverts contient un sous-recouvrement fini.*

Premiers exemples :

$\mathbb{Z}$ ou $K[X]$ (pour n'importe quel corps K) sont des anneaux nœthériens puisque tout idéal y est engendré par un élément. □

On a :

Lemme I.28. –

Si A est un anneau nœthérien, il en est de même des anneaux de polynômes $A\,[X_1, \ldots, X_d]$, $d \geq 1$, des quotients A/I de A et de ses localisations A_S.

Remarque :

Si K est un corps, tout idéal de $K\,[X_1, \ldots, X_d]$ est donc engendré par un nombre fini d'éléments mais pas nécessairement par un seul si $d \geq 2$. □

On déduit de ce lemme :

Corollaire I.29. –

Si Y est un schéma nœthérien, ses anneaux locaux $\mathcal{O}_y$ en les points $y \in Y$ sont nœthériens, et tout schéma X de type fini sur Y est nœthérien.

On peut maintenant poser :

Définition I.30. –

Un $\mathcal{O}_X$-$\mathcal{M}$odule quasi-cohérent $\mathcal{M}$ sur un schéma nœthérien X est dit cohérent si, pour tout ouvert affine $U = \mathrm{Spec}\,(A)$ de X, le A-module $\mathcal{M}(U)$ est de type fini. □

Si $f : X \to Y$ est un morphisme entre deux schémas nœthériens, et que $\mathcal{N}$ est un $\mathcal{O}_Y$-$\mathcal{M}$odule cohérent sur Y, alors $f^*(\mathcal{N})$ est un $\mathcal{O}_X$-$\mathcal{M}$odule cohérent sur X.

En sens inverse, on a le très important théorème suivant :

Théorème I.31. –

Soient un schéma nœthérien Y, un morphisme propre $X \to Y$ *et un $\mathcal{O}_X$-$\mathcal{M}$odule cohérent $\mathcal{M}$ sur X. Alors le $\mathcal{O}_Y$-$\mathcal{M}$odule quasi-cohérent $f_*(\mathcal{M})$ sur Y est cohérent.* □

On peut maintenant introduire une nouvelle classe de morphismes de schémas :

Définition I.32. –

(i) *Une algèbre B sur un anneau nœthérien A est dite finie si elle est de type fini en tant que A-module.*

(ii) *Un schéma X sur un schéma nœthérien Y est dit fini sur Y si, pour tout ouvert affine $U = \mathrm{Spec}\,(A)$ de Y, son image réciproque dans X est un ouvert affine $V = \mathrm{Spec}\,(B)$ associé à une A-algèbre B qui est finie.*

Remarques :

(i) Les morphismes finis $X \xrightarrow{f} Y$ sont donc les morphismes affines tels que le faisceau de $\mathcal{O}_Y$-algèbres $f_*(\mathcal{O}_X)$ soit cohérent en tant que $\mathcal{O}_Y$-$\mathcal{M}$odule sur Y.

(ii) Les morphismes finis $X \to Y$ sont respectés par composition ainsi que par changement de base nœthérienne $Y' \to Y$.

□

On déduit du théorème I.31 :

Corollaire I.33. –

Un morphisme affine

$$f : X \to Y$$

vers un schéma nœthérien Y est fini si et seulement si il est propre.

Démonstration :

Si f est propre, $f_*(\mathcal{O}_X)$ est un $\mathcal{O}_Y$-$\mathcal{M}$odule cohérent sur Y d'après le théorème I.31.

L'implication en sens inverse est plus élémentaire.

Il suffit de prouver que si B est une algèbre sur un anneau A qui est de type fini comme A-module, alors l'application $\mathrm{Spec}\,(B) \to \mathrm{Spec}\,(A)$ transforme tout fermé en un fermé.

Puis il suffit de prouver que si $A \to B$ est injectif, l'application $\mathrm{Spec}\,(B) \to \mathrm{Spec}\,(A)$ est surjective.

En remplaçant A par son localisé en n'importe quel idéal premier, on peut supposer encore que A est local, et il suffit de montrer que son idéal maximal m est dans l'image de $\mathrm{Spec}\,(B)$.

Pour cela, il suffit de prouver que le quotient $B/m \cdot B$ est non trivial, car alors tout idéal maximal m' de B qui contient l'idéal $m \cdot B$ a pour image m. Cela résulte du lemme suivant :

Lemme I.34 ("Lemme de Nakayama"). –

Si A est un anneau local d'idéal maximal m et M un A-module de type fini, toute famille d'éléments de M qui engendre l'espace vectoriel de dimension finie $M/m \cdot M$ engendre le A-module M.

Démonstration :

Soit $x_1, \ldots, x_k$ une famille d'éléments de M qui l'engendre comme A-module et soit $y_1, \ldots, y_d$ une famille d'éléments de M qui engendre l'espace vectoriel $M/m \cdot M$.

Pour $1 \leq i \leq k$, on peut écrire

$$x_i = (a_{i,1} \cdot y_1 + \ldots + a_{i,d} \cdot y_d) + (m_{i,1} \cdot x_1 + \ldots + m_{i,k} \cdot x_k)$$

avec $a_{i,j} \in A$, $1 \leq j \leq d$ et $m_{i,j} \in m$, $1 \leq j \leq k$.

La différence de la matrice $(m_{i,j})_{1 \leq i,j \leq k}$ et de la matrice I est inversible dans A/m donc aussi dans A, ce qui signifie que $x_1, \ldots, x_k$ appartiennent au sous-module de M engendré par $y_1, \ldots, y_d$.

$\square$

II. Revêtements finis étales

1 Morphismes plats

Étant donné un anneau A, on appelle suite (finie) de A-modules tout diagramme

$$M_0 \xrightarrow{u_1} M_1 \xrightarrow{u_2} \dots \longrightarrow M_{k-1} \xrightarrow{u_k} M_k$$

de morphismes de A-modules dont les composés successifs $u_{i+1} \circ u_i$ valent tous 0, soit

$$\mathrm{Im}\,(u_i) \subset \mathrm{Ker}\,(u_{i+1})\,, \qquad \forall\, i\,.$$

Une telle suite est dite exacte si

$$\mathrm{Im}\,(u_i) = \mathrm{Ker}\,(u_{i+1})\,, \qquad \forall\, i\,.$$

On montre que pour toute suite exacte de A-modules

$$0 \longrightarrow M_1 \longrightarrow M_2 \longrightarrow M_3 \longrightarrow 0$$

et pour tout A-module N, la suite

$$M_1 \otimes_A N \longrightarrow M_2 \otimes_A N \longrightarrow M_3 \otimes_A N \longrightarrow 0$$

est exacte, sans que

$$M_1 \otimes_A N \longrightarrow M_2 \otimes_A N$$

soit nécessairement injectif.

Cela conduit à poser la définition :

Définition II.1. –

(i) *Un A-module M est dit plat [resp. fidèlement plat] si l'exactitude d'une suite de A-modules*

$$0 \longrightarrow N_1 \longrightarrow N_2 \longrightarrow N_3 \longrightarrow 0$$

entraîne [resp. est équivalente à] l'exactitude de la suite

$$0 \longrightarrow N_1 \otimes_A M \longrightarrow N_2 \otimes_A M \longrightarrow N_3 \otimes_A M \longrightarrow 0\,.$$

(ii) *Une A-algèbre B est dite plate [resp. fidèlement plate] sur A si elle l'est en tant que A-module.*

Remarques :

(i) Tout A-module libre (c'est-à-dire isomorphe à une puissance de A) est plat. Il est fidèlement plat s'il est non nul.

(ii) Le produit tensoriel de deux A-modules plats [resp. fidèlement plats] est plat [resp. fidèlement plat] sur A.

(iii) Si M est un A-module plat [resp. fidèlement plat] et $A \to B$ un morphisme d'anneaux, $M \otimes_A B$ est un B-module plat [resp. fidèlement plat] puisque, pour tout B-module N,

$$(M \otimes_A B) \otimes_B N = M \otimes_A N \,.$$

La réciproque est vraie si B est fidèlement plat sur A puisque, pour tout A-module N

$$(M \otimes_A N) \otimes_A B = (M \otimes_A B) \otimes_B (N \otimes_A B) \,.$$

(iv) Si B est une A-algèbre plate et M un B-module plat, M est plat également comme A-module.

□

On a :

Lemme II.2. –

(i) *Toute localisation d'un anneau A est plate sur A.*
En particulier, si A est intègre, son corps des fractions Frac (A) *est plat sur A.*

(ii) *Un module M sur un anneau A est plat si* Spec (A) *peut être recouvert par des ouverts affines* Spec (A_f) *tels que chaque $M_f = M \otimes_A A_f$ soit plat sur A_f.*

(iii) *Une A-algèbre B est plate sur A si elle peut être recouverte par des ouverts affines* Spec $(B_{f'})$ *s'envoyant dans des ouverts affines* Spec (A_f) *de* Spec (A) *tels que chaque $B_{f'}$ soit plat sur A_f.*

(iv) *Un A-module plat M est fidèlement plat si et seulement si, pour tout idéal maximal m de A, le quotient $M/m \cdot M$ est non nul.*
En particulier, une A-algèbre plate B est fidèlement plate si et seulement si l'image de Spec $(B) \to$ Spec (A) *contient tous les points fermés.*

Il résulte de ce lemme que tout A-module localement libre est plat. Il est fidèlement plat si ses fibres en les points fermés de Spec (A) ne sont jamais nulles.

D'autre part, ce lemme permet de géométriser les notions de platitude ou de fidèle platitude :

Définition II.3. –

(i) *Un $\mathcal{O}_X$-$\mathcal{M}$odule quasi-cohérent sur un schéma X est dit plat [resp. fidèlement plat] si, pour tout ouvert affine $U =$* Spec (A) *de X, $\mathcal{O}_X(U)$ est un A-module plat [resp. fidèlement plat].*

(ii) *Un morphisme de schémas $X \to Y$ est dit plat [resp. fidèlement plat] si, pour tout ouvert affine U de X s'envoyant dans un ouvert affine V de Y, $\mathcal{O}_X(U)$ est une $\mathcal{O}_Y(V)$-algèbre plate [resp. et si de plus l'image de $X \to Y$ contient les points fermés de Y].*

Exemples :

(i) Les immersions ouvertes sont des morphismes plats.

(ii) Un morphisme fini vers un schéma nœthérien

$$f : X \to Y$$

est plat s'il est localement de la forme

$$f^{-1}(U) \cong \text{Spec}\,(A[T]/P)$$

où les $U = \mathrm{Spec}\,(A)$ décrivent un recouvrement affine de Y et les

$$P(T) = T^d + a_{d-1}\,T^{d-1} + \ldots a_1\,T + a_0$$

sont des polynômes à coefficients dans A de coefficient dominant 1.

□

Le lemme II.2 combiné avec les remarques qui suivent la définition I.1 implique les deux corollaires suivants :

Corollaire II.4. –

Pour tout morphisme de schémas $X \xrightarrow{f} Y$, on a :

(i) *Si $\mathcal{M}$ est un $\mathcal{O}_Y$-$\mathcal{M}$odule quasi-cohérent plat [resp. fidèlement plat] sur Y, alors $f^*(\mathcal{M})$ est un $\mathcal{O}_X$-$\mathcal{M}$odule quasi-cohérent plat [resp. fidèlement plat] sur X.*

(ii) *Si f est plat, toute suite de $\mathcal{O}_Y$-$\mathcal{M}$odules quasi-cohérents sur Y*

$$0 \to \mathcal{M}_1 \to \mathcal{M}_2 \to \mathcal{M}_3 \to 0$$

qui est exacte (au sens qu'elle l'est sur tout ouvert affine) est transformée par f^* en une suite de $\mathcal{O}_X$-$\mathcal{M}$odules quasi-cohérents

$$0 \to f^*(\mathcal{M}_1) \to f^*(\mathcal{M}_2) \to f^*(\mathcal{M}_3) \to 0$$

qui est exacte.
La réciproque est vraie si f est fidèlement plat.

□

Corollaire II.5. –

(i) *Le composé de deux morphismes plats $X \to Y \to Z$ est plat.*

(ii) *Pour tout morphisme de schémas*

$$X \to Y$$

et tout morphisme de changement de base $Y' \to Y$, le morphisme obtenu par changement de base

$$X \times_Y Y' \to Y'$$

est plat si $X \to Y$ est plat.
La réciproque est vraie si $Y' \to Y$ est supposé fidèlement plat.

□

Si M est un module sur un anneau intègre A, on appelle partie de torsion de M le sous-module

$$M_{\mathrm{tors}} = \{x \in M \mid \exists\, a \in A - \{0\}\,, \quad a \cdot x = 0\}\,.$$

On dit que M est "sans torsion" si $M_{\mathrm{tors}} = 0$.

Il existe une double relation entre modules plats et modules sans torsion :

Lemme II.6. –

Soit A un anneau intègre. Alors :

(i) *Tout module plat sur A est sans torsion.*

(ii) *Supposons que pour tout idéal premier p de A, tout idéal non trivial du localisé A_p soit engendré par un unique élément.*
Alors tout A-module sans torsion est plat.

Remarque :

L'hypothèse de (ii) implique, si A n'est pas un corps, qu'il est de dimension 1. Elle est satisfaite si A est l'anneau $\mathbb{Z}$, ou $K[T]$ (pour n'importe quel corps K), ou l'un de leurs localisés.

Démonstration :

(i) Si M est un A-module contenant un élément $x \neq 0$ tel que $a \cdot x = 0$ pour un $a \in A - \{0\}$, la tensorisation par M ne préserve pas l'exactitude de la suite $0 \longrightarrow A \xrightarrow{a} A \longrightarrow A/a \cdot A \longrightarrow 0$.

(ii) Il suffit de traiter le cas où A est un anneau local. Alors tout idéal non trivial de A est libre donc plat. D'autre part, toute réunion filtrante de modules plats est un module plat. Donc il suffit de montrer que tout A-module M de type fini et sans torsion est libre. En notant $F = \mathrm{Frac}\,(A)$, M se plonge dans $M \otimes_A F$, donc dans une puissance F^r puis dans une puissance A^r.
On conclut par récurrence sur r en remarquant que dans toute suite exacte $0 \to M' \to M \to M'' \to 0$, M est libre si M' et M'' le sont.

□

Enfin, pour les $\mathcal{M}$odules cohérents sur les schémas localement nœthériens, "plat" équivaut à "localement libre" :

Lemme II.7. –

(i) *Sur un schéma S localement nœthérien, un $\mathcal{O}_S$-$\mathcal{M}$odule cohérent $\mathcal{M}$ est plat si et seulement si il est localement libre de rang fini.*

(ii) *Si S est connexe, le rang de $\mathcal{M}$ est alors constant et $\mathcal{M}$ est fidèlement plat s'il n'est pas* 0.

Démonstration :

Il suffit de prouver que si A est un anneau local nœthérien d'idéal maximal m, un A-module de type fini M est plat si et seulement si il est libre.

Si M est libre, il est plat.

Réciproquement, supposons que M est de type fini et plat.

Soient $x_1, \ldots, x_d$ des éléments de M dont les images dans l'espace vectoriel $M/m \cdot M$ constituent une base sur le corps A/m. Ces éléments définissent un morphisme

$$A^d \to M$$

qui, d'après le lemme de Nakayama I.34, est surjectif. Il faut montrer que son noyau M' est 0. Comme A est nœthérien, M' est de type fini et il suffit de prouver que $m \cdot M' = M'$, autrement dit que la suite

$$0 \longrightarrow M'/m \cdot M' \longrightarrow (A/m)^d \longrightarrow M/m \cdot M \longrightarrow 0$$

est exacte.

C'est un cas particulier de l'important lemme suivant :

Lemme II.8. –

Soient A un anneau arbitraire et M un A-module plat qui s'inscrit dans une suite exacte de A-modules

$$0 \longrightarrow M_1 \longrightarrow M_2 \longrightarrow M \longrightarrow 0\,.$$

Alors, pour tout A-module N, la suite

$$0 \longrightarrow M_1 \otimes_A N \longrightarrow M_2 \otimes_A N \longrightarrow M \otimes_A N \longrightarrow 0$$

est exacte.

Démonstration :

Il existe un A-module libre, donc plat, N_2 tel que N s'inscrive dans une suite exacte

$$0 \longrightarrow N_1 \longrightarrow N_2 \longrightarrow N \longrightarrow 0\,.$$

La conclusion résulte de ce que, dans le diagramme commutatif ci-dessous, toutes les lignes horizontales ou verticales sont exactes :

$$\begin{tikzcd}
 & & & 0 \arrow[d] & \\
 & M_1 \otimes_A N_1 \arrow[r] \arrow[d] & M_2 \otimes_A N_1 \arrow[r] \arrow[d] & M \otimes_A N_1 \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & M_1 \otimes_A N_2 \arrow[r] \arrow[d] & M_2 \otimes_A N_2 \arrow[r] \arrow[d] & M \otimes_A N_2 \arrow[r] \arrow[d] & 0 \\
 & M_1 \otimes_A N \arrow[r] \arrow[d] & M_2 \otimes_A N \arrow[r] \arrow[d] & M \otimes_A N \arrow[r] \arrow[d] & 0 \\
 & 0 & 0 & 0 &
\end{tikzcd}$$

□

2 Morphismes nets ou non-ramifiés

Commençons par introduire le module des différentielles d'une algèbre de type fini :

Lemme II.9. –

Soit B une algèbre de type fini sur un anneau A.

Soit $\Omega^1_{B/A}$ le B-module défini comme le quotient du B-module libre de base notée formellement

$$db\,, \quad b \in B\,,$$

par le sous-B-module engendré par les relations

$$d(ab) = a \cdot db\,, \quad \forall\, a \in A\,, \quad \forall\, b \in B\,,$$

$$\left.\begin{aligned} d(b+b') &= db + db' \\ d(bb') &= b \cdot db' + b' \cdot db \end{aligned}\right\} \qquad \forall\, b, b' \in B\,.$$

Alors $\Omega^1_{B/A}$ est un B-module de type fini et il s'identifie au quotient I/I^2 si I est le noyau du morphisme surjectif

$$B \otimes_A B \to B \,.$$

Exemple :

Si $B = A[X_1, \dots, X_d]$, $\Omega^1_{B/A}$ est le B-module libre sur la base $dX_1, \dots, dX_d$.

Démonstration :

Par hypothèse, B est engendré sur A par un nombre fini d'éléments $b_1, \dots, b_n$. Alors le B-module $\Omega^1_{B/A}$ est engendré par ses éléments $db_1, \dots, db_n$.

L'isomorphisme

$$\Omega^1_{B/A} \xrightarrow{\sim} I/I^2$$

est défini en associant à tout élément db, $b \in B$, la différence

$$1 \otimes b - b \otimes 1 \,.$$

L'isomorphisme réciproque est défini en associant à tout élément $\sum\limits_i b_i \otimes b'_i$ de $I \subset B \otimes_A B$ la somme

$$\sum_i b_i \cdot d\, b'_i \,.$$

□

Les propriétés principales du module des différentielles $\Omega^1_{B/A}$ sont :

Lemme II.10. –

(i) *Si B est une A-algèbre de type fini, la formation de $\Omega^1_{B/A}$ commute à la localisation et au changement de base au sens que*

- *si B_f est la localisation de B en un élément f, on a*

$$\Omega^1_{B_f/A} = \Omega^1_{B/A} \otimes_B B_f \,,$$

- *si A' est une A-algèbre, on a*

$$\Omega^1_{B \otimes_A A'/A'} = \Omega^1_{B/A} \otimes_B (B \otimes_A A') = \Omega^1_{B/A} \otimes_A A' \,.$$

(ii) *Si $A \to B \to C$ sont des morphismes de type fini d'anneaux, on a une suite exacte canonique de C-modules*

$$\Omega^1_{B/A} \otimes_B C \longrightarrow \Omega^1_{C/A} \longrightarrow \Omega^1_{C/B} \longrightarrow 0 \,.$$

Exemple :

Si B est le quotient de $A[X_1, \dots, X_d]$ par l'idéal engendré par des polynômes

$$P(X_1, \dots, X_d) \,,$$

alors $\Omega^1_{B/A}$ est le quotient du B-module libre sur les éléments

$$dX_1, \dots, dX_d$$

par le sous-module engendré par les

$$\sum_{1 \leq i \leq d} \frac{\partial P}{\partial X_i} \, (X_1, \ldots, X_d) \cdot dX_i \, .$$

□

Pour tout morphisme de schémas

$$X \to Y$$

qui est localement de type fini, le lemme II.10(i) permet de définir $\Omega^1_{X/Y}$ en tant que $\mathcal{O}_X$-$\mathcal{M}$odule quasi-cohérent de type fini (et donc cohérent si X est nœthérien) sur X.

On déduit du lemme précédent :

Corollaire II.11. –

(i) *Pour tout morphisme de schémas localement de type fini*

$$X \to Y$$

et tout morphisme de changement de base $Y' \to Y$, on a

$$\Omega^1_{X \times_Y Y'/Y'} = f^*(\Omega^1_{X/Y})$$

si f désigne le morphisme $X \times_Y Y' \to X$ déduit de $Y' \to Y$.

(ii) *Pour tous morphismes localement de type fini*

$$X \xrightarrow{f} Y \longrightarrow Z \, ,$$

on a une suite exacte canonique de $\mathcal{O}_X$-$\mathcal{M}$odules quasi-cohérents

$$f^*(\Omega^1_{Y/Z}) \longrightarrow \Omega_{X/Z} \longrightarrow \Omega^1_{X/Y} \longrightarrow 0 \, .$$

□

On peut maintenant introduire la notion de morphisme non ramifié ou net :

Lemme II.12. –

Pour tout morphisme localement de type fini

$$X \to Y$$

les deux conditions suivantes sont équivalentes :

(1) *On a $\Omega^1_{X/Y} = 0$.*

(2) *L'immersion diagonale*

$$X \to X \times_Y X$$

est une immersion ouverte.

Lorsqu'elles sont vérifiées, on dit que $X \to Y$ est net ou que X est non ramifié sur Y.

Exemples :

(i) Toute immersion localement fermée est nette.

(ii) Si B est le quotient de $A[X]$ par l'idéal engendré par une famille de polynômes $P(X)$, B est net sur A si et seulement si l'idéal engendré par les polynômes dérivés $P'(X)$ et les $P(X)$ est tout $A[X]$. Il suffit pour cela qu'il en soit ainsi après réduction dans $A/m\,[X]$ pour tout idéal maximal m de A.

(iii) Plus généralement, si B est le quotient de $A[X_1, \ldots, X_d]$ par l'idéal engendré par des polynômes $P(X_1, \ldots, X_d)$, B est net sur A si et seulement si, pour tout idéal maximal m de A, les familles

$$\left(\frac{\partial P}{\partial X_i}\,(X_1, \ldots, X_d) \right)_{1 \leq i \leq d}$$

engendrent tout $(B/m \cdot B)^d$ comme module.

Démonstration :

Il faut prouver que si B est une A-algèbre de type fini et I le noyau du morphisme surjectif

$$B \otimes_A B \to B$$

ce morphisme devient injectif dans un voisinage ouvert de $\mathrm{Spec}\,(B)$ si et seulement si $\Omega^1_{B/A} = I/I^2$ est 0.

Si $I = 0$ dans un voisinage ouvert de $\mathrm{Spec}\,(B)$, on a $I/I^2 = 0$. La réciproque résulte du lemme de Nakayama I.34 puisque I est engendré par un nombre fini d'éléments, les $1 \otimes b_i - b_i \otimes 1$ si $b_1, \ldots, b_n$ engendrent la A-algèbre B.

□

Le corollaire II.11 implique :

Corollaire II.13. –

(i) *Le composé de deux morphismes nets est net.*
Plus généralement, si $X \to Y \to Z$ sont des morphismes localement de type fini et Y est non ramifié sur Z, on a

$$\Omega^1_{X/Y} = \Omega^1_{X/Z}\,.$$

(ii) *Soient $X \to Y$ un morphisme localement de type fini et $Y' \to Y$ un morphisme de changement de base.*
Alors, si $X \to Y$ est net, $X \times_Y Y' \to Y'$ est net.
La réciproque est vraie si $Y' \to Y$ est fidèlement plat.

□

Terminons l'examen des morphismes nets par la description de leurs fibres :

Proposition II.14. –

Soit $X \to Y$ un morphisme net.

Alors, pour tout point y de Y, de corps résiduel κ_y, la fibre

$$X_y = X \times_Y \mathrm{Spec}\,(\kappa_y)$$

est une réunion disjointe de points de la forme

$$\mathrm{Spec}\,(\kappa_x)$$

où les κ_x sont des extensions finies séparables de κ_y.

En particulier, si $X \to Y$ est de type fini, X_y est le spectre d'une κ_y-algèbre finie séparable.

Démonstration :

On peut supposer que $Y = \mathrm{Spec}\,(K)$ est le spectre d'un corps K.

Pour tout point x de X défini sur un corps $K' \supset K$, c'est-à-dire pour tout morphisme

$$x : \mathrm{Spec}\,(K') \to X\,,$$

ce point x s'identifie à un ouvert de $X \otimes_K K' = X \times_{\mathrm{Spec}(K)} \mathrm{Spec}\,(K')$ puisque le plongement diagonal

$$X \otimes_K K' \to (X \otimes_K K') \times_{K'} (X \otimes_K K') = (X \times_K X) \otimes_K K'$$

est une immersion ouverte.

Le morphisme

$$\coprod_{x \in X} \mathrm{Spec}\,(\kappa_x) \to X$$

est un isomorphisme car il le devient au voisinage de tout point de X après extension assez grande du corps de base K.

Les corps résiduels κ_x sont des extensions finies de K car ils sont de type fini comme K-algèbres, puisque X est localement de type fini sur K.

Enfin, ils sont séparables puisque les $\kappa_x \otimes_K K'$ n'admettent jamais d'éléments nilpotents non nuls. □

3 Morphismes étales

On pose :

Définition II.15. –

Un morphisme localement de type fini

$$X \to Y$$

est appelé étale s'il est net et plat.

Exemples :

(i) Les immersions ouvertes sont étales.

(ii) Pour tout anneau A et tout polynôme de coefficient dominant 1

$$P(T) = T^d + a_{d-1} \cdot T^{d-1} + \ldots + a_1 \cdot T + a_0\,,$$

l'algèbre quotient

$$A[T]/P(T)$$

est non ramifiée et donc étale sur A si et seulement si, pour tout idéal maximal m de A, le polynôme induit par P dans

$$(A/m)\,[T]$$

est séparable, c'est-à-dire a toutes ses racines distinctes dans une clôture algébrique du corps A/m.

□

En combinant le corollaire II.5 et le corollaire II.13, on obtient :

Corollaire II.16. –

(i) *Le composé de deux morphismes étales est étale.*

(ii) *Pour tout morphisme localement de type fini*

$$X \to Y$$

et tout morphisme de changement de base $Y' \to Y$, le morphisme

$$X \times_Y Y' \to Y'$$

est étale si $X \to Y$ est étale.
La réciproque est vraie si $Y' \to Y$ est supposé fidèlement plat. □

Voici une propriété fondamentale des morphismes étales :

Proposition II.17. –
Un morphisme $X \to Y$ est un isomorphisme si et seulement si il est étale et universellement bijectif (c'est-à-dire est bijectif sur les points et le reste après n'importe quel changement de base).

Démonstration :
On peut supposer que Y est le spectre d'un anneau local A.

Soit $U = \mathrm{Spec}\,(B)$ un ouvert affine de X qui contient le point de X qui correspond à l'unique point fermé de $\mathrm{Spec}\,(A)$. Alors la A-algèbre B est fidèlement plate.

Comme le morphisme $X \to X \times_Y X$ est une immersion ouverte, il en est de même de $U \to X \times_Y U$.

Or la projection $X \times_Y U \to U$ se déduit de $X \to Y$ par changement de base donc elle est bijective.

Par conséquent, $U \to X \times_Y U$ est un isomorphisme et il en est a fortiori de même de $U \to U \times_Y U$ et donc de

$$B \otimes_A B \to B \qquad \text{ou} \qquad B \to B \otimes_A B\,.$$

Comme B est fidèlement plat sur A, il en résulte que

$$A \to B$$

est un isomorphisme.

Comme $X \to Y$ est bijectif, c'est un isomorphisme. □

On a d'autre part :

Lemme II.18. –
Soit X un schéma étale (ou plus généralement net) et séparé sur un schéma Y connexe.

Alors il y a bijection entre les sections de $X \to Y$ et les composantes connexes de X qui se projettent sur Y par un isomorphisme.

En particulier, deux sections qui coïncident en un point de Y sont égales.

Démonstration :
Par hypothèse, l'immersion diagonale

$$X \to X \times_Y X$$

est à la fois ouverte et fermée.

Or toute section $Y \xrightarrow{s} X$ de $X \to Y$ s'en déduit par le changement de base $X = Y \times_Y X \to X \times_Y X$, donc est une immersion à la fois ouverte et fermée.

□

En combinant la proposition II.17 et le lemme II.18, on obtient :

Corollaire II.19. –

Soient S un schéma de base, S_0 un sous-schéma fermé de même espace sous-jacent, X un schéma arbitraire sur S et Y un schéma étale et séparé sur S.

Alors se donner un morphisme au-dessus de S

$$X \to Y$$

équivaut à se donner un morphisme au-dessus de S_0

$$X_0 = X \times_S S_0 \to Y \times_S S_0 = Y_0 \,.$$

Démonstration :

Par le changement de base $X \to S$, on se ramène au cas où $X = S$ et Y est un schéma étale et séparé sur X.

On peut supposer aussi que X est connexe.

Alors les sections de $Y \to X$ sont les composantes connexes de Y dont la projection sur X est universellement bijective.

Elles ne changent pas si l'on remplace X par X_0 et Y par Y_0. $\square$

Les schémas étales et séparés sur un schéma S donné forment une catégorie dont les morphismes sont les $X \to Y$ rendant commutatifs les diagrammes :

$$\begin{tikzcd} X \arrow[rr] \arrow[dr] & & Y \arrow[dl] \\ & S & \end{tikzcd}$$

Le corollaire précédent implique encore :

Corollaire II.20. –

Soit A un anneau local d'idéal maximal m et de corps résiduel K.

(i) *Si A est artinien, c'est-à-dire si*

$$m^n = 0 \quad \textit{pour un entier } n \geq 1 \textit{ assez grand,}$$

la catégorie des schémas étales sur $\mathrm{Spec}\,(A)$ *est équivalente à celle de* $\mathrm{Spec}\,(K)$.

(ii) *Si l'on note*

$$\widehat{A} = \varprojlim_n A/m^n \,,$$

la catégorie des schémas étales et finis sur $\mathrm{Spec}\,(\widehat{A})$ *est équivalente à celle de* $\mathrm{Spec}\,(K)$.

Exemples :

Si $A = \mathbb{Z}_{(p)}$ est l'anneau local de $\mathbb{Z}$ en un nombre premier p,

$$\widehat{A} = \varprojlim_n \ \mathbb{Z}/p^n \cdot \mathbb{Z}$$

est l'anneau $\mathbb{Z}_p$ des "entiers p-adiques".

De même, si K est un corps et A est l'anneau local de $K[T]$ au point $T = 0$,

$$\widehat{A} = \varprojlim_n K[T]/T^n \cdot K[T]$$

est l'anneau

$$K[[T]] = \left\{ \sum_{n \geq 0} a_n \cdot T^n \mid a_n \in K \right\}$$

des séries formelles en T à coefficients dans K.

Démonstration :

(ii) résulte de (i).

(i) D'après la corollaire II.19, il suffit de prouver que tout schéma étale sur $\mathrm{Spec}\,(K)$ se relève en un schéma étale sur $\mathrm{Spec}\,(A)$.
D'après la proposition II.14, il suffit de traiter le cas du spectre $\mathrm{Spec}\,(K')$ d'une extension finie séparable K' de K. Elle est de la forme

$$K' = K[T]/\overline{P}$$

avec

$$\overline{P} = T^d + \overline{a}_{d-1} \cdot T^{d-1} + \ldots + \overline{a}_0 \in K[T]\,.$$

Le polynôme P se relève en un polynôme de $A[T]$ de la forme

$$P = T^d + a_{d-1} \cdot T^{d-1} + \ldots + a_0$$

et $\mathrm{Spec}\,(A[T]/P)$ répond à la question posée. □

4 Les propriétés des revêtements finis étales

Dans tout ce paragraphe, on se place sur un schéma de base S supposé localement nœthérien.

On pose :

Définition II.21. –

On appelle revêtement (fini) étale de S tout morphisme

$$X \to S$$

qui est étale et fini au sens de la définition I.31.

Autrement dit, pour tout ouvert affine $\mathrm{Spec}\,(A)$ *de S, son image réciproque dans X est un ouvert affine* $\mathrm{Spec}\,(B)$ *dont l'anneau B est non ramifié sur A et localement libre de rang fini comme A-module.*

Exemple :

Si $S = \mathrm{Spec}\,(A)$ et $X = \mathrm{Spec}\,(A[T]/P)$ où $P \in A[T]$ est un polynôme de la forme

$$P = T^d + a_{d-1} \cdot T^{d-1} + \ldots + a_0\,,$$

X est un revêtement étale de S si et seulement si, pour tout idéal maximal m de A et si $\overline{\kappa}$ désigne une clôture algébrique de $\kappa = A/m$, les racines dans $\overline{\kappa}$ du polynôme induit par P dans $\kappa[T]$ sont deux à deux distinctes.

□

Voici le lemme principal pour l'étude des propriétés des revêtements finis étales :

Lemme II.22. –

Soit $\left(X \xrightarrow{f} S\right)$ *un revêtement étale d'un schéma localement nœthérien* S.

Si S *est connexe ou plus généralement si le degré de* X *sur* S *(défini comme le rang du* $\mathcal{O}_S$*-*$\mathcal{M}$*odule localement libre* $f_* \mathcal{O}_X$*) est constant égal à* d*, il existe un morphisme de changement de base fidèlement plat (et même fini étale)*

$$S' \to S$$

tel que le revêtement étale $X \times_S S'$ *de* S' *devienne isomorphe à la somme de* d *copies de* S'.

Démonstration du lemme :

Montrons-le par récurrence sur $d \geq 1$.

Le morphisme $X \to S$ est fidèlement plat.

Considérons le revêtement étale $X \times_S X$ de X déduit de $X \to S$ par le morphisme de changement de base $X \to S$.

Il possède pour section le morphisme diagonal $X \to X \times_S X$. Celui-ci est une immersion fermée puisque X est séparé sur S, et c'est aussi une immersion ouverte puisque X est étale sur S'.

Donc le revêtement étale $X \times_S X$ de X s'écrit comme la somme de la section X et d'un revêtement étale X' de X dont le degré est nécessairement constant égal à $d - 1$.

On conclut d'après l'hypothèse de récurrence. □

On peut introduire la catégorie Rev_S dont les objets sont les revêtements (finis) étales du schéma localement nœthérien S

$$X \to S$$

et dont les morphismes $(X \to S) \to (Y \to S)$ sont les morphismes de schémas $X \to Y$ rendant commutatif le triangle :

$$\begin{tikzcd} X \arrow[rr] \arrow[dr] & & Y \arrow[dl] \\ & S & \end{tikzcd}$$

Montrons :

Théorème II.23. –

La catégorie Rev_S *des revêtements étales d'un schéma localement nœthérien* S *possède les propriétés suivantes :*

(i) Rev_S *a un objet final et le produit fibré dans* Rev_S *de deux objets au-dessus d'un troisième existe.*

(ii) *Les sommes finies dans* Rev_S *existent, ainsi que le quotient d'un objet de* Rev_S *par l'action d'un groupe fini d'automorphismes.*

(iii) *Tout morphisme* $u : X \to Y$ *de* Rev_S *se factorise en*

$$X \xrightarrow{u'} Y' \xrightarrow{u''} Y$$

où u' *est un épimorphisme strict et* u'' *un monomorphisme tel que* Y *s'identifie à la somme de* Y' *et d'un autre objet.*

Démonstration :

(i) L'identité ($S \to S$) est un objet final de Rev_S au sens que tout objet ($X \to S$) possède un unique morphisme vers ($S \to S$).
Si ($X_1 \to S$) et ($X_2 \to S$) sont deux objets de Rev_S au-dessus d'un troisième $Y \to S$, le morphisme

$$X_1 \times_Y X_2 \to S$$

est fini. D'autre part, il est étale car il est le composé de

$$X_1 \times_S X_2 \to S$$

et de

$$X_1 \times_Y X_2 \to X_1 \times_S X_2$$

qui se déduit par changement de base de

$$Y \to Y \times_S Y$$

qui est une immersion ouverte.
Ainsi,

$$X_1 \times_Y X_2 \to S$$

est un objet de Rev_S et il définit un produit fibré dans Rev_S de ($X_1 \to S$) et ($X_2 \to S$) au-dessus de ($Y \to S$).

(ii) Si $(X_1 \to S), \dots, (X_k \to S)$ sont des objets de Rev_S, se donner des morphismes de ces objets dans un autre ($Y \to S$) équivaut à se donner un morphisme

$$X_1 \coprod \dots \coprod X_k \to Y\,.$$

Comme $X_1 \coprod \dots \coprod X_k$ est fini et étale sur S, il définit une somme de $(X_1 \to S), \dots, (X_k \to S)$ dans Rev_S.
On note que si $Y = \mathrm{Spec}\,(A)$ est affine, $X_1 = \mathrm{Spec}\,(B_1), \dots, X_k = \mathrm{Spec}\,(B_k)$ sont affines et leur somme $X_1 \coprod \dots \coprod X_k$ est $\mathrm{Spec}\left(\prod_{1 \le i \le k} B_i\right)$.
Considérons maintenant un objet ($X \to S$) de Rev_S muni de l'action d'un groupe fini G d'automorphismes.
On cherche à construire un objet ($X^G \to S$) de Rev_S tel que se donner un morphisme $X^G \to Y$ vers un objet arbitraire ($Y \to S$) de Rev_S équivale à se donner un morphisme $X \to Y$ fixe par l'action de G.
Il suffit de construire X^G lorsque $S = \mathrm{Spec}\,(A)$ et donc $X = \mathrm{Spec}\,(B)$ sont affines, pouvu que la formation de X^G commute avec les immersions ouvertes $\mathrm{Spec}\,(A_f) \to \mathrm{Spec}\,(A)$.
On définit X^G comme $\mathrm{Spec}\,(B^G)$ où B^G désigne la sous-algèbre de B sur A constituée des éléments fixés par tout $g \in G$.
Comme A-module, B^G est défini comme le noyau de la différence des deux morphismes

$$B \to \prod_{g \in G} B$$

que sont le plongement diagonal et le produit des automorphismes $g \in G$.
Comme on peut supposer A nœthérien et que B est un A-module de type fini, B^G est aussi de type fini comme A-module et le morphisme $\mathrm{Spec}\,(B^G) \to \mathrm{Spec}\,(A)$ est fini.

D'autre part, la formation de la sous-algèbre B^G commute avec toute immersion ouverte et plus généralement avec tout changement de base plat $\mathrm{Spec}\,(A') \to \mathrm{Spec}\,(A)$.

Il reste à prouver que B^G est étale sur A et, pour cela, il suffit de le montrer après n'importe quel changement de base fidèlement plat et donc, d'après le lemme II.22, dans le cas où X est une somme de copies de S.

Or, dans ce cas, la propriété est évidente.

(iii) On doit factoriser un tel morphisme $X \to Y$ de Rev_S en

$$X \to Y' \to Y$$

où

- $Y' \to Y$ est une immersion ouverte et fermée,
- $X \to Y'$ est un épimorphisme strict, ce qui signifie que pour tout objet Z de Rev_S, se donner un morphisme $Y' \to Z$ équivaut à se donner un morphisme $X \to Z$ dont les deux composés avec $X \times_{Y'} X \rightrightarrows X$ coïncident.

Il suffit de construire Y' localement au-dessus de S, pourvu que la construction commute avec les immersions ouvertes $S' \to S$.

Supposons donc que $S = \mathrm{Spec}\,(A)$ est le spectre d'un anneau nœthérien.

Alors $Y = \mathrm{Spec}\,(B)$ et $X = \mathrm{Spec}\,(C)$ sont les spectres de A-algèbres finies reliées par un morphisme

$$B \xrightarrow{u} C\,.$$

On pose $Y' = \mathrm{Spec}\,(B')$ où

$$B' = \mathrm{Im}\,(u) = B/\mathrm{Ker}\,(u)\,.$$

La formation de B' commute aux localisations $\mathrm{Spec}\,(A_f) \to \mathrm{Spec}\,(A)$ et plus généralement à tous les changements de base plats $\mathrm{Spec}\,(A') \to \mathrm{Spec}\,(A)$.

Montrons que le morphisme $X \to Y'$ est étale. Il suffit de le vérifier après n'importe quel changement de base fidèlement plat $S' \to S$. D'après le lemme II.22 ci-dessus, on peut donc supposer que X et Y sont des sommes finies de copies de S et alors c'est évident.

Ainsi, C est une B'-algèbre finie et étale, donc localement libre de rang fini comme B'-module. De plus, le morphisme $B' \to C$ est injectif par construction, et le quotient C/B' est un B'-module plat donc localement libre de rang fini comme cela se prouve une fois de plus après changement de base fidèlement plat.

On en déduit facilement que B' s'identifie au noyau de la différence des deux morphismes

$$C \rightrightarrows C \otimes_{B'} C$$

ce qui entraîne que $\mathrm{Spec}\,(C) \to \mathrm{Spec}\,(B')$ est un épimorphisme strict.

Par construction, $Y' \to Y$ est une immersion fermée.

Il reste à prouver que c'est une immersion ouverte, autrement dit que, au voisinage de tout point de $Y = \mathrm{Spec}\,(B)$, ou bien $B' \to C$ est un isomorphisme, ou bien $B' = 0$. Il suffit de le démontrer après un changement de base fidèlement plat. Cela nous ramène au cas où X et Y sont des sommes finies de copies de S, qui est trivial.

Cela termine la preuve du théorème II.23. On note qu'on a prouvé au passage :

Corollaire II.24. –

Dans la catégorie Rev_S*, tous les morphismes* $X \to Y$ *entre revêtements étales sont eux-mêmes des revêtements étales.* □

Considérons maintenant un “point géométrique” $\overline{s}$ de S, c’est-à-dire un morphisme vers S

$$\mathrm{Spec}\,(\overline{\kappa}) \to S$$

du spectre d’un corps algébriquement clos $\overline{\kappa}$.

Pour tout revêtement étale X de S, $X \times_S \overline{s}$ est un revêtement étale de $\mathrm{Spec}\,(\overline{\kappa})$ c’est-à-dire, d’après la proposition II.14, une somme finie de copies de $\mathrm{Spec}\,(\overline{\kappa})$. L’ensemble $X(\overline{s})$ des points $\mathrm{Spec}\,(\overline{\kappa}) \to X$ au-dessus de $\overline{s}$ est donc fini. Il compte d éléments si X est de degré d au voisinage de l’image de $\overline{s}$.

Le théorème II.23 est complété par :

Proposition II.25. –

Pour tout point géométrique $\overline{s} : \mathrm{Spec}\,(\overline{\kappa}) \to S$ *du schéma de base localement nœthérien* S*,*

$$(X \to S) \to X(\overline{s})$$

définit un foncteur $F_{\overline{s}}$ *de la catégorie* Rev_S *des revêtements (finis) étales de* S *vers la catégorie des ensembles finis.*

Ce foncteur $F_{\overline{s}}$ *possède les propriétés suivantes :*

(i) *Il est exact à gauche, c’est-à-dire transforme objet final en objet final et commute avec la formation des produits fibrés.*

(ii) *Il commute avec la formation des sommes finies, transforme les épimorphismes stricts en épimorphismes (c’est-à-dire en surjections) et commute avec tout passage au quotient par un groupe fini d’automorphismes.*

(iii) *Si* S *est connexe, alors tout morphisme de* Rev_S

$$(X \to S) \xrightarrow{u} (Y \to S)$$

qui induit un isomorphisme, c’est-à-dire une bijection

$$F_{\overline{s}}(u) : X(\overline{s}) \to Y(\overline{s})\,,$$

est un isomorphisme.

Démonstration :

(i) résulte de ce que la formation des produits fibrés dans Rev_S coïncide avec celle dans la catégorie des schémas.

(ii) La formation des sommes finies commute avec $F_{\overline{s}}$ puisque $\mathrm{Spec}\,(\overline{\kappa})$ est connexe.

Les épimorphismes stricts le restent après tout changement de base plat, et le passage au quotient par un groupe fini commute avec tout changement de base plat.

D’après le lemme II.22, il suffit donc de considérer le cas de revêtements étales qui sont des sommes finies de copies de S. C’est alors évident.

(iii) Il suffit de le vérifier après un changement de base $S' \to S$ fidèlement plat. D’après le lemme II.22, on peut donc supposer que X et Y sont des sommes de copies de S et alors c’est évident.

□

5 Catégories galoisiennes et groupes fondamentaux de Grothendieck

Suivant Grothendieck, on pose :

Définition II.26. –

On appelle "catégorie galoisienne" toute catégorie $\mathcal{C}$ qui admet un foncteur F vers la catégorie des ensembles finis, appelé "foncteur fibre", vérifiant les propriétés suivantes :

(1) *$\mathcal{C}$ a un objet final, et les produits fibrés de deux objets de $\mathcal{C}$ au-dessus d'un troisième existent.*

(2) *Les sommes finies existent dans $\mathcal{C}$, ainsi que le quotient d'un objet de $\mathcal{C}$ par un groupe fini d'automorphismes.*

(3) *Tout morphisme $X \xrightarrow{u} Y$ de $\mathcal{C}$ se factorise comme le composé*

$$X \xrightarrow{u'} Y' \xrightarrow{u''} Y$$

d'un épimorphisme strict u' et d'un monomorphisme u'' tel que Y s'identifie à la somme de Y' et d'un autre objet de $\mathcal{C}$.

(1′) *Le foncteur F est exact à gauche.*

(2′) *Il commute avec la formation des sommes finies, transforme les épimorphismes stricts en épimorphismes, et commute avec le passage au quotient par un groupe fini d'automorphismes.*

(3′) *Tout morphisme $X \xrightarrow{u} Y$ de $\mathcal{C}$ tel que*

$$F(X) \xrightarrow{F(u)} F(Y)$$

est une bijection, est un isomorphisme.

Exemples :

(i) Le théorème II.23 et la proposition II.25 se résument donc en disant que pour tout schéma localement nœthérien et connexe S, et pour tout point géométrique $\overline{s}$ de S, la catégorie Rev_S des revêtements étales de S, munie du foncteur de fibre en $\overline{s}$

$$X \mapsto X(\overline{s}),$$

est une catégorie galoisienne.

(ii) La catégorie des ensembles finis munie du foncteur identité est une catégorie galoisienne.

(iii) Si Γ est un groupe fini, soit $\mathcal{C}_\Gamma$ la catégorie des ensembles finis X munis d'une action de Γ

$$\Gamma \times X \ni (g, x) \mapsto g \cdot x \in X .$$

Les morphismes de $\mathcal{C}_\Gamma$ sont donc les applications

$$X \xrightarrow{u} Y$$

telles que

$$u(g \cdot x) = g \cdot u(x) , \qquad \forall\, x \in X , \quad \forall\, g \in \Gamma .$$

Soit d'autre part F_Γ le foncteur qui associe à tout ensemble fini muni d'une action de Γ le même ensemble, en oubliant l'action de Γ.

Alors $\mathcal{C}_\Gamma$ munie du foncteur F_Γ est une catégorie galoisienne.

(iv) Plus généralement, soit Γ un "groupe profini" c'est-à-dire un groupe topologique séparé dans lequel une base de voisinages ouverts de l'unité 1 est constituée de sous-groupes ouverts d'indice fini ou, ce qui revient au même, de sous-groupes ouverts distingués d'indice fini. Autrement dit, Γ s'écrit comme une limite projective filtrante de groupes finis.

Soit alors $\mathcal{C}_\Gamma$ la catégorie des ensembles finis munis d'une action continue de Γ (c'est-à-dire pour laquelle le fixateur de tout élément est un sous-groupe ouvert de Γ). Et soit F_T le foncteur de $\mathcal{C}_\Gamma$ vers la catégorie des ensembles qui consiste à oublier l'action de Γ.

Alors $\mathcal{C}_\Gamma$ munie du foncteur d'oubli F_Γ est encore une catégorie galoisienne.

□

Grothendieck a montré le théorème très général suivant qui fait se correspondre les catégories galoisiennes et les groupes profinis :

Théorème II.27. –

(i) *Soit $(\mathcal{C}, F)$ une catégorie galoisienne munie d'un foncteur fibre F.*

Soit Γ le groupe des automorphismes du foncteur F, c'est-à-dire le groupe des familles $g = (g_X)$ de bijections

$$g_X : F(X) \xrightarrow{\sim} F(X)$$

indexées par les objets X de la catégorie $\mathcal{C}$, qui rendent commutatifs tous les diagrammes :

$$\begin{tikzcd} F(X) \arrow[r, "g_X"] \arrow[d, "F(u)"'] & F(X) \arrow[d, "F(u)"] \\ F(Y) \arrow[r, "g_Y"] & F(Y) \end{tikzcd}$$

Munissons Γ de la topologie dont une base de voisinages ouverts de 1 est constituée des fixateurs d'éléments des ensembles finis $F(X)$.

Alors Γ est un groupe profini, et la catégorie $\mathcal{C}$ munie du foncteur F est équivalente à la catégorie $(\mathcal{C}_\Gamma, F_\Gamma)$.

Cela signifie que :

- *se donner un objet $\mathcal{C}$ (à unique isomorphisme près) équivaut à se donner un ensemble fini muni d'une action de Γ,*
- *étant donnés deux objets de Γ, se donner un morphisme de l'un vers l'autre équivaut à se donner une application entre les ensembles finis associés qui est compatible avec les actions de Γ.*

(ii) *Soient $\mathcal{C}$ et $\mathcal{C}'$ deux catégories galoisiennes munies de deux foncteurs fibres F et F', et soient Γ et Γ' leurs groupes finis d'automorphismes.*

Alors se donner un homomorphisme continu

$$\Gamma \to \Gamma'$$

équivaut à se donner un foncteur

$$G : \mathcal{C}' \to \mathcal{C}$$

et un isomorphisme entre les deux foncteurs $G \circ F$ et F'.

(iii) *Tous les foncteurs fibres d'une catégorie galoisienne $\mathcal{C}$ sont isomorphes, si bien que les groupes profinis associés sont isomorphes, par des isomorphismes déterminés à conjugaison près.*

Pour la démonstration :

Elle ne fait pas partie de la géométrie arithmétique mais de la théorie des catégories. On se reportera à SGA1 (pages 98-107 de la nouvelle édition).

$\square$

Ce théorème combiné avec le théorème II.23 et la proposition II.25 implique :

Théorème II.28. –

(i) *Soient S un schéma localement nœthérien connexe et $\overline{s} : \operatorname{Spec}(\overline{\kappa}) \to S$ un point géométrique de S. Alors la catégorie Rev_S des revêtements (finis) étales de S, munie du foncteur des fibres en $\overline{s}$*

$$X \mapsto X(\overline{s}) \,,$$

est équivalente à la catégorie des ensembles finis munis d'une action d'un certain groupe profini

$$\pi_1(S, \overline{s})$$

appelé le groupe fondamental de S en $\overline{s}$.

(ii) *De plus, si $\overline{s}_1 : \operatorname{Spec}(\overline{\kappa}_1) \to S$ est un autre point géométrique de S, les groupes profinis $\pi_1(S, \overline{s})$ et $\pi_1(S, \overline{s}_1)$ sont reliés par un isomorphisme déterminé à conjugaison près.*

(iii) *Soit un carré commutatif*

$$\begin{tikzcd} \overline{s}' \arrow[r] \arrow[d] & \overline{s} \arrow[d] \\ S' \arrow[r] & S \end{tikzcd}$$

où S et S' sont des schémas localement nœthériens connexes, et $\overline{s}$ et $\overline{s}'$ des points géométriques de ces schémas.

Alors le foncteur

$$\begin{array}{rcl} \mathrm{Rev}_S & \to & \mathrm{Rev}_{S'} \\ X & \mapsto & X \times_S S' \end{array}$$

correspond à un unique homomorphisme continu

$$\pi_1(S', \overline{s}') \to \pi_1(S, \overline{s}) \,.$$

Remarque :

Dans la situation de (i), le degré d'un revêtement étale X est égal au cardinal de $X(\overline{s})$.

L'action de $\pi_1(S, \overline{s})$ sur $X(\overline{s})$ est transitive si et seulement si X est connexe.

Dans ce cas, on a donc

$$\# \operatorname{Aut}_S(X) \leq \# X(\overline{s}) = \deg_S(X)$$

et il y a égalité si et seulement si les fixateurs des éléments $\overline{s}'$ de $X(\overline{s})$ sont tous égaux et sont donc un sous-groupe ouvert distingué de $\pi_1(S, \overline{s})$ isomorphe aux $\pi_1(X, \overline{s}')$.

Alors on a

$$\operatorname{Aut}_S(X) = \pi_1(S, \overline{s}) / \pi_1(X, \overline{s}')$$

et on dit que X est un revêtement fini étale "galoisien" de S.

Exemples :

(i) Si $S = \mathrm{Spec}\,(K)$ est le spectre d'un corps K et $\overline{K}$ est une clôture algébrique de K considérée comme un point géométrique $\mathrm{Spec}\,(\overline{K}) \xrightarrow{\overline{s}} S$ de S, alors

$$\pi_1(S, \overline{s})$$

s'identifie au groupe des automorphismes du corps $\overline{K}$ qui laissent invariants les éléments de K. C'est le groupe de Galois Γ_K de K (qui dépend du choix de $\overline{K}$).
La topologie de Γ_K est caractérisée par le fait que ses sous-groupes ouverts sont les fixateurs des éléments des sous-corps de $\overline{K}$ de dimension finie sur K.

(ii) Si S est un schéma localement nœthérien connexe sur un corps K et $\overline{s} : \mathrm{Spec}(\overline{K}) \to S$ est un point géométrique de S à valeurs dans une clôture algébrique $\overline{K}$ de K, le morphisme de projection de S sur sa base

$$S \to \mathrm{Spec}\,(K)$$

induit un morphisme continu de groupes profinis

$$\pi_1(S, \overline{s}) \to \Gamma_K\,.$$

De plus, tout "point rationnel" de S c'est-à-dire tout point $\mathrm{Spec}\,(K) \to S$ de S à valeurs dans K définit une section

$$\Gamma_K \to \pi_1(S, \overline{s})$$

du morphisme

$$\pi_1(S, \overline{s}) \to \Gamma_K\,.$$

On peut se demander s'il existe des types de variétés S sur un corps K pour lesquelles il y aurait automatiquement bijection entre l'ensemble des points de S à valeurs dans K et celui des sections $\Gamma_K \to \pi_1(S, \overline{s})$ de $\pi_1(S, \overline{s}) \to \Gamma_K$.

$\square$

Le corollaire II.20 se reformule maintenant de la manière suivante :

Corollaire II.29. –

Soit A un anneau local d'idéal maximal m et de corps résiduel κ, et soit $\overline{\kappa}$ une clôture algébrique de κ considérée comme un point géométrique $\overline{s}$ de $\mathrm{Spec}\,(\kappa)$ *ou* $\mathrm{Spec}\,(A)$*.*

Alors :

(i) *Si A est artinien, c'est-à-dire si son idéal maximal m est nilpotent, l'homomorphisme*

$$\Gamma_\kappa = \mathrm{Aut}_\kappa(\overline{\kappa}) \to \pi_1(\mathrm{Spec}\,(A), \overline{s})$$

est un isomorphisme.

(ii) *En notant toujours $\widehat{A} = \varprojlim_n A/m^n$, l'homomorphisme*

$$\Gamma_\kappa \to \pi_1(\mathrm{Spec}\,(\widehat{A}), \overline{s})$$

est un isomorphisme. $\square$

Terminons ce paragraphe par le résultat important suivant :

Proposition II.30. –

Soit S un schéma de type fini sur un corps K, et soit $\overline{s} : \mathrm{Spec}\,(\overline{K}) \to S$ un point géométrique de S à valeurs dans une clôture algébrique $\overline{K}$ de K.

Alors, si S est "géométriquement connexe", c'est-à-dire si $\overline{S} = S \times_{\mathrm{Spec}(K)} \mathrm{Spec}\,(\overline{K})$ est connexe, on a une suite exacte de groupes profinis

$$1 \to \pi_1(\overline{S}, \overline{s}) \to \pi_1(S, \overline{s}) \to \pi_1(\mathrm{Spec}\,(K), \overline{s}) \to 1\,.$$

Démonstration :

(i) Le composé
$$\pi_1(\overline{S}, \overline{s}) \to \pi_1(S, \overline{s}) \to \pi_1(\mathrm{Spec}\,(K), \overline{s})$$
est trivial car il se factorise à travers
$$\pi_1(\mathrm{Spec}\,(\overline{K}), \overline{s})$$
qui est trivial.

(ii) Montrons que $\pi_1(S, \overline{s}) \to \pi_1(\mathrm{Spec}\,(K), \overline{s}) = \Gamma_K$ est surjectif.
Il suffit de prouver que pour toute extension finie séparable non triviale $K' \subset \overline{K}$ de K, $S \times_{\mathrm{Spec}(K)} \mathrm{Spec}\,(K')$ est un revêtement étale non trivial de S. C'est évident puisqu'il est connexe.

(iii) Soit $\overline{K}_s \subset \overline{K}$ la clôture séparable de K dans $\overline{K}$, c'est-à-dire la réunion filtrante des extensions finies non ramifiées $K' \subset \overline{K}$ de K. Notons $\overline{S}_s = S \times_{\mathrm{Spec}(K)} \mathrm{Spec}\,(\overline{K}_s)$.

Montrons que l'homomorphisme
$$\pi_1(\overline{S}, \overline{s}) \to \pi_1(\overline{S}_s, \overline{s})$$
est un isomorphisme.

Cela résulte du lemme suivant :

Lemme II.31. –

Soient S et S' deux schémas localement nœthériens reliés par un morphisme affine, universellement bijectif et plat (donc fidèlement plat)
$$S' \to S\,.$$
Alors le foncteur
$$\mathrm{Rev}_S \to \mathrm{Rev}_{S'} : X \mapsto X \times_S S'$$
est une équivalence de catégories.

Démonstration du lemme :

On peut supposer que $S = \mathrm{Spec}\,(A)$ et $S' = \mathrm{Spec}\,(A')$ sont affines et nœthériens.

Soit $X' = \mathrm{Spec}\,(B')$ un revêtement étale de S'.

Soit $X = \mathrm{Spec}\,(B)$ où B est la A-algèbre définie comme le noyau de la différence des deux morphismes
$$B' \rightrightarrows B' \otimes_A B'\,.$$
Montrons que l'homomorphisme
$$B \otimes_A A' \to B'$$
est un isomorphisme.

D'après le lemme II.22, et quitte à faire un changement de base $S_1 \to S$ fidèlement plat, on peut supposer que X' est une somme finie de copies de S'.

Comme $S' \to S$ est universellement bijectif, on est ramené au lemme suivant :

Lemme II.32. –

Si $A \to A'$ est un morphisme fidèlement plat d'anneaux, A s'identifie à l'égalisateur des deux morphismes

$$A' \rightrightarrows A' \otimes_A A' .$$

Démonstration :

$A \to A'$ est injectif car, pour tout idéal non nul I de A, $I \otimes_A A' = I \cdot A'$ est nécessairement non nul.

Alors tout élément de l'égalisateur de $A' \rightrightarrows A' \otimes_A A'$ est dans A car A est le noyau de $A' \to A'/A$ composé avec le morphisme injectif $A'/A \to (A'/A) \otimes_A A'$.

□

Suite de la démonstration de la proposition II.30.

(iv) Montrons que $\pi_1(\overline{S}_s, \overline{s}) \to \pi_1(S, \overline{s})$ est injectif.
Il suffit de prouver que si X_s est un revêtement étale de $\overline{S}_s = S \otimes_{\mathrm{Spec}(K)} \mathrm{Spec}\,(\overline{K}_s)$, il existe un revêtement étale X de S tel que X_s se plonge dans $X \times_S \overline{S}_s$.
Comme $\overline{S}_s$ est de type fini sur $\overline{K}_s$, il existe une extension finie séparable $K' \subset \overline{K}_s$ de K et un revêtement étale X' de $S \times_{\mathrm{Spec}(K)} \mathrm{Spec}\,(K')$ tel que $X_s \cong X' \times_{\mathrm{Spec}(K')} \mathrm{Spec}\,(\overline{K}_s)$.
Alors $X' \to S \times_{\mathrm{Spec}(K)} \mathrm{Spec}\,(K') \to S$ peut être considéré comme un revêtement étale de S, noté X, et $X_s = X' \times_{\mathrm{Spec}(K')} \mathrm{Spec}\,(\overline{K}_s)$ se plonge dans

$$X \times_{\mathrm{Spec}(K)} \mathrm{Spec}\,(\overline{K}_s) \cong X' \times_{\mathrm{Spec}(K)} \mathrm{Spec}\,(\overline{K}_s)$$

par l'immersion ouverte déduite par changement de base de

$$\mathrm{Spec}\,(K') \to \mathrm{Spec}\,(K') \times_{\mathrm{Spec}(K)} \mathrm{Spec}\,(K') .$$

(v) Montrons enfin que la suite

$$\pi_1(\overline{S}_s, \overline{s}) \to \pi_1(S, \overline{s}) \to \pi_1(\mathrm{Spec}\,(K), \overline{s})$$

est exacte.
Il s'agit de prouver que tout revêtement étale X de S qui est trivial sur $\overline{S}_s$ provient d'un revêtement étale de $\mathrm{Spec}\,(K)$.
On peut écrire

$$X \times_{\mathrm{Spec}(K)} \mathrm{Spec}\,(\overline{K}_s) \cong \coprod_{i \in I} \overline{S}_s$$

pour un certain ensemble fini I.
Alors tout automorphisme de $\overline{K}_s$ définit une bijection de I, et le groupe de Galois $\Gamma_K = \mathrm{Aut}_K(\overline{K}) = \mathrm{Aut}_K(\overline{K}_s)$ agit sur I. Cette action est continue car elle est triviale sur toute extension finie galoisienne $K' \subset \overline{K}_s$ sur laquelle le revêtement $X \times_{\mathrm{Spec}(K)} \mathrm{Spec}\,(K')$ est trivial.
Donc I muni de l'action de Γ_K définit une extension finie séparable K'' de K.
De plus, $X \times_{\mathrm{Spec}(K)} \mathrm{Spec}\,(K')$ et $(S \times_{\mathrm{Spec}(K)} \mathrm{Spec}\,(K'')) \times_{\mathrm{Spec}\,(K)} \mathrm{Spec}\,(K')$ sont isomorphes et l'isomorphisme entre eux est respecté par l'action du groupe de Galois fini $\mathrm{Aut}_K(K')$.
Donc X est isomorphe à $S \times_{\mathrm{Spec}(K)} \mathrm{Spec}\,(K'')$, comme voulu. □

On a d'autre part le lemme général :

Lemme II.33. –

Pour toute suite exacte de groupes (finis, profinis, ...)

$$1 \to G' \to G \to G'' \to 1\,,$$

on a un homomorphisme induit

$$G'' \to \mathrm{Ext}\,(G')$$

où $\mathrm{Ext}\,(G') = \mathrm{Aut}\,(G')/\mathrm{Int}\,(G')$ *désigne le quotient du groupe*

$$\mathrm{Aut}\,(G')$$

des automorphismes de G' par le sous-groupe distingué

$$\mathrm{Int}\,(G')$$

des automorphismes de conjugaison par les éléments de G'.

Démonstration :

En effet, tout élément g de G définit par conjugaison un automorphisme de G qui stabilise G', et dont l'image dans

$$\mathrm{Ext}\,(G') = \mathrm{Aut}\,(G')/\mathrm{Int}\,(G')$$

ne dépend que de l'image de g dans G''. □

On déduit de la proposition et de ce lemme :

Corollaire II.34. –

Soit S un schéma de type fini sur un corps K de clôture algébrique $\overline{K}$, et soit $\overline{s} \in S(\overline{K})$.

Alors, si $\overline{S} = S \times_{\mathrm{Spec}(K)} \mathrm{Spec}\,(\overline{K})$ est connexe, on a un homomorphisme naturel

$$\Gamma_K = \pi_1(\mathrm{Spec}(K), \overline{s}) \to \mathrm{Ext}\,(\pi_1(\overline{S}, \overline{s}))\,.$$

Remarque :

Cela s'applique en particulier à $K = \mathbb{Q}$.

On peut se demander s'il existe une variété S sur $\mathbb{Q}$, géométriquement connexe, et telle que

$$\Gamma_{\mathbb{Q}} \to \mathrm{Ext}\,\big(\pi_1(S \times_{\mathrm{Spec}(\mathbb{Q})} \mathrm{Spec}\,(\overline{\mathbb{Q}}), \overline{s})\big)$$

soit un isomorphisme ... □

III. Géométrie en dimension 1

1 Courbes sur un corps

Définition III.1. –

On appelle courbe sur un corps K tout schéma de type fini et séparé sur K dont la dimension de tout ouvert est égale à 1.

Remarques :

(i) La droite affine $\mathbb{A}^1_K = \mathrm{Spec}\,(K[X])$ et la droite projective $\mathbb{P}^1_K$ sont des courbes sur K.

(ii) Tout ouvert d'une courbe sur K est une courbe sur K.

(iii) Si X est une courbe sur K, tout schéma fini et plat sur X est une courbe sur K. En particulier, tout revêtement (fini) étale de X est une courbe sur X.

□

On appelle "lisses" les courbes sur K qui ont les mêmes propriétés locales que la droite affine $\mathbb{A}^1_K$. Voici la définition précise :

Définition III.2. –

Une courbe X sur K est dite lisse si tout point $x \in X$ possède un voisinage ouvert U qui admet un morphisme étale

$$U \to \mathbb{A}^1_K \,.$$

Remarque :

Plus généralement, un morphisme de schémas

$$X \to S$$

est dit "lisse de dimension relative d" si tout point $x \in X$ admet un voisinage ouvert U qui s'envoie dans un ouvert affine $V = \mathrm{Spec}\,(A)$ de S et tel que le morphisme $U \to V$ se factorise à travers un morphisme étale

$$U \to \mathbb{A}^d_A = \mathrm{Spec}\,(A\,[T_1, \dots, T_d])\,.$$

□

Les propriétés locales des courbes lisses sur K sont formalisées grâce à la notion d'anneau de valuation discrète :

Lemme III.3. –

Soit A un anneau local nœthérien dont l'idéal maximal m_A est engendré par un élément ϖ_A.

Les propriétés suivantes sont équivalentes :

(i) *A est intègre et ϖ_A n'est pas nul.*
(ii) *Pour tout $a \in A$, on a $\varpi_A \cdot a = 0 \Rightarrow a = 0$.*
(iii) *ϖ_A n'est pas nilpotent.*
(iv) *Tout élément $a \neq 0$ de A s'écrit de manière unique sous la forme*

$$a = a' \cdot \varpi_A^k \qquad \textit{avec} \qquad a' \in A^\times \quad \textit{et} \quad k \in \mathbb{N}\,.$$

En particulier, les idéaux non nuls de A sont les m_A^n, $n \geq 1$.

Démonstration :

Il est évident que (i) $\Rightarrow$ (ii), (ii) $\Rightarrow$ (iii) et (iv) $\Rightarrow$ (i).

Reste à prouver que (iii) $\Rightarrow$ (iv).

Si ϖ_A n'est pas nilpotent, chaque m_A^n/m_A^{n+1}, $n \geq 0$, est un espace vectoriel de dimension 1 sur le corps résiduel $\kappa_A = A/m_A$ si bien que l'anneau

$$\bigoplus_{n \geq 0} m_A^n/m_A^{n+1}$$

s'identifie à $\kappa_A[T]$ par $T \leftrightarrow \varpi_A$.

Pour conclure, il reste seulement à montrer que l'idéal $I = \bigcap\limits_{n \geq 0} m_A^n$ est 0. Cela résulte de ce que A est nœthérien.

En effet, considérons l'anneau

$$A^* = \bigoplus_{n \geq 0} m_A^n\,.$$

Il est engendré sur A par ϖ_A placé en degré 1, donc il est nœthérien. Il contient l'idéal

$$I \oplus I \oplus \ldots \oplus I \oplus \ldots$$

qui est la réunion filtrante des idéaux

$$(I \oplus I \oplus \ldots \oplus I) \oplus (m_A\, I \oplus m_A\, I \oplus \ldots \oplus m_A\, I \oplus \ldots)\,.$$

Donc on a $I = m_A \cdot I$ puis $I = 0$ d'après le lemme I.34 de Nakayama. □

Définition III.4. –

Un anneau local (A, m_A) qui vérifie les conditions du lemme III.3 *ci-dessus est appelé un anneau de valuation discrète.*

Si F est le corps des fractions de A, la "valuation" de A est l'unique homomorphisme

$$v_A : F^\times \to \mathbb{Z}$$

tel que

- *$v_A(f) = 0 \Leftrightarrow f \in A^\times$,*
- *$v_A(f) = 1 \Leftrightarrow f$ engendre l'idéal maximal m_A de A,*
- *$v_A(f) \geq 0 \Leftrightarrow f \in A$,*
- *$v_A(f) \geq 1 \Leftrightarrow f \in m_A$.*

Remarques :

(i) Un anneau de valuation discrète est de dimension 1.

(ii) Tout générateur ϖ_A de l'idéal maximal m_A est appelé une "uniformisante" de l'anneau de valuation discrète A.

(iii) Pour tous $f, f' \in F^\times$, on a $v_A(f+f') \geq \inf(v_A(f), v_A(f'))$ si $f + f' \neq 0$.

$\square$

On a :

Lemme III.5. –

Si X est une courbe lisse sur K, alors l'anneau local $\mathcal{O}_x = \mathcal{O}_{x,X}$ de X en tout point fermé x de X est un anneau de valuation discrète.

Démonstration :

C'est vrai si $X = \operatorname{Spec}(K[T])$ car l'anneau $K[T]$ est intègre et tous ses idéaux sont engendrés par un élément.

La conclusion résulte de la partie (i) du lemme suivant :

Lemme III.6. –

Soient (A, m_A) un anneau de valuation discrète, (B, m_B) un anneau local et $u : A \to B$ un morphisme non ramifié tel que

$$u^{-1}(m_B) = m_A \,.$$

Alors m_A engendre m_B et :

(i) *B est un anneau de valuation discrète si u est plat (donc étale).*

(ii) *L'hypothèse de* (i) *est vérifiée si B est de dimension* 1.

Démonstration :

Le produit tensoriel $B \otimes_A A/m_A$ est non ramifié sur le corps A/m_A. Comme c'est un anneau local, c'est un corps (extension finie séparable de A/m_A). Cela signifie que n'importe quelle uniformisante ϖ_A de m_A engendre aussi l'idéal m_B de B.

(i) Si B est plat sur A, la multiplication par ϖ_A, qui est injective dans A, le reste dans B.

(ii) Si B est de dimension 1, l'uniformisante ϖ_A ne peut être nilpotente dans B, donc B est un anneau de valuation discrète.

En particulier, B est intègre. D'après le lemme II.6(ii), il est plat sur A puisque sans A-torsion. $\square$

Nous allons caractériser les anneaux de valuation discrète à l'aide des notions suivantes :

Définition III.7. –

Soit A un sous-anneau d'un corps F.

Un élément $x \in F$ est dit "entier sur A" s'il existe des éléments $a_0, a_1, \ldots, a_{d-1} \in A$ tels que

$$x^d = a_0 + a_1 \cdot x + \ldots + a_{d-1} \cdot x^{d-1} \,.$$

Remarque :

Un élément $x \in F$ est entier sur A si et seulement si le sous-anneau $A[x]$ de F engendré sur A par x est de type fini comme A-module.

$\square$

Définition III.8. –

(i) *Un anneau A est dit "normal" s'il est intègre, donc plongé dans son corps des fractions F, et si tout élément de F qui est entier sur A appartient à A.*

(ii) *Un schéma X est dit localement normal s'il est réunion d'ouverts affines* Spec (A) *associés à des anneaux normaux A.*

$\square$

On remarque aussitôt :

Lemme III.9. –

(i) *Si un anneau A est normal, il en est de même de tous ses localisés.*

(ii) *Réciproquement, un anneau intègre A est normal s'il en est ainsi de tous ses anneaux locaux A_p en les idéaux premiers $p \in \operatorname{Spec}(A)$.*

(iii) *Un schéma X est localement normal si et seulement si tous ses anneaux locaux $\mathcal{O}_{x,X}$, $x \in X$, sont normaux.*

Démonstration :

(i) est évident sur la définition.

(ii) Si F est le corps des fractions de A, on a dans F

$$A = \bigcap_{p \in \operatorname{Spec}(A)} A_p \, .$$

Or toute intersection d'anneaux normaux est normale.

(iii) résulte de (ii).

$\square$

Montrons maintenant :

Proposition III.10. –

Un anneau local nœthérien (A, m_A) de dimension 1 est un anneau de valuation discrète si et seulement si il est normal.

Démonstration :

Supposons que A est un anneau de valuation discrète, et notons v_A sa valuation.

Soit x un élément non nul de $F = \operatorname{Frac}(A)$ qui est entier sur A, c'est-à-dire solution d'une équation de la forme

$$x^d = a_0 + a_1 \cdot x + \ldots + a_{d-1} \cdot x^{d-1} \quad \text{avec} \quad a_0, a_1, \ldots, a_{d-1} \in A \, .$$

On déduit de la remarque (iii) qui suit la définition III.4

$$d \cdot v_A(x) \geq \inf \{0, v_A(x), \ldots, (d-1) \cdot v_A(x)\}$$

et donc $v_A(x) \geq 0$ soit $x \in A$ comme voulu.

Réciproquement, supposons que A est normal.

Soit a un élément non nul de m_A.

L'anneau quotient $A/(a)$ a un seul idéal premier, qui est $m_A/(a)$, donc tout élément de m_A est nilpotent dans $A/(a)$ et on a
$$m_A^a \subset (a) \quad \text{si } n \text{ est assez grand.}$$
Choisissons $n \geq 1$ de façon que
$$m_A^n \subset (a) \qquad \text{et} \qquad m_A^{n-1} \not\subset (a)\,.$$
Soit b un élément de m_A^{n-1} qui n'est pas dans (a) et $x = ab^{-1} \in F = \mathrm{Frac}\,(A)$. On a $x^{-1} \notin A$ donc, par hypothèse, x^{-1} n'est pas entier sur A. Comme A est nœthérien, cela rend impossible que $x^{-1} \cdot m_A \subset m_A$. Mais on a $m_A^n \subset (a)$ et $b \in m_A^{n-1}$ d'où l'on tire
$$x^{-1} \cdot m_A \subset A\,.$$
On conclut que $x^{-1} \cdot m_A = A$ soit $m_A = (x)$ comme voulu. □

On peut maintenant donner la double caractérisation suivante des courbes lisses sur un corps K :

Théorème III.11. –

Soit X une courbe sur un corps K.

(i) *X est lisse sur K si et seulement si le $\mathcal{O}_X$-$\mathcal{M}$odule cohérent $\Omega_{X/K}$ est localement libre de rang 1.*

(ii) *Si X est lisse, X est localement normale. La réciproque est vraie si le corps de base K est parfait (c'es-à-dire si toute extension finie de K est séparable).*

Remarques :

(i) Tout corps fini est parfait.

(ii) Plus généralement, un schéma localement de type fini sur S et dont tout ouvert est de dimension d est lisse sur K si et seulement si le $\mathcal{O}_X$-$\mathcal{M}$odule cohérent $\Omega_{X/K}$ est localement libre de rang d. De plus, il reste vrai qu'un tel schéma lisse est normal (mais la réciproque est fausse même sur un corps parfait en les dimensions ≥ 2).

Démonstration :

Toutes les questions sont locales donc on peut supposer que $X = \mathrm{Spec}\,(A)$.

(i) Supposons que X est étale sur $Y = \mathrm{Spec}\,(K[T])$ et notons $Z = \mathrm{Spec}\,(K)$.
Alors le morphisme diagonal
$$X \to X \times_Z X$$
est le composé de l'immersion ouverte
$$X \to X \times_Y X$$
et du morphisme
$$X \times_Y X \to X \times_Z X$$
qui se déduit par changement de base plat de
$$Y \to Y \times_Z Y\,.$$
Comme $\Omega^1_{K[T]/K}$ est libre de rang 1 sur $K[T]$, on conclut que $\Omega^1_{A/K}$ est libre de rang 1 sur A.
Réciproquement, supposons que $\Omega^1_{A/K}$ soit libre de rang 1 au voisinage d'un point x. Quitte à remplacer $\mathrm{Spec}\,(A)$ par un voisinage affine plus petit de x, on peut supposer que $\Omega^1_{A/K}$ est engendré par la différentielle da d'un élément $a \in A$.

Cet élément a définit un morphisme de K-algèbres

$$K[T] \to A$$

soit

$$X = \mathrm{Spec}\,(A) \to Y = \mathrm{Spec}\,(K[T])\,.$$

La suite exacte

$$\Omega^1_{K[T]/K} \otimes_{K[T]} A \to \Omega^1_{A/K} \to \Omega^1_{A/K[T]} \to 0$$

montre que $\Omega^1_{A/K[T]} = 0$. Autrement dit, $X = \mathrm{Spec}\,(A)$ est non ramifié sur $Y = \mathrm{Spec}\,(K[T])$. On conclut d'après le lemme III.6(ii).

(ii) Si X est lisse sur K, elle est localement normale d'après le lemme III.5 et la proposition III.10.
Réciproquement, supposons que X est localement normale et K parfait.
Soit x un point fermé de X, κ_x son corps résiduel qui est une extension finie de K, et ϖ_x une uniformisante de l'anneau local $\mathcal{O}_{x,X}$.
Alors ϖ_x définit au voisinage de x un morphisme

$$X = \mathrm{Spec}\,(A) \to \mathrm{Spec}\,(K[T]) = Y\,.$$

La fibre $\Omega^1_{A/K[T]} \otimes_A \kappa_x$ s'identifie à $\Omega^1_{\kappa_x/K}$ qui est nul puisque, K étant parfait, l'extension κ_x de K est non ramifiée. D'après le lemme I.34 de Nakayama, $\Omega^1_{A/K[T]}$ est donc nul au voisinage de x et $X \to Y$ est non ramifié dans ce voisinage, donc étale d'après le lemme III.6(ii).

$\square$

Nous allons maintenant étudier les morphismes entre courbes. On a d'abord :

Lemme III.12. –

Soient X et X' deux schémas sur un schéma de base S.

On suppose que X est nœthérien localement normal et de dimension 1 et que X' est propre sur S.

Alors tout morphisme

$$U \to X'$$

défini sur un ouvert dense U de X se prolonge de manière unique en un morphisme

$$X \to X'\,.$$

Démonstration :

Soit X'' l'adhérence schématique de U dans $X \times_S X'$, c'est-à-dire le plus petit sous-schéma fermé de $X \times_S X'$ qui contient U. Ainsi X'' contient U comme ouvert dense.

On a deux morphismes de projection

$$X'' \to X\,, \quad X'' \to X'$$

dont le premier

$$X'' \to X$$

est propre et se réduit au-dessus de $U \subset X$ à un isomorphisme.

Soit x un point fermé arbitraire de X et $\mathcal{O}_{x,X}$ son anneau local qui est un anneau de valuation discrète.

Comme $X'' \to X$ est propre, son image est un fermé de X qui, contenant U, est X tout entier.

Soit alors y un point de X'' au-dessus de x et $\mathcal{O}_{y,X''}$ son anneau local.

Alors $\mathcal{O}_{x,X}$ et $\mathcal{O}_{y,X''}$ ont le même corps des fractions et $\mathcal{O}_{y,X''}$ contient $\mathcal{O}_{x,X}$. Comme $\mathcal{O}_{x,X}$ est un anneau de valuation discrète, cela impose

$$\mathcal{O}_{x,X} = \mathcal{O}_{y,X''} .$$

Comme X'' est séparé sur X, on en déduit encore qu'il y a un unique point y de X'' au-dessus de chaque point x de X, puis que

$$X'' \to X$$

est un isomorphisme.

Cela conclut la démonstration. □

Ce lemme s'applique en particulier aux courbes.

Rappelons qu'un schéma X est dit intègre [resp. normal] s'il est connexe et réunion d'ouverts affines $\mathrm{Spec}\,(A)$ associés à des anneaux intègres [resp. normaux] A.

Si un schéma X est intègre, il est l'adhérence d'un unique point appelé son point générique. Le corps résiduel en ce point – qui s'identifie au corps des fractions $\mathrm{Frac}\,(A)$ de l'anneau A de tout ouvert affine $\mathrm{Spec}\,(A)$ de X – peut être appelé le corps des fonctions (rationnelles) de X et noté F_X.

On déduit du lemme III.12 ci-dessus :

Corollaire III.13. –

Soient X et X' deux courbes sur un corps K.

On suppose que X est normale et que X' est intègre et propre sur K.

Alors se donner un morphisme

$$X \to X'$$

dont l'image n'est pas concentrée en un point équivaut à se donner un morphisme de corps

$$F_{X'} \to F_X .$$

□

Montrons maintenant :

Proposition III.14. –

Soit K un corps de base, et soit F un corps qui est une extension finie séparable de $K(T)$.

Alors il existe une courbe X_F normale (donc lisse si K est parfait) et propre sur K, unique à unique isomorphisme près, dont le corps des fonctions s'identifie à F.

Démonstration :

L'unicité résulte du corollaire III.13 ci-dessus.

L'existence va résulter du lemme suivant :

Lemme III.15. –

(i) *Soient F un corps et A un sous-anneau nœthérien de F.*
Alors l'ensemble $A' \supset A$ des éléments de F qui sont "entiers sur A" (au sens de la définition III.7*) est un sous-anneau appelé le normalisé de A dans F.*

(ii) *Soient A un anneau normal nœthérien, F son corps des fractions et F' un corps extension finie séparable de F.*
Alors le normalisé A' de A dans F' est fini sur A (c'est-à-dire de type fini comme A-module).

Démonstration :

(i) Si x et y sont deux éléments de F entiers sur A, les anneaux $A[x]$ et $A[y]$ qu'ils engendrent sont des A-modules de type fini, donc aussi $A[x,y]$. Comme celui-ci contient $A[x+y]$ et $A[xy]$ et que A est nœthérien, on conclut que $x+y$ et xy sont aussi entiers sur A.

Pour (ii), démontrons d'abord :

Lemme III.16. –

Soit $F \subset F'$ une extension finie séparable de corps.

Associons à tout élément $x \in F'$ sa trace $\mathrm{Tr}\,(x) \in F$ comme endomorphisme $x' \mapsto xx'$ de F' vu comme espace vectoriel sur F.

Alors :

(i) *La forme F-bilinéaire symétrique sur F'*

$$(x_1, x_2) \mapsto \mathrm{Tr}\,(x_1\, x_2)$$

est non dégénérée.

(ii) *Si A est un anneau normal dont le corps des fractions est F, et A' désigne la normalisation de A dans F', on a*

$$\mathrm{Tr}\,(x) \in A\,, \qquad \forall\, x \in A'\,.$$

Démonstration :

Soit $K \supset F$ un corps tel que $K \otimes_F F' \cong K^d$.

(i) Pour prouver que le forme bilinéaire associée à $\mathrm{Tr} : F' \to F$ est non dégénérée, il suffit de prouver que celle associée à

$$\mathrm{Tr} : K \otimes_F F' \to K$$

est non dégénérée. C'est évident puisque $K \otimes_F F' \cong K^d$.

(ii) Soit x un élément de A', solution d'une équation

$$P(x) = x^k + a_{k-1} \cdot x^{k-1} + \ldots + a_1 \cdot x + a_0 = 0$$

à coefficients $a_{k-1}, \ldots, a_1, a_0 \in A$.

L'image de x dans $K \otimes_F F' \cong K^d$ s'écrit $x = (x_1, \ldots, x_d)$ où chaque x_i, $1 \leq i \leq d$, est solution de la même équation

$$P(x_i) = 0\,.$$

Donc $\mathrm{Tr}\,(x) = x_1 + \ldots + x_d$ est aussi entier sur A, et il est élément de A puisqu'il est dans F et que A est normal.

□

Fin de la démonstration du lemme III.15(ii) :

On peut facilement trouver dans F' des vecteurs de base $x_1, \ldots, x_d$ sur F qui sont entiers sur A. Comme la forme bilinéaire

$$(x, x') \mapsto \mathrm{Tr}\,(x\, x')$$

est non dégénérée, il existe dans F' une base duale $x_1^*, \ldots, x_d^*$.

Or, pour tout élément $x \in A'$ et tout indice i, $1 \leq i \leq d$, on a

$$\mathrm{Tr}\,(x\, x_i) \in A\,.$$

Par conséquent, A' est contenu dans le A-module engendré par $x_1^*, \dots, x_d^*$. Comme A est nœthérien, c'est un A-module de type fini.

$\square$

Fin de la démonstration de la proposition III.14 :

Considérons l'extension finie séparable

$$F \supset K(T)\,.$$

Le corps $K(T)$ peut être interprété comme le corps des fonctions de la droite projective $\mathbb{P}^1_K$ sur K, qui est une courbe lisse et propre sur K.

Pour tout ouvert affine $\mathrm{Spec}\,(A)$ de $\mathbb{P}^1_K$, on peut considérer le normalisé A' de A dans F puis le schéma associé $\mathrm{Spec}\,(A')$ qui est fini sur $\mathrm{Spec}\,(A)$.

La formation des $\mathrm{Spec}\,(A')$ à partir de $\mathrm{Spec}\,(A)$ commute aux localisations, donc ils se recollent et définissent un schéma X' sur K muni d'un morphisme fini

$$X' \to X$$

et donc propre sur K.

Par construction, X' est une courbe normale et son corps des fonctions s'identifie à F. $\square$

Terminons ce paragraphe en décrivant les morphismes entre courbes normales propres :

Proposition III.17. –

Soient X, X' deux courbes normales et propres sur un corps K, reliées par un morphisme

$$\alpha : X' \to X$$

dont l'image n'est pas concentrée en un point.

Alors :

(i) *Ce morphisme est fini.*

(ii) *La $\mathcal{O}_X$-Algèbre $\alpha_*(\mathcal{O}_{X'})$ est un $\mathcal{O}_X$-$\mathcal{M}$odule localement libre d'un certain degré d égal à celui de l'extension*

$$F_X \subset F_{X'}\,.$$

(iii) *Pour tout point fermé x de X, on peut écrire*

$$d = \sum_{x' \mapsto x} e_{x'} \cdot f_{x'}$$

où

- *x' décrit l'ensemble fini des points de X' au-dessus de x,*
- *$e_{x'}$ désigne le degré de l'extension résiduelle $\kappa_x \subset \kappa_{x'}$,*
- *$f_{x'}$ désigne la valuation dans $\mathcal{O}_{x',X'}$ de n'importe quelle uniformisante de $\mathcal{O}_{x,X}$.*

(iv) *Pour tout point fermé x' de X', le morphisme $X' \to X$ est non ramifié, donc étale, au voisinage de x', si et seulement si*

- *$f_{x'} = 1$,*
- *l'extension $\kappa_x \subset \kappa_{x'}$ est non ramifiée.*

Remarques :

(i) Si le corps K est fini (ou plus généralement parfait), les extensions $\kappa_x \subset \kappa_{x'}$ sont toujours non ramifiées, si bien que $X' \to X$ est étale au voisinage de x' si et seulement si $f_{x'} = 1$.

(ii) On appelle indice de ramification de $X' \xrightarrow{\alpha} X$ au point x' le produit de $f_{x'}$ et du degré de $\kappa_{x'}$ sur la plus grande extension séparable de κ_x qu'il contient. Si K est parfait, l'indice de ramification de α en x' est $f_{x'}$.

Démonstration :

(i) Comme $\alpha : X' \to X$ est un morphisme propre, la $\mathcal{O}_X$-$\mathcal{A}$lgèbre $\alpha_*(\mathcal{O}_{X'})$ est un $\mathcal{O}_X$-$\mathcal{M}$odule cohérent. Pour tout ouvert U de X, $\alpha_*(\mathcal{O}_{X'})(U) = \mathcal{O}_{X'}(\alpha^{-1}(U))$ est l'intersection dans le corps de fonctions $F_{X'}$ de X' des anneaux de valuation discrète $\mathcal{O}_{x',X'}$ des points fermés $x' \in \alpha^{-1}(U)$. Il en résulte que tous les anneaux $\alpha_*(\mathcal{O}_{X'})(U)$ sont intègres, et même normaux, et que leur corps des fractions est

$$\varinjlim_U \alpha_*(\mathcal{O}_{X'})(U) = \varinjlim_U \mathcal{O}_{X'}(\alpha^{-1}(U)) = F_{X'} \,.$$

La $\mathcal{O}_X$-$\mathcal{A}$lgèbre finie $\alpha_*(\mathcal{O}_{X'})$ définit donc un schéma normal X'', fini sur X donc propre sur X et sur $\mathrm{Spec}\,(K)$, et dont le corps des fonctions s'identifie à $F_{X'}$.

D'après la proposition III.14, X'' s'identifie à X'.

(ii) La $\mathcal{O}_X$-$\mathcal{A}$lgèbre finie $\alpha_*(\mathcal{O}_{X'})$ est sans torsion, donc plate d'après le lemme II.6(ii), donc localement libre d'un certain rang $d \geq 1$ d'après le lemme II.7(i).

(iii) Pour tout point fermé x de X, le schéma $X' \times_X \mathrm{Spec}\,(\kappa_x)$ est fini sur κ_x et associé à une κ_x-algèbre de degré d. Or cette κ_x algèbre n'est autre que

$$\bigoplus_{x' \mapsto x} \mathcal{O}_{x',X'} \big/ (\varpi_x) = \bigoplus_{x' \mapsto x} \mathcal{O}_{x',X'} \big/ (\varpi_{x'}^{f_{x'}}) \,,$$

et chaque facteur $\mathcal{O}_{x',X'} \big/ (\varpi_{x'}^{f_{x'}})$ a pour dimension sur κ_x

$$\sum_{1 \leq i \leq f_{x'}} \dim \left(\varpi_{x'}^{i-1} \cdot \mathcal{O}_{x',X'} \big/ \varpi_{x'}^{i} \cdot \mathcal{O}_{x',X'}\right) = \sum_{1 \leq i \leq f_{x'}} \dim \left(\mathcal{O}_{x',X'} / \varpi'_{x'} \cdot \mathcal{O}_{x',X'}\right) = e_{x'} \cdot f_{x'} \,.$$

(iv) D'après le lemme III.6(ii), X' est étale sur X au voisinage d'un point fermé x' si et seulement $X' \to X$ est non ramifié au voisinage de ce point, c'est-à-dire si X' admet un voisinage ouvert affine $\mathrm{Spec}\,(B)$ s'envoyant dans un ouvert affine $\mathrm{Spec}\,(A)$ de X tel que $\Omega^1_{B/A} = 0$. Or, pour de tels voisinages ouverts affines tels que x' soit le seul point de $\mathrm{Spec}\,(B)$ au-dessus de son image $x \in \mathrm{Spec}\,(A) \subset X$, la fibre

$$\Omega^1_{B/A} \otimes_A \kappa_x$$

s'identifie à

$$\Omega^1_{B \otimes_A \kappa_x / \kappa_x} \,.$$

Elle est nulle si et seulement si la κ_x-algèbre finie locale $B \otimes_A \kappa_x$ est une extension non ramifiée de κ_x, avec en particulier $f_{x'} = 1$.

$\square$

2 Corps de nombres et courbes arithmétiques

Il existe une autre famille de schémas de dimension 1 que les courbes sur un corps. Ce sont les "courbes arithmétiques" au sens suivant :

Définition III.18. –

On appellera "courbe arithmétique" tout schéma de type fini, séparé et plat sur $\mathbb{Z}$ (c'est-à-dire sans $\mathbb{Z}$-torsion) dont la dimension de tout ouvert est égale à 1.

Remarques :

(i) Le schéma de base universelle $\mathrm{Spec}\,(\mathbb{Z})$ est une courbe arithmétique.

(ii) Tout ouvert d'une courbe arithmétique est une courbe arithmétique.

(iii) Si X est une courbe arithmétique, tout schéma fini et plat sur X est une courbe arithmétique. En particulier, tout revêtement (fini) étale de X est une courbe arithmétique.

Pour les courbes arithmétiques, l'analogue des courbes lisses sur un corps est la propriété de régularité :

Définition III.19. –

Une courbe arithmétique X est dite "régulière" si l'idéal maximal m_x de l'anneau local $\mathcal{O}_{x,X}$ de tout point fermé $x \in X$ est engendré par un élément.

On déduit du lemme III.3, du lemme III.9 et de la proposition III.10 :

Corollaire III.20. –

(i) *Une courbe arithmétique X est régulière si et seulement si, pour tout point fermé x de X, l'anneau local $\mathcal{O}_{x,X}$ de x dans X est un anneau de valuation discrète.*

(ii) *Une courbe arithmétique X est régulière si et seulement si elle est normale, c'est-à-dire si tout point x possède dans X un voisinage ouvert affine* $\mathrm{Spec}\,(A)$ *dont l'anneau A est normal.*

□

On déduit d'autre part du lemme III.12 :

Corollaire III.21. –

Soient X et X' deux courbes arithmétiques.

On suppose que X est régulière et que X' est propre sur $\mathbb{Z}$.

Alors tout morphisme

$$U \to X'$$

défini sur un ouvert dense U de X se prolonge de manière unique en un morphisme

$$X \to X'\,.$$

□

La courbe arithmétique de base $\mathrm{Spec}\,(\mathbb{Z})$ est régulière et connexe. Son unique point générique est $\mathrm{Spec}\,(\mathbb{Q})$ et ses points fermés $\mathrm{Spec}\,(\mathbb{F}_p) = \mathrm{Spec}\,(\mathbb{Z}/p\,\mathbb{Z})$ sont indexés par les nombres premiers.

Pour toute courbe arithmétique X munie de son morphisme canonique $X \to \mathrm{Spec}\,(\mathbb{Z})$, la fibre de X au-dessus de tout point de $\mathrm{Spec}\,(\mathbb{Z})$ consiste en un ensemble fini de points. Au-dessus de $\mathrm{Spec}\,(\mathbb{Q})$ leurs corps résiduels sont des extensions finies de $\mathbb{Q}$, c'est-à-dire des "corps de nombres", et au-dessus de chaque $\mathrm{Spec}\,(\mathbb{F}_p)$, les corps résiduels de ces points sont des extensions finies de $\mathbb{F}_p$, donc des corps finis.

Lorsqu'une courbe arithmétique X est intègre, en particulier si elle est régulière et connexe, elle a un unique point générique et le corps résiduel en ce point peut être appelé le corps des fonctions (rationnelles) de la courbe X et noté F_X. Ainsi, les corps de fonctions des courbes arithmétiques intègres sont des corps de nombres. En particulier, le corps des fonctions de $\mathrm{Spec}\,(\mathbb{Z})$ est $\mathbb{Q}$.

On déduit du corollaire précédent :

Corollaire III.22. –

Soient X et X' deux courbes arithmétiques.

On suppose que X est régulière et connexe, et que X' est intègre et propre sur $\mathrm{Spec}\,(\mathbb{Z})$.

Alors se donner un morphisme

$$X \to X'$$

équivaut à se donner un morphisme de corps

$$F_{X'} \to F_X \,.$$

□

Montrons maintenant :

Proposition III.23. –

Soit F un corps de nombres, c'est-à-dire une extension finie de $\mathbb{Q}$.

Alors il existe une courbe arithmétique X_F régulière, connexe et propre sur $\mathrm{Spec}\,(\mathbb{Z})$*, unique à unique isomorphisme près, dont le corps des fonctions s'identifie à F.*

De plus, X_F est finie sur $\mathrm{Spec}\,(\mathbb{Z})$*, donc affine.*

Elle est le spectre $\mathrm{Spec}\,(A_F)$ *de l'anneau A_F normalisé de $\mathbb{Z}$ dans F.*

Remarque :

Cet anneau A_F normalisé de $\mathbb{Z}$ dans le corps de nombres F est appelé l'anneau des entiers de F.

Démonstration :

L'unicité résulte du corollaire III.22.

Pour l'existence, il suffit de démontrer que l'anneau A_F normalisé de $\mathbb{Z}$ dans F est fini sur $\mathbb{Z}$.

Cela résulte du lemme III.15(ii) puisque l'extension

$$\mathbb{Q} \subset F$$

est nécessairement séparable. □

Les $X_F = \mathrm{Spec}\,(A_F)$ peuvent être appelées les courbes arithmétiques régulières entières.

Terminons ce paragraphe en décrivant les morphismes entre courbes arithmétiques régulières entières :

Proposition III.24. –

Soient $X = \mathrm{Spec}\,(A_F)$ et $X' = \mathrm{Spec}\,(A_{F'})$ deux courbes arithmétiques régulières et entières, reliées par un morphisme

$$\alpha : X' \to X \,.$$

Alors :

(i) *Ce morphisme est fini.*

(ii) *La $\mathcal{O}_X$-Algèbre $\alpha_*(\mathcal{O}_{X'})$ est un $\mathcal{O}_X$-$\mathcal{M}$odule localement libre d'un certain degré d égal à celui de l'extension de corps de nombres*

$$F \subset F' .$$

(iii) *Pour tout point fermé x de X, on peut écrire*

$$d = \sum_{x' \mapsto x} e_{x'} \cdot f_{x'}$$

où

- *x' décrit l'ensemble fini des points de X' au-dessus de x,*
- *$e_{x'}$ désigne le degré de l'extension résiduelle $\kappa_x \subset \kappa_{x'}$,*
- *$f_{x'}$ désigne la valuation dans $\mathcal{O}_{x',X'}$ de n'importe quelle uniformisante de $\mathcal{O}_{x,X}$.*

(iv) *Pour tout point fermé x' de X', le morphisme $X' \to X$ est non ramifié, donc étale, au voisinage de x', si et seulement si $f_{x'} = 1$.*

Remarque :

On appelle indice de ramification de $X' \to X$ au point x' l'entier $f_{x'} \geq 1$.

Démonstration :

(i) L'anneau $A_{F'}$ est fini sur A_F car il est fini sur $\mathbb{Z}$.

(ii), (iii) et (iv) se montrent comme les propriétés correspondantes de la proposition III.17. Cette fois, les extensions de corps résiduels

$$\kappa_x \subset \kappa_{x'}$$

sont toujours séparables car ces corps sont finis. □

3 Complétions

Si (A, m_A) est un anneau local, la complétion de A est l'anneau local

$$\widehat{A} = \varprojlim_n A/m_A^n = \{(a_n \in A/m_A^n)_{n\in\mathbb{N}} \mid a_{n+1} \mapsto a_n\,, \quad \forall\, n \in \mathbb{N}\} .$$

Il est muni d'un homomorphisme canonique

$$A \to \widehat{A}$$

et l'idéal maximal m_A de A s'envoie dans l'idéal maximal

$$m_{\widehat{A}} = \varprojlim_n m_A/m_A^n$$

de $\widehat{A}$.

Dans le cas des anneaux de valuation discrète, on a :

Proposition III.25. –

Soit (A, m_A) un anneau de valuation discrète de corps des fractions F et de valuation $v_A : F^\times \to \mathbb{Z}$. Alors :

(i) *La complétion $\widehat{A}$ de A est un anneau de valuation discrète qui admet pour uniformisante toute uniformisante ϖ_A de A.*
Son corps des fractions $\widehat{F}$ contient le corps des fractions F de A et sa valuation $v_{\widehat{A}} : \widehat{F}^\times \to \mathbb{Z}$ prolonge la valuation $v_A : F^\times \to \mathbb{Z}$ de A.

(ii) *Choisissant un réel $q_A > 1$, l'application*

$$\begin{aligned} |\bullet|_A \quad : \quad & \widehat{F} \to q_A^{\mathbb{Z}} \cup \{0\} \subset \mathbb{R}_+ \\ & f \mapsto |f|_A = \begin{cases} q_A^{-v_{\widehat{A}}(f)} & si \quad f \neq 0\,, \\ 0 & si \quad f = 0\,, \end{cases} \end{aligned}$$

est une "norme ultramétrique" de $\widehat{F}$ au sens qu'elle vérifie

$$\forall\, f_1, f_2 \in \widehat{F}\,, \qquad \begin{cases} |f_1 + f_2|_A & \leq \quad \max\{|f_1|_A, |f_2|_A\}\,, \\ |f_1 \cdot f_2|_A & = \quad |f_1|_A \cdot |f_2|_A\,. \end{cases}$$

De plus, F [resp. A] est dense dans $\widehat{F}$ [resp. $\widehat{A}$] relativement à cette norme et $\widehat{F}$ [resp. $\widehat{A}$] est complet au sens que toute suite de Cauchy y est convergente.

Remarque :

Si $A = \mathcal{O}_{x,X} = \mathcal{O}_x$ est l'anneau local en un point fermé x d'une courbe X sur un corps de base K qui est localement normale, ou bien d'une courbe arithmétique X qui est régulière, on notera

$$\begin{aligned} \widehat{A} &= \widehat{\mathcal{O}}_x = O_x\,, \quad m_{\widehat{A}} = m_x\,, \\ \widehat{F} &= F_x\,, \\ v_{\widehat{A}} &= v_x\,, \\ \varpi_A &= \varpi_x\,, \\ q_A &= q_x\,, \\ |\bullet|_A &= |\bullet|_x\,. \end{aligned}$$

Si le corps résiduel κ_x en x est fini (c'est-à-dire si le corps de base K est fini ou bien si X est une courbe arithmétique), on prendra toujours

$$q_x = \#\,\kappa_x$$

pour des raisons qui apparaîtront plus tard.

Démonstration :

(i) Soit ϖ_A une uniformisante de A.
Pour tout élément

$$a = (a_n \in m_A/m_A^n)_{n \in \mathbb{N}}$$

de l'idéal maximal

$$m_{\widehat{A}} = \varprojlim_n m_A/m_A^n\,,$$

on peut écrire pour tout $n \geq 1$

$$a_n = \varpi_A \cdot a_n' \quad \text{avec} \quad a_n' \in A/m_A^{n-1}\,.$$

Alors la suite

$$(a_n' \in A/m_A^{n-1})_{n \geq 1}$$

définit un élément $a' \in \widehat{A}$ qui vérifie

$$a = \varpi_A \cdot a' .$$

Ainsi, ϖ_A engendre l'idéal maximal $m_{\widehat{A}}$ de $\widehat{A}$.

De plus, ϖ_A n'est pas nilpotent dans $\widehat{A}$ donc $\widehat{A}$ est un anneau de valuation discrète.

Son corps des fractions $\widehat{F} = \widehat{A}\,[\varpi_A^{-1}]$ contient le corps des fractions $F = A\,[\varpi_A^{-1}]$ de A et sa valuation $v_{\widehat{A}}$ prolonge celle v_A de A puisque l'uniformisante ϖ_A de A est une uniformisante de $\widehat{A}$.

(ii) L'inégalité

$$|f_1 + f_2|_A \leq \max\{|f_1|_A, |f_2|_A\}$$

est évidente si f_1, f_2 ou $f_1 + f_2$ est 0. Sinon elle équivaut à l'inégalité

$$v_{\widehat{A}}(f_1 + f_2) \geq \min\{v_{\widehat{A}}(f_1), v_{\widehat{A}}(f_2)\}$$

déjà remarquée après la définition III.4.

De même, l'égalité

$$|f_1 \cdot f_2|_A = |f_1|_A \cdot |f_2|_A$$

est évidente si f_1 ou f_2 est 0. Sinon, elle équivaut à l'égalité

$$v_{\widehat{A}}(f_1 \cdot f_2) = v_{\widehat{A}}(f_1) + v_{\widehat{A}}(f_2)$$

c'est-à-dire au fait que $v_{\widehat{A}} : \widehat{F}^\times \to \mathbb{Z}$ est un homomorphisme.

Comme $\widehat{F} = \widehat{A}\,[\varpi_A^{-1}]$, $F = A\,[\varpi_A^{-1}]$, $A = \widehat{A} \cap F$ et

$$\widehat{A} = \{f \in \widehat{F} \mid |f|_A \leq 1\} ,$$

on est réduit à prouver que A est dense dans $\widehat{A}$ et que $\widehat{A}$ est complet.

Soit $a = (\overline{a}_n \in A/m_A^n)_{n\geq 0}$ un élément de $\widehat{A}$.

Pour tout n, la composante $\overline{a}_n \in A/m_A^n$ se relève en un élément a_n de A, bien déterminé modulo m_A^n, et on a

$$|a - a_n|_A \leq q_A^{-n} .$$

Ainsi A est dense dans $\widehat{A}$.

Soit enfin $(f_n)_{n\geq 0}$ une suite de Cauchy d'éléments de $\widehat{A}$. Pour tout n, il existe $N_n \in \mathbb{N}$ tel que

$$|f_{n_1} - f_{n_2}|_A \leq q_A^{-n} , \quad \forall\, n_1, n_2 \geq N_n .$$

Cela signifie que, si $n_1 \geq N_n$, l'image de $f_{n_1} \in \widehat{A}$ dans A/m_A^n ne dépend plus de n_1. Notons $a_n \in A/m_A^n$ cette image commune.

Alors la suite $(a_n \in A/m_A^n)_{n\geq 0}$ définit un élément $f \in \widehat{A}$ qui vérifie

$$\forall\, n , \quad n_1 \geq N_n \Rightarrow |f_{n_1} - f|_A \leq q_A^{-n} .$$

Autrement dit, la suite $(f_n)_{n\geq 0}$ converge vers f dans $\widehat{A}$.

$\square$

Cette proposition est naturellement complétée par le résultat suivant :

Proposition III.26. –

Soient A un anneau de valuation discrète de corps des fractions F, et B une A-algèbre finie et plate (c'est-à-dire sans A-torsion) dont toutes les localisations B_x en les points fermés x de $\mathrm{Spec}\,(B)$ *sont des anneaux de valuation discrète.*

Alors, si x décrit l'ensemble fini de ces points fermés, on a un isomorphisme canonique

$$B \otimes_A \widehat{A} \xrightarrow{\sim} \prod_x \widehat{B}_x$$

et un isomorphisme induit

$$B \otimes_A \mathrm{Frac}\,(\widehat{A}) \xrightarrow{\sim} \prod_x \mathrm{Frac}\,(\widehat{B}_x)\,.$$

Remarque :

Cette proposition s'applique en particulier si

$$X' \to X$$

est un morphisme entre courbes normales propres sur un corps K induit par une extension finie de leurs corps de fonctions

$$F = F_X \hookrightarrow F' = F_{X'}\,,$$

ou bien un morphisme entre courbes arithmétiques connexes régulières entières induit par une extension de corps de nombres

$$F \hookrightarrow F'\,.$$

Dans ce cas, si x est un point fermé de X et x' décrit l'ensemble fini des points fermés de X' au-dessus de x, on a

$$X' \times_X \mathrm{Spec}\,(O_x) = \coprod_{x' \mapsto x} \mathrm{Spec}\,(O_{x'})$$

et

$$X' \times_X \mathrm{Spec}\,(F_x) = \coprod_{x' \mapsto x} \mathrm{Spec}\,(F'_{x'})\,.$$

Démonstration :

Notons ϖ_A une uniformisante de A.

Les points fermés x de $\mathrm{Spec}\,(B)$ sont les points au-dessus du point fermé de $\mathrm{Spec}\,(A)$ puisque B est finie et plate sur A. Pour tout tel point x, on dispose de la valuation

$$f_x = v_x(\varpi_A) \geq 1\,.$$

Pour tout entier $n \geq 1$, la fibre

$$\mathrm{Spec}\,(B) \times_{\mathrm{Spec}\,(A)} \mathrm{Spec}\,(A/m_A^n) = \mathrm{Spec}\,(B/\varpi_A^n \cdot B)$$

est réunion disjointe finie des points x, avec en chacun de ces points l'anneau de structure

$$B_x/\varpi_A^n \cdot B_n = B_x/m_x^{n \cdot f_x}\,.$$

D'où un isomorphisme canonique

$$B \otimes_A A/m_A^n \xrightarrow{\sim} \prod_x B_x/m_x^{n \cdot f_x}\,.$$

En passant à la limite projective sur les $n \in \mathbb{N}$, on obtient

$$B \otimes_A \widehat{A} \xrightarrow{\sim} \prod_x \widehat{B}_x\,.$$

L'isomorphisme

$$B \otimes_A \operatorname{Frac}(\widehat{A}) \xrightarrow{\sim} \prod_x \operatorname{Frac}(\widehat{B}_x)$$

s'en déduit puisque

$$\operatorname{Frac}(\widehat{A}) = \widehat{A}\,[\varpi_A^{-1}]$$

et

$$\operatorname{Frac}(\widehat{B}_x) = \widehat{B}_x\,[\varpi_A^{-1}]\,, \qquad \forall\, x\,.$$

$\square$

IV. Endomorphismes de Frobenius, fibrés inversibles et chtoucas de Drinfeld

1 Les endomorphismes de Frobenius

Soit $\mathbb{F}_q$ un corps fini à q éléments.

Le noyau de l'unique homomorphisme
$$\mathbb{Z} \to \mathbb{F}_q$$
est un idéal premier $p\,\mathbb{Z}$, si bien que $\mathbb{F}_q$ est une extension, nécessairement finie d'un certain degré d, de $\mathbb{F}_p = \mathbb{Z}/p\,\mathbb{Z}$. Par suite, on a $q = p^d$.

Le lemme suivant définit les endomorphismes de Frobenius des $\mathbb{F}_q$-algèbres :

Lemme IV.1. –

Soit $\mathbb{F}_q$ un corps fini à q éléments. Alors :

(i) *Pour toute $\mathbb{F}_q$-algèbre A, l'application*
$$\begin{aligned} \mathrm{Frob}_A \quad : \quad & A \to A \\ & a \mapsto a^q \end{aligned}$$
est un endomorphisme de l'anneau A.

(ii) *Pour tout morphisme $A \to B$ de $\mathbb{F}_q$-algèbres, le diagramme*
$$\begin{tikzcd} A \arrow[r, "\mathrm{Frob}_A"] \arrow[d] & A \arrow[d] \\ B \arrow[r, "\mathrm{Frob}_B"] & B \end{tikzcd}$$
est commutatif.

(iii) *Si $A = \mathbb{F}_q$, Frob_A est l'identité de $\mathbb{F}_q$.*

Démonstration :

(i) Le cardinal q de $\mathbb{F}_q$ est une puissance p^d d'un nombre premier p. Comme $\mathbb{F}_q$ contient $\mathbb{F}_p$, il suffit de traiter le cas où $q = p$. Pour tous éléments $a, a' \in A$, on a évidemment
$$(a \cdot a')^p = a^p \cdot a'^p$$
mais aussi
$$(a + a')^p = \sum_{0 \le i \le p} \frac{p!}{i!\,(p-i)!}\; a^i \cdot a'^{p-i} = a^p + a'^p$$
puisque, p étant un nombre premier, il divise chacun des coefficients
$$\frac{p!}{i!\,(p-i)!} \in \mathbb{Z}\,, \quad 1 \le i \le p-1\,,$$
qui donc s'annule dans $\mathbb{F}_p$ et a fortiori dans A.

(ii) est évident.

(iii) Le groupe multiplicatif $\mathbb{F}_q^\times = \mathbb{F}_q - \{0\}$ compte $q-1$ éléments donc tout élément a de ce groupe vérifie l'équation
$$a^{q-1} = 1$$
et, par conséquent, tout élément de $\mathbb{F}_q$ vérifie
$$a^q = a\,.$$

□

Ce lemme permet de définir l'endomorphisme de Frobenius de n'importe quel schéma sur $\mathbb{F}_q$:

Définition IV.2. –

Pour tout schéma X sur un corps fini $\mathbb{F}_q$, on appelle endomorphisme de Frobenius de X et on note
$$\mathrm{Frob}_X : X \to X$$
l'unique endomorphisme de ce schéma qui stabilise tout ouvert affine $\mathrm{Spec}\,(A)$ *et est induit sur cet ouvert par*
$$\mathrm{Frob}_A : A \to A\,.$$

Remarque :

Pour tout morphisme $X \to Y$ de schémas sur $\mathbb{F}_q$, le carré

$$\begin{tikzcd} X \arrow[r, "\mathrm{Frob}_X"] \arrow[d] & X \arrow[d] \\ Y \arrow[r, "\mathrm{Frob}_Y"] & Y \end{tikzcd}$$

est commutatif.

En particulier, pour tout schéma X sur $\mathbb{F}_q$, on a le triangle commutatif :

$$\begin{tikzcd} X \arrow[rr, "\mathrm{Frob}_X"] \arrow[dr] & & X \arrow[dl] \\ & \mathrm{Spec}\,(\mathbb{F}_q) & \end{tikzcd}$$

□

Voici deux propriétés très importantes des endomorphismes de Frobenius des schémas :

Lemme IV.3. –

Soit X un schéma sur un corps fini $\mathbb{F}_q$. Alors :

(i) *L'endomorphisme de Frobenius*
$$\mathrm{Frob}_X : X \to X$$
est universellement bijectif.

(ii) *Le sous-schéma* $\text{Fixe}\,(\text{Frob}_X)$ *des points fixes de* Frob_X*, défini comme produit fibré dans le carré cartésien*

$$\begin{tikzcd} \text{Fixe}\,(\text{Frob}_X) \arrow[r] \arrow[d] & X \arrow[d, "(\text{Frob}_X\,,\,\text{Id}_X)"] \\ X \arrow[r, "(\text{Id}_X\,,\,\text{Id}_X)"] & X \times_{\text{Spec}(\mathbb{F}_q)} X \end{tikzcd}$$

est le sous-schéma fermé de X *non ramifié sur* $\mathbb{F}_q$

$$\text{Fixe}\,(\text{Frob}_X) = \coprod_{x \in X(\mathbb{F}_q)} \text{Spec}\,(\mathbb{F}_q)$$

supporté par l'ensemble $X(\mathbb{F}_q)$ *des points de* X *à valeurs dans* $\mathbb{F}_q$*.*
Plus généralement, pour toute extension finie $\mathbb{F}_{q'}$ *de* $\mathbb{F}_q$ *d'un certain degré* n*, avec donc* $q' = q^n$*, le sous-schéma des points fixes de* Frob_X^n *est*

$$\text{Fixe}\,(\text{Frob}_X^n) = \coprod_{x \in X(\mathbb{F}_{q^n})} \text{Spec}\,(\kappa_x)\,.$$

Démonstration :

(i) Pour que $\text{Frob}_X : X \to X$ soit universellement bijectif, il faut et il suffit que, pour tout corps algébriquement clos $\overline{\kappa} \supset \mathbb{F}_q$, l'application

$$X(\overline{\kappa}) \xrightarrow{\text{Frob}_X} X(\overline{\kappa})$$

soit bijective.
Cela résulte de ce que $\text{Frob}_{\overline{\kappa}} : a \mapsto a^q$ est un automorphisme de $\overline{\kappa}$ et de ce que tout point géométrique $\text{Spec}\,(\overline{\kappa}) \to X$ de X s'inscrit dans un carré commutatif :

$$\begin{tikzcd} \text{Spec}\,(\overline{\kappa}) \arrow[r, "\text{Frob}_{\overline{\kappa}}", "\sim"'] \arrow[d] & \text{Spec}\,(\overline{\kappa}) \arrow[d] \\ X \arrow[r, "\text{Frob}_X"] & X \end{tikzcd}$$

(ii) Il suffit de traiter le cas où $X = \text{Spec}\,(A)$ est affine et où son anneau de structure A est engendré sur $\mathbb{F}_q$ par un nombre fini d'éléments.
Alors $X' = \text{Fixe}\,(\text{Frob}_X)$ est un sous-schéma fermé de X, donc affine d'anneau un quotient A' de A.
Pour tout élément $a \in A'$, l'équation

$$a - a^q = 0$$

entraîne $da = 0$ dans $\Omega^1_{A'/\mathbb{F}_q}$.
Donc A' est non ramifié sur $\mathbb{F}_q$ et $\text{Fixe}\,(\text{Frob}_X)$ est une réunion disjointe de spectres $\text{Spec}\,(\mathbb{F}_{q'})$ d'extensions finies $\mathbb{F}_{q'}$ de $\mathbb{F}_q$.
De plus, ces $\mathbb{F}_{q'}$ vérifient

$$a^q = a\,, \quad \forall\, a \in \mathbb{F}_{q'}\,,$$

et se confondent donc tous avec $\mathbb{F}_q$.
Le cas des Frob_X^n se déduit de celui de Frob_X en remplaçant $\mathbb{F}_q$ par ses extensions $\mathbb{F}_{q^n}$.

$\square$

On déduit de ce lemme :

Corollaire IV.4. –

Soit S un schéma localement nœthérien sur $\mathbb{F}_q$. Alors :

(i) *Pour tout morphisme étale fini*
$$X \to S\,,$$
le carré commutatif
$$\begin{array}{ccc} X & \xrightarrow{\mathrm{Frob}_X} & X \\ \downarrow & & \downarrow \\ S & \xrightarrow{\mathrm{Frob}_S} & S \end{array}$$
est cartésien.

(ii) *Si S est connexe et $\overline{s}$ désigne un point géométrique de S, l'homomorphisme*
$$\pi_1(S, \overline{s}) \to \pi_1(S, \overline{s})$$
induit par $\mathrm{Frob}_S : S \to S$ est l'identité.

Démonstration :

(i) Considérons l'homomorphisme $X \to S \times_{\mathrm{Frob}_S, S} X$ induit par Frob_X.
D'après le lemme IV.3(i) ci-dessus, il est universellement bijectif.
D'autre part, d'après le corollaire II.24, il est étale.
Donc, d'après la proposition II.17, c'est un isomorphisme.

(ii) traduit (i).

$\square$

L'endomorphisme de Frobenius permet de décrire la catégorie des extensions finies (nécessairement séparables) des corps finis :

Proposition IV.5. –

Soient $\mathbb{F}_q$ un corps fini à q éléments et $\overline{\mathbb{F}}_q$ une clôture algébrique de $\mathbb{F}_q$ munie de l'automorphisme de Frobenius
$$\mathrm{Frob} : a \mapsto a^q\,.$$
Alors :

(i) *Pour tout entier $n \geq 1$*
$$\{a \in \overline{\mathbb{F}}_q \mid \mathrm{Frob}^n(a) = a\} = \{a \in \overline{\mathbb{F}}_q \mid a^{q^n} = a\}$$
est l'unique sous-corps de $\overline{\mathbb{F}}_q$ qui est de degré n sur $\mathbb{F}_q$. On peut le noter $\mathbb{F}_{q^n}$.

(ii) *Les automorphismes de $\overline{\mathbb{F}}_q$ stabilisent chaque $\mathbb{F}_{q^n}$, $n \geq 1$.*

(iii) *Pour tout $n \geq 1$, les automorphismes de $\mathbb{F}_{q^n}$ sont au nombre de n et sont les*
$$\mathrm{Frob}^i\,, \quad 0 \leq i < n\,.$$

Démonstration :

(i) Le sous-ensemble des points fixes de Frob^n dans $\overline{\mathbb{F}}_q$ est un sous-corps qui contient $\mathbb{F}_q$, et il compte q^n éléments puisque le polynôme $T^{q^n} - T$ est séparable. Donc c'est une extension finie de degré n de $\mathbb{F}_q$. Réciproquement, tout sous-corps de $\overline{\mathbb{F}}_q$ qui est fini de degré n sur $\mathbb{F}_q$ est contenu dans celui-là car ses éléments satisfont l'équation

$$a^{q^n} = a\,.$$

(ii) est conséquence immédiate de (i).

(iii) Les Frob^i, $0 \leq i < n$, définissent des automorphismes deux à deux distincts de $\mathbb{F}_{q^n}$ car, pour tous i, j avec $0 \leq i < j < n$, les éléments de $\mathbb{F}_{q^n}$, qui sont au nombre de q^n, ne peuvent être tous des racines du polynôme

$$T^{q^j} - T^{q^i} = T^{q^i}(T^{q^j - q^i} - 1)\,.$$

La conclusion résulte de ce que, d'après la remarque qui suit le corollaire II.28, on connaît a priori l'inégalité

$$\#\,\mathrm{Aut}_{\mathbb{F}_q}(\mathbb{F}_{q^n}) \leq n\,.$$

□

On déduit de cette proposition :

Corollaire IV.6. –

Soit $\mathbb{F}_q$ un corps fini à q éléments. Alors :

(i) *Les groupes de Galois $\pi_1(\mathrm{Spec}\,(\mathbb{F}_q), \overline{s})$ associés aux points géométriques $\overline{s}$ de $\mathrm{Spec}\,(\mathbb{F}_q)$ sont abéliens et donc reliés par des isomorphismes canoniques. On peut les noter $\pi_1(\mathrm{Spec}\,(\mathbb{F}_q))$ ou $\Gamma_{\mathbb{F}_q}$.*

(ii) *Ils sont isomorphes à $\widehat{\mathbb{Z}} = \varprojlim_n \mathbb{Z}/n\,\mathbb{Z}$, de telle façon que l'élément $1 \in \mathbb{Z} \subset \widehat{\mathbb{Z}}$ correspond à l'automorphisme*

$$\mathrm{Frob} : a \mapsto a^q$$

de n'importe quelle clôture algébrique $\overline{\mathbb{F}}_q$ de $\mathbb{F}_q$.

(iii) *Pour tout $n \geq 1$, les extensions $\mathbb{F}_{q^n}$ de degré n de $\mathbb{F}_q$, qui sont toutes isomorphes, correspondent à l'ensemble*

$$\mathbb{Z}/n\,\mathbb{Z} = \widehat{\mathbb{Z}}/n\,\widehat{\mathbb{Z}}$$

muni de l'action naturelle de $\widehat{\mathbb{Z}} = \Gamma_{\mathbb{F}_q} = \pi_1(\mathrm{Spec}\,(\mathbb{F}_q))$. □

Ce corollaire permet de définir des éléments privilégiés dans les groupes fondamentaux $\pi_1(S, \bullet)$ des schémas S connexes et localement de type fini sur $\mathbb{Z}$, tels que les courbes sur un corps fini ou les courbes arithmétiques du chapitre III.

On note préalablement que si S est un schéma localement de type fini sur $\mathbb{Z}$, tous les points fermés x de S ont pour corps résiduels κ_x des corps finis.

Cela permet de poser la définition suivante :

Définition IV.7. –

Soit S un schéma localement de type fini sur $\mathbb{Z}$ et connexe, et soit x un point fermé de S, de corps résiduel κ_x.

(i) *Si $\overline{s}$ est un point géométrique de S qui se factorise à travers* $\mathrm{Spec}\,(\kappa_x)$*, on appelle "élément de Frobenius en x" et on note*

$$\sigma_x \in \pi_1(S, \overline{s})$$

l'image de l'élément

$$1 = \mathrm{Frob} \in \widehat{\mathbb{Z}} = \Gamma_{\kappa_x}$$

par l'homomorphisme du corollaire II.28(iii)

$$\Gamma_{\kappa_x} = \pi_1(\mathrm{Spec}\,(\kappa_x), \overline{s}) \to \pi_1(S, \overline{s})\,.$$

(ii) *Si $\overline{s}$ est un point géométrique arbitraire de S, on appelle encore "élément de Frobenius en x" et on note toujours*

$$\sigma_x \in \pi_1(S, \overline{s})$$

les images du σ_x de (i) *par les isomorphismes du corollaire* II.28(ii)*.*

Remarque :

Dans la situation de (ii), les $\sigma_x \in \pi_1(S, \overline{s})$ sont bien définis à conjugaison près. □

2 Schémas classifiants : le cas des fibrés inversibles sur les courbes

D'après la remarque qui suit le corollaire II.28, se donner un homomorphisme continu surjectif

$$\pi_1(S, \overline{s}) \to G$$

du groupe fondamental d'un schéma localement nœthérien connexe S muni d'un point géométrique $\overline{s}$ vers un groupe fini G, équivaut à construire un revêtement (fini) étale connexe

$$X \to S$$

muni d'une action de G qui soit simplement transitive sur la fibre $X(\overline{s})$.

On peut se demander comment construire, au moins pour certains S, des schémas sur S qui soient munis d'actions non triviales de groupes finis dépendant de S et qui soient des revêtements étales.

Plus généralement, on peut se demander comment construire des schémas.

Un procédé extrêmement général de construction d'objets naturels dans une catégorie $\mathcal{C}$ consiste à considérer des foncteurs contravariants naturels sur cette catégorie et à montrer qu'ils sont "représentables" au sens suivant :

Définition IV.8. –

Soit $\mathcal{C}$ une catégorie.

(i) *On dit que tout objet X de $\mathcal{C}$ "représente" le foncteur contravariant vers la catégorie* Ens *des ensembles*

$$\mathrm{Hom}\,(\bullet, X) : Y \mapsto \mathrm{Hom}\,(Y, X)\,.$$

(ii) *Réciproquement, considérons un foncteur contravariant*

$$F : \mathcal{C} \to \mathrm{Ens}$$

qui associe donc à tout objet Y de $\mathcal{C}$ un ensemble $F(Y)$, et à tout morphisme $Y' \to Y$ de $\mathcal{C}$ une application en sens inverse $F(Y) \to F(Y')$.

On dit que F est "repésentable" par un objet X de $\mathcal{C}$, nécessairement unique à unique isomorphisme près, ou que X "classifie" les éléments de F si les foncteurs F de $\mathrm{Hom}\,(\bullet, X)$ *sont isomorphes.*

Remarque :

L'unicité dans (ii) – qui est appelée "lemme de Yoneda" – résulte de ce que, pour tous objets X, X' de $\mathcal{C}$, se donner un morphisme [resp. un isomorphisme] entre les deux foncteurs qu'ils représentent

$$\mathrm{Hom}\,(\bullet, X') \to \mathrm{Hom}\,(\bullet, X)$$

équivaut à se donner un morphisme [resp. un isomorphisme]

$$X' \to X\,,$$

qui n'est autre que l'image de $\mathrm{Id}_{X'}$.

Exemples :

(i) On sait que pour tout corps K, $\mathbb{P}^n(K)$ s'identifie à l'ensemble des droites de K^{n+1} ou, en identifiant K^{n+1} à son dual, à l'ensemble des classes d'isomorphisme de quotients de dimension 1 de K^{n+1}.
En fait, pour tout schéma S, l'ensemble $\mathbb{P}^n_{\mathbb{Z}}(S)$ des points de l'espace projectif $\mathbb{P}^n_{\mathbb{Z}}$ à valeurs dans S s'identifie à l'ensemble des classes d'isomorphismes de $\mathcal{O}_S$-$\mathcal{M}$odules quotients de $\mathcal{O}_S^{n+1}$

$$\mathcal{O}_S^{n+1} \to \mathcal{L} \to 0$$

qui sont localement libres de rang 1 sur S.

(ii) Plus généralement, pour tous entiers $0 < d < n$, le foncteur contravariant qui associe à tout schéma S l'ensemble des classes d'isomorphismes de $\mathcal{O}_S$-$\mathcal{M}$odules quotients de $\mathcal{O}_S^n$

$$\mathcal{O}_S^n \to \mathcal{E} \to 0$$

qui sont localement libres de rang d, est représentable par un schéma $\mathrm{Gr}^{d,n}$ de type fini sur $\mathbb{Z}$ (et même projectif, c'est-à-dire qui se plonge comme sous-schéma fermé d'un $\mathbb{P}^N_{\mathbb{Z}}$), appelé "grassmannienne".

(iii) Plus généralement, considérons un schéma de base S localement nœthérien, un schéma X qui est projectif sur S (c'est-à-dire se plonge localement sur S comme sous-schéma fermé d'espaces projectifs $\mathbb{P}^N_S = \mathbb{P}^N_{\mathbb{Z}} \times_{\mathrm{Spec}(\mathbb{Z})} S$) et un $\mathcal{O}_X$-$\mathcal{M}$odule cohérent $\mathcal{M}$ sur X qui est plat sur $\mathcal{O}_S$.
Alors, d'après un théorème fondamental de Grothendieck, le foncteur contravariant qui associe à tout schéma S' sur S l'ensemble des classes d'isomorphisme de $\mathcal{O}_{S'\times_S X}$-$\mathcal{M}$odules $\mathcal{M}'$ quotients de $\mathcal{M} \otimes_{\mathcal{O}_S} \mathcal{O}_{S'}$

$$\mathcal{M} \otimes_{\mathcal{O}_S} \mathcal{O}_{S'} = \mathcal{M} \otimes_{\mathcal{O}_X} \mathcal{O}_{X\times_S S'} \to \mathcal{M}' \to 0$$

sur $X \times_S S'$ qui sont plats sur $\mathcal{O}_{S'}$, est représentable par un schéma $\mathcal{H}ilb^{\mathcal{M}}_{X/S}$ localement de type fini sur S appelé "schéma de Hilbert".

(iv) En particulier, si X est un schéma projectif et plat sur un schéma de base S localement nœthérien, le foncteur contravariant qui associe à tout schéma S' sur S l'ensemble des sous-schémas fermés

$$Y \hookrightarrow X \times_S S'$$

qui sont plats sur S', est représentable par un schéma $\mathcal{C}h_{X/S}$ localement de type fini sur S', appelé "schéma de Chow".

(v) En identifiant tout morphisme $X' \to Y'$ au-dessus d'un schéma de base S' à son graphe $X' \hookrightarrow X' \times_{S'} Y'$, on en déduit que si X et Y sont deux schémas projectifs et plats sur un schéma de base localement nœthérien S, le foncteur contravariant

$$(S' \to S) \mapsto \mathrm{Hom}_{S'}(X \times_S S', Y \times_S S')$$

est représentable par un schéma de type fini sur S noté

$$\mathcal{H}om_S(X,Y)\,.$$

Par conséquent, le foncteur contravariant

$$(S' \to S) \mapsto \mathrm{Isom}_{S'}(X \times_S S', Y \times_S S')$$

est représentable par un schéma de type fini sur S

$$\mathcal{I}som_S(X,Y)$$

qui est un sous-schéma fermé de $\mathcal{H}om_S(X,Y) \times_S \mathcal{H}om_S(Y,X)$.

(vi) On en déduit enfin que si X, Y, Z sont trois schémas projectifs et plats reliés par deux morphismes $X \to Z$ et $Y \to Z$ au-dessus d'un schéma de base S localement nœthérien, alors les foncteurs contravariants

$$(S' \to S) \mapsto \mathrm{Hom}_{Z\times_S S'}(X \times_S S', Y \times_S S')$$
$$(S' \to S) \mapsto \mathrm{Isom}_{Z\times_S S'}(X \times_S S', Y \times_S S')$$

sont représentables par des schémas de type fini sur S notés

$$\mathcal{H}om_{Z/S}(X,Y)$$

et

$$\mathcal{I}som_{Z/S}(X,Y)\,.$$

□

Dans ce paragraphe, nous allons rappeler l'existence de schémas classifiant les "fibrés inversibles" sur un schéma donné. Commençons par définir les fibrés inversibles :

Définition IV.9. –

(i) *Un fibré inversible sur un schéma X est un $\mathcal{O}_X$-$\mathcal{M}$odule localement libre de rang* 1.

(ii) *Si $N \hookrightarrow X$ est un sous-schéma fermé d'un schéma X, une structure de niveau N sur un fibré inversible $\mathcal{L}$ sur X est un isomorphisme*

$$\mathcal{L} \otimes_{\mathcal{O}_X} \mathcal{O}_N \xrightarrow{\sim} \mathcal{O}_N$$

appelé une "trivialisation" de la restriction $\mathcal{L} \otimes_{\mathcal{O}_X} \mathcal{O}_N$ de $\mathcal{L}$ à N. □

On a :

Lemme IV.10. –

(i) *Pour tout schéma X [resp. et tout sous-schéma fermé $N \hookrightarrow X$], l'ensemble* $\mathrm{Pic}\,(X)$ *[resp.* $\mathrm{Pic}_N\,(X)$*] des classes d'isomorphisme de fibrés inversibles sur X [resp. avec structure de niveau N], muni du produit tensoriel, a une structure de groupe abélien.*

(ii) *Pour tout morphisme de schémas [resp. tout carré commutatif]*

$$\begin{tikzcd} X' \arrow[d, "f"] \\ X \end{tikzcd} \qquad \text{[resp.} \quad \begin{tikzcd} N' \arrow[r, hook] \arrow[d] & X' \arrow[d, "f"] \\ N \arrow[r, hook] & X \end{tikzcd} \quad]$$

le foncteur

$$\mathcal{L} \mapsto f^*(\mathcal{L})$$

définit un homomorphisme de groupes abéliens

$$\mathrm{Pic}\,(X) \to \mathrm{Pic}\,(X') \qquad \textit{[resp.} \quad \mathrm{Pic}_N\,(X) \to \mathrm{Pic}_{N'}\,(X')\ \textit{]}.$$

(iii) *Pour tout morphisme fini et plat de schémas localement nœthériens $X' \to X$ [resp. et tous sous-schémas fermés $N \hookrightarrow X$, $N' \hookrightarrow X'$ tels que $N \times_X X'$ se plonge dans N'], le déterminant définit un homomorphisme naturel*

$$\det : \mathrm{Pic}\,(X') \to \mathrm{Pic}\,(X) \qquad \textit{[resp.} \quad \mathrm{Pic}_{N'}\,(X') \to \mathrm{Pic}_N\,(X)\ \textit{]}.$$

Démonstration :

(i) Si $\mathcal{L}_1$ et $\mathcal{L}_2$ sont deux fibrés inversibles sur X, c'est-à-dire localement isomorphes à $\mathcal{O}_X$, il en est de même de $\mathcal{L}_1 \otimes_{\mathcal{O}_X} \mathcal{L}_2$. De plus, la formation du produit tensoriel

$$(\mathcal{L}_1, \mathcal{L}_2) \mapsto \mathcal{L}_1 \otimes_{\mathcal{O}_X} \mathcal{L}_2$$

est associative et commutative, et admet $\mathcal{O}_X$ pour tout élément neutre.

Il reste à prouver que tout fibré inversible $\mathcal{L}$ sur X admet un inverse. Considérons un recouvrement de X par des ouverts U_i sur lesquels on a des isomorphismes $\mathcal{O}_{U_i} \xrightarrow{\sim} \mathcal{L}_{|U_i}$. Alors $\mathcal{L}$ est défini par la famille des isomorphismes de recollement induits

$$u_{i,j} : \mathcal{O}_{U_i \cap U_j} \xrightarrow{\sim} \mathcal{O}_{U_j \cap U_i}\,,$$

lesquels sont compatibles sur les intersections triples $U_i \cap U_j \cap U_k$. Les $u_{i,j}$ sont des éléments inversibles des anneaux $\mathcal{O}_X(U_i \cap U_j)$. La famille de leurs inverses vérifie les mêmes conditions de compatibilité et définit un fibré inversible $\mathcal{L}^{-1}$ tel que

$$\mathcal{L} \otimes_{\mathcal{O}_X} \mathcal{L}^{-1} \cong \mathcal{O}_X\,.$$

(ii) est évident.

(iii) Soit $f : X' \to X$ ce morphisme fini et plat. La $\mathcal{O}_X$-$\mathcal{A}$lgèbre $f_*(\mathcal{O}_{X'})$ est un $\mathcal{O}_X$-$\mathcal{M}$odule fini et plat, donc localement libre d'après le lemme II.20. On peut supposer son rang constant égal à un entier $d \geq 1$.

Pour tout fibré inversible $\mathcal{L}'$ sur X', $f_*(\mathcal{L}')$ est un $\mathcal{O}_X$-$\mathcal{M}$odule localement libre de rang d sur X. Considérons un recouvrement de X par des ouverts U_i sur lesquels on a des isomorphismes $\mathcal{O}_{U_i}^d \xrightarrow{\sim} f_*(\mathcal{L}')$. Alors $f_*(\mathcal{L}')$ est défini par la famille des isomorphismes de recollement induits

$$u_{i,j} : \mathcal{O}^d_{U_i \cap U_j} \xrightarrow{\sim} \mathcal{O}^d_{U_j \cap U_i}$$

qui peuvent être vus comme des matrices inversibles de rang d à coefficients dans les anneaux $\mathcal{O}_X(U_i \cap U_j)$. La famille des déterminants de ces matrices

$$\det(u_{i,j}) : \mathcal{O}_{U_i \cap U_j} \xrightarrow{\sim} U_{U_j \cap U_i}$$

vérifie la condition de compatibilité sur les $U_i \cap U_j \cap U_k$ et définit un fibré inversible $\det(f_*(\mathcal{L}')) = \det(\mathcal{L}')$ sur X.

$\square$

On admet l'important théorème suivant :

Théorème IV.11. –

Soit $X \xrightarrow{f} S$ un schéma projectif et plat sur un schéma de base S localement nœthérien, tel que $\mathcal{O}_S \to f_*(\mathcal{O}_X)$ soit un isomorphisme. Alors :

(i) *Pour tout sous-schéma fermé $N \hookrightarrow X$ plat et surjectif sur S, le foncteur contravariant*

$$(S' \to S) \mapsto \mathrm{Pic}_{X \times_S S'}(X \times_S S')$$

est représentable par un schéma $\mathcal{P}ic_{X/S,N}$ localement de type fini et plat sur S.

(ii) *Il existe un schéma localement de type fini et plat sur S, unique à unique isomorphisme près,*

$$\mathcal{P}ic_{X/S} \to S\,,$$

tel que

(1) *pour tout schéma S' sur S tel que $X \times_S S' \to S'$ admette une section $S' \hookrightarrow X \times_S S'$,*

$$\mathcal{P}ic_{X/S}(S') = \mathrm{Hom}_{S'}(S', \mathcal{P}ic_{X/S})$$

s'identifie à

$$\mathrm{Pic}_{S'}(X \times_S S')\,,$$

(2) *pour tout point s : $\mathrm{Spec}\,(K) \to S$ de S à valeurs dans un corps K, et en notant $X_s = X \times_S \mathrm{Spec}\,(K)$, $\mathcal{P}ic_{X/S}(s)$ s'identifie à $\mathrm{Pic}(X_s)$.*

Remarque :

La condition (1) de (ii) signifie que, pour tout $S' \to S$ tel que $X \times_S S' \to S'$ admette une section $S' \hookrightarrow X \times_S S'$, $\mathcal{P}ic_{X/S} \times_S S'$ s'identifie à $\mathcal{P}ic_{X \times_S S'/S',S'}$.

Cas particulier :

Particulièrement important est le cas où X est une courbe projective sur un corps K, telle que $\mathcal{O}_X(X) = K$, et éventuellement munie d'un sous-schéma fermé $N \hookrightarrow X$ fini sur K. On note alors $\mathcal{P}ic_X$ et $\mathcal{P}ic_{X,N}$ les schémas localement de type fini sur K qui classifient les fibrés inversibles sur X sans ou avec structures de niveau.

□

On dit qu'un schéma G sur un schéma de base S a une structure de groupe, ou qu'il est un "schéma en groupes", s'il est muni d'un morphisme de multiplication

$$G \times_S G \to G\,,$$

d'un morphisme d'élément neutre

$$S \to G\,,$$

et d'un morphisme de passage à l'inverse

$$G \to G$$

qui vérifient les propriétés de définition des groupes.

Il revient au même de demander que le foncteur

$$(S' \to S) \mapsto G(S') = \mathrm{Hom}_S(S', G)$$

soit défini de la catégorie des schémas sur S vers la catégorie des groupes.

Demander que tous les groupes $G(S')$ soient abéliens équivaut à demander que le morphisme de multiplication $G \times_S G \to G$ soit laissé invariant par la permutation des 2 facteurs G. On parle dans ce cas de “schéma en groupes abéliens”.

On déduit du théorème IV.11 ci-dessus et du lemme IV.10 :

Corollaire IV.12. –

(i) *Soit S un schéma de base localement nœthérien.*

Pour tout schéma $X \xrightarrow{f} S$ projectif et plat sur S [resp. et tout sous-schéma fermé $N \hookrightarrow X$ plat et surjectif sur S], tel que $\mathcal{O}_S \to f_*(\mathcal{O}_X)$ soit un isomorphisme, le classifiant

$$\mathcal{P}ic_{X/S} \qquad [\textit{resp.} \quad \mathcal{P}ic_{X/S,N}\,]$$

est un schéma en groupes abéliens sur S.

De plus, les morphismes d'oubli des structures de niveau

$$\mathcal{P}ic_{X/S,N} \to \mathcal{P}ic_{X/S}$$

sont des homomorphismes de schémas en groupes abéliens.

(ii) *Soit $S' \to S$ un morphisme de schémas de base localement nœthériens.*

Pour tout morphisme de tels schémas sur S et S' [resp. et tout carré commutatif de tels sous-schémas fermés]

$$\begin{array}{ccc} X' & \longrightarrow & S' \\ \downarrow & & \downarrow \\ X & \longrightarrow & S \end{array} \qquad [\textit{resp.} \quad \begin{array}{ccccc} N' & \hookrightarrow & X' & \longrightarrow & S' \\ \downarrow & & \downarrow & & \downarrow \\ N & \hookrightarrow & X & \longrightarrow & S \end{array} \quad],$$

les foncteurs d'images réciproques induisent des homomorphismes de schémas en groupes abéliens

$$\mathcal{P}ic_{X/S} \to \mathcal{P}ic_{X'/S'} \qquad [\text{resp.} \quad \mathcal{P}ic_{X/S,N} \to \mathcal{P}ic_{X'/S',N'}\,]\,.$$

(iii) *Pour tout morphisme fini et plat $X' \to X$ de tels schémas sur $S' \to S$ [resp. et tous tels sous-schémas fermés $N \hookrightarrow X$, $N' \hookrightarrow X'$ tels que $N \times_X X'$ se plonge dans N'], on a un homomorphisme de déterminant entre schémas en groupes abéliens*

$$\det : \mathcal{P}ic_{X'/S'} \to \mathcal{P}ic_{X/S} \qquad [\text{resp.} \quad \mathcal{P}ic_{X'/S',N'} \to \mathcal{P}ic_{X/S,N}\,]\,.$$

Si X est un schéma projectif sur un corps K tel que $\mathcal{O}_X(X) = K$, $\mathcal{P}ic_X = \mathcal{P}ic_{X/\mathrm{Spec}(K)}$ est bien défini en tant que schéma en groupe localement de type fini sur K et il possède un élément unité dans $\mathcal{P}ic\,(K)$. La composante connexe $\mathcal{P}ic_X^0$ de l'élément unité est un sous-schéma en groupes de $\mathcal{P}ic_X$ et le quotient $\mathcal{P}ic_X/\mathcal{P}ic_X^0$ est un groupe abélien discret, appelé le groupe de Néron-Severi de X.

On admet encore le résultat suivant :

Proposition IV.13. –

Soit X une courbe projective sur un corps K, telle que $\mathcal{O}_X(X) = K$. Si X est lisse sur K on a :

(i) *La composante connexe $\mathcal{P}ic_X^0 = \mathcal{J}ac_X$, appelée aussi la “jacobienne de X”, est un schéma projectif géométriquement connexe (c'est-à-dire connexe et qui le reste sur n'importe quel corps algébriquement clos $\overline{K} \supset K$) et lisse sur K d'une certaine dimension g, appelée le “genre” de la courbe X.*

Ainsi $\mathcal{J}ac_X$ est ce que l'on appelle une “variété abélienne” de dimension g sur K.

(ii) *Le quotient discret $\mathcal{P}ic_X / \mathcal{J}ac_X$ s'identifie à $\mathbb{Z}$ via un homomorphisme surjectif*

$$\deg : \mathcal{P}ic_X \to \mathbb{Z}$$

appelé le "degré".

(iii) *Pour tout corps $K' \supset K$, l'application*

$$\deg : \mathcal{P}ic_X(K') \to \mathbb{Z}$$

se calcule de la manière suivante :
Si $\mathcal{L} \in \mathcal{P}ic_X(K')$ est un fibré inversible sur $X' = X \otimes_K K'$ et ℓ est un vecteur de base arbitraire de la fibre de $\mathcal{L}$ au point générique de X', on a

$$\deg(\mathcal{L}) = \sum_{x'} \dim_{K'}(\kappa_{x'}) \cdot v_{x'}(\ell)$$

où

- *x' décrit l'ensemble des points fermés de X', avec leurs corps résiduels $\kappa_{x'}$ qui sont des extensions finies de K',*
- *chaque $v_{x'}$ désigne la valuation $\mathrm{Frac}\,(\mathcal{O}_{x',X'})^\times \to \mathbb{Z}$ de l'anneau de valuation discrète $\mathcal{O}_{x',X'}$, et $v_{x'}(\ell)$ désigne l'image par $v_{x'}$ de l'image de ℓ par n'importe quel isomorphisme*

$$\mathcal{L}_{|U'} \xrightarrow{\sim} \mathcal{O}_{U'}$$

dans un voisinage $U' \subset X'$ de x'.

Remarques :

(i) D'après le corollaire III.13 et la proposition III.17, toute courbe X propre et lisse sur un corps K admet un morphisme fini (et plat)

$$X \to \mathbb{P}^1_K$$

vers la droite projective $\mathbb{P}^1_K$.
On en déduit que toute telle courbe est projective sur K.
En fait, c'est vrai de toute courbe propre sur K.

(ii) Pour tout degré $d \in \mathbb{Z}$, on peut noter $\mathcal{P}ic_X^d$ la composante connexe de $\mathcal{P}ic_X$ qui s'envoie sur d par l'homomorphisme deg.
Ainsi, $\mathcal{P}ic_X^d$ est un schéma projectif sur K muni d'une action simplement transitive de $\mathcal{P}ic_X^0 = \mathcal{J}ac_X$.

□

La proposition IV.13 ci-dessus est complétée par le lemme suivant :

Lemme IV.14. –
Soit toujours X une courbe projective et lisse sur un corps K, avec $\mathcal{O}_X(X) = K$. Alors :

(i) *Pour tout sous-schéma fermé fini $N = \mathrm{Spec}\,(\mathcal{O}_N) \hookrightarrow X$ [resp. pour tous sous-schémas fermés finis $N = \mathrm{Spec}\,(\mathcal{O}_N) \hookrightarrow N' = \mathrm{Spec}\,(\mathcal{O}_{N'}) \hookrightarrow X$], l'homomorphisme de schémas en groupes abéliens*

$$\mathcal{P}ic_{X,N} \to \mathcal{P}ic_X \qquad [\textit{resp.} \quad \mathcal{P}ic_{X,N'} \to \mathcal{P}ic_{X,N}\,]$$

est surjectif, et son noyau est le schéma en groupes abéliens qui associe à tout schéma affine $\mathrm{Spec}\,(A)$ *sur K le groupe*

$$\mathrm{Coker}\,(A^\times \to (A \otimes_K \mathcal{O}_N)^\times) \qquad [\textit{resp.} \quad \mathrm{Ker}\,((A \otimes_K \mathcal{O}_{N'})^\times \to (A \otimes_K \mathcal{O}_N)^\times)\,].$$

(ii) *Si $\overline{K} \supset K$ et un corps séparablement clos, ce noyau admet sur $\overline{K}$ une filtration par des sous-schémas en groupes dont tous les quotients sont isomorphes au groupe multiplicatif*

$$\mathbb{G}_m = \mathrm{Spec}\,(K[T,T^{-1}]) : \mathrm{Spec}\,(A) \mapsto A^\times$$

ou au groupe additif

$$\mathbb{A}^1 = \mathrm{Spec}\,(K[T]) : \mathrm{Spec}\,(A) \mapsto A\,.$$

(iii) *Ce noyau est lisse sur K, et le morphisme*

$$\mathcal{P}ic_{X,N} \to \mathcal{P}ic_X \qquad \textit{[resp.} \quad \mathcal{P}ic_{X,N'} \to \mathcal{P}ic_{X,N}\,\textit{]}$$

est lisse.

Esquisse de démonstration :

(i) La surjectivité résulte de ce que, pour tout corps $K' \supset K$ et tout fibré inversible $\mathcal{L} \in \mathcal{P}ic_X(K')$ sur $X_{K'} = X \times_{\mathrm{Spec}(K)} \mathrm{Spec}\,(K')$, la restriction de $\mathcal{L}$ au schéma fini $\mathrm{Spec}\,(\mathcal{O}_N \otimes_K K')$ est nécessairement isomorphe au fibré trivial $\mathcal{O}_N \otimes_K K'$.
La description des noyaux est évidente sur les définitions.

(ii) résulte de (i) puisque, si $\overline{K}$ est algébriquement clos, la $\overline{K}$-algèbre finie $\mathcal{O}_N \otimes_K \overline{K}$ est un produit fini d'algèbres de la forme

$$\overline{K}\,[\varpi]/(\varpi^n) \quad \text{avec} \quad n \geq 1\,.$$

(iii) résulte de (ii) puisque la lissité peut être vérifiée après n'importe quel changement du corps de base (et en fait, plus généralement, après n'importe quel changement de base fidèlement plat).

□

Enfin, on a :

Lemme IV.15. –
Soit toujours X une courbe projective et lisse sur un corps K, avec $\mathcal{O}_X(X) = K$.

(i) *Le faisceau d'idéaux qui définit le sous-schéma fermé diagonal*

$$X \hookrightarrow X \times_{\mathrm{Spec}(K)} X$$

est un fibré inversible et définit donc un morphisme

$$X \to \mathcal{P}ic_X$$

noté

$$x \mapsto \mathcal{O}_X(-x)\,.$$

(ii) *Ce fibré inversible sur $X \times_{\mathrm{Spec}(K)} X$ est naturellement isomorphe au fibré trivial en dehors de la diagonale X.*
Par conséquent, pour tout sous-schéma fermé fini $N \hookrightarrow X$, le morphisme

$$x \mapsto \mathcal{O}_X(-x)$$

se relève canoniquement en un morphisme

$$X - N \to \mathcal{P}ic_{X,N}\,.$$

Remarques :

(i) On notera $x \mapsto \mathcal{O}_X(x)$ les morphismes $X \to \mathcal{P}ic_X$ ou $X - N \to \mathcal{P}ic_{X,N}$ déduits de $x \mapsto \mathcal{O}_X(-x)$ par composition avec les morphismes $\mathcal{P}ic_X \to \mathcal{P}ic_X$ ou $\mathcal{P}ic_{X,N} \to \mathcal{P}ic_{X,N}$ de passage à l'opposé.

(ii) Le morphisme $x \mapsto \mathcal{O}_X(-x)$ envoie X dans la composante connexe $\mathcal{P}ic_X^{-1}$ de $\mathcal{P}ic_X$, et $x \mapsto \mathcal{O}_X(x)$ envoie X dans la composante $\mathcal{P}ic_X^1$.

Démonstration :

Soit $\mathcal{J}$ ce faisceau d'idéaux sur $X \times_{\mathrm{Spec}(K)} X$.

Sa restriction à l'ouvert complémentaire de la diagonale est isomorphe au fibré trivial par définition.

De plus, sa restriction $\mathcal{J}/\mathcal{J}^2$ à la diagonale X est un $\mathcal{O}_X$-$\mathcal{M}$odule localement libre de rang 1 puisqu'elle s'identifie à $\Omega^1_{X/K}$ et que la courbe X est lisse sur K.

D'après le lemme de Nakayama I.34, tout isomorphisme au voisinage d'un point de $X \hookrightarrow X \times_{\mathrm{Spec}(K)} X$

$$\mathcal{O}_X \xrightarrow{\sim} \mathcal{J}/\mathcal{J}^2$$

se relève localement en un morphisme surjectif

$$\mathcal{O}_{X \times_{\mathrm{Spec}(K)} X} \to \mathcal{J}\,.$$

Ce morphisme est nécessairement injectif puisqu'il l'est en dehors de la diagonale. $\square$

3 Chtoucas de Drinfeld de rang 1

Dans ce paragraphe, on considère une courbe X propre et lisse, donc projective, sur un corps fini $\mathbb{F}_q$.

On suppose que X est connexe, si bien que $\mathcal{O}_X(X)$ est un corps extension finie de $\mathbb{F}_q$. Quitte à remplacer $\mathbb{F}_q$ par cette extension finie, on peut supposer que $\mathcal{O}_X(X) = \mathbb{F}_q$.

On dispose donc des schémas en groupes abéliens

$$\mathcal{P}ic_X = \coprod_{d \in \mathbb{Z}} \mathcal{P}ic_X^d \qquad \text{et} \qquad \mathcal{P}ic_{X,N}$$

classifiant les fibrés inversibles sur X sans ou avec structures de niveau $N \hookrightarrow X$, un sous-schéma fermé fini arbitraire de X.

Comme tout schéma sur $\mathbb{F}_q$, ces schémas sont munis de leur endomorphisme de Frobenius. Cela permet de définir les "chtoucas de Drinfeld (de rang 1)" et leurs schémas classifiants.

Définition IV.16. –

On fixe comme ci-dessus une courbe X projective, lisse et géométriquement connexe sur le corps fini $\mathbb{F}_q$.

(i) *Pour tout schéma S sur $\mathbb{F}_q$, on appelle "chtouca (de rang 1)" sur S la donnée de*

- *un fibré inversible $\mathcal{L}$ sur $X \times_{\mathbb{F}_q} S$,*
- *deux morphismes $0 : S \to X$ et $\infty : S \to X$,*
- *un isomorphisme entre fibrés inversibles sur $X \times_{\mathbb{F}_q} S$*

$${}^\tau\mathcal{L} \xrightarrow{\sim} \mathcal{L} \otimes_{\mathcal{O}_X} \mathcal{O}_X(0 - \infty) = \mathcal{L}(0 - \infty)$$

où ${}^\tau\mathcal{L} = (\mathrm{Id}_X \times \mathrm{Frob}_S)^*(\mathcal{L})$.

(ii) *Pour tout sous-schéma fermé fini $N \hookrightarrow X$, on appelle structure de niveau N sur un chtouca $(\mathcal{L}, 0, \infty, {}^\tau\mathcal{L} \xrightarrow{\sim} \mathcal{L}(0-\infty))$ sur un schéma S tel que $\infty, 0 : S \rightrightarrows X$ se factorisent à travers $X - N$, la donnée d'un isomorphisme*

$$u : \mathcal{L}_{|S \times_{\mathbb{F}_q} N} = \mathcal{L} \otimes_{\mathcal{O}_X} \mathcal{O}_N \xrightarrow{\sim} \mathcal{O}_{S \times_{\mathbb{F}_q} N}$$

rendant commutatif le triangle :

$$\begin{tikzcd}
{}^\tau\mathcal{L}_{|S \times_{\mathbb{F}_q} N} \arrow[rr, "\sim"] \arrow[dr, "{}^\tau u"'] & & \mathcal{L}_{|S \times_{\mathbb{F}_q} N} \arrow[dl, "u"] \\
& \mathcal{O}_{S \times_{\mathbb{F}_q} N} &
\end{tikzcd}$$

Remarque :

Si $(\mathcal{L}, 0, \infty, {}^\tau\mathcal{L} \xrightarrow{\sim} \mathcal{L}(0-\infty))$ est un chtouca sur un schéma S sur $\mathbb{F}_q$, les deux morphismes $0 : S \to X$ et $\infty : S \to X$ s'appellent le "zéro" et le "pôle" de ce chtouca.

□

On déduit aussitôt du théorème IV.11 :

Corollaire IV.17. –

Considérant toujours comme fixée la courbe X, on a :

(i) *Le foncteur contravariant qui associe à tout schéma S sur $\mathbb{F}_q$ l'ensemble des classes d'isomorphisme de chtoucas sur S est représentable par un schéma localement de type fini*

$$\mathrm{Cht}^1_X$$

qui est défini comme produit fibré dans le carré cartésien :

$$\begin{tikzcd}
\mathrm{Cht}^1_X \arrow[r] \arrow[d] & \mathcal{P}ic_X \arrow[d] & \mathcal{L} \arrow[d, mapsto] \\
X \times X \arrow[r] & \mathcal{P}ic_X & {}^\tau\mathcal{L} \otimes \mathcal{L}^{-1} \\
(0,\infty) \arrow[r, mapsto] & \mathcal{O}_X(0-\infty) &
\end{tikzcd}$$

(ii) *Pour tout sous-schéma fermé $N = \mathrm{Spec}\,(\mathcal{O}_N) \hookrightarrow X$ fini sur $\mathbb{F}_q$, le foncteur contravariant qui associe à tout schéma S sur $\mathbb{F}_q$ l'ensemble des classes d'isomorphisme de chtoucas avec structure de niveau N sur S est représentable par un schéma localement de type fini*

$$\mathrm{Cht}^1_{X,N}$$

qui est défini comme produit fibré dans le carré cartésien :

$$\begin{tikzcd}
\mathrm{Cht}^1_{X,N} \arrow[r] \arrow[d] & \mathcal{P}ic_{X,N} \arrow[d] & \mathcal{L} \arrow[d, mapsto] \\
(X-N) \times (X-N) \arrow[r] & \mathcal{P}ic_{X,N} & {}^\tau\mathcal{L} \otimes \mathcal{L}^{-1} \\
(0,\infty) \arrow[r, mapsto] & \mathcal{O}_X(0-\infty) &
\end{tikzcd}$$

Remarque :

Comme $\mathcal{P}ic_X$ est la réunion disjointe de ses composantes connexes $\mathcal{P}ic_X^d$, $d \in \mathbb{Z}$, Cht_X^1 ou les $\mathrm{Cht}_{X,N}^1$ sont les réunions disjointes des images réciproques $\mathrm{Cht}_X^{1,d}$ ou $\mathrm{Cht}_{X,N}^{1,d}$ des $\mathcal{P}ic_X^d$.

□

On remarque :

Lemme IV.18. –

Considérant toujours la courbe X [resp. et un niveau $N \hookrightarrow X$], on a :

(i) *Le groupe abélien discret $\mathcal{P}ic_X(\mathbb{F}_q)$ [resp. $\mathcal{P}ic_{X,N}(\mathbb{F}_q)$] des fibrés inversibles [resp. avec structure de niveau N] sur X agit naturellement sur le schéma*

$$\mathrm{Cht}_X^1 \qquad \textit{[resp. } \mathrm{Cht}_{X,N}^1 \textit{]}$$

au-dessus de $X \times X$ [resp. $(X - N) \times (X - N)$].

(ii) *Pour tout point (à valeurs dans un corps) de $X \times X$ [resp. $(X - N) \times (X - N)$], l'action du groupe discret $\mathcal{P}ic_X(\mathbb{F}_q)$ [resp. $\mathcal{P}ic_{X,N}(\mathbb{F}_q)$] sur la fibre de Cht_X^1 [resp. $\mathrm{Cht}_{X,N}^1$] au-dessus de ce point est simplement transitive.*

Démonstration :

Si $\mathcal{L}_0$ est un point de $\mathcal{P}ic_X(\mathbb{F}_q)$ [resp. $\mathcal{P}ic_{X,N}(\mathbb{F}_q)$] et $(\mathcal{L}, 0, \infty, {}^\tau\mathcal{L} \xrightarrow{\sim} \mathcal{L}(0-\infty))$ est un chtouca [resp. avec structure de niveau N] sur un schéma S sur $\mathbb{F}_q$, alors le produit tensoriel

$$\mathcal{L} \otimes_{\mathcal{O}_X} \mathcal{L}_0$$

complété par le même zéro 0 et le même pôle ∞ ainsi que par l'isomorphisme induit

$${}^\tau(\mathcal{L} \otimes \mathcal{L}_0) = {}^\tau\mathcal{L} \otimes \mathcal{L}_0 \xrightarrow{\sim} \mathcal{L}(0-\infty) \otimes \mathcal{L}_0 = (\mathcal{L} \otimes \mathcal{L}_0)(0-\infty)$$

[resp. et par l'isomorphisme $\mathcal{L} \otimes \mathcal{L}_{0|S\times N} \xrightarrow{\sim} \mathcal{O}_{S\times N}$ déduit de $\mathcal{L}_{|S\times N} \xrightarrow{\sim} \mathcal{O}_{S\times N}$ et $\mathcal{L}_{0|N} \xrightarrow{\sim} \mathcal{O}_N$] est un chtouca [resp. avec structure de niveau N] sur S.

Réciproquement, considérons deux chtoucas $\mathcal{L}$ et $\mathcal{L}'$ sur un schéma S qui ont le même zéro 0 et le même pôle ∞. Alors

$$\mathcal{L}_0 = \mathcal{L}' \otimes \mathcal{L}^{-1}$$

est muni d'un isomorphisme

$${}^\tau\mathcal{L}_0 \xrightarrow{\sim} \mathcal{L}_0\,,$$

autrement dit définit un point du fixateur de Frob dans $\mathcal{P}ic_X$. D'après le lemme IV.3(ii), si S est connexe, $\mathcal{L}_0$ provient d'un élément de $\mathcal{P}ic_X(\mathbb{F}_q)$.

De plus, si les chtoucas $\mathcal{L}$ et $\mathcal{L}'$ sont munis de structures de niveau N, le fibré inversible $\mathcal{L}_0$ sur $S \times X$ est muni d'une structure de niveau N compatible avec Frob_S, autrement dit définit un point du fixateur de Frob dans $\mathcal{P}ic_{X,N}$. Si S est connexe, $\mathcal{L}_0$ provient donc d'un élément de l'ensemble $\mathcal{P}ic_{X,N}(\mathbb{F}_q)$.

□

D'après ce lemme, le groupe $\mathcal{P}ic_X^0(\mathbb{F}_q) = \mathcal{J}ac_X(\mathbb{F}_q)$ agit sur chaque schéma $\mathrm{Cht}_X^{1,d}$ sur $X \times X$, et son action sur les fibres est simplement transitive. Or, comme $\mathcal{P}ic_X^0 = \mathcal{J}ac_X$ est un schéma de type fini d'après la proposition IV.13(i), le groupe abélien $\mathcal{P}ic_X^0(\mathbb{F}_q)$ est fini. Donc les fibres non vides de chaque $\mathrm{Cht}_X^{1,d}$, $d \in \mathbb{Z}$, au-dessus de $X \times X$ sont finies et ont toutes le même cardinal.

Comme le schéma $\mathcal{P}ic_{X,N}$ est de type fini sur $\mathcal{P}ic_X$, le noyau de l'homomorphisme surjectif

$$\mathcal{P}ic_{X,N}(\mathbb{F}_q) \to \mathcal{P}ic_X(\mathbb{F}_q)$$

est fini. Par conséquent, les fibres non vides de chaque $\mathrm{Cht}_{X,N}^{1,d}$, $d \in \mathbb{Z}$, au-dessus de $(X-N)\times(X-N)$ sont également finies et ont toutes le même cardinal.

En fait, on a :

Proposition IV.19. –

Considérant toujours la courbe X sur $\mathbb{F}_q$, on a :

(i) *Pour tout $d \in \mathbb{Z}$, le schéma*

$$\mathrm{Cht}_X^{1,d}$$

définit un revêtement fini étale de $X \times X$.

(ii) *De même, pour tout niveau $N \hookrightarrow X$ et tout $d \in \mathbb{Z}$, le schéma*

$$\mathrm{Cht}_{X,N}^{1,d}$$

définit un revêtement fini étale de $(X-N)\times(X-N)$.

Démonstration :

Il suffit de démontrer que, pour tout degré $d \in \mathbb{Z}$, le morphisme

$$\begin{array}{rcl} \mathcal{L} & \mapsto & {}^{\tau}\mathcal{L} \otimes \mathcal{L}^{-1} = \mathrm{Frob}\,(\mathcal{L}) \otimes \mathcal{L}^{-1} \\ \mathcal{P}ic_X^d & \to & \mathcal{P}ic_X^0 \\ \text{[resp.} \quad \mathcal{P}ic_{X,N}^d & \to & \mathcal{P}ic_{X,N}^0 \ ] \end{array}$$

est fini et étale.

Comme $\mathcal{L} \mapsto {}^{\tau}\mathcal{L} \otimes \mathcal{L}^{-1}$ est un homomorphisme et les $\mathcal{P}ic_X^d$ [resp. $\mathcal{P}ic_{X,N}^d$] sont des translatés de $\mathcal{P}ic_X^0$ [resp. $\mathcal{P}ic_{X,N}^0$], il suffit de traiter le cas où $d = 0$. Dans ce cas, $\mathcal{L} \mapsto {}^{\tau}\mathcal{L} \otimes \mathcal{L}^{-1}$ est un endomorphisme du schéma en groupes abéliens $\mathcal{P}ic_X^0 = \mathcal{J}ac_X$ [resp. $\mathcal{P}ic_{X,N}^0$] qui est de type fini sur $\mathbb{F}_q$.

Pour montrer qu'il est non ramifié, il suffit de montrer que ses fibres au-dessus des points sont non ramifiées sur ces points. Pour cela, il suffit de montrer que la fibre au-dessus du point unité est non ramifiée. Or cette fibre s'identifie au schéma des points fixes de Frob. Elle est non ramifiée d'après le lemme IV.3(ii).

En particulier, toutes les fibres non vides de $\mathcal{L} \mapsto {}^{\tau}\mathcal{L} \otimes \mathcal{L}^{-1}$ dans $\mathcal{P}ic_X^0 = \mathcal{J}ac_X$ [resp. $\mathcal{P}ic_{X,N}^0$] sont finies de même cardinal.

D'après la proposition IV.13(i), $\mathcal{J}ac_X$ est un schéma projectif, donc propre, et connexe. L'image de $\mathcal{L} \mapsto {}^{\tau}\mathcal{L} \otimes \mathcal{L}^{-1}$ dans $\mathcal{J}ac_X$ est un sous-schéma fermé qui a la même dimension que $\mathcal{J}ac_X$. Donc cette image est $\mathcal{J}ac_X$ tout entier.

De plus, $\mathcal{L} \mapsto {}^{\tau}\mathcal{L} \otimes \mathcal{L}^{-1}$ est également surjectif dans $\mathcal{P}ic_{X,N}^0$. Pour le voir, il suffit d'après le lemme IV.14(i) de vérifier que pour corps $K \supset \mathbb{F}_q$ et tout élément $a \in (K \otimes_{\mathbb{F}_q} \mathcal{O}_N)^\times$, il existe une extension (finie) $K' \supset K$ et un élément $a' \in (K' \otimes_{\mathbb{F}_q} \mathcal{O}_N)^\times$ tel que

$$(\mathrm{Frob}_{K'} \otimes \mathrm{Id}_{\mathcal{O}_N})(a') \cdot a'^{-1} = a\,.$$

On peut supposer que N est supporté par un seul point fermé x de X, avec donc $\mathcal{O}_N = \mathcal{O}_{x,X}/(\varpi_x^n)$, et que K contient le corps résiduel κ_x de x. On raisonne par récurrence sur n. Si $n = 1$, on est réduit à résoudre l'équation

$$T^{q-1} = a$$

qui définit une extension (finie séparable) K' de K. Et si $n \geq 2$, on peut supposer que a est de la forme

$$a = \varpi_x^{n-1} \cdot b \quad \text{avec} \quad b \in K'\,.$$

On cherche alors une solution de la forme $a' = \varpi_x^{n-1} \cdot b'$ et on est réduit à résoudre l'équation

$$T^q - T = b$$

qui définit encore une extension (finie séparable) K' de K.

La fibre du morphisme $\mathcal{L} \mapsto {}^\tau\mathcal{L} \otimes \mathcal{L}^{-1}$ au-dessus du point générique de $\mathcal{P}ic_X^0$ [resp. $\mathcal{P}ic_{X,N}^0$] est finie et étale. Comme ce morphisme est de type fini, il est fini et étale au-dessus d'un voisinage ouvert du point générique, c'est-à-dire au-dessus d'un ouvert non vide. Mais comme c'est un homomorphisme de groupes abéliens et qu'il est surjectif, il est fini et étale au-dessus d'un voisinage ouvert de tout point de $\mathcal{P}ic_X^0$ [resp. $\mathcal{P}ic_{X,N}^0$]. C'est un revêtement (fini) étale.

□

Ainsi, le schéma

$$\mathrm{Cht}_X^1 = \coprod_{d \in \mathbb{Z}} \mathrm{Cht}_X^{1,d} \qquad [\text{resp.} \quad \mathrm{Cht}_{X,N}^1 = \coprod_{d \in \mathbb{Z}} \mathrm{Cht}_{X,N}^{1,d}\ ]$$

est une réunion disjointe de revêtements finis étales de $X \times X$ [resp. $(X - N) \times (X - N)$] et il est muni d'une action du groupe discret $\mathcal{P}ic_X(\mathbb{F}_q)$ [resp. $\mathcal{P}ic_{X,N}(\mathbb{F}_q)$] qui est simplement transitive sur toutes les fibres au-dessus des points géométriques.

Si donc $\overline{s}$ est un point géométrique de $X \times X$ [resp. $(X - N) \times (X - N)$], il correspond à ce schéma un ensemble discret (infini mais écrit comme une réunion disjointe indexée par $\mathbb{Z}$ d'ensembles finis) muni d'une action continue de

$$\pi_1(X \times X, \overline{s}) \qquad [\text{resp.} \ \ \pi_1((X - N) \times (X - N), \overline{s})\ ]$$

et d'une action simplement transitive de $\mathcal{P}ic_X(\mathbb{F}_q)$ [resp. $\mathcal{P}ic_{X,N}(\mathbb{F}_q)$] qui commute avec la précédente.

De plus, on a :

Lemme IV.20. –

Soit $x = (0, \infty)$ un point de $X \times X$ [resp. $(X - N) \times (X - N)$] défini dans une extension $\mathbb{F}_{q^n}$ de $\mathbb{F}_q$, et soit $\overline{s}$ un point géométrique de $X \times X$ au-dessus de x.

Soient n_0 et n_∞ les degrés de $\mathbb{F}_{q^n}$ sur les corps résiduels κ_0 et κ_∞ de 0 et ∞.

Alors l'élément de Frobenius

$$\sigma_x \in \pi_1(X \times X, \overline{s}) \qquad [\text{resp.} \quad \sigma_x \in \pi_1((X - N) \times (X - N), \overline{s})\ ]$$

agit sur la fibre au-dessus de $\overline{s}$ de

$$\mathrm{Cht}_X^1 \qquad [\text{resp.} \quad \mathrm{Cht}_{X,N}^1\ ]$$

comme l'élément

$$\mathcal{O}_X(n_0 \cdot 0 - n_\infty \cdot \infty) = \mathcal{O}_X(0)^{\otimes n_0} \otimes \mathcal{O}_X(-\infty)^{\otimes n_\infty}$$

du groupe $\mathcal{P}ic_X(\mathbb{F}_q)$ [resp. $\mathcal{P}ic_{X,N}(\mathbb{F}_q)$].

Démonstration :

On peut supposer que le point géométrique $\overline{s} = (\overline{0}, \overline{\infty})$ est à valeurs dans une clôture algébrique $\overline{\mathbb{F}}_q$ de $\mathbb{F}_q$.

Les chtoucas [resp. avec structure de niveau N] au-dessus de ce point sont les fibrés inversibles [resp. avec structures de niveau N] $\mathcal{L}$ sur $\overline{X} = X \otimes_{\mathbb{F}_q} \overline{\mathbb{F}}_q$ munis d'un isomorphisme

$$(\mathrm{Frob}_{\overline{\mathbb{F}}_q} \otimes \mathrm{Id}_X)^*(\mathcal{L}) = {}^\tau\mathcal{L} \xrightarrow{\sim} \mathcal{L}(\overline{0} - \overline{\infty}) = \mathcal{L} \otimes_{\mathcal{O}_{\bar{X}}} \mathcal{O}_{\bar{X}}(\overline{0} - \overline{\infty})\,.$$

L'élément de Frobenius $\sigma_x = \mathrm{Frob}^n_{\mathbb{F}_q}$ agit sur cette fibre comme le fibré inversible [resp. avec structure de niveau] sur X

$$\mathcal{O}_X(n_0 \cdot 0 - n_\infty \cdot \infty)$$

puisque, sur $\overline{X}$, celui-ci devient isomorphe à

$$\mathcal{O}_{\bar{X}}(n \cdot \overline{0} - n \cdot \overline{\infty}) = \mathcal{O}_{\bar{X}}(\overline{0} - \overline{\infty})^{\otimes n}\,.$$

□

Or on a encore :

Lemme IV.21. –

(i) *Si x décrit l'ensemble des points fermés de X [resp. $X - N$], les fibrés inversibles [resp. avec structure de niveau N]*

$$\mathcal{O}_X(x)$$

engendrent le groupe $\mathcal{P}ic_X(\mathbb{F}_q)$ [resp. $\mathcal{P}ic_{X,N}(\mathbb{F}_q)$].

(ii) *Sous les mêmes conditions, les entiers*

$$\deg(x) = \dim_{\mathbb{F}_q}(\kappa_x)$$

sont globalement premiers entre eux, c'est-à-dire engendrent $\mathbb{Z}$.

(iii) *Si $x = (0, \infty)$ décrit l'ensemble des points fermés de $X \times X$ [resp. $(X - N) \times (X - N)$], en notant $n_0 = \dim_{\kappa_0} \kappa_x$ et $n_\infty = \dim_{\kappa_\infty} \kappa_x$, les fibrés inversibles [resp. avec structures de niveau N]*

$$\mathcal{O}_X(n_0 \cdot 0 - n_\infty \cdot \infty)$$

engendrent le groupe $\mathcal{P}ic^0_X(\mathbb{F}_q)$ [resp. $\mathcal{P}ic^0_{X,N}(\mathbb{F}_q)$].

Démonstration :

(i) résulte de ce que tout fibré inversible [resp. avec structure de niveau N] sur X possède une section rationnelle non nulle [resp. et qui est bien définie au voisinage des points de N et s'envoie sur l'élément 1 de $\mathcal{O}_N$].

(ii) D'après (i), il s'agit de prouver que $\mathcal{P}ic^1_X$ [resp. $\mathcal{P}ic^1_{X,N}$] possède au moins un point défini sur $\mathbb{F}_q$. Il possède en tout cas un point $\mathcal{L}_1$ défini sur $\overline{\mathbb{F}}_q$. Alors ${}^\tau\mathcal{L}_1$ est également de degré 1, et ${}^\tau\mathcal{L}_1 \otimes \mathcal{L}_1^{-1}$ est de degré 0. Comme l'endomorphisme $\mathcal{L} \mapsto {}^\tau\mathcal{L} \otimes \mathcal{L}^{-1}$ de $\mathcal{P}ic^0_X$ [resp. $\mathcal{P}ic^0_{X,N}$] est surjectif, il existe un point $\mathcal{L}_0$ de $\mathcal{P}ic^0_X$ [resp. $\mathcal{P}ic^0_{X,N}$] défini sur $\overline{\mathbb{F}}_q$ tel que

$${}^\tau\mathcal{L}_1 \otimes \mathcal{L}_1^{-1} \cong {}^\tau\mathcal{L}_0 \otimes \mathcal{L}_0^{-1}\,.$$

Alors $\mathcal{L}_1 \otimes \mathcal{L}_0^{-1}$ est un fibré de rang 1 muni d'un isomorphisme avec ${}^\tau(\mathcal{L}_1 \otimes \mathcal{L}_0^{-1})$, ce qui signifie qu'il est défini sur $\mathbb{F}_q$.

(iii) résulte de (i) et (ii) puisque, pour chaque $x = (0, \infty)$, $\dim_{\mathbb{F}_q} \kappa_x = \deg(x)$ est le plus petit commun multiple de $\dim_{\mathbb{F}_q} \kappa_0 = \deg(0)$ et $\dim_{\mathbb{F}_q} \kappa_\infty = \deg(\infty)$.

□

On déduit des deux lemmes précédents :

Corollaire IV.22. –

Les revêtements finis étales

$$\mathrm{Cht}_X^{1,d} \qquad \textit{[resp. } \mathrm{Cht}_{X,N}^{1,d}\textit{]}, \quad d \in \mathbb{Z},$$

de $X \times X$ *[resp.* $(X-N) \times (X-N)$*] sont tous connexes.*

Ils définissent un même homomorphisme continu surjectif

$$\pi_1(X \times X, \overline{s}) \to \mathcal{P}ic_X^0(\mathbb{F}_q)$$

[resp.

$$\pi_1((X-N) \times (X-N), \overline{s}) \to \mathcal{P}ic_{X,N}^0(\mathbb{F}_q)\,]$$

pour n'importe quel point géométrique $\overline{s}$ *de* $X \times X$ *[resp.* $(X-N) \times (X-N)$*].*

Démonstration :

Soit $\overline{s}$ un point géométrique de $X \times X$ [resp. $(X-N) \times (X-N)$].

Considérons tous les éléments de Frobenius σ_x dans $\pi_1(X \times X, \overline{s})$ [resp. $\pi_1((X-N) \times (X-N), \overline{s})$] associés aux points fermés $x = (0, \infty)$ de $X \times X$ [resp. $(X-N) \times (X-N)$].

D'après les lemmes IV.20 et IV.21, leurs actions sur la fibre $\mathrm{Cht}_X^{1,d}(\overline{s})$ [resp. $\mathrm{Cht}_{X,N}^{1,d}(\overline{s})$] sont les mêmes que celles d'éléments du groupe $\mathcal{P}ic_X^0(\mathbb{F}_q)$ [resp. $\mathcal{P}ic_{X,N}^0(\mathbb{F}_q)$] qui engendrent ce groupe.

D'après le lemme IV.18(ii), cela implique que l'action de $\pi_1(X \times X, \overline{s})$ [resp. $\pi_1((X-N) \times (X-N), \overline{s})$] sur la fibre $\mathrm{Cht}_X^{1,d}(\overline{s})$ [resp. $\mathrm{Cht}_{X,N}^{1,d}(\overline{s})$] est transitive, autrement dit que $\mathrm{Cht}_X^{1,d}$ [resp. $\mathrm{Cht}_{X,N}^{1,d}$] est un revêtement fini étale connexe de $X \times X$ [resp. $(X-N) \times (X-N)$].

On conclut d'après le lemme IV.18(i) combiné avec la remarque qui suit le théorème II.28. □

4 Retour de la surface $X \times X$ à la courbe X

Considérons d'abord de manière générale deux schémas X_1 et X_2 de type fini et géométriquement connexes sur $\mathbb{F}_q$. Ainsi, $X_1 \times X_2 = X_1 \times_{\mathrm{Spec}(\mathbb{F}_q)} X_2$ est aussi de type fini et géométriquement connexe sur $\mathbb{F}_q$.

Pour tout point géométrique $\overline{x} = (\overline{x}_1, \overline{x}_2)$ de $X_1 \times X_2$, on a un carré commutatif :

$$\begin{tikzcd}
\pi_1(X_1 \times X_2, \overline{x}) \arrow[r] \arrow[d] & \pi_1(X_1, \overline{x}_1) \arrow[d] \\
\pi_1(X_2, \overline{x}_2) \arrow[r] & \pi_1(\mathrm{Spec}\,(\mathbb{F}_q)) = \Gamma_{\mathbb{F}_q} = \widehat{\mathbb{Z}}
\end{tikzcd}$$

De plus, on a :

Lemme IV.23. –

Soient comme ci-dessus X_1 *et* X_2 *deux schémas de type fini et géométriquement connexes sur* $\mathbb{F}_q$.

Les deux endomorphismes $(\mathrm{Frob}_{X_1} \times \mathrm{Id}_{X_2})$ *et* $(\mathrm{Id}_{X_1} \times \mathrm{Frob}_{X_2})$ *de* $X_1 \times X_2$ *induisent deux automorphismes de*

$$\pi_1(X_1 \times X_2, \overline{x})$$

qui sont inverses l'un de l'autre et sont compatibles avec chacune des deux projections

$$\pi_1(X_1 \times X_2, \overline{x}) \rightrightarrows \pi_1(X_1, \overline{x}_1),\ \pi_2(X_2, \overline{x}_2)\,.$$

Démonstration :

Cela résulte de ce que, d'après le corollaire IV.4(ii), l'endomorphisme $\mathrm{Frob}_{X_1} \times \mathrm{Frob}_{X_2}$ de $X_1 \times X_2$ induit l'identité de $\pi_1(X_1 \times X_2, \overline{x})$ et, de même, les endomorphismes Frob_{X_1} et Frob_{X_2} de X_1 et X_2 induisent l'identité de $\pi_1(X_1, \overline{x}_1)$ et $\pi_2(X_2, \overline{x}_2)$.

□

Nous allons utiliser les deux définitions suivantes de théorie des groupes :

Définition IV.24. –

(i) *Si G et H sont deux groupes munis d'un homomorphisme*

$$\alpha : G \to \mathrm{Aut}\,(H)$$

d'action de G sur H, on appelle "produit semi-direct de G par H" et on note

$$H \rtimes G$$

le groupe constitué des couples (h, g), $h \in H$, $g \in G$, avec la loi de multiplication

$$(h_1, g_1) \cdot (h_2, g_2) = (h_1 \cdot \alpha(g_1)(h_2), g_1 \cdot g_2)\,.$$

Il s'inscrit dans une suite exacte

$$1 \to H \to H \rtimes G \to G \to 1\,.$$

(ii) *Si G est un groupe topologique, on note $\widehat{G}$ sa "complétion profinie", définie comme la limite projective filtrante*

$$\widehat{G} = \varprojlim_i G/G_i = \{(g_i \in G/G_i) \mid g_i \mapsto g_j \quad si \quad G_i \subset G_j\}$$

des quotients G/G_i de G par ses sous-groupes ouverts distingués d'indice fini.

Remarque :

Dans la sitution de (ii), $\widehat{G}$ est un groupe profini. Il est universel au sens que, pour tout groupe profini H, se donner un homomorphisme continu $G \to H$ équivaut à se donner un homomorphisme continu $\widehat{G} \to H$.

□

Dans la situation du lemme IV.23, l'automorphisme de $\pi_1(X_1 \times X_2, \overline{x})$ défini par $\mathrm{Frob}_{X_1} \times \mathrm{Id}_{X_2}$ induit une action de $\mathbb{Z}$ sur ce groupe, ce qui permet de définir le produit semi-direct

$$\pi_1(X_1 \times X_2, \overline{x}) \rtimes \mathbb{Z}\,.$$

Il est muni d'un morphisme naturel vers le produit

$$\pi_1(X_1, \overline{x}_1) \times \pi_2(X_2, \overline{x}_2)\,.$$

Nous allons prouver :

Proposition IV.25. –

Considérons comme dans le lemme IV.23 *deux schémas X_1 et X_2 de type fini et géométriquement connexes sur $\mathbb{F}_q$.*

Alors, pour tout point géométrique $\overline{x} = (\overline{x}_1, \overline{x}_2)$ de $X_1 \times X_2$, le produit

$$\pi_1(X_1, \overline{x}_1) \times \pi_2(X_2, \overline{x}_2)$$

s'identifie à la complétion profinie du produit semi-direct

$$\pi_1(X_1 \times X_2, \overline{x}) \rtimes \mathbb{Z}\,.$$

Remarque :

Si, comme au paragraphe précédent, X est une courbe propre et lisse sur $\mathbb{F}_q$, donc projective, et telle que $\mathcal{O}_X(X) = \mathbb{F}_q$, cette proposition s'applique en particulier à $X_1 = X_2 = X$.

Elle s'applique également à $X_1 = X_2 = X - N$ pour tout sous-schéma fermé fini $N \hookrightarrow X$.

Ce sont les cas qui nous intéressent.

Démonstration :

La proposition résulte du lemme suivant :

Lemme IV.26. –

Tout revêtement étale Y de $X_1 \times X_2$ muni de deux endomorphismes $\mathrm{Frob}_{Y,1}$ et $\mathrm{Frob}_{Y,2}$ au-dessus de $\mathrm{Frob}_{X_1} \times \mathrm{Id}_{X_2}$ et $\mathrm{Id}_{X_2} \times \mathrm{Frob}_{X_1}$ s'écrit de manière unique comme une réunion disjointe de produits $X_1' \times X_2'$ de revêtements étales connexes X_1' et X_2' de X_1 et X_2.

Démonstration :

Considérons n'importe quel sous-schéma fermé

$$Z \hookrightarrow X_1 \times X_2$$

qui

- contient le point géométrique $\overline{x} = (\overline{x}_1, \overline{x}_2)$,
- est respecté par les endomorphismes $\mathrm{Frob}_{X_1} \times \mathrm{Id}_{X_2}$ et $\mathrm{Id}_{X_1} \times \mathrm{Frob}_{X_2}$,
- est un "croisillon" au sens que son support est la réunion de

  $$X_1 \times N_2 \qquad \text{et} \qquad N_1 \times X_2$$

  où N_1 et N_2 sont deux sous-schémas fermés finis non vides de X_1 et X_2.

On remarque que Z est géométriquement connexe sur $\mathbb{F}_q$.

Si Y est un revêtement étale de $X_1 \times X_2$, sa restriction $Y \times_{X_1 \times X_2} Z$ au-dessus de Z devient triviale après changement de base par des revêtements étales de X_1 et X_2 convenables. Autrement dit, $Y \times_{X_1 \times X_2} Z$ se plonge dans la réunion disjointe d'un ensemble fini de revêtements étales de la forme

$$(X_1' \times X_2') \times_{X_1 \times X_2} Z$$

associés à des revêtements étales connexes X_1' et X_2' de X_1 et X_2.

Or, comme Z est géométriquement connexe, les endomorphismes $\mathrm{Frob}_{X_1'} \times \mathrm{Id}_{X_2'}$ et $\mathrm{Id}_{X_1'} \times \mathrm{Frob}_{X_2'}$ agissent transitivement sur l'ensemble des composantes connexes de chaque revêtement étale produit $(X_1' \times X_2') \times_{X_1 \times X_2} Z$ dès lors que les facteurs X_1' et X_2' sont connexes.

Par conséquent, $Y \times_{(X_1 \times X_2)} Z$ muni des endomorphismes $\mathrm{Frob}_{Y,1}$ et $\mathrm{Frob}_{Y,2}$ s'écrit canoniquement comme une réunion disjointe finie de revêtements $(X_1' \times X_2') \times_{X_1 \times X_2} Z$ induits par des revêtements étales connexes X_1' et X_2' de X_1 et X_2.

Cette décomposition ne dépend pas du choix du croisillon Z.

Notons Y' le revêtement étale de $X_1 \times X_2$ défini comme la réunion disjointe des $X'_1 \times X'_2$. Ainsi, Y et Y' sont canoniquement isomorphes au-dessus de tout croisillon Z de $X_1 \times X_2$.

Il existe un revêtement étale connexe galoisien W de $X_1 \times X_2$ tels que les revêtements étales Y et Y' deviennent triviaux au-dessus de W.

Puis il existe un unique isomorphisme de $Y \times_{X_1 \times X_2} W$ et $Y' \times_{X_1 \times X_2} W$ compatible avec celui de $Y \times_{X_1 \times X_2} Z$ et $Y' \times_{X_1 \times X_2} Z$ au-dessus de tout croisillon Z, au sens qu'ils coïncident au-dessus de tout revêtement étale connexe de Z qui se factorise à travers W.

Alors cet isomorphisme de Y et Y' défini au-dessus de W est nécessairement fixé par le groupe des automorphismes de W. Il provient d'un isomorphisme de Y et Y' défini au-dessus de $X_1 \times X_2$.

Cela achève la preuve du lemme IV.26 et donc aussi de la proposition IV.25. $\square$

La proposition IV.25 s'applique dans le contexte des chtoucas de Drinfeld du fait de la structure supplémentaire suivante des schémas classifiant les chtoucas :

Lemme IV.27. –

Les foncteurs

$$(\mathcal{L},\, {}^\tau\mathcal{L} \cong \mathcal{L}(0-\infty)) \mapsto (\mathcal{L}(0),\, {}^\tau\mathcal{L}(0) \cong \mathcal{L}(0)(\mathrm{Frob}(0)-\infty))$$

et

$$(\mathcal{L},\, {}^\tau\mathcal{L} \cong \mathcal{L}(0-\infty)) \mapsto (\mathcal{L}(-\infty),\, {}^\tau\mathcal{L}(-\infty) \cong \mathcal{L}(-\infty)(0-\mathrm{Frob}(\infty))$$

définissent deux endomorphismes Frob_1 *et* Frob_2 *du schéma classifiant*

$$\mathrm{Cht}_X^1 \qquad \textit{[resp.} \quad \mathrm{Cht}_{X,N}^1 \textit{]}$$

au-dessus des endomorphismes $\mathrm{Frob}_X \times \mathrm{Id}_X$ *et* $\mathrm{Id}_X \times \mathrm{Frob}_X$ *de* $X \times X$ *[resp.* $(X-N)\times(X-N)$*].*

Remarques :

(i) Il est immédiat que le composé de Frob_1 et Frob_2 dans un sens ou dans l'autre est l'endomorphisme de Frobenius de Cht_X^1 ou $\mathrm{Cht}_{X,N}^1$.

(ii) On observe que Frob_1 envoie chaque $\mathrm{Cht}_X^{1,d}$ dans $\mathrm{Cht}_X^{1,d+1}$ et que Frob_2 envoie chaque $\mathrm{Cht}_X^{1,d}$ dans $\mathrm{Cht}_X^{1,d-1}$.

$\square$

On en déduit :

Corollaire IV.28. –

Si $\overline{s} = (\overline{0}, \overline{\infty})$ *est un point géométrique de* $X \times X$ *[resp.* $(X-N)\times(X-N)$*], on a :*

(i) *Les endomorphismes* Frob_1 *et* Frob_2 *de* Cht_X^1 *[resp.* $\mathrm{Cht}_{X,N}^1$*] induisent un homomorphisme*

$$\pi_1(X \times X, \overline{s}) \rtimes \mathbb{Z} \to \mathcal{P}ic_X(\mathbb{F}_q)$$

[resp.

$$\pi_1((X-N)\times(X-N), \overline{s}) \rtimes \mathbb{Z} \to \mathcal{P}ic_{X,N}(\mathbb{F}_q) \textit{]}.$$

(ii) *En passant aux complétions profinies, ils induisent un homomorphisme*

$$\pi_1(X, \overline{0}) \times \pi_1(X, \overline{\infty}) \to \widehat{\mathcal{P}ic_X(\mathbb{F}_q)}$$

[resp.

$$\pi_1(X-N, \overline{0}) \times \pi_1(X-N, \overline{\infty}) \to \widehat{\mathcal{P}ic_{X,N}(\mathbb{F}_q)} \textit{]}.$$

(iii) *L'échange des deux facteurs X [resp. $X - N$] transforme cet homomorphisme en son opposé.*

(iv) *Pour tous points fermés 0 et ∞ de X [resp. $X - N$], cet homomorphisme envoie les éléments de Frobenius σ_0 et σ_∞ sur $\mathcal{O}_X(0)$ et $\mathcal{O}_X(-\infty)$.*

Remarque :

Les groupes $\mathcal{P}ic^0_X(\mathbb{F}_q)$ et $\mathcal{P}ic^0_{X,N}(\mathbb{F}_q)$ sont toujours finis, si bien que les suites exactes

$$0 \longrightarrow \mathcal{P}ic^0_X(\mathbb{F}_q) \longrightarrow \mathcal{P}ic_X(\mathbb{F}_q) \xrightarrow{\deg} \mathbb{Z} \longrightarrow 0\,,$$

$$0 \longrightarrow \mathcal{P}ic^0_{X,N}(\mathbb{F}_q) \longrightarrow \mathcal{P}ic_{X,N}(\mathbb{F}_q) \xrightarrow{\deg} \mathbb{Z} \longrightarrow 0$$

induisent des suites exactes

$$0 \longrightarrow \mathcal{P}ic^0_X(\mathbb{F}_q) \longrightarrow \widehat{\mathcal{P}ic_X(\mathbb{F}_q)} \longrightarrow \widehat{\mathbb{Z}} \longrightarrow 0\,,$$

$$0 \longrightarrow \mathcal{P}ic^0_{X,N}(\mathbb{F}_q) \longrightarrow \widehat{\mathcal{P}ic_{X,N}(\mathbb{F}_q)} \longrightarrow \widehat{\mathbb{Z}} \longrightarrow 0\,.$$

Démonstration :

(i) résulte de ce que $\mathcal{P}ic_X(\mathbb{F}_q)$ [resp. $\mathcal{P}ic_{X,N}(\mathbb{F}_q)$] agit simplement transitivement sur les fibres géométriques de Cht^1_X [resp. $\mathrm{Cht}^1_{X,N}$].

(ii) résulte de la proposition IV.25.

(iii) résulte de ce que le foncteur

$$(\mathcal{L},\, {}^\tau\mathcal{L} \cong \mathcal{L}(0-\infty)) \mapsto (\mathcal{L}^{-1},\, {}^\tau\mathcal{L}^{-1} \cong \mathcal{L}^{-1}(\infty - 0))$$

définit un automorphisme du schéma classifiant Cht^1_X [resp. $\mathrm{Cht}^1_{X,N}$] au-dessus de l'automorphisme de permutation des 2 facteurs X [resp. $X - N$].

(iv) résulte du lemme IV.20 complété par le lemme IV.21(ii).

$\square$

Ainsi, l'étude des revêtements étales de $X \times X$ ou $(X-N)\times(X-N)$ fournis par les schémas classifiants les chtoucas de Drinfeld de rang 1 a permis de démontrer :

Théorème IV.29. –

Si $\overline{x}$ est un point géométrique de X [resp. de $X - N$], les chtoucas définissent un homomorphisme continu surjectif

$$\pi_1(X, \overline{x}) \longrightarrow \widehat{\mathcal{P}ic_X(\mathbb{F}_q)}$$

[resp.

$$\pi_1(X - N, \overline{x}) \longrightarrow \widehat{\mathcal{P}ic_{X,N}(\mathbb{F}_q)}$$

et donc

$$\pi_1(X - N, \overline{x}) \longrightarrow \varprojlim_{\substack{N' \hookrightarrow X \\ X - N' = X - N}} \widehat{\mathcal{P}ic_{X,N'}(\mathbb{F}_q)}\ ],$$

tel que :

- *cet homomorphisme est compatible avec les projections sur le groupe de Galois de $\mathbb{F}_q$ identifié à $\widehat{\mathbb{Z}}$,*
- *pour tout point fermé x de X [resp. $X - N$], cet homomorphisme envoie les éléments de Frobenius σ_x sur $\mathcal{O}_X(x)$.*

$\square$

Remarque :

Si F est le corps des fonctions de X et $\overline{F}$ une clôture algébrique de F, on a un homomorphisme continu surjectif induit

$$\Gamma_F = \mathrm{Aut}_F(\overline{F}) \longrightarrow \lim_{N \hookrightarrow X} \widehat{\mathcal{P}ic_{X,N}}(\mathbb{F}_q)\,.$$

Il est compatible avec les projections sur $\widehat{\mathbb{Z}}$. □

Nous allons considérer maintenant non plus une mais deux courbes reliées par un morphisme fini et plat. On a d'abord le lemme suivant qui complète le lemme IV.15 :

Lemme IV.30. –

Soient X et X' deux courbes projectives et lisses sur un corps K, connexes et reliées par un morphisme

$$X' \to X$$

qui est non constant, donc est fini et plat [resp. ainsi que deux niveaux $N \hookrightarrow X$, $N' \hookrightarrow X'$ tels que $N \times_X X' \hookrightarrow N'$].

Alors le carré

$$\begin{tikzcd} X' \arrow[r] \arrow[d] & \mathcal{P}ic_{X'} \arrow[d, "\det"] \\ X \arrow[r] & \mathcal{P}ic_X \end{tikzcd} \qquad \textit{[resp.} \quad \begin{tikzcd} X' - N' \arrow[r] \arrow[d] & \mathcal{P}ic_{X',N'} \arrow[d, "\det"] \\ X - N \arrow[r] & \mathcal{P}ic_{X,N} \end{tikzcd} \quad \textit{]},$$

dessiné par les morphismes $x' \mapsto \mathcal{O}_{X'}(-x')$ et $x \mapsto \mathcal{O}_X(-x)$ est commutatif.

Démonstration :

L'égalité des deux morphismes composés $X' \rightrightarrows \mathcal{P}ic_X$ [resp. $X' - N' \rightrightarrows \mathcal{P}ic_{X,N}$] définit un sous-schéma fermé de X' [resp. $X' - N'$].

Pour démontrer qu'il est égal à tout, il suffit de prouver qu'il contient tous les points géométriques.

Or, si $\overline{x}'$ est un point géométrique de X' à coefficients dans un corps algébriquement clos $\overline{K}$ et $\overline{X}' = X \otimes_K \overline{K}$, $\overline{X} = X \otimes_K \overline{K}$, le foncteur det transforme le plongement

$$\mathcal{O}_{\bar{X}'}(-\overline{x}') \hookrightarrow \mathcal{O}_{\bar{X}'}$$

en

$$\mathcal{O}_{\bar{X}}(-\overline{x}) \hookrightarrow \mathcal{O}_{\bar{X}}$$

si $\overline{x}$ désigne l'image de $\overline{x}'$ par $\overline{X}' \to \overline{X}$. □

On déduit de ce lemme :

Corollaire IV.31. –

Soient X et X' deux courbes projectives, lisses et géométriquement connexes sur deux corps finis $\mathbb{F}_q$ et $\mathbb{F}_{q'}$, reliées par un plongement de leurs corps de fonctions

$$F_X \hookrightarrow F_{X'}\,, \quad \textit{avec donc} \quad \mathbb{F}_q \hookrightarrow \mathbb{F}_{q'}\,,$$

ou, ce qui revient au même, par un morphisme fini et plat

$$X' \to X\,.$$

Alors :

(i) *Le morphisme* $\det : \mathcal{P}ic_{X'} \to \mathcal{P}ic_X$ *induit un morphisme*

$$\mathrm{Cht}^1_{X'} \xrightarrow{\det} \mathrm{Cht}^1_X$$

au-dessus de $X' \times X' \to X \times X$.

(ii) *Si* $N \hookrightarrow X$ *et* $N' \hookrightarrow X'$ *sont deux niveaux tels que* $N \times_X X' \hookrightarrow N'$, *le morphisme* $\det : \mathcal{P}ic_{X',N'} \to \mathcal{P}ic_{X,N}$ *induit un morphisme*

$$\mathrm{Cht}^1_{X',N'} \xrightarrow{\det} \mathrm{Cht}^1_{X,N}$$

au-dessus de $\mathrm{Cht}^1_{X'} \to \mathrm{Cht}^1_X$.

□

Comme les morphismes det commutent avec les endomorphismes de Frobenius partiels Frob_1 et Frob_2 des schémas classifiants de chtoucas, on obtient :

Corollaire IV.32. –

(i) *Dans la situation du corollaire* IV.31(i) *ci-dessus, et si* $\overline{x}'$ *est un point géométrique de* X', *on a un carré commutatif :*

$$\begin{tikzcd}
\pi_1(X', \overline{x}') \arrow[r] \arrow[d] & \widehat{\mathcal{P}ic_{X'}(\mathbb{F}_{q'})} \arrow[d, "\det"] \\
\pi_1(X, \overline{x}') \arrow[r] & \widehat{\mathcal{P}ic_X(\mathbb{F}_q)}
\end{tikzcd}$$

(ii) *Dans la situation du corollaire* IV.31(ii) *ci-dessus, et si* $\overline{x}'$ *est un point géométrique de* X', *on a un carré commutatif*

$$\begin{tikzcd}
\pi_1(X' - N', \overline{x}') \arrow[r] \arrow[d] & \widehat{\mathcal{P}ic_{X',N'}(\mathbb{F}_{q'})} \arrow[d, "\det"] \\
\pi_1(X - N, \overline{x}') \arrow[r] & \widehat{\mathcal{P}ic_{X,N}(\mathbb{F}_q)}
\end{tikzcd}$$

et donc aussi :

$$\begin{tikzcd}
\pi_1(X' - N', \overline{x}') \arrow[r] \arrow[d] & \varprojlim_{\substack{N'_1 \hookrightarrow X' \\ X' - N'_1 = X' - N'}} \widehat{\mathcal{P}ic_{X',N'_1}(\mathbb{F}_{q'})} \arrow[d, "\det"] \\
\pi_1(X - N, \overline{x}') \arrow[r] & \varprojlim_{\substack{N_1 \hookrightarrow X \\ X - N_1 = X - N}} \widehat{\mathcal{P}ic_{X,N_1}(\mathbb{F}_q)}
\end{tikzcd}$$

□

Si G est un groupe fini [resp. profini], il existe un unique groupe abélien fini [resp. profini] G^{ab}, tel que se donner un morphisme

$$G \to A$$

vers un groupe abélien fini [resp. profini] A équivale à se donner un morphisme

$$G^{\mathrm{ab}} \to A\,.$$

Ce groupe G^{ab}, l'abélianisé de G, est la limite projective filtrante

$$\varprojlim G/G_i$$

des quotients de G par des sous-groupes distingués [resp. et ouverts] G_i tels que G/G_i soit abélien.

Le théorème IV.29 et le corollaire IV.32 se reformulent donc de la manière suivante :

Théorème IV.33. –

Pour tout ouvert U de la courbe X, et si $\overline{x}$ désigne un point géométrique de U, on a :

(i) *Les chtoucas définissent un homomorphisme continu surjectif*

$$\pi_1(U,\overline{x})^{\mathrm{ab}} \longrightarrow \varprojlim_{\substack{N\hookrightarrow X\\ N\cap U=\emptyset}} \widehat{\mathcal{P}ic_{X,N}(\mathbb{F}_q)}$$

qui est compatible avec les projections sur $\widehat{\mathbb{Z}}$ et envoie chaque élément de Frobenius σ_x en un point fermé x de U sur $\mathcal{O}_X(x)$.

(ii) *Si U' est un revêtement étale connexe de U, X' l'unique courbe projective, lisse et connexe dont U' est un ouvert, et $\overline{x}'$ est un point géométrique de U' qui relève $\overline{x}$, on a un diagramme commutatif :*

$$\begin{tikzcd}
\pi_1(U',\overline{x}')^{\mathrm{ab}} \arrow[r] \arrow[d] & \varprojlim\limits_{\substack{N'\hookrightarrow X'\\ N'\cap U'=\emptyset}} \widehat{\mathcal{P}ic_{X',N'}(\mathbb{F}_q)} \arrow[d, "\det"] \\
\pi_1(U,\overline{x}')^{\mathrm{ab}} \arrow[r] & \varprojlim\limits_{\substack{N\hookrightarrow X\\ N\cap U=\emptyset}} \widehat{\mathcal{P}ic_{X,N}(\mathbb{F}_q)}
\end{tikzcd}$$

(iii) *Si de plus le revêtement étale U' de U est abélien, avec donc*

$$\mathrm{Aut}_U(U') = \pi_1(U,\overline{x})/\pi_1(U',\overline{x}') = \pi_1(U,\overline{x})^{\mathrm{ab}}/\pi_1(U',x')^{\mathrm{ab}}\,,$$

on a un homomorphisme surjectif

$$\mathrm{Aut}_U(U') \longrightarrow \varprojlim_{\substack{N\hookrightarrow X\\ N\cap U=\emptyset}} \widehat{\mathcal{P}ic_{X,N}(\mathbb{F}_q)} \Big/ \det\left(\varprojlim_{\substack{N'\hookrightarrow X'\\ N'\cap U'=\emptyset}} \widehat{\mathcal{P}ic_{X',N'}(\mathbb{F}_q)}\right).$$

Remarque de complément :

Dans la situation de (iii), le groupe abélien $\mathrm{Aut}_U(U')$ a pour cardinal le degré d du revêtement fini plat $U'\to U$ ou $X'\to X$.

Or on peut démontrer par ailleurs que, dans ce cas, le quotient

$$\varprojlim_{\substack{N\hookrightarrow X\\ N\cap U=\emptyset}} \widehat{\mathcal{P}ic_{X,N}(\mathbb{F}_q)} \Big/ \det\left(\varprojlim_{\substack{N'\hookrightarrow X'\\ N'\cap U'=\emptyset}} \widehat{\mathcal{P}ic_{X',N'}(\mathbb{F}_q)}\right)$$

compte au moins d éléments.

On en déduit que l'homomorphisme surjectif de (iii) est toujours un isomorphisme, et donc aussi l'homomorphisme continu surjectif de (i) :

$$\pi_1(U,\overline{x})^{\mathrm{ab}} \xrightarrow{\sim} \varprojlim_{\substack{N\hookrightarrow X\\ N\cap U=\emptyset}} \widehat{\mathcal{P}ic_{X,N}(\mathbb{F}_q)}\,.$$

Enfin, si $\overline{F}$ est une clôture algébrique du corps des fonctions F de la courbe X, il en est encore de même de l'homomorphisme continu

$$\Gamma_F^{\mathrm{ab}} = \mathrm{Aut}_F(\overline{F})^{\mathrm{ab}} \xrightarrow{\sim} \varprojlim_{N \hookrightarrow X} \widehat{\mathcal{P}ic_{X,N}}(\mathbb{F}_q)\,.$$

C'est "l'isomorphisme du corps de classe". $\square$

V. Adèles et idèles

1 Le cas des corps de fonctions

Dans ce paragraphe, on considère une courbe X projective, lisse et géométriquement connexe sur un corps fini $\mathbb{F}_q$. Se donner une telle courbe équivaut à se donner son corps des fonctions rationnelles F.

Dans l'étude des chtoucas sur X, on a constamment fait appel aux "niveaux" de X, c'est-à-dire aux sous-schémas fermés finis

$$N = \mathrm{Spec}\,(\mathcal{O}_N) \hookrightarrow X$$

et au système projectif filtrant qu'ils forment.

Cela conduit à définir :

Définition V.1. –

Pour $F = F_X$ un corps de fonctions comme ci-dessus, on appelle "anneau des entiers adéliques" de F la limite projective

$$O_{\mathbb{A}_F} = \varprojlim_{N \hookrightarrow X} \mathcal{O}_N \,.$$

C'est donc l'anneau des familles

$$(a_N \in \mathcal{O}_N)_{N \hookrightarrow X}$$

indexées par les sous-schémas fermés finis $N = \mathrm{Spec}\,(\mathcal{O}_N)$ de X et telles que, pour tout $N \hookrightarrow N' \hookrightarrow X$, $a_{N'} \in \mathcal{O}_{N'}$ s'envoie sur $a_N \in \mathcal{O}_N$.

Il est muni d'homomorphismes surjectifs canoniques

$$O_{\mathbb{A}_F} \to \mathcal{O}_N \,,$$

dont les noyaux sont des idéaux d'indice fini notés $I_{\mathbb{A}_F,N}$, et de la topologie invariante dont les $I_{\mathbb{A}_F,N}$ fournissent une base de voisinages ouverts de 0.

Remarque :

Ainsi, $O_{\mathbb{A}_F}$ est un anneau topologique.

En tant que groupe additif, c'est un groupe profini.

En tant qu'espace topologique, il est séparé et compact. □

Tout sous-schéma fermé fini $N \hookrightarrow X$ consiste en un nombre fini de points fermés x de X, avec des multiplicités m_x, ce qui signifie que N a la forme

$$N = \coprod_x \mathrm{Spec}\,(\mathcal{O}_x/(\varpi_x^{m_x}))\,,$$

ou encore que $\mathcal{O}_N$ se décompose canoniquement en

$$\mathcal{O}_N = \prod_x \mathcal{O}_x/(\varpi_x^{m_x})\,.$$

On en déduit :

Lemme V.2. –

En tant qu'anneau topologique, l'anneau des entiers adéliques de F s'identifie au produit

$$O_{\mathbb{A}_F} = \prod_{x \in |X|} O_x$$

où $|X|$ désigne l'ensemble (infini dénombrable) des points fermés de X et $O_x = \widehat{\mathcal{O}}_x$ désigne l'anneau de valuation discrète complété de l'anneau local $\mathcal{O}_x$ en tout point $x \in |X|$.

Remarque :

Pour tout niveau $N = \mathrm{Spec}\,(\mathcal{O}_N) = \coprod\limits_x \mathrm{Spec}\,(\mathcal{O}_x/(\varpi_x^{m_x}))$, l'idéal $I_{\mathbb{A}_F,N}$ de $O_{\mathbb{A}_F,N}$ s'identifie donc à

$$\prod_{x \in |X|} \varpi_x^{m_x} \cdot O_x \,.$$

Il est ouvert puisque $m_x = 0$ en presque tout point fermé $x \in |X|$, c'est-à-dire en tous les points sauf un nombre fini.

□

On rappelle que l'on a noté F_x le corps des fractions de chaque O_x. Il est le complété de F pour la norme ultramétrique

$$f \mapsto |f|_x = \begin{cases} q_x^{-v_x(f)} & \text{si} \quad f \neq 0 \\ 0 & \text{si} \quad f = 0 \end{cases}$$

où q_x est le cardinal du corps résiduel κ_x au point x, avec donc

$$q_x = q^{\deg(x)}$$

si $\deg(x)$ est le degré de l'extension finie κ_x de $\mathbb{F}_q$.

On définit encore :

Définition V.3. –

L'anneau des "adèles" de F est le sous-anneau

$$\mathbb{A}_F \subset \prod_{x \in |F|} F_x$$

constitué des familles d'éléments

$$(f_x \in F_x)_{x \in |X|}$$

telles que $f_x \in O_x$ pour presque tout $x \in |X|$.

Il est muni de la topologie induite par la topologie produit de $\prod\limits_{x \in |X|} F_x$.

C'est l'unique topologie invariante pour laquelle le sous-groupe

$$O_{\mathbb{A}_F} \subset \mathbb{A}_F$$

est un sous-groupe ouvert et est muni de la topologie déjà définie.

Remarque :

Toute fonction rationnelle de X est définie sur un ouvert non vide, c'est-à-dire partout en dehors d'un ensemble fini de points. Par conséquent, le plongement diagonal

$$F \hookrightarrow \prod_{x \in |X|} F_x$$

se factorise en

$$F \hookrightarrow \mathbb{A}_F \, .$$

De plus, $\mathbb{F}_q = \mathcal{O}_X(X)$ est l'intersection de F et de $O_{\mathbb{A}_F} \subset \mathbb{A}_F$. □

Considérons maintenant la situation relative d'un morphisme entre deux courbes :

Lemme V.4. –

Soit F' une extension finie de degré d de F, soit X' l'unique courbe projective, lisse et géométriquement connexe sur une extension finie $\mathbb{F}_{q'}$ de $\mathbb{F}_q$ dont le corps des fonctions est F', et soit

$$X' \to X$$

le morphisme fini et plat de degré d qui est associé à l'extension $F \subset F'$.

Alors :

(i) *L'anneau des adèles de X' s'identifie au produit tensoriel*

$$\mathbb{A}_{F'} = \mathbb{A}_F \otimes_F F' \, .$$

(ii) *Pour tous points fermés $x \in |X|$ et $x' \in |X'|$ au-dessus de x, l'extension finie*

$$F_x \subset F'_{x'}$$

définit un morphisme F_x-linéaire

$$F'_{x'} \to \mathrm{End}_{F_x}(F'_{x'})$$

et donc un morphisme F_x-linéaire de trace [resp. un morphisme multiplicatif de déterminant]

$$\mathrm{Tr} : F'_{x'} \to F_x$$

$$\textit{[resp.} \quad \mathrm{Nm} = \det : F'^{\times}_{x'} \to F_x^{\times} \textit{]}$$

qui envoie $O_{x'}$ dans O_x [resp. $O_{x'}^{\times}$ dans $O_x^{\times}$].

(iii) *Le produit sur tous les x, x' des morphismes*

$$\mathrm{Tr} : F'_{x'} \to F_x \qquad \textit{[resp.} \quad \mathrm{Nm} : F'^{\times}_{x'} \to F_x^{\times} \textit{]}$$

définit un morphisme $\mathbb{A}_F$-linéaire [resp. multiplicatif]

$$\mathrm{Tr} : \mathbb{A}_{F'} \to \mathbb{A}_F \qquad \textit{[resp.} \quad \mathrm{Nm} : \mathbb{A}_{F'}^{\times} \to \mathbb{A}_F^{\times} \textit{]}$$

qui envoie $O_{\mathbb{A}_{F'}}$ dans $O_{\mathbb{A}_F}$ [resp. $O_{\mathbb{A}_{F'}}^{\times}$ dans $O_{\mathbb{A}_F}^{\times}$] et F' dans F [resp. $F'^{\times}$ dans $F^{\times}$].
Comme $\mathbb{A}_{F'}$ est un $\mathbb{A}_F$-module libre de rang d, il n'est autre que le composé du morphisme $\mathbb{A}_F$-linéaire

$$\mathbb{A}_F \to \mathrm{End}_{\mathbb{A}_F}(\mathbb{A}_{F'}) \cong M_d(\mathbb{A}_F)$$

et de la trace [resp. du déterminant] des algèbres de matrices.

Démonstration :

(i) Cela résulte de la proposition III.26 qui implique que, pour tout point fermé $x \in |X|$,

$$F_x \otimes_F F' \quad \text{s'identifie à} \quad \prod_{\substack{x' \in |X'| \\ x' \mapsto x}} F'_{x'}$$

et que, pour tout ouvert affine $\mathrm{Spec}\,(A) \subset X$ d'image réciproque $\mathrm{Spec}\,(A') \subset X'$ et tout point fermé x de $\mathrm{Spec}\,(A)$,

$$O_x \otimes_A A' \quad \text{s'identifie à} \quad \prod_{\substack{x' \in |X'| \\ x' \mapsto x}} O_{x'} \,.$$

(ii) est évident, sauf la dernière assertion qui résulte de ce que $O_{x'}$ est libre sur O_x de même rang que $F'_{x'}$ considéré comme un espace vectoriel sur F_x.

(iii) Les premières assertions résultent de (ii).
Les suivantes résultent de ce que toute base de F' sur F définit une base de $\mathbb{A}_{F'}$ sur $\mathbb{A}_F$ puisque, d'après (i), $\mathbb{A}_{F'}$ s'identifie à $\mathbb{A}_F \otimes_F F'$.

$\square$

L'anneau $\mathbb{A}_F$ est aussi le sous-anneau des familles

$$(f_x \in F_x)_{x \in |F|}$$

telles que $|f_x|_x \leq 1$ en “presque tout” $x \in |X|$.

Donc son groupe multiplicatif $\mathbb{A}_F^\times$, qui est appelé le groupe des “idèles” de F, est constitué des familles

$$(f_x \in F_x^\times)_{x \in |F|}$$

telles que $|f_x|_x = 1$, soit $v_x(f_x) = 0$, en “presque tout” $x \in |X|$.

Cela permet de poser :

Définition V.5. –

On appelle “degré” l'homomorphisme

$$\begin{array}{rcl} \deg : \mathbb{A}_F^\times & \to & \mathbb{Z} \\ (f_x)_{x \in |X|} & \mapsto & -\displaystyle\sum_{x \in |X|} \deg(x) \cdot v_x(f_x) \end{array}$$

et “norme globale” l'homomorphisme

$$\begin{array}{rcl} |\bullet| : \mathbb{A}_F^\times & \to & q^{\mathbb{Z}} \\ f = (f_x)_{x \in |X|} & \mapsto & q^{\deg(f)} = |f| = \displaystyle\prod_{x \in |F|} |f_x|_x \,. \end{array}$$

$\square$

On a :

Lemme V.6. –

Dans la situation du lemme V.4, *et si d' désigne le degré de l'extension $\mathbb{F}_{q'}$ de $\mathbb{F}_q$, le carré*

$$\begin{tikzcd} \mathbb{A}_{F'}^\times \arrow[r, "\mathrm{Nm}"] \arrow[d, "\deg"'] & \mathbb{A}_F^\times \arrow[d, "\deg"] \\ \mathbb{Z} \arrow[r, "n \mapsto d' \cdot n"'] & \mathbb{Z} \end{tikzcd}$$

est commutatif.

Démonstration :

Il faut prouver que si x est un point fermé de X et x' un point fermé de X' au-dessus de x, alors on a pour tout $f' \in F_{x'}^\times$ la relation

$$\deg(x) \cdot v_x(\mathrm{Nm}(f')) = d' \cdot \deg(x') \cdot v_{x'}(f')$$

soit

$$v_x(\mathrm{Nm}(f')) = \dim_{\kappa_x}(\kappa_{x'}) \cdot v_{x'}(f')\,.$$

Comme Nm envoie $O_{x'}^\times$ dans $O_x^\times$, il suffit de prouver cette relation pour un seul élément $f' \in F_{x'}^\times$ de valuation non nulle, par exemple pour une uniformisante ϖ_x de O_x considérée comme un élément de $O_{x'}$. Alors

$$\mathrm{Nm}(\varpi_x) = \varpi_x^{\mathrm{rg}_{O_x}(O_{x'})}$$

et la relation à démontrer se réduit à

$$\mathrm{rg}_{O_x}(O_{x'}) = \dim_{\kappa_x}(\kappa_{x'}) \cdot v_{x'}(\varpi_x)$$

qui résulte de ce que

$$O_{x'} \otimes_{O_x} O_x/(\varpi_x) \cong O_{x'}/(\varpi_{x'}^{v_{x'}(\varpi_x)})\,.$$

$\square$

Ce lemme permet de démontrer facilement la très importante proposition suivante, appelée “formule du produit” :

Proposition V.7. –

Pour tout élément $f \in F^\times$, on a

$$\prod_{x \in |X|} |f|_x = |f| = 1$$

ou, ce qui revient au même,

$$-\sum_{x \in |X|} \deg(x) \cdot v_x(f) = \deg(f) = 0\,.$$

Remarque :

Autrement dit, les homomorphismes

$$|\bullet| : \mathbb{A}_F^\times \to q^{\mathbb{Z}} \quad \text{ou} \quad \deg : \mathbb{A}_F^\times \to \mathbb{Z}$$

se factorisent en

$$|\bullet| : \mathbb{A}_F^\times/F^\times \to q^{\mathbb{Z}} \quad \text{ou} \quad \deg : \mathbb{A}_F^\times/F^\times \to \mathbb{Z}\,.$$

Démonstration :

Le corps de fonctions F peut s'écrire comme une extension finie de $\mathbb{F}_q(T)$ si bien que X peut s'écrire comme un revêtement fini plat de la droite projective $\mathbb{P}^1_{\mathbb{F}_q}$.

Comme le morphisme induit Nm envoie $F^\times$ dans $\mathbb{F}_q(T)^\times$, le lemme V.6 nous ramène au cas où $X = \mathbb{P}^1_{\mathbb{F}_q}$ et $F = \mathbb{F}_q(T)$.

On peut même supposer que f est un polynôme, élément de $\mathbb{F}_q[T]$.

Alors si x décrit l'ensemble des points fermés de l'ouvert

$$\mathbb{A}^1_{\mathbb{F}_q} = \mathrm{Spec}\,(\mathbb{F}_q[T]) \subset \mathbb{P}^1_{\mathbb{F}_q}$$

complémentaire du point à l'infini ∞ de $\mathbb{P}^1_{\mathbb{F}_q}$, la somme

$$\sum_x \deg(x) \cdot v_x(f)$$

est égale au nombre de racines du polynôme f dans une clôture algébrique $\overline{\mathbb{F}}_q$ de $\mathbb{F}_q$, comptées avec multiplicités, tandis que

$$\deg(\infty) \cdot v_\infty(f) = v_\infty(f)$$

est égal au degré du polynôme f.

D'où la conclusion. $\square$

On déduit de cette proposition :

Corollaire V.8. –

(i) *Le plongement*

$$F \hookrightarrow \mathbb{A}_F$$

fait de F un sous-groupe discret du groupe topologique $\mathbb{A}_F$.

(ii) *Le plongement*

$$F^\times \hookrightarrow \mathbb{A}_F^\times$$

fait de $F^\times$ un sous-groupe discret du groupe topologique $\mathbb{A}_F^\times$.

Démonstration :

(i) Considérons n'importe quelle famille de réels $r_x > 0$, $x \in |X|$, qui sont presque tous égaux à 1 et vérifient la relation

$$\prod_{x \in |X|} r_x < 1\,.$$

Alors, pour tout élément $f \in F$, le sous-ensemble

$$\{(f_x)_{x\in|X|} \in \mathbb{A}_F \mid |f_x - f|_x \le r_x\,, \quad \forall\, x \in |X|\}$$

est un voisinage ouvert de f dans $\mathbb{A}_F$ qui ne contient aucun autre élément de F.

(ii) L'application $f \mapsto (f, f^{-1})$ identifie $\mathbb{A}_F^\times$ muni de sa topologie à un fermé de $\mathbb{A}_F \times \mathbb{A}_F$. Alors le sous-groupe $F^\times$ de $\mathbb{A}_F^\times$ s'identifie à l'intersection de ce fermé et du sous-groupe discret $F \times F$ de $\mathbb{A}_F \times \mathbb{A}_F$.

$\square$

On a le résultat fondamental suivant dû à André Weil :

Proposition V.9. –

(i) *Le quotient discret*

$$F^\times \backslash \mathbb{A}_F^\times / O_{\mathbb{A}_F}^\times$$

s'identifie au groupe $\mathcal{P}ic_X(\mathbb{F}_q)$ des fibrés inversibles sur X.
De plus, cette identification échange les homomorphismes de degrés $\mathbb{A}_F^\times \to \mathbb{Z}$ et $\mathcal{P}ic_X \to \mathbb{Z}$.

(ii) *Pour tout sous-schéma fermé fini $N = \operatorname{Spec}(\mathcal{O}_N) \hookrightarrow X$, et si l'on note J_N le noyau (ouvert) de l'homomorphisme surjectif*

$$O_{\mathbb{A}_F}^\times \to \mathcal{O}_N^\times \, ,$$

le quotient discret

$$F^\times \backslash \mathbb{A}_F^\times / J_N$$

s'identifie au groupe $\mathcal{P}ic_{X,N}(\mathbb{F}_q)$ des fibrés inversibles avec structure de niveau N sur X.

(iii) *Pour tout ouvert non vide U de X, le quotient*

$$F^\times \backslash \mathbb{A}_F^\times / \prod_{x \in U} O_x^\times$$

s'identifie à la limite projective

$$\varprojlim_{\substack{N \hookrightarrow X \\ N \cap U = \emptyset}} \mathcal{P}ic_{X,N}(\mathbb{F}_q) \, .$$

(iv) *Le quotient*

$$F^\times \backslash \mathbb{A}_F^\times$$

s'identifie à la limite projective

$$\varprojlim_{N \hookrightarrow X} \mathcal{P}ic_{X,N}(\mathbb{F}_q) \, .$$

Démonstration :

(i) Tout idéal non nul d'un anneau local $\mathcal{O}_x$ en un point fermé x de X est libre de rang 1 comme $\mathcal{O}_x$-module. Par conséquent, tout faisceau d'idéaux non nul $\mathcal{I} \subset \mathcal{O}_X$ est localement libre de rang 1.
Se donner un $\mathcal{O}_X$-$\mathcal{M}$odule inversible $\mathcal{L}$ muni d'un plongement partout défini sur X

$$\mathcal{L} \hookrightarrow \mathcal{O}_X$$

équivaut donc à se donner une famille d'idéaux non nuls

$$(I_x \subset \mathcal{O}_x)_{x \in |X|}$$

telle que $I_x = \mathcal{O}_x$ en presque toute place $x \in |X|$.
Or, pour tout point x, se donner un idéal non nul $I_x \subset \mathcal{O}_x$ équivaut à se donner ses générateurs, qui forment une classe d'équivalence, élément du quotient

$$F^\times / \mathcal{O}_x^\times = F_x^\times / O_x^\times \, ,$$

dont la valuation est ≥ 0. De plus, cette valuation doit être 0 en presque toute place x.
Se donner un $\mathcal{O}_X$-$\mathcal{M}$odule inversible $\mathcal{L}$ muni d'un plongement $\mathcal{L} \hookrightarrow \mathcal{O}_X$ équivaut donc à se donner un élément de

$$\mathbb{A}_F^\times / O_{\mathbb{A}_F}^\times$$

dont toutes les valuations sont ≥ 0.

Or l'ensemble des $(\mathcal{L}, \mathcal{L} \hookrightarrow \mathcal{O}_X)$ muni du produit tensoriel forme un monoïde abélien dont le groupe abélien associé est l'ensemble des classes d'isomorphisme de fibrés inversibles $\mathcal{L}$ munis d'une section rationnelle, c'est-à-dire d'un vecteur de base ℓ de leur fibre générique $\mathcal{L} \otimes_{\mathcal{O}_X} F$.

Le groupe abélien des $(\mathcal{L}, \ell)$ s'identifie donc à

$$\mathbb{A}_F^\times / O_{\mathbb{A}_F}^\times .$$

Comme les sections rationnelles non nulles $\ell' \in \mathcal{L} \otimes_{\mathcal{O}_X} F$ d'un tel $\mathcal{O}_X$-$\mathcal{M}$odule inversible $\mathcal{L}$ se déduisent de ℓ par multiplication par les éléments de $F^\times$, on obtient l'identification

$$\mathcal{P}ic_X(\mathbb{F}_q) = F^\times \backslash \mathbb{A}_F^\times / O_{\mathbb{A}_F}^\times .$$

Elle préserve les degrés d'après la formule de calcul de la proposition IV.13(iii).

(ii) Considérons un fibré inversible $\mathcal{L}$ sur X qui correspond à un élément de $F^\times \backslash \mathbb{A}_F^\times / O_{\mathbb{A}_F}^\times$. Le choix d'une section rationnelle de $\mathcal{L}$, c'est-à-dire d'un isomorphisme $\mathcal{L} \otimes_{\mathcal{O}_X} F \cong F$, relève cet élément en un

$$a \in \mathbb{A}_F^\times / O_{\mathbb{A}_F}^\times .$$

La composante $a_x \in F_x^\times / O_x^\times$ de a en tout point $x \in |X|$ est l'ensemble des générateurs du O_x-module libre $\mathcal{L} \otimes_{\mathcal{O}_X} O_x$ dans $\mathcal{L} \otimes_{\mathcal{O}_X} F_x \cong F_x$.

Mettre une structure de niveau $N \hookrightarrow X$ sur $\mathcal{L}$ permet de choisir en tout point x de N, ceux des générateurs de $\mathcal{L} \otimes_{\mathcal{O}_X} O_x$ dont la restriction à $N \times_X \mathrm{Spec}\,(O_x) = \mathrm{Spec}\,(\mathcal{O}_N \otimes_{\mathcal{O}_X} O_x)$ s'envoie sur 1 par l'isomorphisme $(\mathcal{L} \otimes_{\mathcal{O}_X} \mathcal{O}_N) \otimes_{\mathcal{O}_X} O_x \cong \mathcal{O}_N \otimes_{\mathcal{O}_X} O_x$. Cela définit une classe d'équivalence, élément de $\mathbb{A}_F^\times / J_N$.

En oubliant le choix de la section rationnelle, on obtient un homomorphisme de groupes abéliens $\mathcal{P}ic_{X,N}(\mathbb{F}_N) \to F^\times \backslash \mathbb{A}_F^\times / J_N$ qui s'inscrit dans un carré commutatif :

$$\begin{tikzcd}
\mathcal{P}ic_{X,N}(\mathbb{F}_q) \arrow[r] \arrow[d] & F^\times \backslash \mathbb{A}_F^\times / J_N \arrow[d] \\
\mathcal{P}ic_X(\mathbb{F}_q) \arrow[r, "\sim"] & F^\times \backslash \mathbb{A}_F^\times
\end{tikzcd}$$

C'est un isomorphisme car sa fibre au-dessus de l'unité $\mathcal{O}_X$ de $\mathcal{P}ic_X(\mathbb{F}_q)$ muni de sa section canonique 1 est un isomorphisme.

(iii) et (iv) sont des conséquences immédiates de (ii). □

Cette proposition est complétée par la suivante :

Proposition V.10. –

Comme dans le lemme V.4, *considérons une extension finie $F' \supset F$ de degré d et l'unique morphisme fini et plat de degré d*

$$X' \to X$$

entre courbes projectives, lisses et connexes qui lui est associé.

Alors :

(i) *Le carré*

$$\begin{tikzcd}
\mathcal{P}ic_{X'}(\mathbb{F}_{q'}) \arrow[r, "\sim"] \arrow[d, "\det"'] & F'^\times \backslash \mathbb{A}_{F'}^\times / O_{\mathbb{A}_{F'}}^\times \arrow[d, "\mathrm{Nm}"] \\
\mathcal{P}ic_X(\mathbb{F}_q) \arrow[r, "\sim"] & F^\times \backslash \mathbb{A}_F^\times / O_{\mathbb{A}_F}^\times
\end{tikzcd}$$

est commutatif.

(ii) *Si $N \hookrightarrow X$ et $N' \hookrightarrow X'$ sont deux sous-schémas fermés finis tels que $N \times_X X' \hookrightarrow X'$ se factorise à travers N', l'homomorphisme*

$$\mathrm{Nm} : \mathbb{A}_{F'}^{\times} \to \mathbb{A}_F^{\times}$$

envoie $J_{N'} \subset O_{\mathbb{A}_{F'}}^{\times}$ dans $J_N \subset O_{\mathbb{A}_F}^{\times}$, et le carré

$$\begin{tikzcd}
\mathcal{P}ic_{X',N'}(\mathbb{F}_{q'}) \arrow[r, "\sim"] \arrow[d, "\det"'] & F'^{\times}\backslash \mathbb{A}_{F'}^{\times}/J_{N'} \arrow[d, "\mathrm{Nm}"] \\
\mathcal{P}ic_{X,N}(\mathbb{F}_q) \arrow[r, "\sim"] & F^{\times}\backslash \mathbb{A}_F^{\times}/J_N
\end{tikzcd}$$

est commutatif.

Démonstration :

Cela résulte de ce que toutes les flèches verticales sont définies en passant aux déterminants d'endomorphismes de multiplication agissant dans des espaces ou des modules libres (ou localement libres) de rang d.

□

Compte tenu des propositions V.9 et V.10, le théorème IV.33 se réécrit de la manière suivante :

Théorème V.11. –

Pour tout ouvert U de la courbe X, et si $\overline{x}$ désigne un point géométrique de U, on a :

(i) *Les chtoucas définissent un homomorphisme continu surjectif*

$$\pi_1(U,\overline{x})^{\mathrm{ab}} \to \widehat{F^{\times}\backslash \mathbb{A}_F^{\times}/\prod_{x\in U} O_x^{\times}}$$

qui est compatible avec les projections sur $\widehat{\mathbb{Z}}$ et envoie chaque élément de Frobenius σ_x en un point fermé x de U sur la classe de ϖ_x^{-1}.

(ii) *Si U' est un revêtement étale connexe de U de corps des fonctions F', et $\overline{x}'$ est un point géométrique de U' qui relève $\overline{x}$, on a un carré commutatif :*

$$\begin{tikzcd}
\pi_1(U',\overline{x}')^{\mathrm{ab}} \arrow[r] \arrow[d] & \widehat{F'^{\times}\backslash \mathbb{A}_{F'}^{\times}/\prod_{x'\in U'} O_{x'}^{\times}} \arrow[d, "\mathrm{Nm}"] \\
\pi_1(U,\overline{x})^{\mathrm{ab}} \arrow[r] & \widehat{F^{\times}\backslash \mathbb{A}_F^{\times}/\prod_{x\in U} O_x^{\times}}
\end{tikzcd}$$

(iii) *Si de plus le revêtement étale U' de U est abélien, on a un homomorphisme surjectif*

$$\mathrm{Aut}_U(U') \to F^{\times}\backslash \mathbb{A}_F^{\times}/\mathrm{Nm}(\mathbb{A}_{F'}^{\times}) \cdot \prod_{x\in U} O_x^{\times} .$$

Remarque de complément :

Il résulte de la remarque qui suit le théorème IV.33 que l'homomorphisme de (iii) est un isomorphe.

De plus, on peut démontrer que dans la situation de (iii), on a

$$\mathrm{Nm}\left(\prod_{x'\in U'} O_{x'}^{\times}\right) = \prod_{x\in U} O_x^{\times}$$

et donc on a un isomorphisme

$$\mathrm{Aut}_F(F') = \mathrm{Aut}_U(U') \xrightarrow{\sim} F^{\times}\backslash\mathbb{A}_F^{\times}/\mathrm{Nm}(\mathbb{A}_{F'}^{\times})\,.$$

On en déduit que l'homomorphisme de (i)

$$\pi_1(U,\overline{x})^{\mathrm{ab}} \to F^{\times}\backslash\widehat{\mathbb{A}_F^{\times}/\prod_{x\in U}} O_x^{\times}$$

est un isomorphisme et que, si $\overline{F}$ est une clôture algébrique de F, on a un isomorphisme

$$\Gamma_F^{\mathrm{ab}} = \mathrm{Aut}_F(\overline{F})^{\mathrm{ab}} \xrightarrow{\sim} \widehat{F^{\times}\backslash\mathbb{A}_F^{\times}}\,.$$

□

2 Le cas des corps de nombres

On considère maintenant un corps de nombres F, c'est-à-dire une extension finie, nécessairement séparable, de $\mathbb{Q}$.

Le corps de nombres F est le corps des fonctions d'une unique courbe arithmétique régulière, connexe et fini sur $\mathrm{Spec}\,(\mathbb{Z})$. C'est le spectre $X_F = \mathrm{Spec}\,(A_F)$ de l'anneau A_F normalisé de $\mathbb{Z}$ dans F.

Comme dans le cas des courbes projectives lisses sur un corps fini, on peut considérer le système projectif filtrant des sous-schémas fermés finis

$$N = \mathrm{Spec}\,(\mathcal{O}_N) \hookrightarrow X_F = \mathrm{Spec}\,(A_F)\,,$$

autrement dit des quotients finis

$$A_F \twoheadrightarrow \mathcal{O}_N$$

et définir :

Définition V.12. –

Pour F un corps de nombres vu comme le corps des fonctions de la courbe arithmétique régulière $X_F = \mathrm{Spec}\,(A_F)$ associée, on appelle "anneau des entiers adéliques" de F la limite projective

$$O_{\mathbb{A}_F^u} = \varprojlim_{N\hookrightarrow X_F} \mathcal{O}_N\,.$$

Il est muni d'homomorphismes surjectifs canoniques

$$O_{\mathbb{A}_F^u} \to \mathcal{O}_N\,,$$

dont les noyaux sont des idéaux d'indice fini notés $I_{\mathbb{A}_F,N}$, et de la topologie invariante dont les $I_{\mathbb{A}_F,N}$ fournissent une base de voisinages ouverts de 0.

Remarque :

Comme dans le cas des corps de fonctions de courbes sur un corps fini, $O_{\mathbb{A}_F}$ est un anneau topologique. En tant que groupe additif, c'est un groupe profini. En tant qu'espace topologique, il est séparé et compact. $\square$

On a l'exact analogue du lemme V.2 :

Lemme V.13. –

En tant qu'anneau topologique, l'anneau $O_{\mathbb{A}_F^u}$ des entiers adéliques du corps de nombres F s'identifie au produit

$$\prod_{x \in |X_F|} O_x$$

où $|X_F|$ désigne l'ensemble (infini dénombrable) des points fermés de X_F et $O_x = \widehat{\mathcal{O}_x}$ désigne l'anneau de valuation discrète complété de l'anneau local $\mathcal{O}_x$ en tout point $x \in |X_F|$.

Remarque :

Tout sous-schéma fermé fini $N = \operatorname{Spec}(\mathcal{O}_N)$ de X_F se décompose canoniquement en une réunion disjointe finie

$$\coprod_x \operatorname{Spec}(\mathcal{O}_x/(\varpi_x^{m_x}))$$

si bien que l'idéal correspondant $I_{\mathbb{A}_F,N}$ de $O_{\mathbb{A}_F^u}$ s'identifie à

$$\prod_x \varpi_x^{m_x} \cdot O_x \,.$$

Il est ouvert puisque $m_x = 0$ en presque tout point fermé $x \in |X_F|$. $\square$

On rappelle que l'on a noté F_x le corps des fractions de chaque O_x. C'est le complété de F pour la norme ultramétrique

$$f \mapsto |f|_x = \begin{cases} q_x^{-v_x(f)} & \text{si} \quad f \neq 0 \\ 0 & \text{si} \quad f = 0 \end{cases}$$

où q_x désigne le cardinal du corps résiduel κ_x au point x, avec

$$q_x = p_x^{\deg(x)}$$

si p_x est la caractéristique de κ_x, qui est un nombre premier dépendant de x, et $\deg(x)$ est le degré de l'extension finie κ_x de $\mathbb{F}_{p_x} = \mathbb{Z}/p_x\,\mathbb{Z}$.

On a l'analogue de la définition V.3 :

Définition V.14. –

L'anneau des "adèles ultramétriques" ou "adèles finis" de F est le sous-anneau

$$\mathbb{A}_F^u \subset \prod_{x \in |X_F|} F_x$$

constitué des familles d'éléments

$$(f_x \in F_x)_{x \in |X_F|}$$

telles que $f_x \in O_x$ pour presque tout $x \in |X_F|$.

Il est muni de la topologie induite par la topologie produit de $\prod\limits_{x \in |F|} F_x$.

C'est l'unique topologie invariante pour laquelle le sous-groupe

$$O_{\mathbb{A}_F^u} \subset \mathbb{A}_F^u$$

est un sous-groupe ouvert et se trouve muni de la topologie déjà définie.

Remarque :

Le plongement diagonal $F \hookrightarrow \prod\limits_{x \in |X_F|} F_x$ se factorise en

$$F \hookrightarrow \mathbb{A}_F^u \,,$$

A_F est l'intersection de F et de $O_{\mathbb{A}_F^u} \subset \mathbb{A}_F^u$ et l'homomorphisme

$$F \otimes_{A_F} O_{\mathbb{A}_F^u} \to \mathbb{A}_F^u$$

est un isomorphisme. □

Puis on a l'exact analogue du lemme V.4 :

Lemme V.15. –

Soit F' une extension finie de degré d du corps de nombres F, soit $X_{F'} = \mathrm{Spec}\,(A_{F'})$ la courbe régulière connexe et finie sur $\mathrm{Spec}\,(\mathbb{Z})$ associée, et soit

$$X_{F'} \to X_F$$

le morphisme fini et plat de degré d qui est associé à l'extension $F \subset F'$.

Alors :

(i) *L'anneau des adèles ultramétriques de F' s'identifie au produit tensoriel*

$$\mathbb{A}_{F'}^u = \mathbb{A}_F^u \otimes_F F' \,.$$

(ii) *Pour tous points fermés $x \in |X_F|$ et $x' \in |X_{F'}|$ au-dessus de x, l'extension finie*

$$F_x \subset F'_{x'}$$

définit un morphisme F_x-linéaire

$$F'_{x'} \to \mathrm{End}_{F_x}(F'_{x'})$$

et donc un morphisme F_x-linéaire de trace [resp. un morphisme multiplicatif de déterminant]

$$\mathrm{Tr} : F'_{x'} \to F_x$$

[resp.

$$\mathrm{Nm} = \det : F'^{\times}_{x'} \to F_x^{\times} \;]$$

qui envoie $O_{x'}$ dans O_x [resp. $O_{x'}^{\times}$ dans $O_x^{\times}$].

(iii) *Le produit sur tous les x, x' des morphismes*

$$\mathrm{Tr} : F'_{x'} \to F_x \qquad [resp. \quad \mathrm{Nm} : F'^{\times}_{x'} \to F_x^{\times} \;]$$

définit un morphisme $\mathbb{A}_F^u$-linéaire [resp. multiplicatif]

$$\mathrm{Tr} : \mathbb{A}_{F'}^u \to \mathbb{A}_F^u \qquad [resp. \quad \mathrm{Nm} : \mathbb{A}_{F'}^{u,\times} \to \mathbb{A}_F^{u,\times} \;]$$

qui envoie $O_{\mathbb{A}^u_{F'}}$ dans $O_{\mathbb{A}^u_F}$ [resp. $O^\times_{\mathbb{A}^u_{F'}}$ dans $O^\times_{\mathbb{A}^u_F}$] et F' dans F [resp. $F'^\times$ dans $F^\times$].

Comme $\mathbb{A}^u_{F'}$ est un $\mathbb{A}^u_F$-module libre de rang d, il n'est autre que le composé du morphisme $\mathbb{A}_F$-linéaire

$$\mathbb{A}^u_{F'} \to \mathrm{End}_{\mathbb{A}^u_F}(\mathbb{A}^u_{F'}) \cong M_d(\mathbb{A}^u_F)$$

et de la trace [resp. du déterminant] des algèbres de matrices.

Démonstration :

Elle est identique à celle du lemme V.4. □

Le groupe multiplicatif $\mathbb{A}^{u,\times}_F$, qui est appelé le groupe des "idèles" ultramétriques (ou finis) de F, est constitué des familles

$$(f_x \in F^\times_x)_{x\in|X_F|}$$

telles que $|f_x|_x = 1$, soit $v_x(f_x) = 0$, en "presque tout" $x \in |X_F|$.

Cela permet de définir une "norme globale"

$$\begin{array}{rcl} |\bullet| : \mathbb{A}^{u,\times}_F & \to & \mathbb{Q}^\times_+ \\ f = (f_x)_{x\in|X_F|} & \mapsto & |f| = \displaystyle\prod_{x\in|X_F|} |f_x|_x \,. \end{array}$$

On a même l'analogue suivant du lemme V.6, qui se démontre de la même façon :

Lemme V.16. –

Dans la situation du lemme V.15*, le triangle*

$$\begin{tikzcd} \mathbb{A}^{u,\times}_{F'} \arrow[rr, "\mathrm{Nm}"] \arrow[dr, "|\bullet|"'] & & \mathbb{A}^{u,\times}_F \arrow[dl, "|\bullet|"] \\ & \mathbb{Q}^\times_+ & \end{tikzcd}$$

est commutatif. □

Cependant, il apparaît ici une différence essentielle avec le cas des corps de fonctions :

Lemme V.17. –

(i) *Pour tout nombre rationnel non nul $r \in \mathbb{Q}^\times$, sa "norme globale" comme élément de $\mathbb{A}^{u,\times}_{\mathbb{Q}}$*

$$\prod_{p\in|\mathrm{Spec}\,(\mathbb{Z})|} |r|_p$$

est égale à l'inverse

$$|r|^{-1}_\infty$$

de sa "norme archimédienne" (c'est-à-dire sa valeur absolue) $|r|_\infty$ comme élément de $\mathbb{R}$.

(ii) *Pour tout corps de nombre F et tout élément $f \in F^\times$, sa "norme globale" comme élément de $\mathbb{A}^{u,\times}_F$*

$$\prod_{x\in|X_F|} |f|_x$$

est égale à l'inverse

$$|\mathrm{Nm}\,(f)|^{-1}_\infty$$

de la "norme archimédienne" $|\mathrm{Nm}\,(f)|_\infty$ de son image $\mathrm{Nm}\,(f)$ par l'homomorphisme $\mathrm{Nm} : F^\times \to \mathbb{Q}^\times$.

Démonstration :

(i) Il suffit de le vérifier lorsque $r = p$ est un nombre premier. Dans ce cas, on a

$$|p|_{p'} = \begin{cases} p^{-1} & \text{si } p' = p\,, \\ 1 & \text{pour tout nombre premier } p' \neq p\,, \end{cases}$$

d'où se déduit la formule annoncée.

(ii) résulte de (i) et du lemme V.16. $\square$

L'absence de "formule de produit" dans les $\mathbb{A}_F^{u,\times}$ se traduit d'ailleurs par le résultat supplémentaire suivant qui exprime une autre grande différence avec le cas des corps de fonctions :

Lemme V.18. –

Pour tout corps de nombres F, le plongement

$$F \hookrightarrow \mathbb{A}_F^u$$

fait de F un sous-groupe dense de $\mathbb{A}_F^u$.

Remarque :

En revanche, s'il est vrai que $F^\times \hookrightarrow \mathbb{A}_F^{u,\times}$ n'est pas discret, il n'est pas dense en général. En particulier, le quotient

$$F^\times \backslash \mathbb{A}_F^{u,\times} / O_{\mathbb{A}_F^u}^\times$$

n'est pas trivial en général.

Démonstration :

Comme $\mathbb{A}_F^u = O_{\mathbb{A}_F^u} \otimes_{A_F} F$, il suffit de prouver que A_F est dense dans $O_{\mathbb{A}_F^u}$. Cela résulte de la définition de $O_{\mathbb{A}_F^u}$ comme $\varprojlim\limits_{N \hookrightarrow \mathrm{Spec}(A_F)} \mathcal{O}_N$.

$\square$

Le lemme V.17 amène à considérer aussi le plongement de $\mathbb{Q}$ dans $\mathbb{R}$ muni de sa "norme archimédienne" ou "valeur absolue"

$$|\bullet|_\infty : \mathbb{R} \to \mathbb{R}_+\,.$$

On a :

Lemme V.19. –

(i) *Si F est un corps de nombres, la $\mathbb{R}$-algèbre de dimension finie*

$$F_\infty = F \otimes_{\mathbb{Q}} \mathbb{R}\,,$$

munie de la topologie induite par celle de $\mathbb{R}$, se décompose canoniquement comme un produit

$$F_\infty = \prod_{x \in |F|_\infty} F_x$$

de facteurs F_x tous isomorphes à $\mathbb{R}$ ou $\mathbb{C}$ et indexés par un ensemble fini noté $|F|_\infty$.

(ii) *Si $F' \supset F$ est une extension de corps de nombres de degré d, il existe une unique application*

$$|F'|_\infty \to |F|_\infty$$

telle que, pour tout indice $x \in |F|_\infty$, la F_x-algèbre de dimension d

$$F' \otimes_F F_x$$

s'identifie au produit

$$\prod_{\substack{x' \in |F'|_\infty \\ x' \mapsto x}} F'_{x'}$$

des $F'_{x'}$, $x' \mapsto x$, qui sont donc des extensions de F_x (égales à F_x si $F_x \cong \mathbb{C}$, et égales à $\mathbb{R}$ ou isomorphes à $\mathbb{C}$ si $F_x = \mathbb{R}$).

Démonstration :

(i) résulte de ce que les seules extensions finies de $\mathbb{R}$ sont $\mathbb{R}$ et $\mathbb{C}$.

(ii) résulte de la double décomposition

$$F' \otimes_{\mathbb{Q}} \mathbb{R} = \prod_{x' \in |F'|_\infty} F'_{x'}$$

et

$$F' \otimes_{\mathbb{Q}} \mathbb{R} = F' \otimes_F (F \otimes_{\mathbb{Q}} \mathbb{R}) = \prod_{x \in |F|_\infty} (F' \otimes_F F_x)\,.$$

□

On déduit de ce lemme le corollaire suivant qui est l'analogue "archimédien" du lemme V.15 :

Corollaire V.20. –

Soit $F' \supset F$ une extension de corps de nombres de degré d. Alors :

(i) *Pour tous indices $x \in |F|_\infty$ et $x' \in |F'|_\infty$ au-dessus de x, l'extension finie*

$$F_x \subset F'_{x'}$$

définit un morphisme F_x-linéaire

$$F'_{x'} \to \mathrm{End}_{F_x}(F'_{x'})$$

et donc un morphisme F_x-linéaire de trace [resp. un morphisme multiplicatif de déterminant]

$$\mathrm{Tr} : F'_{x'} \to F_x$$

$$\textit{[resp.} \qquad \mathrm{Nm} = \det : F'^{\times}_{x'} \to F^{\times}_x \;\;].$$

(ii) *Le produit sur tous les x, x' des morphismes*

$$\mathrm{Tr} : F'_{x'} \to F_x \qquad \textit{[resp.} \quad \mathrm{Nm} : F'^{\times}_{x'} \to F^{\times}_x \;\;]$$

définit un morphisme F_∞-linéaire [resp. multiplicatif]

$$\mathrm{Tr} : F'_\infty \to F_\infty \qquad \textit{[resp.} \quad \mathrm{Nm} : F'^{\times}_\infty \to F^{\times}_\infty \;\;].$$

Comme F'_∞ est une F_∞-algèbre libre de rang d, il n'est autre que le composé du morphisme F_∞-linéaire

$$F'_\infty \to \mathrm{End}_{F_\infty}(F'_\infty) \cong M_d(F_\infty)$$

et de la trace [resp. du déterminant] des algèbres de matrices.
En particulier, sa restriction à F' [resp. $F'^\times$] n'est autre que le morphisme

$$\mathrm{Tr} : F' \to F \qquad \textit{[resp.} \quad \mathrm{Nm} : F'^\times \to F^\times \textit{]}$$

déjà défini.

Remarque :

Dans la situation de (i), le morphisme

$$\mathrm{Tr} : F'_{x'} \to F_x \qquad [\text{resp.} \quad \mathrm{Nm} : F'^\times_{x'} \to F^\times_x \ ]$$

est l'identité si $F'_{x'} = F_x \cong \mathbb{R}$ ou $\mathbb{C}$, et il est

$$z \mapsto z + \overline{z} \qquad [\text{resp.} \quad z \mapsto z \cdot \overline{z} \ ]$$

si $F_x = \mathbb{R}$ et $F'_{x'} \cong \mathbb{C}$.

Démonstration :

C'est formellement la même que celle des lemmes V.4 et V.15. $\square$

On note encore :

Corollaire V.21. –

Si F est un corps de nombres et x un élément de $|F|_\infty$, on a :

(i) *Le corps F plongé dans le facteur F_x de $F \otimes_{\mathbb{Q}} \mathbb{R}$ est dense.*

(ii) *Le composé*

$$|\bullet|_x : F_x^\times \xrightarrow{\mathrm{Nm}} \mathbb{R}^\times \xrightarrow{|\bullet|_\infty} \mathbb{R}_+^\times$$

se confond avec la valeur absolue usuelle

$$\lambda \mapsto |\lambda|_\infty$$

si $F_x = \mathbb{R}$, et avec le carré du module

$$z \mapsto z \cdot \overline{z} = |z|_\infty^2$$

si $F_x \cong \mathbb{C}$. $\square$

On est amené à poser :

Définition V.22. –

Soit F un corps de nombres.

(i) *On appelle "places" de F les éléments de la réunion disjointe*

$$|F| = |X_F| \coprod |F|_\infty \,.$$

(ii) *On appelle "anneau des adèles" de F l'anneau topologique produit*

$$\mathbb{A}_F = \mathbb{A}_F^u \times F_\infty = \mathbb{A}_F^u \times \prod_{x \in |F|_\infty} F_x \,.$$

Remarques :

(i) Ainsi, à toute place $x \in |F|$ est associé un corps

$$F_x \supset F$$

muni d'une norme et qui s'identifie à la complétion de F pour cette norme.
Le groupe multiplicatif $F_x^\times$ est muni d'un homomorphisme

$$|\bullet|_x : F_x^\times \to \mathbb{R}_+^\times$$

qui se confond avec la norme de F_x si $x \in |X_F|$ ou $F_x = \mathbb{R}$ mais qui est égal au carré du module si $F_x \cong \mathbb{C}$.

(ii) Si, comme au paragraphe précédent, F est le corps des fonctions d'une courbe X_F projective, lisse et géométriquement connexe sur un corps fini $\mathbb{F}_q$, on pourra noter

$$|F| = |X_F|$$

et appeler ses éléments les places de F. □

On déduit du lemme V.15 et du corollaire V.20 :

Corollaire V.23. –

Soit $F' \supset F$ une extension de corps de nombres de degré d. Alors :

(i) *Les anneaux des adèles de F et F' sont reliés par un isomorphisme canonique*

$$\mathbb{A}_{F'} \cong \mathbb{A}_F \otimes_F F'$$

si bien que $\mathbb{A}_{F'}$ est libre de rang d sur $\mathbb{A}_F$.

(ii) *Le produit des morphismes*

$$\mathrm{Tr} : F'_{x'} \to F_x \qquad \textit{[resp.} \quad \mathrm{Nm} : F'^\times_{x'} \to F_x^\times \ \textit{]}$$

lorsque x, x' décrivent l'ensemble des paires de places de F et F' telles que x' s'envoie sur x, définit un morphisme $\mathbb{A}_F$-linéaire [resp. multiplicatif]

$$\mathrm{Tr} : \mathbb{A}_{F'} \to \mathbb{A}_F \qquad \textit{[resp.} \quad \mathrm{Nm} : \mathbb{A}_{F'}^\times \to \mathbb{A}_F^\times \ \textit{]}.$$

Il n'est autre que le composé du morphisme $\mathbb{A}_F$-linéaire

$$\mathbb{A}_{F'} \to \mathrm{End}_{\mathbb{A}_F}(\mathbb{A}_{F'}) \cong M_d(\mathbb{A}_F)$$

et de la trace [resp. du déterminant] des algèbres de matrices.
En particulier, sa restriction à F' [resp. $F'^\times$] n'est autre que le composé du morphisme F-linéaire

$$F' \to \mathrm{End}_F(F') \cong M_d(F)$$

et de la trace [resp. du déterminant] des matrices.

Si F est un corps de nombres, on peut munir le groupe multiplicatif $\mathbb{A}_F^\times$, qui est appelé le groupe des "idèles" de F, de l'homomorphisme de "norme globale"

$$\begin{array}{rcl} |\bullet| : \mathbb{A}_F^\times & \to & \mathbb{R}_+^\times \\ f = (f_x)_{x \in |F|} & \mapsto & |f| = \prod_{x \in |F|} |f_x|_x \, . \end{array}$$

Le corollaire V.23 entraîne l'analogue suivant du lemme V.6 :

Corollaire V.24. –

Pour toute extension finie de corps de nombres $F \hookrightarrow F'$, on a un triangle commutatif :

$$\begin{tikzcd} \mathbb{A}_{F'}^\times \arrow[rr] \arrow[dr, "|\bullet|"'] & & \mathbb{A}_F^\times \arrow[dl, "|\bullet|"] \\ & \mathbb{R}_+^\times & \end{tikzcd}$$

□

Puis on a l'analogue suivant de la proposition V.7 :

Proposition V.25. –

Pour tout élément non nul f d'un corps de nombre F, considéré comme un élément de $\mathbb{A}_F^\times$, on a la "formule du produit"

$$\prod_{x \in |F|} |f|_x = |f| = 1 \, .$$

Démonstration :

D'après le corollaire V.24, il suffit de démontrer le résultat dans le cas où $F = \mathbb{Q}$.

Mais alors c'est une conséquence immédiate du lemme V.17(i). □

Comme la proposition V.7 implique le corollaire V.8, la proposition V.25 ci-dessus entraîne :

Corollaire V.26. –

Pour tout corps de nombres F, on a :

(i) *Le plongement*

$$F \hookrightarrow \mathbb{A}_F$$

fait de F un sous-groupe discret du groupe topologique $\mathbb{A}_F$.

(ii) *Le plongement*

$$F^\times \hookrightarrow \mathbb{A}_F^\times$$

fait de $F^\times$ un sous-groupe discret du groupe topologique $\mathbb{A}_F^\times$. □

Enfin, les corollaires V.8 et V.26 sont complétés par le théorème suivant :

Théorème V.27. –

Soit F un "corps global", c'est-à-dire un corps de nombres, ou bien le corps des fonctions d'une courbe projective, lisse et connexe sur un corps fini. Alors :

(i) *Le quotient*

$$\mathbb{A}_F / F$$

du groupe topologique $\mathbb{A}_F$ par son sous-groupe discret F est compact.

(ii) *Si $\mathbb{A}_F^{\times 0}$ désigne le noyau de l'homomorphisme*

$$\mathbb{A}_F^\times \xrightarrow{|\bullet|} \mathbb{R}_+^\times \qquad \textit{[resp.} \quad \mathbb{A}_F^\times \xrightarrow{\deg} \mathbb{Z}\ \textit{]},$$

son quotient

$$\mathbb{A}_F^{\times 0} / F^\times$$

par le sous-groupe discret $F^\times$ est compact.

Remarque :

Nous connaissons déjà (ii) dans le cas où F est le corps des fonctions d'une courbe X_F projective, lisse et géométriquement connexe sur un corps fini $\mathbb{F}_q$.

Dans ce cas, il s'agit en effet de prouver que le quotient

$$F^\times \backslash \mathbb{A}_F^{\times 0} / O_{\mathbb{A}_F}^\times$$

est fini.

Or, d'après la proposition V.9(i), ce quotient s'identifie à

$$\mathcal{P}ic^0_{X_F}(\mathbb{F}_q)$$

qui est l'ensemble des points à valeurs dans $\mathbb{F}_q$ du schéma $\mathcal{P}ic^0_{X_F} = \mathcal{J}ac_{X_F}$ sur $\mathbb{F}_q$. Comme ce schéma est projectif et a fortiori de type fini sur $\mathbb{F}_q$ d'après la proposition IV.13(i), l'ensemble $\mathcal{P}ic^0_{X_F}(\mathbb{F}_q)$ est fini.

Démonstration :

Si F est un corps de nombres, on dispose du sous-anneau $A_F \subset F$ des éléments entiers sur $\mathbb{Z}$ et de la $\mathbb{R}$-algèbre finie

$$F_\infty = F \otimes_{\mathbb{Q}} \mathbb{R} = \prod_{x \in |F|_\infty} F_x \,.$$

Si F est un corps de fonctions, écrivons-le comme une extension finie séparable de $\mathbb{F}_q(T)$. Alors la courbe projective lisse X_F sur $\mathbb{F}_q$ associée à F est munie d'un morphisme fini et plat

$$X_F \to \mathbb{P}^1_{\mathbb{F}_q} \,.$$

Notons dans ce cas ∞ le point à l'infini de la droite projective $\mathbb{P}^1_{\mathbb{F}_q}$, $|F|_\infty$ l'ensemble fini des places $x \in |F|$ au-dessus de ∞, puis

$$F_\infty = \prod_{x \in |F|_\infty} F_x = F \otimes_{\mathbb{F}_q(T)} \mathbb{F}_q(T)_\infty$$

et A_F la normalisation de $\mathbb{F}_q[T]$ dans F. Ainsi, $\mathrm{Spec}\,(A_F)$ est l'ouvert de X_F image réciproque de la droite affine $\mathrm{Spec}\,(\mathbb{F}_q[T]) = \mathbb{P}^1_{\mathbb{F}_q} - \{\infty\}$ par le morphisme $X_F \to \mathbb{P}^1_{\mathbb{F}_q}$.

Alors A_F est dense dans

$$O_{\mathbb{A}_F^u} = \prod_{x \in |\mathrm{Spec}(A_F)|} O_x = \varprojlim_{N \hookrightarrow \mathrm{Spec}(A_F)} \mathcal{O}_N$$

donc F est dense dans

$$\mathbb{A}_F^u = F \otimes_{A_F} O_{\mathbb{A}_F^\infty} \,,$$

et l'on remarque que
$$\mathbb{A}_F = \mathbb{A}_F^u \times F_\infty \,.$$
C'est l'analogue pour les corps de fonctions du lemme V.18 pour les corps de nombres.

(i) Comme F est dense dans $\mathbb{A}_F^u$ et $A_F = F \cap O_{\mathbb{A}_F^u}$, il est équivalent de démontrer que $A_F \backslash (O_{\mathbb{A}_F^u} \times F_\infty)$ est compact.

Et comme $O_{\mathbb{A}_F^u}$ est compact, cela équivaut au lemme suivant :

Lemme V.28. –

Avec les notations ci-dessus, et que F soit un corps de nombres ou un corps de fonctions, le plongement
$$A_F \hookrightarrow F_\infty$$
fait de A_F un sous-groupe discret de F_∞, et le quotient
$$F_\infty / A_F$$
est compact.

Démonstration :

Comme F est un sous-groupe discret de $\mathbb{A}_F = \mathbb{A}_F^u \times F_\infty$, $A_F = F \cap O_{\mathbb{A}_F^u}$ est un sous-groupe discret de F_∞.

Si F est un corps de nombres, A_F est un $\mathbb{Z}$-module libre de rang fini. Le quotient F_∞ / A_F est compact car
$$A_F \otimes_{\mathbb{Z}} \mathbb{R} = (A_F \otimes_{\mathbb{Z}} \mathbb{Q}) \otimes_{\mathbb{Q}} \mathbb{R} = F \otimes_{\mathbb{Q}} \mathbb{R} = F_\infty \,.$$

Si F est un corps de fonctions, A_F est un $\mathbb{F}_q[T]$-module libre de rang fini et on a
$$A_F \otimes_{\mathbb{F}_q[T]} \mathbb{F}_q(T)_\infty = (A_F \otimes_{\mathbb{F}_q[T]} \mathbb{F}_q(T)) \otimes_{\mathbb{F}_q(T)} \mathbb{F}_q(T)_\infty = F \otimes_{\mathbb{F}_q(T)} \mathbb{F}_q(T)_\infty = F_\infty$$
ce qui ramène le problème au cas où $F = \mathbb{F}_q(T)$ et $X_F = \mathbb{P}^1_{\mathbb{F}_q}$.

Dans ce cas, la conclusion résulte de ce que, pour tout $f \in \mathbb{F}_q(T)_\infty$, il existe un $P \in \mathbb{F}_q[T]$ tel que $v_\infty(f - P) \geq 0$.

$\square$

Pour démontrer la partie (ii) de la proposition V.27, on a besoin du lemme suivant :

Lemme V.29. –

Il existe une constante $C > 0$ telle que, pour toute famille de réels $N_x > 0$, $x \in |F|$, vérifiant

- *$N_x = 1$ en presque toute place $x \in |F|$,*
- *$N_x \in q_x^{\mathbb{Z}}$ en toute place ultramétrique $x \in |X_F|$,*
- *$\prod\limits_{x \in |F|} N_x \geq C$,*

il existe un élément $f \in F^\times$ vérifiant
$$|f_x|_x \leq N_x \,, \qquad \forall\, x \in |F| \,.$$

Démonstration :

Munissons F_∞ d'une mesure invariante par translation, et notons V le volume fini du quotient compact de F_∞ par son sous-groupe discret A_F.

Alors

$$I = \{f \in F \mid |f|_x \leq N_x\,, \quad \forall\, x \in |F| - |F|_\infty\}$$

se plonge dans F_∞ comme un sous-groupe discret, et le quotient

$$F_\infty / I$$

est compact de volume

$$V \cdot \prod_{x \in |F| - |F|_\infty} N_x^{-1}\,.$$

D'autre part, l'ensemble des $f_\infty = (f_x)_{x \in |F|_\infty} \in F_\infty = \prod_{x \in |F|_\infty} F_x$ tels que

$$\begin{cases} |f_x|_x \leq \frac{1}{2}\, N_x & \text{si} \quad F_x = \mathbb{R}\,, \\ |f_x|_x^{1/2} \leq \frac{1}{2}\, N_x^{1/2} & \text{si} \quad F_x \cong \mathbb{C}\,, \\ |f_x|_x \leq N_x & \text{si} \quad \text{F est un corps de fonctions,} \end{cases}$$

a pour volume le produit de

$$\prod_{x \in |F|_\infty} N_x$$

et d'une constante $V' > 0$.

Si donc $V' \cdot \prod_{x \in |F|_\infty} N_x > V \cdot \prod_{x \in |F| - |F|_\infty} N_x^{-1}$, cet ensemble ne peut s'envoyer injectivement dans F_∞ / I. Il contient au moins deux éléments distincts $f_\infty = (f_x)_{x \in |F|_\infty}$ et $f'_\infty = (f'_x)_{x \in |F|_\infty}$ dont la différence $f = f_\infty - f'_\infty$ est élément de $I \subset F$.

Alors f est un élément de $F^\times$ qui vérifie

$$|f|_x \leq N_x\,, \quad \forall\, x \in |F|\,.$$

$\square$

Fin de la démonstration du théorème V.27(ii) :

Soit $(f_x)_{x \in |F|}$ un élément de $\mathbb{A}^{\times 0}$, avec donc

$$\prod_{x \in |F|} |f_x|_x = 1\,.$$

Choisissons une place $x_0 \in |F|$. D'après le lemme V.29 ci-dessus, il existe un élément non nul $f \in F^\times$ tel que

$$|f|_x \leq |f_x|_x\,, \quad \forall\, x \in |F| - \{x_0\} \qquad \text{et} \qquad |f|_{x_0} \leq C \cdot |f_{x_0}|_{x_0}\,.$$

D'après la formule du produit, cela impose aussi

$$|f|_x \geq C^{-1} \cdot |f_x|_x\,, \quad \forall\, x \in |F| - \{x_0\} \qquad \text{et} \qquad |f|_{x_0} \geq |f_{x_0}|_{x_0}\,.$$

Comme chaque norme ultramétrique $|\bullet|_x$, $x \in |X_F|$, prend ses valeurs dans $q_x^{\mathbb{Z}}$, cela impose encore

$$|f|_x = |f_x|_x \quad \text{en toute place } x \in |X_F| \text{ telle que } q_x > C.$$

On conclut en remarquant que l'ensemble $\{x \in |X_F| \mid q_x \leq C\}$ est fini. $\square$

3 Isomorphisme du corps de classes et caractères cyclotomiques

Bien qu'il n'existe pas d'analogue sur les corps de nombres de la construction géométrique des chtoucas de Drinfeld sur les corps de fonctions, le langage des adèles permet de formuler exactement dans les mêmes termes que le théorème V.11 le théorème suivant propre aux corps de nombres :

Théorème V.30. –

Soit F un corps de nombres, et soit U un ouvert non vide de la courbe arithmétique X_F. Alors :

(i) *Il existe un unique isomorphisme*

$$\pi_1(U,\overline{x})^{\mathrm{ab}} \xrightarrow{\sim} \widehat{F^\times\backslash\mathbb{A}_F^\times/\prod_{x\in U} O_x}$$

qui envoie chaque élément de Frobenius σ_x en un point fermé x de U sur la classe de ϖ_x^{-1}.

(ii) *Si U' est un revêtement étale connexe de U, de corps des fonctions $F' \supset F$, et $\overline{x}'$ est un point géométrique de U' qui relève $\overline{x}$, on a un carré commutatif :*

$$\begin{tikzcd}
\pi_1(U',\overline{x}')^{\mathrm{ab}} \arrow[r, "\sim"] \arrow[d] & \widehat{F'^\times\backslash\mathbb{A}_{F'}^\times/\prod_{x'\in U'} O_{x'}^\times} \arrow[d, "\mathrm{Nm}"] \\
\pi_1(U,\overline{x})^{\mathrm{ab}} \arrow[r, "\sim"] & \widehat{F^\times\backslash\mathbb{A}_F^\times/\prod_{x\in U} O_x^\times}
\end{tikzcd}$$

(iii) *Si de plus le revêtement étale U' de U est abélien, on a un isomorphisme*

$$\mathrm{Aut}_U(U') \xrightarrow{\sim} F^\times\backslash\mathbb{A}_F^\times/\mathrm{Nm}(\mathbb{A}_{F'}^\times)$$

avec $\mathrm{Nm}(\mathbb{A}_{F'}^\times) \supset \mathrm{Nm}(O_{\mathbb{A}_{F'}^u}^\times) \supset \prod_{x\in U} O_x^\times$. □

Ce théorème, que nous énonçons sans démonstration, entraîne l'énoncé suivant, appelé "isomorphisme du corps de classes" ou "loi de réciprocité d'Artin" :

Corollaire V.31. –

Soient F un corps de nombres et Γ_F le groupe profini des automorphismes d'une clôture algébrique $\overline{F}$ de F. Alors :

(i) *Les isomorphismes du théorème* V.30 *induisent un isomorphisme*

$$\Gamma_F^{\mathrm{ab}} \xrightarrow{\sim} \widehat{F^\times\backslash\mathbb{A}_F^\times}\,.$$

(ii) *Si F' est une extension finie de F plongée dans $\overline{F}$ et $\Gamma_{F'} \subset \Gamma_F$ est le sous-groupe ouvert d'indice fini des fixateurs de ses éléments, on a un carré commutatif :*

$$\begin{tikzcd}
\Gamma_{F'}^{\mathrm{ab}} \arrow[r, "\sim"] \arrow[d] & \widehat{F'^\times\backslash\mathbb{A}_{F'}^\times} \arrow[d, "\mathrm{Nm}"] \\
\Gamma_F^{\mathrm{ab}} \arrow[r, "\sim"] & \widehat{F^\times\backslash\mathbb{A}_F^\times}
\end{tikzcd}$$

(iii) *Si de plus l'extension finie F' de F est abélienne, on a un isomorphisme*

$$\mathrm{Aut}_F(F') \xrightarrow{\sim} F^\times \backslash \mathbb{A}_F^\times / \mathrm{Nm}(\mathbb{A}_{F'}^\times)\,.$$

Remarque :

Ainsi, se donner une extension abélienne F' du corps de nombres F plongée dans $\overline{F}$ équivaut à se donner un sous-groupe ouvert d'indice fini I de $F^\times \backslash \mathbb{A}_F^\times$, et l'on a alors l'identité entre sous-groupes de $F^\times \backslash \mathbb{A}_F^\times$

$$I = \mathrm{Nm}(F'^\times \backslash \mathbb{A}_{F'}^\times)\,.$$

□

Une autre analogie importante entre corps de fonctions et corps de nombres F est l'existence d'un homomorphisme surjectif naturel, appelé "caractère cyclotomique", du groupe de Galois de F vers $\widehat{\mathbb{Z}}$:

Proposition V.32. –

Soient F un corps de nombres et Γ_F le groupe profini des automorphismes d'une clôture algébrique $\overline{F}$ de F. Alors :

(i) *Le sous-corps de $\overline{F}$ engendré sur F par les racines de l'unité 1 d'ordre arbitraire est réunion filtrante d'extensions finies abéliennes de F.*

Son groupe de Galois s'identifie à un sous-groupe ouvert d'indice fini de

$$\widehat{\mathbb{Z}}^\times = \prod_{p \text{ premier}} \mathbb{Z}_p^\times \cong (\mathbb{Z}/2\,\mathbb{Z} \times \mathbb{Z}_2) \times \prod_{p\neq 2} (\mathbb{Z}/(p-1)\,\mathbb{Z} \times \mathbb{Z}_p) = \widehat{\mathbb{Z}} \times \left(\prod_{p \neq 2} \mathbb{Z}/(p-1)\,\mathbb{Z} \right) \times \mathbb{Z}/2\,\mathbb{Z}\,,$$

et possède un unique quotient isomorphe à $\widehat{\mathbb{Z}}$, avec donc un homomorphisme continu surjectif induit

$$\deg_F : \Gamma_F \to \widehat{\mathbb{Z}}\,.$$

(ii) *Si $F' \supset F$ est une extension finie de F plongée dans $\overline{F}$, et $\Gamma_{F'} \subset \Gamma_F$ est le sous-groupe ouvert correspondant, il existe un unique entier $f_{F'/F} \geq 1$ rendant commutatif le carré :*

$$\begin{tikzcd} \Gamma_{F'} \arrow[r, "\deg_{F'}"] \arrow[d] & \widehat{\mathbb{Z}} \arrow[d, "f_{F'/F}"] \\ \Gamma_F \arrow[r, "\deg_F"] & \widehat{\mathbb{Z}} \end{tikzcd}$$

(iii) *Pour tout nombre premier p, et si $X_{F,p}$ désigne l'ouvert de la courbe arithmétique X_F où p est inversible, la composante*

$$\Gamma_F \to \mathbb{Z}_p$$

du composé

$$\Gamma_F \xrightarrow{\deg_F} \widehat{\mathbb{Z}} \xrightarrow{f_{F/\mathbb{Q}}} \widehat{\mathbb{Z}} = \prod_\ell \mathbb{Z}_\ell$$

se factorise à travers

$$\pi_1(X_{F,p}, \overline{F}) \longrightarrow \mathbb{Z}_p^\times \longrightarrow \mathbb{Z}_p$$

et envoie chaque élément de Frobenius σ_x, $x \in |X_{F,p}|$, sur l'entier q_x (défini comme le cardinal du corps résiduel en x) dans $\mathbb{Z}_p^\times$.

(iv) *Si $F = \mathbb{Q}$ et $\overline{F} = \overline{\mathbb{Q}}$ est plongé dans $\mathbb{C}$, $\deg_{\mathbb{Q}}$ envoie l'automorphisme de conjugaison complexe de $\overline{\mathbb{Q}}$ sur l'image de l'entier -1 par $\widehat{\mathbb{Z}}^\times \to \widehat{\mathbb{Z}}$.*

Démonstration :

On commence par le lemme suivant :

Lemme V.33. –

Soient K un corps de clôture algébrique $\overline{K}$, $n \geq 1$ un entier non divisible par la caractéristique de K, et $K(\mu_n) \subset \overline{K}$ l'extension finie de K dans $\overline{K}$ engendrée par le groupe $\mu_n = \{a \in \overline{K} \mid a^n = 1\}$.

Alors :

(i) *Le groupe multiplicatif μ_n est cyclique d'ordre n, c'est-à-dire isomorphe à $\mathbb{Z}/n\,\mathbb{Z}$.*

(ii) *L'extension $K(\mu_n) \supset K$ est abélienne, et on a un plongement canonique*

$$\mathrm{Aut}_K(K(\mu_n)) \hookrightarrow (\mathbb{Z}/n\,\mathbb{Z})^\times .$$

(iii) *Si $n = p_1^{m_1} \dots p_k^{m_k}$ est la décomposition de n en produit de facteurs premiers, K_n est la composée des extensions abéliennes $K_{p_i^{m_i}}$, avec donc*

$$\mathrm{Aut}_K(K(\mu_n)) = \prod_{1 \leq i \leq k} \mathrm{Aut}_K(K(\mu_{p_i^{m_i}})) .$$

(iv) *Si $K = \mathbb{Q}_p$ et n est premier avec p, l'image du plongement*

$$\mathrm{Aut}_K(K(\mu_n)) \hookrightarrow (\mathbb{Z}/n\,\mathbb{Z})^\times$$

est constituée des puissances de p.

(v) *Si $K = \mathbb{Q}$, le plongement*

$$\mathrm{Aut}_K(K(\mu_n)) \hookrightarrow (\mathbb{Z}/n\,\mathbb{Z})^\times$$

est un isomorphisme, quel que soit l'entier $n \geq 1$.

Démonstration :

(i) Le groupe μ_n compte n éléments puisque le polynôme $T^n - 1$ est séparable.
S'il n'était pas cyclique, il existerait un diviseur non trivial n' de n tel que

$$a^{n'} = 1 , \qquad \forall\, a \in \mu_n ,$$

ce qui est impossible.

(ii) Tout automorphisme de $\overline{K}$ préserve le groupe μ_n, donc l'extension $K(\mu_n)$ est galoisienne.
De plus, on a un plongement

$$\mathrm{Aut}_K(K(\mu_n)) \hookrightarrow \mathrm{Aut}\,(\mu_n)$$

et, comme μ_n est cyclique d'ordre n, $\mathrm{Aut}\,(\mu_n)$ s'identifie au groupe abélien $(\mathbb{Z}/n\,\mathbb{Z})^\times$.

(iii) résulte de la décomposition canonique

$$\mathbb{Z}/n\,\mathbb{Z} = \prod_{1 \leq i \leq k} \mathbb{Z}/p_i^{m_i}\mathbb{Z} .$$

(iv) L'équation

$$T^n - 1 = 0$$

définit un revêtement fini étale de $\mathrm{Spec}\,(\mathbb{Z}_p)$.

Comme $\mathbb{Z}_p$ et $\mathbb{F}_p$ ont le même groupe fondamental engendré par Frob_p, le groupe des automorphismes de toute composante connexe de ce revêtement étale est engendré par Frob_p.

(v) Comme $\mathbb{Q}$ est contenu dans $\mathbb{Q}_p$ quel que soit le nombre premier p, il résulte de (iv) que l'image de l'homomorphisme

$$\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}\,(\mu_n)) \hookrightarrow (\mathbb{Z}/n\,\mathbb{Z})^\times$$

contient les puissances de tout nombre premier p qui ne divise pas n. Cette image est donc égale à $(\mathbb{Z}/n\,\mathbb{Z})^\times$ tout entier.

□

On déduit de ce lemme :

Corollaire V.34. –

Dans une clôture algébrique $\overline{\mathbb{Q}}$ de $\mathbb{Q}$, le sous-corps $\mathbb{Q}\,(\mu_\infty)$ réunion des $\mathbb{Q}\,(\mu_n)$, $n \geq 1$, est respecté par tout automorphisme de $\overline{\mathbb{Q}}$.

De plus, le groupe des automorphismes de $\mathbb{Q}\,(\mu_\infty)$ est canoniquement isomorphe à

$$\varprojlim_{n\geq 1} (\mathbb{Z}/n\,\mathbb{Z})^\times = \widehat{\mathbb{Z}}^\times = \prod_p \mathbb{Z}_p^\times\,.$$

□

Avant de démontrer la proposition V.32, on a encore besoin du lemme suivant :

Lemme V.35. –

Pour tout nombre premier p, le groupe multiplicatif $\mathbb{Z}_p^\times$ est canoniquement isomorphe à

- $\mu_{p-1} \times \mathbb{Z}_p$ *si* $p \neq 2$,
- $\mu_2 \times \mathbb{Z}_2$ *si* $p = 2$.

Démonstration :

Si $p \neq 2$, l'équation $T^{p-1} = 1$ définit un revêtement fini étale de $\mathbb{Z}_p$ qui devient trivial sur le corps résiduel $\mathbb{F}_p$. Donc ce revêtement étale est trivial sur $\mathbb{Z}_p$. Autrement dit, l'équation $T^{p-1} = 1$ a $p-1$ solutions dans $\mathbb{Z}_p$, et celles-ci forment un sous-groupe μ_{p-1} de $\mathbb{Z}_p^\times$.

Alors $\mathbb{Z}_p^\times$ est le produit de μ_{p-1} et du sous-groupe

$$\mathrm{Ker}\,(\mathbb{Z}_p^\times \to \mathbb{F}_p^\times)\,.$$

Ce dernier est isomorphe au groupe additif $\mathbb{Z}_p$ via l'homomorphisme

$$v \mapsto \frac{1}{p} \sum_{n\geq 1} (-1)^{n-1} \cdot \frac{(v-1)^n}{n}$$

et son inverse

$$u \mapsto \sum_{n\geq 0} \frac{(p\,u)^n}{n!}\,.$$

Ces deux séries sont en effet bien définies et convergentes dans $\mathbb{Z}_p$ puisqu'on a pour tout entier n

$$v_p(n) \leq v_p(n!) < \frac{n}{p} + \frac{n}{p^2} + \frac{n}{p^3} + \ldots = \frac{1}{p-1} \cdot n\,.$$

De même, $\mathbb{Z}_2^\times$ est le produit de son sous-groupe

$$\{\pm 1\} = \mu_2$$

et de son sous-groupe

$$\mathrm{Ker}\,(\mathbb{Z}_2^\times \to (\mathbb{Z}/4\,\mathbb{Z})^\times)\,,$$

lequel est isomorphe au groupe additif $\mathbb{Z}_2$ via l'homomorphisme

$$v \mapsto \frac{1}{4} \cdot \sum_{n \geq 1} (-1)^{n-1} \cdot \frac{(v-1)^n}{n}$$

et son inverse

$$\mu \mapsto \sum_{n \geq 0} \frac{(4u)^n}{n!}\,.$$

Ces deux séries sont en effet bien définies et convergentes dans $\mathbb{Z}_2$ puisque, pour tout entier n, $v_2(n) \leq v_2(n!) < \frac{n}{2} + \frac{n}{4} + \frac{n}{8} + \ldots = n$.

□

Avant de reprendre la démonstration de la proposition V.32, on note le corollaire suivant de ce lemme :

Corollaire V.36. –

(i) *Le groupe des automorphismes de l'extension $\mathbb{Q}\,(\mu_\infty) \subset \overline{\mathbb{Q}}$ de $\mathbb{Q}$ est canoniquement isomorphe au groupe abélien*

$$\left(\prod_{p \neq 2} (\mu_{p-1} \times \mathbb{Z}_p)\right) \times (\mu_2 \times \mathbb{Z}_2) = \widehat{\mathbb{Z}} \times \left(\prod_{p \neq 2} \mu_{p-1}\right) \times \mu_2\,.$$

(ii) *Le sous-corps de $\mathbb{Q}\,(\mu_\infty)$ des éléments fixés par le sous-groupe de torsion de ce groupe*

$$\left(\prod_{p \neq 2} \mu_{p-1}\right) \times \mu_2 \cong \left(\prod_{p \neq 2} \mathbb{Z}/(p-1)\,\mathbb{Z}\right) \times \mathbb{Z}/2\,\mathbb{Z}$$

est une extension $\mathbb{Q}_{\mathrm{cycl}}$ de $\mathbb{Q}$, qui est respectée par tout automorphisme de $\overline{\mathbb{Q}}$, et dont le groupe des automorphismes est canoniquement isomorphe à $\widehat{\mathbb{Z}}$.

Remarque :

L'extension $\mathbb{Q}_{\mathrm{cycl}}$ de $\mathbb{Q}$ est appelée l'extension cyclotomique. □

Fin de la démonstration de la proposition V.32 :

(i) est une réécriture du corollaire V.36 ci-dessus dans le cas où $F = \mathbb{Q}$.
Si F est une extension finie de $\mathbb{Q}$, $\Gamma_F = \pi_1(F, \overline{F})$ est un sous-groupe ouvert d'indice fini de $\pi_1(\mathbb{Q}, \overline{F}) \cong \pi_1(\mathbb{Q}, \overline{\mathbb{Q}})$, d'où la première assertion.

Le composé

$$\pi_1(F,\overline{F}) \hookrightarrow \pi_1(\mathbb{Q},\overline{F}) \xrightarrow{\deg_{\mathbb{Q}}} \widehat{\mathbb{Z}}$$

a pour image un sous-groupe ouvert d'indice fini de $\widehat{\mathbb{Z}}$.
Il est nécessairement de la forme

$$f_{F/\mathbb{Q}} \cdot \widehat{\mathbb{Z}} \subset \widehat{\mathbb{Z}}$$

pour un unique entier $f_{F/\mathbb{Q}} \geq 1$.

On conclut en définissant $\deg_F$ comme le quotient par $f_{F/\mathbb{Q}}$ du composé $\pi_1(F,\overline{F}) \to \pi_1(\mathbb{Q},\overline{F}) \xrightarrow{\deg_{\mathbb{Q}}} \widehat{\mathbb{Z}}$.

(ii) Si F' est une extension finie de F, on a les inclusions

$$f_{F'/\mathbb{Q}} \cdot \widehat{\mathbb{Z}} \subset f_{F/\mathbb{Q}} \cdot \widehat{\mathbb{Z}} \subset \widehat{\mathbb{Z}}$$

ce qui signifie que $f_{F/\mathbb{Q}}$ divise $f_{F'/\mathbb{Q}}$ et il suffit de poser

$$f_{F'/F} = f_{F'/\mathbb{Q}} \cdot f_{F/\mathbb{Q}}^{-1} .$$

(iii) Il suffit de traiter le cas où $F = \mathbb{Q}$.
Les extensions $\mathbb{Q}\,(\mu_{p^m})$, $m \geq 1$, sont définies par les équations

$$T^{p^m} - 1 = 0 \,, \qquad m \geq 1 \,,$$

et définissent des revêtements finis étales de $\mathbb{Z}_{(p)} = \mathbb{Z}\,[p^{-1}]$.
De plus, pour tout nombre premier $\ell \neq p$, l'action de $\sigma_\ell = \mathrm{Frob}_\ell$ sur les groupes multiplicatifs $\{a \in \overline{\mathbb{F}}_\ell \mid a^{p^m} = 1\}$ se fait par $a \mapsto a^\ell$, si bien que l'image de σ_ℓ dans $\mathbb{Z}_p^\times$ est ℓ.

(iv) En effet, l'action de la conjugaison complexe sur les racines de l'unité a se fait par $a \mapsto a^{-1}$.

□

D'autre part, on a :

Proposition V.37. –

(i) *Il existe un unique homomorphisme continu*

$$\mathbb{Q}^\times \backslash \mathbb{A}_{\mathbb{Q}}^\times \to \widehat{\mathbb{Z}}^\times = \prod_p \mathbb{Z}_p^\times$$

tel que :

- *pour tout nombre premier p, la composante*

$$\mathbb{Q}^\times \backslash \mathbb{A}_{\mathbb{Q}}^\times \to \mathbb{Z}_p^\times$$

se factorise en

$$\mathbb{Q}^\times \backslash \mathbb{A}_{\mathbb{Q}}^\times / \prod_{\ell \neq p} \mathbb{Z}_\ell^\times \to \mathbb{Z}_p^\times$$

et envoie chaque uniformisante $\ell \in \mathbb{Q}_\ell$, $\ell \neq p$, sur l'entier $\ell \in \mathbb{Z}_p^\times$,

- *la composante*

$$\mathbb{Q}_\infty^\times = \mathbb{R}^\times \to \widehat{\mathbb{Z}}^\times$$

est égale à

$$a \mapsto \mathrm{signe}\,(a) \in \{\pm 1\} \,.$$

(ii) *Cet homomorphisme continu*

$$\mathbb{Q}^\times\backslash\mathbb{A}_\mathbb{Q}^\times \to \widehat{\mathbb{Z}}^\times$$

est surjectif, et il en est a fortiori de même du composé

$$\deg_\mathbb{Q} : \widehat{\mathbb{Q}^\times\backslash\mathbb{A}_\mathbb{Q}^\times} \to \widehat{\mathbb{Z}}^\times \to \widehat{\mathbb{Z}}\,.$$

Démonstration :

(i) Pour tout nombre premier p, l'homomorphisme

$$\mathbb{A}_\mathbb{Q}^\times \to \mathbb{Q}^\times\backslash\mathbb{A}_\mathbb{Q}^\times \to \mathbb{Z}_p^\times$$

est déjà déterminé en les facteurs $\mathbb{Q}_\ell^\times$ de $\mathbb{A}_\mathbb{Q}^\times$, $\ell \neq p$, et en le facteur $\mathbb{Q}_\infty^\times = \mathbb{R}^\times$.
Reste seulement le facteur $\mathbb{Q}_p^\times$.
Tout élément $f_p \in \mathbb{Q}_p^\times$ s'écrit de manière unique sous la forme

$$f_p = p^{v_p(f_p)} \cdot f'_p\,, \qquad \text{avec} \quad f'_p \in \mathbb{Z}_p^\times\,,$$

et l'unique possibilité est de définir l'homomorphisme

$$\mathbb{Q}_p^\times \to \mathbb{Z}_p^\times$$

par

$$f_p \mapsto f_p'^{-1}\,.$$

(ii) est évident sur la construction. □

Nous pouvons maintenant énoncer, sans démonstration, le théorème suivant :

Théorème V.38. –

(i) *Il existe une unique famille d'homomorphismes continus*

$$\Gamma_F = \pi_1(F,\overline{\mathbb{Q}}) \to \widehat{F^\times\backslash\mathbb{A}_F^\times}$$

indexés par les extensions finies F de $\mathbb{Q}$ plongées dans $\overline{\mathbb{Q}}$, vérifiant les deux conditions suivantes :

- *pour toutes extensions finies $F \subset F' \subset \overline{\mathbb{Q}}$, le carré*

$$\begin{tikzcd}
\Gamma_{F'} \arrow[r] \arrow[d] & \widehat{F'^\times\backslash\mathbb{A}_{F'}^\times} \arrow[d, "\mathrm{Nm}"] \\
\Gamma_F \arrow[r] & \widehat{F^\times\backslash\mathbb{A}_F^\times}
\end{tikzcd}$$

  est commutatif,

- *pour toute extension finie $F \subset \overline{\mathbb{Q}}$, le carré*

$$\begin{tikzcd}
\Gamma_F \arrow[rr, "\deg_F"] \arrow[d] & & \widehat{\mathbb{Z}} \arrow[d, "f_{F/\mathbb{Q}}"] \\
\widehat{F^\times\backslash\mathbb{A}_F^\times} \arrow[r, "\mathrm{Nm}"] & \widehat{\mathbb{Q}^\times\backslash\mathbb{A}_\mathbb{Q}^\times} \arrow[r, "\deg_\mathbb{Q}"] & \widehat{\mathbb{Z}}
\end{tikzcd}$$

  est commutatif.

(ii) *Pour toute extension finie F, l'homomorphisme continu induit*

$$\Gamma_F^{\mathrm{ab}} \to \widehat{F^\times \backslash \mathbb{A}_F^\times}$$

n'est autre que l'isomorphisme du corps de classes du corollaire V.31(i).

$\square$

VI. Transformation de Fourier et formule de Poisson sur les adèles

1 Transformation de Fourier et formule de Poisson sur $\mathbb{R}$

Munissons $\mathbb{R}$ du caractère continu unitaire non trivial

$$\begin{array}{rcl} \psi_\infty : \mathbb{R} & \to & U(1) = \{z \in \mathbb{C}^\times \mid |z| = 1\}\,, \\ t & \mapsto & e^{2\pi i t}\,, \end{array}$$

et de l'unique mesure additive dt qui attribue le volume 1 au quotient compact $\mathbb{R}/\mathbb{Z}$ de $\mathbb{R}$ par le sous-groupe discret $\mathrm{Ker}\,(\psi_\infty) = \mathbb{Z}$.

Voici la définition de la transformation de Fourier sur $\mathbb{R}$:

Définition VI.1. –

Pour toute fonction intégrable

$$f : \mathbb{R} \to \mathbb{C}\,,$$

on appelle ψ_∞-transformée de Fourier de f la fonction

$$\begin{array}{rcl} \hat{f} : \mathbb{R} & \to & \mathbb{C}\,, \\ t' & \mapsto & \displaystyle\int_{\mathbb{R}} dt \cdot f(t) \cdot \psi_\infty(tt')\,. \end{array}$$

$\square$

On appelle fonctions de Schwartz sur $\mathbb{R}$ les fonctions

$$f : \mathbb{R} \to \mathbb{C}$$

qui sont

- de classe C^∞ au sens qu'elles admettent des dérivées $f^{(n)}$ à n'importe quel ordre $n \in \mathbb{N}$,
- à décroissance rapide au sens que pour tout $n \in \mathbb{N}$ et toute fonction polynomiale $P : \mathbb{R} \to \mathbb{R}$, le produit

  $$\mathbb{R} \ni t \mapsto |f^{(n)}(t) \cdot P(t)|$$

  est borné sur $\mathbb{R}$ par une constante.

On note $\mathcal{S}(\mathbb{R})$ le $\mathbb{C}$-espace vectoriel des fonctions de Schwartz.

Voici les principales propriétés formelles de la transformation de Fourier sur $\mathbb{R}$:

Proposition VI.2. –

(i) *La ψ_∞-transformation de Fourier*

$$f \mapsto \hat{f}$$

définit un endomorphisme $\mathbb{C}$-linéaire de l'espace $\mathcal{S}(\mathbb{R})$ des fonctions de Schwartz sur $\mathbb{R}$. De plus, on a pour toute fonction $f \in \mathcal{S}(\mathbb{R})$

$$\hat{f}'(t') = 2\pi i \cdot \int_{\mathbb{R}} dt \cdot (t \cdot f(t)) \cdot \psi_\infty(tt')$$

et

$$t' \cdot \hat{f}(t') = -\frac{1}{2\pi i} \int_{\mathbb{R}} dt \cdot f'(t) \cdot \psi_\infty(tt') \, .$$

(ii) *Pour toutes fonctions $f_1, f_2 \in \mathcal{S}(\mathbb{R})$, leur produit de convolution*

$$\begin{array}{rcl} f_1 * f_2 : \mathbb{R} & \to & \mathbb{C} \\ t' & \mapsto & \displaystyle\int_{\mathbb{R}} dt \cdot f_1(t) \cdot f_2(t' - t) \end{array}$$

est aussi dans $\mathcal{S}(\mathbb{R})$, et on a

$$\widehat{f_1 * f_2} = \hat{f}_1 \cdot \hat{f}_2 \, .$$

De même, leur produit $f_1 \cdot f_2$ est dans $\mathcal{S}(\mathbb{R})$, et on a

$$\widehat{f_1 \cdot f_2} = \hat{f}_1 * \hat{f}_2 \, .$$

(iii) *Pour toute $f \in \mathcal{S}(\mathbb{R})$ et tout élément $t_1 \in \mathbb{R}$, le produit*

$$t \mapsto f(t) \cdot \psi_\infty(tt_1)$$

est dans $\mathcal{S}(\mathbb{R})$ et admet pour ψ_∞-transformée de Fourier la fonction translatée

$$t' \mapsto \hat{f}(t' + t_1) \, .$$

De même, la fonction translatée

$$t \mapsto f(t + t_1)$$

est dans $\mathcal{S}(\mathbb{R})$ et admet pour ψ_∞-transformée de Fourier la fonction produit

$$t' \mapsto \hat{f}(t') \cdot \psi_\infty(-t_1 t') \, .$$

(iv) *Pour toute $f \in \mathcal{S}(\mathbb{R})$ et tout $\lambda \in \mathbb{R}^\times$, la fonction*

$$t \mapsto f^\lambda(t) = f(\lambda \cdot t)$$

est dans $\mathcal{S}(\mathbb{R})$ et admet pour ψ_∞-transformée de Fourier la fonction

$$\widehat{f^\lambda} : t' \mapsto \frac{1}{|\lambda|} \cdot \hat{f}\left(\frac{1}{\lambda} \cdot t'\right) \, .$$

Démonstration :

(i) La première formule se démontre en permutant l'opérateur de dérivation en t' et l'opérateur d'intégration $\int_{\mathbb{R}} dt$.

La seconde formule se déduit de la formule d'intégration par parties.

Le fait que la ψ_∞-transformation de Fourier stabilise $\mathcal{S}(\mathbb{R})$ résulte de ces deux formules.

(ii), (iii), (iv) Toutes les formules résultent de simples changements de variables d'intégration et sont laissées en exercice.

$\square$

On déduit de cette proposition :

Corollaire VI.3. –

(i) *La ψ_∞-transformation de Fourier définit un automorphisme de l'espace $\mathcal{S}(\mathbb{R})$.*
Son automorphisme réciproque est la $\overline{\psi}_\infty$-transformation de Fourier

$$f \mapsto \left[t' \mapsto \int_{\mathbb{R}} dt \cdot f(t) \cdot \overline{\psi}_\infty(tt')\right]$$

associée au caractère conjugué $\overline{\psi}_\infty = \psi_\infty^{-1} : t \mapsto e^{-2\pi i t}$.

(ii) *La ψ_∞-transformation de Fourier de $\mathcal{S}(\mathbb{R})$ est unitaire relativement au produit hermitien*

$$(f_1, f_2) \mapsto \langle f_1, f_2 \rangle = \int_{\mathbb{R}} dt \cdot f_1(t) \cdot \overline{f_2(t)}\,,$$

c'est-à-dire vérifie la formule

$$\langle \hat{f}_1, \hat{f}_2 \rangle = \langle f_1, f_2 \rangle\,, \qquad \forall\, f_1, f_2 \in \mathcal{S}(\mathbb{R})\,,$$

et donc en particulier

$$\|\hat{f}\|_2 = \|f\|_2\,, \qquad \forall\, f \in \mathcal{S}(\mathbb{R})\,,$$

si l'on note

$$\|f\|_2 = \left(\int_{\mathbb{R}} dt \cdot |f(t)|^2\right)^{\frac{1}{2}}\,.$$

Remarques :

(i) Il résulte de ces propriétés que la ψ_∞-transformation de Fourier définit un automorphisme de l'espace de Hilbert des fonctions de carré intégrable de $\mathbb{R}$ dans $\mathbb{C}$.

(ii) Un simple changement de variable montre que ces propriétés restent valides si l'on remplace le caractère $\psi_\infty : t \mapsto e^{2\pi i t}$ par

$$t \mapsto e^{2\pi i \cdot c_\infty \cdot t}\,, \quad \text{avec} \quad c_\infty \in \mathbb{R}^\times\,,$$

et que l'on multiplie la mesure de Lebesgue usuelle dt par le facteur $|c_\infty|^{1/2}$.

(iii) De même, si $\mathbb{C}$ est muni d'un caractère de la forme

$$\psi_\infty : \mathbb{C} \ni t \mapsto e^{2\pi i \cdot (c_\infty \cdot t + \overline{c}_\infty \cdot \overline{t})}\,, \quad \text{avec} \quad c_\infty \in \mathbb{C}^\times\,,$$

et de la mesure de Lebesgue usuelle multipliée par le facteur $2\,|c_\infty|$, notée dt, alors la ψ_∞-transformation de Fourier associée

$$f \mapsto \left[t' \mapsto \int_{\mathbb{C}} dt \cdot f(t) \cdot \psi_\infty(tt')\right]$$

définit un automorphisme de l'espace $\mathcal{S}(\mathbb{R})$ des fonctions de Schwartz sur $\mathbb{C} \cong \mathbb{R}^2$, et son automorphisme réciproque est la $\overline{\psi}_\infty$-transformation de Fourier

$$f \mapsto \left[t' \mapsto \int_{\mathbb{C}} dt \cdot f(t) \cdot \overline{\psi}_\infty(tt')\right].$$

De plus, la ψ_∞-transformation de Fourier sur $\mathbb{C}$ est unitaire, c'est-à-dire respecte le produit hermitien

$$(f_1, f_2) \mapsto \langle f_1, f_2\rangle = \int_{\mathbb{C}} dt \cdot f_1(t) \cdot \overline{f_2(t)}.$$

Ces propriétés se déduisent facilement de celles sur $\mathbb{R}$ en utilisant l'isomorphisme $\mathbb{C} \cong \mathbb{R}^2$.

Démonstration :

(i) Il s'agit de prouver que, pour toute fonction $f \in \mathcal{S}(\mathbb{R})$, on a

$$\hat{\hat{f}}(t) = f(-t), \qquad \forall\, t \in \mathbb{R}.$$

Or on sait déjà d'après la proposition VI.2 que l'opérateur composé

$$f \mapsto \hat{\hat{f}}$$

commute avec la multiplication des fonctions

$$(f_1, f_2) \mapsto f_1 \cdot f_2$$

et qu'il transforme l'opérateur de multiplication par t

$$f \mapsto [t \mapsto t \cdot f(t)]$$

en l'opérateur de multiplication par $-t$.
Or, pour toutes fonctions $f_1, f_2 \in \mathcal{S}(\mathbb{R})$ et tout élément $t_0 \in \mathbb{R}$, il existe une fonction $f \in \mathcal{S}(\mathbb{R})$ telle que

$$f_1(t) \cdot f_2(t_0) - f_2(t) \cdot f_1(t_0) = (t - t_0) \cdot f(t), \qquad \forall\, t \in \mathbb{R}.$$

On en déduit

$$\hat{\hat{f}}_1(t) \cdot f_2(t_0) - \hat{\hat{f}}_2(t) \cdot f_1(t_0) = (-t - t_0) \cdot \hat{\hat{f}}(t), \qquad \forall\, t \in \mathbb{R},$$

et donc

$$\hat{\hat{f}}_1(-t_0) \cdot f_2(t_0) = \hat{\hat{f}}_2(-t_0) \cdot f_1(t_0).$$

Par conséquent, il existe une fonction

$$\mathbb{R} \ni t \mapsto g(t)$$

telle que, pour toute $f \in \mathcal{S}(\mathbb{R})$, on ait

$$\hat{\hat{f}}(t) = f(-t) \cdot g(t), \qquad \forall\, t \in \mathbb{R}.$$

De plus, l'opérateur $f \mapsto \hat{\hat{f}}$ transforme les translations par $t \in \mathbb{R}$ en les translations par $-t$. Donc la fonction g est constante, et il existe $\lambda \in \mathbb{R}$ tel que

$$\hat{\hat{f}}(t) = \lambda \cdot f(-t), \qquad \forall\, f \in \mathcal{S}(\mathbb{R}), \quad \forall\, t \in \mathbb{R}.$$

Enfin, on a $\lambda = 1$ puisque

$$\widehat{\widehat{f_1 \cdot f_2}} = \hat{\hat{f}}_1 \cdot \hat{\hat{f}}_2, \qquad \forall\, f_1, f_2 \in \mathcal{S}(\mathbb{R}).$$

(ii) résulte de (i) puisque le conjugué $\overline{U}$ de l'opérateur U de ψ_∞-transformation de Fourier est son inverse. En effet, pour tous $f_1, f_2 \in \mathcal{S}(\mathbb{R})$, on a

$$\langle U(f_1), U(f_2)\rangle = \langle \overline{U} \circ U(f_1), f_2\rangle = \langle f_1, f_2\rangle \, .$$

□

Une autre propriété très importante de la transformation de Fourier sur $\mathbb{R}$ est la formule de Poisson :

Théorème VI.4. –

Pour toute fonction $f \in \mathcal{S}(\mathbb{R})$, la série

$$\sum_{n\in\mathbb{Z}} f(n)$$

est absolument convergente, et on a la formule

$$\sum_{n\in\mathbb{Z}} f(n) = \sum_{n\in\mathbb{Z}} \hat{f}(n) \, .$$

Démonstration :

Comme f est à décroissance rapide ainsi que $\hat{f}$, la fonction

$$\begin{array}{rcl} h : \mathbb{R}/\mathbb{Z} & \to & \mathbb{C} \\ t & \mapsto & \left(\displaystyle\sum_{n\in\mathbb{Z}} f(t+n)\right) - \displaystyle\sum_{n\in\mathbb{Z}} \hat{f}(n) \cdot e^{-2\pi i \cdot nt} \end{array}$$

est bien définie et continue.

De plus, on a

$$\int_{\mathbb{R}/\mathbb{Z}} dt \cdot h(t) \cdot e^{2\pi i \cdot nt} = 0 \, , \qquad \forall \, n \in \mathbb{Z} \, ,$$

puisque, pour tous entiers $n, n' \in \mathbb{Z}$

$$\int_{\mathbb{R}/\mathbb{Z}} dt \cdot e^{2\pi i \cdot nt} \cdot e^{-2\pi i \cdot n't} = \begin{cases} 1 & \text{si } n = n' \, , \\ 0 & \text{sinon} \, . \end{cases}$$

Pour conclure, il suffit de démontrer que si une fonction continue

$$h : U(1) = \{z \in \mathbb{C} \mid |z| = 1\} \to \mathbb{C}$$

vérifie

$$\int_{U(1)} dz \cdot h(z) \cdot P(z, \overline{z}) = 0$$

pour tout polynôme P en z et $\overline{z}$, alors on a nécessairement

$$h = 0 \, .$$

Cela résulte de ce que, pour tout $z_0 \in U(1)$ et tout $\lambda \in \mathbb{R}$

$$e^{-\lambda \cdot |z - z_0|^2} = \sum_{n \geq 0} \frac{(-\lambda)^n}{n!} \, (z - z_0)^n \cdot (\overline{z} - \overline{z}_0)^n$$

uniformément en $z \in \mathbb{C}$, et

$$\lim_{\lambda \mapsto +\infty} \int_{U(1)} dz \cdot \sqrt{\lambda} \cdot h(z) \cdot e^{-\lambda \cdot (z - z_0)^2} = h(z_0) \cdot \int_{U(1)} dz \cdot e^{-|z|^2} \, .$$

□

2 Transformation de Fourier sur un corps local ultramétrique

Dans ce paragraphe, on considère un corps global F puis le corps local ultramétrique F_x associé à n'importe quel point fermé $x \in |X_F|$ de la courbe X_F.

On considère également n'importe quel caractère continu unitaire non trivial

$$\psi_x : F_x \to U(1) = \{z \in \mathbb{C}^\times \mid |z| = 1\}\,.$$

On appelle "conducteur de ψ_x" et on note N_{ψ_x} le plus petit entier $N \in \mathbb{Z}$ tel que la restriction de ψ_x à

$$\{a_x \in F_x \mid |a_x|_x \leq q_x^{-N}\}$$

soit triviale.

On munit F_x de l'unique mesure additive da_x qui attribue au sous-groupe ouvert compact O_x de F_x le volume

$$\mathrm{vol}\,(O_x) = q_x^{N_{\psi_x}/2}\,.$$

Ces choix étant faits, on peut définir l'opérateur de ψ_x-transformation de Fourier sur F_x :

Définition VI.5. –

Pour toute fonction intégrable

$$f_x : F_x \to \mathbb{C}\,,$$

on appelle ψ_x-transformée de Fourier de f_x la fonction

$$\begin{array}{rcl} \hat{f}_x : F_x & \to & \mathbb{C}\,, \\ b_x & \mapsto & \displaystyle\int_{F_x} da_x \cdot f_x(a_x) \cdot \psi_x(a_x\, b_x)\,. \end{array}$$

$\square$

On appelle fonctions de Schwartz sur F_x les fonctions

$$f_x : F_x \to \mathbb{C}$$

qui sont localement constantes et supportées par une partie compacte de F_x.

On note $\mathcal{S}(F_x)$ le $\mathbb{C}$-espace vectoriel des fonctions de Schwartz.

Voici les principales propriétés formelles de la ψ_x-transformation de Fourier sur F_x :

Proposition VI.6. –

(i) *La ψ_x-transformation de Fourier*

$$f_x \mapsto \hat{f}_x$$

définit un endomorphisme $\mathbb{C}$-linéaire de l'espace $\mathcal{S}(F_x)$ des fonctions de Schwartz sur F_x.

De plus, en notant $\mathbb{I}_{x,N}$, $N \in \mathbb{Z}$, les fonctions caractéristiques des sous-groupes ouverts compacts

$$\{a_x \in F_x \mid |a_x|_x \leq q_x^{-N}\}\,,$$

on a

$$\widehat{\mathbb{I}_{x,N}} = q_x^{-N} \cdot q_x^{N_{\psi_x}/2} \cdot \mathbb{I}_{x,N_{\psi_x}-N}\,.$$

(ii) *Pour toutes fonctions $f_1, f_2 \in \mathcal{S}(F_x)$, leur produit de convolution*

$$\begin{array}{rcl} f_1 * f_2 : \mathbb{R} & \to & \mathbb{C} \\ b_x & \mapsto & \displaystyle\int_{F_x} da_x \cdot f_1(a_x) \cdot f_2(b_x - a_x) \end{array}$$

est aussi dans $\mathcal{S}(F_x)$, et on a

$$\widehat{f_1 * f_2} = \hat{f}_1 \cdot \hat{f}_2 \, .$$

De même, leur produit $f_1 \cdot f_2$ est dans $\mathcal{S}(F_x)$, et on a

$$\widehat{f_1 \cdot f_2} = \hat{f}_1 * \hat{f}_2 \, .$$

(iii) *Pour toute $f_x \in \mathcal{S}(F_x)$ et tout élément $t_x \in F_x$, le produit*

$$a_x \mapsto f_x(a_x) \cdot \psi_x(a_x \, t_x)$$

est dans $\mathcal{S}(F_x)$ et admet pour ψ_x-transformée de Fourier la fonction translatée

$$b_x \mapsto \hat{f}_x(b_x + t_x) \, .$$

De même, la fonction translatée

$$a_x \mapsto f_x(a_x + t_x)$$

est dans $\mathcal{S}(F_x)$ et admet pour ψ_x-transformée de Fourier la fonction produit

$$b_x \mapsto \hat{f}_x(b_x) \cdot \psi_x(-b_x \, t_x) \, .$$

(iv) *Pour toute $f_x \in \mathcal{S}(F_x)$ et tout $\lambda \in F_x^\times$, la fonction*

$$a_x \mapsto f_x^\lambda(a_x) = f_x(\lambda \cdot a_x)$$

est dans $\mathcal{S}(F_x)$ et admet pour ψ_x-transformée de Fourier la fonction

$$\widehat{f_x^\lambda} : b_x \mapsto \frac{1}{|\lambda|_x} \cdot \hat{f}_x \left(\frac{1}{\lambda} \cdot b_x \right) \, .$$

Démonstration :

(i) Soit $f_x \in \mathcal{S}(F_x)$.
Il existe un entier $N_1 \in \mathbb{Z}$ tel que f_x soit supportée par le sous-groupe ouvert compact

$$\left\{ a_x \in F_x \mid |a_x|_x \le q_x^{-N_1} \right\} ,$$

et il existe un entier $N_2 \in \mathbb{Z}$ tel que f_x soit invariante par le sous-groupe ouvert compact

$$\left\{ a_x \in F_x \mid |a_x|_x \le q_x^{-N_2} \right\} .$$

Alors $\hat{f}_x$ est invariante par

$$\left\{ b_x \in F_x \mid |b_x|_x \le q_x^{-N_{\psi_x} + N_1} \right\}$$

et elle est supportée par

$$\left\{ b_x \in F_x \mid |b_x|_x \le q_x^{-N_{\psi_x} + N_2} \right\} .$$

Cela résulte en effet du lemme suivant :

Lemme VI.7. –

Pour tout caractère continu

$$\psi'_x : F_x \to \mathbb{C}^\times$$

et pour tout sous-groupe ouvert compact V_x de F_x, on a

$$\int_{V_x} da_x \cdot \psi'_x(a_x) = \begin{cases} 0 & \textit{si } \psi'_x \textit{ est non trivial sur } V_x, \\ \mathrm{vol}\,(V_x) & \textit{si } \psi'_x \textit{ est trivial sur } V_x. \end{cases}$$

Démonstration du lemme :

Comme la mesure da_x est invariante par translation, on a pour tout élément $v_x \in V_x$

$$\int_{V_x} da_x \cdot \psi'_x(a_x) = \int_{V_x} da_x \cdot \psi'_x(a_x + v_x) = \psi'_x(v_x) \cdot \int_{V_x} da_x \cdot \psi'_x(a_x)\,.$$

Cela impose

$$\int_{V_x} da_x \cdot \psi'_x(a_x) = 0$$

si ψ'_x est non trivial sur V_x.

Sinon, la formule est tautologique. □

Suite de la démonstration de la proposition VI.6 :

Le calcul des $\widehat{\mathbb{1}_{x,N}}$ dans (i) se déduit également du lemme VI.7 ci-dessus.

Enfin, toutes les formules de (ii), (iii) et (iv) résultent de simples changements de variables d'intégration et sont laissées en exercice.

□

On déduit de la proposition VI.6 :

Corollaire VI.8. –

(i) *La ψ_x-transformation de Fourier définit un automorphisme de l'espace $\mathcal{S}(F_x)$.*
Son automorphisme réciproque est la $\overline{\psi}_x$-transformation de Fourier

$$f_x \mapsto \left[b_x \mapsto \int_{F_x} da_x \cdot f_x(a_x) \cdot \overline{\psi}_x(a_x\, b_x) \right]$$

associé au caractère conjugué $\overline{\psi}_x = \psi_x^{-1} : F_x \to U(1) \subset \mathbb{C}^\times$.

(ii) *La ψ_x-transformation de Fourier $\mathcal{S}(F_x)$ est un opérateur unitaire relativement au produit hermitien*

$$(f_1, f_2) \mapsto \langle f_1, f_2 \rangle = \int_{F_x} da_x \cdot f_1(a_x) \cdot \overline{f_2(a_x)}\,.$$

Remarque :

Il résulte de (ii) que la ψ_x-transformation de Fourier définit un automorphisme de l'espace de Hilbert des fonctions de carré intégrable de F_x dans $\mathbb{C}$.

Démonstration :

(i) Il résulte de la proposition VI.6(i) que l'opérateur composé

$$f_x \mapsto \hat{\hat{f}}_x$$

transforme chaque fonction caractéristique $\mathbb{1}_{x,N}$, $N \in \mathbb{Z}$, en elle-même.
De plus, il résulte de la proposition VI.6(iii) qu'il transforme les translations par les $t_x \in F_x$ en les translations par les $-t_x$.
On conclut comme voulu que, pour toute $f_x \in \mathcal{S}(F_x)$,

$$\hat{\hat{f}}_x(a_x) = f_x(-a_x)\,, \quad \forall\, a_x \in F_x\,.$$

(ii) est conséquence de (i). □

3 Transformation de Fourier sur les adèles

Dans ce paragraphe, on considère un corps global F, c'est-à-dire

- ou bien le corps des fonctions rationnelles d'une courbe X_F projective, lisse et géométriquement connexe sur un corps fini $\mathbb{F}_q$,
- ou bien une extension finie de $\mathbb{Q}$, à laquelle sont associés l'anneau A_F normalisé de $\mathbb{Z}$ dans F et la courbe arithmétique régulière $X_F = \mathrm{Spec}\,(A_F)$.

Que F soit un corps de fonctions ou un corps de nombres, il est plongé comme sous-groupe discret dans l'anneau topologique $\mathbb{A}_F$ des adèles. On a :

Lemme VI.9. –

(i) *Le quotient compact $\mathbb{A}_F/F$ admet des caractères continus unitaires non triviaux*

$$\psi : \mathbb{A}_F/F \to U(1) \subset \mathbb{C}^\times\,.$$

(ii) *Tout tel caractère continu unitaire non trivial*

$$\psi : \mathbb{A}_F \to U(1) \subset \mathbb{C}^\times$$

invariant par F, se décompose comme un produit

$$\psi = \prod_{x \in |F|} \psi_x$$

de caractères continus unitaires non triviaux

$$\psi_x : F_x \to U(1) \subset \mathbb{C}^\times\,.$$

En toute place ultramétrique $x \in |X_F|$, ψ_x a un conducteur N_{ψ_x}, et celui-ci est égal à 0 en presque toute place.

(iii) *De plus, si F est un corps de nombres et x une place archimédienne en laquelle $F_x \cong \mathbb{R}$ [resp. $F_x \cong \mathbb{C}$], le caractère continu unitaire non trivial*

$$\psi_x : F_x \to U(1) \subset \mathbb{C}^\times$$

s'écrit de manière unique sous la forme

$$F_x \cong \mathbb{R} \ni t \mapsto e^{2\pi i \cdot c_x \cdot t}\,, \quad \textit{avec} \quad c_x \in \mathbb{R}^\times\,,$$

[resp.

$$F_x \cong \mathbb{C} \ni t \mapsto e^{2\pi i \cdot (c_x \cdot t + \bar{c}_x \cdot \bar{t})}\,, \quad \textit{avec} \quad c_x \in \mathbb{C}^\times \;]\,.$$

Démonstration :

(i) Si F est un corps de nombres [resp. un corps de fonctions], c'est une extension finie séparable de $\mathbb{Q}$ [resp. de $\mathbb{F}_q(T)$], et on dispose de l'homomorphisme continu surjectif induit

$$\mathrm{Tr} : \mathbb{A}_F/F \to \mathbb{A}_{\mathbb{Q}}/\mathbb{Q}$$

[resp.

$$\mathrm{Tr} : \mathbb{A}_F/F \to \mathbb{A}_{\mathbb{F}_q(T)}/\mathbb{F}_q(T) \ ] .$$

Il suffit donc de considérer le cas où

$$F = \mathbb{Q} \qquad [\text{resp.} \quad F = \mathbb{F}_q(T) \ ] .$$

Si $F = \mathbb{Q}$, le quotient $\mathbb{A}_F/(F + O_{\mathbb{A}_F^u})$ s'identifie à

$$F_\infty/A_F = \mathbb{R}/\mathbb{Z}$$

qui admet des caractères continus unitaires non triviaux.
Si $F = \mathbb{F}_q(T)$, $\mathbb{A}_F/F$ admet pour quotient

$$\mathbb{F}_q(T)_\infty/\mathbb{F}_q[T] = \mathbb{F}_q[\![T^{-1}]\!][T]/\mathbb{F}_q[T]$$

qui admet des caractères continus unitaires non triviaux.

(ii) Comme

$$\mathbb{A}_F = \{(f_x \in F_x)_{x\in|F|} \mid |f_x|_x \le 1 \quad \text{en presque toute place} \quad x \in |X_F|\} ,$$

tout caractère continu unitaire

$$\psi : \mathbb{A}_F \to U(1) \subset \mathbb{C}^\times$$

se décompose de manière unique comme un produit de caractères continus unitaires

$$\psi_x : F_x \to U(1) \subset \mathbb{C}^\times .$$

Si ψ est non trivial, il en est de même de chaque facteur ψ_x, $x \in |F|$, car la somme $F+F_x$ est toujours dense dans $\mathbb{A}_F$.
Alors tous les ψ_x, $x \in |X_F|$, ont un conducteur $N_{\psi_x} \in \mathbb{Z}$.
Tout voisinage ouvert de 1 dans le cercle $U(1)$ a pour image réciproque dans $\mathbb{A}_F^u$ un ouvert qui contient 0 et donc aussi un sous-groupe ouvert. Donc le noyau de ψ contient nécessairement un sous-groupe ouvert de $\mathbb{A}_F^u$. Cela impose que

$$N_{\psi_x} \le 0$$

en presque toute place $x \in |X_F|$.
Comme ψ est trivial sur le sous-groupe

$$F + \left\{(f_x \in F_x)_{x\in|X_F|} \mid |f_x|_x \le q_x^{-N_{\psi_x}}\right\} ,$$

celui-ci ne peut être dense dans $\mathbb{A}_F$, et cela impose que

$$N_{\psi_x} \ge 0$$

en presque toute place $x \in |X_F|$.

(iii) Tout caractère continu unitaire non trivial de $\mathbb{R}$ ou $\mathbb{C}$ s'écrit en effet sous cette forme. □

Choisissons donc un caractère continu unitaire non trivial

$$\psi = \prod_{x \in |F|} \psi_x : \mathbb{A}_F / F \to U(1) \subset \mathbb{C}^\times .$$

En toute place ultramétrique $x \in |X_F|$, on munit F_x de l'unique mesure additive da_x qui attribue au sous-groupe ouvert compact O_x de F_x le volume

$$\mathrm{vol}\,(O_x) = q_x^{N_{\psi_x}/2} .$$

Si F est un corps de nombres et $x \in |F|_\infty$ une de ses places archimédiennes, on munit $F_x \cong \mathbb{R}$ [resp. $F_x \cong \mathbb{C}$] de la mesure de Lebesgue usuelle multipliée par le facteur $|c_x|^{1/2}$ [resp. $2\,|c_x|$] si le caractère $\psi_x : F_x \to U(1) \subset \mathbb{C}^\times$ a la forme

$$\mathbb{R} \ni t \mapsto e^{2\pi i \cdot c_2 \cdot t} \qquad [\text{resp.} \quad \mathbb{C} \ni t \mapsto e^{2\pi i \cdot (c_x \cdot t + \overline{c}_x \cdot \overline{t})}\;] .$$

Alors $F_\infty = \prod\limits_{x \in |F|_\infty} F_x$ se trouve muni du caractère non trivial

$$\psi_\infty = \prod_{x \in |F|_\infty} \psi_x : F_\infty \to U(1) \subset \mathbb{C}^\times$$

et de la mesure $da_\infty = \bigotimes\limits_{x \in |F|_\infty} da_x$.

Puis, que F soit un corps de nombres ou un corps de fonctions, $\mathbb{A}_F$ se trouve muni de la mesure additive produit

$$da = \bigotimes_{x \in |F|} da_x .$$

On peut maintenant définir l'opérateur de ψ-transformation de Fourier sur $\mathbb{A}_F$:

Définition VI.10. –

Pour toute fonction intégrable

$$f : \mathbb{A}_F \to \mathbb{C} ,$$

on appelle ψ-transformée de Fourier de f la fonction

$$\begin{aligned} \hat{f} : \mathbb{A}_F &\to \mathbb{C} , \\ b &\mapsto \int_{\mathbb{A}_F} da \cdot f(a) \cdot \psi(ab) . \end{aligned}$$

□

Si F est un corps de fonctions, on appelle fonctions de Schwartz sur $\mathbb{A}_F$ les fonctions

$$f : \mathbb{A}_F \to \mathbb{C}$$

qui sont localement constantes et supportées par une partie compacte de $\mathbb{A}_F$. On note $\mathcal{S}(\mathbb{A}_F)$ leur espace.

Si F est un corps de nombres, on appelle fonctions de Schwartz sur $F_\infty = F \otimes_{\mathbb{Q}} \mathbb{R}$ les fonctions

$$f : F_\infty \to \mathbb{C}$$

qui sont :

- de classe C^∞ au sens qu'elles admettent des dérivées partielles
$$\frac{\partial^{n_1}}{\partial t_1} \cdots \frac{\partial^{n_d}}{\partial t_d} f$$
de n'importe quels ordres $n_1, \ldots, n_d \in \mathbb{N}$, pour un choix de coordonnées $(t_1, \ldots, t_d)$ de $F_\infty \cong \mathbb{R}^d$,
- à décroissance rapide au sens que pour tous $n_1, \ldots, n_d \in \mathbb{N}$ et toute fonction polynomiale $P : F_\infty \cong \mathbb{R}^d \to \mathbb{R}$, le produit
$$\mathbb{R}^d \ni t \mapsto \left| \frac{\partial^{n_1}}{\partial t_1} \cdots \frac{\partial^{n_d}}{\partial t_d} f(t) \cdot P(t) \right|$$
est borné sur $\mathbb{R}^d$ par une constante. On note $\mathcal{S}(F_\infty)$ leur espace.

Puis on appelle fonctions de Schwartz sur $\mathbb{A}_F$ les fonctions
$$f : \mathbb{A}_F = \mathbb{A}_F^u \times F_\infty \to \mathbb{C}$$
telles que
- pour tout $a \in \mathbb{A}_F^u$, la fonction induite
$$F_\infty \ni t \mapsto f(a,t)$$
est élément de $\mathcal{S}(F_\infty)$,
- en la variable $a \in \mathbb{A}_F^u$, les fonctions $a \mapsto f(a,t)$, $t \in F_\infty$, sont supportées par une partie compacte de $\mathbb{A}_F^u$ indépendante de t et invariantes par un sous-groupe ouvert de $\mathbb{A}_F^u$ indépendant de t.

Les transformations de Fourier locales et globales sont compatibles au sens suivant :

Lemme VI.11. –

En les places ultramétriques $x \in |X_F|$ de F, considérons des fonctions de Schwartz
$$f_x : F_x \to \mathbb{C}$$
presque toutes égales aux fonctions caractéristiques $\mathbb{I}_{O_x}$ des sous-groupes ouverts compacts $O_x \subset F_x$.

De plus, si F est un corps de nombres, considérons une fonction de Schwartz
$$f_x : F_x \to \mathbb{C}$$
en chaque place archimédienne $x \in |F|_\infty$.

Alors la fonction produit
$$f = \bigotimes_{x \in |F|} f_x : \mathbb{A}_F \to \mathbb{C}$$
est une fonction de Schwartz, et on a
$$\hat{f} = \bigotimes_{x \in |F|} \hat{f}_x$$
à condition de poser en chaque place x archimédienne
$$\hat{f}_x(t'_x) = \int_{F_x} dt_x \cdot \psi_x(t_x\, t'_x) \cdot f_x(t_x)$$
où dt_x désigne la mesure additive de $F_x \cong \mathbb{R}$ ou $\mathbb{C}$ choisie plus haut en fonction de ψ_x.

Démonstration :

C'est immédiat sur les définitions. $\square$

Les propriétés formelles des transformations de Fourier locales entraînent celles de la transformation de Fourier globale :

Corollaire VI.12. –

(i) *La ψ-transformation de Fourier*
$$f \mapsto \hat{f}$$
définit un automorphisme $\mathbb{C}$-linéaire de l'espace $\mathcal{S}(\mathbb{A}_F)$ des fonctions de Schwartz sur $\mathbb{A}_F$.

(ii) *Pour toutes fonctions $f_1, f_2 \in \mathcal{S}(\mathbb{A}_F)$, leur produit de convolution*
$$\begin{array}{rcl} f_1 * f_2 : \mathbb{A}_F & \to & \mathbb{C} \\ b & \mapsto & \displaystyle\int_{\mathbb{A}_F} da \cdot f_1(a) \cdot f_2(b-a) \end{array}$$
est aussi dans $\mathcal{S}(\mathbb{A}_F)$, et on a
$$\widehat{f_1 * f_2} = \hat{f}_1 \cdot \hat{f}_2 \,.$$
De même, leur produit $f_1 \cdot f_2$ est dans $\mathcal{S}(\mathbb{A}_F)$, et on a
$$\widehat{f_1 \cdot f_2} = \hat{f}_1 * \hat{f}_2 \,.$$

(iii) *Pour toute $f \in \mathcal{S}(\mathbb{A}_F)$ et tout élément $t \in \mathbb{A}_F$, le produit*
$$a \mapsto f(a) \cdot \psi(ta)$$
est dans $\mathcal{S}(\mathbb{A}_F)$ et admet pour ψ-transformée de Fourier la fonction translatée
$$b \mapsto \hat{f}(b+t) \,.$$
De même, la fonction translatée
$$a \mapsto f(a+t)$$
est dans $\mathcal{S}(\mathbb{A}_F)$ et admet pour ψ-transformée de Fourier la fonction produit
$$b \mapsto \hat{f}(b) \cdot \psi(-tb) \,.$$

(iv) *Pour toute $f \in \mathcal{S}(\mathbb{A}_F)$ et tout $\lambda = (\lambda_x)_{x \in |F|} \in \mathbb{A}_F^\times$, la fonction*
$$a \mapsto f^\lambda(a) = f(\lambda \cdot a)$$
est dans $\mathcal{S}(\mathbb{A}_F)$ et admet pour ψ-transformée de Fourier la fonction
$$\widehat{f^\lambda} : b \mapsto \frac{1}{|\lambda|} \cdot \hat{f}\left(\frac{1}{\lambda} \cdot b\right)$$
où $|\lambda| = \prod_{x \in |F|} |\lambda_x|_x$. $\square$

Corollaire VI.13. –

(i) *La ψ-transformation de Fourier définit un automorphisme de l'espace $\mathcal{S}(\mathbb{A}_F)$.*
Son automorphisme réciproque est la $\overline{\psi}$-transformation de Fourier

$$f \mapsto \left[b \mapsto \int_{\mathbb{A}_F} da \cdot f(a) \cdot \overline{\psi}(ab) \right]$$

associée au caractère conjugué

$$\overline{\psi} = \psi^{-1} : \mathbb{A}_F \to \mathbb{A}_F/F \to U(1) \subset \mathbb{C}^\times \,.$$

(ii) *La ψ-transformation de Fourier $\mathcal{S}(\mathbb{A}_F)$ est un opérateur unitaire relativement au produit hermitien*

$$(f_1, f_2) \mapsto \langle f_1, f_2 \rangle = \int_{\mathbb{A}_F} da \cdot f_1(a) \cdot \overline{f_2(a)} \,.$$

4 Formule de Poisson sur les adèles

Comme au paragraphe précédent, on considère un corps global F et un caractère continu unitaire non trivial

$$\psi = \prod_{x \in |F|} \psi_x : \mathbb{A}_F \to \mathbb{A}_F/F \to U(1) \subset \mathbb{C}^\times \,.$$

Ce caractère induit une mesure additive da_x de F_x en toute place $x \in |F|$ puis une mesure additive globale

$$da = \bigotimes_{x \in |F|} da_x$$

de $\mathbb{A}_F$.

Le but de ce paragraphe est de démontrer la formule suivante, appelée formule de Poisson pour les adèles :

Théorème VI.14. –

Pour toute fonction de Schwartz

$$f : \mathbb{A}_F \to \mathbb{C} \,,$$

la série

$$\sum_{\gamma \in F} f(\gamma)$$

est absolument convergente et on a

$$\sum_{\gamma \in F} f(\gamma) = \sum_{\gamma \in F} \hat{f}(\gamma) \,.$$

Démonstration :

On commence par le lemme suivant :

Lemme VI.15. –

L'ensemble des $a \in \mathbb{A}_F$ tels que

$$\psi(a \cdot \gamma) = 1 \,, \qquad \forall \, \gamma \in F \,,$$

se confond avec le sous-groupe discret F de $\mathbb{A}_F$.

Démonstration :

Notons F^* cet ensemble. Il contient évidemment F.

De plus, il est stable par addition et par multiplication par les éléments de F. C'est donc un espace vectoriel sur F.

Tout élément $a \in F^*$ définit un caractère

$$\begin{array}{rcl} \psi_a : \mathbb{A}_F \longrightarrow \mathbb{A}_F/F & \longrightarrow & U(1) \subset \mathbb{C}^\times \\ b & \longmapsto & \psi_a(b) = \psi(ab) \end{array}$$

et pour tous éléments $a \neq a'$ de F^* les caractères associés

$$\psi_a, \psi_{a'} : \mathbb{A}_F/F \to U(1) \subset \mathbb{C}^\times$$

sont distincts.

Comme $\mathbb{A}_F/F$ est compact, il en résulte que le sous-groupe F^* de $\mathbb{A}_F$ est discret, donc aussi le sous-groupe F^*/F de $\mathbb{A}_F/F$.

Par conséquent, ce quotient F^*/F est fini. Mais comme F^* est un espace vectoriel sur F et que F est infini, on conclut comme voulu

$$F^* = F\,.$$

□

On déduit de ce lemme :

Corollaire VI.16. –

Les caractères continus unitaires

$$\psi' : \mathbb{A}_F/F \to \mathbb{C}^\times$$

sont exactement les caractères de la forme

$$\begin{array}{rcl} \mathbb{A}_F/F & \to & \mathbb{C}^\times \\ a & \mapsto & \psi(\gamma \cdot a)\,, \quad \textit{avec} \quad \gamma \in F\,. \end{array}$$

Démonstration :

En toute place $x \in |F|$, les caractères continus unitaires

$$\psi'_x : F_x \to \mathbb{C}^\times$$

sont exactement les caractères de la forme

$$\begin{array}{rcl} F_x & \to & \mathbb{C}^\times \\ a_x & \mapsto & \psi'_x(a_x) = \psi_x(c_x \cdot a_x)\,, \quad \text{avec} \quad c_x \in F_x\,, \end{array}$$

comme il résulte de la formule d'inversion de Fourier

$$f_x(a_x) = \int_{F_x} dt_x \cdot \hat{f}_x(-t_x) \cdot \psi_x(t_x\, a_x)$$

pour toute fonction de Schwartz $f_x \in \mathcal{S}(F_x)$.

Pour tout caractère continu unitaire

$$\psi' = \prod_{x \in |F|} \psi'_x : \mathbb{A}_F \to \mathbb{C}^\times \, ,$$

ses facteurs ψ'_x, $x \in |F|$, s'écrivent chacun sous la forme

$$\psi'_x(\bullet) = \psi_x(c_x \, \bullet) \, , \qquad \text{avec} \quad c_x \in F_x \, .$$

De plus, ψ' est nécessairement invariant par un sous-groupe ouvert de $O_{\mathbb{A}_F^u}$, ce qui signifie que les conducteurs $N_{\psi'_x}$ des ψ'_x vérifient

$$N_{\psi'_x} \leq 0$$

en presque toute place ultramétrique x.

Comme on a $N_{\psi_x} = 0$ en presque toute telle place, cela impose

$$v_x(c_x) \geq 0$$

en presque tout telle place, si bien que

$$c = (c_x)_{x \in |F|}$$

est un élément de $\mathbb{A}_F$.

On conclut d'après le lemme VI.15. □

On a d'autre part :

Lemme VI.17. –

Dans un groupe topologique abélien compact A tel que

- *un groupe abélien fini,*
- *une puissance finie de $\mathbb{R}/\mathbb{Z}$,*
- *un quotient $\mathbb{A}_F/F$ associé à un corps global F,*

et muni d'une mesure additive da, on a :

(i) *Pour toute paire de caractères continus unitaires*

$$\chi, \chi' : A \to \mathbb{C}^\times \, ,$$

on a la formule

$$\int_A da \cdot \chi(a) \cdot \overline{\chi'(a)} = \begin{cases} \mathrm{vol}\,(A) & si \quad \chi = \chi' \, , \\ 0 & si \quad \chi \neq \chi' \, . \end{cases}$$

(ii) *Le sous-espace engendré par les caractères continus unitaires*

$$\chi : A \to \mathbb{C}^\times$$

est dense dans l'espace de toutes les fonctions continues.

Démonstration :

(i) résulte de ce que, pour tout caractère continu unitaire

$$\chi : A \to \mathbb{C}^\times \, ,$$

on a

$$\int_A da \cdot \chi(a) = \begin{cases} \mathrm{vol}\,(A) & \text{si } \chi \text{ est trivial} \, , \\ 0 & \text{sinon} \, . \end{cases}$$

(ii) est déjà connu si A est égal à $\mathbb{R}/\mathbb{Z}$ et donc aussi s'il est isomorphe à une puissance de $\mathbb{R}/\mathbb{Z}$.
Tout groupe abélien A est un produit de groupes de la forme $\mathbb{Z}/n\,\mathbb{Z}$, donc on peut supposer que $A = \mathbb{Z}/n\,\mathbb{Z}$. Comme les caractères de $\mathbb{Z}/n\,\mathbb{Z}$ sont deux à deux orthogonaux, il suffit, pour montrer qu'ils engendrent tout l'espace de dimension n des applications

$$h : \mathbb{Z}/n\,\mathbb{Z} \to \mathbb{C}\,,$$

de prouver que leur nombre est égal à n. Or, ceci résulte de ce que $\{z \in \mathbb{C}^\times \mid z^n = 1\}$ compte exactement n éléments.
Voyons enfin le cas où

$$A = \mathbb{A}_F/F$$

pour n'importe quel corps global F.
Si F est un corps de fonctions, le quotient

$$I\backslash\mathbb{A}_F/F$$

de $\mathbb{A}_F/F$ par n'importe quel sous-groupe ouvert I de $O_{\mathbb{A}_F}$ est fini. Donc l'espace des fonctions

$$\mathbb{A}_F/F \to \mathbb{C}$$

invariantes par I est engendré par les caractères

$$\chi : I\backslash\mathbb{A}_F/F \to \mathbb{C}$$

et cela suffit à conclure.
Si F est un corps de nombres, le quotient

$$I\backslash\mathbb{A}_F/F$$

de $\mathbb{A}_F/F$ par n'importe quel sous-groupe ouvert I de $O_{\mathbb{A}_F^u}$ est isomorphe au produit d'un groupe abélien fini A et d'une puissance finie de $\mathbb{R}/\mathbb{Z}$. À nouveau, cela suffit à conclure.

□

On peut maintenant donner :

Fin de la démonstration du théorème VI.14 :

Pour toute fonction de Schwartz

$$f : \mathbb{A}_F \to \mathbb{C}\,,$$

la fonction

$$\begin{array}{rcl} h : \mathbb{A}_F/F & \to & \mathbb{C} \\ a & \mapsto & \left(\displaystyle\sum_{\gamma \in F} f(a+\gamma)\right) - \dfrac{1}{\mathrm{vol}\,(\mathbb{A}_F/F)} \cdot \displaystyle\sum_{\gamma\in F} \hat{f}(\gamma)\cdot\psi(-\gamma\cdot a) \end{array}$$

est bien définie et continue.

Considérons n'importe quel caractère continu unitaire

$$\chi : \mathbb{A}_F/F \to \mathbb{C}^\times\,.$$

D'après le corollaire VI.16, il est nécessiarement de la forme

$$a \mapsto \chi(a) = \psi(\gamma\cdot a)$$

pour un certain $\gamma \in F$.

Donc, d'après le lemme VI.17(i), on a nécessairement

$$\int_{\mathbb{A}_F/F} da \cdot h(a) \cdot \chi(a) = 0\,.$$

Le lemme VI.17(ii) impose alors que la fonction h est uniformément nulle, avec en particulier

$$\sum_{\gamma \in F} f(\gamma) = \frac{1}{\mathrm{vol}\,(\mathbb{A}_F/F)} \cdot \sum_{\gamma \in F} \hat{f}(\gamma)\,.$$

Mais comme

$$\hat{\hat{f}}(a) = f(-a)\,, \qquad \forall\, a \in \mathbb{A}_F\,,$$

on obtient

$$\mathrm{vol}\,(\mathbb{A}_F/F)^2 = 1$$

puis

$$\mathrm{vol}\,(\mathbb{A}_F/F) = 1\,.$$

Cela termine la démonstration du théorème. □

On note que l'on a prouvé au passage :

Corollaire VI.18. –

Pour tout corps global F, et si $\mathbb{A}_F$ est muni de la mesure additive "autoduale" da associée à un caractère non trivial

$$\psi = \prod_{x \in |F|} \psi_x : \mathbb{A}_F/F \to \mathbb{C}^\times\,,$$

c'est-à-dire pour laquelle l'opérateur

$$f \mapsto \hat{f} = \left[a' \mapsto \int_{\mathbb{A}_F} da \cdot f(a) \cdot \psi(aa')\right]$$

vérifie la formule

$$\hat{\hat{f}}(a) = f(-a)\,, \qquad \forall\, a \in \mathbb{A}_F\,, \qquad \forall\, f \in \mathcal{S}(\mathbb{A}_F)\,,$$

alors on a pour la mesure quotient induite par da

$$\mathrm{vol}\,(\mathbb{A}_F/F) = 1\,.$$

□

Bibliographie

- M. Atiyah et J.G. Macdonald, “Introduction to Commutative Algebra”, Addison-Wesley.
- J.W. Cassels et A. Fröhlich, “Algebraic Number Theory”, London Mathematical Society.
- A. Grothendieck, “SGA I : Revêtements étales et groupe fondamental”, réédition par la Société Mathématique de France.
- A. Grothendieck et J. Dieudonné, “EGA I : Le langage des schémas”, Publications mathématiques de l’IHES n$^{\text{o}}$ 4.
- D. Mumford, “The red book of varieties and schemes”, 2$^{\text{e}}$ édition, Springer LNM 1358.
- J. Neukirch, “Class Field Theory”, Springer GMW 280.