Sur le théorème de l'image ouverte pour les représentations galoisiennes associées aux modules de Drinfeld

Hanecart Valentin

2025

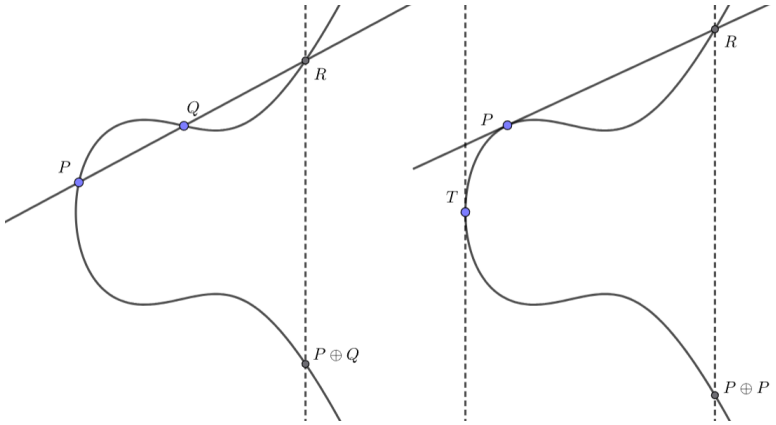
Sommaire

Introduction

1 - Le cas des courbes elliptiques

Avant de parler de modules de Drinfeld à proprement parler, commençons par faire un "état des lieux" au niveau des courbes elliptiques.

Considérons E une courbe elliptique sur un corps $\mathbb{K}$ donnée par une équation de Weierstrass. $E \subseteq \mathbb{P}^2_{\overline{\mathbb{K}}}$ consiste alors en l'ensemble des points $P := (x, y)$ satisfaisant l'équation de Weierstrass définissant E ainsi que le point à l'infini $O := [0, 1, 0]$. En considérant également une ligne $L \subseteq \mathbb{P}^2_{\overline{\mathbb{K}}}$, on obtient que L intersecte E en exactement 3 points notés P, Q et R pas nécessairement distincts (c'est-à-dire comptés avec multiplicité). Il est alors possible de munir E d'une loi $\oplus$ qui lui confère une structure de groupe abélien et dont la construction est brièvement rappelée via les deux dessins suivants (l'un dans le cas où les deux points sont distincts et l'autre dans le cas où l'on additionne un point avec lui-même) :



Pour tout $m \in \mathbb{Z}$, on définit également l'endomorphisme de E de multiplication-par-m (noté $[m]$) de la manière suivante :

$$[m](P) := \underbrace{P + P + \cdots + P}_{m \text{ fois si } m>0}, \quad [m](P) := \underbrace{-P - P - \cdots - P}_{m \text{ fois si } m<0} \text{ et } [0](P) := O.$$

Lorsque m est non nul, l'endomorphisme $[m]$ est non constant de sorte que l'application $[\cdot] : \mathbb{Z} \longrightarrow \mathrm{End}(E)$ est injective. De plus, lorsque $\mathrm{car}(\mathbb{K}) = 0$, alors généralement l'application $[\cdot]$ est surjective et donc l'ensemble des endomorphismes de E est réduit aux endomorphismes de multiplication-par-m pour tout $m \in \mathbb{Z}$. Cependant, il arrive que ça ne soit pas toujours le cas et on parle alors de **multiplication complexe** (ces courbes elliptiques possèdent également des propriétés intéressantes et on peut remarquer que lorsque $\mathbb{K}$ est un corps fini alors E est toujours à multiplication complexe). Un exemple de ce phénomène est donné lorsque $\mathbb{K} = \mathbb{C}$ et que E est définie par l'équation $y^2 = x^3 - x$ puisque dans ce cas on trouve un endomorphisme noté $[i]$ défini par $[i](x, y) = (-x, iy)$ (où $i^2 = -1$).

On peut également s'intéresser au sous-groupe des points de m-torsion sur E défini pour $m \in \mathbb{N}^*$ par

$$E[m] := \{P \in E \mid [m](P) = O\}$$

et à partir de maintenant on prend $\mathbb{K}$ de caractéristique nulle afin de simplifier les énoncés. Pour $m \in \mathbb{N}^*$, on a l'isomorphisme de groupes abstraits $E[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$. Or, le groupe $E[m]$ vient avec une structure bien plus

considérable qu'un groupe abstrait. En effet, par exemple, chaque élément σ de $\mathrm{Gal}\left(\overline{\mathbb{K}}/\,\mathbb{K}\right)$ agit sur $E[m]$ puisque si $[m](P) = O$, alors on a

$$[m]\left(P^{\sigma}\right) = \left([m](P)\right)^{\sigma} = O^{\sigma} = O.$$

On obtient ainsi une représentation

$$\overline{\rho}_{E,m} : \mathrm{Gal}_{\mathbb{K}} := \mathrm{Gal}\left(\overline{\mathbb{K}}/\,\mathbb{K}\right) \longrightarrow \mathrm{Aut}(E[m]) \cong \mathrm{GL}_2(\mathbb{Z}/m\,\mathbb{Z})$$

où le dernier isomorphisme implique un choix de base pour $E[m]$. Individuellement, pour chaque m, ces représentations ne sont pas complètement satisfaisantes puisqu'il est généralement plus simple de travailler avec des représentations dont les matrices sont à coefficients dans un anneau de caractéristique nulle. Nous avons donc "gluer" ensemble ces représentations-modulo-m pour tous les m dans le but de créer une représentation dont les matrices sont à coefficients dans un anneau de caractéristique nulle. Pour faire cela, nous allons copier la construction des entiers ℓ-adiques $\mathbb{Z}_\ell$ à partir de la limite inverse des groupes finis $\mathbb{Z}/\ell^n\,\mathbb{Z}$.

Pour un nombre premier ℓ, on définit le **module de Tate ℓ-adique** comme étant le groupe

$$T_\ell(E) := \varprojlim_{n\in\mathbb{N}} E\left[\ell^n\right]$$

avec la limite inverse obtenue via les applications naturelles

$$E\left[\ell^{n+1}\right] \xrightarrow{[\ell]} E\left[\ell^n\right].$$

Puisque chaque $E\left[\ell^n\right]$ est un $\mathbb{Z}/\ell^n\,\mathbb{Z}$-module, le module de Tate a naturellement une structure de $\mathbb{Z}_\ell$-module. De plus, puisque les multiplication-par-m sont surjectives, la topologie de la limite inverse sur $T_\ell(E)$ est équivalente à la topologie ℓ-adique qu'elle acquiert en étant un $\mathbb{Z}_\ell$-module et on a $T_\ell(E) \cong \mathbb{Z}_\ell \times \mathbb{Z}_\ell$. L'action de $\mathrm{Gal}\left(\overline{\mathbb{K}}/\,\mathbb{K}\right)$ sur chaque $E\left[\ell^n\right]$ commute avec l'application de multiplication-par-ℓ utilisée pour former la limite inverse, donc $\mathrm{Gal}\left(\overline{\mathbb{K}}/\,\mathbb{K}\right)$ agit également sur $T_\ell(E)$. De plus, puisque le groupe profini $\mathrm{Gal}\left(\overline{\mathbb{K}}/\,\mathbb{K}\right)$ agit continûment sur chaque groupe fini (et discret) $E\left[\ell^n\right]$, l'action résultant sur $T_\ell(E)$ est aussi continue. On obtient alors la **représentation ℓ-adique**

$$\rho_{E,\ell} : \mathrm{Gal}\left(\overline{\mathbb{K}}/\,\mathbb{K}\right) \longrightarrow \mathrm{Aut}\left(T_\ell(E)\right) \cong \mathrm{GL}_2\left(\mathbb{Z}_\ell\right)$$

induite par l'action de $\mathrm{Gal}\left(\overline{\mathbb{K}}/\,\mathbb{K}\right)$ sur les points de ℓ^n-torsion de E (et où le dernier isomorphisme implique un choix de base pour $T_\ell(E)$).

En combinant des bases compatibles, on peut combiner les représentations $\rho_{E,\ell}$ en une **représentation adélique**

$$\rho_E : \mathrm{Gal}_{\mathbb{K}} \longrightarrow \mathrm{GL}_2(\widehat{\mathbb{Z}}).$$

Enfin, lorsque $\mathbb{K}$ est un corps de nombres, beaucoup de propriétés arithmétiques de E sont déterminées par les représentations ℓ-adiques $\rho_{E,\ell}$. En particulier, Jean-Pierre Serre démontra le théorème ainsi que le corollaire suivants :

Théorème 0.1 : Théorème de l'image ouverte :
Soit $E/\,\mathbb{K}$ une courbe elliptique sur un corps de nombres $\mathbb{K}$ sans multiplication complexe.
Le groupe $\rho_E(\mathrm{Gal}_{\mathbb{K}})$ est un sous-groupe ouvert de $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ (ou de manière équivalente, est d'indice fini dans $\mathrm{GL}_2(\widehat{\mathbb{Z}})$).

Corollaire 0.1 :
Soit $E/\,\mathbb{K}$ une courbe elliptique sur un corps de nombres $\mathbb{K}$ sans multiplication complexe.

- Pour tout nombre premier ℓ, l'image de $\rho_{E,\ell}$ est d'indice fini dans $\mathrm{Aut}\left(T_\ell(E)\right)$;
- Pour presque tout nombre premier ℓ, l'image de $\rho_{E,\ell}$ est égale à $\mathrm{Aut}\left(T_\ell(E)\right)$.

Serre observa également que pour une courbe elliptique définie sur $\mathbb{Q}$, on ne peut jamais avoir $\mathrm{SL}_2(\widehat{\mathbb{Z}}) \subseteq \rho_E\left(\mathrm{Gal}_{\mathbb{Q}}\right)$ (cf. proposition 22 à la page 310 de [Ser72]). Un ingrédient à cette obstruction est que $\det\circ\rho_E : \mathrm{Gal}_{\mathbb{Q}} \longrightarrow \widehat{\mathbb{Z}}^{\times}$

est le caractère cyclotomique et donc le sous-corps de $\overline{\mathbb{Q}}$ fixé par son noyau est l'extension abélienne maximale de $\mathbb{Q}$ par le théorème de Kronecker-Weber. De plus, lorsque $\mathbb{K} \neq \mathbb{Q}$, il n'y a pas de telle obstruction et on a $\mathrm{SL}_2(\widehat{\mathbb{Z}}) \subseteq \rho_E(\mathrm{Gal}_{\mathbb{Q}})$ pour une courbe elliptique $E/\mathbb{K}$ "aléatoire" (cf. [Zyw11]) et Nathan Jones (cf. [Jon10]) prouva que $\left[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \rho_E(\mathrm{Gal}_{\mathbb{Q}})\right] = 2$ pour une courbe elliptique $E/\mathbb{Q}$ "aléatoire".

2 - Analogie avec les modules de Drinfeld

Pourquoi avons nous commencé par parler de courbes elliptiques plutôt que de modules de Drinfeld ? Nous l'avons fait car il existe une longue série de profondes analogies entre d'une part les courbes elliptiques sur les corps des nombres et d'autre part les modules de Drinfeld sur les corps de fonctions en caractéristique p. Tout comme les courbes elliptiques pour les corps des nombres, les modules de Drinfeld jouent un rôle majeur dans l'arithmétique des corps de fonctions et dans leur programme de Langlands. Nous allons donc commencer par donner des rappels sur les notions de base concernant les modules de Drinfeld (qui seront détaillés d'avantage dans le chapitre 1).

Fixons nous un corps fini $\mathbb{F}_q$ à q éléments, notons $A := \mathbb{F}_q[T]$, $F := \mathbb{F}_q(T)$ son corps des fractions et $\mathbb{K}$ **un A-corps** (c'est-à-dire un corps $\mathbb{K}$ avec un morphisme d'anneaux $\iota : A \longrightarrow \mathbb{K}$ fixé - en utilisant ι on peut alors voir $\mathbb{K}$ comme une extension de corps de $\mathbb{F}_q$).

On note $\mathbb{K}\{\tau\}$ l'anneau des polynômes tordus sur $\mathbb{K}$ (c'est-à-dire l'anneau des polynômes en l'indéterminée τ à coefficients dans $\mathbb{K}$ qui vérifient la règle de commutativité $\tau c = c^q \tau$ pour tout $c \in \mathbb{K}$). On peut alors identifier $\mathbb{K}\{\tau\}$ avec un sous-anneau de $\mathrm{End}(\mathbb{G}_{a,\mathbb{K}})$ en identifiant τ avec l'endomorphisme de Frobenius $X \longrightarrow X^q$. On note également $\partial_0 : \mathbb{K}\{\tau\} \longrightarrow \mathbb{K}$ le morphisme d'anneaux $\sum_{i=0}^{n} a_i \tau^i \longrightarrow a_0$.

Un **A-module de Drinfeld sur** $\mathbb{K}$ est un morphisme d'anneaux $\phi : A \longrightarrow \mathbb{K}\{\tau\}$ tel que $\partial_0 \circ \phi = \iota$ et $\phi(A) \subsetneq \mathbb{K}$. La **caractéristique de** ϕ est le noyau $\mathfrak{p}_0$ de ι (ou de manière équivalente le noyau de $\partial_0 \circ \phi$) et lorsque $\mathfrak{p}_0 = (0_A)$ on dit que ϕ a une **caractéristique générique** et on peut ainsi utiliser ι pour voir $\mathbb{K}$ comme une extension de corps de F. De plus, le module de Drinfeld ϕ est déterminé par $\phi(T) := \phi_T := \sum_{i=0}^{r} a_i \tau^i$ avec les $a_i \in \mathbb{K}$ et $a_r \neq 0$ et l'entier r est appelé le **rang de** ϕ.

Fixons nous désormais une clôture séparable $\mathbb{K}^{sep}$ de $\mathbb{K}$. Le module de Drinfeld ϕ muni $\mathbb{K}^{sep}$ d'une structure de A-module, plus précisément, on a $a \cdot x := \phi_a(x)$ pour tout $a \in A$ et $x \in \mathbb{K}^{sep}$ (ici on utilise l'identification de $\mathbb{K}\{\tau\}$ avec un sous-anneau de $\mathrm{End}(\mathbb{G}_{a,\mathbb{K}})$. On notera ${}^{\phi}\mathbb{K}^{sep}$ pour stipuler qu'on munit $\mathbb{K}^{sep}$ de la structure de A-module mentionnée précédemment.

Pour un idéal non nul $\mathfrak{a}$ de A, la **$\mathfrak{a}$-torsion** de ϕ est le A-module

$$\phi[\mathfrak{a}] := \left\{x \in^{\phi} \mathbb{K}^{sep} \mid \forall a \in \mathfrak{a},\ a \cdot x = 0\right\} = \left\{x \in \mathbb{K}^{sep} \mid \forall a \in \mathfrak{a},\ \phi_a(x) = 0\right\}.$$

Supposons que $\mathfrak{a}$ est premier avec la caractéristique $\mathfrak{p}_0$. La $\mathfrak{a}$-torsion $\phi[\mathfrak{a}]$ est un $A/\mathfrak{a}$-module libre de rang r et le groupe de Galois absolu $\mathrm{Gal}_{\mathbb{K}} := \mathrm{Gal}\left(\mathbb{K}^{sep} / \mathbb{K}\right)$ agit sur $\phi[\mathfrak{a}]$ et respecte la structure de A-module. Cette action peut être exprimée en termes de représentation galoisienne (comme dans le cas des courbes elliptiques) avec

$$\overline{\rho}_{\phi,\mathfrak{a}} : \mathrm{Gal}_{\mathbb{K}} \longrightarrow \mathrm{Aut}(\phi[\mathfrak{a}]) \cong \mathrm{GL}_r(A/\mathfrak{a}).$$

Pour la suite de cette partie de l'introduction, on suppose que ϕ a une caractéristique générique. En choisissant des bases compatibles et en prenant la limite projective, on obtient une représentation

$$\rho_{\phi} : \mathrm{Gal}_{\mathbb{K}} \longrightarrow \mathrm{GL}_r(\widehat{A})$$

qui encode l'action de Galois sur le A-sous-module de torsion de ${}^{\phi}\mathbb{K}^{sep}$ (avec $\widehat{A}$ la complétion profinie de A). De plus, la représentation ρ_{ϕ} est continue lorsque les groupes sont munis de leurs topologies profinies.

Pour un idéal premier non nul λ de A, notons $\rho_{\phi,\lambda} : \mathrm{Gal}_{\mathbb{K}} \longrightarrow \mathrm{GL}_r(A_\lambda)$ la représentation obtenue en composant ρ_{ϕ} avec l'application quotient $\mathrm{GL}_r(\widehat{A}) \longrightarrow \mathrm{GL}_r(A_\lambda)$ (où A_λ est la limite projective des anneaux A/λ^i pour $i \in \mathbb{N}^*$). On peut alors identifier ρ_{ϕ} avec $\prod_{\lambda \in \mathrm{Spec}(A)\setminus\{(0_A)\}} \rho_{\phi,\lambda}$ en utilisant l'isomorphisme naturel donné par $\mathrm{GL}_r(\widehat{A}) \cong \prod_{\lambda \in \mathrm{Spec}(A)\setminus\{(0_A)\}} \mathrm{GL}_r(A_\lambda)$.

Richard Pink et Egon Rütsche ont décrit l'image de ρ_ϕ lorsque $\mathbb{K}$ est de type fini. Par soucis de simplicité, nous citons seulement la version du théorème pour laquelle ϕ n'a pas d'endomorphismes supplémentaires et rappelons que l'**anneau des endomorphismes** $\mathrm{End}_{\overline{\mathbb{K}}}(\phi)$ est le centralisateur de $\phi(A)$ dans $\overline{K}\{\tau\}$, avec $\overline{\mathbb{K}}$ une clôture algébrique de $\mathbb{K}$ contenant $\mathbb{K}^{sep}$.

Théorème 0.2 : Théorème de Pink et Rütsche :
Soit ϕ un A-module de Drinfeld de rang r sur un corps $\mathbb{K}$ de type fini.
Si ϕ a une caractéristique générique et que $\mathrm{End}_{\overline{\mathbb{K}}}(\phi) = \phi(A)$, alors $\rho_\phi(\mathrm{Gal}_{\mathbb{K}})$ est un sous-groupe ouvert de $\mathrm{GL}_r(\widehat{A})$ (ou de manière équivalente, $\rho_\phi(\mathrm{Gal}_{\mathbb{K}})$ est d'indice fini dans $\mathrm{GL}_r(\widehat{A})$).

On notera que ce théorème est un analogue du théorème 0.1 lorsque $r \geq 2$.

Le but de ce projet est de créer des représentations galoisiennes ρ_ϕ d'image la plus grande possible et nous allons en particulier nous intéresser au cas immédiat où $r = 2$ et $\mathbb{K} = F$ et ϕ de caractéristique générique. Nous allons montrer qu'il y a un nombre infini de modules de Drinfeld ϕ sur F de rang 2 et non isomorphes tels que $\rho_\phi(\mathrm{Gal}_F) = \mathrm{GL}_2(\widehat{A})$.

3 - Notion de densité

Avant de donner notre résultat principal, nous allons avoir besoin d'introduire la notion de densité puisque pour $n \in \mathbb{N}^*$ fixé nous allons parler de propriétés qui sont vraies pour "presque tous" $a \in A^n$.

Pour tout sous-ensemble S de A^n et tout entier naturel non nul d, on note $S(d)$ l'ensemble des n-uplets $(a_1, ..., a_n)$ de S tels que pour tout $i \in [\![1; n]\!]$ on ait $\deg(a_i) \leq d$. On peut alors définir les notions de **densité supérieure** et de **densité inférieure** données respectivement par :

$$\overline{\delta}(S) := \varlimsup_{d\to+\infty} \frac{\mathrm{Card}(S(d))}{\mathrm{Card}\,(A^n(d))} \text{ et } \underline{\delta}(S) := \varliminf_{d\to+\infty} \frac{\mathrm{Card}(S(d))}{\mathrm{Card}\,(A^n(d))}.$$

Lorsque ces deux valeurs coïncident, on appelle cette quantité commune la **densité de** S. Bien évidemment, on a $\mathrm{Card}\,(A^n(d)) = q^{n(d+1)}$ et $\delta(A) = 1$.

4 - Énoncés des résultats principaux

Nous allons voir ici F comme un A-corps via l'inclusion naturelle $A \subseteq F$. Pour toute paire $a := (a_1, a_2) \in A^2$ avec $a_2 \neq 0$, on pose

$$\phi(a) : \left| \begin{array}{ccc} A & \longrightarrow & F\{\tau\} \\ \alpha & \longmapsto & \phi(a)_\alpha := \phi(a)(\alpha) \end{array} \right.$$

le A-module de Drinfeld sur F défini par $\phi(a)_T := T + a_1\tau + a_2\tau^2$. Le module de Drinfeld $\phi(a)$ est de rang 2 et a une caractéristique générique. De plus, associé à $\phi(a)$, on a une représentation galoisienne $\rho_{\phi(a)} : \mathrm{Gal}_F \longrightarrow \mathrm{GL}_2(\widehat{A})$ qui est unique à l'isomorphisme près.

On définit désormais 3 sous-ensembles de A^2 pour lesquels $\rho_{\phi(a)}$ a une grande image :

* Posons S_1 l'ensemble des $a := (a_1, a_2) \in A^2$ avec $a_2 \neq 0$ tels que $\rho_{\phi(a)}(\mathrm{Gal}_F) = \mathrm{GL}_2(\widehat{A})$.
* Pour $q \neq 2$, posons S_2 l'ensemble des $a := (a_1, a_2) \in A^2$ avec $a_2 \neq 0$ tels que $\mathrm{SL}_2(\widehat{A}) \subseteq \rho_{\phi(a)}(\mathrm{Gal}_F)$ et $\left[\mathrm{GL}_2(\widehat{A}) : \rho_{\phi(a)}(\mathrm{Gal}_F)\right]$ divise $q - 1$.
* Pour $q = 2$, posons S_2 l'ensemble des $a := (a_1, a_2) \in A^2$ avec $a_2 \neq 0$ tels que $\rho_{\phi(a)}(\mathrm{Gal}_F)$ contienne le sous-groupe dérivé de $\mathrm{GL}_2(\widehat{A})$ et $\left[\mathrm{GL}_2(\widehat{A}) : \rho_{\phi(a)}(\mathrm{Gal}_F)\right]$ divise 4.
* Posons S_3 l'ensemble des $a := (a_1, a_2) \in A^2$ avec $a_2 \neq 0$ tels que pour tout idéal premier non nul λ de A on ait $\rho_{\phi(a),\lambda}(\mathrm{Gal}_F) = \mathrm{GL}_2(A_\lambda)$.

Notre théorème principal est le suivant et montre que S_1, S_2 et S_3 sont "grands" :

Théorème 0.3 :

- Il existe un sous-ensemble de S_1 de densité strictement positive ;
- L'ensemble S_2 a pour densité 1 ;
- L'ensemble S_3 a pour densité 1.

De manière grossière, le deuxième point du théorème 0.3 dit que pour un $a \in A^2$ "choisi aléatoirement", l'indice de $\rho_{\phi(a)}(\mathrm{Gal}_F)$ dans $\mathrm{GL}_2(\widehat{A})$ est fini et divise $q-1$ (respectivement 4) lorsque $q \neq 2$ (respectivement $q = 2$). De même le premier point du théorème 0.3 dit que $\rho_{\phi(a)}(\mathrm{Gal}_F) = \mathrm{GL}_2(\widehat{A})$ pour "beaucoup" de $a \in A^2$.

Remarques :

- Supposons que $q \neq 2$ et considérons $a := (a_1, a_2) \in A^2$ avec a_2 unitaire et $\deg(a_2) \equiv 1\ [q-1]$.
  On a $\left[\widehat{A}^\times : \det\left(\rho_{\phi(a)}(\mathrm{Gal}_F)\right)\right] = q-1$ (cf. théorème 4.2) et donc $\left[\mathrm{GL}_2(\widehat{A}) : \rho_{\phi(a)}(\mathrm{Gal}_F)\right] \geq q-1$. Ceci montre que S_1 n'a pas pour densité 1 et que l'entier $q-1$ apparaissant dans la définition de S_2 est optimal.
- Le groupe dérivé de $\mathrm{GL}_2(\widehat{A})$ est $\mathrm{SL}_2(\widehat{A})$ lorsque $q \neq 2$. Une complication théorique apparaît lorsque $q = 2$ puisque le groupe dérivé de $\mathrm{GL}_2(\widehat{A})$ est un sous-groupe stricte de $\mathrm{SL}_2(\widehat{A})$ (plus exactement, il est d'indice 4 dans $\mathrm{GL}_2(\widehat{A})$). C'est la raison pour laquelle la définition de S_2 varie lorsque $q = 2$.

Pour toute puissance $q > 1$ d'un nombre premier, on donne un exemple de module de Drinfeld de rang 2 dont la représentation galoisienne est surjective :

Théorème 0.4 :
Soit $\phi : A \longrightarrow F\{\tau\}$ le module de Drinfeld défini par

$$\phi_T := \begin{cases} T + \tau - T^{q-1}\tau^2 & \text{si } q \neq 2 \\ T + T^3\tau + \left(1 + T + T^2\right)\tau^2 & \text{si } q = 2. \end{cases}$$

On a $\rho_\phi(\mathrm{Gal}_F) = \mathrm{GL}_2(\widehat{A})$.

5 - Articulation du projet

Ce projet s'articule autour de deux grandes parties. Dans la partie A nous commençons par donner les définitions et résultats de base sur les modules de Drinfeld (généralités sur les modules de Drinfeld, morphismes entre modules de Drinfeld, points de torsion, etc.) puis dans un deuxième chapitre nous étudierons rapidement les séries dans un corps complet non archimédien. Enfin dans un troisième chapitre nous parlerons de modules de Drinfeld sur des corps locaux. Ces trois chapitres concentrent les définitions et résultats sur les modules de Drinfeld qui seront utilisés par la suite au cours de la deuxième partie.

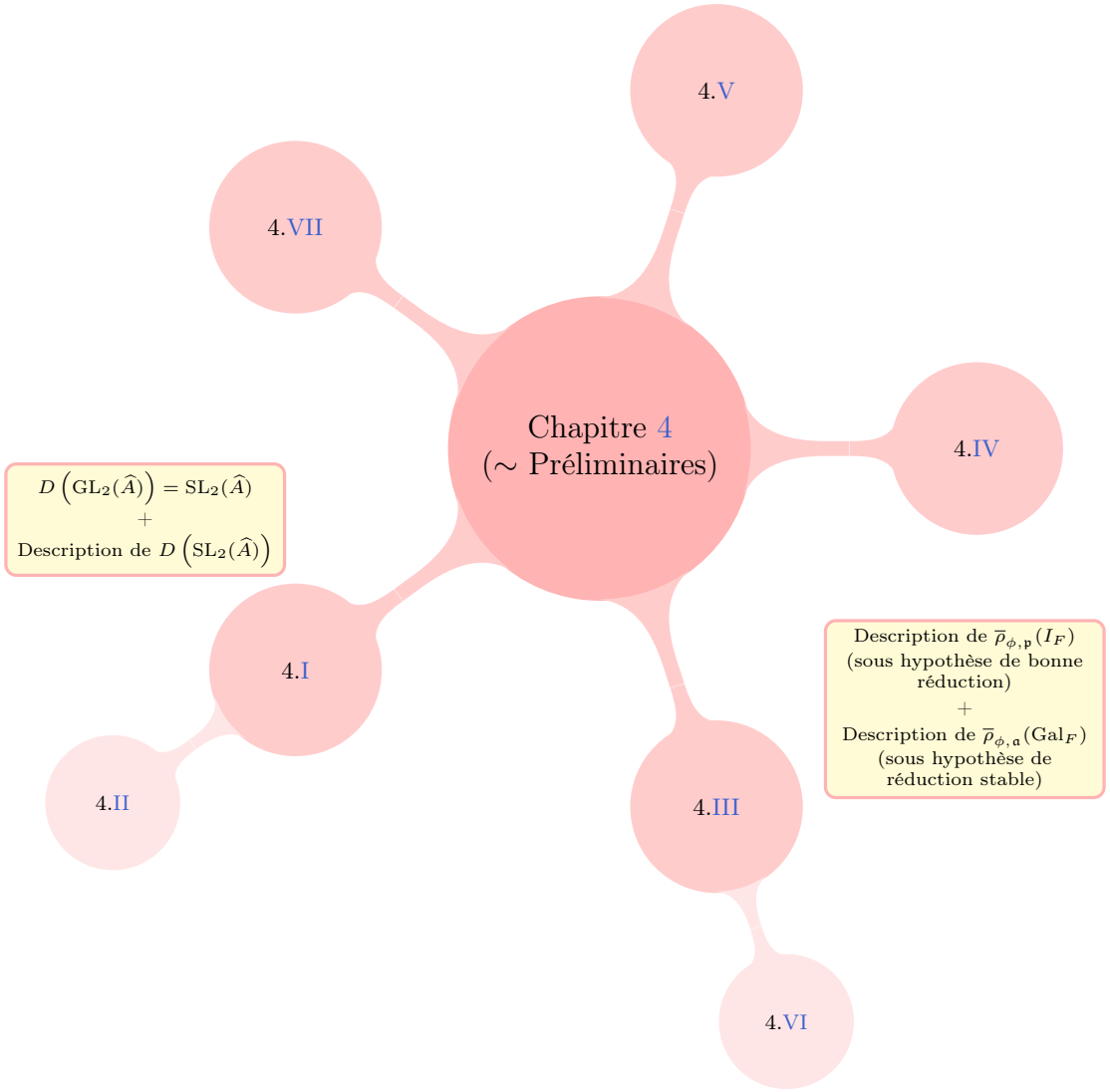
Dans la partie B, nous suivons la même logique que dans l'article de David Zywina (cf. [Zyw25]) puisqu'il s'agit de reprendre ce même article et d'en détailler les preuves ainsi que les arguments. Considérons un module de Drinfeld $\phi : A \longrightarrow F\{\tau\}$ de rang 2 tel que $\mathrm{End}_{\overline{F}}(\phi) = \phi(A)$.
Le chapitre 4 est consacré à des résultats préliminaires qui nous seront utiles pour démontrer les théorèmes 0.3 et 0.4. Dans la partie I nous donnons un critère qui nous permet d'affirmer qu'un sous-groupe de $\mathrm{GL}_2(A_\lambda)$ est en réalité égal à $\mathrm{GL}_2(A_\lambda)$ tout entier. Dans la partie II nous donnons un critère qui nous permet de dire qu'un sous-groupe de $\mathrm{GL}_2(\widehat{A})$ contient son groupe dérivé. Nous appliquerons par la suite ces critères avec le sous-groupe $\rho_{\phi(a)}(\mathrm{Gal}_F)$ de $\mathrm{GL}_2(\widehat{A})$ et se sont ces résultats théoriques de théorie des groupes qui motivent la structure de cette partie.
Les représentations galoisienne pour des modules de Drinfeld définis sur des corps locaux seront étudiées dans la partie III. Ces résultats seront utilisés dans nos preuves pour comprendre l'action du groupe d'inertie sur la torsion de ϕ en des idéaux premiers non nuls $\mathfrak{p}$ pour lesquels notre module de Drinfeld a une réduction semi-stable (c'est-à-dire isomorphe à un module de Drinfeld ψ à coefficients dans l'anneau des entiers $\mathcal{O}_{\mathbb{K}_\mathfrak{p}}$ et dont la réduction modulo l'idéal maximal est un module de Drinfeld de rang non nul sur le corps résiduel). En particulier, ceci nous permettra de construire des sous-groupes de $\overline{\rho}_{\phi,\mathfrak{a}}(\mathrm{Gal}_F)$ sur lesquels nous avons des informations précises.
Dans la partie IV nous rappelons que les représentations $\overline{\rho}_{\phi,\mathfrak{a}}(\mathrm{Gal}_F)$ sont compatibles et donnent des polynômes

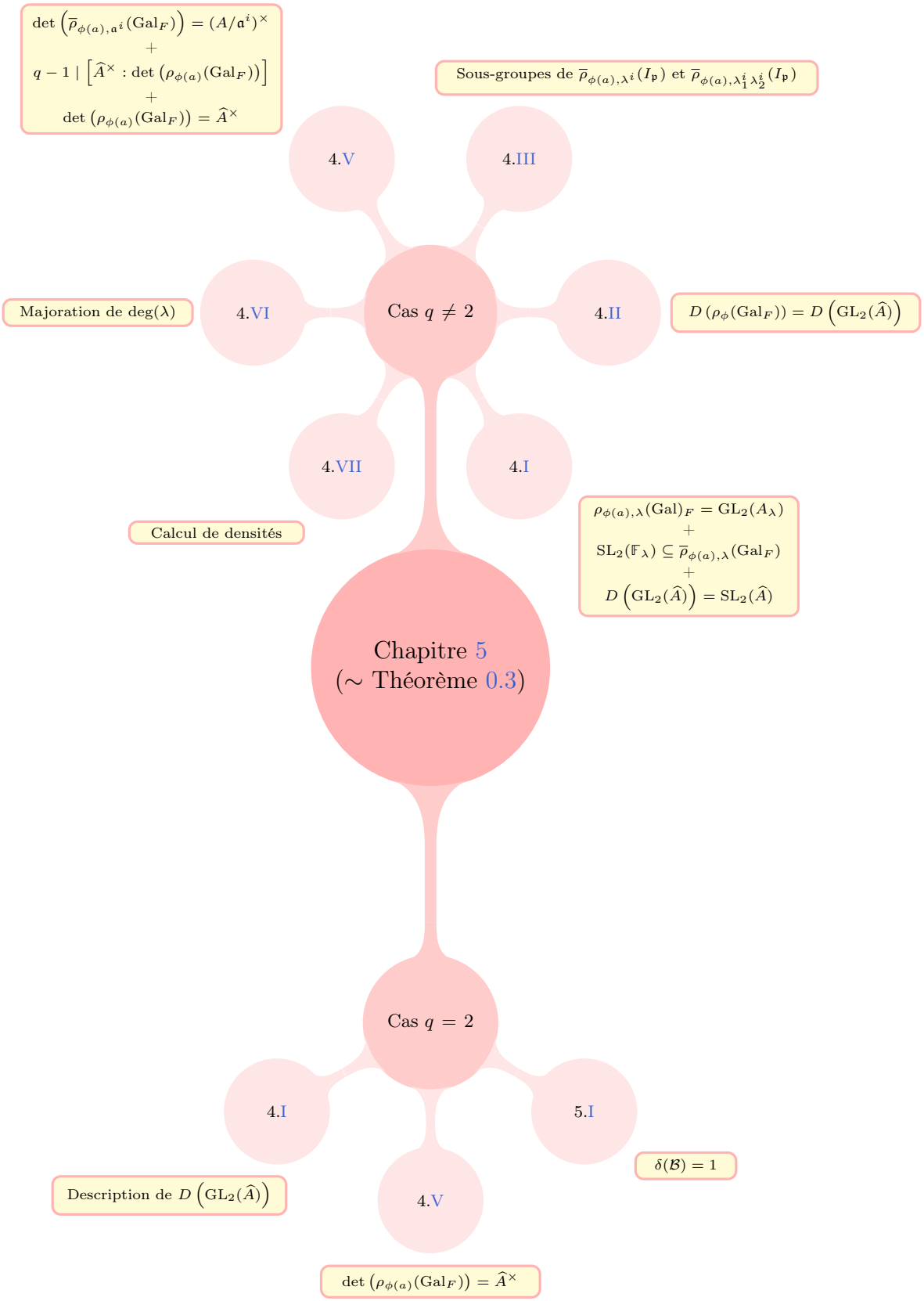
caractéristiques du Frobenius (ceux-ci sont à coefficients dans A et sont calculables). Dans la partie V nous rappelons un théorème de Ernst-Ulrich Gekeler qui nous donne une expression explicite de l'indice de $\det(\rho_\phi(\mathrm{Gal}_F))$ dans $\widehat{A}^\times$.
Une étape importante pour montrer que ρ_ϕ a une grande image est de montrer que les différentes représentations $\overline{\rho}_{\phi,\lambda} : \mathrm{Gal}_F \longrightarrow \mathrm{GL}_2(\mathbb{F}_\lambda)$ sont irréductibles pour tout idéal premier non nul λ de A. Dans la partie VI nous montrons que c'est le cas pour presque tout λ et nous donnons une borne explicite de la norme des idéaux qui font exception. Enfin on termine ce chapitre avec la partie VII où l'on prouve une version du théorème d'irréductibilité de Hilbert. Nous l'utiliserons pour montrer que pour un idéal non nul $\mathfrak{a}$ de A fixé, on a $\overline{\rho}_{\phi(a),\mathfrak{a}} = \mathrm{GL}_2(A/\mathfrak{a})$ pour tout $a \in A^2$ en dehors d'un ensemble de densité nulle. Notons que cet ensemble de densité nulle dépend de $\mathfrak{a}$ et donc on ne peut pas utiliser le théorème d'irréductibilité de Hilbert en lui-même pour démontrer le théorème 0.3.
Dans le chapitre 5 nous allons démontrer le théorème 0.3. Tout d'abord pour le cas où $q \neq 2$, nous allons utiliser les ingrédients précédents ainsi que des techniques de dénombrement pour obtenir des informations sur l'image de $\rho_{\phi(a)}$ pour tout $a \in A^2$ en dehors d'un ensemble de densité nulle. En particulier, pour tout $a \in A^2$ en dehors de ce même ensemble, on montrera que $\rho_{\phi(a),\lambda} = \mathrm{GL}_2(A_\lambda)$ pour tout idéal premier non nul λ de A et que $\rho_{\phi(a)}(\mathrm{Gal}_F)$ et $\mathrm{GL}_2(\widehat{A})$ ont le même sous-groupe dérivé. Nous passerons ensuite au cas où $q = 2$ en donnant tout d'abord un critère sur ϕ qui nous assure que le morphisme $\mathrm{Gal}_F \longrightarrow \mathrm{GL}_2(\widehat{A})/D\left(\mathrm{GL}_2(\widehat{A})\right)$ (obtenu en composant ρ_ϕ avec la projection) est surjectif (en regardant la ramification de la place ∞ de F) puis en donnant la preuve du théorème 0.3 dans le cas où $q = 2$.
Enfin dans un dernier chapitre on démontre le théorème 0.4 en calculant les images des groupes de Galois absolus en commençant par le cas où $q \neq 2$ puis en s'intéressant ensuite au cas $q = 2$.

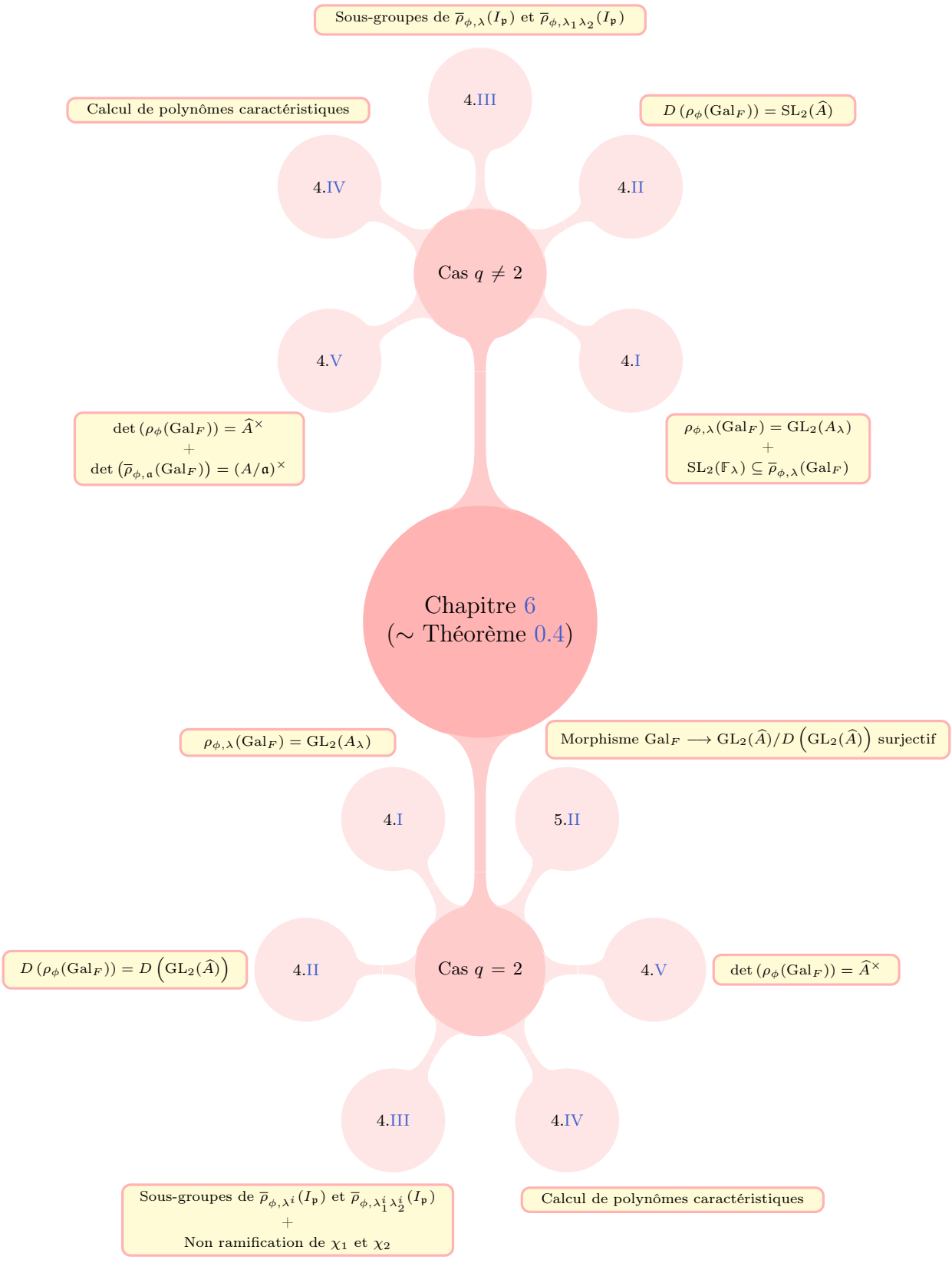
Finalement, on trouvera l'annexe A qui traite des généralités du groupe de Galois absolu ainsi que de son sous-groupe d'inertie (c'est-à-dire de leur construction ainsi que des propriétés fondamentales) en commençant par rappeler des résultats dans le cas des extensions galoisiennes finies en partie I avant de les exploiter en partie II.

6 - Cartes mentales

Afin d'avoir plus de clarté sur les liens entre les différentes parties des divers chapitres, on ajoute ci-dessous une carte mentale pour les chapitres 4,5 et 6 (les 3 premiers chapitres n'étant que des outils cela n'est pas nécessaire pour eux). On ajoutera au dessus de chaque bulle (lorsque cela est nécessaire) les résultats importants utilisés et on ne fera pas apparaître les résultats démontrés dans une partie et qui servent dans cette même partie. Enfin, les notations utilisées dans les cartes mentales sont celles des parties concernées, on invite donc le lecteur à se rendre dans ces parties afin d'avoir un contexte et une définition claire des objets (ces cartes mentales sont donc un outil à utiliser une fois la lecture des chapitres terminés).


Chapitre 4
(∼ Préliminaires)
4.I
4.II
4.III
4.IV
4.V
4.VI
4.VII
$D\left(\mathrm{GL}_2(\widehat{A})\right) = \mathrm{SL}_2(\widehat{A})$
+
Description de $D\left(\mathrm{SL}_2(\widehat{A})\right)$
Description de $\overline{\rho}_{\phi,\mathfrak{p}}(I_F)$
(sous hypothèse de bonne réduction)
+
Description de $\overline{\rho}_{\phi,\mathfrak{a}}(\mathrm{Gal}_F)$
(sous hypothèse de réduction stable)


$\det\left(\overline{\rho}_{\phi(a),\mathfrak{a}^i}(\mathrm{Gal}_F)\right) = (A/\mathfrak{a}^i)^\times$
+
$q-1 \mid \left[\widehat{A}^\times : \det\left(\rho_{\phi(a)}(\mathrm{Gal}_F)\right)\right]$
+
$\det\left(\rho_{\phi(a)}(\mathrm{Gal}_F)\right) = \widehat{A}^\times$
Sous-groupes de $\overline{\rho}_{\phi(a),\lambda^i}(I_\mathfrak{p})$ et $\overline{\rho}_{\phi(a),\lambda_1^i\lambda_2^i}(I_\mathfrak{p})$
4.V
4.III
Majoration de deg(λ)
4.VI
Cas $q \neq 2$
4.II
$D\left(\rho_\phi(\mathrm{Gal}_F)\right) = D\left(\mathrm{GL}_2(\widehat{A})\right)$
4.VII
4.I
Calcul de densités
$\rho_{\phi(a),\lambda}(\mathrm{Gal})_F = \mathrm{GL}_2(A_\lambda)$
+
$\mathrm{SL}_2(\mathbb{F}_\lambda) \subseteq \overline{\rho}_{\phi(a),\lambda}(\mathrm{Gal}_F)$
+
$D\left(\mathrm{GL}_2(\widehat{A})\right) = \mathrm{SL}_2(\widehat{A})$
Chapitre 5
($\sim$ Théorème 0.3)
Cas $q = 2$
4.I
5.I
$\delta(\mathcal{B}) = 1$
Description de $D\left(\mathrm{GL}_2(\widehat{A})\right)$
4.V
$\det\left(\rho_{\phi(a)}(\mathrm{Gal}_F)\right) = \widehat{A}^\times$


Sous-groupes de $\overline{\rho}_{\phi,\lambda}(I_{\mathfrak{p}})$ et $\overline{\rho}_{\phi,\lambda_1\lambda_2}(I_{\mathfrak{p}})$
4.III
Calcul de polynômes caractéristiques
$D\left(\rho_\phi(\mathrm{Gal}_F)\right) = \mathrm{SL}_2(\widehat{A})$
4.IV
4.II
Cas $q \neq 2$
4.V
4.I
$\det\left(\rho_\phi(\mathrm{Gal}_F)\right) = \widehat{A}^\times$
+
$\det\left(\overline{\rho}_{\phi,\mathfrak{a}}(\mathrm{Gal}_F)\right) = (A/\mathfrak{a})^\times$
$\rho_{\phi,\lambda}(\mathrm{Gal}_F) = \mathrm{GL}_2(A_\lambda)$
+
$\mathrm{SL}_2(\mathbb{F}_\lambda) \subseteq \overline{\rho}_{\phi,\lambda}(\mathrm{Gal}_F)$
Chapitre 6
(∼ Théorème 0.4)
$\rho_{\phi,\lambda}(\mathrm{Gal}_F) = \mathrm{GL}_2(A_\lambda)$
Morphisme $\mathrm{Gal}_F \longrightarrow \mathrm{GL}_2(\widehat{A})/D\left(\mathrm{GL}_2(\widehat{A})\right)$ surjectif
4.I
5.II
$D\left(\rho_\phi(\mathrm{Gal}_F)\right) = D\left(\mathrm{GL}_2(\widehat{A})\right)$
4.II
Cas $q = 2$
4.V
$\det\left(\rho_\phi(\mathrm{Gal}_F)\right) = \widehat{A}^\times$
4.III
4.IV
Sous-groupes de $\overline{\rho}_{\phi,\lambda^i}(I_{\mathfrak{p}})$ et $\overline{\rho}_{\phi,\lambda_1^i\lambda_2^i}(I_{\mathfrak{p}})$
+
Non ramification de χ_1 et χ_2
Calcul de polynômes caractéristiques

Notations

- $\mathbb{F}_q$ est corps fini avec q éléments, où q est une puissance d'un nombre premier p.
- $A = \mathbb{F}_q[T]$ est anneau des polynômes en l'indéterminée T et à coefficients dans $\mathbb{F}_q$.
- $F = \mathbb{F}_q(T)$ est corps des fractions de A.
- Un idéal de A sera noté par des lettres $\mathfrak{gothiques}$. Chaque idéal non nul $\mathfrak{n}$ de A a un unique générateur unitaire qui, par abus de notation, sera encore noté $\mathfrak{n}$ (cependant il sera toujours clair dans le contexte si $\mathfrak{n}$ désigne un idéal de A ou son générateur unitaire).
- $\mathrm{Spec}(A)$ est l'ensemble des idéaux premiers de A.
- A_+ est l'ensemble des polynômes unitaires de A.
- $\mathbb{F}_\mathfrak{p}$ est l'anneau quotient $A/\mathfrak{p}$ de A par un idéal premier $\mathfrak{p}$ (remarquons que $\mathbb{F}_\mathfrak{p} \cong \mathbb{F}_{q^{\deg(\mathfrak{p})}}$ est un corps puisque $\mathfrak{p}$ est maximal).
- $N(\mathfrak{p})$ est le cardinal de $\mathbb{F}_\mathfrak{p}$.
- $\deg(\mathfrak{p})$ est le degré de l'extension $\mathbb{F}_\mathfrak{p}/\mathbb{F}_q$.
- $\mathbb{F}_{\mathfrak{p}^n}$ est une extension de degré n de $\mathbb{F}_\mathfrak{p}$.
- $F_\mathfrak{p}$ est la complétion de F pour la valuation $\mathrm{val}_\mathfrak{p} : F_\mathfrak{p}^\times \longrightarrow \mathbb{Z}$ normalisée de telle sorte que $\mathrm{val}_\mathfrak{p}\left(F_\mathfrak{p}^\times\right) = \mathbb{Z}$ (et on pose $\mathrm{val}_\mathfrak{p}(0) = +\infty$), où $\mathfrak{p}$ est un idéal premier de A.
- $A_\mathfrak{p}$ est l'anneau des entiers de $F_\mathfrak{p}$ (c'est-à-dire $A_\mathfrak{p} = \varprojlim_{n\in\mathbb{N}^*} A/\mathfrak{p}^n$).
- On a les isomorphismes $\widehat{A} \cong \prod_{\mathfrak{p}\in \mathrm{Spec}(A)\setminus\{(0_A)\}} A_\mathfrak{p}$ et $A_\mathfrak{a} \cong \prod_{\substack{\mathfrak{p}\in \mathrm{Spec}(A)\setminus\{(0_A)\} \\ \mathfrak{a}\subseteq\mathfrak{p}}} A_\mathfrak{p}$.
- F_∞ est la complétion de F pour la norme archimédienne val_∞.
- A_∞ est l'anneau des entiers de F_∞.
- $\mathcal{M}_\infty$ est l'idéal maximal de A_∞.
- $\mathbb{F}_\infty \cong A_\infty/\mathcal{M}_\infty \cong \mathbb{F}_q$.
- $\mathbb{C}_\infty$ est la complétion d'une clôture algébrique de F_∞.
- $|\cdot|$ est l'unique extension à $\mathbb{C}_\infty$ de la valeur absolue sur F_∞ normalisée de telle sorte que $|T| = q$. Remarquons au passage que la restriction de $|\cdot|$ à A peut être définie de manière équivalente par :

$$\forall a \in A\setminus\{0_A\},\ |a| = \mathrm{Card}(A/(a)) = q^{\deg(a)} \text{ et } |0| = 0.$$

- $\mathbb{K}^{sep}$ est une clôture séparable d'un corps $\mathbb{K}$
- $\mathrm{Gal}_\mathbb{K} := \mathrm{Gal}\left(\mathbb{K}^{sep}/\mathbb{K}\right)$ est le groupe de Galois absolu d'un corps $\mathbb{K}$.
- $I_\mathbb{K}$ est le groupe d'inertie du groupe de Galois absolu d'un corps $\mathbb{K}$.
- $D(G)$ est le groupe dérivé du groupe G.

Première partie

Notions préliminaires sur les modules de Drinfeld

Chapitre 1

Rudiments sur les modules de Drinfeld

L'objectif central de ce premier chapitre est d'introduire tous les concepts de base sur les modules de Drinfeld et qui seront utilisés dans toute la suite de ce document (notamment de la partie B). Dans la partie I nous introduisons la notion de polynôme additif qui motivera l'introduction de l'anneau des polynômes tordus. Dans la partie II nous introduirons les modules de Drinfeld ainsi que les premières définitions et quelques propriétés. Dans la partie III nous étudierons les morphismes entre modules de Drinfeld puis dans la partie la partie IV nous étudierons les points de torsion qui auront un rôle considérable à jouer par la suite pour enfin finir par la partie V où nous chercherons à classifier les modules de Drinfeld de rang 2 à l'isomorphisme près.

Dans tout ce premier chapitre, on considère $\mathbb{K}$ un corps quelconque sauf mention explicite du contraire.

I Polynômes additifs

Définition 1.1 : Polynôme additif :
On considère x et y deux indéterminées.
Un polynôme $f(x) \in \mathbb{K}[x]$ est appelé **polynôme additif** lorsque l'on a l'égalité

$$f(x+y) = f(x) + f(y) \tag{1.1}$$

dans $\mathbb{K}[x,y]$.

Lemme 1.1 :
Soit $f(x) \in \mathbb{K}[x]$.

- Si $\mathbb{K}$ est un corps de caractéristique nulle, alors $f(x)$ est un polynôme additif si, et seulement si, $f(x) = \alpha x$ pour un certain $\alpha \in \mathbb{K}$;
- Si $\mathbb{K}$ est un corps de caractéristique $p > 0$, alors $f(x)$ est un polynôme additif si, et seulement si, il est de la forme
$$f(x) = \sum_{i=0}^{n} a_i x^{p^i}$$
pour un certain $n \in \mathbb{N}$ et des $a_0, \dots, a_n \in \mathbb{K}$.

Preuve :

- Si $\mathrm{car}(\mathbb{K}) = 0$:
On a clairement que tout polynôme de la forme $f(x) = \alpha x$ (pour un certain $\alpha \in \mathbb{K}$) est additif. Il nous suffit donc de montrer la réciproque :
Les cas où $\deg(f) = -\infty$ et $\deg(f) = 0$ se traitent directement en remarquant que le polynôme nul est additif et on a $\alpha = 0$ (respectivement un polynôme additif constant est en réalité nul et on retombe sur le cas précédent). Dans les autres cas, nous allons démontrer par récurrence sur $n \in \mathbb{N}^*$ la propriété :
$$\mathcal{P}_n : \text{"Pour tout } f \in \mathbb{K}_n[x] \text{ additif, on a } f(x) = \alpha x \text{ pour un certain } \alpha \in \mathbb{K}\text{"}.$$

- Initialisation pour $n = 1$:
Soit $f(x) = ax + b \in \mathbb{K}_1[x]$ additif.
Par hypothèse, on a

$$f(x+y) = f(x) + f(y),$$

c'est-à-dire :

$$a(x+y) + b = a(x+y) + 2b.$$

En particulier en évaluant (1.1) en $x = 0$ et $y = 0$ on trouve $b = 2b$ et donc $b = 0$.
Ainsi, on a $f(x) = ax$ pour $a \in \mathbb{K}$ et donc $\mathcal{P}_1$ est vérifiée.

- Hérédité :
On suppose $\mathcal{P}_n$ vraie pour un certain $n \in \mathbb{N}^*$.
On considère $f(x) = \sum_{k=0}^{n+1} a_k x^k \in \mathbb{K}_{n+1}[x]$ additif.
Par hypothèse, on a

$$f(x+y) = f(x) + f(y),$$

c'est-à-dire :

$$\sum_{k=0}^{n+1} \left(\sum_{\ell=0}^{k} a_k \binom{k}{\ell} x^\ell y^{k-\ell} \right) = \sum_{k=0}^{n+1} a_k \left(x^k + y^k \right).$$

En particulier en extrayant le terme pour $k = n+1$, on trouve que

$$a_{n+1} \sum_{\ell=0}^{n+1} \binom{n+1}{\ell} x^\ell y^{n+1-\ell} = a_{n+1} \left(x^{n+1} + y^{n+1} \right)$$

c'est-à-dire :

$$a_{n+1} \left(\sum_{\ell=1}^{n} \binom{n+1}{\ell} x^\ell y^{n+1-\ell} \right) = 0.$$

Or en regardant l'égalité précédente dans $\mathbb{K}[x, y]$, qui est un anneau intègre, on obtient que $a_{n+1} = 0$ et donc $f \in \mathbb{K}_n[x]$. Finalement, en utilisant l'hypothèse de récurrence, on obtient que $f(x) = \alpha x$ pour un certain $\alpha \in \mathbb{K}$. Ainsi la propriété est héréditaire et on a démontré le sens direct par récurrence simple.

On a donc démontré le premier point par double implication.

∗ Si $\mathrm{car}(\mathbb{K}) = p > 0$:
On sait déjà qu'un polynôme de la forme $\sum_{i=0}^{n} a_i x^{p^i}$ est additif par le morphisme de Frobenius (puisqu'ici le corps $\mathbb{K}$ est de caractéristique p). Il nous suffit donc de montrer la réciproque :
Les cas où $\deg(f) = -\infty$ et $\deg(f) = 0$ se traitent directement en remarquant que le polynôme nul est additif et on a $\alpha = 0$ (respectivement un polynôme additif constant est en réalité nul et on retombe sur le cas précédent). Dans les autres cas, nous allons démontrer par récurrence sur $n \in \mathbb{N}^*$ la propriété :

$$\mathcal{P}_n : \text{"Pour tout } f \in \mathbb{K}_n[x] \text{ additif, on a } f(x) = \alpha x \text{ pour un certain } \alpha \in \mathbb{K}\text{"}.$$

- Initialisation pour $n = 1$:
Soit $f(x) = ax + b \in \mathbb{K}_1[x]$ additif.
Par hypothèse, on a

$$a + b(x+y) = a + bx + a + by$$

En particulier en évaluant (1.1) en $x = 0$ et $y = 0$ on trouve $b = 2b$ et donc $b = 0$.
Ainsi, on a $f(x) = ax$ pour $a \in \mathbb{K}$ et donc $\mathcal{P}_1$ est vérifiée.

- Hérédité :
On suppose $\mathcal{P}_n$ vraie pour un certain $n \in \mathbb{N}^*$.
On considère $f(x) = \sum_{k=0}^{n+1} a_k x^k \in \mathbb{K}_{n+1}[x]$ additif.
Considérons l'égalité $f(x+y) = f(x) + f(y)$ dans $\mathbb{K}[x,y] = \mathbb{K}[y][x]$ et en la dérivant formellement par rapport à x, on obtient $f'(x+y) = f'(x)$. En particulier en $x = 0$ on a $f'(y) = f'(0)$, ce qui implique que $f'(x)$ est constant. Ainsi, on a

$$f(x) = ax + h(x)$$

pour un certain $h(x) = \sum_{i=1}^{n+1} h_i x^i \in \mathbb{K}[x]$ tel que $h_i = 0$ pour $p \nmid i$.

De plus, étant donné que $f(x)$ est un polynôme additif dans $\mathbb{K}[x]$, il le reste dans $\overline{\mathbb{K}}[x]$ et on peut donc supposer que $\mathbb{K}$ est algébriquement clos. On obtient alors que

$$h(x) = \sum_{i=1}^{n+1} h_i x^i = \left(\sum_{i=1}^{n+1} h_i^{\frac{1}{p}} x^{\frac{i}{p}} \right)^p = g(x)^p.$$

Ainsi on obtient que $f(x) = ax + g(x)^p$ et comme $f(x) - ax$ est un polynôme additif, on obtient que $g(x+y)^p = g(x)^p + g(y)^p$, c'est-à-dire :

$$(g(x+y) - g(x) - g(y))^p = 0.$$

Or le morphisme de Frobenius est injectif sur $\mathbb{K}[x,y]$, donc $g(x)$ est un polynôme additif et de degré inférieur ou égal à n, donc par hypothèse de récurrence, $g(x)$ ainsi que $g(x)^p$ sont de la forme voulue et par conséquent $f(x)$ également. Ainsi la propriété est héréditaire et on a démontré le sens direct par récurrence simple.

On a donc démontré le deuxième point par double implication.

■

On s'aperçoit alors que les polynômes additifs en caractéristique nulle ont une structure bien moins riche qu'en caractéristique positive. On suppose donc à partir de maintenant que $\mathbb{F}_q$ est un sous-corps de $\mathbb{K}$.

Définition 1.2 : Polynôme $\mathbb{F}_q$-linéaire :
Un polynôme $f(x) \in \mathbb{K}[x]$ est un **polynôme $\mathbb{F}_q$-linéaire** lorsqu'il est additif et vérifie la condition

$$\forall \alpha \in \mathbb{F}_q,\ f(\alpha x) = \alpha f(x). \tag{1.2}$$

Lemme 1.2 :
Un polynôme $f(x) \in \mathbb{K}[x]$ est $\mathbb{F}_q$-linéaire si, et seulement si, il est de la forme

$$f(x) = \sum_{i=0}^{n} a_i x^{q^i}$$

pour un certain $n \in \mathbb{N}$ et des $a_0, \dots, a_n \in \mathbb{K}$.

Preuve :
Raisonnons par double implication :

* Soit $f(x) \in \mathbb{K}[x]$ de la forme $\sum_{i=0}^{n} a_i x^{q^i}$.
Par le lemme 1.1, on sait que $f(x)$ est un polynôme additif et puisque pour tout $\alpha \in \mathbb{F}_q$ et tout $i \in \mathbb{N}$ on a $\alpha^{q^i} = \alpha$, on en déduit que $f(x)$ est bien $\mathbb{F}_q$-linéaire.

* Réciproquement, considérons $f(x) \in \mathbb{K}[x]$ qui est $\mathbb{F}_q$-linéaire.
Toujours par le lemme 1.1, on sait que $f(x)$ est de la forme $\sum_{j=0}^{m} b_j x^{p^j}$. De plus, la condition de linéarité implique que pour tout $j \in [\![0; n]\!]$ et tout $\alpha \in \mathbb{F}_q$ on a $b_j \alpha^{p^j} = b_j \alpha$. Ainsi, pour $b_j \neq 0$ on obtient que

$\alpha^{p^j} = \alpha$ pour tout $\alpha \in \mathbb{F}_q$. D'autre part, la dernière égalité implique que $\mathbb{F}_q$ est un sous-corps de $\mathbb{F}_{p^j}$ et donc en considérant $\mathbb{F}_{p^j}$ comme un $\mathbb{F}_q$-espace vectoriel, on obtient que $p^j = q^i$ pour un certain $i \in \mathbb{N}$ et donc $f(x)$ est de la forme voulue.

■

Pour $f(x) \in \mathbb{K}[x]$ un polynôme $\mathbb{F}_q$-linéaire, il est clair que 0 est toujours racine de $f(x)$ et que toute $\mathbb{F}_q$-combinaison linéaire de racines de $f(x)$ reste une racine de f. Ainsi, l'ensemble des racines du polynôme $\mathbb{F}_q$-linéaire $f(x)$ forme un $\mathbb{F}_q$-espace vectoriel de $\overline{\mathbb{K}}$ et qui est de dimension finie. Réciproquement, on a le résultat suivant :

Lemme 1.3 :
Soit W un $\mathbb{F}_q$-sous-espace vectoriel de $\mathbb{K}$ de dimension finie.
Le polynôme $f(x) = \prod_{w \in W} (x - w)$ est $\mathbb{F}_q$-linéaire et séparable.

Preuve :
Soient W un $\mathbb{F}_q$-sous-espace vectoriel de $\mathbb{K}$ de dimension finie et $f(x) = \prod_{w \in W} (x - w)$.
En notant $n = \dim_{\mathbb{F}_q}(W)$, on obtient que $\deg(f) = q^n$ et comme f est unitaire, on a :

$$f(x) = x^{q^n} + \text{ termes de plus petit degré.}$$

De plus, comme $f(x)$ n'a pas de racines multiples, il est séparable.

Considérons désormais le polynôme $H(x) = f(x + y) - f(x) - f(y)$ vu dans $\mathbb{K}(y)[x]$.
Puisque $(x + y)^{q^n} - x^{q^n} - y^{q^n} = 0$, on a $\deg(H(x)) < \deg(f(x)) = q^n$. De plus, pour tout $w \in W$, on a

$$H(w) = f(w + y) - f(w) - f(y) = f(y) - 0 - f(y) = 0,$$

où la deuxième égalité résulte du changement de variable bijectif $w'' = w' - w$ dans la définition de $f(w + y)$. Ainsi, comme H ne peut avoir plus de zéros que son degré, à moins qu'il soit nul, on en déduit que $H(x)$ est nul et donc $f(x)$ est additif.

Finalement, pour $\alpha \in \mathbb{F}_q^\times$, on a

$$f(\alpha x) = \prod_{w \in W} (\alpha x - w) = a^{q^n} \prod_{w \in W} \left(x - \frac{\omega}{\alpha}\right) = \alpha \prod_{w' \in W} (x - w') = \alpha f(x),$$

où la troisième égalité découle du fait que $\alpha^q = \alpha$ (car $\alpha \in \mathbb{F}_q$) et du changement de variable bijectif $w' = \frac{w}{\alpha}$. Donc $f(x)$ est $\mathbb{F}_q$-linéaire.

Ainsi, on a bien montré que $f(x)$ est $\mathbb{F}_q$-linéaire et séparable.

■

Notons $\mathbb{K}\langle x \rangle$ l'ensemble de tous les polynômes $\mathbb{F}_q$-linéaire de $\mathbb{K}[x]$. Il est alors clair que $\mathbb{K}\langle x \rangle$ est stable par addition dans $\mathbb{K}[x]$ mais n'est cependant pas stable pour la multiplication usuelle de polynômes. Pour remédier à cela, on munit plutôt $\mathbb{K}\langle x \rangle$ de la composition usuelle des polynômes. On obtient alors que pour tout $f \in \mathbb{K}\langle x \rangle$ et tout $m \in \mathbb{N}$, le polynôme f^{q^m} (où la puissance est à comprendre au sens de la composition) appartient aussi à $\mathbb{K}\langle x \rangle$ (via la linéarité du Frobenius), donc $\mathbb{K}\langle x \rangle$ est stable par la composition.

De plus, la composition est associative dans $\mathbb{K}\langle x \rangle$ et pour tous $f, g, h \in \mathbb{K}\langle x \rangle$ on a toujours

$$(f + g) \circ h = (f \circ h) + (g \circ h)$$

et puisque f est additif, on a également

$$f \circ (g + h) = f \circ g + f \circ h.$$

Ainsi, $(\mathbb{K}\langle x \rangle, +, \circ)$ est un anneau dont le neutre additif est le polynôme nul et le neutre pour la composition le polynôme x. Cependant, cet anneau n'est pas nécessairement commutatif.

Exemple 1.1 :
Posons $f(x) = ax + bx^q \in \mathbb{K}\langle x\rangle$ et $g(x) = x^q \in \mathbb{K}\langle x\rangle$.
On a alors :

$$f \times g = (ax + bx^q) \times x^q = ax^{q+1} + bx^{2q} \notin \mathbb{K}\langle x\rangle$$

$$f \circ g = ax^q + bx^{q^2} \in \mathbb{K}\langle x\rangle$$

$$g \circ f = (ax + bx^q)^q = a^q x^q + b^q x^{q^2}.$$

De plus, si $a, b \notin \mathbb{F}_q$, alors $f \circ g \neq g \circ f$.

Remarque :
L'anneau $(\mathbb{K}\langle x\rangle, +, \circ)$ a été étudié pour la première fois par Oystein Ore et donc cet anneau porte parfois le nom de **l'anneau des polynômes de Ore**.

Pour étudier des propriétés d'anneau de $(\mathbb{K}\langle x\rangle, +, \circ)$, il est plus commode d'introduire une autre version de cet anneau que nous utiliserons par la suite.

Définition 1.3 : Anneau des polynômes tordus :
On considère R une $\mathbb{F}_q$-algèbre commutative.
On définit **l'anneau des polynômes tordus** (noté $(R\{\tau\}, +, \cdot)$) comme étant l'ensemble des polynômes en l'indéterminée τ muni de l'addition usuelle des polynômes et de la multiplication définie tout d'abord par

$$\left(a\tau^i\right) \cdot \left(b\tau^j\right) = ab^{q^i}\tau^{i+j},$$

puis que l'on étend à tous les polynômes par la distributivité des lois.

Exemple 1.2 :
Pour tous $a, b, c, d \in \mathbb{K}$, on a

$$(a + b\tau)(c + d\tau) = ac + ad\tau + bc^q\tau + bd^q\tau^2 = ac + (ad + bc^q)\,\tau + bd^q\tau^2.$$

On définit désormais l'application

$$\iota : \left| \begin{array}{ccc} (\mathbb{K}\{\tau\}, +, \cdot) & \longrightarrow & (\mathbb{K}\langle x\rangle, +, \circ) \\ \sum_{i=0}^n a_i\tau^i & \longmapsto & \sum_{i=0}^n a_i x^{q^i} \end{array} \right. .$$

On obtient alors que ι est bijective et vérifie $\iota(0) = 0$, $\iota(1) = x$, $\iota(f + g) = \iota(f) + \iota(g)$ et $\iota(f \cdot g) = \iota(f) \circ \iota(g)$. Ainsi, ι est un isomorphisme d'anneaux et par abus de notation on notera $f(x)$ pour désigner $\iota(f)$.

Définition 1.4 : Hauteur et degré d'un polynôme tordu :
On considère un polynôme $f = \sum_{k=h}^n a_k\tau^k$ avec $h \in [\![0; n]\!]$ et $a_h \neq 0$.
On appelle :

* **hauteur de** f la quantité $\mathrm{ht}(f) = h$;
* **degré de** f la quantité $\deg_\tau(f) = n$.

Remarques :

* Pour distinguer le degré de f de celui de $f(x)$ en tant polynôme en la variable x, on note $\deg_\tau(f)$ le degré de f dans $\mathbb{K}\{\tau\}$ et on note $\deg(f)$ le degré de f usuel en tant que polynôme en la variable x.
* Formellement, on pose $\deg_\tau(0) = -\infty$ et $\mathrm{ht}(0) = +\infty$.
* On dira que f est **séparable** lorsque $\mathrm{ht}(f) = 0$ et **inséparable** sinon. Cela étant équivalent au fait que $f(x)$ soit séparable au sens usuel.
* Si $f \neq 0$ et $\mathrm{ht}(f) = h$, alors on peut toujours écrire

  $$f = f_{sep} \cdot \tau^h$$

  pour un unique polynôme séparable $f_{sep} \in \mathbb{K}\{\tau\}$ de degré $n - h$. Cependant, il n'existe pas nécessairement de polynôme g tel que $f = \tau^h \cdot g$ (à moins que $\mathbb{K}$ soit un corps parfait). En traduisant cela au

niveau des polynômes $\mathbb{F}_q$-linéaires correspondants, la décomposition $f = f_{sep} \cdot \tau^h$ correspond à l'écriture $f(x) = \sum_{k=h}^{n} a_k x^{q^k} = f_{sep}\left(x^{q^h}\right)$ avec $f_{sep}(x) = \sum_{k=0}^{n-h} a_{k+h} x^{q^k}$, tandis que l'écriture $f = \tau^h \cdot g$ correspond à $f(x) = g(x)^{q^h}$, où $g(x) = \sum_{k=0}^{n-h} a_{k+h}^{\frac{1}{q^h}} x^{q^k}$.

Lemme 1.4 :
Pour tous polynômes non nuls $f, g \in \mathbb{K}\{\tau\}$, on a

$$\mathrm{ht}(f \cdot g) = \mathrm{ht}(f) + \mathrm{ht}(g) \text{ et } \mathrm{ht}(f+g) \geq \min(\mathrm{ht}(f); \mathrm{ht}(g))$$

ainsi que

$$\deg_\tau(f \cdot g) = \deg_\tau(f) + \deg_\tau(g) \text{ et } \deg_\tau(f+g) \leq \max(\deg_\tau(f); \deg_\tau(g)).$$

La démonstration pour les deux dernières relations étant la même que dans le cas classique et celle des deux premières suivant le même principe, elles sont laissées au lecteur.

Définition 1.5 : Morphisme dérivé :
On appelle **morphisme dérivé** le morphisme ∂ défini par :

$$\partial : \left| \begin{array}{ccc} \mathbb{K}\{\tau\} & \longrightarrow & \mathbb{K} \\ \sum_{i=0}^{n} a_i \tau^i & \longmapsto & a_0 \end{array} \right.$$

Remarque :
Pour tout $f \in \mathbb{K}\{\tau\}$, on a $\partial(f) = f'(x)$.

Bien que l'anneau $(\mathbb{K}\{\tau\}, +, \cdot)$ ne soit pas commutatif, il possède une propriété cruciale en commun avec l'anneau des polynômes classique : **la division euclidienne à droite**.

Théorème 1.1 : Algorithme de division euclidienne à droite :
Soient $f, g \in \mathbb{K}\{\tau\}$ avec $g \neq 0$.
Il existe un unique couple $(h, r) \in \mathbb{K}\{\tau\}^2$ tel que :

$$f = h \cdot g + r \text{ et } \deg_\tau(r) < \deg_\tau(g).$$

La preuve étant également très similaire au cas classique, elle est laissée au lecteur qui pourra en trouver une démonstration dans [Pap23] à la page 137.

Remarque :
Il est très important que h soit mis à la gauche de g ! En effet, supposons que $\mathbb{K}$ ne soit pas un corps parfait. On peut alors trouver $a \in \mathbb{K}$ tel que a ne soit pas une puissance q-ième d'un élément de $b \in \mathbb{K}$ et en posant $f = a\tau^2$ et $g = \tau$, alors pour $h = a\tau$ on a bien $f = h \cdot g$. Cependant il n'existe pas de tel h tel que $\deg_\tau(f - g \cdot h) < \deg_\tau(g)$ et donc le théorème devient faux. Pour voir cela, on peut remarquer que h doit être de degré 1 et donc être de la forme $h = b\tau + c$ et on doit alors avoir $\deg_\tau\left(a\tau^2 - b^q\tau^2 - c^q\tau\right) < 2$. Ainsi on trouve $a = b^q$, ce qui contredit notre hypothèse de départ.

Corollaire 1.1 :
Tout idéal à gauche de $(\mathbb{K}\{\tau\}, +, \cdot)$ est principal.

De même que pour le théorème précédent, la preuve est laissée au lecteur qui pourra en trouver une démonstration dans [Pap23] à la page 138 et qui correspond à la démonstration classique dans le cas de $\mathbb{K}[x]$.

Corollaire 1.2 :
Soient $f, g \in \mathbb{K}\{\tau\}$ tels que $g \neq 0$ et $\mathrm{ht}(f) \geq \mathrm{ht}(g)$.
Les racines de $g(x)$ sont racines de $f(x)$ si, et seulement si, il existe $h \in \mathbb{K}\{\tau\}$ tel que $f = h \cdot g$.
Dans ce cas, si f et g commutent dans $\mathbb{K}\{\tau\}$, alors on a également $f = g \cdot h$.

Preuve :
Soient $f, g \in \mathbb{K}\{\tau\}$ tels que $g \neq 0$ et $\mathrm{ht}(f) \geq \mathrm{ht}(g)$.

* Montrons le résultat principal par double implication :
  — Supposons qu'il existe $h \in \mathbb{K}\{\tau\}$ tel que $f = h \cdot g$.
  Soit $\alpha \in \overline{\mathbb{K}}$ une racine de $g(x)$.
  On a alors $f(\alpha) = (h \circ g)(\alpha) = h(g(\alpha)) = h(0) = 0$, donc α est également une racine de $f(x)$.

  — Réciproquement, supposons que les racines de $g(x)$ soient racines de $f(x)$.
  Par le théorème 1.1, il existe un unique couple $(h, r) \in \mathbb{K}\{\tau\}^2$ tel que l'on ait $f(x) = (h \circ g)(x) + r(x)$ avec $\deg_\tau(r) < \deg_\tau(g)$.

  De plus, en considérant α une racine de $g(x)$, on a alors par hypothèse :

$$f(\alpha) = (h \circ g)(\alpha) + r(\alpha) = h(0) + r(\alpha) = r(\alpha) = 0.$$

  Ainsi, chaque racine de $g(x)$ est racine de $r(x)$ sans comptées avec multiplicité. Cela implique donc que $\deg_\tau(r_{sep}) \leq \deg_\tau(r_{sep})$. De plus, on a par le lemme 1.4 que :

$$\mathrm{ht}(r) = \mathrm{ht}(f - h \cdot g) \geq \min(\mathrm{ht}(f), \mathrm{ht}(hg)) \geq \min(\mathrm{ht}(f); \mathrm{ht}(g)) = \mathrm{ht}(g).$$

  Enfin, en supposant que $r \neq 0$, on obtient que

$$\deg_\tau(r) = \deg_\tau(r_{sep}) + \mathrm{ht}(r) \geq \deg_\tau(g_{sep}) + \mathrm{ht}(g) = \deg_\tau(g),$$

  ce qui contredit l'hypothèse faite sur $\deg_\tau(r)$. On obtient alors que $r = 0$ et donc $f = h \cdot g$.

* Enfin, supposons de plus que $f = h \cdot g$ et que f et g commutent dans $\mathbb{K}\{\tau\}$.
  On obtient alors que $f \cdot g = g \cdot f = g \cdot (h \cdot g) = (g \cdot h) \cdot g$, ce qui donne $(f - g \cdot h) \cdot g = 0$ et puisque $\mathbb{K}\{\tau\}$ est intègre et que $g \neq 0$ par hypothèse, on trouve que $f = h \cdot g$.

■

II Modules de Drinfeld

Définition 1.6 : A-corps :
On appelle **A-corps**, tout corps $\mathbb{K}$ muni d'un morphisme de $\mathbb{F}_q$-algèbres $\gamma : A \longrightarrow \mathbb{K}$.

Puisque $\mathbb{K}$ est un corps et que tout idéal premier de A est maximal, on a alors deux possibilités :

* $\mathrm{Ker}(\gamma) = (0)$ (c'est-à-dire que γ est injectif). Dans ce cas, $\mathbb{K}$ est une extension de corps de F (non nécessairement algébrique) et on dit que $\mathbb{K}$ a pour A-caractéristique 0, que l'on note $\mathrm{car}_A(\mathbb{K}) = 0$.
* $\mathrm{Ker}(\gamma) = \mathfrak{p}$ est un idéal premier de A. Dans ce cas, γ se factorise au travers de la projection canonique $\pi : A \longrightarrow A/\mathfrak{p}$ et donc $\mathbb{K}$ est une extension de corps de $\mathbb{F}_\mathfrak{p}$ et on dit que $\mathbb{K}$ a pour A-caractéristique $\mathfrak{p}$, que l'on note $\mathrm{car}_A(\mathbb{K}) = \mathfrak{p}$.

Remarque :
Il est important de noter que le même corps peut avoir différentes structures de A-corps. Par exemple, $\mathbb{K} = \mathbb{F}_q$ est un A-corps via $\gamma_1 : A \longrightarrow A/(T) \cong \mathbb{F}_q$ mais aussi via $\gamma_2 : A \longrightarrow A/(T-1) \cong \mathbb{F}_q$. Pire encore, $\mathbb{K} = \mathbb{F}_q(T)$ est un A-corps via $\gamma_1 : A \longrightarrow \mathbb{K}$ étant le plongement naturel de A dans son corps des fractions, mais aussi via $\gamma_2 : A \longrightarrow A/(T) \cong \mathbb{F}_q \hookrightarrow \mathbb{F}_q(T)$. Dans le premier cas, on trouve que $\mathrm{car}_A(\mathbb{K}) = 0$ et dans le second cas que $\mathrm{car}_A(\mathbb{K}) = (T)$!

Pour le reste de cette partie, sauf indication contraire, $\mathbb{K}$ sera un A-corps avec un morphisme de $\mathbb{F}_q$-algèbres $\gamma : A \longrightarrow \mathbb{K}$. De plus, on identifiera $\mathbb{F}_q \subseteq A$ avec son image dans $\mathbb{K}$.

Définition 1.7 : Module de Drinfeld de rang r :
On appelle **module de Drinfeld de rang** $r \in \mathbb{N}^*$ **sur** $\mathbb{K}$ tout morphisme de $\mathbb{F}_q$-algèbres

$$\phi : \left| \begin{array}{ccc} A & \longrightarrow & \mathbb{K}\{\tau\} \\ a & \longmapsto & \phi_a := \gamma(a) + \sum_{i=1}^{n} g_i(a)\tau^i \end{array} \right. ,$$

où pour $a \neq 0$ on a $n = \deg(a)r$ et $g_n(a) \neq 0$.

Remarques :

* Si $\deg(a) > 0$, alors $\deg_\tau(\phi_a) > 0$, ainsi le morphisme ϕ est toujours injectif et cela nous donne une plongement de l'anneau commutatif $(A, +, \times)$ dans l'anneau non commutatif $(\mathbb{K}\{\tau\}, +, \cdot)$.
* Les coefficients $g_1(a), \ldots, g_n(a) \in \mathbb{K}$ de ϕ_a dépendent de a. D'autre part, pour $a = \sum_{i=0}^{m} a_i T^i \in A$, on a

$$\phi_a = \sum_{i=0}^{m} a_i \phi_{T^i} = \sum_{i=0}^{m} a_i \phi_T^i.$$

Ainsi, ϕ_T détermine entièrement ϕ. De plus, si $\deg_\tau(\phi_T) = r$ et que le terme constant de ϕ_T est $\gamma(T)$, alors

$$\deg_\tau(\phi_a) = \deg_\tau(\phi_T^m) = m \deg_\tau(\phi_T) = \deg(a)r$$

et le terme constant de ϕ_a est

$$\sum_{i=0}^{m} a_i \gamma(T)^i = \sum_{i=0}^{m} a_i \gamma\left(T^i\right) = \gamma\left(\sum_{i=0}^{m} a_i T^i\right) = \gamma(a).$$

Par conséquent, les conditions sur ϕ_a dans la définition d'un module de Drinfeld de rang r sont automatiquement vérifiées dès lors qu'elles le sont pour ϕ_T. Pour finir, on en déduit que pour définir un module de Drinfeld de rang r, il suffit de choisir $g_1, \ldots, g_r \in \mathbb{K}$ tels que $g_r \neq 0$ et poser

$$\phi_T = \gamma(T) + \sum_{i=1}^{r} g_i \tau^i.$$

À partir de maintenant, afin de simplifier les notations, on notera $t = \gamma(T)$.

Définition 1.8 : Module de Carlitz :
On appelle **module de Carlitz** le module de Drinfeld défini par $\phi_T := t + \tau$.

Le module de Carlitz est ainsi le module de Drinfeld le plus simple possible et on le distinguera des autres modules de Drinfeld en le notant C (ici $C_T = t + \tau$). De plus, le module de Carlitz est un module de Drinfeld de rang 1.

Exemple 1.3 :
Pour calculer C_{T^2-T+1}, on peut commencer par calculer

$$C_{T^2} = (C_T)^2 = (t+\tau)(t+\tau) = t^2 + t\tau + \tau t + \tau^2 = t^2 + t\tau + t^q\tau + \tau^2 = t^2 + (t + t^q)\tau + \tau^2$$

puis remarquer que

$$C_{T^2-T+1} = C_{T^2} - C_T + 1 = \left(t^2 + (t+t^q)\tau + \tau^2\right) - (t+\tau) + 1 = \left(t^2 - t + 1\right) + (t + t^q - 1)\tau + \tau^2.$$

Remarques :

* Il existe une formule récursive générale pour calculer les coefficients de

$$C_a = C_0(a) + C_1(a)\tau + \cdots + C_d(a)\tau^d, \ a \in A, \ d = \deg(a).$$

Pour l'obtenir, supposons que C est défini sur F avec $\gamma : A \longrightarrow F$ étant le plongement naturel de A dans son corps des fractions. En comparant les coefficients des τ^m de chaque côté de l'équation $C_a \cdot C_T = C_T \cdot C_a$, on obtient :

$$C_m(a)T^{q^m} + C_{m-1}(a) = TC_m(a) + C_{m-1}(a)^q. \tag{1.3}$$

Ainsi,

$$C_m(a) = \frac{C_{m-1}(a)^q - C_{m-1}(a)}{T^{q^m} - T}$$

peut être calculé récursivement en commençant avec $C_0(a) = a$, puis $C_1(a) = \frac{a^q - a}{T^q - T}$, etc.

* De plus, chaque $C_i(a)$ appartient à A bien qu'il est exprimé comme fractions de polynômes (cela vient du fait que chaque $C_{T^n} = (C_T)^n$ est à coefficients dans A).
* Finalement, si C est défini sur un A-corps $\mathbb{K}$ général, alors on obtient le m-ième coefficient de C_a en appliquant γ au membre de droite de (1.3).

Remarquons désormais que $\mathbb{K}$ possède une structure de A-algèbre mais possède également une structure naturelle de A-module définie par $a * \beta = \gamma(a)\beta$. Ainsi, via $\phi : A \longrightarrow \mathbb{K}\{\tau\}$, $\mathbb{K}$ acquiert une nouvelle structure de A-module (tordu) définie par $a * \beta = \phi_a(\beta)$ (où $\phi_a(\beta)$ est le polynôme $\mathbb{F}_q$-linéaire $\phi_a(x)$ évalué en β) et nous noterons ce A-module par ${}^{\phi}\mathbb{K}$.

Remarque :
Le fait que ϕ donne une nouvelle structure de A-module à $\mathbb{K}$ est la raison pour laquelle on appelle ϕ un "module" alors qu'il ne s'agit que d'un morphisme de $\mathbb{F}_q$-algèbres.

Exemple 1.4 :
Posons $\mathbb{K} = A/(T) \cong \mathbb{F}_q$ avec $\gamma : A \longrightarrow A/(T)$ la projection naturelle.
Le A-module ${}^{C}\mathbb{K}$ est un $\mathbb{F}_q$-espace vectoriel de dimension 1, il est donc isomorphe à $A/\mathfrak{p}$ avec $\mathfrak{p}$ un idéal premier de A de degré 1. Pour trouver $\mathfrak{p}$, on peut remarquer que $t = \gamma(T) = \overline{0}$ et donc $C_T = \tau$ et T agit sur ${}^{C}\mathbb{K}$ par $T * \beta = \beta^q = \beta$. Ainsi, T agit comme 1 et donc ${}^{C}\mathbb{K} \cong A/(T-1)$.

Soit $a \in A \setminus \{0_A\}$.
On a $\partial(\phi_a) = \gamma(a)$ et donc si $\mathrm{car}_A(\mathbb{K}) = 0$, alors $\mathrm{ht}(\phi_a) = 0$ (c'est-à-dire ϕ_a est séparable). D'autre part, si $\mathrm{car}_A(K) = \mathfrak{p} \neq 0$, alors ϕ_a n'est pas séparable et donc $\mathrm{ht}(\phi_a) \geq 1$.

Le lemme suivant donne une information plus raffinée sur l'inséparabilité de $\phi_{\mathfrak{p}}(x)$ à partir de $\mathrm{ht}(\phi_{\mathfrak{p}})$:

Lemme 1.5 :
Soit ϕ un module de Drinfeld de rang r sur $\mathbb{K}$.
Si $\mathrm{car}_A(\mathbb{K}) = \mathfrak{p} \neq 0$, alors il existe un entier $H(\phi) \in [\![1; r]\!]$ tel que pour tout $a \in A \setminus \{0_A\}$ on ait

$$\mathrm{ht}(\phi_a) = H(\phi)\,\mathrm{val}_{\mathfrak{p}}(a)\,\deg(\mathfrak{p}).$$

Preuve :
Soit ϕ un module de Drinfeld de rang r sur $\mathbb{K}$.
Supposons que $\mathrm{car}_A(\mathbb{K}) = \mathfrak{p} \neq 0$ et posons $h := \mathrm{ht}(\phi_{\mathfrak{p}}) \geq 1$.
Remarquons que $h \leq \deg_\tau(\phi_{\mathfrak{p}}) = r\deg(\mathfrak{p})$ et pour $a \in A \setminus \{0_A\}$ que l'on écrit sous la forme $a = \mathfrak{p}^s b$ avec $\mathfrak{p} \nmid b$, on a $\gamma(b) \neq 0$ et $\mathrm{ht}(\phi_b) = 0$, donc par le lemme 1.4 on obtient :

$$\mathrm{ht}(\phi_a) = \mathrm{ht}(\phi_{\mathfrak{p}^s b}) = \mathrm{ht}(\phi_{\mathfrak{p}^s} \cdot \phi_b) = \mathrm{ht}(\phi_{\mathfrak{p}^s}) + \mathrm{ht}(\phi_b) = \mathrm{ht}(\phi_{\mathfrak{p}^s}) = \mathrm{ht}((\phi_{\mathfrak{p}})^s) = s\,\mathrm{ht}(\phi_{\mathfrak{p}}) = \mathrm{val}_{\mathfrak{p}}(a)h.$$

Il nous suffit alors de prouver que h est divisible par $\deg(\mathfrak{p})$.
Or on a $\phi_{\mathfrak{p}} = \sum_{i=h}^{n} c_i \tau^i$ avec $c_h \neq 0$ et puisque l'on a $\phi_a\phi_{\mathfrak{p}} = \phi_{\mathfrak{p}}\phi_a$, on en déduit que $\gamma(a)c_h = c_h\gamma(a)^{q^h}$.

Or puisque cela est vrai pour tout $a \in A$, on en déduit que $\gamma(A) = \mathbb{F}_{\mathfrak{p}} \cong \mathbb{F}_{q^{\deg(\mathfrak{p})}} \subseteq \mathbb{F}_{q^h}$ et donc par inclusion de corps finis on a h qui divise $\deg(\mathfrak{p})$. Il existe alors un entier $H(\phi) \in [\![1; r]\!]$ (car ϕ est de rang r) tel que $\deg(\mathfrak{p}) = H(\phi)h$ et ainsi :

$$\mathrm{ht}(\phi_a) = \mathrm{val}_{\mathfrak{p}}(a)h = H(\phi)\,\mathrm{val}_{\mathfrak{p}}(a)\,\deg(\mathfrak{p}).$$

■

Définition 1.9 : Hauteur d'un module de Drinfeld :
On considère ϕ un module de Drinfeld de rang r.
On appelle **hauteur de** ϕ l'entier $H(\phi)$ défini dans le lemme précédent.

Exemple 1.5 :
Posons $q := 2$, $\mathbb{K} := A/\mathfrak{p}$ où $\mathfrak{p} := \left(1 + T + T^2\right)$ et considérons ϕ le module de Drinfeld de rang 2 défini par $\phi_T := t + \tau + \tau^2$.
On a (en utilisant le fait que la caractéristique est égale à 2) :

$$\begin{aligned}\phi_{\mathfrak{p}} &= \phi_T^0 + \phi_T^1 + \phi_T^2 = 1 + \left(t + \tau + \tau^2\right) + \left(t + \tau + \tau^2\right)\left(t + \tau + \tau^2\right) \\ &= 1 + t + \tau + \tau^2 + t^2 + t\tau + t\tau^2 + t^2\tau + \tau^2 + \tau^3 + t^{2^2}\tau^2 + \tau^3 + \tau^4 \\ &= (1 + t + t^2) + \left(1 + t + t^2\right)\tau + \left(2 + t + t^4\right)\tau^2 + 2\tau^3 + \tau^4 \\ &= \left(2 + t + t^4\right)\tau^2 + 2\tau^3 + \tau^4 = 2(t+2)\tau^2 + \tau^4 = \tau^4\end{aligned}$$

On a alors par le lemme 1.5 que $4 = H(\phi) \times 1 \times 2$, donc $H(\phi) = 2$.

Exemple 1.6 :
Utilisons le lemme 1.5 pour généraliser l'exemple 1.4 à un idéal premier non nul de A :
Soient $\mathfrak{p}$ un idéal premier non nul de A, $\mathbb{K} = A/\mathfrak{p}$ et $\gamma : A \longrightarrow \mathbb{K}$ la projection naturelle.
Par le théorème de structure des modules de type fini sur un anneau principal, on a

$$^C\mathbb{K} \cong \bigoplus_{i=1}^{s} A/(a_i)$$

avec $a_1 \mid a_2 \mid \cdots \mid a_s$ et unitaires. Ainsi, on obtient que

$$q^{\sum_{i=1}^{s} \deg(a_i)} = \mathrm{Card}(\mathbb{K}) = q^{\deg(\mathfrak{p})}.$$

De plus, chaque élément de $\mathbb{K}$ est une racine de $C_{a_s}(x)$ puisque a_s annule $^C\mathbb{K}$. Cela implique alors que

$$\deg\left(C_{a_s}(x)\right) = q^{\deg(a_s)} \geq q^{\deg(\mathfrak{p})}.$$

Ainsi, on trouve que $s = 1$ et $\deg(a_s) = \deg(\mathfrak{p})$ et puisque le module de Carlitz est de rang 1, le lemme 1.5 donne que $H(C) = 1$ et donc $C_{\mathfrak{p}} = \tau^{\deg(\mathfrak{p})}$.

Or, puisque $\tau^{\deg(\mathfrak{p})}$ fixe tous les éléments de $\mathbb{K}$ (en effet, $\mathbb{K}$ est un corps fini à $q^{\deg(\mathfrak{p})}$ éléments, donc pour tout $\alpha \in \mathbb{K}$, $\tau^{\deg(\mathfrak{p})}(\alpha) = \alpha^{q^{\deg(\mathfrak{p})}} = \alpha$, d'où $C_{\mathfrak{p}-1}(\alpha) = 0$), on en déduit que $\mathfrak{p} - 1$ annule $^C\mathbb{K}$ et donc a_1 divise $\mathfrak{p} - 1$.
Mais puisque l'on a prouvé que $\deg(a_1) = \deg(\mathfrak{p}) = \deg(\mathfrak{p} - 1)$, on en déduit que $a_1 = \mathfrak{p} - 1$ et donc en tant que A-module :

$$^C(A/\mathfrak{p}) \cong A/(\mathfrak{p} - 1).$$

La définition d'un module de Drinfeld sur un corps peut facilement être étendue au cas d'un anneau commutatif quelconque. En effet, considérons R une A-algèbre commutative (c'est-à-dire un anneau R munit d'un morphisme d'anneaux $\gamma : A \longrightarrow R$) et on identifie $\mathbb{F}_q \subseteq A$ avec son image isomorphe dans R.

Un module de Drinfeld de rang r sur R est un morphisme d'anneaux $\phi : A \longrightarrow R\{\tau\}$ satisfaisant les mêmes conditions que celles imposées pour les modules de Drinfeld sur un corps (c'est-à-dire $\partial(\phi_a) = \gamma(a)$ ainsi que $\deg_\tau(\phi_a) = \deg(a)r$). Encore une fois, ϕ est uniquement déterminé par

$$\phi_T = t + \sum_{i=1}^{r} g_i \tau^i,$$

où les coefficients $g_1, \ldots, g_r \in R$ peuvent être choisis arbitrairement à l'exception de g_r qui doit être un élément non nilpotent de l'anneau R (en effet, dans le cas contraire, la relation sur les degrés peut ne plus être vérifiée).

Via ϕ, on obtient une fois de plus une nouvelle structure de A-module sur R définie par $a * \beta = \phi_a(\beta)$ et on note encore ${}^{\phi}R$ cette structure. De plus, le passage de la structure de A-algèbre sur R à celle de A-module sur R se comporte bien vis-à-vis des morphismes de A-algèbres. En effet, si $f : R \longrightarrow S$ est un morphisme de A-algèbres, alors pour tout $\beta \in R$ on a $f(\phi_a(\beta)) = \phi_a(f(\beta))$ et donc $f :{}^{\phi} R \longrightarrow {}^{\phi} S$ est un morphisme de A-modules (on a même que l'application $R \longrightarrow {}^{\phi} R$ est un foncteur de la catégorie des A-algèbres dans la catégorie des A-modules).

Nous aurons plus tard besoin du lemme suivant qui généralise le lemme 1.5 :

Lemme 1.6 :
Soient R une A-algèbre commutative munie d'un morphisme d'anneaux $\gamma : A \longrightarrow R$, un module de Drinfeld $\phi : A \longrightarrow R\{\tau\}$ de rang r défini par $\phi : a \longmapsto \phi_a = \sum_{i=0}^{r \deg(a)} g_i(a)\tau^i$ et $\mathfrak{p}$ un idéal premier non nul de A de degré d.
Il existe un entier $H \in [\![1; r]\!]$ tel que pour tout $i \in [\![0; Hd-1]\!]$ et tout $n \in \mathbb{N}^*$ on ait $g_i(\mathfrak{p}^n) \in \gamma(\mathfrak{p}^n) R$.

Preuve :
Soient R une A-algèbre commutative munie d'un morphisme d'anneaux $\gamma : A \longrightarrow R$, un module de Drinfeld $\phi : A \longrightarrow R\{\tau\}$ de rang r défini par $\phi : a \longmapsto \phi_a = \sum_{i=0}^{r \deg(a)} g_i(a)\tau^i$ et $\mathfrak{p}$ un idéal premier non nul de A de degré d.
Considérons la A-algèbre $B = A[g_1, \dots, g_r]$ (où $g_1, \dots, g_r$ sont des indéterminées) et posons $\widetilde{\phi} : A \longrightarrow B\{\tau\}$ le module de Drinfeld défini par $\widetilde{\phi}_T := T + \sum_{i=1}^{r} g_i\tau^i$.

Tout d'abord, montrons qu'il existe un entier $H \in [\![1; r]\!]$ tel que pour tout $n \in \mathbb{N}^*$ on ait

$$\widetilde{\phi}_{\mathfrak{p}^n} = \mathfrak{p}^n f_n + g_n,$$

où $f_n, g_n \in B\{\tau\}$, $\deg_\tau(f_n) \leq Hd-1$ et $\mathrm{ht}_\tau(g_n) \geq Hd$. Pour cela, raisonnons par récurrence simple :

$*$ Initialisation pour $n = 1$:
Considérons l'application de réduction modulo $\mathfrak{p}$ que l'on notera $\iota : B \longrightarrow B' = \mathbb{F}_{\mathfrak{p}}[g_1, ..., g_r]$. Cette application s'étend naturellement en une application encore noté ι de $B\{\tau\}$ dans $B'\{\tau\}$. La composition $\overline{\phi} = \iota \circ \widetilde{\phi} : A \longrightarrow B'\{\tau\}$ est un module de Drinfeld sur B', qui peut également être vu comme un module de Drinfeld sur le corps des fractions $\mathbb{K}$ de B'.

De plus, on a $\mathrm{car}_A(\mathbb{K}) = \mathfrak{p} \neq 0$, donc par le lemme 1.5, il existe un entier $H \in [\![1; r]\!]$ tel que $\mathrm{ht}\left(\overline{\phi_{\mathfrak{p}}}\right) = Hd$. Ainsi, on a $\widetilde{\phi}_{\mathfrak{p}} = \mathfrak{p} f_1 + g_1$, avec $f_1, g_1 \in B\{\tau\}$, $\deg(f_1) \leq Hd-1$ et $\mathrm{ht}(g_1) \geq Hd$. La propriété est donc bien initialisée.

$*$ Hérédité :
Supposons que l'on ait montré que $\widetilde{\phi}_{\mathfrak{p}^n} = \mathfrak{p}^n f_n + g_n$ avec $f_n, g_n \in B\{\tau\}$, $\deg_\tau(f_n) \leq Hd-1$ et $\mathrm{ht}_\tau(g_n) \geq Hd$ pour un certain entier naturel $n \in \mathbb{N}^*$.

On a alors :

$$\begin{aligned}\widetilde{\phi}_{\mathfrak{p}^{n+1}} &= \widetilde{\phi}_{\mathfrak{p}}\widetilde{\phi_{\mathfrak{p}^n}} = (\mathfrak{p} f_1 + g_1)(\mathfrak{p}^n f_n + g_n) \\ &= \mathfrak{p} f_1 \mathfrak{p}^n f_n + (\mathfrak{p} f_1 g_n + g_1 \mathfrak{p}^n f_n + g_1 g_n).\end{aligned}$$

En posant $g := \mathfrak{p} f_1 g_n + g_1 \mathfrak{p}^n f_n + g_1 g_n$, on obtient que $\mathrm{ht}(g) \geq Hd$ puisque $\mathrm{ht}(g_1) \geq Hd$ et $\mathrm{ht}(g_n) \geq Hd$ (en prolongeant le lemme 1.5 au cas de $B\{\tau\}$). De plus, remarquons que $\mathfrak{p} f_1 \mathfrak{p}^n f_n = \mathfrak{p}^{n+1} f$ pour $f \in B\{\tau\}$ (mais $f \neq f_1 f_n$ en général !). On peut alors écrire $f = f_{n+1} + h_{n+1}$ avec $\deg(f_{n+1}) \leq Hd-1$ et $\mathrm{ht}(h_{n+1}) \geq Hd$ et en posant $g_{n+1} = \mathfrak{p}^{n+1} h_{n+1} + g$ on a $\widetilde{\phi}_{\mathfrak{p}^{n+1}} = \mathfrak{p}^{n+1} f_{n+1} + g_{n+1}$ avec $\deg(f_{n+1}) \leq Hd-1$ et $\mathrm{ht}(g_{n+1}) \geq Hd$. La proposition est donc héréditaire.

On a donc démontré l'affirmation par récurrence. Pour conclure, il suffit d'observer que ϕ s'obtient via $\widetilde{\phi}$ au travers du morphisme de B dans R qui envoie a sur $\gamma(a)$ et les g_i sur $g_i(T)$. Ainsi, pour tout $i \in [\![0; Hd-1]\!]$, on a $g_i(\mathfrak{p}^n) \in \gamma(\mathfrak{p}^n) R$.

■

III Morphismes de modules de Drinfeld

Maintenant que nous avons donné la définition d'un module de Drinfeld, nous allons nous intéresser à l'étude des morphismes entre de tels objets. Commençons par rappeler la définition d'un morphisme entre deux modules M et N sur un anneau commutatif R.

Définition 1.10 : Morphisme de R-modules :
On considère deux modules M et N sur un anneau commutatif R.
On appelle **morphisme de R-modules** toute application $f : M \longrightarrow N$ telle que :

* $\forall x, y \in M,\ f(x+y) = f(x) + f(y)$;
* $\forall r \in R,\ \forall x \in M,\ f(rx) = rf(x)$.

En considérant désormais deux modules de Drinfeld ϕ et ψ sur un corps $\mathbb{K}$ et en appliquant la définition précédente à ${}^{\phi}\mathbb{K}$ et ${}^{\psi}\mathbb{K}$, on obtient la définition d'un morphisme de modules de Drinfeld :

Définition 1.11 : Morphisme de modules de Drinfeld :
On considère un corps $\mathbb{K}$ et deux modules de Drinfeld ϕ et ψ sur $\mathbb{K}$.
On appelle **morphisme de modules de Drinfeld** tout polynôme $u \in \mathbb{K}\{\tau\}$ tel que pour tout $a \in A$ on ait $u \cdot \phi_a = \psi_a \cdot u$ et on le note $u : \phi \longrightarrow \psi$.

Remarque :
En particulier, u est un morphisme de A-modules de ${}^{\phi}\mathbb{K}$ dans ${}^{\psi}\mathbb{K}$, c'est-à-dire que le diagramme suivant commute :

$$\begin{array}{ccc} \mathbb{K} & \xrightarrow{u} & \mathbb{K} \\ {\scriptstyle \phi_a}\downarrow & & \downarrow{\scriptstyle \psi_a} \\ \mathbb{K} & \xrightarrow{u} & \mathbb{K} \end{array}$$

Définition 1.12 : Isogénie :
On considère un corps $\mathbb{K}$ et deux modules de Drinfeld ϕ et ψ sur $\mathbb{K}$.
On appelle **isogénie** tout morphisme de Drinfeld $u : \phi \longrightarrow \psi$ non nul.

Le groupe des morphismes entre deux modules de Drinfeld ϕ et ψ sur un corps $\mathbb{K}$ est noté $\mathrm{Hom}_{\mathbb{K}}(\phi, \psi)$ et on note également $\mathrm{End}_{\mathbb{K}}(\phi) = \mathrm{Hom}_{\mathbb{K}}(\phi, \phi)$. Muni de l'addition et de la composition usuelle, $\mathrm{End}_{\mathbb{K}}(\phi)$ est un sous-anneau de $(\mathbb{K}\{\tau\}, +, \cdot)$ appelé **anneau des endomorphismes de** ϕ. De plus, l'ensemble des éléments inversibles de $\mathrm{End}_{\mathbb{K}}(\phi)$ forme un groupe appelé **groupe des automorphismes de** ϕ que l'on note $\mathrm{Aut}_{\mathbb{K}}(\phi)$.

Remarques :

* Puisque l'élément T engendre la $\mathbb{F}_q$-algèbre A, il nous suffit d'avoir $u \cdot \phi_T = \psi_T \cdot u$ pour obtenir que pour tout $a \in A,\ u \cdot \phi_a = \psi_a \cdot u$. Ainsi :

$$\mathrm{Hom}_{\mathbb{K}}(\phi, \psi) = \{u \in \mathbb{K}\{\tau\} \mid u \cdot \phi_T = \psi_T \cdot u\}.$$

* Pour une extension de corps $\mathbb{L}/\mathbb{K}$, on définit

$$\mathrm{Hom}_{\mathbb{L}}(\phi, \psi) = \{u \in \mathbb{L}\{\tau\} \mid u \cdot \phi_T = \psi_T \cdot u\},$$

on obtient alors que $\mathrm{Hom}_{\mathbb{K}}(\phi, \psi) \subseteq \mathrm{Hom}_{\mathbb{L}}(\phi, \psi)$ et comme on le verra, l'inclusion peut être stricte.

En considérant $a \in A$ et $u \in \mathrm{Hom}_{\mathbb{K}}(\phi, \psi)$, on définit

$$a \circ u := u \cdot \phi_a = \psi_a \cdot u.$$

On obtient alors que $a \circ u \in \mathrm{Hom}_{\mathbb{K}}(\phi, \psi)$ puisque :

$$(a \circ u) \cdot \phi_T = u \cdot \phi_a \cdot \phi_T = u \cdot \phi_T \cdot \phi_a = \psi_T \cdot u \cdot \phi_a = \psi_T \cdot (a \circ u).$$

Ainsi, $\mathrm{Hom}_{\mathbb{K}}(\phi,\psi)$ est muni d'une structure de A-module et puisque $\mathbb{K}\{\tau\}$ est intègre, $\mathrm{Hom}_{\mathbb{K}}(\phi,\psi)$ n'a pas d'éléments de torsion en tant que A-module. De plus, avec l'action de A, l'anneau $\mathrm{End}_{\mathbb{K}}(\phi)$ est une A-algèbre (puisque $\phi(A)$ appartient au centre de $\mathrm{End}_{\mathbb{K}}(\phi)$) et pour une extension de corps $\mathbb{L}/\mathbb{K}$ donnée on obtient que $\mathrm{Hom}_{\mathbb{K}}(\phi,\psi)$ est un A-sous-module de $\mathrm{Hom}_{\mathbb{L}}(\phi,\psi)$.

Exemple 1.7 :
Si $\mathrm{car}_A(\mathbb{K})=0$, alors de manière générale on a $\phi(A)=\mathrm{End}_{\mathbb{K}}(\phi)$. Cependant, il existe des modules de Drinfeld dont l'anneau des endomorphismes contient strictement $\phi(A)$.

En effet, considérons le module de Drinfeld $\phi : A \longrightarrow F\{\tau\}$ défini par $\phi_T := T+\tau^r$ et posons $\mathbb{K}=\mathbb{F}_{q^r}F$. On obtient alors que $\mathbb{F}_{q^r}\subseteq \mathrm{End}_{\mathbb{K}}(\phi)$ puisque tout élément de $\mathbb{F}_{q^r}$ est fixé par τ^r. Ainsi :

$$\mathbb{F}_{q^r}\phi(A)\cong \mathbb{F}_{q^r}[T]\subseteq \mathrm{End}_{\mathbb{K}}(\phi).$$

D'autre part, $\mathbb{F}_{q^r}[T]$ est la clôture intégrale de A dans l'extension $\mathbb{K}/F$ qui est de degré r, donc en particulier $\mathbb{F}_{q^r}[T]$ est un A-module de type fini et de rang r. On peut alors montrer que $\mathrm{End}_{\mathbb{K}}(\phi)\cong \mathbb{F}_{q^r}[T]$ et $\mathrm{End}_F(\phi)=\phi(A)\subsetneq \mathrm{End}_{\mathbb{K}}(\phi)$.

Exemple 1.8 :
Considérons $\mathbb{K}:=\mathbb{F}_{q^2}$, $\gamma : A\longrightarrow A/(T)\cong \mathbb{F}_q\hookrightarrow \mathbb{K}$ et $\phi : A\longrightarrow \mathbb{K}\{\tau\}$ le module de Drinfeld de rang 2 défini par $\phi_T := t+\tau^2=\tau^2$.
Dans ce cas, on obtient comme dans l'exemple précédent que $\mathbb{F}_{q^2}\subseteq \mathrm{End}_{\mathbb{K}}(\phi)$ mais ici on a également le fait que $\tau\in\mathrm{End}_{\mathbb{K}}(\phi)$. Ainsi, $\mathbb{K}\{\tau\}\subseteq\mathrm{End}_{\mathbb{K}}(\phi)$ et par définition de $\mathrm{End}_{\mathbb{K}}(\phi)$ on a l'inclusion réciproque, d'où l'égalité $\mathbb{K}\{\tau\}=\mathrm{End}_{\mathbb{K}}(\phi)$.

Proposition 1.1 :
Soit $u:\phi\longrightarrow\psi$ une isogénie.

- Le rang de ϕ est égal au rang de ψ ;
- On a $H(\phi)=H(\psi)$;
- Si $\mathrm{car}_A(\mathbb{K})=0$, alors u est séparable ;
- Si $\mathrm{car}_A(\mathbb{K})=\mathfrak{p}\neq 0$, alors $\deg(\mathfrak{p})$ divise $\mathrm{ht}(u)$;
- Si $\mathrm{car}_A(\mathbb{K})=0$, alors le morphisme suivant est injectif :

$$\chi : \left|\begin{array}{ccc}\mathrm{Hom}_{\mathbb{K}}(\phi,\psi) & \longrightarrow & \mathbb{K}\\ u & \longmapsto & \partial(u)\end{array}\right. .$$

En particulier, $\mathrm{End}_{\mathbb{K}}(\phi)$ est un anneau commutatif.

Preuve :
Soit $u:\phi\longrightarrow\psi$ une isogénie.

- En calculant le degré en τ de chaque côté de l'égalité $u\cdot\phi_T=\phi_T\cdot u$, on obtient $\deg(\phi_T)=\deg(\psi_T)$ et donc le rang de ϕ est égal à rang de ψ.

- De même, en calculant la hauteur de chaque côté de l'égalité $u\cdot\phi_{\mathfrak{p}}=\psi_{\mathfrak{p}}\cdot u$ on voit que $\mathrm{ht}\,(\phi_{\mathfrak{p}})=\mathrm{ht}\,(\psi_{\mathfrak{p}})$, ce qui implique que $H(\phi)=H(\psi)$ par le lemme 1.5.

- En comparant les termes de plus bas degré dans l'égalité $u\cdot\phi_T=\psi_T\cdot u$, on obtient que $t^{q^{\mathrm{ht}(u)}}=t$ et en raisonnant comme dans la preuve du lemme 1.5, on obtient les points 3 et 4.

- Enfin, le dernier point est une conséquence immédiate du troisième point.

■

Définition 1.13 : Noyau d'un polynôme tordu :
On considère $u \in \mathbb{K}\{\tau\}$.
On appelle **noyau de** u le noyau de l'application $\mathbb{F}_q$-linéaire $u : \overline{\mathbb{K}} \longrightarrow \overline{\mathbb{K}}$ (c'est-à-dire l'ensemble des racines de $u(x)$ dans $\overline{\mathbb{K}}$ comptées dans multiplicité).

Pour ϕ un module de Drinfeld sur un corps $\mathbb{K}$ et $a \in A \setminus \{0_A\}$, l'ensemble $\mathrm{Ker}\,(\phi_a)$ sera noté $\phi[a]$ et appelé **points de a-torsion de** ϕ. De plus, le polynôme $\mathbb{F}_q$-linéaire $\phi_a(x)$ est appelé **polynôme à a-division de** ϕ (et est à coefficients dans $\mathbb{K}$).

On note également $\mathbb{K}(\phi[a])$ le corps de décomposition de $\phi_a(x)$ que l'on appelle **corps à a-division de** ϕ. Remarquons enfin que si $\mathrm{car}_A(\mathbb{K})$ ne divise pas a, alors $\phi_a(x)$ est séparable (car le degré de $\phi_a(x)$ est $|a|^r$) et donc l'extension $\mathbb{K}(\phi[a])/\mathbb{K}$ est galoisienne et $\mathrm{Card}(\phi[a]) = |a|^r = q^{r\deg(a)}$.

Enfin, si $u : \phi \longrightarrow \psi$ est un morphisme de modules de Drinfeld sur un corps de $\mathbb{K}$, alors u induit un morphisme de A-modules ${}^{\phi}\overline{\mathbb{K}} \longrightarrow {}^{\psi}\overline{\mathbb{K}}$ et donc u envoie $\phi[a]$ sur $\psi[a]$. De manière plus explicite, si $\beta \in \phi[a]$ pour un certain $a \in A$, alors

$$(\psi_a \circ u)(\beta) = (u \circ \phi_a)(\beta) = u(0) = 0$$

d'où $u(\beta) \in \psi[a]$ (en réalité, l'étude des points de torsion des modules de Drinfeld est intimement lié à leurs isogénies).

Exemple 1.9 :
Supposons que $\mathrm{car}_A(\mathbb{K}) = \mathfrak{p} \neq 0$ et posons $d = \deg(\mathfrak{p})$ ainsi que $\pi_{\mathfrak{p}} = \tau^d \in \mathbb{K}\{\tau\}$.
On considère le module de Drinfeld défini sur $\mathbb{K}$ par $\phi_T = t + \sum_{i=1}^{r} g_i\tau^i$ et définissons le module de Drinfeld $\phi^{(\mathfrak{p})}$ de même rang r que ϕ par :

$$\phi_T^{(\mathfrak{p})} = t + \sum_{i=1}^{r} g_i^{q^d}\tau^i.$$

L'application $\pi_{\mathfrak{p}} : \phi \longrightarrow \phi^{\mathfrak{p}}$ est alors une isogénie, appelée **isogénie de Frobenius**, puisque :

$$\pi_{\mathfrak{p}} \cdot \phi_T = \left(t^{q^d} + \sum_{i=1}^{r} g_i^{q^d}\tau^i\right) \cdot \pi_{\mathfrak{p}} = \left(t + \sum_{i=1}^{r} g_i^{q^d}\tau^i\right) \cdot \pi_{\mathfrak{p}} = \phi_T^{(\mathfrak{p})} \cdot \pi_{\mathfrak{p}}.$$

En itérant cette isogénie n-fois, on obtient ainsi $\pi_{\mathfrak{p}^n} : \phi \longrightarrow \phi^{(\mathfrak{p}^n)}$. De plus, en considérant ϕ et ψ deux modules de Drinfeld et $u : \phi \longrightarrow \psi$ une isogénie sur $\mathbb{K}$, on peut décomposer $u = u_{sep}\tau^{q^h}$, où u_{sep} est séparable et $h = \mathrm{ht}(u)$. Par la proposition 1.1, on a que d divise h et donc $\tau^{q^h} = \pi_{\mathfrak{p}}^n$ (avec $n = \frac{h}{d}$) et donc u est la composition des isogénies :

$$\phi \xrightarrow{\pi_{\mathfrak{p}}^n} \phi^{(\mathfrak{p}^n)} \xrightarrow{u_{sep}} \psi$$

Exemple 1.10 :
Posons ϕ le module de Drinfeld défini par $\phi_T := T - \tau$ sur F.
On a que $\phi[T]$ est l'ensemble des racines de $xT - x^q = x\left(T - x^{q-1}\right)$. Or, puisque $\mathbb{F}_q^{\times} \subseteq F$, on obtient que $F(\phi[T]) = F\left(\sqrt[q-1]{T}\right)$ avec $\sqrt[q-1]{T}$ est une racine $(q-1)$-ième de T fixée. Finalement, on a :

$$\mathrm{Gal}(F(\phi[T])/F) \cong \mathbb{F}_q^{\times}.$$

Exemple 1.11 :
Soient $\mathbb{K} := \mathbb{F}_2(y)$ avec y une indéterminée et $\gamma : A \longrightarrow \mathbb{K}$ qui se factorise au travers de $A/(T) \cong \mathbb{F}_2$.
En définissant $\phi_T(x) = yx^2 + x^4$, on trouve que l'extension $K(\phi[T])/K$ est une extension de degré 2 purement inséparable.

Le théorème suivant implique que $\mathrm{Hom}_{K^{sep}}(\phi,\psi)$ contient tous les morphismes $u : \phi \longrightarrow \psi$ définis sur une extension de corps (non nécessairement algébrique) de $\mathbb{K}$:

Théorème 1.2 :
Soient ϕ et ψ deux modules de Drinfeld sur un corps $\mathbb{K}$.
Pour toute extension de corps $\mathbb{L}/\mathbb{K}$ contenant comme sous-corps la clôture séparable de $\mathbb{K}$, on a l'égalité $\mathrm{Hom}_{\mathbb{L}}(\phi,\psi) = \mathrm{Hom}_{K^{sep}}(\phi,\psi)$.

Preuve :
Soit $u \in \mathbb{L}\{\tau\}$ une isogénie de ϕ dans ψ.
Choisissons $a \in A$ non divisible par $\mathrm{car}_A(\mathbb{K})$ et tel que $\mathrm{Card}(\phi[a]) > \deg(u(x))$. Comme $\phi_a(x)$ et $\psi_a(x)$ sont des polynômes séparables, l'extension $\mathbb{K}' = \mathbb{K}(\phi[a],\psi[a])$ de $\mathbb{K}$ est également séparable et puisque u envoie $\phi[a]$ sur $\psi[a]$, il est entièrement déterminé par ses valeurs sur $\phi[a]$ et $u(x)$ est un polynôme dans $\mathbb{K}'[x]$, donc $u \in \mathrm{Hom}_{\mathbb{K}'}(\phi,\psi)$.

■

Afin de simplifier les notations, nous poserons désormais :

$$\mathrm{Hom}(\phi,\psi) := \mathrm{Hom}_{\mathbb{K}^{sep}}(\phi,\psi) = \mathrm{Hom}_{\overline{\mathbb{K}}}(\phi,\psi)$$

$$\mathrm{End}(\phi,\psi) := \mathrm{End}_{\mathbb{K}^{sep}}(\phi,\psi) = \mathrm{End}_{\overline{\mathbb{K}}}(\phi,\psi)$$

$$\mathrm{Aut}(\phi,\psi) := \mathrm{Aut}_{\mathbb{K}^{sep}}(\phi,\psi) = \mathrm{Aut}_{\overline{\mathbb{K}}}(\phi,\psi)$$

Considérons ϕ et ψ deux modules de Drinfeld définis sur un corps $\mathbb{K}$ et $u : \phi \longrightarrow \psi$ une isogénie définie sur une extension de corps de $\mathbb{K}$.
Par le théorème 1.2, u est défini sur $\mathbb{K}^{sep}$ et on observe les faits suivants :

* Pour tout $\beta \in \mathrm{Ker}(u)$ et tout $a \in A$, on a

$$u\left(\phi_a(\beta)\right) = \psi_a(u(\beta)) = \psi_a(0) = 0,$$

  donc $\phi(A)$ envoie $\mathrm{Ker}(u)$ dans lui-même.
* Par la proposition 1.1, on a $\mathrm{ht}(u) = 0$ lorsque $\mathrm{car}_A(\mathbb{K}) = 0$ et $\mathrm{ht}(u)$ est divisible par $\deg(\mathfrak{p})$ dans le cas où $\mathrm{car}_A(\mathbb{K}) = \mathfrak{p} \neq 0$.

Réciproquement, supposons que l'on ait :

* Un module de Drinfeld ϕ défini sur un corps $\mathbb{K}$ et un $\mathbb{F}_q$-espace vectoriel de dimension finie G inclus dans une extension de corps $\mathbb{L}/\mathbb{K}$ qui est invariant sous l'action de ϕ_T (c'est-à-dire que pour tout $\alpha \in G$, $\phi_T(\alpha) \in G$).
* Un entier $h \in \mathbb{N}$ qui est égal à 0 lorsque $\mathrm{car}_A(\mathbb{K}) = 0$ et divisible par $\deg(\mathfrak{p})$ lorsque $\mathrm{car}_A(\mathbb{K}) = \mathfrak{p} \neq 0$.

On souhaiterait construire une isogénie u de ϕ dans un autre module de Drinfeld tel que $\mathrm{Ker}(u) = G$ et $\mathrm{ht}(u) = h$. Pour se faire, on introduit les polynômes $\mathbb{F}_q$-linéaires (cf. lemme 1.3) :

$$w(x) = \prod_{\alpha \in G} (x - \alpha) \text{ et } u(x) = w(x)^{q^h}$$

et on obtient que $\mathrm{Ker}(u) = \mathrm{Ker}(w) = G$.

Proposition 1.2 :
Soit $\mathbb{K}' := \mathbb{K}(G) \subseteq \mathbb{L}$ la plus petite extension de corps de $\mathbb{K}$ dans $\mathbb{L}$ contenant tous les éléments de G.
Il existe deux modules de Drinfeld η et ψ définis sur $\mathbb{K}'$ tels que $w \cdot \phi_T = \eta_T \cdot w$ et $u \cdot \phi_T = \psi_T \cdot u$ (c'est-à-dire que u et w sont des isogénies de ϕ respectivement dans ψ et η).

Preuve :
Remarquons tout d'abord que $w \in \mathbb{K}'\{\tau\}$ et qu'en termes de polynômes dans $\mathbb{K}'\{\tau\}$ on a $u = \tau^h \cdot w$.

* Supposons que l'on ait prouvé l'existence de η donné par $\eta_T := t + \sum_{i=1}^{r} g_i \tau^i \in \mathbb{K}'\{\tau\}$. On pose alors $\psi_T := t + \sum_{i=1}^{r} g_i^{q^h} \tau^i \in \mathbb{K}'\{\tau\}$ et puisque l'on a $t^{q^h} = t$ par hypothèse, on obtient que $\tau^h \cdot \eta_T = \psi_T \cdot \tau^h$. Ainsi, τ^h est une isogénie de η dans ψ et la composition $\phi \xrightarrow{w} \eta \xrightarrow{\tau^h} \psi$ est l'isogénie u.

* Maintenant, pour montrer l'existence de η, on considère $f := w \cdot \phi_T$.
Par hypothèse, on a $\phi_T(\alpha) \in G$ pour tout $\alpha \in G$, d'où $f(\alpha) = w(\phi_T(\alpha)) = 0$. Ainsi G est un sous-ensemble de l'ensemble des racines de f et donc par le corollaire 1.2 on a $f = w \cdot \phi_T = g \cdot w$ pour un certain $g \in \mathbb{K}'\{\tau\}$. Or le terme constant de w est non nul par construction et donc le terme constant de g est égal à t. Finalement, pour avoir le module de Drinfeld η voulu, on pose $\eta_T := g$.

■

Proposition 1.3 :
Soit $u : \phi \longrightarrow \psi$ une isogénie définie sur $\mathbb{K}$.
Il existe une isogénie $\widehat{u} : \psi \longrightarrow \phi$ aussi définie sur $\mathbb{K}$ telle que $\widehat{u} \cdot u = \phi_a$ pour un certain $a \in A$.

Preuve :
Soient $u : \phi \longrightarrow \psi$ une isogénie définie sur $\mathbb{K}$, $\mathfrak{p} = \mathrm{car}_A(\mathbb{K})$ et $h = \mathrm{ht}(u)$.
Si $h \neq 0$, alors $\mathfrak{p} \neq 0$ et $\deg(\mathfrak{p})$ divise h. Dans ce cas, $\phi_{\mathfrak{p}}$ est inséparable et on peut choisir $n \in \mathbb{N}^*$ tel que $\mathrm{ht}\left(\phi_{\mathfrak{p}^n}\right) = nH(\phi)\deg(\mathfrak{p}) \geq h$.

En posant $G := \mathrm{Ker}(u)$, on obtient par ce qui précède que G est invariant par l'action de $\phi(A)$. Or comme G est fini, il existe $b \in A$ non nul tel que ϕ_b s'annule sur G. Donc par le corollaire 1.2, il existe $g \in \mathbb{K}\{\tau\}$ tel que $\phi_{b\mathfrak{p}^n} = g \cdot u$.

Montrons que g définie une isogénie d'un module de Drinfeld ψ dans un autre module de Drinfeld η :
Commençons par remarquer que $\mathrm{ht}(g) = \mathrm{ht}\left(\phi_{b\mathfrak{p}^n}\right) - \mathrm{ht}(u)$ est divisible par $\deg(\mathfrak{p})$. Ainsi, par la proposition 1.2, il suffit de montrer que $\mathrm{Ker}(g)$ est invariant sous l'action de $\psi(A)$.

Soit $\alpha \in \mathrm{Ker}(g)$.
Il existe $\beta \in \overline{\mathbb{K}}$ tel que $u(\beta) = \alpha$ et puisque $\phi_{b\mathfrak{p}^n}(\beta) = g(u(\beta)) = g(\alpha) = 0$, on en déduit que $\beta \in \phi\left[b\mathfrak{p}^n\right]$.

Réciproquement, on voit que si $\beta \in \phi\left[b\mathfrak{p}^n\right]$, alors $u(\beta) \in \mathrm{Ker}(g)$ et ainsi $\mathrm{Ker}(g) = u\left(\phi\left[b\mathfrak{p}^n\right]\right)$ (c'est-à-dire que $\mathrm{Ker}(g)$ est l'image de $\phi\left[b\mathfrak{p}^n\right]$ par u).

De plus, on a

$$g(\psi_T(\alpha)) = g(\psi_T(u(\beta))) = g(u(\phi_T(\beta))) = \phi_{b\mathfrak{p}^n}\left(\phi_T(\beta)\right) = \phi_T\left(\phi_{b\mathfrak{p}^n}(\beta)\right) = \phi_T(0) = 0.$$

Ainsi, on en déduit que $\psi_T(\alpha) \in \mathrm{Ker}(g)$ et donc $\mathrm{Ker}(g)$ est bien invariant par l'action de $\Psi(A)$.

Si l'on montre que $\eta = \phi$, alors on peut prendre $a = b\mathfrak{p}^n$ et $\widehat{u} = g$ pour prouver la proposition. Or, on a

$$g \cdot \psi_T \cdot u = \eta_T \cdot (g \cdot u) = \eta_T \cdot \phi_{b\mathfrak{p}^n}$$

et d'autre part

$$g \cdot \psi_T \cdot u = g \cdot u \cdot \phi_T = \phi_{b\mathfrak{p}^n} \cdot \phi_T = \phi_T \cdot \phi_{b\mathfrak{p}^n}.$$

En combinant ces deux égalités, on obtient que $\eta_T \cdot \phi_{b\mathfrak{p}^n} = \phi_T \cdot \phi_{b\mathfrak{p}^n}$ et donc que $\eta_T = \phi_T$, ce qui nous donne que $\eta = \phi$.

■

Définition 1.14 : Isogénie duale :
On considère $u : \phi \longrightarrow \psi$ une isogénie définie sur $\mathbb{K}$.
On appelle **isogénie duale de** u l'isogénie $\widehat{u}$ définie dans la proposition précédente.

Attention, l'isogénie duale définie ci-dessus n'est pas nécessairement unique ! En effet, en multipliant par exemple $\widehat{u}$ par ϕ_b avec $b \in A \setminus \{0_A\}$ on obtient une autre isogénie duale :

$$\forall c \in A,\ (\phi_b \cdot \widehat{u}) \cdot \psi_c = \phi_b \cdot \phi_c \cdot \widehat{u} = \phi_c \cdot (\phi_b \cdot \widehat{u}) \text{ et } (\phi_b \cdot \widehat{u}) \cdot u = \phi_b \cdot \widehat{u} \cdot u = \phi_{ba}.$$

Cependant, parmi toutes les isogénies duales, on peut en choisir une telle que $\deg_\tau(\widehat{u})$ soit minimal et telle que $\widehat{u} \cdot u = \phi_a$ soit unitaire. Une telle isogénie duale est alors unique.

Le lemme suivant permet de borner le degré de l'isogénie duale :

Lemme 1.7 :
Soit $u : \phi \longrightarrow \psi$ une isogénie définie sur $\mathbb{K}$.
Il existe une isogénie duale $\widehat{u} : \psi \longrightarrow \phi$ telle que $\deg(\widehat{u}) \leq (r-1)\deg(u)$.

Preuve :
Soit $u : \phi \longrightarrow \psi$ une isogénie définie sur $\mathbb{K}$.
Nous utiliserons les notations de la preuve de la proposition précédente.
Choisissons $b \in A_+$ de plus petit degré tel que ϕ_b s'annule sur $G := \mathrm{Ker}(u)$ et posons $n := \frac{\mathrm{ht}(u)}{\deg(\mathfrak{p})}$ (qui est un entier naturel par la proposition 1.1). Ainsi, comme on l'a montré dans la proposition précédente, il existe $\widehat{u}$ tel que

$$\deg_\tau(u) + \deg_\tau(\widehat{u}) = \deg_\tau(\phi_{b\mathfrak{p}^n}) \leq r\left(\deg(b) + \mathrm{ht}(u)\right).$$

De plus, on a par le théorème de structure des A-modules de type fini sur un anneau principal que

$$G \cong \prod_{i=1}^{s} A/(b_i),$$

où les b_i sont unitaires et $b_1|b_2|\cdots|b_s$. On a alors $b = b_s$ et comme $G \subseteq \phi[b]$, on peut montrer que $\phi[b] \subseteq (A/(b))^r$ avec $s \leq r$. On peut alors supposer que $s = r$ en quitte à supposer que certain des b_i sont égaux à 1.

Or, on a également

$$\deg_\tau(u) = \deg_\tau(u_{sep}) + \mathrm{ht}(u)$$

et

$$\deg_\tau(u_{sep}) = \log_q(\mathrm{Card}(G)) = \sum_{i=1}^{r} \deg(b_i).$$

Ainsi :

$$\begin{aligned}\deg_\tau(\widehat{u}) &\leq \sum_{i=1}^{r} (\deg_T(b_r) - \deg_T(b_i)) - (r-1)\,\mathrm{ht}(u) \leq (r-1)\deg_T(b_r) + (r-1)\,\mathrm{ht}(u) \\ &\leq (r-1)\left(\deg_\tau(u_{sep}) + \mathrm{ht}(u)\right) \leq (r-1)\deg_\tau(u)\end{aligned}$$

■

Définition 1.15 : Algèbre des endomorphismes d'un module de Drinfeld :
On considère ϕ un module de Drinfeld sur un corps $\mathbb{K}$.
On appelle **algèbre des endomorphismes de** ϕ l'espace $\mathrm{End}^\circ_{\mathbb{K}}(\phi) := F \otimes_A \mathrm{End}_{\mathbb{K}}(\phi)$.

Remarque :
Puisque $\mathrm{End}_{\mathbb{K}}(\phi)$ est une A-algèbre, $\mathrm{End}^\circ_{\mathbb{K}}(\phi)$ est une F-algèbre.

Corollaire 1.3 :
$\mathrm{End}^{\circ}_{\mathbb{K}}(\phi)$ est une algèbre à division.
En particulier, si $\mathrm{car}_A(\mathbb{K}) = 0$, alors $\mathrm{End}^{\circ}_{\mathbb{K}}(\phi)/F$ est une extension de corps.

Preuve :
Soit $u \in \mathrm{End}^{\circ}_{\mathbb{K}}(\phi)$ un élément non nul.
Chaque élément de $F \otimes_A \mathrm{End}_{\mathbb{K}}(A)$ peut être multiplié par un élément non nul de A pour appartenir à $\mathrm{End}_{\mathbb{K}}(\phi)$.
Ainsi, pour un certain $b \in A$ non nul, on a $bu \in \mathrm{End}_{\mathbb{K}}(\phi)$ non nul.

De plus, par la proposition 1.3, il existe $u' \in \mathrm{End}_{\mathbb{K}}(\phi)$ tel que $u' \cdot (bu) = a \in A \setminus \{0_A\}$. Ainsi, $\left(a^{-1}u'b\right) \cdot u = 1_A$ et de plus peut montrer que l'on a également

$$u\left(a^{-1}u'b\right) = (ub)u'a^{-1} = aa^{-1} = 1_A,$$

donc $a^{-1}u'b$ est l'inverse multiplicatif de u dans $\mathrm{End}^{\circ}_{\mathbb{K}}(\phi)$.

Enfin, si $\mathrm{car}_A(\mathbb{K}) = 0$, alors $\mathrm{End}^{\circ}_{\mathbb{K}}(\phi)$ est commutatif par la proposition 1.1 donc on en déduit que c'est un corps et $\mathrm{End}^{\circ}_{\mathbb{K}}(\phi)/F$ est bien une extension de corps.

■

Corollaire 1.4 :
Soient ϕ et ψ deux modules de Drinfeld sur un corps $\mathbb{K}$.
Il existe un morphisme de A-modules injectif $i : \mathrm{Hom}_{\mathbb{K}}(\phi, \psi) \longrightarrow \mathrm{End}_{\mathbb{K}}(\phi)$ tel que, quand $\mathrm{Hom}_{\mathbb{K}}(\phi, \psi)$ n'est pas réduit à l'application nulle, le quotient $\mathrm{End}_{\mathbb{K}}(\phi)/i(\mathrm{Hom}_{\mathbb{K}}(\phi, \psi))$ est un A-module de torsion.

Preuve :
Soient ϕ et ψ deux modules de Drinfeld sur un corps $\mathbb{K}$.
On peut supposer sans perte de généralités qu'il existe $u \in \mathrm{Hom}_{\mathbb{K}}(\phi, \psi)$ non nul.
L'application

$$\iota : \left| \begin{array}{ccc} \mathrm{Hom}_{\mathbb{K}}(\phi, \psi) & \longrightarrow & \mathrm{End}_{\mathbb{K}}(\phi) \\ w & \longmapsto & \widehat{u} \cdot w \end{array} \right.$$

est l'application injective recherchée.

De plus, l'application

$$\iota' : \left| \begin{array}{ccc} \mathrm{End}_{\mathbb{K}}(\phi) & \longrightarrow & \mathrm{Hom}_{\mathbb{K}}(\phi, \psi) \\ v & \longmapsto & u \cdot v \end{array} \right.$$

est aussi une injection et puisque la composition $\iota' \circ \iota$ correspond à la multiplication par un élément $a := u \cdot \widehat{u} \in A$ non nul sur $\mathrm{Hom}_{\mathbb{K}}(\phi, \psi)$, on en déduit que le quotient est un A-module de torsion.

■

IV Points de torsion

Dans toute cette partie, on considère $\gamma : A \longrightarrow \mathbb{K}$ un A-corps et ϕ un module de Drinfeld sur $\mathbb{K}$ de rang r.

Pour tout $a \in A \setminus \{0_A\}$, on a

$$\phi_a = \gamma(a) + \sum_{i=1}^{n} g_i(a)\tau^i, \ n = r\deg(a).$$

On rappelle également que $\phi[a]$ désigne le $\mathbb{F}_q$-espace vectoriel des racines distinctes de $\phi_a(x)$ et qu'il possède une structure naturelle de A-module via :

$$\forall b \in A, \ \forall \alpha \in \phi[a], \ b \circ \alpha := \phi_b(\alpha).$$

En effet, on a :

$$\phi_a(b \circ \alpha) = \phi_a\left(\phi_b(\alpha)\right) = \phi_b(\phi_a(\alpha)) = \phi_b(0) = 0.$$

Ainsi $\phi[a]$ est un A-module fini et on cherche à s'intéresser à ses diviseurs élémentaires.

Lemme 1.8 :
Soient $a, b \in A$ deux éléments de A premiers entre eux.
En tant que A-modules, on a $\phi[ab] = \phi[a] \times \phi[b]$.

Preuve :
Soient $a, b \in A$ deux éléments de A premiers entre eux.
Puisque ϕ_{ab} s'annule à la fois sur $\phi[a]$ et $\phi[b]$, ce sont donc des sous-modules de $\phi[ab]$. De plus, si $\alpha \in \phi[a] \cap \phi[b]$, alors $\alpha \in \phi[c_1 a + c_2 b]$ pour tout $c_1, c_2 \in A$.

Or, comme a et b sont premiers entre eux, on peut choisir c_1 et c_2 tels que $c_1 a + c_2 b = 1_A$. Ainsi, $\alpha \in \phi[1_A] = \{0_A\}$, donc $\phi[a] \times \phi[b]$ est un sous-module de $\phi[ab]$.

Posons désormais $\mathfrak{p} = \mathrm{car}_A(\mathbb{K})$.
En comparant les cardinaux de $\phi[ab]$ et de son sous-module $\phi[a] \times \phi[b]$, on a :

$$\begin{aligned}
\log_q(\mathrm{Card}(\phi[ab])) &= r\deg(ab) - \mathrm{ht}\,(\phi_{ab}) = r\deg(ab) - H(\phi)\,\mathrm{val}_{\mathfrak{p}}(ab)\deg(\mathfrak{p}) \text{ (par le lemme 1.5)} \\
&= (r\deg(a) - H(\phi)\,\mathrm{val}_{\mathfrak{p}}(a)\deg(\mathfrak{p})) + (r\deg(b) - H(\phi)\,\mathrm{val}_{\mathfrak{p}}(b)\deg(\mathfrak{p})) \\
&= (r\deg(a) - \mathrm{ht}(\phi_a)) + (r\deg(b) - \mathrm{ht}(\phi_b)) \\
&= \log_q(\mathrm{Card}(\phi[a])) + \log_q(\mathrm{Card}(\phi[b])).
\end{aligned}$$

■

Remarque :
On constate que pour tout $\beta \in \mathbb{F}_q^\times$ et tout $a \in A$, on a $\phi[\beta a] = \phi[a]$. Ainsi, pour un idéal non nul $\mathfrak{n}$ de A, on définit $\phi[\mathfrak{n}]$ comme étant les points de torsion de tout générateur de $\mathfrak{n}$ (et par notre convention, on choisit les générateurs unitaires).

Théorème 1.3 :
Soient $\mathfrak{p}$ un idéal premier non nul de A et $n \in \mathbb{N}^*$.

* Si $\mathfrak{p} \neq \mathrm{car}_A(\mathbb{K})$, alors
$$\phi[\mathfrak{p}^n] \cong \prod_{i=1}^{r} A/\mathfrak{p}^n.$$
* Si $\mathfrak{p} = \mathrm{car}_A(\mathbb{K})$, alors
$$\phi[\mathfrak{p}^n] \cong \prod_{i=1}^{r-H(\phi)} A/\mathfrak{p}^n.$$

Preuve :
Soient $\mathfrak{p}$ un idéal premier non nul de A et $n \in \mathbb{N}^*$. Comme $\phi[\mathfrak{p}^n]$ est un A-module de type fini et que A est un anneau principal, on a
$$\phi[\mathfrak{p}^n] \cong \prod_{i=1}^{m} A/\mathfrak{p}_i^{n_i}$$
pour un certain entier naturel m non nul et des puissances strictement positives d'éléments premiers $\mathfrak{p}_i^{n_i}$ (pas forcément distincts). Comme dans le cas de la preuve du lemme précédent, on voit que $\phi[\mathfrak{q}] \cap \phi[\mathfrak{p}^n] = \{0_A\}$ lorsque $\mathfrak{q}$ est un élément premier différent de $\mathfrak{p}$. Ainsi, aucun élément de $\phi[\mathfrak{p}^n]$ n'est annulé par un élément premier $\mathfrak{q}$ différent de $\mathfrak{p}$, ce qui donne que les seuls diviseurs élémentaires dans la décomposition de $\phi[\mathfrak{p}^n]$ sont des puissances de $\mathfrak{p}$:
$$\phi[\mathfrak{p}^n] \cong \prod_{i=1}^{m} A/\mathfrak{p}^{n_i}. \tag{1.4}$$
Puisque $\mathfrak{p}^n$ annule le membre de droite, on doit avoir $n_1, \cdots, n_m \leq n$ et en extrayant le sous-module annulé

par $\mathfrak{p}$ dans chaque membre de (1.4), on a :

$$\phi[\mathfrak{p}] = \prod_{i=1}^{m} A/\mathfrak{p}.$$

Maintenant, en comparant les cardinaux de $\phi[\mathfrak{p}]$ et de $\prod_{i=1}^{m} A/\mathfrak{p}$, on trouve que $m = r - H$ avec $H = 0$ si $\mathfrak{p} \neq \mathrm{car}_A(\mathbb{K})$ et $H = H(\phi)$ sinon.

Finalement, en calculant les cardinaux de chaque membre de (1.4), on a :

$$\log_q\left(\mathrm{Card}\left(\phi\left[\mathfrak{p}^n\right]\right)\right) = n\deg(\mathfrak{p})(r-H).$$

Or on a également :

$$\log_q\left(\mathrm{Card}\left(\prod_{i=1}^{m} A/\mathfrak{p}^{n_i}\right)\right) = \deg(\mathfrak{p})\sum_{i=1}^{r-H} n_i.$$

D'où $\sum_{i=1}^{r-H} n_i = n(r-H)$ et puisque $1 \leq n_1, \ldots, n_m \leq n$, on doit avoir que les n_i sont tous égaux et valent n.

■

Par le lemme 1.8 et le théorème 1.3, on obtient immédiatement le corollaire suivant :

Corollaire 1.5 :
Soit $a \in A$.
Si a n'est pas divisible par $\mathrm{car}_A(\mathbb{K})$, alors

$$\phi[a] \cong \prod_{i=1}^{r} A/(a) = (A/(a))^r.$$

Observons désormais que l'action par $\phi_{\mathfrak{p}}$ donne un morphisme surjectif de $\phi\left[\mathfrak{p}^{n+1}\right]$ dans $\phi\left[\mathfrak{p}^n\right]$ qui est défini par $\alpha \longmapsto \phi_{\mathfrak{p}}(\alpha)$. En prenant la limite inverse de ce système projectif, on obtient la définition suivante :

Définition 1.16 : Module de Tate $\mathfrak{p}$-adique :
On considère $\mathfrak{p}$ un idéal premier non nul de A.
On appelle **module de Tate $\mathfrak{p}$-adique de** ϕ la limite projective :

$$T_{\mathfrak{p}}(\phi) := \varprojlim_{n\in\mathbb{N}^*} \phi\left[\mathfrak{p}^n\right] \cong \begin{cases} \varprojlim_{n\in\mathbb{N}^*} (A/\mathfrak{p}^n)^{\oplus r} \cong A_{\mathfrak{p}}^{\oplus r} & \text{si } \mathfrak{p} \neq \mathrm{car}_A(\mathbb{K}) \\ \varprojlim_{n\in\mathbb{N}^*} (A/\mathfrak{p}^n)^{\oplus (r-H(\phi))} \cong A_{\mathfrak{p}}^{\oplus (r-H(\phi))} & \text{si } \mathfrak{p} = \mathrm{car}_A(\mathbb{K}) \end{cases}$$

Remarque :
La topologie de la limite projective sur $T_{\mathfrak{p}}(\phi)$ est équivalente à la topologie $\mathfrak{p}$-adique et donc $T_{\mathfrak{p}}(\phi)$ est un $A_{\mathfrak{p}}$-module.

Considérons $u : \phi \longrightarrow \psi$ une isogénie de modules de Drinfeld définis sur $\mathbb{K}$.
L'isogénie u induit, pour tout $n \in \mathbb{N}^*$, un morphisme $\phi\left[\mathfrak{p}^n\right] \longrightarrow \psi\left[\mathfrak{p}^n\right]$ et donc induit une application $A_{\mathfrak{p}}$-linéaire

$$u_{\mathfrak{p}} : T_{\mathfrak{p}}(\phi) \longrightarrow T_{\mathfrak{p}}(\psi).$$

On obtient alors un morphisme naturel $\eta : \mathrm{Hom}_{\mathbb{K}}(\phi, \psi) \longrightarrow \mathrm{Hom}_{A_{\mathfrak{p}}}(T_{\mathfrak{p}}(\phi), T_{\mathfrak{p}}(\psi))$ et lorsque $\phi = \psi$, l'application $\eta' : \mathrm{End}_{\mathbb{K}}(\phi) \longrightarrow \mathrm{End}_{A_{\mathfrak{p}}}(T_{\mathfrak{p}}(\phi))$ est un morphisme d'anneaux. De plus, si $\mathfrak{p} \neq \mathrm{car}_A(\mathbb{K})$, alors le morphisme η est injectif puisque si $u_{\mathfrak{p}}$ est l'application nulle, alors $\phi\left[\mathfrak{p}^n\right]$ est un sous-ensemble de $\mathrm{Ker}(u)$ pour tout $n \in \mathbb{N}^*$. Or, $\mathrm{Ker}(u)$ étant de cardinal fixé et $\phi\left[\mathfrak{p}^n\right]$ étant strictement croissant, cela force u à être nul.

Le théorème suivant nous donne que le morphisme η reste injectif après extension à $A_{\mathfrak{p}}$.

Lemme 1.9 :
Soit $a \in A$ non divisible par $\mathrm{car}_A(\mathbb{K})$.
Le morphisme naturel $\mathrm{Hom}_{\mathbb{K}}(\phi, \psi) \otimes_A A/(a) \longrightarrow \mathrm{Hom}_{A/(a)}(\phi[a], \psi[a])$ est injectif.

Preuve :
Soit $a \in A$ non divisible par $\mathrm{car}_A(\mathbb{K})$.
Explicitement, il faut montrer que si $u \in \mathrm{Hom}_{\mathbb{K}}(\phi, \psi)$ induit l'application nulle de $\phi[a]$ dans $\psi[a]$, alors on a $u \in a\,\mathrm{Hom}_{\mathbb{K}}(\phi, \psi)$.

Supposons que $\phi[a]$ est un sous-ensemble de $\mathrm{Ker}(u)$. Par le corollaire 1.2, on a $u = w \cdot \phi_a$ pour un certain $w \in \mathbb{K}\{\tau\}$. On doit alors montrer que $w \in \mathrm{Hom}_{\mathbb{K}}(\phi, \psi)$.

Soit $b \in A$.
On a la relation $u \cdot \phi_b = w \cdot \phi_a \cdot \phi_b = w \cdot \phi_b \cdot \phi_a$ et $u \cdot \phi_b = \psi_b \cdot u = \psi_b \cdot w \cdot \psi_a$. Ainsi, $(w \cdot \phi_b - \psi_b \cdot w) \cdot \phi_a = 0$ et puisque $\mathbb{K}\{\tau\}$ est intègre, on en déduit que $w \cdot \phi_b = \psi_b \cdot w$ et donc $w \in \mathrm{Hom}_{\mathbb{K}}(\phi, \psi)$.

■

Théorème 1.4 :
Soient ψ un module de Drinfeld sur $\mathbb{K}$ et $\mathfrak{p} \neq \mathrm{car}_A(\mathbb{K})$ un idéal premier non nul de A.
L'application

$$\widetilde{\eta} : \left| \begin{array}{ccc} \mathrm{Hom}_{\mathbb{K}}(\phi, \psi) \otimes_A A_{\mathfrak{p}} & \longrightarrow & \mathrm{Hom}_{A_{\mathfrak{p}}}(T_{\mathfrak{p}}(\phi), T_{\mathfrak{p}}(\psi)) \\ u & \longmapsto & u_{\mathfrak{p}} \end{array} \right.$$

est injective.
De plus, le conoyau de ce morphisme est sans torsion.

Preuve :
Soient ψ un module de Drinfeld sur $\mathbb{K}$ et $\mathfrak{p} \neq \mathrm{car}_A(\mathbb{K})$ un idéal premier non nul de A.
Considérons $u \in \mathrm{Hom}_{\mathbb{K}}(\phi, \psi) \otimes_A A_{\mathfrak{p}}$ et supposons que $u_{\mathfrak{p}} = 0$.
L'application u envoie alors $\phi\left[\mathfrak{p}^n\right]$ sur 0 pour tout $n \in \mathbb{N}^*$. Or, on peut montrer que $\mathrm{Hom}_{\mathbb{K}}(\phi, \psi)$ est un A-module libre de rang fini et donc on peut choisir une A-base $(v_1, \cdots, v_s)$ de $\mathrm{Hom}_{\mathbb{K}}(\phi, \psi)$ qui est aussi une $A_{\mathfrak{p}}$-base de $\mathrm{Hom}_{\mathbb{K}}(\phi, \psi) \otimes_A A_{\mathfrak{p}}$.

On peut alors écrire $u = \sum_{i=1}^{s} \alpha_i v_i$ avec $\alpha_1, \cdots, \alpha_s \in A_{\mathfrak{p}}$. De plus, en fixant un entier $n \in \mathbb{N}^*$ et en choisissant des $a_i \in A$ tels que pour tout $i \in [\![1; s]\!]$ on ait $\alpha_i \equiv a_i \ \ [\mathfrak{p}^n]$, on obtient que $u = w + \mathfrak{p}^n v$ avec

$$w = \sum_{i=1}^{s} a_i v_i \in \mathrm{Hom}_{\mathbb{K}}(\phi, \psi) \text{ et } v \in \mathrm{Hom}_{\mathbb{K}}(\phi, \psi) \otimes_A A_{\mathfrak{p}}.$$

On constate alors que $\mathfrak{p}^n v$ envoie $\phi\left[\mathfrak{p}^n\right]$ sur 0 et donc w envoie aussi $\phi\left[\mathfrak{p}^n\right]$ sur 0. Ceci implique que w a pour image 0 lorsque l'on applique l'application de réduction $\mathrm{Hom}_{\mathbb{K}}(\phi, \psi) \longrightarrow \mathrm{Hom}_{A/\mathfrak{p}^n}\left(\phi\left[\mathfrak{p}^n\right], \psi\left[\mathfrak{p}^n\right]\right)$.

De plus, on a le morphisme

$$\mathrm{Hom}_{\mathbb{K}}(\phi, \psi) \otimes_A A/\mathfrak{p}^n \longrightarrow \mathrm{Hom}_{A/\mathfrak{p}^n}\left(\phi\left[\mathfrak{p}^n\right], \psi\left[\mathfrak{p}^n\right]\right)$$

qui est injectif par le lemme 1.9. Ainsi, on a $a_i \equiv 0 \ \ [\mathfrak{p}^n]$ pour tout $i \in [\![1; s]\!]$ et donc $\alpha_i \in \mathfrak{p}^n A_{\mathfrak{p}}$. Enfin, puisque n est quelconque, on en déduit que $\alpha_i = 0$ et donc que $u = 0$.

Finalement, pour démontrer la dernière partie du théorème, on procède de manière similaire (en effet, il y a équivalence entre le fait d'avoir un conoyau sans torsion et le fait qu'une divisibilité dans le codomaine implique une divisibilité dans le domaine) :
Soit $u \in \mathrm{Hom}_{\mathbb{K}}(\phi, \psi) \otimes_A A/\mathfrak{p}^n$ tel que $u_{\mathfrak{p}} = \mathfrak{p} w_{\mathfrak{p}}$ pour un certain $w_{\mathfrak{p}} \in \mathrm{Hom}_{A_{\mathfrak{p}}}\left(T_{\mathfrak{p}}(\phi), T_{\mathfrak{p}}(\psi)\right)$.
L'application $u_{\mathfrak{p}}$ envoie alors $\phi[\mathfrak{p}]$ sur 0 et comme précédemment, cela implique que $\alpha_i \equiv 0 \ \ [\mathfrak{p}]$ pour tout $i \in [\![1; s]\!]$ et donc $u = \mathfrak{p} w$ pour un certain $w \in \mathrm{Hom}_{\mathbb{K}}(\phi, \psi) \otimes_A A_{\mathfrak{p}}$.

■

Considérons $a \in A$ tel que $\mathrm{car}_A(\mathbb{K})$ ne divise pas a.
On rappelle que dans ce cas, $\phi_a(x) \in \mathbb{K}[x]$ est séparable. De plus, le A-module $\phi[a]$ est naturellement muni d'une action provenant du groupe de Galois absolu $G_{\mathbb{K}} := \mathrm{Gal}\left(\mathbb{K}^{sep} / \mathbb{K}\right)$ de $\mathbb{K}$ puisque chaque élément de $G_{\mathbb{K}}$ permute les racines de $\phi_a(x)$. Cette action de $G_{\mathbb{K}}$ commute avec l'action de A sur $\phi[a]$ puisque :

$$\forall \sigma \in G_{\mathbb{K}},\ \forall b \in A,\ \forall \alpha \in \phi[a],\ \phi_b(\sigma(\alpha)) = \sigma(\phi_b(\alpha)).$$

On obtient alors une représentation

$$\rho_{\phi,a} : G_{\mathbb{K}} \longrightarrow \mathrm{Aut}_A(\phi[a]) \cong \mathrm{GL}_r(A/aA)$$

et le groupe de Galois de $\mathbb{K}(\phi[a])/\mathbb{K}$ est isomorphe à $\mathrm{Im}\left(\rho_{\phi,a}\right)$.

Exemple 1.12 :
Considérons $q = 2$ et ϕ le module de Drinfeld défini sur F par $\phi_T = T + \tau + \tau^2$.
$\phi[T]$ est alors l'ensemble des racines de $\phi_T(x) = Tx + x^2 + x^4 = xf(x)$ où $f(x) = x^3 + x + T$. Or, $f(x)$ est irréductible sur F. En effet, il nous suffit de voir si f a des racines dans F et pour cela on applique le critère des racines évidentes qui nous donne que si $x = \frac{P}{Q} \in F$ est une racine de f, alors P divise T et Q divise 1. On a alors $Q = 1$ et ($P = 1$ ou $P = T$). Or on a $f(T) \neq 0$ et $f(1) \neq 0$.
Ainsi, le groupe de Galois de $f(x)$ est un sous-groupe de $\mathfrak{S}_3$ qui agir transitivement sur l'ensemble de ses racines $\{x_1; x_2; x_3\}$ (dans une clôture algébrique), or il n'y a que deux tels sous-groupes : $\mathbb{Z}/3\mathbb{Z}$ et $\mathfrak{S}_3$.

Or, la résolvante quadratique de f est $x^2 + Tx + 1$ qui est irréductible sur F (car le critère des racines évidentes donne que 1 est la seule racine possible mais $f(1) \neq 0$), donc le groupe de Galois de $f(x)$ est le groupe symétrique $\mathfrak{S}_3$ en entier et puisque $\mathfrak{S}_3 \cong \mathrm{GL}_2(\mathbb{F}_2)$, on a :

$$\mathrm{Gal}(F(\phi[T])/F) \cong \mathrm{GL}_2(\mathbb{F}_2) \cong \mathrm{GL}_2(A/TA)$$

et donc $\rho_{\phi,T}$ est surjective.

Soit $\mathfrak{p}$ un idéal premier non nul de A et différent de $\mathrm{car}_A(\mathbb{K})$. L'action de $G_{\mathbb{K}}$ sur chaque $\phi\left[\mathfrak{p}^n\right]$ commute avec l'action de $\phi_{\mathfrak{p}}$ et donc $G_{\mathbb{K}}$ agit sur $T_{\mathfrak{p}}(\phi)$ et cela nous donne une représentation

$$\widehat{\rho_{\phi,\mathfrak{p}}} : G_{\mathbb{K}} \longrightarrow \mathrm{Aut}_{A_{\mathfrak{p}}} T_{\mathfrak{p}}(\phi) \cong \mathrm{GL}_r(A_{\mathfrak{p}}).$$

De plus, étant donné une isogénie $u \in \mathrm{Hom}_{\mathbb{K}}(\phi, \psi)$, on constante que l'application $u_{\mathfrak{p}} : T_{\mathfrak{p}}(\phi) \longrightarrow T_{\mathfrak{p}}(\psi)$ induite par u commute avec l'action de $G_{\mathbb{K}}$, donc l'image de η (défini avant le théorème 1.4) appartient au $A_{\mathfrak{p}}$-sous-module $\mathrm{Hom}_{A_{\mathfrak{p}}}(T_{\mathfrak{p}}(\phi), T_{\mathfrak{p}}(\psi))$ contenant les morphismes de $T_{\mathfrak{p}}(\phi)$ dans $T_{\mathfrak{p}}(\psi)$ qui commutent alors l'action de $G_{\mathbb{K}}$.

Le théorème 1.4 peut être raffiné en ajoutant qu'il y a un morphisme injectif de $\mathrm{Hom}_{\mathbb{K}}(\phi, \psi) \otimes_A A_{\mathfrak{p}}$ dans $\mathrm{Hom}_{A_{\mathfrak{p}}[G_{\mathbb{K}}]}\left(T_{\mathfrak{p}}(\phi), T_{\mathfrak{p}}(\psi)\right)$ dont le conoyau est sans torsion. On notera d'ailleurs que ce même morphisme peut être bijectif (notamment lorsque $\mathbb{K}$ est un corps fini ou une extension finie de F) mais ça n'est pas toujours le cas (par exemple en prenant $\phi = \psi$ sur un corps algébriquement clos avec $\mathrm{End}(\phi) = A$).

Pour finir, on notera qu'étant donné une matrice M de $\mathrm{GL}_r(A)$ ou $\mathrm{GL}_r(A_{\mathfrak{p}})$, on peut réduire ses coefficients modulo $\mathfrak{p}^n$ afin d'obtenir une matrice $\overline{M}$ dans $M_r(A/\mathfrak{p}^n)$. On constate alors que la réduction modulo $\mathfrak{p}^n$ est compatible avec la multiplication et on obtient en réalité le morphisme de réduction modulo $\mathfrak{p}^n$ de $\mathrm{GL}_r(A)$ dans $\mathrm{GL}_r(A/\mathfrak{p}^n)$ (et de même pour $\mathrm{GL}_r(A_{\mathfrak{p}}) \longrightarrow \mathrm{GL}_r(A/\mathfrak{p}^n)$).

V Isomorphismes

Pour conclure ce premier chapitre, on s'intéresse à la classification des modules de Drinfeld à l'isomorphisme près. Ce problème de classification est d'une importance centrale en arithmétique des corps de fonctions car ses solutions sont données par une variété algébrique appelée **variété modulaire de Drinfeld**. Ici, on considère la version la plus simple de ce problème avec la classification des modules de Drinfeld de rang 2 à l'isomorphisme près.

Considérons deux modules de Drinfeld ϕ et ψ sur $\mathbb{K}$.
Une isogénie $u : \phi \longrightarrow \psi$ sur $\mathbb{K}$ est un isomorphisme lorsque u possède un inverse dans $\mathbb{K}\{\tau\}$ (c'est-à-dire qu'il existe $v \in \mathbb{K}\{\tau\}$ tel que $u \cdot v = v \cdot u = 1$). En remarquant que l'on a $\deg_\tau(u \cdot v) = \deg_\tau(u) + \deg_\tau(v) = 0$, on en déduit qu'un isomorphisme de module de Drinfeld $u : \phi \longrightarrow \psi$ sur $\mathbb{K}$ est donné par une constante non nulle $c \in \mathbb{K}$ telle que :

$$c \cdot \phi_T \cdot c^{-1} = \psi_T. \tag{1.5}$$

Or, si l'on a

$$\phi_T := t + \sum_{i=1}^{r} g_i \tau^i \text{ et } \psi_T := t + \sum_{i=1}^{r} h_i \tau^i,$$

alors l'égalité (1.5) est équivalente à :

$$\forall i \in [\![1; r]\!],\ g_i = h_i c^{q^i - 1}. \tag{1.6}$$

On dit alors que ϕ et ψ sont des modules de Drinfeld isomorphes sur une extension de corps $\mathbb{L}$ de $\mathbb{K}$ lorsqu'il existe $c \in \mathbb{L}^\times$ satisfaisant (1.6).

Exemple 1.13 :
Considérons ϕ et ψ deux modules de Drinfeld sur un corps $\mathbb{K}$ de rang 1 et c une racine de $x^{q-1} = \frac{g_1}{h_1}$ (en conservant les notations ci-dessus).
On a $c \cdot \phi_T \cdot c^{-1} = \psi_T$, donc ϕ et ψ sont isomorphes sur $\mathbb{K}\left(\sqrt[q-1]{\frac{g_1}{h_1}}\right)$. Cela implique que, à l'isomorphisme près, le module de Carlitz $C_T = t + \tau$ est le seul module de Drinfeld de rang 1 sur $\mathbb{K}^{\text{sep}}$ (cependant, il est possible que $x^{q-1} = \frac{g_1}{h_1}$ n'ait pas de racines dans $\mathbb{K}$ et donc que ϕ et ψ ne soient pas isomorphes sur $\mathbb{K}$).

Lemme 1.10 :
Soit ϕ un module de Drinfeld de rang r sur $\mathbb{K}$ défini par $\phi_T := t + \sum_{i=1}^{r} g_i \tau^i$.
Si l'on pose $m := \text{PGCD}(\{i \in [\![1; r]\!] \mid g_i \neq 0\})$, alors $\text{Aut}(\phi) \cong \mathbb{F}_{q^m}^\times$.

Preuve :
Soit ϕ un module de Drinfeld de rang r sur $\mathbb{K}$ défini par $\phi_T := t + \sum_{i=1}^{r} g_i \tau^i$.
Posons $m := \text{PGCD}(\{i \in [\![1; r]\!] \mid g_i \neq 0\})$.

- Soit $c \in \text{Aut}(\phi) \subseteq \mathbb{K}^{\text{sep}}$ non nul.
  D'après (1.6), on a $c^{q^i - 1} = 1$ si $g_i \neq 0$. Ainsi pour les $g_i \neq 0$, on a $c \in \mathbb{F}_{q^i}^\times$ et puisque $\mathbb{F}_{q^i} \cap \mathbb{F}_{q^j} = \mathbb{F}_{q^{\text{PGCD}(i,j)}}$, on a $c \in \mathbb{F}_{q^m}^\times$.

- Réciproquement, si $c \in \mathbb{F}_{q^m}^\times$, alors il vérifie (1.6).

Ainsi, on a bien par double inclusion que $\text{Aut}(\phi) \cong \mathbb{F}_{q^m}^\times$.

■

Définition 1.17 : j-invariant d'un module de Drinfeld de rang 2 :
Considérons ϕ un module de Drinfeld de rang 2 défini sur $\mathbb{K}$ par $\phi_T = t + g_1\tau + g_2\tau^2$.
On appelle **j-invariant de** ϕ le rapport $j_\phi := \frac{g_1^{q+1}}{g_2}$.

Remarque :
La terminologie est justifiée par celle employée sur les courbes elliptiques où le j-invariant d'une courbe elliptique permet de déterminer sa classe d'isomorphisme.

Lemme 1.11 :
Deux modules de Drinfeld ϕ et ψ et de rang 2 sont isomorphes sur $\mathbb{K}^{\text{sep}}$ si, et seulement si, $j_\phi = j_\psi$.

Preuve :
Soient ϕ et ψ deux modules de Drinfeld de rang 2.

* Si $c \in \mathbb{K}$ vérifie (1.6), alors :

$$j_\phi = \frac{g_1^{q+1}}{g_2} = \frac{h_1^{q+1} c^{(q-1)(q+1)}}{h_2 c^{q^2-1}} = \frac{h_1^{q+1}}{h_2} = j_\psi,$$

avec $\phi_T := t + g_1\tau + g_2\tau^2$ et $\psi_T := t + h_1\tau + h_2\tau^2$.

* Réciproquement, supposons que $j_\phi = j_\psi$.
  — Si $g_1 = 0$, alors $h_1 = 0$ et dans ce cas, en notant c une racine de $x^{q^2-1} = \frac{g_2}{h_2}$ dans $\mathbb{K}^{\text{sep}}$ on obtient que $c^{-1} \cdot \psi \cdot c = \phi$.

  — Si maintenant $g_1 \neq 0$, alors en notant c une racine de $x^{q-1} = \frac{g_1}{h_1}$ on obtient que $h_1 c^{q-1} = g_1$ et l'égalité $j_\phi = j_\psi$ implique que $\frac{h_1 c^{q^2-1}}{g_2} = \frac{h_1}{h_2}$. Ainsi, on a également que $h_2 c^{q^2-1} = g_2$ et donc la relation (1.6) est vérifiée et finalement ϕ et ψ sont isomorphes.

Finalement, on a bien démontré le résultat par double implication.

■

Remarque :
De même qu'à l'exemple 1.13, deux modules de Drinfeld ϕ et ψ de rang 2 avec $j_\phi = j_\psi$ peuvent ne pas être isomorphes sur $\mathbb{K}$. En effet, en prenant par exemple $\phi_T := t + t\tau^2$ et $\psi_T := t + \tau^2$, alors leur j-invariant est nul mais ils sont isomorphes si, et seulement si, t est une puissance $\left(q^2-1\right)$-ième dans $\mathbb{K}$.

Corollaire 1.6 :
Soit ϕ un module de Drinfeld de rang 2 sur $\mathbb{K}$.
On a la relation :

$$\text{Aut}(\phi) \cong \begin{cases} \mathbb{F}_{q^2}^\times & \text{si } j_\phi = 0 \\ \mathbb{F}_q^\times & \text{si } j_\phi \neq 0 \end{cases}$$

Preuve :
Soit ϕ un module de Drinfeld de rang 2 sur $\mathbb{K}$ défini par $\phi_T := t + g_1\tau + g_2\tau^2$.

* Si $j_\phi = 0$, alors on a $g_1 = 0$ et donc $\text{PGCD}(i \in [\![1;2]\!] \mid g_i \neq 2) = \text{PGCD}(2) = 2$, d'où par le lemme 1.10, on a $\text{Aut}(\phi) \cong \mathbb{F}_{q^2}^\times$.

* Si $j_\phi \neq 0$, alors on a $g_1 \neq 0$ et donc $\text{PGCD}(i \in [\![1;2]\!] \mid g_i \neq 2) = \text{PGCD}(1,2) = 1$, d'où par le lemme 1.10, on a $\text{Aut}(\phi) \cong \mathbb{F}_q^\times$.

■

Remarques :

* Pour tout $j \in \mathbb{K}$, il y a un module de Drinfeld de rang 2 défini sur $\mathbb{F}_q(t,j)$ dont le j-invariant est j. En effet, $\phi_T := t + \tau^2$ a un j-invariant nul et pour $j \in \mathbb{K}^\times$, $\phi_T = t + \tau + j^{-1}\tau^2$ a pour j-invariant j.
* Il est possible de classifier les modules de Drinfeld de rang $r > 2$ via cette fois-ci un j-invariant qui est un $(r-1)$-uplet mais cela dépasse notre cadre d'étude et nous nous contenterons du résultat pour des modules de Drinfeld de rang 2.

Chapitre 2

Séries dans un corps complet non archimédien

Ce deuxième chapitre est consacré à l'étude des séries dans le cas d'un corps non archimédien $\mathbb{K}$. Dans la partie I on donne les généralités sur les séries en parlant de convergence et de substitution formelle. Dans la partie II on donne les théorèmes de préparation et de factorisation de Weierstrass ainsi que d'autres résultats qui seront utiles pour la proposition 2.3 de la partie suivante. Enfin dans la partie III on parle de séries additives et on introduit l'exponentielle de Drinfeld-Carlitz pour un $\mathbb{F}_q$-sous-espace vectoriel de $\mathbb{C}_\mathbb{K}$.

Dans tout ce chapitre, on considère $\mathbb{K}$ un corps complet pour une valeur absolue non archimédienne non triviale notée $|\cdot|$ et on suppose que $\mathbb{F}_q$ est un sous-corps de $\mathbb{K}$.

Nous utiliserons les notations suivantes dans ce chapitre :

- $\mathcal{R} := \{x \in \mathbb{K} \mid |x| \leq 1\}$ est l'anneau des entiers de $\mathbb{K}$.
- $\mathcal{M} := \{x \in \mathbb{K} \mid |x < 1\}$ est l'idéal maximal de $\mathcal{R}$.
- $k := \mathcal{R}/\mathcal{M}$ est le corps résiduel de $\mathcal{R}$.
- $\mathbb{C}_\mathbb{K}$ est la complétion d'une clôture algébrique de $\mathbb{K}$ par rapport à une unique extension de la valeur absolue de $\mathbb{K}$ à $\overline{\mathbb{K}}$ (et qui sera encore notée $|\cdot|$).
- $\mathcal{B}_o(a,r) := \{z \in \mathbb{C}_\mathbb{K} \mid |z-a| < r\}$.
- $\mathcal{B}_f(a,r) := \{z \in \mathbb{C}_\mathbb{K} \mid |z-a| \leq r\}$.
- Pour $q > 1$, on note $v : \mathbb{K}^\times \longrightarrow \mathcal{R}$ la valuation définie par $v(x) := -\log_q(|x|)$.

I Généralités sur les séries dans un corps complet pour une valeur absolue non archimédienne non triviale

I.1 Convergence

Ici, nous utilisons les séries formelles pour définir des fonctions sur $\mathbb{K}$. Plus précisément, étant donnée une série $f(x) := \sum_{n\geq 0} a_n x^n \in \mathbb{K}[[x]]$, on la définit sur $\mathbb{K}$ comme une fonction dont le domaine de définition est l'ensemble des $\alpha \in \mathbb{K}$ tels que la série $f(\alpha) = \sum_{n\geq 0} a_n \alpha^n$ converge.

On rappelle le lemme suivant dont une preuve est donnée à la page 106 de [Pap23] :

Lemme 2.1 :
Soit $\sum_{n\geq 0} a_n$ une série sur $\mathbb{K}$.
La série $\sum_{n\geq 0} a_n$ converge si, et seulement si, $\lim_{n\to+\infty} |a_n| = 0$.

De plus, en cas de convergence on a :

$$\left|\sum_{n=0}^{+\infty} a_n\right| \leq \max_{n\in\mathbb{N}} |a_n|.$$

Remarque :
Ici, le fait que la norme soit non archimédienne est crucial. En effet, le lemme est faux dans le cas contraire puisque, par exemple dans $\mathbb{R}$, la série $\sum_{n\geq 1} \frac{1}{n}$ diverge bien que son terme général tende vers 0 quand n tend vers $+\infty$.

Lemme 2.2 :
Soient $\sum_{n\geq 0} a_n$ et $\sum_{m\geq 0} b_m$ deux séries sur $\mathbb{K}$.
Si les séries $\sum_{n\geq 0} a_n$ et $\sum_{m\geq 0} b_m$ convergent, alors la série de terme général $c_t := \sum_{k=0}^{t} a_k b_{n-k}$ converge et on a :

$$\left(\sum_{n=0}^{+\infty} a_n\right)\left(\sum_{m=0}^{+\infty} b_m\right) = \sum_{t=0}^{+\infty} c_t.$$

Preuve :
Soient $\sum_{n\geq 0} a_n$ et $\sum_{m\geq 0} b_m$ deux séries sur $\mathbb{K}$ que l'on suppose convergentes.
En notant respectivement A la somme de la première série, B celle de la seconde ainsi que $(A_m)_{m\in\mathbb{N}}$ et $(B_m)_{m\in\mathbb{N}}$ respectivement la suite des sommes partielles de la première série et de la seconde série, on a $(A_m)_{m\in\mathbb{N}}$ qui converge vers A et $(B_m)_{m\in\mathbb{N}}$ qui converge vers B et ainsi $(A_m B_m)_{m\in\mathbb{N}}$ converge vers AB.

Le problème est que l'on a pas $\sum_{n=0}^{m} c_n \neq A_m B_m$. Pour montrer la convergence et l'égalité voulue, il va nous falloir estimer la différence. Or, on a :

$$\forall m \in \mathbb{N},\ A_m B_m = \sum_{n=0}^{m}\sum_{k=0}^{m} a_n b_k \text{ et } \sum_{\ell=0}^{m} c_\ell = \sum_{\ell=0}^{m}\sum_{n+k=\ell} a_n b_k.$$

La première somme portant sur les $a_n b_k$ avec $0 \leq n, k \leq m$ et la seconde sur les $a_n b_k$ avec $n + k \leq m$, leur différence est donc la somme sur les $a_n b_k$ avec $0 \leq n, k \leq m$ et $n + k > m$. Ainsi, on remarque que ni n ni k ne sont nuls et que l'on a $\max(n, k) > \frac{m}{2}$, on peut donc séparer la différence en deux de sorte à avoir :

$$\forall m \in \mathbb{N},\ A_m B_m - \sum_{\ell=0}^{m} c_\ell = \sum_{\substack{0<n,k\leq m \\ n>\frac{m}{2} \\ n+k>m}} a_n b_k + \sum_{\substack{0<n,k\leq m \\ k>\frac{m}{2} \\ n+k>m}} a_n b_k.$$

Fixons nous un $\varepsilon > 0$.
Les suites $(a_n)_{n\in\mathbb{N}}$ et $(b_k)_{k\in\mathbb{N}}$ tendent vers 0, on peut donc choisir un entier $m \in \mathbb{N}$ tel que pour tous entiers $n, k > \frac{m}{2}$ on ait $0 \leq |a_n|, |b_k| \leq \varepsilon$.

Ainsi, pour chaque terme de la première somme on a $|a_n b_k| \leq \varepsilon \max_{k\in\mathbb{N}} |b_k|$ et pour chaque terme de la seconde somme on a $|a_n b_k| \leq \varepsilon \max_{n\in\mathbb{N}} |a_n|$. Par l'inégalité ultramétrique, on a alors

$$\left|A_m B_m - \sum_{\ell=0}^{m} c_\ell\right| \leq \varepsilon \left(\max_{n\in\mathbb{N}} |a_n| + \max_{k\in\mathbb{N}} |b_k|\right).$$

Finalement, la série $\sum_{\ell\geq 0} c_\ell$ est convergente (car sa suite des sommes partielles a la même limite que la suite $(A_m b_m)_{m\in\mathbb{N}}$) et on a

$$\left(\sum_{n=0}^{+\infty} a_n\right)\left(\sum_{m=0}^{+\infty} b_m\right) = \sum_{t=0}^{+\infty} c_t.$$

■

Remarques :

* Contrairement au cas classique où la convergence absolue des deux séries est exigée (ou juste une seule dans le cas du théorème de Mertens), ici la convergence des deux séries implique la convergence du produit de Cauchy.
* Il existe également d'autres résultats analogues tels que le réarrangement de termes ou la sommation de séries doubles.

Corollaire 2.1 :
Soient $f(x), g(x) \in \mathbb{K}[[x]]$ et $\alpha \in \mathbb{K}$.
Si $f(x)$ et $g(x)$ convergent en α, alors leur produit $h(x) := f(x)g(x) \in \mathbb{K}[[x]]$ converge et on a $h(\alpha) = f(\alpha)g(\alpha)$.

Preuve :
Soient $f(x), g(x) \in \mathbb{K}[[x]]$ et $\alpha \in \mathbb{K}$ tels que $f(x)$ et $g(x)$ convergent en α.
Le produit $h(x) := f(x)g(x) \in \mathbb{K}[[x]]$ est le produit de Cauchy de $f(x)$ et $g(x)$ et il converge en α par le lemme 2.2 et par ce même lemme on a également que $h(\alpha) = f(\alpha)g(\alpha)$.

■

Définition 2.1 : Rayon de convergence :
On considère $f(x) := \sum_{n\geq 0} a_n x^n \in \mathbb{K}[[x]]$.
On appelle **rayon de convergence de** $f(x)$ et on le note $\rho(f)$ la valeur

$$\rho(f) := \frac{1}{\overline{\lim}_{n\to+\infty} \sqrt[n]{|a_n|}}$$

avec les conventions usuelles utilisées dans le cas de $\mathbb{C}$.

Remarques :

* La définition donnée ici du rayon de convergence correspond à la règle d'Hadamard dans le cas classique des séries entières sur $\mathbb{C}$.
* On peut également définir le rayon de convergence par la formule $\log_q(\rho(f)) := \overline{\lim}_{n\to+\infty} \frac{v(a_n)}{n}$.

Définition 2.2 : Série entière :
On considère une série $f(x) := \sum_{n\geq 0} a_n x^n \in \mathbb{K}[[x]]$.
On dit que $f(x)$ est **entière** lorsque $\rho(f) = +\infty$.

Lemme 2.3 :
Soient $f(x) := \sum_{n\geq 0} a_n x^n \in \mathbb{K}[[x]]$ et $\alpha \in \mathbb{K}$.
La série $f(x)$ converge en α lorsque $|\alpha| < \rho(f)$ et diverge lorsque $|\alpha| > \rho(f)$.

Preuve :
Soient $f(x) := \sum_{n\geq 0} a_n x^n \in \mathbb{K}[[x]]$ et $\alpha \in \mathbb{K}$.
Par le lemme 2.1, la série $f(\alpha) = \sum_{n\geq 0} a_n \alpha^n$ converge si, et seulement si, on a

$$\lim_{n\to+\infty} |a_n \alpha^n| = \lim_{n\to+\infty} \left(|\alpha| \sqrt[n]{|a_n|}\right)^n = 0.$$

* Si $|\alpha| > \rho(f)$, alors on a $\frac{1}{\alpha} < \frac{1}{\rho(f)} = \overline{\lim}_{n\to+\infty} \sqrt[n]{a_n}$. Ainsi, on a $\frac{1}{\alpha} < \sqrt[n]{|a_n|}$ infiniment souvent, c'est-à-dire $|\alpha_n|\alpha^n > 1$ infiniment souvent. Ainsi, $f(\alpha)$ ne converge pas.

* Si $|\alpha| < \rho(f)$, alors on a $\frac{1}{\alpha} > \frac{1}{\rho(f)} = \overline{\lim}_{n\to+\infty} \sqrt[n]{a_n}$. Ainsi, il existe $\varepsilon \in]0;1[$ et $N \in \mathbb{N}$ tels que pour tout $n \geq N$ on ait $1 - \varepsilon > |\alpha| \sqrt[n]{|a_n|}$. Par conséquent, on obtient que

$$\forall n \in \mathbb{N},\ 0 \leq |a_n \alpha^n| \leq (1-\varepsilon)^n \underset{n\to+\infty}{\longrightarrow} 0$$

et donc $f(\alpha)$ converge par le lemme 2.1.

■

Par le lemme 2.3, on obtient que $f(x)$ définie une fonction $z \longmapsto f(z)$ du disque ouvert $\{z \in \mathbb{K} \mid |z| < \rho(f)\}$ dans $\mathbb{K}$.

Exemple 2.1 :

* Pour $f(x) := \sum_{n\geq 0} x^n$, on a $\rho(f) = 1$ et de plus $f(\alpha)$ ne converge pas pour tout $\alpha \in \mathbb{K}$ de norme 1.
* Fixons nous $\pi \in \mathcal{M}$ non nul et considérons la série $g(x) := \sum_{n\geq 0} \pi^n x^{n^2}$.
  Puisque $|\pi| \in]0;1[$, on a $\frac{1}{\rho(g)} = \overline{\lim}_{n\to+\infty} |\pi|^{\frac{n}{n^2}} = 1$ et donc $\rho(g) = 1$. De plus, $g(\alpha)$ converge pour tout $\alpha \in \mathbb{K}$ de norme 1.

Remarque :
Plus généralement, la série $f(x)$ converge en α de norme $\rho(f)$ si, et seulement si, $\lim_{n\to+\infty} |a_n|\rho(f)^n = 0$.

Lemme 2.4 :
Soit $u(x) \in \mathcal{R}[[x]]^\times$.
La série $u(\alpha)$ converge et ne s'annule pas pour tout $\alpha \in \mathbb{C}_\mathbb{K}$ tel que $|\alpha| < 1$.

Preuve :
Soit $u(x) \in \mathcal{R}[[x]]^\times$.
Puisque les coefficients de $u(x)$ sont dans $\mathcal{R}$, on a $\rho(f) \geq 1$ et donc $u(\alpha)$ converge pour tout $\alpha \in \mathbb{C}_\mathbb{K}$ tel que $|\alpha| < 1$.

De plus $u(x)$ est inversible dans $\mathcal{R}[[x]]$ et on a le même résultat pour $u(x)^{-1}$ et par le corollaire 2.1 on a $u(\alpha)u(\alpha)^{-1} = 1$ et ainsi $u(\alpha) \neq 0$.

■

I.2 Substitution formelle

Dans toute cette sous-partie, on se fixe R un anneau commutatif.

Pour les mêmes raisons que l'on ne peut généralement pas évaluer $f(x) := \sum_{n\geq 0} a_n x^n \in R[[x]]$ en tout $a \in R$, on ne peut pas substituer $g(x) \in R[[x]]$ dans $f(x)$ si $g(x)$ a un terme constant non nul. Cependant, lorsque $g(x)$ a un terme constant nul, on a

$$f(g(x)) = \sum_{n\geq 0} a_n g(x)^n$$

qui est définie puisque pour tout $m \in \mathbb{N}$, les m premiers coefficients de $f(g(x))$ coïncide avec les m premiers coefficients de $\sum_{n=0}^{m} a_n g(x)^n$. On note alors $f \circ g$ cette substitution dans $R[[x]]$.

Lemme 2.5 :
Soient $f \in R[[x]]$ et $g, h \in xR[[x]]$.
On a $(f \circ g) \circ h = f \circ (g \circ h)$.

Preuve :
Soient $f \in R[[x]]$ et $g, h \in xR[[x]]$.
Remarquons tout d'abord que pour tout $n \in \mathbb{N}$ on a $(x^n \circ g) \circ h = g^n \circ h$ et pour tous $g_1, g_2 \in xR[[x]]$ on a $(g_1 g_2) \circ h = (g_1 \circ h)(g_2 \circ h)$. Ainsi, pour tout $n \in \mathbb{N}$, on a $(x^n \circ g) \circ h = g^n \circ h = (g \circ h)^n$ et donc en notant $f(x) := \sum_{n\geq 0} a_n x^n$, on a

$$(f \circ g) \circ h = \sum_{n\geq 0} a_n (g \circ h)^n = f \circ (g \circ h).$$

■

Par le lemme 2.5 ci-dessus, la substitution dans $xR[[x]]$ est une opération binaire associative et de plus :

$$\forall f, g, h \in xR[[x]],\ (f+g)\circ h = f\circ h + g\circ h$$

et x est l'élément neutre pour la loi $\circ$ (cependant la loi $\circ$ n'est pas commutative et $f\circ(g+h)$ n'est pas égal à $f\circ g + f\circ h$ en général).

Lemme 2.6 :
Soit $f := \sum_{n\geq 1} a_n x^n \in xR[[x]]$.
Il existe $g \in xR[[x]]$ tel que $f\circ g = x$ si, et seulement si, $a_1 \in R^\times$. Dans ce cas, g est unique et on a également $g\circ f = x$.
En particulier, si R est un corps, alors les éléments de $xR[[x]]$ dont le premier coefficient est non nul forment un groupe pour la substitution qui est non abélien.

Preuve :
Soit $f := \sum_{n\geq 1} a_n x^n \in xR[[x]]$.
En notant $g := \sum_{n\geq 1} b_n x^n$ et en développant formellement $f\circ g := \sum_{n\geq 1} c_n x^n$, on constate que

$$c_1 = a_1 b_1 \text{ et } \forall n \in \mathbb{N}^*,\ c_n = a_1 b_n + (\text{polynôme en } a_2, \dots, a_n \text{ et } b_1, \dots, b_{n-1}).$$

On souhaite donc avoir $c_1 = 1$ et les $c_n = 0$ pour $n \geq 1$. Pour cela, on remarque qu'on peut résoudre les équations précédentes dont les inconnues sont les b_n si, et seulement si, a_1 est inversible dans R.

De plus, cette solution est unique par construction et comme $b_1 = a_1^{-1}$ est inversible, on lui applique ce qui précède et donc il existe un unique $h \in xR[[x]]$ tel que $g\circ h = x$ et enfin on a :

$$h = x\circ h = (f\circ g)\circ h = f\circ(g\circ h) = f\circ x = f.$$

Enfin, dans le cas particulier où R est un corps, tout élément non nul est inversible et par le premier point de la preuve ainsi que le petit paragraphe précédent ce lemme, on a bien que les éléments de $xR[[x]]$ dont le premier coefficient est non nul forment un groupe pour la substitution qui est non abélien.

■

Revenons désormais dans le cadre de la sous-partie I.1 et intéressons nous à la convergence des substitutions dans $\mathbb{K}[[x]]$.

Considérons deux séries formelles $f(x)$ et $g(x)$ avec $g(0) = 0$ telles que $(f\circ g)(x)$ est bien définie et supposons qu'il existe $\alpha \in \mathbb{K}$ tel que $g(\alpha)$ converge et notons $\beta := g(\alpha)$ cette limite et supposons également que $f(x)$ converge en β.

Une question basique est de voir si $(f\circ g)(\alpha)$ converge et si c'est le cas, de regarder si l'on a $(f\circ g)(\alpha) = f(g(\alpha))$. Il s'agit ici en réalité d'une question subtile et la réponse est négative en général comme le montre l'exemple suivant :

Exemple 2.2 :
Considérons $f(x) := \sum_{n\geq 1} a_n x^n \in \mathbb{K}[[x]]$ telle que $a_1 = 1$.
Par le lemme 2.6, il existe $g(x) \in x\,\mathbb{K}[[x]]$ tel que $(f\circ g)(x) = x$ et supposons qu'il existe $\alpha \in \mathbb{K}$ une racine non nulle de g. On a alors $g(\alpha) = 0$ et $f(0) = 0$ mais $(f\circ g)(\alpha) = \alpha \neq 0 = f(g(\alpha))$.

Lemme 2.7 :
Soient $f(x) \in \mathbb{K}[x]$ et $g(x) \in x\,\mathbb{K}[[x]]$.
$(f\circ g)(x)$ converge sur $\mathcal{B}_o(0, \rho(g))$ et pour tout $\alpha \in \mathcal{B}_o(0, \rho(g))$ on a $(f\circ g)(\alpha) = f(g(\alpha))$.

Preuve :
Soient $f(x) \in \mathbb{K}[x]$ et $g(x) \in x\,\mathbb{K}[[x]]$.
En notant $f(x) := \sum_{k=0}^{n} a_k x^k$, on a $(f\circ g)(x) = \sum_{k=0}^{n} a_k g(x)^k$ qui est une somme finie et par linéarité, il suffit de montrer le résultat pour $f(x) = x^n$.

Or, dans ce cas, on a $(f \circ g)(x) = g(x)^n$ et par le corollaire 2.1, $(f \circ g)(x)$ converge sur $\mathcal{B}_o(0, \rho(g))$ (puisque $g(x)$ converge sur $\mathcal{B}_o(0, \rho(g))$) et on a $(f \circ g)(x) = g(x)^n = f(g(x))$.

■

On admet le théorème suivant qui utilise quelques outils techniques (mais dont on pourra en trouver une preuve à la page 295 de [Rob00]).

Théorème 2.1 :
Soient $f(x) := \sum_{n\geq 0} a_n x^n$, $g(x) := \sum_{n\geq 1} b_n x^n \in R[[x]]$ et $\alpha \in \mathbb{C}_{\mathbb{K}}$.
Si $|\alpha| < \rho(g)$ et $\max_{n\in\mathbb{N}} |b_n \alpha^n| < \rho(f)$, alors $(f \circ g)(\alpha)$ et $f(g(\alpha))$ convergent et $(f \circ g)(\alpha) = f(g(\alpha))$.

Corollaire 2.2 :
Soient $f(x) := \sum_{n\geq 0} a_n x^n, g(x) := \sum_{n\geq 1} b_n x^n \in \mathbb{K}[[x]]$.
Si l'une de ces séries est entière et que l'autre est polynomiale, alors pour tout $\alpha \in \mathbb{C}_{\mathbb{K}}$ on a $(f \circ g)(\alpha) = f(g(\alpha))$.

Preuve :
Soient $f(x) := \sum_{n\geq 0} a_n x^n, g(x) := \sum_{n\geq 1} b_n x^n \in \mathbb{K}[[x]]$.
Raisonnons par disjonction de cas :

* Supposons que $f(x)$ soit polynomiale et $g(x)$ entière.
  On a $\rho(f) = \rho(g) = +\infty$ et par le lemme 2.7 on obtient que $(f \circ g)(x)$ converge sur $\mathbb{C}_{\mathbb{K}}$ pour tout $\alpha \in \mathbb{C}_{\mathbb{K}}$ on a $(f \circ g)(\alpha) = f(g(\alpha))$.

* Supposons que $f(x)$ soit entière et $g(x)$ polynomiale.
  On a $\rho(f) = \rho(g) = +\infty$ et par le théorème 2.1 on obtient que $(f \circ g)(x)$ converge sur $\mathbb{C}_{\mathbb{K}}$ pour tout $\alpha \in \mathbb{C}_{\mathbb{K}}$ on a $(f \circ g)(\alpha) = f(g(\alpha))$.

■

II Théorèmes de préparation et de factorisation de Weierstrass

Le but de cette partie est de donner des résultats (et notamment les théorèmes de préparation et de factorisation de Weierstrass) qui nous seront utiles dans la partie III.

II.1 Théorème de préparation de Weierstrass

Le but de cette sous-partie est de donner (sans démonstration) le théorème de préparation de Weierstrass et qui est une analogue de la version "classique" d'analyse complexe dans le cas non archimédien.

Définition 2.3 : Polynôme distingué :
Un polynôme $\sum_{n=0}^{d} a_n x^n \in \mathcal{R}[x]$ est un **polynôme distingué** lorsque $a_0, \ldots, a_{d-1} \in \mathcal{M}$ et $a_d = 1$.

On donne désormais le résultat technique suivant dont on admet la preuve (qui utilise les polygones de Newton) mais dont on pourra en trouver une à la page 110 de [Pap23].

Théorème 2.2 : Théorème de préparation de Weierstrass :
Soit $f(x) := \sum_{n\geq 0} a_n x^n \in \mathcal{R}[[x]]$.
S'il existe $d \in \mathbb{N}$ tel que $a_0, \ldots, a_{d-1} \in \mathcal{M}$ et $a_d \in \mathcal{R}^\times$, alors il existe $u(x) \in \mathcal{R}[[x]]^\times$ et un polynôme distingué $g(x) \in \mathcal{R}[x]$ de degré d tels que $f(x) = u(x)g(x)$.
De plus, $u(x)$ et $g(x)$ avec ces propriétés sont uniquement déterminées par $f(x)$.

II.2 Théorème de factorisation de Weierstrass

En analyse complexe, le théorème de factorisation de Weierstrass nous donne que toute fonction entière peut-être représenté comme un produit (potentiellement infini) impliquant ses zéros (et qui peut être vu comme une "extension" du théorème fondamental de l'algèbre). De plus, toute suite qui tend vers $+\infty$ possède une fonction

entière associée avec des zéros en des points précis de la suite. Ici, nous donnons un analogue de ce théorème dans le cas non archimédien.

Définition 2.4 : Multiplicité d'un zéro :
On considère $a \in \mathbb{C}_{\mathbb{K}}$ et $f(x) \in \mathbb{C}_{\mathbb{K}}[[x]]$.
On dit que α est un **zéro de multiplicité** $m \in \mathbb{N}^*$ lorsqu'il existe $g(x) \in \mathbb{C}_{\mathbb{K}}[[x]]$ tel que $f(x) = (x-\alpha)^m g(x)$, $g(x)$ convergeant en α et $g(\alpha) \neq 0$.

Proposition 2.1 :
Soit $f(x) \in \mathbb{K}[[x]]$.
Si $f(x)$ est entière et non constante, alors :

* $f(x)$ a au moins un zéro dans $\mathbb{C}_{\mathbb{K}}$;
* Les zéros de $f(x)$ sont algébriques sur $\mathbb{K}$;
* Le nombre de zéros de $f(x)$ dans $\mathcal{B}_f(0,r)$ est fini pour tout $r > 0$;
* La fonction $f : \mathbb{C}_{\mathbb{K}} \longrightarrow \mathbb{C}_{\mathbb{K}}$ qui à α associe $f(\alpha)$ est surjective.

Preuve :
Soit $f(x) := \sum_{n\geq 0} a_n x^n \in \mathbb{K}[[x]]$ entière et non constante et posons $d := \min\{m \in \mathbb{N} \mid \forall n \in \mathbb{N},\ |a_n| \leq |a_m|\}$.

* Remarquons que $f_c(x) := f(cx) = \sum_{n\geq 0} a_n c^n x^n$ est entière pour tout $c \in \mathbb{K}$, donc après éventuellement un remplacement de $f(x)$ par $f_c(x)$ pour un c bien choisi, on peut supposer que $d \geq 1$ et $\rho(f) < 1$. Ainsi, en remplaçant $f(x)$ par $a_d^{-1} f(x)$, on peut supposer que $f(x)$ vérifie les hypothèses du théorème 2.2. Il existe donc $u(x) \in \mathcal{R}[[x]]^\times$ et un polynôme distingué $g(x) \in \mathcal{R}[x]$ de degré d tels que $f(x) = u(x)g(x)$. Par le lemme 2.4, $u(x)$ n'a pas de zéros dans $\mathcal{B}_o(0,1)$ et donc les zéros de $f(x)$ sont exactement les zéros du polynôme $g(x)$. Enfin, puisque les zéros de $g(x)$ sont algébriques sur $\mathbb{K}$, on obtient les trois premiers points de la proposition (puisque $\mathbb{C}_{\mathbb{K}}$ est algébriquement clos et $g(x)$ est un polynôme).

* Pour démontrer le dernier point, on considère $\beta \in \mathbb{C}_{\mathbb{K}}$ et on applique le premier point démontré ci-dessus à $f(x) - \beta$ (qui est encore une fonction entière) pour obtenir l'existence de $\alpha \in \mathbb{C}_{\mathbb{K}}$ tel que $f(\alpha) = \beta$ et donc la surjectivité de f de $\mathbb{C}_{\mathbb{K}}$ dans $\mathbb{C}_{\mathbb{K}}$.

■

Définition 2.5 : Ensemble (faiblement) discret :
On considère V un $\mathbb{K}$-espace vectoriel muni d'une norme $\|\cdot\|$.
Un sous-ensemble S de V est dit

* **faiblement discret** lorsque S est discret pour la topologie de V (c'est-à-dire que tout point de S a un voisinage qui ne contient aucun autre point de S) ;
* **discret** lorsque $\{v \in S \mid \|v\| < r\}$ est fini pour tout $r > 0$.

Grâce à cette définition, on peut définir un sous-ensemble faiblement discret (respectivement discret) S de $\mathbb{C}_{\mathbb{K}}$ comme étant faiblement discret (respectivement discret) en considérant $\mathbb{C}_{\mathbb{K}}$ comme un espace vectoriel sur $\mathbb{K}$ et dont la norme est la valeur absolue sur $\mathbb{C}_{\mathbb{K}}$.

Remarque :
Un ensemble discret est faiblement discret mais la réciproque est fausse. En effet, on considérant $\mathbb{K} = \mathbb{F}_q((T))$ on a $S = \overline{\mathbb{F}_q}$ qui est faiblement discret dans $\mathbb{C}_{\mathbb{K}}$ puisque $|\alpha - \beta| = 1$ pour tous $\alpha, \beta \in \overline{\mathbb{F}_q}$ distincts mais S n'est pas discret puisque $S \subseteq \mathcal{B}_f(0,1)$.

Considérons désormais $f(x) \in \mathbb{C}_{\mathbb{K}}[[x]]$ une fonction entière et α un zéro de $f(x)$ dans $\mathbb{C}_{\mathbb{K}}$.
On peut écrire $f(x) = (x-\alpha)^{c_\alpha} g(x)$ où $g(\alpha) \neq 0$ et $c_\alpha \in \mathbb{N}^*$ est la multiplicité de α. De plus, en posant

$$Z(f) := \{(\alpha, c_\alpha) \in \mathbb{C}_{\mathbb{K}} \times \mathbb{N}^*\} \subseteq \mathbb{C}_{\mathbb{K}} \times \mathbb{N}^*$$

l'ensemble des zéros de f comptés avec multiplicité, la proposition 2.1 implique que la projection de $Z(f)$ sur $\mathbb{C}_{\mathbb{K}}$ est discrète.

Nous allons montrer que $Z(f)$ détermine complètement (à une constante multiplicative près) $f(x)$ et que de plus $f(x)$ a une décomposition sur ses zéros qui est similaire à la décomposition des polynômes grâce à leurs racines. Ceci permet d'obtenir une classification complète des fonctions entières sur $\mathbb{C}_{\mathbb{K}}$.

Soit $S \subseteq \mathbb{C}_{\mathbb{K}}$ un ensemble.
Pour tout $\alpha \in S$ on assigne un entier naturel c_α que l'on appelle la multiplicité de α et on pose

$$Z := \{(\alpha, c_\alpha) \in \mathbb{C}_{\mathbb{K}} \times \mathbb{N}^*\} \subseteq \mathbb{C}_{\mathbb{K}} \times \mathbb{N}^*$$

que l'on considère comme un multiensemble de $\mathbb{C}_{\mathbb{K}}$ (c'est-à-dire un ensemble d'éléments de S mais qui apparaissent c_α fois). De plus, si S est discret dans $\mathbb{C}_{\mathbb{K}}$, alors Z l'est également.

Supposons que Z soit discret dans $\mathbb{C}_{\mathbb{K}}$ et définissons

$$f_Z(x) := x^{c_0} \prod_{\alpha \in Z \setminus \{0_{\mathbb{C}_{\mathbb{K}}}\}} \left(1 - \frac{x}{\alpha}\right) = x^{c_0} \prod_{\alpha \in S \setminus \{0_{\mathbb{C}_{\mathbb{K}}}\}} \left(1 - \frac{x}{\alpha}\right)^{c_\alpha},$$

où c_0 est la multiplicité de $0_{\mathbb{C}_{\mathbb{K}}}$ si $0_{\mathbb{C}_{\mathbb{K}}} \in S$ et vaut 0 sinon.
En développant $f_Z(x)$ en série, on trouve que

$$f_Z(x) = x^{c_0} \sum_{n \geq 0} (-1)^n G_n x^n,$$

où

$$G_n := \sum_{\substack{\alpha_1, \ldots, \alpha_n \in Z \\ \alpha_1, \ldots, \alpha_n \neq 0}} \frac{1}{\prod_{i=1}^n \alpha_i}.$$

Il est clair que Z est dénombrable car on peut énumérer ses éléments en énumérant le nombre d'éléments contenus dans des disques de rayon entier croissants. On énumère donc $Z := \{\beta_i\}_{i \in I}$ de sorte que les β_i soient rangés par ordre croissants pour la valeur absolue $|\cdot|$. Puisque S est discret et que les multiplicité c_α sont finis, on a

$$\left| \prod_{j=1}^n \beta_{i_j} \right| \underset{\max\{i_1, \ldots, i_n\} \to +\infty}{\longrightarrow} +\infty.$$

Ainsi, les séries G_n convergent et on peut considérer $f_Z(x)$ comme une série sur $\mathbb{C}_{\mathbb{K}}$ et l'ordre dans lequel on additionne les éléments dans les séries G_n n'impacte pas sa somme (on peut montrer plus généralement tout réarrangement d'une série convergente dans $\mathbb{K}$ converge encore dans $\mathbb{K}$ et la valeur de la somme est inchangée).

Proposition 2.2 :
Avec les notations et hypothèses ci-dessus, $f_Z(x)$ est une fonction entière et l'ensemble de ses zéros est Z.

Preuve :

* Tout d'abord, on obtient par le lemme 2.1 que

$$\forall n \in \mathbb{N},\ |G_n| \leq \frac{1}{\prod_{i=1}^n |\beta_i|}.$$

Soient $z \in \mathbb{C}_{\mathbb{K}}$ et $\varepsilon \in]0;1[$.
Puisque S est discret, il existe un entier naturel N tel que pour tout entier naturel $i \geq N$ on ait $\frac{|z|}{|\beta_i|} \leq \varepsilon$.
Ainsi, pour tout entier naturel $n \geq N$, on a $|G_n z^n| \leq c\varepsilon^{n-N}$, avec c une constante positive indépendante de n.
On a donc $(|G_n z^n|)_{n \in \mathbb{N}}$ qui tend vers 0 quand n tend vers $+\infty$, donc $f_Z(x)$ converge en z et ainsi $f_Z(x)$ est entière.

* Pour prouver que $Z(f_Z) = Z$, il suffit de montrer que $Z \cap (\mathcal{B}_f(0,r) \times \mathbb{N}^*)$ est l'ensemble des zéros de f_Z dans $\mathcal{B}_f(0,r)$, comptés avec multiplicité, pour tout $r > 0$.

Or, il suffit de montrer que

$$h(x) := \prod_{\substack{\alpha\in S\\ |\alpha|>r}} \left(1-\frac{x}{\alpha}\right)^{c_\alpha}$$

n'a pas de zéros dans $\mathcal{B}_f(0,r)$. Ce qui est bien le cas en appliquant le lemme 2.4 à $u(x) := h(\beta x)$ pour tout $\beta \in \mathbb{C}_{\mathbb{K}}^{\times}$ tel que $|\beta| = r$.

■

Théorème 2.3 : Théorème de factorisation de Weierstrass :
Soit $f(x) \in \mathbb{C}_{\mathbb{K}}[[x]]$.
Si $f(x)$ est entière, alors il existe $\beta \in \mathbb{C}_{\mathbb{K}}^{\times}$ tel que

$$f(x) = \beta x^{c_0} \prod_{\alpha\in Z(f)\setminus\{0_{\mathbb{C}_{\mathbb{K}}}\}} \left(1-\frac{x}{\alpha}\right),$$

où c_0 est la multiplicité de $0_{\mathbb{C}_{\mathbb{K}}}$ dans $Z(f)$.
De plus, à une constante près, $f(x)$ est entièrement déterminé le multiensemble de ses zéros.

Preuve :
Soit $f(x) \in \mathbb{C}_{\mathbb{K}}[[x]]$ entière.
Nous avons déjà montré que $Z := Z(f)$ est discret et par la proposition 2.2, la fonction f_Z est entière et Z est le multiensemble de ses zéros.

Montrons que $f(x) = \beta f_Z(x)$ pour un certain $\beta \in \mathbb{C}_{\mathbb{K}}^{\times}$:
Puisque $f(x) = x^{c_0}\widetilde{f}(x)$, avec $\widetilde{f}(x)$ entière et $0 \notin Z(\widetilde{f})$, en considérant $\widetilde{f}(x)$ au lieu de $f(x)$ si nécessaire, on peut supposer que $0 \notin Z(f)$ et donc que le terme constant de $f(x)$ est non nul.

Dans ce cas, $f(x)$ a un inverse $f(x)^{-1}$ dans $\mathbb{C}_{\mathbb{K}}[[x]]$ et on considère $h(x) := f_Z(x)f(x)^{-1} \in \mathbb{C}_{\mathbb{K}}[[x]]$. La fonction $h(x)$ est entière et n'a pas de zéros dans $\mathbb{C}_{\mathbb{K}}$. En effet, pour montrer cela, il suffit de montrer que $h(x)$ converge sur $\mathcal{B}_f(0,r)$ et qu'elle n'a pas de zéros dans ce disque pour tout $r > 0$.

Soit $r > 0$.
En choisissant (si nécessaire) $c \in \mathbb{C}_{\mathbb{K}}^{\times}$ tel que $|c| > r$ et en remplaçant $h(x)$ par $h(cx)$, on peut supposer que $\rho(h) < 1$ (remarquons au passage que $f_c(x) := f(cx)$ est entière et $f_{Z(f_c)}(x) = f_Z(cx)$). De plus, puisque les coefficients de la série $f(x)$ tendent vers 0, quitte à remplacer $f(x)$ par $c'f(x)$ pour un $c' \in \mathbb{C}_{\mathbb{K}}$ bien choisi, on peut supposer que tous les coefficients de $f(x)$ ont une valeur absolue inférieure ou égale à 1.
En utilisant le théorème 2.2 de préparation de Weierstrass, il existe $u(x) := 1 + \sum_{n\geq 1} u_n x^n \in \mathcal{R}[[x]]^{\times}$ avec les u_i de valeur absolue inférieure ou égale à 1 (et sans zéros dans $\mathcal{B}_f(0,r)$ par le lemme 2.4) et $g(x) \in \mathcal{R}[x]$ de degré d et entière tels que $f(x) = g(x)u(x)$. Ainsi, les zéros de $f(x)$ dans $\mathcal{B}_f(0,r)$ sont exactement les zéros de $g(x)$.
En déterminant les coefficients de $u(x)^{-1}$ récursivement, on a $u(x)^{-1} = 1 + \sum_{n\geq 1} w_n x^n$ avec les w_i de valeur absolue inférieure ou égale à 1. Ainsi, $u(x)^{-1}$ converge dans $\mathcal{B}_f(0,r)$ et n'a pas de zéros dans ce disque. Par construction, $\frac{f_Z(x)}{g(x)}$ est entière et n'a pas de zéros dans $\mathcal{B}_f(0,r)$.
Finalement, on en déduit que $h(x) = \frac{f_Z(x)}{g(x)}u(x)^{-1}$ converge et n'a pas de zéros dans $\mathcal{B}_f(0,r)$.

Enfin, puisque $h(x)$ et entière et n'a pas de zéros dans $\mathbb{C}_{\mathbb{K}}$, on en déduit par la proposition 2.1 que $h(x)$ est constante et vaut β et par conséquent, $f(x) = \beta f_Z(x)$.

■

III Théorie analytique de base sur les modules de Drinfeld : séries entières additives

Le but de cette partie est d'utiliser les notions et résultats établis dans les parties I et II dans le cadre des modules de Drinfeld.

Dans toute cette partie, on considère R une $\mathbb{F}_q$-algèbre commutative et on note $R\langle\langle x\rangle\rangle$ l'ensemble des séries de la forme $f(x) := \sum_{n\geq 0} a_n x^{q^n}$ avec les a_n qui sont des éléments de R.

Pour ces séries, de même que pour les polynômes additifs, on a

$$\forall f, g, h \in R\langle\langle x\rangle\rangle,\ f \circ (g+h) = f \circ g + f \circ h.$$

Ainsi, $(R\langle\langle x\rangle\rangle, +, \circ)$ est un anneau non commutatif (par les résultats de la sous-partie I.2).

Définition 2.6 : Série $\mathbb{F}_q$-linéaire :
Une série $f(x) \in R\langle\langle x\rangle\rangle$ est une **série $\mathbb{F}_q$-linéaire** lorsqu'elle vérifie les conditions :
- $f(x+y) = f(x) + f(y)$;
- $\forall \alpha \in \mathbb{F}_q,\ f(\alpha x) = \alpha f(x)$.

De plus, il sera parfois plus avantageux de travailler avec l'anneau des séries tordues noté

$$R\{\{\tau\}\} := \left\{ \sum_{n\geq 0} a_n \tau^n,\ (a_n)_{n\in\mathbb{N}} \in R^{\mathbb{N}} \right\}$$

dont la loi d'addition $+$ et de multiplication $\cdot$ sont respectivement données par

$$\sum_{n\geq 0} a_n \tau^n + \sum_{n\geq 0} b_n \tau^n = \sum_{n\geq 0} (a_n + b_n)\tau^n$$

et

$$\left(\sum_{n\geq 0} a_n \tau^n\right) \cdot \left(\sum_{n\geq 0} b_n \tau^n\right) = \sum_{n\geq 0} \left(\sum_{i=0}^{n} a_i b_{n-i}^{q^i}\right) \tau^n.$$

Enfin, $R\{\{\tau\}\}$ qui est isomorphe à $R\langle\langle x\rangle\rangle$ en tant qu'anneau via l'isomorphisme d'anneaux

$$\iota : \left| \begin{array}{ccc} (R\{\{\tau\}\}, +, \cdot) & \longrightarrow & (R\langle\langle x\rangle\rangle, +, \circ) \\ \sum_{n\geq 0} a_n \tau^n & \longmapsto & \sum_{n\geq 0} a_n x^{q^n} \end{array} \right. .$$

On donne le lemme suivant dont la preuve est similaire à celle du lemme 2.6 :

Lemme 2.8 :
Soit $f := \sum_{n\geq 0} a_n \tau^n \in R\{\{\tau\}\}$.
f est inversible dans $R\{\{\tau\}\}$ si, et seulement si, $a_0 \in R^\times$.

Pour la suite de cette partie, on cherche à s'intéresser aux séries additives sur des corps complets non archimédiens de caractéristique positive.

Définition 2.7 : Exponentielle de Drinfeld-Carlitz :
On considère Λ un $\mathbb{F}_q$-sous-espace vectoriel discret de $\mathbb{C}_\mathbb{K}$.
On appelle **exponentielle de Drinfeld-Carlitz de** Λ la fonction $e_\Lambda(x) := x \prod_{\lambda\in\Lambda\setminus\{0_{\mathbb{C}_\mathbb{K}}\}} \left(1 - \frac{x}{\lambda}\right)$.

Proposition 2.3 :
Soit Λ un $\mathbb{F}_q$-sous-espace vectoriel discret de $\mathbb{C}_{\mathbb{K}}$.

* $e_\Lambda(x)$ est une fonction entière ;
* $e_\Lambda(x) \in \mathbb{C}_{\mathbb{K}}\langle\langle x\rangle\rangle$;
* Si $f(x) := \sum_{n\geq 0} a_n x^n \in \mathbb{C}_{\mathbb{K}}\langle\langle x\rangle\rangle$ est entière et $a_0 \neq 0$, alors tous les zéros de f sont simples et l'ensemble $Z(f) \subseteq \mathbb{C}_{\mathbb{K}}$ est un $\mathbb{F}_q$-sous-espace vectoriel discret de $\mathbb{C}_{\mathbb{K}}$ et on a $f(x) = a_0 e_{Z(f)}(x)$.
  De plus, si $f(x)$ est défini sur $\mathbb{K}$, alors $Z(f) \subseteq \mathbb{K}^{sep}$ et $Z(f)$ est $\mathrm{Gal}_{\mathbb{K}}$-invariante.

Preuve :
Soit Λ un $\mathbb{F}_q$-sous-espace vectoriel discret de $\mathbb{C}_{\mathbb{K}}$.

* Le fait que $e_\Lambda(x)$ est une fonction entière est un cas particulier de la proposition 2.2.

* Soient $n \in \mathbb{N}^*$ et $\Lambda_n := \{\lambda \in \Lambda \mid |\lambda| \leq n\}$.
  L'inégalité ultramétrique donne que Λ_n est un $\mathbb{F}_q$-sous-espace vectoriel de $\mathbb{C}_{\mathbb{K}}$ de dimension fini. De plus, en posant
  $$e_{\Lambda_n}(x) := x \prod_{\lambda\in\Lambda_n\setminus\{0_{\mathbb{C}_{\mathbb{K}}}\}} \left(1 - \frac{x}{\lambda}\right) = \sum_{i=1}^{m} e_i(\Lambda_n) x^i,$$
  avec $m = \mathrm{Card}(\Lambda_n)$ et en développant $e_\Lambda(x) := \sum_{i\geq 0} e_i(\Lambda) x^i$, on trouve que :
  $$\forall i \in \mathbb{N},\ \lim_{n\to+\infty} e_i(\Lambda_n) = e_i(\Lambda).$$
  De plus, par les lemmes 1.1 et 1.3, $e_{\Lambda_n}(x)$ est un polynôme $\mathbb{F}_q$-linéaire et donc $e_i(\Lambda_n) = 0$ sauf éventuellement lorsque i est une puissance de q. Ainsi, la même chose s'applique aux coefficients de $e_\Lambda(x)$ et donc $e_\Lambda(x) \in \mathbb{C}_{\mathbb{K}}\langle\langle x\rangle\rangle$.

* Nous avons déjà montré dans la preuve du théorème 2.3 que le multiensemble des zéros $Z := Z(f)$ de f est discret et que
  $$f(x) = a_0 x \prod_{\lambda\in Z\setminus\{0_{\mathbb{C}_{\mathbb{K}}}\}} \left(1 - \frac{x}{\lambda}\right).$$
  Posons $Z_n := \{\lambda \in Z \mid |\lambda| \leq n\}$ et $f_n(x) := \prod_{\lambda\in Z_n\setminus\{0_{\mathbb{C}_{\mathbb{K}}}\}} \left(1 - \frac{x}{\lambda}\right)$.
  Comme dans le point précédent, les coefficients de $f_n(x) := \sum_{m\geq 1} a_{n,m} x^m$ convergent vers les coefficients de $f(x)$ lorsque n tend vers $+\infty$.
  De plus, pour tout $m \in \mathbb{N}$, il existe un entier naturel N tel que pour tout $n > N$ on ait $|a_m| = |a_{n,m}|$ (car Z est discret). S'il existe $\lambda \in Z$ de multiplicité strictement supérieure à 1, alors les polynômes $f_n(x)$ ne peuvent être $\mathbb{F}_q$-linéaires pour n assez grand puisqu'un polynôme $\mathbb{F}_q$-linéaire avec un premier coefficient non nul est séparable. Ceci implique donc que $a_m \neq 0$ pour un certain m qui n'est pas une puissance de q et ce qui contredit le fait que $f(x) \in \mathbb{C}_{\mathbb{K}}\langle\langle x\rangle\rangle$.
  Ainsi, chaque zéro de $f(x)$ est de multiplicité 1 et tous les $f_n(x)$ sont $\mathbb{F}_q$-linéaires et puisque les racines d'un polynôme $\mathbb{F}_q$-linéaire forment un $\mathbb{F}_q$-sous-espace vectoriel de $\mathbb{C}_{\mathbb{K}}$, on en déduit que Z est un $\mathbb{F}_q$-sous-espace vectoriel discret de $\mathbb{C}_{\mathbb{K}}$.

  Enfin, supposons que $f(x)$ est défini sur $\mathbb{K}$.
  En utilisant la proposition 2.1 et sa preuve, on observe que chaque $\lambda \in Z$ est une racine d'un polynôme $g(x) \in \mathbb{K}[x]$, toutes les racines de $g(x)$ sont dans Z et $g(x)$ est séparable puisque chaque élément de Z a pour multiplicité 1. Par conséquent, on a $Z \subseteq K^{sep}$ et Z est $\mathrm{Gal}_{\mathbb{K}}$-invariant.

■

Chapitre 3

Modules de Drinfeld sur des corps locaux

L'objectif de ce deuxième chapitre est de donner des résultats sur les modules de Drinfeld dans le cas d'un corps $\mathbb{K}$ complet pour une valuation discrète. Plus précisément, on suppose que $\mathbb{K}$ est une extension finie de $F_{\mathfrak{p}}$ où $\mathfrak{p}$ est un idéal non nul de A et on le munit d'une structure de A-corps via les inclusions naturelles :

$$\gamma : A \hookrightarrow F \hookrightarrow F_{\mathfrak{p}} \hookrightarrow \mathbb{K}\,.$$

Dans la partie I nous introduirons la notion de réduction de modules de Drinfeld qui sera centrale dans la partie B puis dans la partie II nous parlerons de l'uniformisation de Tate qui sera utilisée dans une preuve de la sous-partie III.2 du chapitre 4.

Nous utiliserons les notations suivantes dans ce chapitre :

- v est la valuation pour laquelle $\mathbb{K}$ est complet et on la normalise de sorte que $v\left(\mathbb{K}^{\times}\right) = \mathbb{Z}$.
- $\mathcal{R} := \{x \in \mathbb{K} \mid v(x) \geq 0\}$ est l'anneau des entiers de $\mathbb{K}$.
- $\mathcal{M} := \{x \in \mathbb{K} \mid v(x) > 0\}$ est l'idéal maximal de $\mathcal{R}$.
- π est une uniformisante de $\mathcal{R}$ (on a alors en particulier $\mathcal{M} = \pi\mathcal{R}$).
- $k := \mathcal{R}/\mathcal{M}$ est le corps résiduel de $\mathcal{R}$.
- $|\alpha| = \mathrm{Card}(k)^{-v(\alpha)}$ est la valeur absolue normalisée de $\mathbb{K}$ associée à la valuation v.
- $\mathbb{C}_{\mathbb{K}}$ est la complétion d'une clôture algébrique de $\mathbb{K}$ par rapport à une unique extension de la valeur absolue de $\mathbb{K}$ à $\overline{\mathbb{K}}$ (et qui sera encore notée $|\cdot|$).
- On notera par $\overline{x}$ la réduction modulo $\mathcal{M}$ de $x \in \mathcal{R}$.
- On remarque que $\mathfrak{p} = A \cap \mathcal{M}$ et $v(\mathfrak{p}) = e\left(\mathbb{K}\,/F_{\mathfrak{p}}\right)$ est l'indice de ramification de l'extension $\mathbb{K}\,/F_{\mathfrak{p}}$.

I Réduction de modules de Drinfeld

L'objectif de cette partie sera d'introduire la réduction d'un module de Drinfeld modulo $\mathcal{M}$. On verra que via cette opération, la théorie des modules de Drinfeld sur k a une incidence sur la théorie des modules de Drinfeld sur $\mathbb{K}$.

Dans toute cette première partie, on considère $\phi : A \longrightarrow \mathbb{K}\{\tau\}$ un module de Drinfeld de rang r défini par $\phi_T := T + \sum_{i=1}^{r} g_i\tau^i$.

Définition 3.1 : Module de Drinfeld défini sur $\mathcal{R}$:
On dit que ϕ est un **module de Drinfeld défini sur** $\mathcal{R}$ lorsque pour tout $a \in A$ on a $\phi_a \in \mathcal{R}\{\tau\}$.

Lemme 3.1 :
Les assertions suivantes sont équivalentes :

- ϕ est défini sur $\mathcal{R}$;
- $\phi_T \in \mathcal{R}\{\tau\}$;
- $\phi_a \in \mathcal{R}\{\tau\}$ pour un certain $a \in A$ tel que $\deg(a) \geq 1$.

Preuve :
Les deux premiers points sont équivalents par la définition 3.1 et le fait que ϕ_T défini entièrement ϕ et le deuxième point implique le troisième. Il nous suffit donc de montrer que le troisième point implique le deuxième.

Raisonnons par contraposée en supposant que $\phi_T \notin \mathcal{R}\{\tau\}$:
En notant $m \in [\![1; r]\!]$ le plus grand indice pour lequel $v(g_m) < 0$ puis en utilisant le fait que $\phi_{T^n} = \phi_T \cdot \phi_{T^{n-1}}$ et une récurrence, on obtient que le plus grand indice d'un coefficient de ϕ_{T^n} avec une valuation négative est $m + (n-1)r$ et la valuation en question vaut $q^{r(n-1)}v(g_m)$.

Considérons désormais un polynôme $a \in A$ de degré $n \geq 1$ que l'on écrit $a := \sum_{i=0}^{n} a_i T^i$.
Puisque l'on a $\phi_a := \sum_{i=0}^{n} a_i \phi_{T^i}$, on obtient que le $(m-(n-1)r)$-ième coefficient de ϕ_a a pour valuation $q^{r(n-1)}v(g_m) < 0$ et donc $\phi_a \notin \mathcal{R}\{\tau\}$.

■

Remarquons qu'il est toujours possible de trouver un module de Drinfeld ψ isomorphe à ϕ et qui est défini sur $\mathcal{R}$. En effet, il est possible de choisir $c \in \mathbb{K}^\times$ tel que pour tout $i \in [\![1; r]\!]$ on ait $\left(q^i - 1\right) v(c) + v(g_i) \geq 0$. Ainsi, le module de Drinfeld ψ défini par :

$$\psi_T := c^{-1} \cdot \phi_T \cdot c = T + \sum_{i=1}^{r} c^{q^i - 1} g_i \tau^i \in \mathcal{R}\{\tau\}$$

est bien un module de Drinfeld défini sur $\mathcal{R}$ et isomorphe à ϕ.

En réduisant désormais les coefficients de ψ modulo $\mathcal{M}$ on obtient un morphisme $\overline{\psi} : A \longrightarrow k\{\tau\}$. Le problème qui se pose alors est que $\overline{\psi}$ peut être un module de Drinfeld de rang strictement inférieur à r ou pire encore : ne pas être un module de Drinfeld du tout si $\overline{\psi}(A) \subseteq k$ par exemple.

Exemple 3.1 :
Considérons le module de Drinfeld ϕ défini par $\phi_T := T + \frac{1}{\pi}\tau + \tau^2$.
Pour que les coefficients de $\psi := c^{-1} \cdot \phi \cdot c$ soient dans $\mathcal{R}$, il nous faut choisir c tel que $v(c) \geq 1$. En effet, dans ce cas on a $\psi_T = T + \frac{c^{q-1}}{\pi}\tau + c^{q^2-1}\tau^2$.

Cependant, on constate que $v\left(c^{q^2-1}\right) > 0$ et donc $\overline{\psi}$ n'est jamais un module de Drinfeld de rang 2. De plus, si $q > 2$, alors $v\left(\frac{c^{q-1}}{\pi}\right) > 0$ et donc $\overline{\psi}$ n'est même jamais un module de Drinfeld !

Définition 3.2 : Stable/bonne réduction d'un module de Drinfeld :
On dit que ϕ a une :

- **réduction stable sur** $\mathbb{K}$ lorsqu'il existe $c \in \mathbb{K}^\times$ tel que $\psi := c^{-1} \cdot \phi \cdot c$ est défini sur $\mathcal{R}$ et $\overline{\psi}$ est un module de Drinfeld ;
- **bonne réduction sur** $\mathbb{K}$ lorsqu'il existe $c \in \mathbb{K}^\times$ tel que $\psi := c^{-1} \cdot \phi \cdot c$ est défini sur $\mathcal{R}$ et $\overline{\psi}$ est un module de Drinfeld de rang r.

Définition 3.3 : Potentiellement stable/bonne réduction d'un module de Drinfeld :
On dit que ϕ a une :

- **potentielle réduction stable sur** $\mathbb{K}$ lorsque ϕ a une réduction stable en tant que module de Drinfeld sur une extension $\mathbb{L}$ de $\mathbb{K}$;
- **potentielle bonne réduction sur** $\mathbb{K}$ lorsque ϕ a une bonne réduction en tant que module de Drinfeld sur une extension $\mathbb{L}$ de $\mathbb{K}$.

Remarque :
Dans le cas où $r = 1$, les notions de réduction stable et de bonne réduction coïncident. De plus, lorsque ϕ n'a pas de bonne réduction, on dira qu'elle a une **mauvaise réduction**.

Dans toute la suite de cette partie, on considère :

$$e(\phi) := \min\left(\left\{\frac{v(g_i)}{q^i-1},\ i \in [\![1;r]\!]\right\}\right) \text{ et } r'(\phi) := \max\left(\left\{i \in [\![1;r]\!] \;\middle|\; e(\phi) = \frac{v(g_i)}{q^i-1}\right\}\right).$$

Lemme 3.2 :
Soit $\mathbb{L}/\mathbb{K}$ une extension de corps.

- ϕ a une réduction stable sur $\mathbb{L}$ si, et seulement si, $e(\phi) \in v(\mathbb{L})$;
- Si ϕ a une réduction stable sur $\mathbb{L}$ et qu'il existe $c \in \mathbb{L}^\times$ tel que $\overline{\psi} := \overline{c^{-1} \cdot \phi \cdot c}$ soit un module de Drinfeld, alors le rang de $\overline{\psi}$ est $r'(\phi)$.

Preuve :
Soit $\mathbb{L}/\mathbb{K}$ une extension de corps.

- On constate que ϕ a une réduction stable sur $\mathbb{L}$ si, et seulement si, il existe $c \in \mathbb{L}^\times$ tel que $e\left(c^{-1} \cdot \phi \cdot c\right) = 0$.
  Or, on a également :
  $$e\left(c^{-1} \cdot \phi \cdot c\right) = e(\phi) + v(c),$$
  d'où ϕ a une réduction stable sur $\mathbb{L}$ si, et seulement si, il existe $c \in \mathbb{L}^\times$ tel que $e(\phi) = -v(c)$, c'est-à-dire $e(\phi) \in v(\mathbb{L})$.

- Supposons que ϕ a une réduction stable sur $\mathbb{L}$ et qu'il existe $c \in \mathbb{L}^\times$ tel que $\overline{\psi} := \overline{c^{-1} \cdot \phi \cdot c}$ soit un module de Drinfeld.
  On a $e(\psi) = 0$ et donc le rang du module de Drinfeld $\overline{\psi}$ est le plus grand entier $i \in [\![1;r]\!]$ tel que $v(g_i) = 0$, ce qui correspond exactement à $r'(\phi)$.

■

Par le lemme ci-dessus ainsi que sa preuve, on obtient directement la proposition suivante :

Proposition 3.1 :

- ϕ a une réduction stable sur une extension de corps $\mathbb{L}/\mathbb{K}$ totalement modérément ramifiée de degré égal au dénominateur de la fraction réduite $e(\phi)$;
- Toute réduction stable de ϕ est de rang $r'(\phi)$.
  En particulier, ce rang ne dépend pas de l'extension $\mathbb{L}/\mathbb{K}$ sur laquelle ϕ acquière une réduction stable ;
- ϕ a une potentielle bonne réduction si, et seulement si, pour un certain $a \in A$ de degré non nul on a
  $$\forall i \in [\![1;n]\!],\ \frac{v\left(g_n(a)\right)}{q^n-1} \leq \frac{v\left(g_i(a)\right)}{q^i-1},$$
  où $\phi_a := \gamma(a) + \sum_{i=1}^{n} g_i(a)\tau^i$.

Désormais, on étudie les réductions d'isogénies entre modules de Drinfeld.

Soient ϕ et ψ deux modules de Drinfeld sur $\mathbb{K}$, $\alpha, \beta \in \mathbb{K}^\times$ et $u : \phi \longrightarrow \psi$ une isogénie.
Commençons par la simple observation que $\beta \cdot u \cdot \alpha^{-1} : \alpha \cdot \phi \cdot \alpha^{-1} \longrightarrow \beta \cdot \psi \cdot \beta^{-1}$ est encore une isogénie. Ainsi, on a l'isomorphisme

$$\mathrm{Hom}_{\mathbb{K}}(\phi, \psi) \cong \mathrm{Hom}_{\mathbb{K}}\left(\alpha \cdot \phi \cdot \alpha^{-1}, \beta \cdot \psi \cdot \beta^{-1}\right).$$

Cela nous permet, dans les questions concernant les isogénies entre deux modules de Drinfeld ϕ et ψ, de supposer que ϕ et ψ sont définis sur$\mathcal{R}$, et de plus que $\overline{\phi}$ (et/ou $\overline{\psi}$) est un module de Drinfeld si ϕ (et/ou ψ) a une réduction stable.

Lemme 3.3 :
Soient $f, g \in \mathcal{R}\{\tau\}$ et $u \in \mathbb{K}\{\tau\}$ non nul tels que $u \cdot f = g \cdot u$.
Si $\deg_\tau(\overline{g}) > 0$, alors $u \in \mathcal{R}\{\tau\}$.

Preuve :
Soient $f, g \in \mathcal{R}\{\tau\}$ et $u \in \mathbb{K}\{\tau\}$ non nul tels que $u \cdot f = g \cdot u$.
On suppose que $\deg_\tau(\overline{g}) > 0$.
En notant $f := \sum_{i=0}^{n} f_i \tau^i$, $g := \sum_{i=0}^{n'} g_i \tau^i$ et $u := \sum_{i=0}^{n''} u_i \tau^i$, on a pour tout $m \in \mathbb{N}$:

$$\sum_{i+j=m} \left(u_i f_j^{q^i} - u_i^{q^j} g_j\right) = 0. \tag{3.1}$$

Soient i_0 le plus grand entier i tel que $|u_i|^{q^{-i}}$ est maximal et j_0 le plus grand entier j tel que $|g_j| = 1$ (≥ 1 par hypothèse).
Raisonnons par l'absurde en supposant que $u \notin \mathcal{R}\{\tau\}$:
On a alors $|u_{i_0}| > 1$ et dans ce cas, pour $m = i_0 + j_0 = i + j$, on a :

$$\left|u_{i_0}^{q^{j_0}} g_{j_0}\right| = \left|u_{i_0} q^{-i_0}\right|^{q^m} > \left|u_i^{q^{-i}}\right|^{q^m} |g_j| = \left|u_i^{q^j} g_j\right| \text{ pour } i \neq i_0. \tag{3.2}$$

De plus, pour $i \leq m$ tel que $|u_i| > 1$ et $i + j = m$, on a :

$$\left|u_{i_0}^{q^{j_0}} g_{j_0}\right| = \left|u_{i_0} q^{-i_0}\right|^{q^m} \overset{(*)}{\geq} \left|u_i^{q^{-i}}\right|^{q^m} \overset{(\dagger)}{\geq} |u_i| \geq \left|u_i f_j^{q^i}\right|. \tag{3.3}$$

Or, une égalité dans (†) implique que $i = m$ et une égalité dans $(*)$ implique que $\left|u_{i_0}^{q^{-i_0}}\right| = \left|u_i^{q^{-i}}\right|$. Par hypothèse, on a $i_0 \geq i$ et donc une égalité dans (†) et $(*)$ donne que $m \geq i_0 \geq i = m$. Ainsi, on a $i_0 = m$, ce qui contredit le fait que $j_0 = m - i_0 \geq 1$. Enfin, par l'inégalité ultramétrique, des inégalités strictes dans (3.2) et (3.3) contredisent (3.1).

Par conséquent, on a $|u_{i_0}| \leq 1$ et donc $u \in \mathcal{R}\{\tau\}$

■

Dans toute la suite de cette partie, on note $\mathrm{Hom}_{\mathcal{R}}(\phi, \psi) := \{u \in \mathcal{R}\{\tau\} \mid \forall a \in A,\ u \cdot \phi_a = \psi_a \cdot u\}$ ainsi que $\mathrm{Hom}_k\left(\overline{\phi}, \overline{\psi}\right) := \left\{u \in k\{\tau\} \mid \forall a \in A,\ u \cdot \overline{\phi}_a = \overline{\psi}_a \cdot u\right\}$.

Proposition 3.2 :
Soient ϕ et ψ deux modules de Drinfeld sur $\mathcal{R}$.
Si $\overline{\psi}$ est un module de Drinfeld, alors $\mathrm{Hom}_{\mathbb{K}}(\phi, \psi) = \mathrm{Hom}_{\mathcal{R}}(\phi, \psi)$.

Preuve :
Soient ϕ et ψ deux modules de Drinfeld sur $\mathcal{R}$.
Supposons que $\overline{\psi}$ soit un module de Drinfeld.
Il suffit d'appliquer le lemme 3.3 avec $f := \phi_T$ et $g := \psi_T$ pour obtenir l'égalité voulue.

■

Proposition 3.3 :
Soient ϕ et ψ deux modules de Drinfeld sur $\mathcal{R}$.
Si $\overline{\psi}$ est un module de Drinfeld, alors le morphisme naturel $\mathrm{Hom}_{\mathcal{R}}(\phi,\psi) \longrightarrow \mathrm{Hom}_k\left(\overline{\phi},\overline{\psi}\right)$ de réduction modulo $\mathcal{M}$ est injectif.

Preuve :
Soient ϕ et ψ deux modules de Drinfeld sur $\mathcal{R}$.
Supposons que $\overline{\psi}$ soit un module de Drinfeld.
Raisonnons par l'absurde en supposant qu'il existe $u \in \mathrm{Hom}_{\mathcal{R}}(\phi,\psi)$ non nul tel que $\overline{u} = 0$:
On peut écrire $u = \pi^m \cdot w$ avec $m \in \mathbb{N}^*$, $w \in \mathcal{R}\{\tau\}$ tel que $\overline{w} \neq 0$ et de l'égalité $u \cdot \phi_{\mathfrak{p}} = \psi_{\mathfrak{p}} \cdot u$, on obtient $\pi^m \cdot w \cdot \phi_{\mathfrak{p}} = \psi_{\mathfrak{p}} \cdot \pi^m \cdot w$.

Par conséquent, si on écrit $\psi_{\mathfrak{p}} = \sum_{n=0}^{r\deg(\mathfrak{p})} g_n(\mathfrak{p})\tau^n$, alors :

$$\psi_{\mathfrak{p}} \cdot \pi^m = \left(\sum_{n=0}^{r\deg(\mathfrak{p})} g_n(\mathfrak{p})\tau^n\right) \cdot \pi^m = \sum_{n=0}^{r\deg(\mathfrak{p})} g_n(\mathfrak{p})\pi^{mq^n}\tau^n = \pi^m \cdot f,$$

avec $\overline{f} = 0$ car $g_0(\mathfrak{p}) = \mathfrak{p} \in \mathcal{M}$. On obtient alors que $\pi^m \cdot w \cdot \phi_{\mathfrak{p}} = \pi^m \cdot f \cdot w$ et donc $w \cdot \phi_{\mathfrak{p}} = f \cdot w$. En réduisant cette dernière égalité modulo $\mathcal{M}$, on a $\overline{w} \cdot \overline{\phi}_{\mathfrak{p}} = \overline{f} \cdot \overline{w} = 0$ et puisque $\overline{\phi}$ est un module de Drinfeld, on a $\overline{\phi}_{\mathfrak{p}} \neq 0$ et ainsi $\overline{w} = 0$, ce qui contredit l'hypothèse de départ.

Par conséquent, on a nécessairement $u = 0$ et donc le morphisme $\mathrm{Hom}_{\mathcal{R}}(\phi,\psi) \longrightarrow \mathrm{Hom}_k\left(\overline{\phi},\overline{\psi}\right)$ de réduction modulo $\mathcal{M}$ est injectif.

■

Corollaire 3.1 :
Soient ϕ et ψ deux modules de Drinfeld sur $\mathcal{R}$.
Si ϕ et ψ ont une réduction stable sur $\mathbb{K}$, alors il existe un morphisme injectif naturel $\mathrm{Hom}_{\mathbb{K}}(\phi,\psi) \hookrightarrow \mathrm{Hom}_k(\phi,\psi)$.
De plus, si ϕ a une bonne réduction, alors le degré en τ d'un morphisme $u : \phi \longrightarrow \psi$ est préservé après réduction.

Preuve :
Soient ϕ et ψ deux modules de Drinfeld sur $\mathcal{R}$.
Supposons que ϕ et ψ ont une réduction stable sur $\mathbb{K}$ et quitte à remplacer ϕ et ψ par des modules de Drinfeld isomorphes sur $\mathbb{K}$, on peut supposer également que chacun est défini sur $\mathcal{R}$ et que $\overline{\phi}$ et $\overline{\psi}$ sont des modules de Drinfeld.
Par la proposition 3.2, on a $\mathrm{Hom}_{\mathbb{K}}(\phi,\psi) = \mathrm{Hom}_{\mathcal{R}}(\phi,\psi)$ et par la proposition 3.3, l'application

$$\mathrm{Hom}_{\mathbb{K}}(\phi,\psi) = \mathrm{Hom}_{\mathcal{R}}\,\phi,\psi \overset{\mathrm{mod}\,\mathcal{M}}{\longrightarrow} \mathrm{Hom}_k(\phi,\psi)$$

est injective.

Désormais, supposons de plus que ϕ ait une bonne réduction et considérons une isogénie $u : \phi \longrightarrow \psi$ définie sur $\mathbb{K}$.
Comme ϕ a une bonne réduction, on a $\deg_\tau(\phi_T) = \deg_\tau\left(\overline{\phi}_T\right)$ et donc ψ a également une bonne réduction. En effet, puisque $\overline{u} \neq 0$, en calculant les degrés de chaque côté de l'égalité $\overline{u} \cdot \overline{\phi}_T = \overline{\psi}_T \cdot \overline{u}$ on trouve que $\deg_\tau\left(\overline{\phi}_T\right) = \deg_\tau\left(\overline{\psi}_T\right)$. Ainsi, on a :

$$\deg_\tau(\psi_T) = \deg_\tau(\phi_T) = \deg_\tau(\overline{\phi}_T) = \deg_\tau\left(\overline{\psi}_T\right).$$

En notant g_r, g'_r et u_n les coefficients dominants de respectivement ϕ_T, ψ_T et u, l'égalité $u \cdot \phi_T = \psi_T \cdot u$ donne que $u_n g_r^{q^n} = u_n^{q^r} g'_r$, ce qui implique que $u_n \in \mathcal{R}$ puisque $g_r, g'_r \in \mathcal{R}$ et $r > 0$.

■

II Uniformisation de Tate

Définition 3.4 : ϕ-réseau :
On considère ϕ un module de Drinfeld sur $\mathbb{K}$.
On appelle **ϕ-réseau de rang** d tout A-sous-module libre Λ de ${}^{\phi}\mathbb{K}^{sep}$ de rang d qui est invariant par l'action de $\mathrm{Gal}_{\mathbb{K}}$ et discret dans $\mathbb{C}_{\mathbb{K}}$.

Remarque :
Ici, "discret" signifie que toute boule fermée de rayon finie de $\mathbb{C}_{\mathbb{K}}$ ne contient qu'un nombre fini d'éléments de Λ.

Exemple 3.2 :
Considérons ϕ un module de Drinfeld de rang 2 sur $\mathcal{R}$ avec une bonne réduction.
Pour $\omega \in \mathbb{K}^{\times}$ fixé et en posant $\Lambda := \{\phi_a(\omega),\ a \in A\}$, on remarque que Λ est un A-sous-module de ${}^{\phi}\mathbb{K}$ qui est $\mathrm{Gal}_{\mathbb{K}}$-invariant. De plus, si $\omega \notin^{\phi} \mathbb{K}_{tor}$, alors on a Λ qui est libre et de rang 1.

En utilisant les hypothèses sur ϕ, on obtient que

$$v(\phi_a(\omega)) = \begin{cases} v(\omega)q^{r\deg(a)} & \text{si } v(\omega) < 0 \\ \geq 0 & \text{si } v(\omega) \geq 0 \end{cases}$$

Ceci implique que Λ est un ϕ-réseau de rang 1 si, et seulement si, $v(\omega) < 0$ et $\omega \notin^{\phi} \mathbb{K}_{tor}$. Or, puisque les points de torsion de ϕ sont entiers sur $\mathcal{R}$, le fait que $v(\omega) < 0$ implique déjà que $\omega \notin^{\phi} \mathbb{K}_{tor}$. Ainsi, Λ est un ϕ-réseau si, et seulement si, $v(\omega) < 0$.

Désormais, on considère Λ un ϕ-réseau et on pose l'application

$$e_\Lambda : \left| \begin{array}{ccc} \mathbb{C}_{\mathbb{K}} & \longrightarrow & \mathbb{C}_{\mathbb{K}} \\ x & \longmapsto & x\prod_{\lambda\in\Lambda\setminus\{0_{\mathbb{C}_{\mathbb{K}}}\}}\left(1-\frac{x}{\lambda}\right) \end{array} \right. .$$

Puisque Λ est un $\mathbb{F}_q$-sous-espace vectoriel discret de $\mathbb{C}_{\mathbb{K}}$, on obtient que e_Λ est entière et $\mathbb{F}_q$-linéaire (par la proposition 2.3). De plus, puisque Λ est $\mathrm{Gal}_{\mathbb{K}}$-invariant, on en déduit que les coefficients de e_Λ appartiennent à $\mathbb{K}$.

Pour $a \in A\setminus\{0_A\}$, on définit :

$$\Lambda' := \phi_a^{-1}(\Lambda) = \{z \in \mathbb{C}_{\mathbb{K}} \mid \phi_a(z) \in \Lambda\}.$$

On remarque que Λ' est un A-sous-module de ${}^{\phi}\mathbb{C}_{\mathbb{K}}$ tel que $\phi_a(\Lambda') = \Lambda$ et $\Lambda \subseteq \Lambda'$ (car Λ est un A-sous-module de ${}^{\phi}\mathbb{K}^{sep}$). Cependant, Λ' n'est pas un ϕ-réseau puisqu'il contient les éléments de torsion $\phi[a] \subseteq^{\phi} (\mathbb{C}_{\mathbb{K}})_{tor}$. Pour prouver qu'il est néanmoins discret, on utilise le lemme suivant :

Lemme 3.4 : Lemme du noyau-conoyau :
Toute paire de morphismes entre modules sur un anneau commutatif $M_1 \xrightarrow{f} M_2 \xrightarrow{g} M_3$ donne une suite exacte de la forme :

$$0 \longrightarrow \mathrm{Ker}(f) \longrightarrow \mathrm{Ker}(g\circ f) \longrightarrow \mathrm{Ker}(g) \longrightarrow \mathrm{Coker}(f) \longrightarrow \mathrm{Coker}(g\circ f) \longrightarrow \mathrm{Coker}(g) \longrightarrow 0.$$

Preuve :
Pour obtenir le résultat voulu, il suffit d'appliquer le lemme du serpent au diagramme commutatif :

$$\begin{array}{ccccccccc} & & M_1 & \xrightarrow{f} & M_2 & \longrightarrow & \mathrm{Coker}(f) & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle g\circ f} & & \downarrow{\scriptstyle g} & & \downarrow & & \\ 0 & \longrightarrow & M_3 & \xrightarrow{\mathrm{Id}_{M_3}} & M_3 & \longrightarrow & 0 & & \end{array}$$

■

En appliquant le lemme précédent à $\Lambda \overset{\iota}{\hookrightarrow} \Lambda' \overset{\phi_a}{\longrightarrow} \Lambda$, on obtient la suite exacte de A-modules :

$$0 \longrightarrow \mathrm{Ker}(\iota) \longrightarrow \mathrm{Ker}(\phi_a \circ \iota) \longrightarrow \mathrm{Ker}(\phi_a) \longrightarrow \mathrm{Coker}(\iota) \longrightarrow \mathrm{Coker}(\phi_a \circ \iota) \longrightarrow \mathrm{Coker}(\iota) \longrightarrow 0.$$

Or, $\phi_a \circ \iota : \Lambda \longrightarrow \Lambda$ est injective (car Λ est un ϕ-réseau) et $\phi_a : \Lambda' \longrightarrow \Lambda$ est surjective, donc la suite exacte précédente devient la suite exacte courte :

$$0 \longrightarrow \phi[a] \longrightarrow \Lambda'/\iota(\Lambda) \longrightarrow \Lambda/(\phi_a \circ \iota)(\Lambda) \longrightarrow 0.$$

En particulier, Λ est d'indice fini dans Λ', ce qui implique que Λ' est discret. Ainsi, $e_{\Lambda'}$ est une fonction entière sur $\mathbb{C}_{\mathbb{K}}$ et $\mathbb{F}_q$-linéaire.

Lemme 3.5 :
L'ensemble des zéros de $e_\Lambda(\phi_a(x))$ est exactement Λ'.

Preuve :
Posons $h(x) := e_\Lambda(\phi_a(x))$.
Par le corollaire 2.2 on a $h(z) = e_\Lambda(\phi_a(z))$ pour tout $z \in \mathbb{C}_{\mathbb{K}}$. Ainsi, $h(z) = 0$ si, et seulement si, $\phi_a(z) \in \Lambda$ (c'est-à-dire si, et seulement si, $z \in \Lambda'$). Or, puisque $h(x)$ est $\mathbb{F}_q$-linéaire avec un coefficient constant non nul, ses zéros sont simples et donc $Z(h) = \Lambda'$.

■

Par le lemme 3.5 ainsi que le théorème 2.3, on en déduit que $ae_{\Lambda'}(x) = e_\Lambda(\phi_a(x))$. De plus, on peut également montrer qu'il existe un polynôme $\mathbb{F}_q$-linéaire $P_a(x)$ tel que $e_{\Lambda'}(x) = P_a(e_\Lambda(x))$. En notant $\psi_a(x) := aP_a(x)$ on obtient alors :

$$e_\Lambda(\phi_a(x)) = \psi_a(e_\Lambda(x)).$$

Enfin, puisque e_Λ et ϕ_a sont à coefficients dans $\mathbb{K}$, on a également $\psi_a \in \mathbb{K}\{\tau\}$.

On admet la proposition suivante dont on trouvera une démonstration à la suite de la proposition 6.2.6 à la page 355 de [Pap23].

Proposition 3.4 :
Avec les notations et hypothèses précédentes, l'application

$$\psi : \left| \begin{array}{ccc} A & \longrightarrow & \mathbb{K}\{\tau\} \\ a & \longmapsto & \psi_a \end{array} \right.$$

est un module de Drinfeld sur $\mathbb{K}$ de rang $r + d$, où r est le rang de ϕ et d le rang de Λ.

On peut alors résumer les relations entre e_Λ, ϕ et ψ via la suite exacte suivante de A-modules :

$$0 \longrightarrow \Lambda \longrightarrow {}^{\phi}\mathbb{C}_{\mathbb{K}} \overset{e_\Lambda}{\longrightarrow} {}^{\psi}\mathbb{C}_{\mathbb{K}} \longrightarrow 0 \tag{3.4}$$

Lorsque ϕ a une bonne réduction, (3.4) est appelé **uniformisation de Tate de** ψ.

La suite exacte (3.4) signifie plus exactement que le diagramme

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \Lambda & \longrightarrow & \mathbb{C}_{\mathbb{K}} & \overset{e_\Lambda}{\longrightarrow} & \mathbb{C}_{\mathbb{K}} & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \phi_a} & & \downarrow{\scriptstyle \phi_a} & & \downarrow{\scriptstyle \psi_a} & & \\ 0 & \longrightarrow & \Lambda & \longrightarrow & \mathbb{C}_{\mathbb{K}} & \overset{e_\Lambda}{\longrightarrow} & \mathbb{C}_{\mathbb{K}} & \longrightarrow & 0 \end{array} \tag{3.5}$$

est commutatif pour tout $a \in A$. Ainsi, par le lemme du serpent, on a également une suite exacte courte de A-modules :

$$0 \longrightarrow \phi[a] \longrightarrow \psi[a] \longrightarrow \Lambda/\phi_a(\Lambda) \longrightarrow 0. \tag{3.6}$$

De plus, puisque e_Λ, ϕ_a et ψ_a sont à coefficients dans $\mathbb{K}$, le diagramme (3.5) est compatible avec l'action de $\mathrm{Gal}_{\mathbb{K}}$ et donc (3.6) est aussi une suite exacte de $\mathrm{Gal}_{\mathbb{K}}$-modules.

Finalement, notons que $\psi[a]$ peut être décrit explicitement comme $\psi[a] = \{e_\Lambda(z),\ z \in \phi_a^{-1}(\Lambda)\}$. Ainsi, $e_\Lambda(x)$ donne un isomorphisme de A-modules : $\phi_a^{-1}(\Lambda)/\Lambda \cong \psi[a]$.

Exemple 3.3 :
Posons $C_T := T + \tau$ le module de Carlitz, fixons $\omega \in \mathbb{K}$ tel que $v(\omega) < 0$ et considérons $\Lambda := \{C_a(\omega),\ a \in A\}$ le C-réseau correspondant de rang 1.
En notant ψ le module de Drinfeld de rang 2 correspondant à la paire (C, Λ) et en notant $\log_\Lambda := \sum_{n\geq 0} b_n \tau^n$ l'inverse de e_Λ dans $\mathbb{K}\{\{\tau\}\}$, on peut montrer que :

$$\forall n \in \mathbb{N}^*,\ b_n = -\sum_{\lambda \in \Lambda \setminus \{0_{\mathbb{C}_{\mathbb{K}}}\}} \frac{1}{\lambda^{q^n-1}} = \sum_{a \in A^+} \frac{1}{C_a(\omega)^{q^n-1}}.$$

Puisque $v\left(C_a(\omega)^{q^n-1}\right) = (q^n-1)\, q^{\deg(a)} v(\omega) < 0$, on a :

$$\forall n \in \mathbb{N}^*,\ v(b_n) = -v\left(C_1(\omega)^{q^n-1}\right) = -(q^n-1)\, v(\omega) > 0. \tag{3.7}$$

Posons $\psi_T := T + g_1\tau + g_2\tau^2$.
De l'équation fonctionnelle $C_T \circ \log_\Lambda = \log_\Lambda \circ \psi_T$, on en déduit que

$$\begin{cases} g_1 = & 1 + (T - T^q) b_1 \\ g_2 = & \left(T - T^{q^2}\right) b_2 - b_1 + b_1^q + \left(T^{q^2} - T^q\right) b_1^{q+1}. \end{cases}$$

Ainsi, on trouve que grâce à ces formules et avec (3.7) que $\overline{g_1} = 1$ et $\overline{g_2} = 0$, d'où

$$\overline{\psi}_T = \overline{T} + \overline{g_1}\tau + \overline{g_2}\tau^2 = \overline{T} + \tau = \overline{C}_T.$$

Par conséquent, ψ a une mauvaise réduction stable de rang 1 qui coïncide avec la réduction du module de Carlitz. De plus, remarquons que $v(g_1) = 0$ et $v(g_2) = v(b_1) = -(q-1)v(\omega) > 0$, donc

$$v(j_\psi) = v\left(\frac{g_1^{q+1}}{g_2}\right) = (q-1)v(\omega) < 0.$$

Lemme 3.6 :
Soit B une $\mathbb{F}_q$-algèbre.
Si $u := \sum_{i=0}^n u_i \tau^i \in B\{\tau\}$ est tel que u_0 est inversible et $u_1, \ldots, u_n$ sont nilpotents, alors u est inversible dans $B\{\tau\}$.

Preuve :
Soient B une $\mathbb{F}_q$-algèbre et $u := \sum_{i=0}^n u_i \tau^i \in B\{\tau\}$.
Supposons que u_0 est inversible et $u_1, \ldots, u_n$ sont nilpotents.
Quitte à remplacer u par $u_0^{-1}u$, on peut supposer que $u_0 = 1$ et il suffit de montrer qu'il existe $s \in \mathbb{N}^*$ assez grand tel que $u^{p^s} - 1 = (u-1)^{p^s} = 0$ puisqu'alors $u^{p^s-1}u = uu^{p^s-1} = u^{p^s} = 1$.

Or, remarquons que l'on peut écrire, pour un certain $w_m \in B\{\tau\}$, que

$$(u-1)^m = w_m \tau^{m-1} \sum_{i=1}^n u_i \tau^i = w_m \sum_{i=1}^n u_i^{q^{m-1}} \tau^{i+m-1}$$

Ainsi, pour $m \in \mathbb{N}^*$ assez grand, on a pour tout $i \in [\![1; n]\!]$ que $u_i^{q^{m-1}} = 0$, d'où $(u-1)^m = 0$.

■

Lemme 3.7 :
Soient B une $\mathbb{F}_q$-algèbre et $d \in \mathbb{N}^*$.
Si $f := \sum_{i=0}^{n} f_i \tau^i \in B\{\tau\}$ est tel que $f_d \in B^\times$ et $f_{d+1}, \dots, f_n$ sont nilpotents, alors il existe un unique $u := \sum_{j \geq 0} u_j \tau^j \in B\{\tau\}$ tel que :

* $u_0 = 1$;
* Pour tout $j \in \mathbb{N}^*$, u_j est nilpotent ;
* $g := u^{-1} \cdot f \cdot u := \sum_{i=1}^{d} g_i \tau^i$ est de degré d et $g_d \in B^\times$.

Preuve :
Soient B une $\mathbb{F}_q$-algèbre et $d \in \mathbb{N}^*$.
Supposons que l'on ait $f := \sum_{i=0}^{n} f_i \tau^i \in B\{\tau\}$ tel que $f_d \in B^\times$ et $f_{d+1}, \dots, f_n$ sont nilpotents.

* Existence de u :
  Soit $\mathcal{N}$ l'idéal de B engendré par les $f_{d+1}, \dots, f_n$.
  L'idéal $\mathcal{N}$ est nilpotent et donc il existe $s \in \mathbb{N}^*$ tel que $\mathcal{N}^s = 0$. Nous allons désormais construire u en fonction de la valeur de s.
  — Si $s = 1$, alors $f_{d+1} = \dots = f_n = 0$ et $u = 1$ convient.

  — Supposons que $s = 2$ et montrons le résultat par récurrence forte sur $n - d \in \mathbb{N}$:
  Si $n - d = 0$, alors on a $n = d$ et donc il n'y a rien a prouver et on peut prendre $u = 1$ comme dans le cas précédent. La propriété est donc bien initialisée.

  Considérons $N \in \mathbb{N}^*$ et supposons que la propriété soient vraie pour tous $0 \leq n - d < N$. Montrons qu'elle est encore vraie au rang $n - d = N$:
  Posons $w := 1 + \frac{f_n}{f_d^{q^{n-d}}} \tau^{n-d}$ un élément inversible (et d'inverse $w^{-1} = 1 - \frac{f_n}{f_d^{q^{n-d}}} \tau^{n-d}$) ainsi que

$$\widetilde{f} := w^{-1} \cdot f \cdot w = f - \frac{f_n}{f_d^{q^{n-d}}} \left(\sum_{i=0}^{d} f_i^{q^{n-d}} \tau^i \right) \tau^{n-d}.$$

  Remarquons que $\widetilde{f} := \sum_{i=0}^{n-1} \widetilde{f}_i \tau^i$ est de degré inférieur ou égal à $n-1$ et que ses coefficients $\widetilde{f}_i$ sont dans $\mathcal{N}$ pour $i \in [\![d+1; n-1]\!]$ et puisque $f_d + \alpha$ est inversible pour $\alpha \in \mathcal{N}$ (et d'inverse $f_d^{-1} - \frac{\alpha}{f_d^2}$), $\widetilde{f}_d$ est également inversible.
  Par hypothèse de récurrence (puisque $(n-1) - d = N - 1$), il existe $\widetilde{u}$ vérifiant les trois points énoncés. Enfin, en posant $u = w \cdot \widetilde{u}$, on a $u_0 = 1$ (puisque les termes constants de $\widetilde{u}$ et w sont égaux à 1), les coeffiients u_j sont nilpotents pour tout $j \in \mathbb{N}^*$ (puisque les coefficients $\widetilde{u}_j$ et w_j le sont) et on a $g = u^{-1} \cdot f \cdot u$ par construction.
  Finalement, la propriété est héréditaire et on a montré le résultat dans le cas où $s = 2$.

  — Supposons maintenant que $s := M \geq 3$ et montrons le résultat par récurrence forte sur $s \in \mathbb{N}^*$ désormais :
  Si $s = 1$ ou $s = 2$, alors le résultat découle de l'un des deux points précédents et donc la propriété est bien initialisée.

  Supposons désormais que la propriété soit vraie pour tout entier naturel non nul inférieur ou égal à $M - 1$ et montrons qu'elle est encore vraie au rang M :
  Soient $B' := B/\mathcal{N}^{M-1}$ et f' l'image de f dans $B'\{\tau\}$.
  Les coefficients de f' engendrent l'idéal $\mathcal{N}' := \mathcal{N}/\mathcal{N}^{M-1}$ et on a $(\mathcal{N}')^{M-1} = \{0\}$. Par hypothèse de récurrence, il existe $u' := \sum_{j \geq 0} u'_j \tau^j \in B'\{\tau\}$ ayant les propriétés voulues et on pose $z := \sum_{i \geq 0} z_i \tau^i \in B\{\tau\}$ un relèvement de u'. Les coefficients de z sont alors nilpotents (puisque les u'_i sont nilpotents et $\mathcal{N}^{M-1}$ est nilpotent) et on pose finalement $g' := z^{-1} \cdot f \cdot z = \sum_{i=0}^{m} g'_i \tau^i$.
  On a que g_d est inversible et l'idéal I engendré par $g'_{d+1}, \dots, g'_d$ appartient à $\mathcal{N}^{M-1}$. Ainsi $I^2 = 0$ et en appliquant les arguments du cas où $s = 2$ on trouve $y := \sum_{i \geq 0} y_i \tau^i$ tel que les y_i sont dans I

(et donc dans $\mathcal{N}^{M-1}$) et $g := y^{-1} \cdot g' \cdot y \in B\{\tau\}$ de degré d avec y_d inversible et par construction $u := z \cdot y$ vérifie les propriétés voulues.
Finalement, la propriété est héréditaire et on a montré le résultat dans le cas où $s \geq 3$.

* Unicité de u :
Considérons u et supposons qu'il existe un autre v vérifiant les mêmes propriétés.
En posant $h := v^{-1} \cdot f \cdot v$ on a $g := u^{-1} \cdot f \cdot u = \left(v^{-1} \cdot u\right)^{-1} \cdot h \cdot \left(v^{-1} \cdot u\right)$ et puisque g et h sont de degré d et à coefficient dominant inversible, il suffit de montrer que $u = 1$ si $f_{d+1} = \cdots = f_n = 0$ pour avoir que $u = v$.

Raisonnons par l'absurde en supposant que $f_{d+1} = \cdots = f_n = 0$ mais que $\deg(u) = m > 0$.
De l'égalité $f \cdot u = u \cdot g$, on obtient que $u_m g_d^{q^m} = u_m^{q^d} f_d$ et puisque f_d et g_d sont inversibles, il existe $\alpha \in B^\times$ tel que $u_m = \alpha u_m^{q^d}$.
Notons $N > 1$ le plus petit entier naturel tel que $u_m^N = 0$.

* Si $q^d \geq N$, alors on a $u_m^{q^d} = 0$ et donc $u_m = 0$, ce qui contredit le fait que $\deg(u) = m > 0$.

* Si $q^d < N$, alors on a :

$$\alpha^{-1} u_m^{N-q^d+1} = u_m^{N-q^d} \left(\alpha^{-1} u_m\right) = u_m^{N-q^d} u_m^{q^d} = u_m^N = 0.$$

Or comme α est inversible, on a $u_m^{N-q^d+1} = 0$ et comme $N - q^d + 1 < N$, on aboutit à une contradiction sur N.

Finalement, on a $\deg(u) = 0$ et donc $u = 1$ (car $u_0 = 1$), ce qui nous donne bien le résultat.

■

Lemme 3.8 :
Soit $f \in \mathcal{R}\{\tau\}$ avec $d = \deg\left(\overline{f}\right) > 0$.
Il existe un unique $u := u_f \in \mathcal{R}\{\{\tau\}\}$ tel que :

* $u = 1 + \sum_{i \geq 1} \alpha_i \tau^i$, avec $|\alpha_i| < 1$ et $\lim_{i \to +\infty} \alpha_i = 0$;
* $g := u^{-1} f u$ appartient à $\mathcal{R}\{\tau\}$ et $\deg(g) = \deg(\overline{g}) = d$;
* u est une fonction entière.

Preuve :
Soit $f \in \mathcal{R}\{\tau\}$ avec $d = \deg\left(\overline{f}\right) > 0$.
Pour tout $m \in \mathbb{N}^*$, on pose $\mathcal{R}_m := \mathcal{R}/\mathcal{M}^m$ et on note $\overline{f}_m \in \mathcal{R}_m\{\tau\}$ la réduction de f modulo $\mathcal{M}^m$.
Par le lemme 3.7, il existe un unique $u_m \in \mathcal{R}_m\{\tau\}^\times$ tel que le terme constant de u_m vaille 1 et $u_m^{-1} \cdot \overline{f}_m \cdot u_m$ soit un polynôme de degré d dont le coefficient dominant est dans $R_m^\times$.

L'unicité de u_m implique que $u_m \equiv u_{m-1} \left[\mathcal{M}^{m-1}\right]$ et donc en prenant la limite inverse des coefficients, on obtient un élément $u := \varprojlim_{m \in \mathbb{N}^*} u_m \in \mathcal{R}\{\{\tau\}\}$. Par construction, u vérifie les deux premiers points et est unique avec ces propriétés.

Il nous reste à montrer que $u(x)$ est entière.
Soient $f := \sum_{i=1}^n f_i \tau^i$ et $g := \sum_{j=0}^d g_j \tau^j$.
Pour $m > n$, en calculant les coefficients de τ^m de chaque côté de l'équation $u \cdot g = f \cdot u$, on obtient

$$\sum_{i=0}^{d} \alpha_{m-i} g_i^{q^{m-i}} = \sum_{i=0}^{n} \alpha_i^{q^i} f_i$$

que l'on peut réécrire en

$$\alpha_{m-d}\left(g_d^{q^{m-d}} - f_d\alpha_{m-d}^{q^d-1}\right) = -\sum_{i=0}^{d-1}\alpha_{m-i}g_i^{q^{m-i}} + \sum_{\substack{0\leq j\leq n\\ j\neq d}}\alpha_{m-j}^{q^j}f_j. \tag{3.8}$$

De plus, comme $g_d \in R^\times$ et que $f_d\alpha_{m-d}^{q^d-1} \in \mathcal{M}$, on a

$$|\alpha_{m-d}| \times \left|g_d^{q^{m-d}} - f_d\alpha_{m-d}^{q^d-1}\right| = |\alpha_{m-d}|$$

et comme f et g ont des coefficients qui sont entiers, l'inégalité triangulaire appliquée à (3.8) nous donne :

$$|\alpha_{m-d}| \leq \max\left(\{|\alpha_{m-i}|,\ i \in [\![1-d;0]\!]\} \cup \left\{|\alpha_{m-i}|^{q^i},\ i \in [\![0;n]\!]\backslash\{d\}\right\}\right).$$

Puisque $|\alpha_{m-j}| < 1$ pour $j \in [\![0;d-1]\!]$, on a $|\alpha_{m-j}|q^j < |\alpha_{m-j}|$, donc certains des termes de l'inégalité précédente peuvent êtres omis. Après ce changement, on obtient que pour $i > s := n-d$:

$$|\alpha_i| \leq \max\left(\left\{|\alpha_{i-j}|^{q^{d+j}},\ j \in [\![1;s]\!]\right\} \cup \{|\alpha_{i+j}|,\ j \in [\![1;d]\!]\}\right). \tag{3.9}$$

Notons S_i l'union des deux ensembles du membre de droite de l'inégalité précédente et effectuons la procédure itérative suivante :
Commençons par poser $S := S_i$. Si $|\alpha_j|^{q^\ell} \in S$ pour un certain $\ell \geq 1$, alors on supprime cet élément de S. Ensuite, on remplace chaque $|\alpha_j|^{q^\ell} \in S$ avec $j > i$ par $S_j^{q^\ell}$, où $S_j^{q^\ell}$ correspond à l'ensemble des éléments de S_j élevés à la puissance q^ℓ et on appelle S l'ensemble obtenu.
On répète alors le même procédé pour ce nouveau S et on peut voir qu'avec chaque itération, soit les éléments $|\alpha_j|$ apparaissent dans S avec une puissance de q plus grande qu'avant ou bien $|\alpha_j|$ a un indice plus grand que les éléments dans le S précédent. Par (3.9), à chaque étape du procédé on a $|\alpha_i| \leq \max(S)$ et de plus, puisque $0 \leq |\alpha_j| < 1$ pour tout $j \in \mathbb{N}^*$ et que $\lim_{j\to+\infty}|\alpha_j| = 0$, le maximum des éléments de S dont l'indice est plus grand que i tend vers 0. Ainsi :

$$|\alpha_i| \leq \max\left(\left\{|\alpha_{i-j}|^{q^{d+i}},\ j \in [\![1;s]\!]\right\}\right). \tag{3.10}$$

En notant $\beta_j := |\alpha_j|^{\frac{1}{q^j}}$ pour $j \in \mathbb{N}^*$, (3.10) implique que

$$\beta_i \leq \max\left(\{\beta_{i-j},\ j \in [\![1;s]\!]\}\right)^{q^d}. \tag{3.11}$$

Ainsi :

$$\begin{aligned}\beta_{i+1} &\leq \max\left(\{\beta_{i+1-j},\ j \in [\![1;s]\!]\}\right)^{q^d} \leq \max\left(\{\beta_{i-j},\ j \in [\![1;s-1]\!]\} \cup \left\{\beta_{i-j}^{q^d},\ j \in [\![1;s]\!]\right\}\right)^{q^d} \quad \text{(par (3.11))}\\ &\leq \max\left(\left\{\beta_{i-s}^{q^d}\right\} \cup \{\{\beta_{i-j},\ j \in [\![1;s-1]\!]\}\}\right)^{q^d}.\end{aligned}$$

En itérant cet argument, on obtient que

$$\beta_{i+2} \leq \max\left(\left\{\beta_{i-s}^{q^d}, \beta_{i+1-s}^{q^d}\right\} \cup \{\beta_{i-j},\ j \in [\![1;s-2]\!]\}\right)^{q^d},$$

ce qui nous donne

$$\forall j \in \mathbb{N},\ \beta_{i+js} \leq \max\left(\{\beta_{i-j},\ j \in [\![1;s]\!]\}\right)^{q^{d(j+1)}}.$$

Or, puisque $0 \leq \max\left(\{\beta_{i-j},\ j \in [\![1;s]\!]\}\right)^{q^{d(j+1)}} < 1$, ceci implique que β_j tend vers 0 quand j tend vers $+\infty$, ce qui est une condition équivalente au fait que $u(x)$ soit entière par le lemme 2.3.

■

Théorème 3.1 :
L'application qui à une uniformisation de Tate (ϕ, Λ) associe ψ est une bijection de l'ensemble des paires consistant en un module de Drinfeld sur $\mathcal{R}$ de rang r avec une bonne réduction et les ϕ-réseaux Λ de rang d dans l'ensemble des modules de Drinfeld sur $\mathcal{R}$ de rang $r+d$ avec réduction de rang r.
De plus, on a $\overline{\psi} = \overline{\phi}$.

Preuve :

* Soient ϕ un module de Drinfeld sur $\mathcal{R}$ où $\phi_T := T + \sum_{i=1}^{r} g_i \tau^i$ avec $g_r \in \mathcal{R}^\times$ et Λ un ϕ-réseau de rang d. Par la proposition 3.4, l'uniformisation de Tate produit un module de Drinfeld ψ de rang $r+d$. De plus, pour tout $\lambda \in \Lambda$ non nul, on a $|\lambda| > 1$ (en effet, dans le cas contraire on obtient que pour tout $a \in A$, $|\phi_a(\lambda)| \leq 1$ ce qui contredit le fait que Λ est discret).
Ceci implique que $e_\Lambda \in \mathcal{R}\{\{\tau\}\}$ et $e_\Lambda \equiv 1$ $[\mathcal{M}]$ et l'équation fonctionnelle $e_\Lambda \circ \phi_T = \psi_T \circ e_\Lambda$ implique que $\psi_T \in \mathcal{R}\{\tau\}$. En réduisant cette équation fonctionnelle modulo $\mathcal{M}$ on obtient alors que $\overline{\phi}_T = \overline{\psi}_T$ et donc la réduction de ψ est de rang r.

* Réciproquement, supposons que ψ est un module de Drinfeld de rang $r+d$ défini sur $\mathcal{R}$ tel que $\overline{\psi}$ est de rang r.
Le lemme 3.8 appliqué à $f := \psi_T$ nous donne l'existence d'une unique série

$$e := 1 + \sum_{i \geq 1} \alpha_i \tau^i \in 1 + \mathcal{M}\{\{\tau\}\}\tau$$

telle que $\phi_T := e^{-1} \cdot \psi_T \cdot e \in \mathcal{R}\{\tau\}$ est de degré r, $\overline{\phi}_T = \overline{\psi}_T$ et $e(x) \in \mathcal{R}\langle\langle x \rangle\rangle$ est entière. Ainsi ϕ_T défini un module de Drinfeld ϕ sur $\mathcal{R}$ de rang r et qui a une bonne réduction.

Montrons que l'ensemble $\Lambda := Z(e(x))$ des zéros de $e(x)$ est un ϕ-réseau de rang d :
La proposition 2.3 nous donne que Λ est un $\mathbb{F}_q$-sous-espace vectoriel discret de $\mathbb{C}_\mathbb{K}$, il est inclus dans $\mathbb{K}^{sep}$ et est $\mathrm{Gal}_\mathbb{K}$-invariant. De plus, la relation $e \cdot \phi_T = \psi_T \cdot e$ implique que $e \cdot \phi_a = \psi_a \cdot e$ pour tout $a \in A$. En évaluant alors cette relation en $\lambda \in \Lambda$ et par le corollaire 2.2, on trouve que $\phi_a(\lambda) \in \Lambda$ pour tout $a \in A$. Ainsi, Λ est un $\phi(A)$-module discret.

De plus, pour $\lambda \in \Lambda$ non nul, on a $|\lambda| > 1$ (en effet, si l'on a $|\lambda| \leq 1$, alors comme les coefficients de e sont dans $\mathcal{M}$ on aurait $e(\lambda) \in 1 + \mathcal{M}$ et donc $e(\lambda) \neq 0$) et comme les coefficients de $\phi_a(x)$ sont dans $\mathcal{R}$ et que le coefficient dominant est inversbile dans $\mathcal{R}$, on a $|\phi_a(\lambda)| = |\lambda|^{q^{r \deg(a)}}$. Ainsi, Λ est un $\phi(A)$-module sans torsion.

Considérons $a \in A$ de degré strictement positif.
L'équation fonctionnelle $e \cdot \phi_a = \psi_a \cdot e$ donne un diagramme commutatif similaire à (3.5) et de ce diagramme, on obtient le diagramme suivant :

$$0 \longrightarrow \phi[a] \longrightarrow \psi[a] \longrightarrow \Lambda/\phi_a(\Lambda) \longrightarrow 0. \tag{3.12}$$

qui nous donne que $\Lambda/\phi_a(\Lambda) \cong (A/(a))^d$.

Fixons nous désormais S un sous-ensemble fini de Λ qui s'envoie surjectivement sur $\Lambda/\phi_a(\Lambda)$.
Montrons que S engendre Λ :
Pour cela, posons $M := \max_{\lambda \in S} |\lambda|$ ainsi que $m := \min_{\lambda \in \Lambda \setminus \{0_{\mathbb{C}_\mathbb{K}}\}} |\lambda|$ (ces deux quantités sont bien définies, la deuxième à cause du fait que Λ est discret, et strictement plus grandes que 1).
Pour $\lambda \in \Lambda$ quelconque, on peut l'écrire $\lambda = \lambda' + \phi_a(\lambda_1)$ avec $\lambda' \in S$ et $\lambda_1 \in \Lambda$. De plus, on a $|\lambda'| \leq M$ et si $\lambda_1 \neq 0$, alors $|\phi_a(\lambda_1)| \geq m^{q^{r \deg(a)}}$.
Si $\lambda_1 \neq 0$, alors on peut écrire $\lambda_1 = \lambda'' + \phi_a(\lambda_2)$ avec $\lambda'' \in S$ et $\lambda_2 \in \Lambda$, ce qui donne

$$\lambda = \lambda' + \phi_a(\lambda'') + \phi_{a^2}(\lambda_2).$$

De plus, on a $|\lambda' + \phi_a(\lambda'')| \leq M^{q^{r\deg(a)}}$ et si $\lambda_2 \neq 0$, alors $|\phi_{a^2}(\lambda_2)| \geq m^{q^{2r\deg(a)}}$. Enfin, si $\lambda_2 \neq 0$, alors on peut réitérer le processus tant que $\lambda_n \neq 0$. On a alors deux possibilités :

* Si à un certain point on a $\lambda_n = 0$, alors λ peut s'écrire comme une combinaison linéaire d'éléments de S.
* Si $\lambda_n \neq 0$, alors on peut écrire $\lambda = \mu + \phi_{a^n}(\lambda_n)$ avec $|\mu| \leq M^{q^{(n-1)r\deg(a)}}$ et $|\phi_{a^n}(\lambda_n)| \geq m^{q^{nr\deg(a)}}$. Or, comme nous sommes libre de choisir a, on le prend tel que $\frac{\ln(M)}{\ln(m)} < q^{r\deg(a)}$ et puisque $M, m > 1$, on a $\frac{\ln(M)}{\ln(m)} > 0$ et on obtient ainsi

$$M^{q^{(n-1)r\deg(a)}} < m^{q^{nr\deg(a)}}.$$

  Ceci implique donc que $|\lambda| = |\phi_{a^n}(\lambda_n)| \geq m^{q^{nr\deg(a)}}$, or λ est fixé et $m > 1$, donc cette inégalité ne peut pas être vraie pour tout $n \in \mathbb{N}$, donc les λ_n sont nuls à partir d'un certain rang et donc λ peut s'écrire comme une combinaison linéaire d'éléments de S.

Finalement, on a Λ qui est un $\phi(A)$-module libre de rang fini et de plus ce rang est égal à d puisque l'on a $\Lambda/\phi_a\Lambda \cong (A/(a))^d$. Ainsi, à ψ, on a associé une paire (ϕ, Λ) et par l'unicité de e cette paire est unique.

■

Deuxième partie

Étude de l'article

Chapitre 4

Résultats préliminaires

Le but de ce chapitre est de donner tous les résultats préliminaires nécessaire à la preuve du théorème 0.3 (qui sera démontré dans le chapitre 5) ainsi que du théorème 0.4 (qui sera démontré dans le chapitre 6).

Dans les parties I et II on s'intéresse à des critères théoriques de théorie des groupes qui nous donneront des résultats sur le fait qu'un sous-groupe soit égal au groupe tout entier puis qu'il ait le même groupe dérivé. Dans la partie III on s'intéresse à l'image du groupe d'inertie et dans la partie IV on calcule quelques polynômes caractéristiques qui nous seront utiles dans le chapitre 6. Enfin dans la partie V on donne des conditions pour que l'image du groupe de Galois soit la plus grande possible et dans les parties VI et VII on s'intéresse à des résultats d'irréductibilité qui seront utiles dans la sous-partie I.1 du chapitre 4 ainsi que dans le chapitre 5.

I Critère théorique de théorie des groupes sur $\rho_{\phi,\lambda}(\mathrm{Gal}_F)$

Dans toute cette partie on considère $\mathbb{F}_q$ un corps fini à q éléments et $R := \mathbb{F}_q[[\pi]]$ l'anneau des séries formelles en l'indéterminée π. On sait que R est un anneau de valuation discrète, complet, local d'idéal maximal $\mathfrak{p} = (\pi)$ et de corps résiduel $\mathbb{F}_q$.

L'objectif de cette première partie est de démontrer la proposition 4.1 qui sera fondamentale dans la sous-partie I.1 du chapitre 5 et dans le chapitre 6 ainsi que les propositions 4.3 et 4.4 qui nous seront cruciales lorsque nous aborderons la partie II ainsi que la sous-partie I.2 du chapitre 5.

La proposition suivante donne un critère pour vérifier si un sous-groupe de $\mathrm{GL}_2(R)$ est en réalité le groupe tout entier. En particulier, cette proposition donne un critère théorique de théorie des groupes pour vérifier si $\rho_{\phi,\lambda}(\mathrm{Gal}_F)$ est égal au groupe $\mathrm{GL}_2(A_\lambda)$ en entier pour un module de Drinfeld $\phi : A \longrightarrow F\{\tau\}$.

Remarque :
Pour tout idéal premier non nul λ de A, l'anneau A_λ est de la forme $\mathbb{F}_{q,\lambda}[[\pi]]$ (on pourra en trouver une démonstration à la suite du théorème 2 à la page 43 de [Ser04]). On utilisera ce fait par exemple dans la partie II ainsi que la sous-partie I.1 du chapitre 5.

Proposition 4.1 :
Soit G un sous-groupe fermé de $\mathrm{GL}_2(R)$.
Si G vérifie les conditions suivantes :

- $\det(G) = R^\times$;
- L'image de G modulo $\mathfrak{p}$ est $\mathrm{GL}_2(\mathbb{F}_q)$;
- Si $\mathrm{Card}(\mathbb{F}_q) > 2$, alors il existe un élément $I_2 + \pi B$ avec $B \in M_2(R)$ tel que B modulo $\mathfrak{p}$ n'est pas une matrice scalaire dans $M_2(\mathbb{F}_q)$;
- Si $\mathrm{Card}(\mathbb{F}_q) = 2$, alors l'image de G modulo $\mathfrak{p}^2$ est $\mathrm{GL}_2(R/\mathfrak{p}^2)$;
- Si $\mathrm{Card}(\mathbb{F}_q) = 2$, alors $G \cap \mathrm{SL}_2(R)$ contient un élément dont la réduction modulo $\mathfrak{p}$ dans $\mathrm{SL}_2(\mathbb{F}_q)$ est

d'ordre 2,
alors on a $G = \mathrm{GL}_2(R)$.

Cette proposition sera démontrée dans la sous-partie I.3 (on constatera d'ailleurs que lorsque $\mathrm{Card}(\mathbb{F}_q) > 3$, cette proposition est la proposition 4.1 de la page 893 de [PR09a] et on y retrouve certain outils que nous allons utiliser).

I.1 Résultats préliminaires sur les groupes sur un corps fini

Proposition 4.2 :
Soit G un sous-groupe de $\mathrm{GL}_2(\mathbb{F}_q)$.
Si G agit de manière irréductible sur $\mathbb{F}_q^2$ et contient un sous-groupe de cardinal $q := p^n$, alors G contient $\mathrm{SL}_2(\mathbb{F}_q)$.

Preuve :
Soit G un sous-groupe de $\mathrm{GL}_2(\mathbb{F}_q)$.
Supposons que G agit manière irréductible sur $\mathbb{F}_q^2$ et contient un sous-groupe de cardinal $q = p^n$ noté P_1.
Le sous-groupe P_1 est alors un p-Sylow de $\mathrm{GL}_2(\mathbb{F}_q)$ puisque :

$$\mathrm{Card}(\mathrm{GL}_2(\mathbb{F}_q)) = \prod_{k=0}^{2-1} \left(q^2 - q^k\right) = \left(q^2-1\right)\left(q^2-q\right) = p^n \underbrace{\left[\left(p^{2n}-1\right)\left(p^n-1\right)\right]}_{\text{non divisible par } p}.$$

Notons U le sous-groupe de $\mathrm{GL}_2(\mathbb{F}_q)$ constitué des matrices triangulaires supérieures avec des "1" sur la diagonale dans une base de $\mathbb{F}_q^2$ notée (e_1, e_2), c'est-à-dire :

$$U = \left\{ \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix},\ x \in \mathbb{F}_q \right\}.$$

On constate alors que U est aussi un p-Sylow de $\mathrm{GL}_2(\mathbb{F}_q)$ (car isomorphe à $\mathbb{F}_q$ en tant que groupe) et donc par le deuxième théorème de Sylow, P_1 et U sont conjugués entre eux dans $\mathrm{GL}_2(\mathbb{F}_q)$. Autrement dit, il existe $g \in \mathrm{GL}_2(\mathbb{F}_q)$ tel que $P_1 = gUg^{-1}$.

Ainsi, pour tout $p \in P_1$, il existe $u \in U$ tel que l'on ait $p = gug^{-1}$ et donc :

$$p.(g.e_1) = \left(gug^{-1}\right).(g.e_1) = gu.e_1 = g.e_1.$$

Autrement dit, la $\mathbb{F}_q$-droite vectorielle $W_1 = \mathrm{Vect}(g.e_1)$ est fixée par l'action de P_1. De plus, elle est unique puisque s'il en existait une autre notée $\widetilde{W_1}$ alors on aurait $\mathbb{F}_q^2 = W_1 \oplus \widetilde{W_1}$ et dans une base adaptée à cette décomposition, on obtiendrait (à conjugaison près) que les matrices de P sont de la forme

$$\begin{pmatrix} 1 & 0 \\ 0 & x \end{pmatrix},\ x \in \mathbb{F}_q.$$

Or, on a P inclus dans $\mathrm{GL}_2(\mathbb{F}_q)$, donc on a en réalité $x \in \mathbb{F}_q^\times$ et ainsi l'ensemble des matrices de cette forme est de cardinal $q - 1 = p^n - 1$ qui n'est pas un p-Sylow de G. On aboutit alors à une contradiction car la conjugaison est une bijection et donc conserve les cardinaux.

Désormais, si P_1 était distingué dans G, alors W_1 serait stable par l'action de G tout entier puisqu'on aurait

$$\forall \widetilde{g} \in G,\ \widetilde{g}P_1 = P_1\widetilde{g},$$

d'où :

$$\forall \widetilde{g} \in G,\ \widetilde{g}.\left(g.e_1\right) = \widetilde{g}.\left(P_1.\left(g.e_1\right)\right) = P_1\widetilde{g}.\left(g.e_1\right) = P_1.\left(\widetilde{g}.\left(g.e_1\right)\right).$$

Ainsi, P_1 laisse fixe la droite vectorielle engendrée par $\widetilde{g}.g.e_1$ mais puisque P_1 laisse fixe uniquement la droite W_1, on en déduit donc que $\widetilde{g}.g.e_1$ appartient à $W_1 = \mathrm{Vect}(g.e_1)$. Finalement, il existe $\lambda \in \mathbb{F}_q$ tel que l'on ait

l'égalité $\widetilde{g}.(g.e_1) = \lambda(g.e_1)$.

Or cela contredirait notre hypothèse sur l'action de G sur $\mathbb{F}_q^2$, on en déduit que P_1 n'est pas un sous-groupe distingué de $\mathrm{GL}_2(\mathbb{F}_q)$. Donc par le deuxième théorème de Sylow, il existe P_2 un autre sous-groupe de G de cardinal q. Par les mêmes arguments que précédemment, il existe une unique $\mathbb{F}_q$-droite vectorielle W_2 stable par l'action de P_2 et de plus, on a $W_1 \neq W_2$.

Ainsi, il existe $g \in \mathrm{GL}_2(\mathbb{F}_q)$ tel que l'on ait :

$$P_1 = g\left\{\begin{pmatrix}1 & x\\ 0 & 1\end{pmatrix},\ x \in \mathbb{F}_q\right\}g^{-1} \text{ et } P_2 = g\left\{\begin{pmatrix}1 & 0\\ x & 1\end{pmatrix},\ x \in \mathbb{F}_q\right\}g^{-1}.$$

Nous pouvons désormais terminer la preuve en montrant l'inclusion voulue :
On sait que $\mathrm{SL}_2(\mathbb{F}_q)$ est engendré par les transvections, donc pour tout $M \in g\,\mathrm{SL}_2(\mathbb{F}_q)g^{-1}$ on a :

$$M = g\left(\prod_{k=1}^{r} T_{i,j}^{(k)}(\lambda_k)\right)g^{-1} = \prod_{k=1}^{r}\left(gT_{i,j}^{(k)}g^{-1}\right),$$

où les $T_{i,j}^{(k)}$ sont des matrices de transvections.

Or, pour tout $k \in [\![1;r]\!]$, on a $gT_{i,j}^{(k)}g^{-1} \in P_1$ ou P_2, donc $gT_{i,j}^{(k)}g^{-1} \in G$ (car P_1 et P_2 sont des sous-groupes de G). Enfin, comme G est un groupe, on a $M \in G$, d'où $g\,\mathrm{SL}_2(\mathbb{F}_q)g^{-1} \subseteq G$ et puisque $\mathrm{SL}_2(\mathbb{F}_q)$ est distingué dans $\mathrm{GL}_2(\mathbb{F}_q)$ (car noyau du morphisme det), on a $\mathrm{SL}_2(\mathbb{F}_q) = g\,\mathrm{SL}_2(\mathbb{F}_q)g^{-1} \subseteq G$.

■

Lemme 4.1 :

- Si $\mathrm{Card}(\mathbb{F}_q) > 3$, alors le groupe $\mathrm{PSL}_2(\mathbb{F}_q) := \mathrm{SL}_2(\mathbb{F}_q)/\{-I_2; I_2\}$ est simple et non abélien ;
- Si $\mathrm{Card}(\mathbb{F}_q) > 2$, $D(\mathrm{GL}_2(\mathbb{F}_q)) = \mathrm{SL}_2(\mathbb{F}_q)$;
- Si $\mathrm{Card}(\mathbb{F}_q) > 3$, alors $D(\mathrm{SL}_2(\mathbb{F}_q)) = \mathrm{SL}_2(\mathbb{F}_q)$ (autrement dit, $\mathrm{SL}_2(\mathbb{F}_q)$ est un groupe parfait) ;

Ces résultats sont connus et assez classiques. On pourra trouver une démonstration du premier point à la suite du théorème 3.1 de la page 45 de [Wil09] et des deux autres points à la suite du théorème 5.14 à la page 154 de [Rom21].

Désormais, on note $\mathfrak{gl}_2(\mathbb{F}_q) := M_2(\mathbb{F}_q)$ et $\mathfrak{sl}_2(\mathbb{F}_q)$ est le sous-groupe de $M_2(\mathbb{F}_q)$ dont les matrices sont de trace nulle. Ces $\mathbb{F}_q$-espaces vectoriels sont des algèbres de Lie pour le crochet de Lie usuel donné par :

$$\forall x, y \in M_2(\mathbb{F}_q),\ [x,y] := xy - yx.$$

Lemme 4.2 :
Si $\mathrm{Card}(\mathbb{F}_q) > 2$, alors tout sous-groupe de $\mathfrak{gl}_2(\mathbb{F}_q)$ qui est invariant sous l'action de conjugaison par $\mathrm{GL}_2(\mathbb{F}_q)$ contient $\mathfrak{sl}_2(\mathbb{F}_q)$ ou est formé uniquement des matrices scalaires.

Preuve :
Raisonnons par disjonction de cas sur le cardinal de $\mathbb{F}_q$:

- Lorsque $q = p \geq 3$ est un nombre premier, tout sous-groupe de $\mathfrak{gl}_2(\mathbb{F}_p)$ peut-être muni d'une structure de $\mathbb{F}_p$-espace vectoriel et on est alors ramené à chercher les sous-espaces vectoriels de $\mathfrak{gl}_2(\mathbb{F}_p)$ stables sous l'action de conjugaison par $\mathrm{GL}_2(\mathbb{F}_p)$. Or, par l'exercice D.34 à la page 209 de [CG18], on trouve que ces sous-espaces vectoriels sont exactement le sous-espace vectoriel nul, celui des matrices scalaires, celui des matrices de trace nulle et $\mathfrak{gl}_2(\mathbb{F}_p)$ tout entier, ce qui correspond au résultat voulu.

- Dans le cas où $q = p^n$ avec n un entier naturel supérieur ou égal à 2, ce résultat est englobé dans la proposition 2.1 de la page 885 de [PR09a].

■

I.2 Filtration d'un sous-groupe fermé

Dans toute cette partie, on considère G un sous-groupe fermé de $\mathrm{GL}_2(R)$ ainsi que H qui est son sous-groupe dérivé (qui ici est également fermé).

Remarquons tout d'abord qu'ici la topologie considérée n'a pas d'importance. En effet, si $\mathbb{K}$ est un corps valué complet et non discret, alors sur un $\mathbb{K}$-espace vectoriel de dimension finie toutes les normes sont équivalentes. Or ici, le corps des fractions de R est le corps des séries formelles de Laurent (noté $\mathbb{F}_q((\pi))$) et il est encore non discret et complet (car on peut le voir comme un complété de $\mathbb{F}_q(\pi)$). Ainsi, toutes les normes sont équivalentes sur $M_2(\mathbb{F}_q((\pi)))$ et donc on peut en choisir une quelconque et la restreindre sur $\mathrm{GL}_2(R)$. Finalement, les questions d'ouverts ou de fermés qui apparaissent dans la suite de cette partie sont indépendants du choix de la topologie choisie et on l'omettra.

Définition 4.1 : Sous-groupes G^i et H^i :
On considère $i \in \mathbb{N}$.
On appelle :

- G^i le sous-groupe ouvert de G **défini par** $G^i := \left\{g \in G \mid g \equiv I_2 \ \left[\mathfrak{p}^i\right]\right\}$;
- H^i le sous-groupe ouvert de H **défini par** $H^i := \left\{h \in H \mid h \equiv I_2 \ \left[\mathfrak{p}^i\right]\right\} = H \cap G^i$.

Pour tout $i \in \mathbb{N}$, on a alors les groupes quotients

$$G^{[i]} := G^i/G^{i+1} \text{ et } H^{[i]} := H^i/H^{i+1}.$$

De plus, par le théorème de factorisation des morphismes de groupes, on a les deux résultats suivants :

- La réduction modulo $\mathfrak{p}$ induit un morphisme de groupes injectif $\nu_0 : G^{[0]} \longrightarrow \mathrm{GL}_2(\mathbb{F}_q)$.
- De même, pour tout $i \in \mathbb{N}^*$, on a un morphisme de groupes injectif $\nu_i : G^{[i]} \longrightarrow M_2(\mathbb{F}_q) = \mathfrak{gl}_2(\mathbb{F}_q)$ qui envoie $\overline{I_2 + \pi^i B}$ sur B modulo $\mathfrak{p}$.

Définition 4.2 : Sous-groupes $\overline{G}$, $\overline{H}$, $\mathfrak{g}_i$ et $\mathfrak{h}_i$:
On considère $i \in \mathbb{N}^*$.
On définit :

- $\overline{G}$ (respectivement $\overline{H}$) comme étant **l'image de** $G^{[0]}$ (respectivement $H^{[0]}$) **par le morphisme** ν_0 ;
- $\mathfrak{g}_i$ (respectivement $\mathfrak{h}_i$) comme étant **l'image de** $G^{[i]}$ (respectivement $H^{[i]}$) **par le morphisme** ν_i.

Remarque :
Comme on a $H \subseteq \mathrm{SL}_2(R)$, on peut même dire que $\overline{H} \subseteq \mathrm{SL}_2(\mathbb{F}_q)$ et pour tout $i \in \mathbb{N}^*$, $\mathfrak{h}_i \subseteq \mathfrak{sl}_2(\mathbb{F}_q)$.

Soit $i \in \mathbb{N}^*$.
Pour $g = I_2 + \pi^i B \in G^i$, on a $\det(g) \equiv 1 + \pi^i \operatorname{Tr}(B) \ \left[\mathfrak{p}^{i+1}\right]$. En effet, commençons par remarquer que l'on a

$$g = \begin{pmatrix} g_{1,1} & g_{1,2} \\ g_{2,1} & g_{2,2} \end{pmatrix} = \begin{pmatrix} 1 + \pi^i b_{1,1} & \pi^i b_{1,2} \\ \pi^i b_{2,1} & 1 + \pi^i b_{2,2} \end{pmatrix},$$

autrement dit :

$$\forall j, k \in [\![1; 2]\!], \ g_{j,k} = \delta_{j,k} + \pi^i b_{j,k}.$$

En utilisant la définition du déterminant, on obtient que

$$\det(g) = \left(1 + \pi^i b_{1,1}\right)\left(1 + \pi^i b_{2,2}\right) - \pi^{2i} b_{1,2} b_{2,1} = 1 + \pi^i (b_{1,1} + b_{2,2}) + \pi^{2i}(b_{1,1} b_{2,2} - b_{1,2} b_{2,1})$$

et donc modulo $\mathfrak{p}^{i+1}$, on obtient bien :

$$\deg(g) \equiv 1 + \pi^i (b_{1,1} + b_{2,2}) \ \left[\mathfrak{p}^{i+1}\right] \equiv 1 + \pi^i \operatorname{Tr}(B) \ \left[\mathfrak{p}^{i+1}\right].$$

Ainsi, on remarque que pour $g \in G^i$, on a $\det(g) \equiv 1 \ \left[\mathfrak{p}^{i+1}\right]$ si, et seulement si, $\nu_i(\overline{g})$ est de trace nulle, c'est-à-dire appartient à $\mathfrak{sl}_2(\mathbb{F}_q)$.

De plus, on a les deux résultats suivants :

* Les $\mathfrak{g}_i$ et $\mathfrak{h}_i$ sont invariants sous l'action de $\overline{G}$ par conjugaison. En effet, on obtient ce résultat en considérant l'action de conjugaison de G sur les G^i et les H^i :
Par définition des G^i, on remarque qu'ils sont stables par l'action de conjugaison de G et les $G^{[i]}$ sont également stables par l'action de conjugaison de G puisque pour tout $g \in G$ et $h = g_i G^{i+1} \in G^{[i]}$ on a :

$$ghg^{-1} = g\left(g_i G^{i+1}\right) g^{-1} = \underbrace{\left(gg_ig^{-1}\right)}_{\in G^i} \underbrace{gG^{i+1}g^{-1}}_{\in G^{i+1}}.$$

Or, G^{i+1} est distingué dans G (car noyau d'un morphisme de groupes), donc $gG^{i+1}g^{-1} = G^{i+1}$ et ainsi on a bien $ghg^{-1} \in G^i/G^{i+1} = G^{[i]}$. Puisque $G^{[i]}$ est stable par l'action de conjugaison par G, on applique ν_i et on a :

$$\forall g \in G,\ \forall h \in G^{[i]},\ \nu_i\left(ghg^{-1}\right) := \mathrm{Ad}_g(\nu_i(h)),$$

où Ad_g est l'action induite dans $\mathfrak{gl}_2(\mathbb{F}_\lambda)$ par la conjugaison modulo λ. Or, cette action ne dépend que de la classe de g modulo $G^{[1]}$ (puisque $G^{[1]}$ est congru à l'identité modulo λ et donc agit trivialement sur $\mathfrak{gl}_2(\mathbb{F}_\lambda)$). Finalement, l'action de $g \in G$ sur $\mathfrak{g}_i$ ne dépend que de sa classe modulo $G^{[1]}$ et comme $\mathfrak{g}_i = \nu_i\left(G^{[i]}\right)$, cette action préserve $\mathfrak{g}_i$. Par conséquent, $\mathfrak{g}_i$ est stable par l'action de $\overline{G}$ par conjugaison et on peut procéder de la même manière pour les $\mathfrak{h}_i$.

* Pour tout $i \in \mathbb{N}^*$, l'application :

$$d_i : \left| \begin{array}{ccc} G^0 \times G^i & \longrightarrow & H^i \\ (g,h) & \longmapsto & ghg^{-1}h^{-1} \end{array} \right.$$

est bien définie (car H^i est un sous-groupe distingué de G - en tant qu'intersection de deux sous-groupes distingués de G - donc stable par conjugaison) et induit la même application mais de $G^{[0]} \times G^{[i]}$ dans $H^{[i]}$. En effet, considérons $g, g' \in G^0$, $h \in G^1$, $x, x' \in G^i$ et $u \in G^{i+1}$ tels que $g' = gh$ et $x' = xu$. On a :

$$g'x'g'^{-1}x'^{-1} = \underbrace{\left[g\left(hxh^{-1}\right)g^{-1}x^{-1}\right]}_{:=(*)} \underbrace{\left[xg\left(huh^{-1}\right)g^{-1}u^{-1}x^{-1}\right]}_{:=(**)}.$$

Or, on a d'une part que $(*) \equiv gxg^{-1}x^{-1}\ \left[H^{i+1}\right]$ puisque l'on a $hxh^{-1} = xv$ pour un certain $v \in H^{i+1}$ et donc

$$(*) = \left(gxg^{-1}x^{-1}\right)\left((xg)v(xg)^{-1}\right)$$

et puisque H^{i+1} est stable par l'action de conjugaison de G, on a $(xg)v(xg)^{-1} \in H^{i+1}$. D'autre part, on a $(**) \in H^{i+1}$ puisque l'on a $huh^{-1} = uw$ pour un certain $w \in H^{i+2}$ et ainsi

$$(**) = x\ \underbrace{\left(gug^{-1}u^{-1}\right)}_{\in [G^0, G^{i+1}] \subseteq H^{i+1}}\ \underbrace{\left((ug)w(ug)^{-1}\right)}_{\in H^{i+2} \subseteq H^{i+1}} x^{-1}.$$

Enfin, puisque H^{i+1} est un sous-groupe de G, on obtient bien que $(**) \in H^{i+1}$. Par conséquent, on obtient l'application bien définie de $G^{[0]} \times G^{[i]} \longrightarrow H^{[i]}$ souhaitée.
Enfin, on peut associer à cette application :

$$\widetilde{d_i} : \left| \begin{array}{ccc} \overline{G} \times \mathfrak{g}_i & \longrightarrow & \mathfrak{h}_i \\ (g,x) & \longmapsto & gxg^{-1} - x \end{array} \right. \tag{4.1}$$

puisque pour $g \in \overline{G}$ et $x = \nu_i\left(\overline{I_2 + \pi^i x}\right) \in \mathfrak{g}_i$ on a dans $\mathrm{GL}_2(R)$ (en posant $h := I_2 + \pi^i x$) :

$$\begin{aligned}[g,h] = ghg^{-1}h^{-1} &= g(I_2 + \pi^i x)g^{-1}\left(I_2 + \pi^i x\right)^{-1} = \left(I_2 + g\pi^i x g^{-1}\right)\sum_{k=0}^{+\infty}(-1)^k \pi^{ik} x^k \\ &= I_2 + \left(gxg^{-1} - x\right)\pi^i + \text{ termes de plus haut degré en } \pi\end{aligned}$$

et en prenant son image par le morphisme ν_i on trouve bien $gxg^{-1} - x \in \mathfrak{g}_i$. En finalement, puisque $[g,h] \in H$, on a en fait que $gxg^{-1} - x \in \mathfrak{h}_i$.

De même, l'application d_i induit la même application mais cette fois-ci de $G^{[1]} \times G^{[i]}$ dans $H^{[i+1]}$ à laquelle, via ν_0, ν_i et ν_{i+1}, on peut associer l'application :

$$\widehat{d_i} : \left| \begin{array}{ccc} \mathfrak{g}_1 \times \mathfrak{g}_i & \longrightarrow & \mathfrak{h}_i \\ (x,y) & \longmapsto & [x,y] := xy - yx \end{array} \right. . \tag{4.2}$$

Lemme 4.3 :
Si $\mathfrak{g}_1 = \mathfrak{gl}_2(\mathbb{F}_q)$ et $\mathfrak{h}_1 = \mathfrak{sl}_2(\mathbb{F}_q)$, alors H est le sous-groupe de $\mathrm{SL}_2(R)$ des matrices dont l'image modulo $\mathfrak{p}$ appartient à $D\left(\overline{G}\right) \subseteq \mathrm{SL}_2(\mathbb{F}_q)$.

Preuve :
Supposons que $\mathfrak{g}_1 = \mathfrak{gl}_2(\mathbb{F}_q)$ et $\mathfrak{h}_1 = \mathfrak{sl}_2(\mathbb{F}_q)$.
Montrons par récurrence simple que pour tout $i \in \mathbb{N}^*$, $\mathfrak{h}_i = \mathfrak{sl}_2(\mathbb{F}_q)$:

$*$ Initialisation pour $n = 1$:
On a directement que $\mathfrak{h}_1 = \mathfrak{sl}_2(\mathbb{F}_q)$ par hypothèse, la propriété est donc bien initialisée.

$*$ Hérédité :
Supposons que l'on ait $\mathfrak{h}_i = \mathfrak{sl}_2(\mathbb{F}_q)$ pour un certain $i \in \mathbb{N}^*$.
On sait déjà que $\mathfrak{h}_{i+1}$ est contenu dans $\mathfrak{sl}_2(\mathbb{F}_q)$ et par (4.2), on remarque que $\mathfrak{h}_{i+1}$ contient le $\mathbb{F}_q$-espace vectoriel engendré par $[x,y]$ avec $x \in \mathfrak{g}_1 = \mathfrak{gl}_2(\mathbb{F}_q)$ et $y \in \mathfrak{h}_i = \mathfrak{sl}_2(\mathbb{F}_q)$. On obtient alors que $\mathfrak{h}_{i+1} = \mathfrak{sl}_2(\mathbb{F}_q)$ puisque $\mathfrak{sl}_2(\mathbb{F}_q)$ est engendré par

$$\left[\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\right] = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \left[\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}\right] = -\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \text{ et } \left[\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\right] = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}.$$

En effet, $\mathfrak{sl}_2(\mathbb{F}_q)$ est un $\mathbb{F}_q$-espace vectoriel de dimension 3 par le théorème du rang et les trois matrices ci-dessus sont clairement linéairement indépendantes.
La propriété est donc vraie au rang $i+1$, elle est donc héréditaire et on a alors démontré le résultat annoncé par récurrence simple.

De plus, puisque H est un sous-groupe fermé de $\mathrm{SL}_2(R)$ et que pour tout $i \in \mathbb{N}^*$ on a $\mathfrak{h}_i = \mathfrak{sl}_2(\mathbb{F}_q)$, on en déduit que H contient toutes les matrices $A \in \mathrm{SL}_2(R)$ telles que $A \equiv I_2\ [\mathfrak{p}]$. Pour conclure, il suffit de remarquer que $\overline{H} = D\left(\overline{G}\right)$, ce qui nous donne l'inclusion réciproque.

■

Grâce à ces résultats préliminaires, nous pouvons désormais commencer la preuve de la proposition 4.1.

I.3 Preuve de la proposition 4.1

Dans toute cette sous-partie, on reprend les mêmes notations que dans la sous-partie I.2 et on suppose toutes les hypothèses faites dans la proposition 4.1.

Lemme 4.4 :
On a $\mathfrak{g}_1 = \mathfrak{gl}_2(\mathbb{F}_q)$.

Preuve :
Raisonnons par disjonction de cas :

- Si $\mathrm{Card}(\mathbb{F}_q) = 2$, alors on a le résultat par la quatrième hypothèse de la proposition 4.1.
- Si $\mathrm{Card}(\mathbb{F}_q) > 3$, alors le résultat découle de la proposition 4.1 de la page 893 de [PR09a].
- Enfin, supposons que $\mathrm{Card}(\mathbb{F}_q) = 3$.
  D'après la troisième hypothèse de la proposition 4.1, $\mathfrak{g}_1$ contient une matrice qui n'est pas une matrice scalaire et comme $\overline{G} = \mathrm{GL}_2(\mathbb{F}_q)$ (par la deuxième hypothèse de la proposition 4.1), on en déduit que $\mathfrak{g}_1$ est invariant par l'action de $\mathrm{GL}_2(\mathbb{F}_q)$ par conjugaison (en vertu du paragraphe précédant le lemme 4.3).

Par le lemme 4.2, on en déduit que $\mathfrak{sl}_2(\mathbb{F}_q) \subseteq \mathfrak{g}_1$.

Raisonnons par l'absurde en supposant que $\mathfrak{g}_1 \neq \mathfrak{gl}_2(\mathbb{F}_q)$.
On a d'une part que $\mathrm{Card}(\mathfrak{gl}_2(\mathbb{F}_q)) = \mathrm{Card}(M_2(\mathbb{F}_q)) = \mathrm{Card}\left(\mathbb{F}_q^4\right) = q^4 = p^{4n}$, on trouve donc que $\mathrm{Card}(\mathfrak{g}_1)$ divise strictement (par hypothèse) p^{4n}. D'autre part, puisque $\mathfrak{sl}_2(\mathbb{F}_q) \subseteq \mathfrak{g}_1$, on a également $\mathrm{Card}(\mathfrak{g}_1) \geq \mathrm{Card}(\mathfrak{sl}_2(\mathbb{F}_q)) = q^3 = p^{3n}$ et comme p est un nombre premier, cela impose que $\mathrm{Card}(\mathfrak{g}_1) = p^{3n} = q^3$ et donc $\mathfrak{g}_1 = \mathfrak{sl}_2(\mathbb{F}_q)$. Ainsi, en vertu du paragraphe précédant le lemme 4.3, on trouve que pour tout $g \in G^1$, on a $\det(g) \equiv 1 \ \left[\mathfrak{p}^2\right]$ (puisque $\mathfrak{g}_1$ est l'image du morphisme de groupes ν_1).

Posons désormais W le sous-groupe de $\mathrm{GL}_2(R)$ engendré par G^1 et H.
Puisque H est distingué dans G (car $H = D(G)$) et que G^1 est distingué dans $G^0 \cong G$, on obtient par définition du sous-groupe engendré que W est également distingué dans G. De plus, notons que pour tout $g \in W$, $\det(g) \equiv 1 \ \left[\mathfrak{p}^2\right]$ puisque $H \subseteq \mathrm{SL}_2(R)$ et que cette relation est vraie pour tous les éléments $g \in G^1$. Enfin, puisque $\det(G) = R^\times$ (par la première hypothèse de la proposition 4.1) et que $\det(W) \subseteq 1 + \mathfrak{p}^2 R$, on en déduit que $(R/\mathfrak{p}^2)^\times$ est (isomorphe à) un quotient de G/W via l'application $\det : G/W \twoheadrightarrow (R/\mathfrak{p}^2)^\times$ et le premier théorème d'isomorphisme.

Notons désormais $\overline{W}$ l'image de W modulo $\mathfrak{p}$.
On obtient alors

$$\overline{W} = \overline{H} = D\left(\overline{G}\right) = D(\mathrm{GL}_2(\mathbb{F}_q)) = \mathrm{SL}_2(\mathbb{F}_q),$$

où la première égalité résulte de la définition de G^1, la troisième du fait qu'ici $\overline{G} = \mathrm{GL}_2(\mathbb{F}_q)$ et la dernière du deuxième point du lemme 4.1. Or puisque $G^1 \subseteq W$ et que $\overline{W} = \mathrm{SL}_2(\mathbb{F}_q)$, on trouve par passage à la réduction modulo $\mathfrak{p}$ et via l'application det que :

$$G/W \cong \mathrm{GL}_2(\mathbb{F}_q)/\mathrm{SL}_2(\mathbb{F}_q) \cong \mathbb{F}_q^\times.$$

Or on aboutit à une contradiction car comme $(R/\mathfrak{p}^2)^\times$ est un quotient de G/W, le cardinal de G/W est alors strictement plus grand que celui de $\mathbb{F}_q^\times \cong (R/\mathfrak{p})^\times$, ce qui n'est pas le cas ! On en déduit donc que $\mathfrak{g}_1 = \mathfrak{gl}_2(\mathbb{F}_q)$.

■

Lemme 4.5 :
Pour tout $i \in \mathbb{N}^*$, on a $\mathfrak{h}_i = \mathfrak{sl}_2(\mathbb{F}_q)$.

Preuve :
Montrons par récurrence simple que pour tout $i \in \mathbb{N}^*$, on a $\mathfrak{h}_i = \mathfrak{sl}_2(\mathbb{F}_q)$:

$*$ Initialisation pour $i = 1$:
On a $\overline{G} = \mathrm{GL}_2(\mathbb{F}_q)$ par la deuxième hypothèse de la proposition 4.1 ainsi que $\mathfrak{g}_1 = \mathfrak{gl}_2(\mathbb{F}_q)$ par le lemme 4.4. De plus, par (4.1), on a que $\mathfrak{h}_1$ contient le $\mathbb{F}_q$-espace vectoriel engendré par les $gxg^{-1} - x$ avec $g \in \mathrm{GL}_2(\mathbb{F}_q)$ et $x \in \mathfrak{gl}_2(\mathbb{F}_q)$ et en calculant $gxg^{-1} - x$ pour $g \in \left\{\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}; \begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}\right\}$ et $x \in \left\{\begin{pmatrix}0 & 0\\ 0 & 1\end{pmatrix}; \begin{pmatrix}0 & 0\\ 1 & 0\end{pmatrix}\right\}$, on trouve alors que $\mathfrak{sl}_2(\mathbb{F}_q) \subseteq \mathfrak{h}_1$ (par le même argument que dans la preuve du lemme 4.3) et puisque l'autre inclusion est toujours vérifiée, on obtient que $\mathfrak{h}_1 = \mathfrak{sl}_2(\mathbb{F}_q)$.

$*$ Hérédité :
Supposons que l'on ait $\mathfrak{h}_i = \mathfrak{sl}_2(\mathbb{F}_q)$ pour un certain $i \in \mathbb{N}^*$.
On sait déjà que $\mathfrak{h}_{i+1}$ est contenu dans $\mathfrak{sl}_2(\mathbb{F}_q)$ et par (4.2), on remarque que $\mathfrak{h}_{i+1}$ contient le $\mathbb{F}_q$-espace vectoriel engendré par $[x, y]$ avec $x \in \mathfrak{g}_1 = \mathfrak{gl}_2(\mathbb{F}_q)$ et $y \in \mathfrak{h}_i = \mathfrak{sl}_2(\mathbb{F}_q)$. On obtient alors que $\mathfrak{h}_{i+1} = \mathfrak{sl}_2(\mathbb{F}_q)$ puisque $\mathfrak{sl}_2(\mathbb{F}_q)$ est engendré par

$$\left[\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix}, \begin{pmatrix}0 & 1\\ 0 & 0\end{pmatrix}\right] = \begin{pmatrix}0 & 1\\ 0 & 0\end{pmatrix}, \ \left[\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix}, \begin{pmatrix}0 & 0\\ 1 & 0\end{pmatrix}\right] = -\begin{pmatrix}0 & 0\\ 1 & 0\end{pmatrix} \text{ et } \left[\begin{pmatrix}0 & 0\\ 1 & 0\end{pmatrix}, \begin{pmatrix}0 & 1\\ 0 & 0\end{pmatrix}\right] = \begin{pmatrix}-1 & 0\\ 0 & 1\end{pmatrix}.$$

La propriété est donc vraie au rang $i+1$, elle est donc héréditaire.

Finalement, on a donc démontré le résultat voulu par récurrence simple.

■

Lemme 4.6 :
Le groupe dérivé de G coïncide avec le sous-groupe des matrices dans $\mathrm{SL}_2(R)$ dont l'image modulo $\mathfrak{p}$ appartient à $D(\mathrm{GL}_2(\mathbb{F}_q))$.
De plus, si $\mathrm{Card}(\mathbb{F}_q) > 2$, alors $H = \mathrm{SL}_2(R)$.

Preuve :
Notons $\widetilde{H}$ le groupe des matrices dans $\mathrm{SL}_2(R)$ dont l'image modulo $\mathfrak{p}$ appartient à $D(\mathrm{GL}_2(\mathbb{F}_q))$ et pour tout $i \in \mathbb{N}^*$, $\widetilde{H}^i$ le sous-groupe de $\widetilde{H}$ formé des éléments $g \in \widetilde{H}$ tels que $g \equiv I_2 \ \left[\mathfrak{p}^i\right]$.

Puisque $\overline{G} = \mathrm{GL}_2(\mathbb{F}_q)$ (toujours par la même hypothèse), l'image de $\widetilde{H}$ modulo $\mathfrak{p}$ est égale à $D\left(\overline{G}\right) = \overline{H}$. De plus, l'inclusion $H \subseteq \widetilde{H}$ induit un morphisme injectif de H^i/H^{i+1} dans $\widetilde{H}^i/\widetilde{H}^{i+1}$ que l'on peut donc voir comme une inclusion.

Raisonnons désormais par l'absurde en supposant que $H \neq \widetilde{H}$.
Le groupe $\widetilde{H}$ est ouvert dans $\mathrm{SL}_2(R)$ (car image réciproque d'un ouvert par la projection modulo $\mathfrak{p}$), contient H et H est un sous-groupe propre de $\widetilde{H}$ (par hypothèse) qui a la même image modulo $\mathfrak{p}$. Il existe alors un entier $i \in \mathbb{N}^*$ tel que $H^i/H^{i+1} \subsetneq \widetilde{H}^i/\widetilde{H}^{i+1}$. En effet, les $\widetilde{H}^i$ forment une base de voisinage de l'identité dans $\widetilde{H}$ et de plus on a $\widetilde{H}^i/\widetilde{H}^{i+1} \cong \mathfrak{sl}_2(\mathbb{F}_q)$ (comme groupes additifs) et $\widetilde{H}^i = H^i \cap \widetilde{H}$. Or comme on a $H \subsetneq \widetilde{H}$, il existe bien un entier $i \in \mathbb{N}^*$ tel que $H^i/H^{i+1} \subsetneq \widetilde{H}^i/\widetilde{H}^{i+1}$.

Or, puisque $\widetilde{H} \subseteq \mathrm{SL}_2(R)$, on a $\mathfrak{h}_i \neq \mathfrak{sl}_($\mathbb{F}_q$)$, ce qui contredit le lemme 4.5. Ainsi, on a donc bien que $H = H'$.

De plus, si $\mathrm{Card}(\mathbb{F}_q) > 2$, alors $\widetilde{H}$ correspond au groupe des matrices dans $\mathrm{SL}_2(R)$ dont l'image modulo $\mathfrak{p}$ appartient à $D(\mathrm{GL}_2(\mathbb{F}_q)) = \mathrm{SL}_2(\mathbb{F}_q)$ (par le deuxième point du lemme 4.1). Par ce qui précède on a alors $H = \widetilde{H} \subseteq \mathrm{SL}_2(R)$ et puisque l'image de tout élément $\mathrm{SL}_2(R)$ modulo $\mathfrak{p}$ appartient à $\mathrm{SL}_2(R)$ on a finalement $H = \widetilde{H} = \mathrm{SL}_2(R)$.

■

Grâce à ces lemmes, nous pouvons désormais donner la preuve de la proposition 4.1. Pour cela, montrons tout d'abord que $\mathrm{SL}_2(R) \subseteq G$:

- Si $\mathrm{Card}(\mathbb{F}_q) > 2$, alors le lemme 4.6 nous donne que $\mathrm{SL}_2(R) = H \subseteq G$.

- Désormais, si $\mathrm{Card}(\mathbb{F}_q) = 2$, alors on a $\mathrm{GL}_2(\mathbb{F}_q) = \mathrm{SL}_2(\mathbb{F}_q)$ et $D(\mathrm{GL}_2(\mathbb{F}_q)) \cong \mathfrak{A}_3$ (de cardinal 3) et d'indice 2 dans $\mathrm{SL}_2(\mathbb{F}_q)$ (par la formule usuelle du cardinal de $\mathrm{SL}_2(\mathbb{F}_q)$). Par le lemme 4.6, H est le sous-groupe d'indice 2 de $\mathrm{SL}_2(R)$ consistant en l'ensemble des matrices dont la réduction modulo $\mathfrak{p}$ appartient à $D(\mathrm{GL}_2(\mathbb{F}_q))$. Par la dernière hypothèse de la proposition 4.1, il existe un élément $g \in G \cap \mathrm{SL}_2(R)$ dont l'image dans $\mathrm{SL}_2(\mathbb{F}_q)$ par la réduction modulo $\mathfrak{p}$ est d'ordre 2. Ainsi, g représente la classe non triviale de H dans $\mathrm{SL}_2(R)$. Par conséquent, comme H est d'indice 2 dans $\mathrm{SL}_2(R)$, on a la décomposition $SL_2(R) = H \cup gH$ avec $H \subseteq G$ et $gH \subseteq G$ (car $g \in G$) donc on a bien que $\mathrm{SL}_2(R) \subseteq G$.

Enfin, nous pouvons conclure la preuve :
On remarque tout d'abord que $\mathrm{SL}_2(R) \subseteq G$ et que par hypothèse $\det(G) = R^\times$. Ainsi $\mathrm{SL}_2(R) \subsetneq G \subseteq \mathrm{GL}_2(R)$ et par le premier théorème d'isomorphisme appliqué aux morphismes de groupes det et $f := \det|_G$, on a les isomorphismes $\mathrm{GL}_2(R)/\mathrm{SL}_2(R) \cong R^\times$ (dont les classes seront notées $\overline{N}$ pour $N \in \mathrm{GL}_2(R)$) ainsi que $G/\mathrm{SL}_2(R) \cong R^\times$ (dont les classes seront notées $\overline{\overline{N}}$ pour $N \in G$).

Soit $M \in \mathrm{GL}_2(R)$.
On a $\det\left(\overline{M}\right) \in R^\times$, donc il existe $\overline{\overline{N}} \in G/\mathrm{SL}_2(R)$ tel que $\det\left(\overline{M}\right) = \det(\overline{\overline{N}})$. Or, il existe $N \in G$ tel que $\det(M) = \det(N)$ et par conséquent, $\det\left(MN^{-1}\right) = 1$ et ainsi $MN^{-1} \in \mathrm{SL}_2(R) \subseteq G$. Finalement, on a l'égalité $M = \underbrace{\left(MN^{-1}\right)}_{\in G}\underbrace{N}_{\in G} \in G$, c'est-à-dire $\mathrm{GL}_2(R) \subseteq G$ et donc $G = \mathrm{GL}_2(R)$.

I.4 Sous-groupes dérivés de $\mathrm{GL}_2(R)$ et $\mathrm{SL}_2(R)$

Dans cette dernière sous-partie on donne des résultats sur les sous-groupes dérivés de $\mathrm{GL}_2(R)$ et $\mathrm{SL}_2(R)$.

Proposition 4.3 :

- Si $\mathrm{Card}(\mathbb{F}_q) > 2$, alors le groupe dérivé de $\mathrm{GL}_2(R)$ est $\mathrm{SL}_2(R)$;
- Si $\mathrm{Card}(\mathbb{F}_q) = 2$, alors le groupe dérivé de $\mathrm{GL}_2(R)$ est $\{B \in \mathrm{SL}_2(R) \mid \overline{B}$ appartient à $D(\mathrm{GL}_2(\mathbb{F}_q))\}$.
  En particulier, $[\mathrm{SL}_2(R) : D(\mathrm{GL}_2(R))] = 2$.

Preuve :
Posons $G := \mathrm{GL}_2(R)$.
On remarque que G vérifie toutes les hypothèses de la proposition 4.1, donc en particulier celles du lemme 4.6 et donc on obtient que $D(G)$ est le sous-groupe de $\mathrm{SL}_2(R)$ correspondant aux matrices dont l'image par la réduction modulo $\mathfrak{p}$ appartient à $D(\mathrm{GL}_2(\mathbb{F}_q))$.

- Si $\mathrm{Card}(\mathbb{F}_q) = 2$, il ne nous reste plus qu'à démontrer le résultat sur l'indice. Or la définition de $D(G)$ donnée ci-dessus nous montre qu'il y a 2 classes dans le quotient $\mathrm{SL}_2(R)/D(G)$ (respectivement appartenir ou ne pas appartenir à $D(\mathrm{GL}_2(\mathbb{F}_q))$ après réduction modulo $\mathfrak{p}$).

- Si $\mathrm{Card}(\mathbb{F}_q) > 2$, alors par le lemme 4.6, on trouve que $D(G) = H = \mathrm{SL}_2(R)$.

■

Proposition 4.4 :
Si $\mathrm{Card}(\mathbb{F}_q) > 3$, alors :

- Le groupe $\mathrm{SL}_2(R)$ est égal à son propre groupe dérivé ;
- Le seul sous-groupe distingué et fermé de $\mathrm{SL}_2(R)$ dont le quotient est simple est le groupe des matrices $A \in \mathrm{SL}_2(R)$ telles que $A \equiv \pm I_2\ [\mathfrak{p}]$.

Preuve :
Supposons que $\mathrm{Card}(\mathbb{F}_q) > 3$:

- Posons $G := \mathrm{SL}_2(R)$ et H son groupe dérivé.
  En reprenant les mêmes notations que dans la sous-partie I.2, on a $\overline{G} = \mathrm{SL}_2(\mathbb{F}_q)$ et pour tout $i \in \mathbb{N}^*$, $\mathfrak{h}_i \subseteq \mathfrak{g}_i = \mathfrak{sl}_2(\mathbb{F}_q)$ (par le paragraphe précédant le lemme 4.3). De plus, l'image de H par la réduction modulo $\mathfrak{p}$ est
  $$\overline{H} = D\left(\overline{G}\right) = D(\mathrm{SL}_2(\mathbb{F}_q)) = \mathrm{SL}_2(\mathbb{F}_q)$$
  où la dernière égalité provient du troisième point du lemme 4.1.

  Fixons nous un $i \in \mathbb{N}^*$.
  Pour $g = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \in \overline{G}$ et $x = \begin{pmatrix} 0 & -1 \\ 0 & 0 \end{pmatrix} \in \mathfrak{g}_i$, on obtient que la matrice $gxg^{-1} - x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ appartient à $\mathfrak{h}_i$ via (4.1). Ainsi, on a $\mathfrak{h}_i \subseteq \mathfrak{sl}_2(\mathbb{F}_q)$ qui contient une matrice non scalaire et qui est stable par l'action de $\mathrm{GL}_2(\mathbb{F}_q)$ par conjugaison (puisque G est un sous-groupe de $\mathrm{GL}_2(R)$ qui est distingué). Par le lemme 4.2, on a alors $\mathfrak{h}_i = \mathfrak{sl}_2(\mathbb{F}_q)$.
  Nous avons donc montré que H est un sous-groupe fermé de $\mathrm{SL}_2(R)$ pour lequel $\overline{H} = \mathrm{SL}_2(\mathbb{F}_q)$ et pour tout $i \in \mathbb{N}^*$, $\mathfrak{h}_i = \mathfrak{sl}_2(\mathbb{F}_q)$, on a donc finalement que $H = \mathrm{SL}_2(R)$ puisque H est fermé.

∗ Soit N un sous-groupe distingué et fermé de $\mathrm{SL}_2(R)$ pour lequel $S := \mathrm{SL}_2(R)/N$ est simple.
Puisque S est simple et profini, il est fini. En effet, S est non trivial et on peut donc choisir $g \in S$ qui n'est pas l'élément neutre. De plus S est séparé (car N est fermé) donc il existe un voisinage ouvert U de l'identité ne contenant pas g et comme G est profini il existe un sous-groupe distingué ouvert T de S contenu dans U. Ainsi on a $T \neq S$ et donc par simplicité T est le groupe trivial. Finalement, $\{e_S\}$ est un ouvert donc tout point de S est ouvert, d'où S est discret et comme il est compact il est donc fini.

Posons $\varphi : \mathrm{SL}_2(R) \longrightarrow S$ l'application quotient et W le sous-groupe de $\mathrm{SL}_2(R)$ constitué des matrices $A \in \mathrm{SL}_2(R)$ telles que $A \equiv \pm I_2\ [\mathfrak{p}]$.
Le groupe S est non abélien puisque $\mathrm{SL}_2(R)$ est égal à son groupe dérivé (par le premier point) et que φ est surjective et de plus W est distingué et fermé (car noyau de l'application $\mathrm{SL}_2(R) \longrightarrow \mathrm{SL}_2(\mathbb{F}_q)/\{\pm I_2\}$). De plus, le groupe W est prorésoluble car $W = \varprojlim_{n\in\mathbb{N}} W_n$ (où $W_n := \mathrm{Ker}(\mathrm{SL}_2(R/T^n) \longrightarrow \mathrm{SL}_2(\mathbb{F}_q)/\{\pm I_2\})$) et les W_n sont des groupes nilpotents donc résolubles et finis. Par conséquent, $\varphi(W)$ est un sous-groupe distingué (car φ est surjective) et résoluble de S. On a alors $\varphi(W) = \{e_S\}$ puisque S est simple et non abélien. On a alors $W \subseteq N$ et $\mathrm{SL}_2(R)/W \cong \mathrm{SL}_2(\mathbb{F}_q)/\{-I_2; I_2\}$ qui est simple (par le premier point du lemme 4.1). Finalement, par la correspondance entre les sous-groupes et les sous-groupes quotients, on en déduit que $W = N$.

■

II Critère théorique de théorie des groupes sur $\mathrm{GL}_2(\widehat{A})$

Dans toute cette partie, on considère G un sous-groupe de $\mathrm{GL}_2(\widehat{A})$, $H = D(G)$ qui est un sous-groupe fermé de $\mathrm{SL}_2(\widehat{A})$ et pour un idéal non nul $\mathfrak{a}$ de A, on note $G_\mathfrak{a}$ (respectivement $H_\mathfrak{a}$) l'image de G (respectivement H) par la projection canonique $\pi : \mathrm{GL}_2(\widehat{A}) \longrightarrow \mathrm{GL}_2(A_\mathfrak{a})$.

L'objectif de cette deuxième partie est de démontrer le théorème 4.1 (qui donne des conditions assurant que G et $\mathrm{GL}_2(\widehat{A})$ ont le même groupe dérivé) que nous utiliserons dans la sous-partie I.1 du chapitre 5 ainsi que dans le chapitre 6.

Théorème 4.1 :
Soit G un sous-groupe fermé de $\mathrm{GL}_2(\widehat{A})$.
Si G vérifie les conditions suivantes :

∗ Pour tout $\lambda \in \mathrm{Spec}(A)\backslash\{(0_A)\}$, on a $\mathrm{SL}_2(A_\lambda) \subseteq G_\lambda$;

∗ Pour tous $\lambda_1, \lambda_2 \in \mathrm{Spec}(A)\backslash\{(0_A)\}$ distincts tels que $N(\lambda_1) = N(\lambda_2) > 3$, G modulo $\lambda_1\lambda_2$ a un sous-groupe de cardinal $N(\lambda_1)^2$;

∗ Pour tous $\lambda_1, \lambda_2 \in \mathrm{Spec}(A)\backslash\{(0_A)\}$ distincts tels que $N(\lambda_1) = N(\lambda_2) = 2$, le groupe $G_{\lambda_1\lambda_2} \cap \mathrm{SL}_2(A_{\lambda_1\lambda_2})$ contient un sous-groupe qui est conjugué dans $\mathrm{GL}_2(A_{\lambda_1\lambda_2})$ à $\left\{\begin{pmatrix}1 & b\\ 0 & 1\end{pmatrix},\ b \in A_{\lambda_1\lambda_2}\right\}$;

∗ Si $q \in \{2;3\}$ et $\mathfrak{a}$ est l'idéal qui est le produit d'idéaux premiers de A de norme q, alors $\det(G_\mathfrak{a}) = A_\mathfrak{a}^\times$,

alors $D(G) = D\left(\mathrm{GL}_2(\widehat{A})\right)$.
En particulier, lorsque $q > 2$, on a $D(G) = \mathrm{SL}_2(\widehat{A})$.

Afin de démontrer ce théorème, nous allons avoir besoin de quelques lemmes préliminaires.

Dans toute la suite de cette partie, on suppose vérifiées les hypothèses du théorème 4.1.

Lemme 4.7 :
Soient λ_1 et λ_2 des idéaux premiers distincts et non nuls de A.
Si $N(\lambda_1), N(\lambda_2) \geq 4$, alors $H_{\lambda_1\lambda_2} = \mathrm{SL}_2(A_{\lambda_1}) \times \mathrm{SL}_2(A_{\lambda_2})$.

Preuve :
Soient λ_1 et λ_2 des idéaux premiers distincts et non nuls de A.
Supposons que $N(\lambda_1), N(\lambda_2) \geq 4$.
Pour tout $i \in \{1;2\}$, on a $\mathrm{SL}_2(A_{\lambda_i}) \subseteq G_{\lambda_i}$ par la première hypothèse du théorème 4.1 et puisque $\mathrm{SL}_2(A_{\lambda_i})$ est parfait (on peut appliquer le premier point de la proposition 4.4 car $\mathrm{Card}(A_{\lambda_i}) \geq 4$ et grâce à la remarque du début de la partie I) on a alors $H_{\lambda_i} := D(G_{\lambda_i}) = \mathrm{SL}_2(A_{\lambda_i})$ (l'une des deux inclusions étant par définition de H_{λ_i} et l'autre résultant de ce qui précède). On a alors l'inclusion de groupes $H_{\lambda_1\lambda_2} \subseteq H_{\lambda_1} \times H_{\lambda_2} = \mathrm{SL}_2(A_{\lambda_1}) \times \mathrm{SL}_2(A_{\lambda_2})$ de telle sorte que chaque projection $p_i : H_{\lambda_1\lambda_2} \longrightarrow \mathrm{SL}_2(A_{\lambda_i})$ est surjective.

Notons N_1 et N_2 les noyaux de respectivement p_2 et p_1.
On peut identifier N_1 et N_2 à des sous-groupes distingués et fermés de respectivement $\mathrm{SL}_2(A_{\lambda_1})$ et $\mathrm{SL}_2(A_{\lambda_2})$ (car noyaux de morphismes de groupes continus et surjectif) et on a l'inclusion $N_1 \times N_2 \subseteq H_{\lambda_1\lambda_2}$.

Par le lemme de Goursat (dont on pourra trouver un énoncé ainsi qu'une preuve au lemme 5.2.1 de la page 793 de [Rib76]), l'inclusion $H_{\lambda_1\lambda_2} \subseteq \mathrm{SL}_2(A_{\lambda_1}) \times \mathrm{SL}_2(A_{\lambda_2})$ induit un morphisme

$$H_{\lambda_1\lambda_2}/(N_1 \times N_2) \hookrightarrow \mathrm{SL}_2(A_{\lambda_1})/N_1 \times \mathrm{SL}_2(A_{\lambda_2})/N_2$$

dont l'image est le graphe de l'isomorphisme $\mathrm{SL}_2(A_{\lambda_1})/N_1 \cong \mathrm{SL}_2(A_{\lambda_2})/N_2$.

Raisonnons désormais par disjonction de cas :

* Si le groupe quotient $\mathrm{SL}_2(A_{\lambda_1})/N_1$ est trivial, alors par l'isomorphisme précédent, on obtient que pour tout $i \in \{1;2\}$, $\mathrm{SL}_2(A_{\lambda_i}) = N_i$ et donc :

  $$\mathrm{SL}_2(A_{\lambda_1}) \times \mathrm{SL}_2(A_{\lambda_2}) = N_1 \times N_2 \subseteq H_{\lambda_1\lambda_2} \subseteq \mathrm{SL}_2(A_{\lambda_1}) \times \mathrm{SL}_2(A_{\lambda_2}).$$

  On obtient alors le résultat désiré.

* Si le groupe quotient $\mathrm{SL}_2(A_{\lambda_1})/N_1$ n'est pas trivial, alors N_1 et N_2 sont des sous-groupes distingués et fermés stricts de respectivement $\mathrm{SL}_2(A_{\lambda_1})$ et $\mathrm{SL}_2(A_{\lambda_2})$. Or, pour tout $i \in \{1;2\}$, on a $N(\lambda_i) \geq 4$, donc en appliquant le deuxième point de la proposition 4.4 avec $R := A_{\lambda_i}$, on obtient :

  $$N_i \subseteq \{B \in \mathrm{SL}_2(A_{\lambda_i}) \mid B \equiv \pm I_2\ [\lambda_i]\}.$$

  Ainsi, le morphisme :

  $$H_{\lambda_1\lambda_2} \longrightarrow \mathrm{SL}_2(\mathbb{F}_{\lambda_1})/\{-I_2; I_2\} \times \mathrm{SL}_2(\mathbb{F}_{\lambda_2})/\{-I_2; I_2\},$$

  obtenu en composant la réduction modulo $\lambda_1\lambda_2$ avec la projection, a pour image le graphe de l'isomorphisme de groupes finis simples $\mathrm{SL}_2(\mathbb{F}_{\lambda_1})/\{-I_2; I_2\} \cong \mathrm{SL}_2(\mathbb{F}_{\lambda_2})/\{-I_2; I_2\}$ (par le premier point du lemme 4.1 puisque $N(\lambda_1), N(\lambda_2) \leq 4$). En comparant alors les cardinaux des isomorphismes précédents et en utilisant le fait que la suite $q \longmapsto \mathrm{Card}(\mathrm{SL}_2(\mathbb{F}_q))$ est strictement croissante on trouve que $N(\lambda_1) = N(\lambda_2)$.

  Considérons désormais le morphisme

  $$\varphi : G_{\lambda_1\lambda_2} \longrightarrow \mathrm{SL}_2(\mathbb{F}_{\lambda_1})/\{-I_2; I_2\} \times \mathrm{SL}_2(\mathbb{F}_{\lambda_2})/\{-I_2; I_2\},$$

  obtenu en composant la réduction modulo $\lambda_1\lambda_2$ avec la projection.
  Par la deuxième hypothèse du théorème 4.1, $\varphi(G_{\lambda_1\lambda_2})$ contient un sous-groupe dont le cardinal est $N(\lambda_1)^2 = N(\lambda_1)N(\lambda_2)$ et qui est un p-Sylow de $\mathrm{SL}_2(\mathbb{F}_{\lambda_1})/\{-I_2; I_2\} \times \mathrm{SL}_2(\mathbb{F}_{\lambda_2})/\{-I_2; I_2\}$ (avec p le

nombre premier divisant q). En effet, on a :

$$\begin{aligned}
&\mathrm{Card}\left(\mathrm{SL}_2\left(\mathbb{F}_{\lambda_1}\right)/\{-I_2;I_2\}\times \mathrm{SL}_2\left(\mathbb{F}_{\lambda_2}\right)/\{-I_2;I_2\}\right) \underset{N(\lambda_1)=N(\lambda_2)}{=} \mathrm{Card}\left(\mathrm{SL}_2\left(\mathbb{F}_{\lambda_1}\right)/\{-I_2;I_2\}\right)^2\\
&= \frac{1}{4}\prod_{k=0}^{1}\left(N(\lambda_1)^2-N(\lambda_1)^k\right)^2 = \frac{1}{4}\left(N(\lambda_1)^2-1\right)^2\left(N(\lambda_1)^2-N(\lambda_1)\right)^2\\
&= \frac{N(\lambda_1)N(\lambda_2)}{4}\underbrace{\left(N(\lambda_1)^2-1\right)^2\left(N(\lambda_1)-1\right)^2}_{\text{non divisible par } p}
\end{aligned}$$

En particulier, il existe $g \in G_{\lambda_1\lambda_2}$ tel que $\varphi(g) = (I_2, g_2)$ avec $g_2 \in \mathrm{GL}_2(\mathbb{F}_{\lambda_2})/\{-I_2;I_2\}$ d'ordre une puissance non nulle de p. De plus, nous avons montré que $\varphi(H_{\lambda_1\lambda_2})$ est le graphe de l'isomorphisme $\mathrm{SL}_2\left(\mathbb{F}_{\lambda_1}\right)/\{-I_2;I_2\} \cong \mathrm{SL}_2\left(\mathbb{F}_{\lambda_2}\right)/\{-I_2;I_2\}$. Ainsi, il existe un élément $(h_1, h_2) \in \varphi(H_{\lambda_1\lambda_2})$ pour lequel h_2 et g_2 ne commutent pas (un élément de $\mathrm{GL}_2(\mathbb{F}_{\lambda_2})/\{-I_2;I_2\}$ qui commute avec $\mathrm{SL}_2(\mathbb{F}_{\lambda_2})/\{-I_2;I_2\}$ serait représenté par une matrice scalaire et donc aurait pour ordre un nombre premier à p). Or, comme H est distingué dans G, on obtient :

$$(I_2, g_2)(h_1, h_2)(I_2, g_2)^{-1} = \left(h_1, g_2h_2g_2^{-1}\right) \in \varphi(H_{\lambda_1\lambda_2}).$$

Enfin, puisque $(h_1, g_2h_2g_2^{-1})$ et (h_1, h_2) sont des éléments distincts de $\varphi(H_{\lambda_1\lambda_2})$, cela contredit le fait que le groupe $\varphi(H_{\lambda_1\lambda_2})$ est le graphe d'une fonction.

■

Lemme 4.8 :
Soient $r \in \mathbb{N}^*$, $S_1, \ldots, S_r$ des groupes profinis qui sont parfaits et H un sous-groupe fermé de $S_1 \times \cdots \times S_r$. Si pour tous $1 \leq i < j \leq r$ la projection $H \longrightarrow S_i \times S_j$ est surjective, alors $H = S_1 \times \cdots \times S_r$.

Preuve :
Soient $r \in \mathbb{N}^*$, $S_1, \ldots, S_r$ des groupes profinis qui sont parfaits et H un sous-groupe fermé de $S_1 \times \cdots \times S_r$. Supposons que pour tous $1 \leq i < j \leq r$ la projection $H \longrightarrow S_i \times S_j$ est surjective.
Le cas où les S_i sont des groupes finis et parfaits résulte du lemme 5.2.2 à la page 793 de [Rib76]. Le cas général s'obtient alors en écrivant les S_i comme des limites projectives et en utilisant le fait que H est fermé.

En effet, pour tout $i \in [\![1; r]\!]$, S_i est un groupe profini et parfait, donc S_i est la limite projective de groupes finis discrets :

$$S_i = \varprojlim_{N_i \lhd S_i} S_i/N_i$$

où les N_i sont les sous-groupes ouverts distingués de S_i et S_i/N_i est un groupe fini parfait. On a alors :

$$\prod_{i=1}^{r} S_i = \varprojlim_{N_1,\ldots,N_r} \prod_{i=1}^{r} (S_i/N_i)$$

et de même le sous-groupe fermé H est la limite projective de ses images $H_{(N_1,\ldots,N_r)}$ dans les groupes finis $\prod_{i=1}^{r}(S_i/N_i)$. De plus, chaque des images $H_{(N_1,\ldots,N_r)}$ est un sous-groupe d'un produit fini de groupes finis parfaits et les projections $H \longrightarrow S_i \times S_j$ sont surjectives donc leurs images modulo N_i et N_j donnent $H_{(N_1,\ldots,N_r)} \longrightarrow S_i/N_i \times S_j/N_j$ qui sont encore surjectives (car la projection canonique est continue et ouverte).

Ainsi, chaque image $H_{(N_1,\ldots,N_r)}$ vérifie les hypothèses du lemme dans le cas fini et donc on a l'égalité $H_{(N_1,\ldots,N_r)} = \prod_{i=1}^{r} S_i/N_i$. Par conséquent, on a donc :

$$H = \varprojlim_{N_1,\ldots,N_r} H_{(N_1,\ldots,N_r)} = \varprojlim_{N_1,\ldots,N_r} \prod_{i=1}^{r} S_i/N_i = \prod_{i=1}^{r} \varprojlim_{N_1,\ldots,N_r} S_i/N_i = \prod_{i=1}^{r} S_i.$$

■

Lemme 4.9 :
Soit Λ_1 l'ensemble des idéaux premiers de A non nuls de norme au moins 4.
La projection $H \longrightarrow \prod_{\lambda\in\Lambda_1} \mathrm{SL}_2(A_\lambda)$ est surjective.

Preuve :
Soit Λ_1 l'ensemble des idéaux premiers de A non nuls de norme au moins 4.
Considérons I un sous-ensemble non vide et fini de Λ_1 de cardinal au moins 2.
Par le premier point de la proposition 4.4, le groupe $\mathrm{SL}_2(A_\lambda)$ est parfait pour tout $\lambda \in \Lambda_1$. De plus, pour $\lambda_1, \lambda_2 \in I$ distincts (possible car $\mathrm{Card}(\Lambda_1) \geq 2$), la projection $H \longrightarrow \mathrm{SL}_2(A_{\lambda_1}) \times \mathrm{SL}_2(A_{\lambda_2})$ est surjective par le lemme 4.7. Ainsi, par le lemme 4.8, la projection $H \longrightarrow \prod_{\lambda\in I} \mathrm{SL}_2(A_\lambda)$ est surjective.

Finalement, en augmentant le cardinal de I on trouve que H est dense dans $\prod_{\lambda\in\Lambda_1} \mathrm{SL}_2(A_\lambda)$ (car l'ensemble des projections partielles sur des produits finis forme une base de voisinage de l'identité pour la topologie de $\prod_{\lambda\in\Lambda_1} \mathrm{SL}_2(A_\lambda)$) et puisque H est un sous-groupe fermé de $\mathrm{SL}_2(\widehat{A}) = \prod_{\lambda\in\mathrm{Spec}(A)\setminus\{(0_A)\}} \mathrm{SL}_2(A_\lambda)$, on aboutit au résultat.

■

Lemme 4.10 :
Soit Λ_2 l'ensemble des idéaux premiers de A non nuls de norme au plus 3.
La projection $H \longrightarrow \prod_{\lambda\in\Lambda_2} D(\mathrm{GL}_2(A_\lambda))$ est surjective.

Preuve :
Soit Λ_2 l'ensemble des idéaux premiers de A non nuls de norme au plus 3.
On peut supposer sans perte de généralités que Λ_2 est non vide (car dans le cas contraire le résultat est immédiat) et donc supposer que $q \in \{2; 3\}$. Afin de démontrer le lemme, nous allons montrer que la projection $G \longrightarrow \prod_{\lambda\in\Lambda_2} \mathrm{GL}_2(A_\lambda)$ est surjective (on obtient alors le résultat en prenant les groupes dérivés).

Pour cela, raisonnons par l'absurde en supposant que la projection n'est pas surjective :
Il existe un ensemble non vide minimal $\Lambda_2' \subseteq \Lambda_2$ pour lequel la projection $G \longrightarrow \prod_{\lambda\in\Lambda_2'} \mathrm{GL}_2(A_\lambda)$ n'est pas surjective et on note B son image. De plus, pour tout $\lambda \in \Lambda_2'$ on a $G_\lambda = \mathrm{GL}_2(A_\lambda)$ par la première et la quatrième hypothèse du théorème 4.1 et ainsi $\mathrm{Card}(\Lambda_2') \geq 2$ (car il faut donc au moins deux éléments pour faire échouer la surjectivité).

Donnons nous désormais une place $\lambda_1 \in \Lambda_2'$ et posons $B_1 := \mathrm{GL}_2(A_{\lambda_1})$ et $B_2 := \prod_{\lambda\in\Lambda_2'\setminus\{\lambda_1\}} \mathrm{GL}_2(A_\lambda)$ (le produit étant non vide car $\mathrm{Card}(\Lambda_2') \geq 2$).
On peut alors voir B comme un sous-groupe du groupe produit $B_1 \times B_2$ et les projections $p_1 : B \longrightarrow B_1$ et $p_2 : B \longrightarrow B_2$ sont surjectives par minimalité de Λ_2'. En notant alors N_1 et N_2 les noyaux respectifs de p_2 et p_1, il est possible de les voir comme des sous-groupes de respectivement B_1 et B_2 et donc $N_1 \times N_2 \subseteq B$. Ainsi, par le lemme de Goursat (dont on pourra trouver un énoncé ainsi qu'une preuve au lemme 5.2.1 de la page 793 de [Rib76]), l'image de l'application quotient $G \longrightarrow B_1/N_1 \times B_2/N_2$ est le graphe de l'isomorphisme $B_1/N_1 \cong B_2/N_2$.

Si de plus B_1/N_1 ou B_2/N_2 est trivial, alors on a $N_1 = B_1$ et $N_2 = B_2$ et par conséquent on a l'inclusion $B_1 \times B_2 = \prod_{\lambda\in\Lambda_2'} \mathrm{GL}_2(A_\lambda) \subseteq B$ ce qui contredirait notre choix de Λ_2'. Ainsi, on peut supposer que les N_i sont des sous-groupes propres des B_i et de plus ils sont fermés et distingués (car noyaux de morphismes de groupes continus). Il existe alors des sous-groupes propres fermés et distingués M_i des B_i tels que $N_i \subseteq M_i$ et l'image $G \longrightarrow B_1/M_1 \times B_2/M_2$ est le graphe de l'isomorphisme de groupes finis simples $B_1/M_1 \cong B_2/M_2$. Or le groupe B_1 est prorésoluble. En effet, on a :

$$B_1 = \mathrm{GL}_2(A_{\lambda_1}) \cong \mathrm{GL}_2(A/\lambda_1[[\pi]]) \cong \varprojlim_{i\in\mathbb{N}^*} \underbrace{\mathrm{GL}_2\left((A/\lambda_1)[[\pi]]/(\pi)^i\right)}_{:=B_{1,i}}$$

De plus, l'application $\pi : B_{1,i} \longrightarrow \mathrm{GL}_2(\mathbb{F}_q)$ qui consiste à réduire les coefficients modulo π est une surjection de noyau $U := \{M \in \mathrm{GL}_2(B_{1,i}) \mid M \equiv I_2\ [\pi]\}$, ce qui nous donne la suite extacte courte

$$0 \longrightarrow U \overset{\iota}{\hookrightarrow} B_{1,i} \overset{\pi}{\twoheadrightarrow} \mathrm{GL}_2(\mathbb{F}_q) \longrightarrow 0.$$

Mais ici $\mathrm{GL}_2(\mathbb{F}_q)$ est résoluble car $q \in \{2;3\}$ (on peut le vérifier en étudiant la suite des groupes dérivée) et U est un p-groupe (par le premier théorème d'isomorphisme) donc il est nilpotent et donc résoluble. Enfin, puisqu'une extension d'un groupe résoluble par un autre groupe résoluble est encore un groupe résoluble, on en déduit que les $B_{1,i}$ sont tous résolubles et ainsi que B_1 est bien un groupe prorésoluble. Enfin, B_1/M_1 est résoluble (car quotient d'un groupe résoluble) et puisqu'il est simple on en déduit qu'il est commutatif, ce qui impose que B_1/M_1 soit un groupe d'ordre premier (et donc cyclique).

Terminons la preuve en raisonnant par disjonction de cas sur q :

- Supposons que $q = 3$:
  Puisque les B_i/M_i sont abéliens, on a par le premier point de la proposition 4.4 que $\mathrm{SL}_2(A_{\lambda_1}) \subseteq M_1$ et $\prod_{\lambda \in \Lambda_2' \setminus \{\lambda_1\}} \mathrm{SL}_2(A_\lambda) \subseteq M_2$. Or puisque le morphisme $G \longrightarrow B_1/M_1 \times B_2/M_2$ n'est pas surjectif, on en déduit que la projection $\det(G) \longrightarrow \prod_{\lambda \in \Lambda_2'} A_\lambda^\times$ n'est pas surjective, ce qui contredit la dernière hypothèse du théorème 4.1.

- Supposons maintenant que $q = 2$:
  On a alors $\Lambda_2 = \Lambda_2' = \{\lambda_1; \lambda_2\}$ et puisque chaque quotient B_i/M_i est abélien et $B_i = \mathrm{GL}_2(A_{\lambda_i})$, on a $D\left(\mathrm{GL}_2(A_{\lambda_i})\right) \subseteq M_i$. Par la troisième hypothèse du théorème 4.1, il existe $g \in G_{\lambda_1\lambda_2} \cap \mathrm{SL}_2(A_{\lambda_1\lambda_2})$ dont la projection g_1 dans $\mathrm{GL}_2(A_{\lambda_1\lambda_2})$ modulo λ_1 est d'ordre 2 et dont la projection dans $\mathrm{GL}_2(A_{\lambda_2})$ est I_2 (concrètement on prend $b \in A_{\lambda_1\lambda_2}$ tel que $b \equiv 1\ [\lambda_1]$ et $b \equiv 0\ [\lambda_2]$). On a donc $g_1 \in N_1 \subseteq M_1$ et en utilisant le deuxième point de la proposition 4.3 on obtient que $\mathrm{SL}_2(A_{\lambda_1})$ est engendré par g_1 et $D\left(A_{\lambda_1}\right)$, d'où $\mathrm{SL}_2(A_{\lambda_1}) \subseteq M_1$.
  Par un argument identique on trouve que $\mathrm{SL}_2(A_{\lambda_2}) \subseteq M_2$ et puisque le morphisme $G \longrightarrow B_1/M_1 \times B_2/M_2$ n'est pas surjectif, la projection $\det(G) \longrightarrow \prod_{\lambda \in \Lambda_2'} A_\lambda^\times$ n'est pas surjective, ce qui contredit la dernière hypothèse du théorème 4.1.

■

Nous pouvons désormais donner la preuve du théorème 4.1 :
Posons $B_1 := \prod_{\lambda \in \Lambda_1} \mathrm{SL}_2(A_\lambda)$ et $B_2 := \prod_{\lambda \in \Lambda_2} D\left(\mathrm{GL}_2(A_\lambda)\right)$.
On a les inclusions naturelles (à l'identification près) :

$$\begin{aligned} H \subseteq D\left(\mathrm{GL}_2(\widehat{A})\right) \cong D\left(\mathrm{GL}_2\left(\prod_{\mathfrak{p} \in \mathrm{Spec}(A) \setminus \{(0_A)\}} A_\mathfrak{p}\right)\right) &= \prod_{\mathfrak{p} \in \mathrm{Spec}(A) \setminus \{(0_A)\}} D\left(\mathrm{GL}_2(A_\mathfrak{p})\right) \\ = \prod_{\lambda \in \Lambda_1 \sqcup \Lambda_2} D\left(\mathrm{GL}_2(A_\mathfrak{p})\right) &= B_1 \times B_2, \end{aligned}$$

où l'on a utilisé le premier point de la proposition 4.3 dans la dernière égalité. De plus, les projections $H \longrightarrow B_1$ et $H \longrightarrow B_2$ sont surjectives par les lemmes 4.9 et 4.10.

Supposons que H est un sous-groupe propre de $B_1 \times B_2$.
Par le lemme de Goursat (dont on pourra trouver un énoncé ainsi qu'une preuve au lemme 5.2.1 de la page 793 de [Rib76]), il existe deux sous-groupes N_1 et N_2 qui sont distingués, fermés et propres de respectivement B_1 et B_2 pour lesquels on a un isomorphisme $B_1/N_1 \cong B_2/N_2$.

Ainsi il existe un groupe fini et simple Q qui est un quotient à la fois de B_1 et B_2 (la construction est la même que celle faite dans la preuve du lemme 4.10) et puisque B_1 est un groupe parfait (par le premier point de la proposition 4.4) on obtient que Q est non-abélien. De plus B_2 est un groupe prorésoluble (même construction que dans la preuve du lemme 4.10) donc Q est cyclique et d'ordre premier, ce qui contredit le fait que Q est non-abélien.

Par conséquent, on a $H = B_1 \times B_2 = D\left(\mathrm{GL}_2(\widehat{A})\right)$. En particulier pour $q > 2$, on a $D\left(\mathrm{GL}_2(\widehat{A})\right) = \mathrm{SL}_2(\widehat{A})$ par le premier point de la proposition 4.3 et donc $H = \mathrm{SL}_2(\widehat{A})$.

III Corps locaux et image du groupe d'inertie

Dans toute cette partie, on considère $\mathfrak{p}$ un idéal premier non nul de A et $\mathbb{K}$ une extension finie séparable de $F_{\mathfrak{p}}$ que l'on considère comme un A-corps via les inclusions $A \subseteq F_{\mathfrak{p}} \subseteq \mathbb{K}$.

La clôture intégrale de $A_{\mathfrak{p}}$ dans $\mathbb{K}$ est un anneau de valuation discrète $\mathcal{O}$ qui est complet, dont l'idéal maximal sera noté $\mathfrak{m}$ et dont le corps résiduel est $\mathbb{F} := \mathcal{O}/\mathfrak{m}$. On pose ainsi $v : \mathbb{K}^\times \longrightarrow \mathbb{Z}$ la valuation discrète correspondant à $\mathcal{O}$ normalisée telle que $v\left(\mathbb{K}^\times\right) = \mathbb{Z}$ et on prolonge v en 0 par $v(0) = +\infty$. Enfin, on notera encore v la valuation correspondante dans une clôture séparable fixée $\mathbb{K}^{sep}$ de $\mathbb{K}$ et à valeurs dans $\mathbb{Q}$.

Dans cette partie on utilisera les résultats démontrés dans le chapitre 3 (en particulier la partie I du chapitre 3 sera utilisée dans toute cette partie et la partie II du chapitre 3 sera uniquement utilisée dans la sous-partie III.2) ainsi que le fait que pour ϕ un module de Drinfeld de rang 2, ϕ a une potentielle bonne réduction si, et seulement si, $v(j_\phi) \geq 0$ (on pourra en trouver une démonstration à la suite du lemme 5.2 de la page 250 de [Ros03]).

III.1 Image du groupe d'inertie sous hypothèse de bonne réduction

Dans toute cette sous-partie, on considère $\phi : A \longrightarrow \mathbb{K}\{\tau\}$ un module de Drinfeld de rang 2 qui a une bonne réduction en $\mathfrak{p}$.

Pour un idéal non nul $\mathfrak{a}$ de A, l'action du groupe de Galois sur la $\mathfrak{a}$-torsion de ϕ donne une représentation $\overline{\rho}_{\phi,\mathfrak{a}} : \mathrm{Gal}_{\mathbb{K}} \longrightarrow \mathrm{GL}_2(A/\mathfrak{a})$ et lorsque $\mathfrak{p} \nmid \mathfrak{a}$ on a $\overline{\rho}_{\phi,\mathfrak{a}}(I_{\mathbb{K}}) = \{I_2\}$ (on pourra en trouver une preuve après le théorème 6.3.1 à la page 366 de [Pap23]).

On étudie désormais le groupe $\overline{\rho}_{\phi,\mathfrak{p}}(I_{\mathbb{K}})$ lorsque ϕ a une bonne réduction :

Proposition 4.5 :
Si $\mathbb{K}/F_{\mathfrak{p}}$ est une extension non ramifiée, alors on est dans l'une des deux situations suivantes :

* $\overline{\rho}_{\phi,\mathfrak{p}}(I_{\mathbb{K}})$ est conjugué dans $\mathrm{GL}_2(\mathbb{F}_{\mathfrak{p}})$ à un sous-groupe de $\left\{\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix},\ a \in \mathbb{F}_{\mathfrak{p}}^\times,\ b \in \mathbb{F}_{\mathfrak{p}}\right\}$;
* $\overline{\rho}_{\phi,\mathfrak{p}}(I_{\mathbb{K}})$ est un groupe cyclique de $\mathrm{GL}_2(\mathbb{F}_{\mathfrak{p}})$ d'ordre $q^{2\deg(\mathfrak{p})} - 1$.

Preuve :
Supposons que $\mathbb{K}/F_{\mathfrak{p}}$ soit une extension non ramifiée.
Quitte à remplacer ϕ par un module de Drinfeld isomorphe, on peut supposer que ϕ est défini sur $\mathcal{O}$ et que lorsque l'on réduit ϕ modulo $\mathfrak{m}$ on obtient encore un module de Drinfeld de rang 2.

$\phi[\mathfrak{p}]$ s'étend en un schéma en groupe fini et plat sur $\mathcal{O}$ et les composantes étales et connexes de $\phi[\mathfrak{p}]$ donnent la suite exacte de schémas en groupe fini et plat :

$$0 \longrightarrow \phi[\mathfrak{p}]^0 \longrightarrow \phi[\mathfrak{p}] \longrightarrow \phi[\mathfrak{p}]^{ét} \longrightarrow 0.$$

En prenant les $\mathbb{K}^{sep}$ points on obtient une suite exacte de $\mathbb{F}_{\mathfrak{p}}$-espaces vectoriels $\mathrm{Gal}_{\mathbb{K}}$-invariants :

$$0 \longrightarrow \phi[\mathfrak{p}]^0\left(\mathbb{K}^{sep}\right) \longrightarrow \phi[\mathfrak{p}]\left(\mathbb{K}^{sep}\right) \longrightarrow \phi[\mathfrak{p}]^{ét}\left(\mathbb{K}^{sep}\right) \longrightarrow 0. \tag{4.3}$$

Notons désormais h la hauteur de ϕ modulo $\mathfrak{p}$.
Le $\mathbb{F}_{\mathfrak{p}}$-espace vectoriel $\phi[\mathfrak{p}]^0\left(\mathbb{K}^{sep}\right)$ est alors de dimension h et de plus l'action de $I_{\mathbb{K}}$ sur $\phi[\mathfrak{p}]^{ét}\left(\mathbb{K}^{sep}\right)$ est triviale (par la définition d'un schéma en groupe étale). On peut maintenant finir la preuve en raisonnant par disjonction de cas sur h :

* Si $h = 1$, alors on obtient le premier point via la suite exacte donnée en (4.3).

* Si $h = 2$, alors on a le résultat par la proposition 2.7 à la page 870 de [PR09b] qui montre que $I_{\mathbb{K}}$ agit sur $\phi[\mathfrak{p}]^0\,(\mathbb{K}^{sep})$ via le caractère fondamental dont l'image est cyclique et d'ordre $q^{2\deg(\mathfrak{p})} - 1$.

■

III.2 Image du groupe d'inertie sous hypothèse de réduction stable

Dans toute cette sous-partie, on considère $\phi : A \longrightarrow \mathbb{K}\{\tau\}$ un module de Drinfeld de rang 2 qui a une réduction stable de rang 1.

Comme précédemment, pour un idéal non nul $\mathfrak{a}$ de A, l'action du groupe de Galois sur la $\mathfrak{a}$-torsion de ϕ donne une représentation $\overline{\rho}_{\phi,\mathfrak{a}} : \mathrm{Gal}_{\mathbb{K}} \longrightarrow \mathrm{GL}_2(A/\mathfrak{a})$.

La proposition suivante nous donne des contraintes sur $\overline{\rho}_{\phi,\mathfrak{a}}(I_{\mathbb{K}})$ lorsque ϕ a une mauvaise et stable réduction :

Proposition 4.6 :
Soit $\mathfrak{a} = \mathfrak{p}^e\mathfrak{a}'$ un idéal de A avec $e \in \mathbb{N}$ et $\mathfrak{a}'$ un idéal non nul de A premier à $\mathfrak{p}$.

* Le groupe $\overline{\rho}_{\phi,\mathfrak{a}}(\mathrm{Gal}_{\mathbb{K}})$ est conjugué dans $\mathrm{GL}_2(A/\mathfrak{a})$ à un sous-groupe de

$$\left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix},\ a \in (A/\mathfrak{a})^{\times},\ a \equiv 1\ [\mathfrak{a}'],\ b \in A/\mathfrak{a} \text{ et } c \in \mathbb{F}_q^{\times} \right\};$$

* Le cardinal de $\overline{\rho}_{\phi,\mathfrak{a}}(I_{\mathbb{K}})$ est divisible par le dénominateur de la fraction réduite $\frac{v(j_\phi)}{N(\mathfrak{a})} \in \mathbb{Q}$;
* Si $\mathrm{PGCD}(v(j_\phi); q) = 1$ et $e \leq 1$, alors $\overline{\rho}_{\phi,\mathfrak{a}}(I_{\mathbb{K}})$ contient un sous-groupe qui est conjugué dans $\mathrm{GL}_2(A/\mathfrak{a})$ à $\left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix},\ b \in A/\mathfrak{a} \right\}$.

Preuve :
Soit $\mathfrak{a} = \mathfrak{p}^e\mathfrak{a}'$ un idéal de A avec $e \in \mathbb{N}$ et $\mathfrak{a}$ un idéal non nul de A premier à $\mathfrak{p}$.

* Quitte à remplacer ϕ par un module de Drinfeld sur $\mathbb{K}$ qui lui est isomorphe, on peut supposer que ϕ est défini sur $\mathcal{O}$ et que sa réduction modulo $\mathfrak{m}$ est un module de Drinfeld de rang 1. De plus, on a $j_\phi \neq 0$ puisque ϕ a une réduction stable de rang 1.

  Commençons par rappeler quelques résultats sur l'uniformisation de Tate (on pourra en retrouver les résultats préliminaires dans la partie II du chapitre 3) :
  Il existe un unique module de Drinfeld $\psi : A \longrightarrow \mathbb{K}\{\tau\}$ défini sur $\mathcal{O}$ de rang 1 et une unique série $u := \tau^0 + \sum_{i=1}^{+\infty} a_i\tau^i \in \mathcal{O}\{\{\tau\}\}$ tel que les a_i appartiennent à $\mathfrak{m}$, $\lim_{i\to+\infty} a_i = 0$ dans $\mathbb{K}$ et

$$\forall a \in A,\ u \cdot \psi_a = \phi_a \cdot u. \tag{4.4}$$

  On peut identifier u avec la série $u(x) := x + \sum_{i=1}^{+\infty} a_i x^{q^i}$ et on peut montrer que $u(z)$ converge pour tout $z \in \mathbb{K}^{sep}$. De plus, en considérant les propriétés analytiques de u et (4.4), on peut montrer que l'application

$$u : \left| \begin{array}{ccc} {}^{\psi}\mathbb{K}^{sep} & \longrightarrow & {}^{\phi}\mathbb{K}^{sep} \\ z & \longmapsto & u(z) \end{array} \right. \tag{4.5}$$

  est un morphisme de A-modules dont le noyau Γ est un ψ-réseau et puisque ϕ est de rang 2 et a une réduction stable de rang 1, on en déduit que le A-module Γ est de rang $2 - 1 = 1$.

  Posons $a \in A$ tel que $\mathfrak{a} = (a)$.
  D'après le morphisme de A-modules (4.5), on obtient l'isomorphisme de A-modules

$$\psi_a^{-1}(\Gamma)/\Gamma \cong \phi[a] = \phi[\mathfrak{a}]$$

donné par l'application $z+\Gamma \longrightarrow u(z)$ et qui est $\mathrm{Gal}_{\mathbb{K}}$-équivariant. On a également la suite exacte courte de A-modules $\mathrm{Gal}_{\mathbb{K}}$-équivariante :

$$0 \longrightarrow \psi[a] = \psi_a^{-1}(0) \longrightarrow \psi_a^{-1}(\Gamma)/\Gamma \xrightarrow{\psi_a} \Gamma/a\Gamma \longrightarrow 0. \tag{4.6}$$

En combinant alors l'isomorphisme précédent et (4.6), on obtient alors également la suite exacte courte de A-modules qui est $\mathrm{Gal}_{\mathbb{K}}$-équivariante :

$$0 \longrightarrow \psi[\mathfrak{a}] \longrightarrow \phi[\mathfrak{a}] \longrightarrow \Gamma/\mathfrak{a}\Gamma \longrightarrow 0. \tag{4.7}$$

Enfin, remarquons que le $A/\mathfrak{a}$-module $\phi[\mathfrak{a}]$ est libre et de rang 1 puisque ψ est de rang 1.

Définissions le caractère $\chi_1 := \overline{\rho}_{\psi,\mathfrak{a}} : \mathrm{Gal}_{\mathbb{K}} \longrightarrow \mathrm{Aut}_A(\psi[\mathfrak{a}]) = (A/\mathfrak{a})^\times$.
Puisque A est un anneau principal et intègre, Γ est un A-module libre de rang 1. L'action de $\mathrm{Gal}_{\mathbb{K}}$ sur Γ est donc donnée par un caractère $\chi_2 : \mathrm{Gal}_{\mathbb{K}} \longrightarrow \mathrm{Aut}_A(\Gamma) = A^\times = \mathbb{F}_q^\times$ (le caractère χ_2 décrit également l'action de $\mathrm{Gal}_{\mathbb{K}}$ sur le quotient $\Gamma/a\Gamma$). De (4.7), on peut assumer après un choix de base approprié pour $\phi[\mathfrak{a}]$ si nécessaire que :

$$\forall \sigma \in \mathrm{Gal}_{\mathbb{K}},\ \overline{\rho}_{\phi,\mathfrak{a}}(\sigma) = \begin{pmatrix} \chi_1(\sigma) & * \\ 0 & \chi_2(\sigma) \end{pmatrix}.$$

Pour compléter la preuve du premier point, il nous reste à montrer que pour tout $\sigma \in I_{\mathbb{K}}$ on a la congruence $\chi_1(\sigma) \equiv 1\ [\mathfrak{a}']$. De manière équivalente, on doit montrer que l'action de $I_{\mathbb{K}}$ sur $\psi[\mathfrak{a}']$ est triviale. Or pour montrer cela, il suffit de montrer que ψ a une bonne réduction, ce qui est le cas puisque l'on a $\psi_T \equiv \phi_T\ [\mathfrak{m}]$ en réduisant la relation (4.4) modulo $\mathfrak{m}$ et que $\overline{\phi}$ est un module de Drinfeld de rang 1 (comme ψ).

∗ Choisissons γ un générateur du A-module Γ et choisissons $z \in \mathbb{K}^{sep}$ tel que $\psi_a(z) = \gamma$.
Montrons tout d'abord que $v(z) = \frac{v(j_\phi)}{(q-1)N(\mathfrak{a})}$:

— Supposons tout d'abord que $v(z) \geq 0$.
Puisque ψ_a est à coefficients dans $\mathcal{O}$, on a $v(\gamma) = v(\psi_a(z)) \geq 0$. Or, puisque γ est non nul et que v est une valuation discrète, on a

$$u(\gamma) = \gamma + \sum_{i=1}^{+\infty} a_i \gamma^{q^i} = 0,$$

d'où $v(\gamma) \geq v\left(a_i \gamma^{q^i}\right)$ pour un certain $i \in \mathbb{N}^*$ tel que $a_i \neq 0$.
Finalement, on a alors $v(\gamma) \geq v(a_i) + q^i v(\gamma) > q^i v(\gamma)$, ce qui n'est pas possible puisque $v(\gamma) \geq 0$.

— Supposons désormais que $v(z) < 0$.
On a la relation :

$$v(\gamma) = v(\psi_a(z)) = v\left(z^{q^{\deg(a)}}\right) = q^{deg(a)} v(z) = N(\mathfrak{a}) v(z).$$

Or, on a également que $v(\gamma) = \frac{v(j_\phi)}{q-1}$ (cf. lemme 5.3 de la page 251 de [Ros03]), d'où :

$$v(z) = \frac{v(\gamma)}{N(\mathfrak{a})} = \frac{v(j_\phi)}{(q-1)N(\mathfrak{a})}.$$

Posons désormais d le dénominateur de la fraction réduite $\frac{v(j_\phi)}{N(\mathfrak{a})} \in \mathbb{Q}$, $\mathbb{K}^t$ l'extension maximale modérément ramifiée de $\mathbb{K}$ dans $\mathbb{K}^{sep}$ ainsi que $\mathbb{L}$ la plus petite extension de $\mathbb{K}^t$ dans $\mathbb{K}^{sep}$ telle que $\mathrm{Gal}\left(\mathbb{K}^{sep}/\mathbb{L}\right)$ fixe $z+\Gamma$.
Le groupe de Galois $\mathrm{Gal}\left(\mathbb{K}^{sep}/\mathbb{K}^t\right)$ agit trivialement sur Γ puisque l'action du groupe de Galois que Γ est donnée par χ_2. On a alors que $\mathbb{L} = \mathbb{K}^t(z)$ (car $\mathbb{L}$ est minimal pour cette propriété et contient $\mathbb{K}^t(z)$) et par l'isomorphisme $\psi_a^{-1}(\Gamma)/\Gamma \cong \phi[a] = \phi[\mathfrak{a}]$ on trouve que $\mathbb{K}^t(z) \subseteq \mathbb{K}^t(\phi[\mathfrak{a}])$. Un nombre rationnel

s'écrit comme un $v(\alpha)$ pour $\alpha \in \mathbb{K}^t$ si, et seulement si, son dénominateur est relativement premier à p. Or, on a montré que $v(z) = \frac{v(j_\phi)}{(q-1)N(\mathfrak{a})}$ donc on trouve que d est le plus petit entier positif pour lequel $dv(z) \in v\left(\mathbb{K}^t \setminus \{0_{\mathbb{K}^t}\}\right)$. Ainsi, $\left[\mathbb{K}^t(z) : \mathbb{K}^t\right]$ est divisible par d et par le théorème de la base télescopique on obtient que d divise $\left[\mathbb{K}^t(\phi[\mathfrak{a}]) : \mathbb{K}^t\right]$, c'est-à-dire Card $\left(\overline{\rho}_{\phi,\mathfrak{a}}(I_{\mathbb{K}})\right)$.

∗ Supposons que $\text{PGCD}(v(j_\phi); q) = 1$ et $e \leq 1$.
Posons $G \subseteq \text{GL}_2(A/\mathfrak{a})$ le sous-groupe $\left\{\begin{pmatrix} a & b \\ 0 & c \end{pmatrix},\ a \in (A/\mathfrak{a})^\times,\ a \equiv 1\ [\mathfrak{a}'],\ b \in A/\mathfrak{a} \text{ et } c \in \mathbb{F}_q^\times\right\}$.
Puisque $e \leq 1$, le groupe $B := \left\{\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix},\ b \in A/\mathfrak{a}\right\}$ est un p-Sylow de G (avec p le nombre premier divisant q). Par le premier point démontré plus haut, on a $\overline{\rho}_{\phi,\mathfrak{a}}(I_{\mathbb{K}}) \subseteq G$ (quitte à conjuguer), donc il suffit de montrer que $\overline{\rho}_{\phi,\mathfrak{a}}(I_{\mathbb{K}})$ contient un sous-groupe d'ordre $N(\mathfrak{a})$ (puisqu'il s'agira d'un p-Sylow de G et donc est conjugué à B).

Or le groupe $\overline{\rho}_{\phi,\mathfrak{a}}(I_{\mathbb{K}})$ a un cardinal divisible par $N(\mathfrak{a})$ (par le point précédent et le fait que $\text{PGCD}(v(j_\phi); q) = 1$) et $\overline{\rho}_{\phi,\mathfrak{a}}(I_{\mathbb{K}})$ est conjugué à un sous-groupe de G. De plus, et on peut montrer après calcul (en regardant quand $e = 0$ et $e = 1$) que G a un cardinal divisible par $N(\mathfrak{a})$ exactement (d'où le fait que B est un p-Sylow de G) donc par le théorème de Lagrange on obtient que le cardinal de $\overline{\rho}_{\phi,\mathfrak{a}}(I_{\mathbb{K}})$ est exactement divisible par $N(\mathfrak{a})$ et par le premier théorème de Sylow il contient un sous-groupe d'ordre $N(\mathfrak{a})$.

■

IV Polynôme caractéristique du Frobenius

Dans toute cette partie, on considère un module de Drinfeld $\phi : A \longrightarrow F\{\tau\}$ de rang r, $\mathfrak{p}$ un idéal premier non nul de A pour lequel ϕ a une bonne réduction ainsi que $P_{\phi,\mathfrak{p}} \in A[x]$ le polynôme caractéristique de l'endomorphisme de Frobenius défini par $\pi_{\mathfrak{p}} := \tau^{\deg(\mathfrak{p})} \in \text{End}_{\mathbb{F}_{\mathfrak{p}}}\left(\overline{\phi}\right)$.

Quitte à remplacer ϕ par un module de Drinfeld isomorphe, on peut supposer que les coefficients de ϕ sont entiers en $\mathfrak{p}$ et que la réduction de ϕ modulo $\mathfrak{p}$ donne un module de Drinfeld $\overline{\phi} : A \longrightarrow \mathbb{F}_{\mathfrak{p}}\{\tau\}$ de rang r.

Le but de cette partie sera de donner un résultat sur le polynôme caractéristique du Frobenius ainsi que d'en connaître explicitement quelques-uns en vue du chapitre 6. Commençons par le résultat suivant qui est une conséquence du théorème 4.12.12 à la page 108 de [Gos96] :

Proposition 4.7 :
Soit $\mathfrak{a}$ un idéal non nul de A premier avec $\mathfrak{p}$.
La représentation résiduelle $\overline{\rho}_{\phi,\mathfrak{a}}$ est non ramifiée en $\mathfrak{p}$ et $P_{\phi,\mathfrak{p}}(x) \equiv \det\left(xI_r - \overline{\rho}_{\phi,\mathfrak{a}}\left(\text{Frob}_{\mathfrak{p}}\right)\right)\ [\mathfrak{a}]$.

Enfin, nous allons calculer trois polynômes caractéristiques avec toujours comme objectif de les utiliser ultérieurement dans le chapitre 6. Cependant, avant de nous lancer dans les calculs, nous allons commencer par rappeler des résultats issus de la fin de la partie 4.2 de [Pap23] :

Fixons nous $\mathfrak{q}$ un idéal premier non nul de A et $\mathbb{L}$ une extension finie de $\mathbb{F}_{\mathfrak{q}}$ de degré m muni d'une structure de A-corps via l'inclusion naturelle de $\mathbb{F}_{\mathfrak{q}}$ dans A. Par le théorème de la base télescopique, on pose :

$$n := [\mathbb{L} : \mathbb{F}_q] = [\mathbb{L} : \mathbb{F}_{\mathfrak{q}}][\mathbb{F}_{\mathfrak{q}} : \mathbb{F}_q] := m \deg(\mathfrak{q}).$$

En notant $P_{\phi,\mathbb{L}}(x) = \sum_{i=0}^{r-1} a_i x^i + x^r \in A[x]$ le polynôme caractéristique du Frobenius, on sait que pour tout $i \in [\![0; r-1]\!]$, $\deg(a_i) \leq \frac{(r-i)n}{r} < \deg(\mathfrak{p})$ (les a_i sont uniquement déterminés par leur reste modulo $\mathfrak{p}$ lorsque $\mathbb{L} = \mathbb{F}_{\mathfrak{q}}$), $a_0 = c \times \mathfrak{q}$ avec $c \in \mathbb{F}_q^\times$ (où c peut être obtenu par une forme explicite). Il nous reste donc à déterminer les autres

a_i et pour cela, on remarque que :

$$\tau^{dr} + \sum_{i=0}^{r-1} \phi_{a_i} \tau^{di} = 0.$$

Ainsi, en notant $f_i := \sum_{k=0}^{i} \phi_{a_k} \tau^{dk}$ et $f_i^\dagger := \sum_{k=i+1}^{r} \phi_{a_k} \tau^{dk}$ pour $i \in [\![0; r]\!]$, on constate que $\deg_\tau \left(\phi_{a_j} \tau^{dj}\right) \geq dj$ et donc le coefficient de $\tau^{d(i+1)}$ dans $f_i^\dagger$ est le terme constant de $\phi_{a_{i+1}}$ (c'est-à-dire $\gamma(a_{i+1})$). Finalement, on a que $\gamma(a_{i+1})$ est égal à l'opposé du coefficient de $\tau^{d(i+1)}$ dans f_i et comme on connaît f_0 explicitement on peut trouver les a_i récursivement en utilisant $a_0, \ldots, a_{i-1}$ pour calculer a_i.

De plus, lorsque $\mathbb{L} = \mathbb{F}_\mathfrak{q}$ et $r = 2$, il est possible de trouver les coefficients de $P_{\phi,\mathbb{L}}$ différemment. En effet, on sait déjà que pour $\phi : A \longrightarrow \mathbb{L}\{\tau\}$ un module de Drinfeld de rang 2 défini par $\phi_T := \gamma(T) + g\tau + \Delta\tau^2$ et de polynôme caractéristique $P_{\phi,\mathbb{L}}(x) := x^2 - ax + b$ sur $\mathbb{L}$, le terme constant de $P_{\phi,\mathbb{L}}(x)$ est donné par $b = (-1)^n N_{\mathbb{F}_\mathfrak{p}/\mathbb{F}_q}(\Delta)^{-1}\mathfrak{q}^m$. Pour trouver a, on procède de la manière suivante :

Pour $n \in \mathbb{N}^*$, on pose $[n] :\equiv T^{q^n} - T$ $[\mathfrak{q}]$ et on définit de manière récursive $f_0 := 1$, $f_1 := g$ ainsi que $f_n := -[n-1]f_{n-2}\Delta^{q^{n-2}} + f_{n-1}g^{q^{n-1}}$ pour $n \geq 2$. Ainsi l'élément a est entièrement déterminé via :

$$a \equiv (-1)^{\deg(\mathfrak{p})} N_{\mathbb{F}_\mathfrak{p}/\mathbb{F}_q}(\Delta)^{-1} f_d \ [\mathfrak{p}] \text{ et } \deg(a) \leq \frac{\deg(\mathfrak{p})}{2}.$$

Ici, nous regarderons nos polynômes caractéristiques sur $\mathbb{F}_\mathfrak{q}$ et donc en particulier on a $\mathbb{L} = \mathbb{F}_\mathfrak{q}$ et $m = 1$. De plus, jusqu'à la fin de cette partie on considère le module de Drinfeld $\phi : A \longrightarrow F\{\tau\}$ de rang 2 défini par :

$$\phi_T := \begin{cases} t + \tau - T^{q-1}\tau^2 & \text{si } q \neq 2 \\ t + T^3\tau + \left(T^2 + T + 1\right)\tau^2 & \text{sinon.} \end{cases}$$

Lemme 4.11 :
Soit $c \in \mathbb{F}_q$ non nul.
Si $q \neq 2$, alors on a $P_{\phi,(T-c)}(x) = x^2 - x + (T - c)$.

Preuve :
Soit $c \in \mathbb{F}_q$ non nul avec $q \neq 2$.
Considérons l'idéal premier $\mathfrak{q} := (T - c)$ de A et remarquons que ϕ a une bonne réduction en $\mathfrak{q}$ puisque c est non nul. On obtient ainsi un module de Drinfeld $\overline{\phi} : A \longrightarrow \mathbb{F}_\mathfrak{q}\{\tau\} = \mathbb{F}_q\{\tau\}$ qui est de rang 2 et défini par $\overline{\phi}_T := c + \tau - c^{q-1}\tau^2 = c + \tau - \tau^2$.

Puisque $T - c$ est un polynôme de degré 1, on a $n = [\mathbb{L} : \mathbb{F}_q] = m \deg(\mathfrak{q}) = 1$ et en appliquant ce qui précède on obtient :

$$a = -N_{\mathbb{F}_\mathfrak{p}/\mathbb{F}_q}(-1)^{-1} \times f_1 = f_1 = 1 \text{ et } b = (-1)^1 \times N_{\mathbb{F}_\mathfrak{p}/\mathbb{F}_q}(-1)^{-1} \times \mathfrak{q}^1 = -1 \times (-1) \times (T - c) = T - c.$$

Finalement, on trouve que bien que $P_{\phi,(T-c)}(x) = x^2 - x + (T - c)$.

■

Lemme 4.12 :
Si $q = 2$, alors $P_{\phi,(T)}(x) = x^2 + T$ et $P_{\phi,(T+1)}(x) = x^2 + x + T + 1$.

Preuve :
Supposons que $q = 2$, alors :

* En posant $\mathfrak{q} := (T)$, on obtient comme précédemment que $\mathbb{L} = \mathbb{F}_\mathfrak{q} = \mathbb{F}_q$ (donc en particulier $n = m = 1$) et $\overline{\phi}_T = \tau^2$. Ainsi, on trouve que

  $$a = (-1)^1 \times N_{\mathbb{F}_\mathfrak{p}/\mathbb{F}_q}(1)^{-1} \times 0 = 0 \text{ et } b = (-1)^1 \times N_{\mathbb{F}_\mathfrak{p}/\mathbb{F}_q}(1)^{-1} \times T = -T = T,$$

  d'où $P_{\phi,(T)}(x) = x^2 + T$.

∗ De même, on obtient $\overline{\phi}_T = -1 - \tau + \tau^2 = 1 + \tau + \tau^2$, d'où :

$$a = -N_{\mathbb{F}_\mathfrak{p}/\mathbb{F}_q}(1)^{-1} \times 1 = -1 \text{ et } b = (-1)^1 \times N_{\mathbb{F}_\mathfrak{p}/\mathbb{F}_q}(1)^{-1} \times (T+1) = -(T+1) = T+1.$$

Finalement, on trouve bien que $P_{\phi,(T+1)}(x) = x^2 + x + T + 1$.

■

Lemme 4.13 :
Si $q = 3$, alors $P_{\phi,(T^2+T+2)}(x) = x^2 + 2x + (T^2 + T + 2)$.

Preuve :
On a ici $q = 3$ et $n = 2$ et :

$$f_2 = -[1]f_0 g_2^{q^0} + f_1 g_1^{q^1} = -(T^q - T)(-T^{q-1}) + 1 = T^q(T^{q-1} - 1) + 1 = T^3(T^2 - 1) + 1.$$

De plus, $N_{\mathbb{F}_\mathfrak{p}/\mathbb{F}_q}(-T^2) = (-1)^2 N_{\mathbb{F}_\mathfrak{p}/\mathbb{F}_q}(T)^2 = 2^2 = 4 = 1$, d'où :

$$a = (-1)^2 \times 1^{-1} \times \left(T^3(T^2-1) + 1\right) = -7 = 2 \text{ et } b = (-1)^2 \times N_{\mathbb{F}_\mathfrak{p}/\mathbb{F}_q}(-T^2)^{-1} \times \mathfrak{p} = T^2 + T + 2.$$

Ainsi, on trouve bien que $P_{\phi,(T^2+T+2)}(x) = x^2 + 2x + (T^2 + T + 2)$.

■

V Déterminant de l'image du groupe de Galois

Dans toute cette partie, on considère $a_1, a_2 \in A$ deux polynômes avec $a_2 \neq 0$. On notera d le degré de a_2 et $\phi : A \longrightarrow F\{\tau\}$ le module de Drinfeld de rang 2 défini par $\phi_T := T + a_1\tau + a_2\tau^2$.

Le but de cette partie est de démontrer le théorème suivant (qui donne une formule explicite concernant l'indice de $\det(\rho_\phi(\mathrm{Gal}_F))$ dans $\widehat{A}^\times$) ainsi que le théorème 4.3 et qui nous seront très utiles dans les chapitres 5 et 6.

Théorème 4.2 :
Soient $\zeta \in \mathbb{F}_q^\times$ le coefficient dominant de $(-1)^{d+1}a_2$ et e l'ordre de $\zeta \in \mathbb{F}_q^\times$.
L'indice de $\det(\rho_\phi(\mathrm{Gal}_F))$ dans $\widehat{A}^\times$ est donné par la formule :

$$\left[\widehat{A}^\times : \det(\rho_\phi(\mathrm{Gal}_F))\right] = \mathrm{PGCD}\left(d-1; \frac{q-1}{e}\right).$$

Nous donnons également une condition qui peut être utilisée pour montrer que le déterminant de l'image de $\overline{\rho}_{\phi,\mathfrak{a}}$ est égal à $\widehat{A}^\times$ tout entier :

Proposition 4.8 :
Soient $\mathfrak{a}$ un idéal non nul de A et $g := \mathrm{PGCD}\left(\{d-1; q-1\} \cup \{v_\mathfrak{p}(a_2),\ \mathfrak{p} \nmid \mathfrak{a} \text{ idéal premier non nul de } A\}\right)$.
Si $g = 1$, alors $\det\left(\overline{\rho}_{\phi,\mathfrak{a}}(\mathrm{Gal}_F)\right) = (A/\mathfrak{a})^\times$.

Avant de démontrer ces deux résultats dans la sous-partie V.2, nous allons commencer par essayer de donner des résultats similaires pour les modules de Drinfeld de rang 1 puis de les réinvestir pour traiter le cas de ceux de rang 2.

V.1 Cas des modules de Drinfeld de rang 1

Dans toute cette sous-partie, on considère $\Delta \in A$ non nul et $\psi : A \longrightarrow F\{\tau\}$ le module de Drinfeld de rang 1 défini par $\psi_T := T + \Delta\tau$.

Rappelons que pour tout idéal non nul $\mathfrak{a}$ de A, $\psi[\mathfrak{a}]$ est un $A/\mathfrak{a}$-module libre de rang 1 dont l'action par le groupe

de Galois est donnée par la représentation galoisienne

$$\overline{\rho}_{\psi,\mathfrak{a}} : \mathrm{Gal}_F \longrightarrow \mathrm{Aut}_A(\psi[\mathfrak{a}]) \cong (A/\mathfrak{a})^\times.$$

Enfin, en prenant la limite inverse on obtient alors une représentation $\rho_\psi : \mathrm{Gal}_F \longrightarrow \widehat{A}^\times$.

Théorème 4.3 :
Soient d le degré de Δ, $\zeta \in \mathbb{F}_q^\times$ le coefficient dominant de $(-1)^d\Delta$ et e son ordre dans $\mathbb{F}_q^\times$.

* Pour tout idéal non nul $\mathfrak{a}$ de A, l'entier $\left[(A/\mathfrak{a})^\times : \overline{\rho}_{\psi,\mathfrak{a}}(\mathrm{Gal}_F)\right]$ est le plus grand diviseur commun entre $d-1$, $\frac{q-1}{e}$ et les $v_\mathfrak{p}(\Delta)$ où $\mathfrak{p} \nmid \mathfrak{a}$ est un idéal premier non nul de A ;
* Le groupe $\rho_\psi(\mathrm{Gal}_F)$ est d'indice fini dans $\widehat{A}^\times$ et $\left[\widehat{A}^\times : \rho_\psi(\mathrm{Gal}_F)\right] = \mathrm{PGCD}\left(d-1; \frac{q-1}{e}\right)$.

Preuve :
Soient d le degré de Δ, $\zeta \in \mathbb{F}_q^\times$ le coefficient dominant de $(-1)^d\Delta$ et e son ordre dans $\mathbb{F}_q^\times$.

* Tout d'abord, remarquons que la représentation $\overline{\rho}_{\psi,\mathfrak{a}}$ ne dépend que de $\mathfrak{a}$ est de la classe de Δ dans $F^\times/(F^\times)^{q-1}$ (cf. (1.6)). Ainsi, quitte à diviser par une puissance $(q-1)$-ième d'un polynôme unitaire, on peut supposer que

$$\Delta = (-1)^d\zeta\prod_{i=1}^{s} P_i^{k_i}$$

où les $P_i \in A$ sont des polynômes unitaires irréductibles distincts et de degré $k_i \in [\![1; q-2]\!]$ (les PGCD sont inchangés en utilisant la propriété de transitivité ainsi que des combinaisons linéaires de ses arguments).

Désormais, quitte à renuméroter les P_i, on peut supposer que les $P_1, ..., P_r$ divisent $\mathfrak{a}$ et que les $P_{r+1}, ..., P_s$ sont premiers avec $\mathfrak{a}$ et on fixe également c un générateur du groupe cyclique $\mathbb{F}_q^\times$.
Ainsi, puisque $(-1)^d\zeta, \zeta \in \mathbb{F}_q^\times$, il existe un unique couple $(k_0, k_0^*) \in [\![0; q-2]\!]$ tel que $(-1)^d\zeta = c^{k_0}$ et $\zeta = c^{k_0^*}$. Remarquons également que l'on a $k_0 = k_0^*$ lorsque $(-1)^d = 1$, autrement dit lorsque $q = 2$ ou d est pair, et dans le cas où $q \neq 2$ et d impair, on a $k_0^* \equiv \frac{q-1}{2} + k_0\ [q-1]$.

Or, par le théorème 3.13 à la page 325 de [Gek16], on sait que

$$\left[(A/\mathfrak{a})^\times : \overline{\rho}_{\psi,\mathfrak{a}}(\mathrm{Gal}_F)\right] = \mathrm{PGCD}(\{d-1; q-1; k_0^*\} \cup \{k_i,\ i \in [\![r+1; s]\!]\}).$$

Mais puisque $\zeta = c^{k_0^*}$ et que c est d'ordre $q-1$ dans $\mathbb{F}_q^\times$ (car générateur), on a $e = \frac{q-1}{\mathrm{PGCD}(q-1;k_0^*)}$. Ainsi, $\mathrm{PGCD}(q-1; k_0^*) = \frac{q-1}{e}$ et par transitivité du PGCD, on obtient :

$$\left[(A/\mathfrak{a})^\times : \overline{\rho}_{\psi,\mathfrak{a}}(\mathrm{Gal}_F)\right] = \mathrm{PGCD}\left(\left\{d-1; \frac{q-1}{e}\right\} \cup \{k_i,\ i \in [\![r+1; s]\!]\}\right).$$

Enfin, on conclut le premier point en remarquant que l'ensemble $\{k_i,\ i \in [\![r+1; s]\!]\}$ correspond exactement à l'ensemble $\{v_\mathfrak{p}(\Delta),\ \mathfrak{p} \nmid \mathfrak{a}$ est un idéal premier non nul de $A\}$ (quitte à ajouter des 0 qui ne changent pas le PGCD).

* Pour le deuxième point, il suffit de remarquer que lorsque $\mathfrak{a}$ est divisible par tous les polynômes irréductibles $P_1, \ldots, P_s$, on a simplement

$$\left[(A/\mathfrak{a})^\times : \overline{\rho}_{\psi,\mathfrak{a}}(\mathrm{Gal}_F)\right] = \mathrm{PGCD}\left(\left\{d-1; \frac{q-1}{e}\right\}\right)$$

Or ici $\rho_\psi : \mathrm{Gal}_F \longrightarrow \widehat{A}^\times$ est continu, $\rho_\psi(\mathrm{Gal}_F)$ est fermé dans $\widehat{A}^\times$ et $\rho_\psi(\mathrm{Gal}_F)$ contient le sous-groupe ouvert $U := \mathrm{Ker}\left(\widehat{A}^\times \longrightarrow (A/\mathfrak{a})^\times\right)$ (car $\mathfrak{a}$ est divisible par tous les P_i), d'où :

$$\left[\widehat{A}^\times : \rho_\psi(\mathrm{Gal}_F)\right] = \left[(A/\mathfrak{a})^\times : \overline{\rho}_{\psi,\mathfrak{a}}(\mathrm{Gal}_F)\right] = \mathrm{PGCD}(d-1; q-1)$$

■

V.2 Preuve du théorème 4.2 et de la proposition 4.8

Dans toute cette sous-partie, on considère le module de Drinfeld $\psi : A \longrightarrow F\{\tau\}$ de rang 1 défini par $\psi_T := T - a_2\tau$.

$*$ Commençons par démontrer le théorème 4.2 :
Par le corollaire 4.6 à la page 322 de [Ham93], on sait que :

$$\det(\rho_\phi) = \rho_\psi. \tag{4.8}$$

Ainsi, on a

$$\left[\widehat{A}^\times : \det(\rho_\phi(\mathrm{Gal}_F))\right] = \left[\widehat{A}^\times : \rho_\psi(\mathrm{Gal}_F)\right]$$

et en appliquant le deuxième point du théorème 4.3 avec $\Delta := -a_2$, on obtient bien que :

$$\left[\widehat{A}^\times : \det(\rho_\phi(\mathrm{Gal}_F))\right] = \mathrm{PGCD}\left(d-1; \frac{q-1}{e}\right).$$

$*$ Passons à la preuve de la proposition 4.8 :
Par (4.8), on obtient que $\det\left(\overline{\rho}_{\phi,\mathfrak{a}}\right) = \overline{\rho}_{\psi,\mathfrak{a}}$. De plus, en appliquant le premier point du théorème 4.3 avec $\Delta := -a_2$, on obtient que $\left[(A/\mathfrak{a})^\times : \det\left(\overline{\rho}_{\phi,\mathfrak{a}}(\mathrm{Gal}_F)\right)\right] = \left[(A/\mathfrak{a})^\times : \overline{\rho}_{\psi,\mathfrak{a}}(\mathrm{Gal}_F)\right]$ divise g.

Or, si $g = 1$, on obtient par positivité de l'indice que $\left[(A/\mathfrak{a})^\times : \det\left(\overline{\rho}_{\phi,\mathfrak{a}}(\mathrm{Gal}_F)\right)\right] = 1$ et donc on trouve bien que $\det\left(\overline{\rho}_{\phi,\mathfrak{a}}(\mathrm{Gal}_F)\right) = (A/\mathfrak{a})^\times$.

VI Irréductibilité

Dans toute cette partie, on considère $\phi : A \longrightarrow F\{\tau\}$ un module de Drinfeld de rang 2.

Supposons qu'il existe λ un idéal premier non nul de A pour lequel la représentation $\overline{\rho}_{\phi,\lambda} : \mathrm{Gal}_F \longrightarrow \mathrm{GL}_2(\mathbb{F}_\lambda)$ est réductible et ϕ a une réduction stable par λ. Quitte à conjuguer $\overline{\rho}_{\phi,\lambda}$ on peut supposer que :

$$\forall \sigma \in \mathrm{Gal}_F,\ \overline{\rho}_{\phi,\lambda}(\sigma) = \begin{pmatrix} \chi_1(\sigma) & * \\ 0 & \chi_2(\sigma) \end{pmatrix} \tag{4.9}$$

où $\chi_1, \chi_2 : \mathrm{Gal}_F \longrightarrow \mathbb{F}_\lambda^\times$ sont deux caractères.

Le but de cette partie est de donner une borne sur la norme de λ.

Lemme 4.14 :
Soit $n := (q-1)^2(q+1)$.

- Les caractères χ_1^n et χ_2^n sont tous les deux non ramifiés en tout idéal premier non nul $\mathfrak{p} \neq \lambda$ de A ;
- L'un des caractères χ_1^n ou χ_2^n est non ramifié en λ.

Preuve :
Soient $n := (q-1)^2(q+1)$ et $\mathfrak{p}$ un idéal premier non nul de A.
En regardant ϕ comme étant défini sur $F_\mathfrak{p}$, on obtient que $\overline{\rho}_{\phi,\lambda}$, χ_1 et χ_2 sont des représentations de $\mathrm{Gal}_{F_\mathfrak{p}}$ et on note $I_\mathfrak{p}$ le sous-groupe d'inertie de $\mathrm{Gal}_{F_\mathfrak{p}}$.

$*$ Ici on prend $\mathfrak{p} \neq \lambda$.
On a $\phi_T := T + a_1\tau + a_2\tau^2$ avec $a_1 \in F$ et $a_2 \in F^\times$. Posons alors $m := \min\left(\frac{v_\mathfrak{p}(a_1)}{q-1}; \frac{v_\mathfrak{p}(a_2)}{q^2-1}\right)$ et on prend $j \in \{1;2\}$ maximal tel que $\frac{v_\mathfrak{p}(a_j)}{q^j-1} = m$ ainsi que $\mathbb{K}$ le corps de décomposition de $x^{q^j-1} - a_j = 0$ sur $F_\mathfrak{p}$ dont on fixe une racine $b \in \mathbb{K}$.

L'extension $\mathbb{K}/F_\mathfrak{p}$ est finie et galoisienne et l'indice de ramification $e := e(\mathbb{K}/F_\mathfrak{p})$ de cette extension divise $q^j - 1$. En notant $I_\mathbb{K}$ le sous-groupe d'inertie de $\mathrm{Gal}_\mathbb{K} \subseteq \mathrm{Gal}_{F_\mathfrak{p}}$, on obtient que pour tout $\sigma \in I_\mathfrak{p}$, $\sigma^e \in I_\mathbb{K}$.

En effet, pour $\sigma \in I_{\mathfrak{p}}$, son action sur $\mathbb{F}_{\mathfrak{p}}^{sep}$ est triviale modulo la valuation $v_{\mathfrak{p}}$, c'est-à-dire que :

$$\forall x \in \mathcal{O}_{\mathbb{F}_{\mathfrak{p}}^{sep}},\ \sigma(x) \equiv x\ [\mathfrak{m}],$$

en ce sens que $v_{\mathfrak{p}}(\sigma(x) - x) > 0$ et où $\mathfrak{m}$ est l'idéal maximal de $\mathcal{O}_{\mathbb{F}_{\mathfrak{p}}^{sep}}$. De plus, la valuation $v_{\mathbb{K}}$ est reliée à la valuation $v_{\mathfrak{p}}$ par la formule $v_{\mathbb{K}} = ev_{\mathfrak{p}}$. Ainsi, pour $x \in \mathcal{O}_{\mathbb{F}_{\mathfrak{p}}^{sep}}$, en écrivant $\sigma(x) = \mathrm{Id}(x) + \delta(x)$ avec $\delta(x) = \sigma(x) - x$ on a :

$$\sigma^e(x) - x = \sum_{i=1}^{e} \binom{e}{i} (\sigma(x) - x)^i$$

et on a :

$$\forall i \in [\![1; e]\!],\ v_{\mathfrak{p}}\left(\binom{e}{i}(\sigma(x) - x)^i\right) \geq i v_{\mathfrak{p}}(\sigma(x) - x) > 0.$$

Par conséquent, on a donc $v_{\mathbb{K}}\left(\sigma^e(x) - x\right)$, d'où $\sigma^e \in I_{\mathbb{K}}$.
Ainsi, il suffit donc de montrer que $\chi_1^{\frac{n}{e}}(I_{\mathbb{K}}) = \{1\}$ et $\chi_2^{\frac{n}{e}}(I_{\mathbb{K}}) = \{1\}$.

Considérons $\mathcal{O}$ la clôture intégrale de $A_{\mathfrak{p}}$ dans $\mathbb{K}$ et $\phi' : A \longrightarrow \mathbb{K}\{\tau\}$ un module de Drinfeld isomorphe à ϕ sur $\mathbb{K}$ et à coefficients dans $\mathcal{O}$.
Raisonnons par disjonction de cas sur j :

— Supposons que $j = 2$.
Le module de Drinfeld ϕ' est alors défini sur $\mathcal{O}$ et a une bonne réduction. En effet, on a $\phi'_T = T + a_1 b^{1-q}\tau + a_2 b^{2-q^2}\tau^2 = T + a_1 b^{1-q}\tau + \tau^2$ (par le choix de b) et de plus on a également que $v_{\mathfrak{p}}\left(a_1 b^{1-q}\right) = v_{\mathfrak{p}}(a_1) + (1-q)v_{\mathfrak{p}}(b) = v_{\mathfrak{p}}(a_1) - (q-1)m \geq 0$ (par définition de m). Par conséquent, les coefficients de ϕ'_T sont dans $\mathcal{O}$ et a pour coefficient dominant une unité donc sa réduction est bien un module de Drinfeld de rang 2. Or, puisqu'ici $\mathfrak{p} \neq \lambda$, on a $\overline{\rho}_{\phi',\lambda}(I_{\mathbb{K}}) = \{I_2\}$ et donc $\chi_1(I_{\mathbb{K}}) = \chi_2(I_{\mathbb{K}}) = \{1\}$. Enfin, e divise $q^2 - 1$ et donc n et ainsi on trouve bien que $\chi_1^{\frac{n}{e}}(I_{\mathbb{K}}) = \{1\}$ et $\chi_2^{\frac{n}{e}}(I_{\mathbb{K}}) = \{1\}$.

— Supposons désormais que $j = 1$.
Le module de Drinfeld ϕ' est alors défini sur $\mathcal{O}$ et a une réduction stable de rang 1 (par la même démarche que pour le cas $j = 2$). Par le premier point de la proposition 4.6 et le fait que $\lambda \neq \mathfrak{p}$ on trouve que $\chi_1(I_{\mathbb{K}}) = \{1\}$ (et donc $\chi_1^{q-1}(I_{\mathbb{K}}) = \{1\}$) et $\chi_2^{q-1}(I_{\mathbb{K}}) = \{1\}$. Or, comme $\frac{n}{e}$ est divisible par $\frac{n}{q-1} = (q-1)(q+1)$, on a bien que $\chi_1^{\frac{n}{e}}(I_{\mathbb{K}}) = \{1\}$ et $\chi_2^{\frac{n}{e}}(I_{\mathbb{K}}) = \{1\}$.

∗ On prend $\mathfrak{p} = \lambda$ ici et on raisonne par disjonction de cas sur ϕ :

— Supposons que ϕ ait une bonne réduction en λ.
Par (4.9), on obtient par le théorème de Lagrange que le cardinal du groupe $\overline{\rho}_{\phi,\lambda}(\mathrm{Gal}_F)$ divise $q^{\deg(\lambda)}\left(q^{\deg(\lambda)-1}\right)^2$ et donc en particulier $\overline{\rho}_{\phi,\lambda}(\mathrm{Gal}_F)$ ne contient aucun sous-groupe de cardinal $q^{2\deg(\lambda)-1}$. De plus, l'extension $F_{\mathfrak{p}}/F_{\mathfrak{p}}$ est non ramifiée, donc par la proposition 4.5, on en déduit que $\overline{\rho}_{\phi,\mathfrak{p}}(I_{\mathfrak{p}})$ est conjugué dans $\mathrm{GL}_2(\mathbb{F}_{\mathfrak{p}})$ à un sous-groupe de $\left\{\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix},\ a \in \mathbb{F}_{\mathfrak{p}}^{\times},\ b \in \mathbb{F}_{\mathfrak{p}}\right\}$. Donc χ_1 ou χ_2 est non ramifié en λ et ainsi χ_1^n ou χ_2^n est non ramifié en λ.

— Supposons désormais que ϕ n'ait pas une bonne réduction en λ.
Par hypothèse sur λ, ϕ a une réduction stable par λ de rang 1. En appliquant le premier point de la proposition 4.6, on obtient que χ_1^{q-1} ou χ_2^{q-1} est non ramifié en λ et on a le résultat puisque $q - 1$ divise n.

■

Désormais, jusqu'à la fin de cette partie, pour un polynôme unitaire $P(x) \in A[x]$ et un entier naturel non nul n, on note $P^{(n)}(x) \in A[x]$ le polynôme dont les racines (comptées avec multiplicité), dans une clôture algébrique, sont exactement les racines de $P(x)$ élevées à la puissance n.

Lemme 4.15 :
Soit n un entier naturel non nul tel que les deux points du lemme 4.14 soient vrais.
Il existe $\zeta \in \mathbb{F}_\lambda^\times$ tel que pour tout idéal premier non nul $\mathfrak{p} \neq \lambda$ de A où ϕ a une bonne réduction on ait l'égalité $P_{\phi,\mathfrak{p}}^{(n)}\left(\zeta^{\deg(\mathfrak{p})}\right) = 0$ dans $\mathbb{F}_\lambda$.

Preuve :
Soit n un entier naturel non nul tel que les deux points du lemme 4.14 soient vrais.
Par hypothèse, il existe $i \in \{1;2\}$ tel que χ_i^n est non ramifié en tout idéal premier non nul de A.

Montrons que $\chi_i^n\left(\mathrm{Gal}\left(F^{sep}/\overline{\mathbb{F}_q}(T)\right)\right) = \{1\}$:
En notant $\mathbb{L}$ la plus petite extension de $\overline{\mathbb{F}_q}(T)$ dans F^{sep} pour laquelle $\chi_i^n\left(\mathrm{Gal}\left(F^{sep}/\mathbb{L}\right)\right) = \{1\}$, on remarque que l'extension $\mathbb{L}/\overline{\mathbb{F}_q}(T)$ correspond à un morphisme $\pi : C \longrightarrow \mathbb{P}^1_{\overline{\mathbb{F}_q}}$ de courbes lisses et irréductibles sur $\overline{\mathbb{F}_q}$.
Or par nos hypothèses sur χ_i^n, π est non ramifiée hors des points de $\mathbb{P}^1_{\overline{\mathbb{F}_q}}$ sauf éventuellement en ∞.
Le morphisme π est de degré $N := \left[\mathbb{L} : \overline{\mathbb{F}_q}(T)\right]$ qui est premier avec q. En effet, $\mathbb{L}$ est le corps fixe par χ_i^n et donc $\mathrm{Gal}(\mathbb{L}/\overline{\mathbb{F}_q}(T)) \cong \mathrm{Im}(\chi_i^n) \subseteq \mathbb{F}_\lambda^\times$, d'où :

$$\left[\mathbb{L} : \overline{\mathbb{F}_q}(T)\right] = \mathrm{Card}\left(\mathrm{Gal}(\mathbb{L}/\overline{\mathbb{F}_q}(T))\right) = \mathrm{Card}(\mathrm{Im}(\chi_i^n)).$$

Ainsi, $\left[\mathbb{L} : \overline{\mathbb{F}_q}(T)\right]$ divise $q^{\deg(\lambda)} - 1$ qui est premier à q, d'où $\left[\mathbb{L} : \overline{\mathbb{F}_q}(T)\right]$ premier à q.

De plus, puisque $\mathbb{L}/\overline{\mathbb{F}_q}(T)$ est modérément ramifiée, la formule de Riemann-Hurwitz donne

$$2g - 2 = N \times (2 \times 0 - 2) + \sum_{i=1}^{s} (e_i - 1),$$

où g est le genre de C et les $e_i \geq 1$ sont les indices de ramification des points s de C au-dessus de ∞. Or, on a $\sum_{i=1}^{s} e_i = N$, donc on obtient que $2g = 2 - N - s$, soit $N = 2(1-g) - s \leq 2 - s$ et puisque N et s sont des entiers naturels strictement positifs et que $g \geq 0$, on en déduit que $N = 1$ et donc $\mathbb{L} = \overline{\mathbb{F}_q}(T)$ et on a le résultat.

Pour conclure, il suffit de remarquer que par ce qui précède χ_i^n se factorise au travers du groupe de Galois cyclique $\mathrm{Gal}\left(\mathbb{F}_{q^d}F/F\right) \cong \mathbb{Z}/d\mathbb{Z}$ pour un certain $d \in \mathbb{N}^*$ (engendré par le Frobenius). Ainsi, il existe $\zeta \in \mathbb{F}_\lambda^\times$ pour lequel pour tout idéal premier non nul $\mathfrak{p}$ de A on ait $\chi_i^n(\mathrm{Frob}_\mathfrak{p}) = \zeta^{\deg(\mathfrak{p})}$. Enfin, pour $\mathfrak{p} \neq \lambda$ et en utilisant le fait que ϕ ait une bonne réduction en $\mathfrak{p}$, on trouve que $\chi_i^n(\mathrm{Frob}_\mathfrak{p}) = \zeta^{\deg(\mathfrak{p})}$ est une racine de $(x - \chi_1^n(\mathrm{Frob}_\mathfrak{p}))\,(x - \chi_2^n(\mathrm{Frob}_\mathfrak{p})) \equiv \det(xI_2 - \overline{\rho}_{\phi,\lambda}(\mathrm{Frob}_\mathfrak{p})^n) \equiv P_{\phi,\mathfrak{p}}^{(n)}(x)\ [\lambda]$ (par la proposition 4.7).

■

Proposition 4.9 :
Soient n un entier naturel non tel que les deux points du lemme 4.14 soient vrais et $d \in \mathbb{N}^*$ tel que ϕ ait une bonne réduction en plusieurs idéaux premiers non nuls de A de degré d.
On a la majoration $\deg(\lambda) \leq 2nd$.

Preuve :
Soient n un entier naturel non tel que les deux points du lemme 4.14 soient vrais et $d \in \mathbb{N}^*$ tel que ϕ ait une bonne réduction pour plusieurs idéaux premiers non nuls de A de degré d.

Posons $\mathfrak{p}_1$ et $\mathfrak{p}_2$ deux idéaux premiers non nuls de A distincts tels que $\deg(\mathfrak{p}_1) = \deg(\mathfrak{p}_2) = d$ et ϕ ait bonne réduction en $\mathfrak{p}_1$ et $\mathfrak{p}_2$. Nous pouvons supposer que $\lambda \notin \{\mathfrak{p}_1;\mathfrak{p}_2\}$ car sinon on a directement $\deg(\lambda) = d \leq 2nd$.

Pour tout $i \in \{1;2\}$, notons $Q_i(x) := P^{(n)}_{\phi,\mathfrak{p}_i}(x) \in A[x]$ ainsi que r le résultant des polynômes $Q_1(x)$ et $Q_2(x)$. Grâce à notre choix de n, par le lemme 4.15 on obtient que $Q_1(x)$ et $Q_2(x)$ ont une racine commune modulo λ et donc $r \equiv 0\ [\lambda]$.

Soient $\mathbb{L}/\mathbb{F}$ le corps de décomposition de $P_{\phi,\mathfrak{p}_1}(x)$ et $P_{\phi,\mathfrak{p}_2}(x)$ et $|\cdot|_\infty$ une valeur absolue sur $\mathbb{L}$ telle que $|a|_\infty = q^{\deg(a)}$ pour tout $a \in A$.
Pour tout $\pi \in \mathbb{L}$ racine des $P_{\phi,\mathfrak{p}_i}(x)$ on a $|\pi|_\infty = N(\mathfrak{p}_i)^{\frac{1}{2}} = q^{\frac{\deg(\mathfrak{p}_i)}{2}} = q^{\frac{d}{2}}$ par le cinquième point du théorème 4.12.8 à la page 105 de [Gos96].

Ainsi, pour toute racine $\pi \in \mathbb{L}$ de $Q_i(x)$, on a $|\pi|_\infty = q^{\frac{nd}{2}}$. Or dans $\mathbb{L}$, on a une expression de r comme le produit des $\pi_1 - \pi_2$ (car les $Q_i(x)$ sont unitaires) avec π_1 racine de $Q_1(x)$ et π_2 racine de $Q_2(x)$ dans $\mathbb{L}$. D'où :

$$|r|_\infty = \left|\prod_{i=1}^{2}\prod_{j=1}^{2}(\pi_{1,i} - \pi_{2,j})\right|_\infty = \prod_{i=1}^{2}\prod_{j=1}^{2}|\pi_{1,i} - \pi_{2,j}|_\infty \leq \prod_{i=1}^{2}\prod_{j=1}^{2} q^{\frac{nd}{2}} = q^{2nd}.$$

Montrons par l'absurde que $Q_1(x)$ et $Q_2(x)$ n'ont pas de racines communes dans $\mathbb{L}$:
Considérons $\pi \in \mathbb{L}$ une racine de $Q_1(x)$ et $Q_2(x)$ et $i \in \{1;2\}$.
Par le premier point du théorème 4.12.8 à la page 105 de [Gos96] appliqué à la réduction de ϕ modulo $\mathfrak{p}_i$, il existe une unique place de $F(\pi)$ pour laquelle π a une racine et qui est située au dessus de $\mathfrak{p}_i$. On aboutit alors à une contradiction étant donné que $\mathfrak{p}_1 \neq \mathfrak{p}_2$.

Finalement, comme $Q_1(x)$ et $Q_2(x)$ n'ont pas de racines communes dans $\mathbb{L}$, on obtient que $r \neq 0$ et puisque $q \geq 2$ et $|r|_\infty \leq q^{2nd}$ on a $\deg(r) \leq 2nd$. Enfin, puisque r est non nul et que $r \equiv 0\ [\lambda]$, on a $\deg(\lambda) \leq \deg(r)$ et ainsi :

$$\deg(\lambda) \leq \deg(r) \leq 2nd.$$

■

VII Irréductibilité de Hilbert

Dans toute cette partie, on considère un entier naturel $r \geq 2$ et $\mathfrak{a}$ un idéal non nul de A.

Pour tout $a := (a_1, ..., a_r) \in A^r$ tel que $a_r \neq 0$, on pose $\phi(a) : A \longrightarrow F\{\tau\}$ le module de Drinfeld de rang r défini par $\phi(a)_T := T + \sum_{i=1}^{r} a_i \tau^i$ et on pose

$$\overline{\rho}_{\phi(a),\mathfrak{a}} : \mathrm{Gal}_F \longrightarrow \mathrm{GL}_r(A/\mathfrak{a})$$

la représentation galoisienne correspondante.

Le but de cette partie est de démontrer le théorème suivant (qui dit grossièrement que $\overline{\rho}_{\phi(a),\mathfrak{a}}$ est surjective "pour presque tout" a) :

Théorème 4.4 :
L'ensemble des $a := (a_1, ..., a_r) \in A^r$ tels que $a_r \neq 0$ et $\overline{\rho}_{\phi(a),\mathfrak{a}}(\mathrm{Gal}_F) = \mathrm{GL}_r(A/\mathfrak{a})$ a pour densité 1.

VII.1 Une version du théorème d'irréductibilité de Hilbert

Considérons un entier naturel non nul r, un sous-schéma ouvert non vide U de $\mathbb{A}^r_F$ ainsi qu'une représentation continue et surjective $\rho : \pi_1(U) \longrightarrow G$, où $\pi_1(U)$ est le groupe fondamental étale et G un groupe fini.

Ici, on supprime le point de base de notre groupe fondamental, ainsi la représentation ρ est uniquement déterminée à conjugaison près par un élément de G. En prenant un point $u \in U(F) \subseteq F^r$ et en évaluant en u, on obtient une représentation continue

$$\rho_u : \mathrm{Gal}_F \xrightarrow{u_*} \pi_1(U) \xrightarrow{\rho} G$$

qui est uniquement déterminée à conjugaison près par un élément de G. En particulier, le groupe $\rho_u(\mathrm{Gal}_F) \subseteq G$ est aussi uniquement déterminée à conjugaison près par un élément de G.

Nous allons donc montrer que $\rho_u(\mathrm{Gal}_F) = G$ pour tout $u \in U(F) \cap A^r$ hors d'un ensemble de densité 0 après avoir montré le lemme suivant :

Lemme 4.16 :
Soient I un idéal non nul de A et B un sous-ensemble de $(A/I)^r$.
L'ensemble des éléments $a \in A^r$ dont l'image modulo I appartient à B a pour densité $\frac{\mathrm{Card}(B)}{N(I)^r}$.

Preuve :
Soient I un idéal non nul de A et B un sous-ensemble de $(A/I)^r$.
Considérons un entier naturel non nul d ainsi que l'application $\varphi_d : A^r(d) \longrightarrow (A/I)^r$.
φ_d est un morphisme de groupes additifs finis et on a $I = (Q)$ avec $Q \in A$ (car $A = \mathbb{F}_q[T]$ est principal). De plus, on a les égalités :

$$\mathrm{Card}(A^r(d)) = \mathrm{Card}(\{(a_1, ..., a_r) \in A^r \mid \forall i \in [\![1; r]\!],\ \deg(a_i) \leq d\}) = \left(q^{d+1}\right)^r = q^{r(d+1)}$$

et

$$\mathrm{Card}\left((A/I)^r\right) = \left(q^{\deg(Q)}\right)^r = q^{r\deg(Q)}.$$

Ainsi, en prenant $d \geq \deg(Q) - 1$, on trouve que φ_d est un morphisme de groupes finis surjectif et ainsi les $\varphi_d^{-1}(b)$ ont tous le même cardinal pour tout $b \in (A/I)^r$. En effet, $\left(\varphi_d^{-1}(\{b\})\right)_{b \in (A/I)^r}$ forme une partition de $A^r(d)$ (par surjectivité de φ_d) pour la relation d'équivalence :

$$\forall g, \widetilde{g} \in A^r(d),\ g \sim \widetilde{g} \iff \varphi_d(g) = \varphi_d\left(\widetilde{g}\right).$$

Or, φ_d est un morphisme de groupes, donc les classes d'équivalences sont exactement les $\mathrm{Ker}(\varphi_d).g$ pour $g \in A^r(d)$. En effet, pour $g, \widetilde{g} \in A^r(d)$, on a :

$$g \sim \widetilde{g} \iff \varphi_d(g) = \varphi_d\left(\widetilde{g}\right) \iff \varphi_d\left(g\widetilde{g}^{-1}\right) = \left(\overline{0}, \ldots, \overline{0}\right) \iff g\widetilde{g}^{-1} \in \mathrm{Ker}(\varphi_d) \iff g = \mathrm{Ker}(\varphi_d).\widetilde{g}.$$

On a alors une bijection entre toutes les classes d'équivalences et ainsi elles ont toutes le même cardinal.

Par conséquent, on a $\mathrm{Card}\left(\varphi_d^{-1}(B)\right) = \mathrm{Card}(B)$ et donc par surjectivité de φ_d on a :

$$\frac{\mathrm{Card}\left(\varphi_d^{-1}(B)\right)}{\mathrm{Card}\left(A^r(d)\right)} = \frac{\sum_{b \in B} \mathrm{Card}\left(\varphi_d^{-1}(\{b\})\right)}{\mathrm{Card}\left(A^r(d)\right)} = \frac{\mathrm{Card}(B) \times \frac{\mathrm{Card}(A^r(d))}{\mathrm{Card}((A/I)^r)}}{\mathrm{Card}\left(A^r(d)\right)} = \frac{\mathrm{Card}(B)}{\mathrm{Card}\left((A/I)^r\right)} = \frac{\mathrm{Card}(B)}{N(I)^r},$$

donc $\delta(B)$ existe et :

$$\delta(B) = \lim_{d \to +\infty} \frac{\mathrm{Card}\left(\varphi_d^{-1}(B)(d)\right)}{\mathrm{Card}\left(A^r(d)\right)} = \lim_{d \to +\infty} \frac{\mathrm{Card}(B(d))}{\mathrm{Card}\left((A/I)^r\right)} = \lim_{d \to +\infty} \frac{\mathrm{Card}(B)}{\mathrm{Card}\left((A/I)^r\right)} = \frac{\mathrm{Card}(B)}{N(I)^r}.$$

■

Théorème 4.5 :
L'ensemble des $u \in U(F) \cap A^r$ pour lesquels $\rho_u(\mathrm{Gal}_F) = G$ a pour densité 1.

Preuve :
Pour une clôture algébrique $\overline{F}$ de F, on définit le groupe $G_g := \rho(\pi_1(U_{\overline{F}}))$ qui est un sous-groupe fermé et distingué de G.

En notant F'/F la plus petite extension dans $\overline{F}$ pour laquelle $G_g = \rho(\pi_1(U_{F'}))$, on obtient que cette extension est galoisienne et on a la suite exacte courte suivante :

$$1 \longrightarrow G_g \longrightarrow G \xrightarrow{\pi} \mathrm{Gal}(F'/F) \longrightarrow 1 \ .$$

Considérons H un sous-groupe propre de G et S l'ensemble des $u \in U(F) \cap A^r$ tels que $\rho_u(\mathrm{Gal}_F)$ est conjugué dans G à un sous-groupe de H.
Nous allons démontrer que S a pour densité 0 et cela nous donnera le résultat puisque G n'a qu'un nombre fini de sous-groupes propres.

Pour tout $u \in U(F)$, on a $\pi(\rho_u(\mathrm{Gal}_F)) = \mathrm{Gal}(F'/F)$, on peut donc supposer que $\pi(H) = \mathrm{Gal}(F'/F)$ puisque sinon S est vide et on a le résultat. On a alors $H \cap G_g \subsetneq G_g$ puisque H est un sous-groupe propre de G. De plus, en posant $C := \bigcup_{g \in G} gHg^{-1}$, on a

$$C \cap G_g = \bigcup_{g \in G} g(H \cap G_g)g^{-1} = \bigcup_{g \in G_g} g(H \cap G_g)g^{-1}$$

puisque G_g est un sous-groupe distingué de G et que $\pi(H) = \mathrm{Gal}(F'/F)$. Comme $H \cap G_g$ est un sous-groupe propre de G_g, on a également que $C \cap G_g \subsetneq G_g$ par le lemme de Jordan (dont on pourra trouver un énoncé au théorème 4' de la page 435 de [Ser03]).

Il existe un anneau $R := A\left[\frac{1}{n}\right] \subseteq F$ avec $n \in A$ non nul, un R-sous-schéma $\mathcal{U} \subseteq \mathbb{A}^r_R$ et une représentation $\varrho : \pi_1(\mathcal{U}) \longrightarrow G$ tels que $\mathcal{U}_F = U$ et le changement de base de ϱ par F donne ρ.
Considérons un idéal premier non nul $\mathfrak{p}$ de A qui ne divise pas n et nous noterons également par $\mathfrak{p}$ l'idéal premier $\mathfrak{p}R$ de R.
On a alors $R/\mathfrak{p} = A/\mathfrak{p} = \mathbb{F}_\mathfrak{p}$. De plus, pour tout $u \in \mathcal{U}(\mathbb{F}_\mathfrak{p})$, l'évaluation donne un morphisme $u_* : \mathrm{Gal}_{\mathbb{F}_\mathfrak{p}} \longrightarrow \pi_1(\mathcal{U})$ et on note Frob_u l'image de la puissance $N(\mathfrak{p})$-ième du Frobenius (remarquons au passage que Frob_u dans $\pi_1(\mathcal{U})$ est uniquement déterminé à la conjugaison près).

Considérons désormais l'ensemble

$$\Omega_\mathfrak{p} := \{u \in \mathcal{U}(\mathbb{F}_\mathfrak{p}) \mid \varrho(\mathrm{Frob}_u) \in G \backslash C\}.$$

Pour $u \in S$, on a $\rho_u(\mathrm{Gal}_F) \subseteq C$ et si u modulo $\mathfrak{p}$ appartient à $\mathcal{U}(\mathbb{F}_\mathfrak{p})$, alors ρ_u est non ramifiée en $\mathfrak{p}$ et $\rho_u(\mathrm{Frob}_\mathfrak{p})$ appartient à la même classe de conjugaison dans G que $\varrho(\mathrm{Frob}_u)$. Ainsi, si u modulo $\mathfrak{p}$ appartient à $\Omega_\mathfrak{p}$, alors $\rho_u(\mathrm{Frob}_\mathfrak{p})$ appartient à $G \backslash C$, ce qui contredit le fait que $\rho_u(\mathrm{Gal}_F) \subseteq C$.

Ainsi, l'image de S modulo $\mathfrak{p}$ appartient à $\mathbb{F}_\mathfrak{p}^r \backslash \Omega_\mathfrak{p}$, donc par le lemme 4.16, on a :

$$\overline{\delta}(S) \leq \prod_{p \in \mathcal{P}} \frac{\mathrm{Card}(\mathbb{F}_\mathfrak{p}^r \backslash \Omega_\mathfrak{p})}{\mathrm{Card}(\mathbb{F}_\mathfrak{p}^r)} = \prod_{p \in \mathcal{P}} \left(1 - \frac{\mathrm{Card}(\Omega_\mathfrak{p})}{N(\mathfrak{p})^r}\right),$$

où $\mathcal{P}$ est un ensemble fini d'idéaux premiers non nuls de A ne divisant pas n.

Ainsi, pour montrer que S a pour densité 0, il suffit de montrer qu'il existe une constante $c \in]0;1[$ telle que pour presque tout idéal premier $\mathfrak{p}$ de A on ait $1 - \frac{\mathrm{Card}(\Omega_\mathfrak{p})}{N(\mathfrak{p})^r} < c$.

Considérons maintenant un idéal premier non nul $\mathfrak{p}$ de A qui se décompose complètement dans F' et qui ne divise pas n (le fait que $\mathfrak{p}$ se décompose totalement dans F' implique que $\varrho(\pi_1(\mathcal{U}_{\mathbb{F}_\mathfrak{p}})) \subseteq G_g$).
Montrons que $\varrho(\pi_1(\mathcal{U}_{\overline{\mathbb{F}}_\mathfrak{p}})) = G_g$ pour presque tout les tels $\mathfrak{p}$ sauf en nombre fini :
Notons R' la clôture intégrale de R dans F'.

On peut faire un changement de base pour ρ pour obtenir une représentation surjective $\varrho' : \pi_1(\mathcal{U}_{R'}) \longrightarrow G_g$.

Pour prouver notre résultat, il nous suffit de montrer que $\varrho'(\pi_1((\mathcal{U})_{\mathbb{F}_\mathfrak{P}}))$ est égal à G_g pour presque tout idéal premier non nul $\mathfrak{P}$ de R' sauf un nombre fini.
La représentation ϱ' correspond à un recouvrement étale $Y \longrightarrow \mathcal{U}_{R'}$ de R'-schémas tel que $Y_{F'}$ et $(\mathcal{U}_{R'})_{F'} = \mathcal{U}_{F'}$ soient tous les deux géométriquement irréductibles. Or, pour tout idéal premier non nul $\mathfrak{P}$ de R', on a un recouvrement étale $Y_{\mathbb{F}_\mathfrak{P}} \longrightarrow \mathcal{U}_{\mathbb{F}_\mathfrak{P}}$ de degré $\mathrm{Card}(G_g)$ et le résultat suit du fait que $Y_{\mathbb{F}_\mathfrak{P}}$ et $\mathcal{U}_{\mathbb{F}_\mathfrak{P}}$ sont tous les deux géométriquement irréductibles pour presque tout idéal $\mathfrak{P}$ de R' (cf. proposition 9.7.8 à la page 82 de [Gro66]).

Ainsi, en excluant un nombre fini de $\mathfrak{p}$, on peut supposer que $\varrho(\pi_1(\mathcal{U}_{\mathbb{F}_\mathfrak{p}})) = \varrho(\pi_1(\mathcal{U}_{\overline{\mathbb{F}}_\mathfrak{p}})) = G_g$. Par conséquent, un résultat d'équidistribution ressemblant au théorème 3 de la page 9 de [Ent21] donne :

$$\mathrm{Card}(\Omega_\mathfrak{p}) = \mathrm{Card}(\{u \in \mathcal{U}(\mathbb{F}_\mathfrak{p}) \mid \varrho(\mathrm{Frob}_u) \in G_g \backslash (C \cap G_g)\}) = \frac{\mathrm{Card}(G_g \backslash (C \cap G_g))}{\mathrm{Card}(G_g)} + O\left(N(\mathfrak{p})^{r-\frac{1}{2}}\right),$$

où la constante implicite ne dépend pas de $\mathfrak{p}$.

Pour appliquer le théorème 3 de la page 9 de [Ent21], on utilise le fait que la "complexité" des $Y_{\mathbb{F}_\mathfrak{P}} \longrightarrow \mathcal{U}_{\mathbb{F}_\mathfrak{P}}$ peut être bornée indépendamment de l'idéal premier non nul $\mathfrak{P}$ de R' considéré puisqu'ils proviennent d'un seul morphisme $Y \longrightarrow \mathcal{U}_{R'}$.

Finalement, on a

$$1 - \frac{\mathrm{Card}(\Omega_\mathfrak{p})}{N(\mathfrak{p})^r} = \frac{\mathrm{Card}(C \cap G_g)}{\mathrm{Card}(G_g)} + O\left(N(\mathfrak{p})^{-\frac{1}{2}}\right)$$

et puisque $C \cap G_g \subsetneq G_g$, il existe une constante $c \in]0;1[$ telle que $1 - \frac{\mathrm{Card}(\Omega_\mathfrak{p})}{N(\mathfrak{p})^r} < c$ pour presque tout idéal premier non nul $\mathfrak{p}$ de A qui se décompose totalement sur F'. Le résultat en découle alors puisqu'il y a une infinité d'idéaux premiers $\mathfrak{p}$ de A qui se décomposent totalement sur F'.

■

VII.2 Preuve du théorème 4.4

Dans toute cette sous-partie, on considère la F-algèbre $R := F\left[b_1, \ldots, b_r, \frac{1}{b_r}\right]$ avec $b_1, \ldots, b_r$ des indéterminées sur F et $\phi : A \longrightarrow \mathcal{R}\{\tau\}$ le morphisme de $\mathbb{F}_q$-algèbres défini par $\phi_T := T + \sum_{i=1}^{r} b_i \tau^i$.

On constate que ϕ est un module de Drinfeld de rang r sur le schéma $U := \mathrm{Spec}(R)$ (avec U non vide et qui est un sous-schéma ouvert de $\mathbb{A}^r_F := \mathrm{Spec}(F[b_1, \ldots, b_r])$.

La $\mathfrak{a}$-torsion de ϕ nous donne comme d'habitude une représentation $\overline{\rho}_{\phi,\mathfrak{a}} : \pi_1(U) \longrightarrow \mathrm{GL}_r(A/\mathfrak{a})$. De plus, pour $a := (a_1, \ldots, a_r) \in U(F) \subseteq F^r$, on a $a_r \neq 0$ et en remplaçant les b_i par des a_i dans la définition de ϕ on obtient un nouveau module de Drinfeld $\phi(a) : A \longrightarrow F\{\tau\}$ de rang r.

Lemme 4.17 :
On a $\overline{\rho}_{\phi,\mathfrak{a}}(\pi_1(U)) = \mathrm{GL}_r(A/\mathfrak{a})$.

Preuve :
Soit V une sous-variété fermée de U définie par l'équation $b_r = 1$ (c'est-à-dire correspondant à l'idéal premier $\beta = (b_r - 1)$).
En évaluant $\overline{\rho}_{\phi,\mathfrak{a}}$ en β, on obtient une représentation $\varrho : \pi_1(V) \longrightarrow \mathrm{GL}_r(A/\mathfrak{a})$. Il nous suffit donc de montrer que ϱ est surjective. Or, la représentation ϱ correspond à $\overline{\rho}_{\psi,\mathfrak{a}}$, avec $\psi : A \longrightarrow R'\{\tau\}$ le module de Drinfeld défini par $\psi_T := T + \sum_{i=1}^{r-1} b_i \tau^i + \tau^i$ et $R' := F[b_1, ..., b_{r-1}]$.

Ainsi, en posant $\mathbb{K} := F(b_1, ..., b_{r-1})$ et en voyant ψ comme un module de Drinfeld sur $\mathbb{K}$, il nous suffit de

montrer que $\mathrm{Gal}(\mathbb{K}(\psi[\mathfrak{a}])/\mathbb{K}) \cong \mathrm{GL}_r(A/\mathfrak{a})$ (avec $\psi[\mathfrak{a}]$ la $\mathfrak{a}$-torsion de ψ dans une clôture séparable fixée de $\mathbb{K}$). Or, c'est exactement le théorème 6 de la page 442 de [Bre16].

■

Enfin, en évaluant la représentation $\overline{\rho}_{\phi,\mathfrak{a}}$ en $a = (a_1, \ldots, a_r) \in A^r$ avec $a_r \neq 0$ on obtient une représentation $\overline{\rho}_{\phi,\mathfrak{a}} \circ \rho_a : \mathrm{Gal}_F \longrightarrow \mathrm{GL}_r(A/\mathfrak{a})$ (avec $\rho_a : \mathrm{Gal}_F \longrightarrow \pi_1(U)$ la spécialisation en a) qui est isomorphe à $\overline{\rho}_{\phi(a),\mathfrak{a}}$. De plus, par le théorème 4.5, il existe un sous-ensemble $\mathcal{E}$ de $A^r \cap U(F)$ de densité 1 tel que

$$\forall a \in \mathcal{E},\ \rho_a(\mathrm{Gal}_F) = \pi_1(U)$$

et en particulier on a par le lemme 4.17 que :

$$\forall a \in \mathcal{E},\ \overline{\rho}_{\phi(a),\mathfrak{a}}(\mathrm{Gal}_F) = \overline{\rho}_{\phi,\mathfrak{a}}(\pi_1(U)) = \mathrm{GL}_r(A/a),$$

d'où le résultat annoncé dans le théorème 4.4.

Chapitre 5

Preuve du théorème 0.3

Le but de ce cinquième chapitre est de démontrer le théorème 0.3 donné en introduction. Pour cela, nous allons le séparer en deux parties : dans la partie I nous allons donner la preuve du théorème dans le cas où $q \neq 2$ puis dans la partie II nous allons traiter le cas où $q = 2$. Dans tout ce chapitre, nous utiliserons donc les résultats préliminaires établis dans le chapitre 4.

I Preuve dans le cas $q \neq 2$

Dans toute cette partie, on considère $\mathcal{B}$ l'ensemble des $a = (a_1, a_2) \in A^2$ tels que $a_2 \neq 0$ pour lesquels on a :

* $\rho_{\phi(a),\lambda}(\mathrm{Gal}_F) = \mathrm{GL}_2(A_\lambda)$ pour tout idéal premier non nul λ de A ;
* Le groupe dérivé de $\rho_{\phi(a)}(\mathrm{Gal}_F) \subseteq \mathrm{GL}_2(\widehat{A})$ est égal à $D\left(\mathrm{GL}_2(\widehat{A})\right)$.

L'objectif principal de la sous-partie I.1 est de prouver le théorème suivant qui sera utilisé dans la sous-partie I.2 pour démontrer le théorème 0.3 dans le cas $q \neq 2$.

Théorème 5.1 :
L'ensemble $\mathcal{B}$ a pour densité 1.

Pour toute la suite de cette partie, on considère un entier naturel $m \geq 2$ et on pose les ensembles suivants :

* $\mathcal{R}$ est l'ensemble des $(a_1, a_2) \in A^2$ pour lesquels il existe au moins deux idéaux premiers distincts non nuls $\mathfrak{p}$ de A tels que $\deg(\mathfrak{p}) > 1$, $v_\mathfrak{p}(a_1) = 0$ et $v_\mathfrak{p}(a_2) = 1$;
* $\mathcal{S}_m$ est l'ensemble des $(a_1, a_2) \in A^2$ pour lesquels $a_1 \not\equiv 0\ [p]$ ou $a_2 \not\equiv 0\ [p]$ pour tout idéal premier non nul $\mathfrak{p}$ de A tel que $\deg(\mathfrak{p}) > m$;
* $\mathcal{T}_m$ est l'ensemble des $(a_1, a_2) \in A^2$ pour lesquels il existe deux idéaux premiers distincts $\mathfrak{p}_1$ et $\mathfrak{p}_2$ de A de même degré $d \leq \frac{m}{2(q-1)^2(q+1)}$ tels que $a_2 \not\equiv 0\ [\mathfrak{p}_1]$ et $a_2 \not\equiv 0\ [\mathfrak{p}_2]$;
* $\mathcal{U}_m$ est l'ensemble des $(a_1, a_2) \in A^2$ pour lesquels $a_2 \neq 0$ et $\overline{\rho}_{\phi(a),\lambda^2}(\mathrm{Gal}_F) = \mathrm{GL}_2(A/\lambda^2)$ pour tout idéal premier non nul $\lambda \in A$ tel que $\deg(\lambda) \leq m$.

Nous introduisons ces ensembles pour la raison suivante : plutôt que de montrer que $\mathcal{B}$ a pour densité 1, nous allons montrer que $\mathcal{R} \cap \mathcal{S}_m \cap \mathcal{T}_m \cap \mathcal{U}_m$ est un sous-ensemble de $\mathcal{B}$ et qu'il a pour densité 1.

I.1 Utilisation de techniques de dénombrement

Lemme 5.1 :
Pour tout $a \in \mathcal{R} \cap \mathcal{S}_m \cap \mathcal{T}_m \cap \mathcal{U}_m$ et tout idéal premier non nul λ de A, on a $\rho_{\phi(a),\lambda}(\mathrm{Gal}_F) = \mathrm{GL}_2(A_\lambda)$.

Preuve :
Soient $a \in \mathcal{R} \cap \mathcal{S}_m \cap \mathcal{T}_m \cap \mathcal{U}_m$, λ un idéal premier non nul de A et posons $G := \rho_{\phi(a),\lambda}(\mathrm{Gal}_F)$ un sous-groupe fermé de $\mathrm{GL}_2(A_\lambda)$ (car $\rho_{\phi(a),\lambda}$ est continue et Gal_F est un groupe compact).

Pour l'anneau $R := A_\lambda$, nous allons montrer que G vérifie les hypothèses de la proposition 4.1 et on obtiendra alors par cette même proposition que $G = \mathrm{GL}_2(A_\lambda)$.

* Puisque $a \in \mathcal{R}$, on obtient qu'il existe un idéal premier $\mathfrak{p}$ non nul de A et différent de λ tel que $\deg(\mathfrak{p}) > 1$, $v_\mathfrak{p}(a_1) = 0$ et $v_\mathfrak{p}(a_2) = 1$. De plus, puisque $v_\mathfrak{p}(a_2) = 1$ et que $\mathfrak{p} \neq \lambda$, on obtient par la proposition 4.8 que $\det(G) = A_\lambda^\times$. Ainsi, on a vérifié la première hypothèse de la proposition 4.1.

* Notons $I_\mathfrak{p}$ le groupe d'inertie de Gal_F pour l'idéal premier non nul $\mathfrak{p}$ et considérons $i \in \mathbb{N}^*$.
Puisque $a \in \mathcal{R}$, il existe un idéal premier $\mathfrak{p}$ non nul de A et différent de λ tel que $\deg(\mathfrak{p}) > 1$, $v_\mathfrak{p}(a_1) = 0$ et $v_\mathfrak{p}(a_2) = 1$. En particulier, $\phi(a)$ a une réduction stable de rang 1 par $\mathfrak{p}$ et on note $j_{\phi(a)} := \frac{a_1^{q+1}}{a_2} \in F$ son j-invariant. On a alors $v_\mathfrak{p}\left(j_{\phi(a)}\right) = (q+1)v_\mathfrak{p}(a_1) - v_\mathfrak{p}(a_2) = -1$ et par le troisième point de la proposition 4.6 nous donne que $\overline{\rho}_{\phi(a),\lambda^i}(I_\mathfrak{p})$ contient un sous-groupe d'ordre $N(\lambda)^i$ qui est conjugué dans $\mathrm{GL}_2(A/\lambda^i)$ à $\left\{\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix},\ b \in A/\lambda^i\right\}$. Après avoir choisi une base appropriée de $\phi\left[\lambda^i\right]$, on peut supposer que

$$\left\{\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix},\ b \in A/\lambda^i\right\} \subseteq \overline{\rho}_{\phi(a),\lambda^i}(\mathrm{Gal}_F). \tag{5.1}$$

On a alors $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in G$, ce qui nous donne la cinquième hypothèse de la proposition 4.1. De plus, avec $i = 2$, (5.1) nous donne également la troisième hypothèse de la proposition 4.1 et si $N(\lambda) = 2$, alors $\overline{\rho}_{\phi(a),\lambda^2}(\mathrm{Gal}_F) = \mathrm{GL}_2(A/\lambda^2)$ (puisque $a \in \mathcal{U}_m$ et que $m \geq 2$) ce qui nous donne aussi la quatrième hypothèse de la proposition 4.1.

* Il nous reste à vérifier la deuxième hypothèse de la proposition 4.1, c'est-à-dire à montrer que l'on a l'égalité $\overline{\rho}_{\phi(a),\lambda}(\mathrm{Gal}_F) = \mathrm{GL}_2(A/\lambda) = \mathrm{GL}_2(\mathbb{F}_\lambda)$.
Puisque $a \in \mathcal{U}_m$, il nous suffit de traiter le cas où $\deg(\lambda) > m$ (sinon le résultat est alors immédiat). De plus, puisque $a \in \mathcal{S}_m$, on a $a_1 \not\equiv 0\ [\lambda]$ ou $a_2 \not\equiv 0\ [\lambda]$. Ainsi, $\phi(a)$ a une réduction stable en λ et puisque $\overline{\rho}_{\phi(a),\lambda}(\mathrm{Gal}_F)$ contient un sous-groupe d'ordre $N(\lambda) = \mathrm{Card}(A/\lambda)$ (par (5.1) en prenant $i = 1$), on obtient par la proposition 4.2 que $\overline{\rho}_{\phi(a),\lambda}$ est réductible ou bien irréductible et donc $\mathrm{SL}_2(\mathbb{F}_\lambda) \subseteq \overline{\rho}_{\phi(a),\lambda}(\mathrm{Gal}_F)$.

Supposons que $\overline{\rho}_{\phi(a),\lambda}$ est réductible.
Puisque $a \in \mathcal{T}_m$, il existe deux idéaux premiers distincts $\mathfrak{p}_1$ et $\mathfrak{p}_2$ de A de même degré $d \leq \frac{m}{2(q-1)^2(q+1)}$ tels que $\phi(a)$ ait une bonne réduction en $\mathfrak{p}_1$ et $\mathfrak{p}_2$. Or, par la proposition 4.9 avec $n := (q-1)^2(q+1)$, on obtient :

$$\deg(\lambda) \leq 2nd \leq \frac{2(q-1)^2(q+1)m}{2(q-1)^2(q+1)} \leq m.$$

Ce qui aboutit à une contradiction car on a supposé que $\deg(\lambda) > m$ et donc $\overline{\rho}_{\phi(a),\lambda}$ est irréductible et donc $\mathrm{SL}_2(\mathbb{F}_\lambda) \subseteq \overline{\rho}_{\phi(a),\lambda}(\mathrm{Gal}_F)$.

Enfin, puisque $\det(G) = A_\lambda^\times$, on en déduit que $\det\left(\overline{\rho}_{\phi(a),\lambda}(\mathrm{Gal}_F)\right) = \mathbb{F}_\lambda^\times$ et donc on a l'égalité $\overline{\rho}_{\phi(a),\lambda}(\mathrm{Gal}_F) = \mathrm{GL}_2(\mathbb{F}_\lambda)$. En effet, par le théorème de factorisation des morphismes de groupes on a le diagramme commutatif suivant :

$$\begin{array}{ccc} \overline{\rho}_{\phi(a),\lambda}(\mathrm{Gal}_F) & \xrightarrow{f := \det|_{G_\lambda}} & \mathbb{F}_\lambda^\times \\ \downarrow & \nearrow & \\ \overline{\rho}_{\phi(a),\lambda}(\mathrm{Gal}_F)/\,\mathrm{SL}_2(\mathbb{F}_\lambda) & & \end{array}$$

On a alors $\overline{\rho}_{\phi(a),\lambda}(\mathrm{Gal}_F)/\,\mathrm{Ker}(f) \cong \mathbb{F}_\lambda^\times$ par le premier théorème d'isomorphisme et comme les groupes en jeu sont finis on a également que $\mathrm{Card}\left(\overline{\rho}_{\phi(a),\lambda}(\mathrm{Gal}_F)\right) = \mathrm{Card}(\mathrm{Ker}(f))\,\mathrm{Card}(\mathbb{F}_\lambda^\times)$. Or, $\mathrm{SL}_2(\mathbb{F}_\lambda) \subseteq \mathrm{Ker}(f)$,

d'où la majoration $\mathrm{Card}(\mathrm{SL}_2(\mathbb{F}_\lambda)) \leq \mathrm{Card}(\mathrm{Ker}(f))$, d'où :

$$\mathrm{Card}\left(\overline{\rho}_{\phi(a),\lambda}(\mathrm{Gal}_F)\right) \geq \mathrm{Card}(\mathrm{SL}_2(\mathbb{F}_\lambda)) \times \mathrm{Card}(\mathbb{F}_\lambda^\times) = \mathrm{Card}(\mathrm{GL}_2(\mathbb{F}_\lambda)).$$

Or, comme $\overline{\rho}_{\phi(a),\lambda}(\mathrm{Gal}_F)$ est un sous-groupe de $\mathrm{GL}_2(\mathbb{F}_\lambda)$, on a bien que $\overline{\rho}_{\phi(a),\lambda}(\mathrm{Gal}_F) = \mathrm{GL}_2(\mathbb{F}_\lambda)$. On obtient ainsi la deuxième hypothèse de la proposition 4.1.

Comme dit au début de la preuve, on peut alors appliquer la proposition 4.1 et on obtient que $G = \mathrm{GL}_2(A_\lambda)$.

■

Lemme 5.2 :
Soit $a \in \mathcal{R} \cap \mathcal{S}_m \cap \mathcal{T}_m \cap \mathcal{U}_m$.
Le groupe dérivé de $\rho_{\phi(a)}(\mathrm{Gal}_F) \subseteq \mathrm{GL}_2(\widehat{A})$ est égal à $D\left(\mathrm{GL}_2(\widehat{A})\right)$.

Preuve :
Soit $a \in \mathcal{R} \cap \mathcal{S}_m \cap \mathcal{T}_m \cap \mathcal{U}_m$ et posons $G := \rho_{\phi(a)}(\mathrm{Gal}_F)$ un sous-groupe fermé de $\mathrm{GL}_2(\widehat{A})$ (car $\rho_{\phi(a)}$ est continue et Gal_F est un groupe compact).
Pour montrer le résultat, il suffit de montrer que G vérifie les conditions du théorème 4.1 :

* Pour tout idéal premier non nul λ de A, on a $G_\lambda = \mathrm{GL}_2(\mathbb{F}_\lambda)$ par le lemme 5.1 (où G_λ est l'image de G par la projection $\mathrm{GL}_2(\widehat{A}) \longmapsto \mathrm{GL}_2(A_\lambda)$) et donc G vérifie la première hypothèse du théorème 4.1.

* Soient λ_1, λ_2 deux idéaux premiers non nuls distincts de A tels que $N(\lambda_1) = N(\lambda_2) > 3$.
Puisque $a \in \mathcal{R}$, il existe un idéal premier non nul $\mathfrak{p}$ de A tel que $v_\mathfrak{p}(a_1) = 0$, $v_\mathfrak{p}(a_2) = 1$ et $\deg(\mathfrak{p}) > 1$.
En particulier, $\phi(a)$ a une réduction stable de rang 1 et $v_\mathfrak{p}\left(j_{\phi(a)}\right) = -1$.
Notons $I_\mathfrak{p}$ le sous-groupe d'inertie de Gal_F pour l'idéal premier $\mathfrak{p}$. Par le troisième point de la proposition 4.6 on obtient que $\overline{\rho}_{\phi(a),\lambda_1\lambda_2}(I_\mathfrak{p})$ contient un sous-groupe de cardinal $N(\lambda_1\lambda_2) = N(\lambda_1)N(\lambda_2) = N(\lambda_1)^2$.
En particulier, l'image de G modulo $\lambda_1\lambda_2$ a un sous-groupe de cardinal $N(\lambda_1)^2$, ce qui montre que G vérifie la deuxième hypothèse du théorème 4.1.

* Soient λ_1, λ_2 deux idéaux premiers non nuls distincts de A tels que $N(\lambda_1) = N(\lambda_2) = 2$.
Puisque $a \in \mathcal{R}$, il existe un idéal premier non nul $\mathfrak{p}$ de A tel que $v_\mathfrak{p}(a_1) = 0$, $v_\mathfrak{p}(a_2) = 1$ et $\deg(\mathfrak{p}) > 1$. En particulier, on a $\mathfrak{p} \notin \{\lambda_1; \lambda_2\}$ (car $\deg(\mathfrak{p}) > 1$), $\phi(a)$ a une réduction stable de rang 1 et $v_\mathfrak{p}\left(j_{\phi(a)}\right) = -1$.
Pour tout $i \in \mathbb{N}^*$, le troisième point de la proposition 4.6 implique que $\overline{\rho}_{\phi(a),\lambda_1^i\lambda_2^i}(I_\mathfrak{p})$ contient un sous-groupe qui est conjugué dans $\mathrm{GL}_2(A/\lambda_1^i\lambda_2^i)$ à $\left\{\begin{pmatrix}1 & b\\ 0 & 1\end{pmatrix},\ b \in A/(\lambda_1^i\lambda_2^i)\right\}$ et donc le cardinal de $\overline{\rho}_{\phi(a),\lambda_1^i\lambda_2^i}(I_\mathfrak{p})$ est divisible par $N\left(\lambda_1^i\lambda_2^i\right)$ (par le théorème de Lagrange).
De plus, après avoir choisi des bases appropriées pour les $\phi\left[\lambda_1^i\lambda_2^i\right]$, on peut supposer que

$$\left\{\begin{pmatrix}1 & b\\ 0 & 1\end{pmatrix},\ b \in A_{\lambda_1\lambda_2}\right\} \subseteq \rho_{\phi(a),\lambda_1\lambda_2}(\mathrm{Gal}_F).$$

Ainsi, G vérifie la troisième hypothèse du théorème 4.1.

* Supposons que $q \in \{2;3\}$ et que $\mathfrak{a}$ soit un idéal de A qui est le produit des idéaux premiers de A de degré égal à 1.
Puisque $a \in \mathcal{R}$, il existe un idéal premier non nul $\mathfrak{p}$ de A tel que $v_\mathfrak{p}(a_1) = 0$, $v_\mathfrak{p}(a_2) = 1$ et $\deg(\mathfrak{p}) > 1$.
En particulier, on a également que $\mathfrak{p} \nmid \mathfrak{a}$ et donc par la proposition 4.8 on trouve que pour tout $i \in \mathbb{N}^*$, $\det\left(\overline{\rho}_{\phi,\mathfrak{a}^i}(\mathrm{Gal}_F)\right) = (A/\mathfrak{a}^i)^\times$.
Finalement, G vérifie la dernière hypothèse du théorème 4.1 (car G est dense par ce qui précède et fermé).

Ainsi, par le théorème 4.1, on trouve que le groupe dérivé de $G := \rho_\phi(\mathrm{Gal}_F)$ est égal à $D\left(\mathrm{GL}_2(\widehat{A})\right)$.

■

Grâce aux lemmes 5.1 et 5.2, on obtient l'inclusion $\mathcal{R}\cap\mathcal{S}_m\cap\mathcal{T}_m\cap\mathcal{U}_m\subseteq\mathcal{B}$ et ainsi :

$$A^2\backslash\mathcal{B}\subseteq\left(A^2\backslash\mathcal{R}\right)\cup\left(A^2\backslash\mathcal{S}_m\right)\cup\left(A^2\backslash\mathcal{T}_m\right)\cup\left(A^2\backslash\mathcal{U}_m\right). \tag{5.2}$$

Pour obtenir le résultat du théorème 5.1, il nous suffit de majorer les densités supérieures de chaque terme de l'union par 0 ou une quantité arbitrairement petite.

Lemme 5.3 :
On a $\delta\left(A^2\backslash\mathcal{R}\right)=0$.

Preuve :
Commençons par rappeler que la fonction réciproque de la fonction zêta sur $\mathbb{A}^1_{\mathbb{F}_q}:=\mathrm{Spec}(A)$ est donnée par $\prod_{\mathfrak{p}\in\mathrm{Spec}(A)\backslash\{0_A\}}\left(1-T^{\deg(\mathfrak{p})}\right)=1-qT$.

En considérant $T=\frac{1}{q}$, on a $T^{\deg(\mathfrak{p})}=\frac{1}{q^{\deg(\mathfrak{p})}}=\frac{1}{N(\mathfrak{p})}$ et donc :

$$\lim_{d\to+\infty}\prod_{\substack{\mathfrak{p}\in\mathrm{Spec}(A)\backslash\{0_A\}\\ \deg(\mathfrak{p})\leq d}}\left(1-T^{\deg(\mathfrak{p})}\right)=1-q\times\frac{1}{q}=0.$$

On peut choisir deux ensembles disjoints $\mathcal{P}_1$ et $\mathcal{P}_2$ d'idéaux premiers non nuls de A de degré au moins 2 tels que :

$$\forall i\in\{1;2\},\ \lim_{d\to+\infty}\prod_{\substack{\mathfrak{p}\in\mathcal{P}_i\\ \deg(\mathfrak{p})\leq d}}\left(1-\frac{1}{N(\mathfrak{p})}\right)=0. \tag{5.3}$$

En effet, par la correspondance entre les produits infinis et les séries, il suffit de montrer que l'on peut partitionner la série $\sum_{\mathfrak{p}\in\mathrm{Spec}(A)\backslash\{(0_A)\}}\frac{1}{N(\mathfrak{p})}$ en deux sous-séries divergentes et on peut se resteindre au cas où les idéaux sont de degré au moins 2 car cela ne change rien à la nature des séries en jeux.

Or, on peut dénombrer l'ensemble des idéaux premiers de A de degré supérieur ou égal à 2 et les ranger par degré croissant pour obtenir une suite $(\mathfrak{p}_i)_{i\in\mathbb{N}}$. Ainsi, on pose $\mathcal{P}_1$ comme étant l'ensemble de ces idéaux premiers dont l'indice est pair et $\mathcal{P}_2$ l'ensemble de ces idéaux premiers dont l'indice est impair. On obtient donc que $\mathcal{P}_1$ et $\mathcal{P}_2$ forment la partition voulue car ils contiennent une proportion strictement positive des termes de la suite $(\mathfrak{p}_i)_{i\in\mathbb{N}}$ (autrement dit, les séries $\sum_{p\in\mathcal{P}_1}\frac{1}{N(\mathfrak{p})}$ et $\sum_{p\in\mathcal{P}_2}\frac{1}{N(\mathfrak{p})}$ divergent grâce à une généralisation du test de condensation de Cauchy où l'on prend la suite extraite des temes pairs puis des termes impairs).

Soit $i\in\{1;2\}$.
Considérons l'ensemble S_i des couples $(a_1,a_2)\in A^2$ tels que pour tout $\mathfrak{p}\in\mathcal{P}_i$ on ait $(v_{\mathfrak{p}}(a_1);v_{\mathfrak{p}}(a_2))\neq(0;1)$. Pour $\mathfrak{p}\in\mathcal{P}_i$, on considère également l'ensemble $\Omega_{\mathfrak{p}}$ des couples $(b_1,b_2)\in\left(A/\mathfrak{p}^2\right)^2$ tels que l'on ait $b_1\not\equiv 0\ [\mathfrak{p}]$, $b_2\equiv 0\ [\mathfrak{p}]$ et $b_2\not\equiv 0\ [\mathfrak{p}^2]$.

Pour $\mathfrak{p}\in\mathcal{P}_i$, en écrivant la division euclidienne de b_1 par $\mathfrak{p}$ puis de b_2 par $\mathfrak{p}$ dans $A/\mathfrak{p}^2$, on obtient l'égalité $\mathrm{Card}(\Omega_{\mathfrak{p}})=N(\mathfrak{p})(N(\mathfrak{p})-1)^2$ et on a alors :

$$\begin{aligned}\alpha_{\mathfrak{p}}:=\frac{\mathrm{Card}\left(\left(A/\mathfrak{p}^2\right)^2\backslash\Omega_{\mathfrak{p}}\right)}{\mathrm{Card}\left(\left(A/\mathfrak{p}^2\right)^2\right)}&=1-\frac{\mathrm{Card}(\Omega_{\mathfrak{p}})}{\mathrm{Card}\left(\left(A/\mathfrak{p}^2\right)^2\right)}=1-\left(1-\frac{1}{N(\mathfrak{p})}\right)\left(\frac{1}{N(\mathfrak{p})}-\frac{1}{N(\mathfrak{p}^2)}\right)\\&\leq\left(1-\frac{1}{N(\mathfrak{p})}\right)\left(1+\frac{c}{N(\mathfrak{p}^2)}\right),\end{aligned}$$

où $c=3\geq 1$ est obtenu après une étude de fonction.

Remarquons que l'image de S_i modulo $\mathfrak{p}^2$ appartient à $\left(A/\mathfrak{p}^2\right)^2\backslash\Omega_p$, donc par le lemme 4.16, on obtient :

$$\forall d\in\mathbb{N}^*,\ \overline{\delta}\left(S_i\right)\leq\prod_{\substack{\mathfrak{p}\in\mathcal{P}_i\\ \deg(\mathfrak{p})\leq d}}\alpha_p\leq\prod_{\substack{\mathfrak{p}\in\mathcal{P}_i\\ \deg(\mathfrak{p})\leq d}}\left[\left(1-\frac{1}{N(\mathfrak{p})}\right)\left(1+\frac{c}{N(\mathfrak{p}^2)}\right)\right].$$

En utilisant la fonction zêta sur $\mathbb{A}^1_{\mathbb{F}_q}$, on trouve que $\prod_{\substack{\mathfrak{p}\in \mathrm{Spec}(A)\setminus\{(0_A)\}\\ \deg(\mathfrak{p})\leq d}} \left(1+\frac{c}{N(\mathfrak{p}^2)}\right)$ peut être majoré uniformément en d. En effet, à d fixé on a :

$$\log\left(\prod_{\substack{\mathfrak{p}\in \mathrm{Spec}(A)\setminus\{(0_A)\}\\ \deg(\mathfrak{p})\leq d}} \left(1+\frac{c}{N(\mathfrak{p})^2}\right)\right) = \sum_{\substack{\mathfrak{p}\in \mathrm{Spec}(A)\setminus\{(0_A)\}\\ \deg(\mathfrak{p})\leq d}} \log\left(1+\frac{c}{N(\mathfrak{p})^2}\right) \leq c \sum_{\substack{\mathfrak{p}\in \mathrm{Spec}(A)\setminus\{(0_A)\}\\ \deg(\mathfrak{p})\leq d}} \frac{1}{N(\mathfrak{p})^2}.$$

Or, le nombre exact de polynômes premiers (c'est-à-dire irréductibles) de degré $n \in \mathbb{N}^*$ de $\mathbb{F}_q[T]$ est donné par

$$\pi_q(n) := \frac{1}{n}\sum_{\substack{d|n\\ d>0}} \mu(d) q^{\frac{n}{d}} \leq \frac{q^n}{n},$$

où μ est la fonction de Möbius. Ainsi, on a la majoration

$$\sum_{\substack{\mathfrak{p}\in \mathrm{Spec}(A)\setminus\{(0_A)\}\\ \deg(\mathfrak{p})\leq d}} \frac{1}{N(\mathfrak{p})^2} = \sum_{n=1}^{d}\left(\sum_{\substack{\mathfrak{p}\in \mathrm{Spec}(A)\setminus\{(0_A)\}\\ \deg(\mathfrak{p})= n}} \frac{1}{q^{2n}}\right) = \sum_{n=1}^{d}\frac{\pi_q(n)}{q^{2n}} \leq \sum_{n=1}^{d}\left(\frac{q^n}{n}\times\frac{1}{q^{2n}}\right) = \sum_{n=1}^{d}\frac{1}{nq^n}.$$

Enfin, la dernière série en jeu est une série convergente et elle est à termes positifs, donc on obtient finalement :

$$\prod_{\substack{\mathfrak{p}\in \mathrm{Spec}(A)\setminus\{(0_A)\}\\ \deg(\mathfrak{p})\leq d}} \left(1+\frac{c}{N(\mathfrak{p}^2)}\right) \leq \exp\left(c\sum_{n=1}^{+\infty}\frac{1}{nq^n}\right) \text{ (indépendant de } d).$$

Ainsi, il existe une constante $C > 0$ telle que :

$$\begin{aligned}\forall d \in \mathbb{N}^*,\ \overline{\delta}(S_i) &\leq \prod_{\substack{\mathfrak{p}\in \mathcal{P}_i\\ \deg(\mathfrak{p})\leq d}} \left(1+\frac{c}{N(\mathfrak{p})^2}\right) \prod_{\substack{\mathfrak{p}\in \mathcal{P}_i\\ \deg(\mathfrak{p})\leq d}} \left(1-\frac{1}{N(\mathfrak{p})}\right)\\ &\leq \prod_{\substack{\mathfrak{p}\in \mathrm{Spec}(A)\setminus\{(0_A)\}\\ \deg(\mathfrak{p})\leq d}} \left(1+\frac{c}{N(\mathfrak{p})^2}\right) \prod_{\substack{\mathfrak{p}\in \mathcal{P}_i\\ \deg(\mathfrak{p})\leq d}} \left(1-\frac{1}{N(\mathfrak{p})}\right) \leq C \prod_{\substack{\mathfrak{p}\in \mathcal{P}_i\\ \deg(\mathfrak{p})\leq d}} \left(1-\frac{1}{N(\mathfrak{p})}\right).\end{aligned}$$

Par (5.3), on trouve en passant à la limite que $\overline{\delta}(S_i) = 0$ et donc $\delta(S_i) = 0$.

Finalement, puisque $\mathcal{P}_1$ et $\mathcal{P}_2$ sont disjoints, on trouve que $A^2\setminus(S_1 \cup S_2) \subseteq \mathcal{R}$ et donc :

$$\delta(\mathcal{R}) \geq \delta\left(A^2\setminus(S_1\cup S_2)\right) = \delta\left(A^2\right) - \delta(S_1\cup S_2) \geq 1 - (\delta(S_1)+\delta(S_2)) = 1-0 = 1.$$

Ainsi, on a $\delta(\mathcal{R}) = 1$ et par additivité de la densité, $\delta\left(A^2\setminus\mathcal{R}\right) = 0$.

■

Lemme 5.4 :
Soit $\varepsilon > 0$.
Pour $m \in \mathbb{N}^*$ assez grand, on a $\overline{\delta}\left(A^2\setminus\mathcal{S}_m\right) \leq \varepsilon$.

Preuve :
Considérons $\mathcal{C} := A^2\setminus\mathcal{S}_m$ l'ensemble des couples $(a_1, a_2) \in A^2$ tels que $a_1 \equiv 0\ [\mathfrak{p}]$ et $a_2 \equiv 0\ [\mathfrak{p}]$ pour un certain idéal premier non nul $\mathfrak{p}$ de A où $\deg(\mathfrak{p}) > m$.
Fixons nous également un entier $d > m$ et posons $\mathcal{P}(d)$ l'ensemble des couples $(a_1, a_2) \in A^2$ tels que $\deg(a_1) \leq d$ et $\deg(a_2) \leq d$ ainsi que $\mathcal{C}(d) := \mathcal{C} \cap \mathcal{P}(d)$.

Soit $(a_1, a_2) \in \mathcal{P}(d)\backslash\{(0;0)\}$ tel qu'il existe un idéal premier non nul $\mathfrak{p}$ de A tel que $a_1 \equiv 0\ [\mathfrak{p}]$ et $a_2 \equiv 0\ [\mathfrak{p}]$.
En choisissant $i \in \{1;2\}$ pour lequel $a_i \neq 0$ (possible par définition du couple (a_1, a_2)) on a alors $a_i \equiv 0\ [\mathfrak{p}]$ et donc $\deg(\mathfrak{p}) \leq \deg(a_i) \leq d$.

En écrivant $\beta_{\mathfrak{p}}(d)$ le nombre de couples $(a_1, a_2) \in \mathcal{P}(d)$ tels que $a_1 \equiv 0\ [\mathfrak{p}]$ et $a_2 \equiv 0\ [\mathfrak{p}]$, on a :

$$\mathrm{Card}(\mathcal{C}(d)) \leq \sum_{\substack{\mathfrak{p}\in \mathrm{Spec}(A)\backslash\{0_A\} \\ m<\deg(\mathfrak{p})\leq d}} \beta_{\mathfrak{p}}(d). \tag{5.4}$$

Considérons $\mathfrak{p}$ un idéal premier non nul de A tel que $m < \deg(\mathfrak{p}) \leq d$.
La réduction modulo $\mathfrak{p}$ de $\mathcal{P}(d)$ dans $\mathbb{F}_{\mathfrak{p}}^2$ est un morphisme surjectif de $\mathbb{F}_q$-espaces vectoriels, donc par le théorème du rang son noyau est un $\mathbb{F}_q$-espace vectoriel de dimension $2(d+1) - 2\deg(\mathfrak{p})$. Or ici, le cardinal de ce noyau est exactement $\beta_{\mathfrak{p}}(d)$, donc $\beta_{\mathfrak{p}}(d) = q^{2(d+1-\deg(\mathfrak{p}))}$. Par la relation (5.4), on obtient que

$$\frac{\mathrm{Card}(\mathcal{C}(d))}{\mathrm{Card}(\mathcal{P}(d))} \leq \sum_{\substack{\mathfrak{p}\in \mathrm{Spec}(A)\backslash\{0_A\} \\ m<\deg(\mathfrak{p})\leq d}} q^{-2\deg(\mathfrak{p})} \leq \sum_{\substack{\mathfrak{p}\in \mathrm{Spec}(A)\backslash\{0_A\} \\ \deg(\mathfrak{p})>m}} q^{-2\deg(\mathfrak{p})}.$$

Or la dernière somme de l'égalité ci-dessus est le reste d'une série convergente, donc pour tout $\varepsilon > 0$, en prenant $m \in \mathbb{N}^*$ assez grand, on trouve que pour tout $d > m$ on a $\frac{\mathrm{Card}(\mathcal{C}(d))}{\mathrm{Card}(\mathcal{P}(d))} \leq \varepsilon$. En passant à la limite supérieure, on obtient :

$$\overline{\delta}\left(A^2\backslash\mathcal{S}_m\right) = \overline{\delta}(\mathcal{C}) \leq \varepsilon.$$

■

Lemme 5.5 :
Soit $\varepsilon > 0$.
Pour $m \in \mathbb{N}^*$ assez grand, on a $\overline{\delta}\left(A^2\backslash\mathcal{T}_m\right) \leq \varepsilon$.

Preuve :
Soit $m \in \mathbb{N}^*$.
Notons $d(m)$ le plus grand entier naturel tel que $d(m) \leq \frac{m}{2(q-1)^2(q+1)}$.

En prenant m assez grand, on peut supposer qu'il existe deux idéaux premiers non nuls distincts $\mathfrak{p}_1$ et $\mathfrak{p}_2$ de A tels que $\deg(\mathfrak{p}_1) = \deg(\mathfrak{p}_2) = d(m)$ (par le dénombrement des polynômes irréductibles sur $\mathbb{F}_q[x]$).

Posons également Ω l'ensemble des éléments $b \in A/(\mathfrak{p}_1\mathfrak{p}_2)$ tels que $b \equiv 0\ [\mathfrak{p}_1]$ ou $b \equiv 0\ [\mathfrak{p}_2]$.
L'image de $A^2\backslash\mathcal{T}_m$ modulo $\mathfrak{p}_1\mathfrak{p}_2$ appartient à Ω, donc par le lemme 4.16 on trouve :

$$\delta\left(A^2\backslash\mathcal{T}_m\right) = \frac{\mathrm{Card}(\Omega)}{\mathrm{Card}(A/(\mathfrak{p}_1\mathfrak{p}_2))} = \frac{\mathrm{Card}(\Omega)}{N(\mathfrak{p}_1)N(\mathfrak{p}_2)}.$$

Or, $\mathrm{Card}(\Omega) = 2q^{d(m)} - 1$ et $N(\mathfrak{p}_1) = N(\mathfrak{p}_2) = q^{d(m)}$, d'où :

$$\delta\left(A^2\backslash\mathcal{T}_m\right) \leq \frac{2q^{d(m)}}{N(\mathfrak{p}_1)N(\mathfrak{p}_2)} = \frac{N(\mathfrak{p}_1) + N(\mathfrak{p}_2)}{N(\mathfrak{p}_1)N(\mathfrak{p}_2)} = \frac{1}{N(\mathfrak{p}_1)} + \frac{1}{N(\mathfrak{p}_2)} = \frac{2}{q^{d(m)}}.$$

Enfin, pour $\varepsilon > 0$ fixé, comme $d(m)$ tend vers $+\infty$ quand m tend vers $+\infty$, on trouve que $\delta\left(A^2\backslash\mathcal{T}_m\right) \leq \varepsilon$ pour m assez grand.

■

Lemme 5.6 :
On a $\delta\left(A^2\backslash\mathcal{U}_m\right) = 0$.

Preuve :
Par additivité de la densité, il suffit de montrer que $\delta(\mathcal{U}_m) = 1$.
Pour λ un idéal premier non nul de A, on note

$$S_\lambda := \left\{ a := (a_1, a_2) \in A^2 \mid a_2 \neq 0 \text{ et } \overline{\rho}_{\phi(a),\lambda^2}(\mathrm{Gal}_F) = \mathrm{GL}_2(A/\lambda)^2 \right\}.$$

On a alors :

$$\mathcal{U}_m = \bigcap_{\substack{\lambda \in \mathrm{Spec}(A)\backslash\{(0_A)\} \\ \deg(\lambda) \leq m}} S_\lambda$$

où l'intersection est finie.

Or, une intersection finie d'ensembles de densité est de densité 1. En effet, pour tout $\lambda \in \mathrm{Spec}(A)\backslash\{(0_A)\}$ tel que $\deg(\lambda) \leq m$, on a $\delta\left(A^2 \backslash S_\lambda\right) = 0$ (par additivité de la densité) et donc :

$$0 \leq \delta\left(\bigcup_{\substack{\lambda \in \mathrm{Spec}(A)\backslash\{(0_A)\} \\ \deg(\lambda) \leq m}} \left(A^2 \backslash S_\lambda\right) \right) \leq \sum_{\substack{\lambda \in \mathrm{Spec}(A)\backslash\{(0_A)\} \\ \deg(\lambda) \leq m}} \delta\left(A^2 \backslash S_\lambda\right) = 0$$

et par conséquent :

$$\delta\left(A^2 \Bigg\backslash \left(\bigcap_{\substack{\lambda \in \mathrm{Spec}(A)\backslash\{(0_A)\} \\ \deg(\lambda) \leq m}} S_\lambda \right) \right) = \delta\left(\bigcup_{\substack{\lambda \in \mathrm{Spec}(A)\backslash\{(0_A)\} \\ \deg(\lambda) \leq m}} \left(A^2 \backslash S_\lambda\right) \right) = 0.$$

Finalement, on a bien :

$$\delta(\mathcal{U}_m) = \delta\left(\bigcap_{\substack{\lambda \in \mathrm{Spec}(A)\backslash\{(0_A)\} \\ \deg(\lambda) \leq m}} S_\lambda \right) = 1 - \delta\left(A^2 \Bigg\backslash \left(\bigcap_{\substack{\lambda \in \mathrm{Spec}(A)\backslash\{(0_A)\} \\ \deg(\lambda) \leq m}} S_\lambda \right) \right) = 1 - 0 = 1.$$

■

Nous pouvons désormais finir la preuve du théorème 5.1 :
Grâce à l'inclusion (5.2), on trouve en passant à la limite supérieure que :

$$\overline{\delta}\left(A^2 \backslash \mathcal{B}\right) \leq \overline{\delta}\left(A^2 \backslash \mathcal{R}\right) + \overline{\delta}\left(A^2 \backslash \mathcal{S}_m\right) + \overline{\delta}\left(A^2 \backslash \mathcal{T}_m\right) + \overline{\delta}\left(A^2 \backslash \mathcal{U}_m\right).$$

Enfin, par les lemmes 5.3, 5.4, 5.5 et 5.6 on trouve que pour $\varepsilon > 0$ fixé et $m \in \mathbb{N}^*$ assez grand on a $\overline{\delta}\left(A^2 \backslash \mathcal{B}\right) \leq 2\varepsilon$. Or ici ε est arbitrairement petit, donc on en déduit que $\overline{\delta}\left(A^2 \backslash \mathcal{B}\right) = 0$ et donc $\mathcal{B}$ possède une densité dans A^2 et celle-ci vaut 1.

I.2 Preuve du théorème

Dans toute cette sous-partie, on suppose $q \neq 2$.

Considérons $a \in \mathcal{B}$.

* Par définition de $\mathcal{B}$, on a pour tout idéal premier non nul λ de A que $\rho_{\phi(a),\lambda}(\mathrm{Gal}_F) = \mathrm{GL}_2(A_\lambda)$. Ainsi, on a $a \in S_3$ et donc $\mathcal{B} \subseteq S_3$. Or, par le théorème 5.1, on en déduit que S_3 admet une densité et elle est égale à 1.

* Comme $q \neq 2$, par le théorème 4.1 (avec $G := \mathrm{GL}_2(\widehat{A})$), on a $D\left(\mathrm{GL}_2(\widehat{A})\right) = \mathrm{SL}_2(\widehat{A})$ et par définition de $\mathcal{B}$, le groupe dérivé de $\rho_{\phi(a)}(\mathrm{Gal}_F)$ est alors égal à $\mathrm{SL}_2(\widehat{A})$ et en particulier on a $\mathrm{SL}_2(\widehat{A}) \subseteq \rho_{\phi(a)}(\mathrm{Gal}_F)$. De plus

l'indice $\left[\mathrm{GL}_2(\widehat{A}) : \rho_{\phi(a)}(\mathrm{Gal}_F)\right]$ est le même que $\left[\widehat{A}^\times : \det\left(\rho_{\phi(a)}(\mathrm{Gal}_F)\right)\right]$. En effet, considérons l'application

$$\Psi : \left| \begin{array}{ccc} \mathrm{GL}_2(\widehat{A})/\rho_{\phi(a)}(\mathrm{Gal}_F) & \longrightarrow & \widehat{A}^\times / \det\left(\rho_{\phi(a)}(\mathrm{Gal}_F)\right) \\ \overline{M} & \longmapsto & \overline{\det(M)} \end{array} \right.$$

qui est bien définie puisque si l'on a l'égalité $\overline{M} = \overline{M'}$, alors $M^{-1}M' \in \rho_{\phi(a)}(\mathrm{Gal}_F)$ et donc on a l'égalité $\det(M') = \det(M)\det(H) \in \det(M')\det(\rho_{\phi(a)}(\mathrm{Gal}_F))$ avec $H \in \rho_{\phi(a)}(\mathrm{Gal}_F)$. De plus cette application est surjective car tout $u \in \widehat{A}^\times$ est le déterminant de la matrice $uI_2 \in \mathrm{GL}_2(\widehat{A})$ et elle est également injective car si $\overline{\det(M)} = \overline{\det(M')}$, alors $\det(M^{-1}M') \in \det(\rho_{\phi(a)}(\mathrm{Gal}_F))$ et donc il existe $H \in \rho_{\phi(a)}(\mathrm{Gal}_F)$ tel que $\det(H) = \det(M^{-1}M')$, d'où $M^{-1}M'H^{-1} \in \mathrm{SL}_2(\widehat{A}) \subseteq \rho_{\phi(a)}(\mathrm{Gal}_F)$ et donc $M' \in M\rho_{\phi(a)}(\mathrm{Gal}_F)$. Ainsi, Ψ est une bijection et on a le résultat voulu.

Or, par le théorème 4.2, $\left[\widehat{A}^\times : \det\left(\rho_{\phi(a)}(\mathrm{Gal}_F)\right)\right]$ est fini et divise $q-1$.
Ainsi, on a $a \in S_2$ et donc $\mathcal{B} \subseteq S_2$. Or, par le théorème 5.1, on en déduit que S_2 admet une densité et elle est égale à 1.

∗ Soit $\mathcal{P}$ l'ensemble des couples $(a_1, a_2) \in A^2$ tels que $a_2 \neq 0$ et le coefficient dominant de $(-1)^{\deg(a_2)+1}a_2$ engendre le groupe cyclique $\mathbb{F}_q^\times$.
L'ensemble $\mathcal{P}$ a une densité positive. En effet, en notant, pour $d \in \mathbb{N}$ fixé,

$$\mathcal{P}(d) := \{(a_1, a_2) \in \mathcal{P} \mid \deg(a_1), \deg(a_2) \leq d\},$$

on trouve que :

$$\mathrm{Card}(\mathcal{P}(d)) = \mathrm{Card}(A(d)) \sum_{k=0}^{d} \left(\varphi(q-1)q^k\right) = \mathrm{Card}(A(d))\varphi(q-1) \times \frac{1-q^{d+1}}{1-q}.$$

Ainsi, on obtient que :

$$\forall d \in \mathbb{N},\ \frac{\mathrm{Card}(\mathcal{P}(d))}{\mathrm{Card}(A(d))} = \frac{\varphi(q-1)\left(1-q^{d+1}\right)}{q^{d+1}(1-q)} = \frac{\varphi(q-1)}{(1-q)q^{d+1}} - \frac{\varphi(q-1)}{1-q}.$$

En passant à la limite en d, on a :

$$\delta(\mathcal{P}) = \lim_{d \to +\infty} \left(\frac{\varphi(q-1)}{(1-q)q^{d+1}} - \frac{\varphi(q-1)}{1-q} \right) = \frac{\varphi(q-1)}{q-1}.$$

De plus, pour $a \in \mathcal{P}$, on a $\left[\widehat{A}^\times : \det\left(\rho_{\phi(a)}(\mathrm{Gal}_F)\right)\right] = 1$ par le théorème 4.2 (car ici $e = q-1$). Ainsi, on a $\mathcal{P} \cap \mathcal{B} \subseteq S_1$ puisque pour tout $a \in \mathcal{P} \cap \mathcal{B}$ on a $\mathrm{SL}_2(\widehat{A}) \subseteq \rho_{\phi(a)}(\mathrm{Gal}_F)$ et $\det(\rho_{\phi(a)}(\mathrm{Gal}_F)) = \widehat{A}^\times$. En effet, on a que $\mathrm{SL}_2(\widehat{A}) \subsetneq \rho_{\phi(a)}(\mathrm{Gal}_F) \subseteq \mathrm{GL}_2(\widehat{A})$ et par le premier théorème d'isomorphisme appliqué aux morphismes de groupes det et $f := \det|_{\rho_{\phi(a)}(\mathrm{Gal}_F)}$, on a $\mathrm{GL}_2(\widehat{A})/\mathrm{SL}_2(\widehat{A}) \cong \widehat{A}^\times$ (dont les classes seront notées $\overline{N}$ pour $N \in \mathrm{GL}_2(\widehat{A})$) ainsi que $\rho_{\phi(a)}(\mathrm{Gal}_F)/\mathrm{SL}_2(\widehat{A}) \cong \widehat{A}^\times$ (dont les classes seront notées $\overline{\overline{N}}$ pour $N \in \rho_{\phi(a)}(\mathrm{Gal}_F)$).

Soit $M \in \mathrm{GL}_2(\widehat{A})$.
On a $\det\left(\overline{M}\right) \in \widehat{A}^\times$, donc il existe $\overline{\overline{N}} \in \rho_{\phi(a)}(\mathrm{Gal}_F)/\mathrm{SL}_2(\widehat{A})$ tel que $\det\left(\overline{M}\right) = \det\left(\overline{\overline{N}}\right)$. Or, il existe également $N \in \rho_{\phi(a)}(\mathrm{Gal}_F)$ tel que $\det(M) = \det(N)$ et par conséquent, on a $\det\left(MN^{-1}\right) = 1$ et ainsi $MN^{-1} \in \mathrm{SL}_2(\widehat{A}) \subseteq \rho_{\phi(a)}(\mathrm{Gal}_F)$. Finalement, on a $M = \underbrace{\left(MN^{-1}\right)}_{\in \rho_{\phi(a)}(\mathrm{Gal}_F)} \underbrace{N}_{\in \rho_{\phi(a)}(\mathrm{Gal}_F)} \in \rho_{\phi(a)}(\mathrm{Gal}_F)$, c'est-à-dire $\mathrm{GL}_2(\widehat{A}) \subseteq \rho_{\phi(a)}(\mathrm{Gal}_F)$ et par conséquent $\rho_{\phi(a)}(\mathrm{Gal}_F) = \mathrm{GL}_2(\widehat{A})$.

Or, comme $\mathcal{B}$ est de densité 1, on a également que

$$\delta(\mathcal{P} \cap \mathcal{B}) = \delta(\mathcal{P}) = \frac{\varphi(q-1)}{q-1} > 0.$$

Finalement, S_1 possède un sous-ensemble de densité strictement positive (en l'occurrence $\mathcal{P} \cap \mathcal{B}$).

II Preuve dans le cas $q = 2$

Dans toute cette partie, on suppose que $q = 2$ et on considère $\phi : A \longrightarrow F\{\tau\}$ un module de Drinfeld de rang 2 ainsi que $v_\infty : F^\times \longrightarrow \mathbb{Z}$ la valuation définie par :

$$\forall a \in A\backslash\{0_A\}\,,\ v_\infty(a) = -\deg(a).$$

L'objectif de cette partie est de donner une condition qui nous assure que $\rho_\phi(\mathrm{Gal}_F)$ est égal à $\mathrm{GL}_2(\widehat{A})$ en supposant qu'il contienne $D\left(\mathrm{GL}_2(\widehat{A})\right)$. Pour cela, nous commencerons par démontrer le résultat suivant qui nous sera utile dans la sous-partie II.4.

Proposition 5.1 :
Si $v_\infty(j_\phi)$ est impair et $v_\infty(j_\phi) \leq -5$, alors le morphisme $\mathrm{Gal}_F \longrightarrow \mathrm{GL}_2(\widehat{A})/D\left(\mathrm{GL}_2(\widehat{A})\right)$ (obtenu en composant ρ_ϕ avec la projection) est surjectif.

Avant de donner la preuve de la proposition 5.1, nous allons commencer par donner un premier lemme ainsi qu'un résultat sur les polynômes du troisième degré. En particulier, on suppose dans les sous-parties II.1, II.2 et II.3 que $v_\infty(j_\phi)$ est impair et inférieur ou égal à -5.

II.1 Quotient abélien maximal

Pour tout $i \in \mathbb{F}_2$, on définit l'idéal premier $\lambda_i := (T + i)$ de A ainsi que le morphisme

$$\gamma_i : \mathrm{GL}_2(\widehat{A}) \longrightarrow \mathrm{GL}_2(\mathbb{F}_{\lambda_i}) \cong \mathrm{GL}_2(\mathbb{F}_2) \longrightarrow \mathrm{GL}_2(\mathbb{F}_2)/D(\mathrm{GL}_2(\mathbb{F}_2)) \cong \{-1;1\}$$

obtenu en composant la projection puis la réduction modulo λ_i avec l'application quotient.

On obtient ainsi un morphisme continu et surjectif (car la réduction modulo λ_i et l'application quotient le sont) :

$$\beta : \left| \begin{array}{ccc} \mathrm{GL}_2(\widehat{A}) & \longrightarrow & \widehat{A}^\times \times \{-1;1\} \times \{-1;1\} \\ B & \longmapsto & (\det(B); \gamma_0(B); \gamma_1(B)) \end{array} \right. .$$

Le lemme suivant nous donne le noyau de ce morphisme β :

Lemme 5.7 :
Le noyau de β est $D\left(\mathrm{GL}_2(\widehat{A})\right)$.

Preuve :
On sait que

$$\mathrm{GL}_2(\widehat{A}) \cong \prod_{\lambda \in \mathrm{Spec}(A)\backslash\{(0_A)\}} \mathrm{GL}_2(A_\lambda),$$

donc :

$$D\left(\mathrm{GL}_2(\widehat{A})\right) \cong \prod_{\lambda \in \mathrm{Spec}(A)\backslash\{(0_A)\}} D\left(\mathrm{GL}_2(A_\lambda)\right).$$

Or la proposition 4.3 nous une description des $D(A_\lambda)$ donnée par :

$$\forall \lambda \in \{\lambda_0; \lambda_1\},\ D\left(\mathrm{GL}_2(A_\lambda)\right) = \{B \in \mathrm{SL}_2(A_\lambda) \mid \overline{B} \text{ appartient à } D(\mathrm{GL}_2(\mathbb{F}_2))\}$$

ainsi que :

$$\forall \lambda \in \mathrm{Spec}(A)\backslash\{\lambda_0; \lambda_1; (0_A)\},\ D(\mathrm{GL}_2(A_\lambda)) = \mathrm{SL}_2(A_\lambda).$$

Or, pour $B \in \mathrm{GL}_2(\widehat{A})$ on a $B \in \mathrm{Ker}(\beta)$ si, et seulement si, $B \in \mathrm{SL}_2(\widehat{A})$ et $\gamma_0(B) = \gamma_1(B) = 1$. Ainsi, on a $\mathrm{Ker}(\beta) = D\left(\mathrm{GL}_2(\widehat{A})\right)$.

■

II.2 Polynômes du troisième degré

Dans toute cette sous-partie, on considère le polynôme séparable $P(x) = x^3 + bx + c \in \mathbb{K}[x]$ avec $\mathbb{K}$ un corps.

Considérons r_1, r_2 et r_3 les racines distinctes (car P séparable) de $P(x)$ dans une clôture séparable de $\mathbb{K}$ et posons $\mathbb{K}' := \mathbb{K}(r_1, r_2, r_3)$ le corps de décomposition de P. En utilisant la numérotation des racines, on obtient un morphisme injectif $\iota : \mathrm{Gal}(\mathbb{K}'/\mathbb{K}) \hookrightarrow \mathfrak{S}_3$ ainsi qu'un morphisme $\varepsilon : \mathrm{Gal}(\mathbb{K}'/\mathbb{K}) \longrightarrow \{-1;1\}$ en composant ι avec la signature.

Posons $\mathbb{L}/\mathbb{K}$ un sous-corps de $\mathbb{K}'$ fixé par le noyau de ε (ce qui a bien un sens via la correspondance de Galois finie). Notre objectif ici est de donner une description explicite de l'extension $\mathbb{L}/\mathbb{K}$ (dans le cas où la caractéristique de $\mathbb{K}$ est impaire, $\mathbb{L}$ est obtenu en adjoignant à $\mathbb{K}$ une racine carré du discriminant de $P(x)$ mais puisqu'ici on a $q = 2$ cette méthode n'est pas satisfaisante...) en utilisant une technique tirée de la partie 2 de [Con].

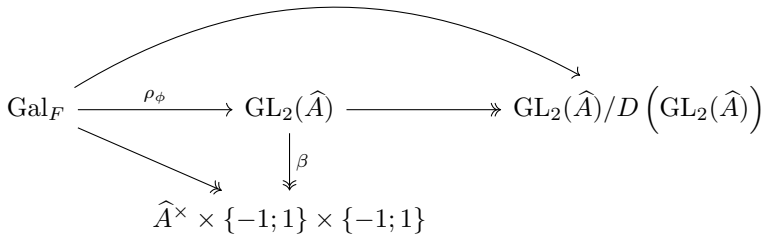
Définissons le polynôme $R_2(x) := \left(x - \left(r_1^2 r_2 + r_2^2 r_3 + r_3^2 r_1\right)\right)\left(x - \left(r_2^2 r_1 + r_1^2 r_3 + r_3^2 r_2\right)\right)$.
En développant le polynôme $R_2(x)$, on trouve que ses coefficients sont des polynômes symétriques en r_1, r_2 et r_3 donc sont des polynômes en b et c (par les relations coefficients-racines). De plus, un calcul direct montre que :

$$R_2(x) = x^2 - 3cx + \left(b^3 + 9c^2\right).$$

De plus, les discriminants de $R_2(x)$ et $P(x)$ sont identiques (et égaux à $-4b^3 - 27c^2$) et ainsi $R_2(x)$ est séparable puisque $P(x)$ l'est. Enfin, on remarque que $r_1^2 r_2 + r_2^2 r_3 + r_3^2 r_1$ et $r_2^2 r_1 + r_1^2 r_3 + r_3^2 r_2$ sont tous les deux fixés par une permutation paire des r_i mais échangés par une permutations impaire des r_i. Ainsi, par définition de ε, on trouve que $\mathbb{L}$ est le corps de décomposition de $R_2(x)$ dans $\mathbb{K}'$.

II.3 Preuve de la proposition 5.1

Par le lemme 5.7, il suffit de montrer que $\beta \circ \rho_\phi : \mathrm{Gal}_F \longrightarrow \widehat{A}^\times \times \{-1;1\} \times \{-1;1\}$ est surjective. En effet, si c'est le cas, on a le diagramme suivant :



En considérant $\overline{M}$ la classe de $M \in \mathrm{GL}_2(\widehat{A})$ dans $\mathrm{GL}_2(\widehat{A})/D\left(\mathrm{GL}_2(\widehat{A})\right)$ ainsi que $g \in \mathrm{Gal}_F$ tel que $\beta(\rho_\phi(g)) = \beta(M)$, on obtient que $\rho_\phi(g)M^{-1} \in \mathrm{Ker}(\beta) = D\left(\mathrm{GL}_2(\widehat{A})\right)$, d'où $\overline{\rho_\phi(g)M^{-1}} = 1$ et ainsi $\overline{\rho_\phi(g)} = \overline{M}$.

Dans toute cette sous partie, pour $i \in \{1;2\}$, on reprend γ_i et λ_i comme dans la sous-partie II.1 et on pose $\mathbb{L}_i$ le sous-corps de F^{sep} fixé par le noyau du morphisme $\gamma_i \circ \rho_\phi : \mathrm{Gal}_F \longrightarrow \{-1;1\}$.

Lemme 5.8 :
Soit $i \in \{1;2\}$.
On a $\mathbb{L}_i = F(\alpha)$ avec α une racine du polynôme $x^2 - x + \frac{j_\phi}{(T+i)^2} + 1 \in F[x]$.

Preuve :
Soit $i \in \{1;2\}$.
On a $\phi_T = T + a_1\tau + a_2\tau^2$ pour $a_1 \in F$ et $a_2 \in F^\times$ et donc $\phi_{T+i} = (T+i) + a_1\tau + a_2\tau^2$. En particulier, on a $\phi[\lambda_i] \cong \mathbb{F}_2^2$ d'où $\phi[\lambda_i] \cong \{0; r_1; r_2; r_3\}$ avec les r_i des éléments non nuls de F^{sep}.

Les valeurs r_1, r_2 et r_3 sont des racines distinctes dans F^{sep} du polynôme

$$P(x) := x^3 + \left(\frac{a_1}{a_2}\right) x + \frac{T+i}{a_2} = a_2^{-1} x^{-1} \left((T+i)x + a_1 x^2 + a_2 x^4\right) \in F[x].$$

En reprenant le caractère $\varepsilon : \mathrm{Gal}_F \longrightarrow \{-1;1\}$ correspondant à $P(x)$ comme dans la sous-partie II.2 et en remarquant qu'en choisissant une base de $\phi[\lambda_i] \cong \mathbb{F}_2^2$, l'action du groupe $\mathrm{GL}_2(\mathbb{F}_2)$ sur $\{r_1; r_2; r_3\}$ est fidèle et transitive et donc induit un isomorphisme $\mathrm{GL}_2(\mathbb{F}_2) \cong \mathfrak{S}_3$. En utilisant ce résultat, on trouve que ε coïncide avec $\gamma_i \circ \rho_\phi$. Ainsi, $\mathbb{L}_i$ est le sous-corps de F^{sep} fixé par le noyau de ε.

Par la sous-partie II.2, on trouve que $\mathbb{L}_i \subseteq F^{sep}$ est le corps de décomposition sur F du polynôme

$$R_2(x) := x^2 - 3\left(\frac{T+i}{a_2}\right) x + \left(\frac{a_1}{a_2}\right)^3 + 9\left(\frac{T+i}{a_2}\right)^2 \in F[x].$$

En posant $y := \frac{a_2}{T+i} x$ et en utilisant le fait que les corps en jeu sont de caractéristique 2, on trouve que $\mathbb{L}_i$ est le corps de décomposition sur F du polynôme $y^2 - y + \frac{a_1^3}{a_2(T+i)^2} + 1 = y^2 - y + \frac{j_\phi}{(T+i)^2} + 1$.

■

Lemme 5.9 :
Le morphisme

$$\beta' : \left| \begin{array}{ccc} \mathrm{Gal}_F & \longrightarrow & \{-1;1\} \times \{-1;1\} \\ \sigma & \longmapsto & (\gamma_0(\rho_\phi(\sigma)); \gamma_1(\rho_\phi(\sigma))) \end{array} \right.$$

est surjectif et totalement ramifié en la place ∞ de F.

Preuve :
Posons $\mathbb{L}$ le sous-corps de F^{sep} fixé par le noyau de β (possible par la correspondance de Galois infinie).
On a alors $\mathbb{L} = \mathbb{L}_0\mathbb{L}_1$ et pour tout $i \in \mathbb{F}_2$, le lemme 5.8 implique que $\mathbb{L}_i = F(\alpha_i)$ avec α_i une racine de $P_i(x) := x^2 - x + \frac{j_\phi}{(T+i)^2} + 1$.

Montrons que les extensions $\mathbb{L}_i/F$ sont des extensions quadratiques totalement ramifiées en la place ∞ de F : Puisque les corps en jeu ont pour caractéristique 2, on a que les racines de P_i sont α_i et $\alpha_i + 1$ (par les relations coefficients-racines). En particulier, toujours par les relations coefficients-racines, $\alpha_i(\alpha_i + 1) = \frac{j_\phi}{(T+i)^2} + 1$ et puisque $v_\infty\left(\frac{j_\phi}{(T+i)^2}\right) = v_\infty(j_\phi) + 2 \leq -5 + 2 = -3 < 0$, on a :

$$v_\infty\left(\alpha_i(\alpha_i+1)\right) = v_\infty\left(\frac{j_\phi}{(T+i)^2} + 1\right) = v_\infty\left(\frac{j_\phi}{(T+i)^2}\right) = v_\infty(j_\phi) + 2 < 0.$$

Ainsi, puisque par hypothèse $v_\infty(j_\phi)$ est un entier impair, on en déduit que $v_\infty\left(\alpha_i(\alpha_i+1)\right)$ est un entier strictement négatif impair. Par conséquent, après avoir étendu v_∞ en une valuation définie sur F^{sep} et à valeurs dans $\mathbb{Q}$, on en déduit que l'un des nombres rationnels $v_\infty(\alpha_i)$ ou $v_\infty(\alpha_i + 1)$ est strictement négatif et donc $v_\infty(\alpha_i) = v_\infty(\alpha_i + 1) < 0$.

Ainsi, on a $2v_\infty(\alpha_i) = v_\infty\left(\alpha_i(\alpha_i+1)\right) \in \mathbb{Z}$ qui est un entier impair négatif, d'où $v_\infty(\alpha_i) \notin \mathbb{Z}$. Par conséquent, $\mathbb{L}_i = F(\alpha_i)$ est une extension non triviale de F et qui est ramifiée en la place ∞ (en effet, dans une extension non ramifiée, les valuations restent entières et donc la valuation de $F(\alpha_i)$ serait une extension de v_∞ avec un indice de ramification $e = 1$ donc les valuations dans l'extension prennent les mêmes valeurs que dans F et par conséquent restent dans $\mathbb{Z}$). On a alors le résultat voulu puisque $[\mathbb{L}_i : F] \leq \deg(P_i) = 2$ (en effet, cela force le degré de l'extension et l'indice de ramification à être égaux et valoir 2).

Posons désormais $\alpha := \alpha_0 + \alpha_1$.
On a α racine du polynôme

$$x^2 - x + \left[\left(\frac{j_\phi}{T^2} + 1\right) + \left(\frac{j_\phi}{(T+1)^2} + 1\right)\right] = x^2 - x + \frac{j_\phi}{(T(T+1))^2}. \tag{5.5}$$

Montrons que $F(\alpha)$ est une extension quadratique de F qui est totalement ramifiée en la place ∞ :
De même que précédemment, les racines de (5.5) sont α et $\alpha+1$, d'où :

$$v_\infty(\alpha(\alpha+1)) = v_\infty\left(\frac{j_\phi}{(T(T+1))^2}\right) = v_\infty(j_\phi)+4 \leq -5+4 = -1 < 0$$

et $v_\infty(\alpha(\alpha+1))$ est un entier strictement négatif impair. Par conséquent, $v_\infty(\alpha) = v_\infty(\alpha+1)$ et $2v_\infty(\alpha)$ est un entier impair. Finalement, $v_\infty(\alpha) \notin \mathbb{Z}$ et donc $F(\alpha)/F$ est une extension non triviale et ramifiée en la place ∞ (par le même arugment que précédemment) et on a le résultat voulu car $[F(\alpha):F] \leq 2$ (même argument que précédemment).

Montrons désormais que β' est surjectif :
Il nous suffit de montrer que $[\mathbb{L}:F] = 4$ et puisque $\mathbb{L} = \mathbb{L}_0\mathbb{L}_1$ avec $[\mathbb{L}_1:F] = [\mathbb{L}_2:F] = 2$, il nous suffit de montrer que $\mathbb{L}_0 \neq \mathbb{L}_1$. Pour cela, raisonnons par l'absurde en supposant que $\mathbb{L}_0 = \mathbb{L}_1$.
Pour tout $\sigma \in \mathrm{Gal}_F$, on a alors pour tout $i \in \mathbb{F}_2$ que $\sigma(\alpha_i)$ a la même valeur et vaut α_i ou α_i+1. Ainsi, $\alpha := \alpha_0+\alpha_1$ est fixé par Gal_F et donc appartient à F mais puisque l'on a montré que $F(\alpha)/F$ est une extension de corps non triviale, on aboutit à une contradiction.
Finalement, on a bien $\mathbb{L}_0 \neq \mathbb{L}_1$ et donc β' est surjectif.

Supposons enfin que $\mathbb{L}/F$ n'est pas totalement ramifiée en la place ∞. Puisque β' induit l'isomorphisme $\mathrm{Gal}(\mathbb{L}/F) \cong \{-1;1\}\times\{-1;1\}$, l'une des trois extensions quadratiques intermédiaires de F dans $\mathbb{L}$ (par la correspondance de Galois finie) doit être non ramifiée en la place ∞ (par multiplicativité de l'indice de ramification dans les extensions). Or, les trois extensions quadratiques intermédiaires de F dans $\mathbb{L}$ sont à l'isomorphisme près $\mathbb{L}_0$, $\mathbb{L}_1$ et $F(\alpha)$ et nous avons déjà montré qu'elles sont toutes ramifiées en la place ∞, d'où une contradiction.
Finalement, $\mathbb{L}/F$ est donc une extension totalement ramifiée en la place ∞.

■

Lemme 5.10 :
Le morphisme $\det\circ\rho_\phi : \mathrm{Gal}_F \longrightarrow \widehat{A}^\times$ est surjectif et modérément ramifié en la place ∞ de F.

Preuve :
Écrivons $\phi_T := T + a_1\tau + a_2\tau^2$ avec $a_1 \in F$ et $a_2 \in F^\times$.
En posant $\psi : A \longrightarrow F\{\tau\}$ le module de Drinfeld de rang 1 défini par $\psi_T := T - a_2\tau = T + a_2\tau$, on obtient par le corollaire 4.6 à la page 322 de [Ham93], on a $\det\circ\rho_\phi = \rho_\psi$.

Ainsi, pour démontrer le lemme, il suffit de montrer que $\rho_\psi : \mathrm{Gal}_F \longrightarrow \widehat{A}^\times$ est surjectif et modérément ramifié en la place ∞ de F. De plus, on remarque que $a_2 \cdot \psi_T \cdot a_2^{-1} = T + \tau$ est le module de Carlitz, donc quitte à remplacer ψ par un module de Drinfeld qui lui est isomorphe, on peut supposer que ψ est le module de Carlitz.

Enfin, par les théorèmes 2.3 et 3.1 aux pages respectives 82 et 83 de [Hay74], on a $\overline{\rho}_\psi$ qui est surjective et modérément ramifié en la place ∞ de F. Finalement, on a bien que le caractère $\det\circ\overline{\rho}_\phi : \mathrm{Gal}_F \longrightarrow \widehat{A}^\times$ est surjectif et modérément ramifié en la place ∞ de F. (puisque $\det\circ\overline{\rho}_\phi = \overline{\rho}_\psi$).

■

Nous allons maintenant donner la preuve de la proposition 5.1 en montrant (comme indiqué au début de cette sous-partie) que le morphisme $\beta\circ\rho_\phi : \mathrm{Gal}_F \longrightarrow \widehat{A}^\times \times \{-1;1\}\times\{-1;1\}$ est surjectif :

La composition $\beta\circ\rho_\phi$ avec la projection sur $\widehat{A}^\times$ nous donne le morphisme $\det\circ\rho_\phi$ qui est surjectif et modérément ramifié en la place ∞ par le lemme 5.10. De même, la composition $\beta\circ\rho_\phi$ avec la projection sur $\{-1;1\}\times\{-1;1\}$ nous donne le morphisme β' qui est surjectif par le lemme 5.9.

Raisonnons par l'absurde en supposant que $\beta\circ\rho_\phi$ n'est pas surjective. Par le lemme 5.2.1 à la page 793 de [Rib76], il existe un morphisme continu et surjectif $\varphi : \mathrm{Gal}_F \longrightarrow Q$ avec Q un groupe fini non trivial et qui se factorise à la fois via $\det\circ\rho_\phi$ et β' (car les projections $\det\circ\rho_\phi$ et β' sont surjectives). Par conséquent, le morphisme

φ est modérément ramifié en la place ∞ puisqu'il se factorise via $\det \circ \rho_\phi$ mais il est également sauvagement ramifié en la place ∞ puisqu'il se factorise via β' (par le lemme 5.9). Ainsi, comme φ n'est pas l'identité, on aboutit à une contradiction et donc $\beta \circ \rho_\phi$ et surjectif et on a le résultat de la proposition 5.1.

II.4 Preuve du théorème

Dans toute cette sous-partie, on suppose toujours que $q = 2$ et on considère $\mathcal{C}$ le sous-ensemble de A^2 constitué des couples (a_1, a_2) tels que $a_1 a_2 \neq 0$ et $\deg(a_1) = \deg(a_2) - 1$.

* En reprenant l'ensemble $\mathcal{B}$ de la partie I, on obtient que $\mathcal{B} \subseteq S_3$ et puisque $\mathcal{B}$ a pour densité 1 (par le théorème 5.1), on en déduit que S_3 a pour densité 1.

* Considérons maintenant $a \in \mathcal{B}$.
Par le théorème 4.2 on a $\det\left(\rho_{\phi(a)}(\mathrm{Gal}_F)\right) = \widehat{A}^\times$ (car $q = 2$). De plus, puisque l'on a également que $D\left(\mathrm{GL}_2(\widehat{A})\right) \subseteq \rho_{\phi(a)}(\mathrm{Gal}_F)$ (car $a \in \mathcal{B}$), on en déduit par le lemme 5.7 que $\left[\mathrm{GL}_2(\widehat{A}) : \rho_{\phi(a)}(\mathrm{Gal}_F)\right]$ divise 4. En effet, on a $\mathrm{GL}_2(\widehat{A})/D\left(\mathrm{GL}_2(\widehat{A})\right) \cong \widehat{A}^\times \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ (par le premier théorème d'isomorphisme) et de plus l'image de $\rho_{\phi(a)}(\mathrm{Gal}_F)$ par β est de la forme $\widehat{A}^\times \times H$ avec H un sous-groupe de $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. En appliquant alors le premier théorème d'isomorphisme et puisque $D\left(\mathrm{GL}_2(\widehat{A})\right) \subseteq \rho_{\phi(a)}(\mathrm{Gal}_F)$ on a :

$$\rho_{\phi(a)}(\mathrm{Gal}_F)/D\left(\mathrm{GL}_2(\widehat{A})\right) \cong \beta(\rho_{\phi(a)}(\mathrm{Gal}_F)) = \widehat{A}^\times \times H$$

et par le troisième théorème d'isomorphisme on a

$$\begin{aligned}
\mathrm{GL}_2(\widehat{A})/\rho_{\phi(a)}(\mathrm{Gal}_F) &\cong \left(\mathrm{GL}_2(\widehat{A})/D\left(\mathrm{GL}_2(\widehat{A})\right)\right) / \left(\rho_{\phi(a)}(\mathrm{Gal}_F)/D\left(\mathrm{GL}_2(\widehat{A})\right)\right) \\
&\cong \beta\left(\mathrm{GL}_2(\widehat{A})\right)/\beta\left(\rho_{\phi(a)}(\mathrm{Gal}_F)\right) \cong \left(\widehat{A}^\times \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}\right) / \left(\widehat{A}^\times \times H\right) \\
&\cong \left(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}\right)/H,
\end{aligned}$$

où le dernier isomorphisme est justifié grâce au premier théorème d'isomorphisme avec l'application de projection coordonnée par coordonnée. Par conséquent, on en déduit que l'indice $\left[\mathrm{GL}_2(\widehat{A}) : \rho_{\phi(a)}(\mathrm{Gal}_F)\right]$ divise 4 (puisque $\mathrm{Card}(H) \in \{1; 2; 4\}$).

Ainsi, on a $a \in S_2$, d'où $\mathcal{B} \subseteq S_2$ et puisque $\mathcal{B}$ a pour densité 1 (par le théorème 5.1), on en déduit que S_2 a pour densité 1.

* Enfin, considérons $a \in \mathcal{C} \cap S_2$.
Pour tout $d \in \mathbb{N}^*$, on a :

$$\mathrm{Card}(\mathcal{C}(d)) = \sum_{i=1}^{d} (q-1)q^{i-1}(q-1)q^i = (q-1)^2 q \frac{1-q^{2d}}{1-q^2}$$

D'où :

$$\delta(\mathcal{C}) = \lim_{d \to +\infty} \frac{(q-1)^2 q \frac{1-q^{2d}}{1-q^2}}{q^{2(d+1)}} = \frac{(q-1)^2 q}{q^2(q^2-1)} = \frac{2}{4 \times 3} = \frac{1}{6}.$$

De plus, on a $j_{\phi(a)} = \frac{a_1^{q+1}}{a_2} = \frac{a_1^3}{a_2}$ et donc comme $a \in \mathcal{C}$ on a :

$$v_\infty(j_{\phi(a)}) = 3v_\infty(a_1) - v_\infty(a_2) = \deg(a_2) - 3\deg(a_1) = -2\deg(a_2) + 3.$$

Ainsi, $v_\infty(j_{\phi(a)})$ est un entier impair et on a $v_\infty(j_{\phi(a)}) \leq -5$ lorsque $\deg(a_2) \geq 4$. Donc pour tout $a \in \mathcal{C} \cap S_2$ tel que $\deg(a_2) \geq 4$, la proposition 5.1 et le fait que $D\left(\mathrm{GL}_2(\widehat{A})\right) \subseteq \rho_{\phi(a)}(\mathrm{Gal}_F)$ impliquent que l'on a

$\rho_{\phi(a)}(\mathrm{Gal}_F) = \mathrm{GL}_2(\widehat{A})$. En effet, on a en toute généralité que $\rho_{\phi(a)}(\mathrm{Gal}_F) \subseteq \mathrm{GL}_2(\widehat{A})$ donc il nous suffit de montrer l'inclusion réciproque.

Soit $g \in \mathrm{GL}_2(\widehat{A})$.
En notant π la projection canonique de $\mathrm{GL}_2(\widehat{A})$ dans $\mathrm{GL}_2(\widehat{A})/D\left(\mathrm{GL}_2(\widehat{A})\right)$, on a

$$\pi\left(\rho_{\phi(a)}(\mathrm{Gal}_F)\right) = \mathrm{GL}_2(\widehat{A})/D\left(\mathrm{GL}_2(\widehat{A})\right),$$

donc il existe un élément $h \in \rho_{\phi(a)}(\mathrm{Gal}_F)$ tel que $\pi(h) = \pi(g)$. Par conséquent, on a $h^{-1}g \in D\left(\mathrm{GL}_2(\widehat{A})\right)$ et donc :

$$g = h\left(h^{-1}g\right) \in \rho_{\phi(a)}(\mathrm{Gal}_F)D\left(\mathrm{GL}_2(\widehat{A})\right).$$

Or, on a $D\left(\mathrm{GL}_2(\widehat{A})\right) \subseteq \rho_{\phi(a)}(\mathrm{Gal}_F)$ et donc par la structure de groupe on a $g \in \rho_{\phi(a)}(\mathrm{Gal}_F)$, c'est-à-dire $\mathrm{GL}_2(\widehat{A}) \subseteq \rho_{\phi(a)}(\mathrm{Gal}_F)$. Finalement, on obtient par double inclusion que $\rho_{\phi(a)}(\mathrm{Gal}_F) = \mathrm{GL}_2(\widehat{A})$ et donc la représentation ρ_ϕ est surjective.

De plus, on a $\delta(\mathcal{C} \cap S_2) = \delta(\mathcal{C}) = \frac{1}{6}$ (car S_2 a pour densité 1) et $\mathcal{C} \cap S_2$ contient un nombre fini de a tels que $\deg(a_2) < 4$. Par conséquent, puisque $\mathcal{C} \cap S_2 \subseteq S_1$, on en déduit que S_1 a un sous-ensemble de densité strictement positive (en l'occurrence $\mathcal{C} \cap S_2$).

Chapitre 6

Étude d'un cas particulier

Le but de ce dernier chapitre est de démontrer le théorème 0.4. Comme dans le chapitre précédent, nous allons séparer le chapitre en deux parties : dans la partie I nous allons donner la preuve du théorème dans le cas où $q \neq 2$ puis dans la partie II nous allons traiter le cas où $q = 2$. En particulier, on utilisera les résultats préliminaires démontrés dans le chapitre 4 ainsi que la proposition 5.1 dans la partie II.

I Le cas $q \neq 2$

Dans toute cette sous-partie, on suppose que $q > 2$, on considère $\phi : A \longrightarrow F\{\tau\}$ le module de Drinfeld défini par $\phi_T := T + \tau - T^{q-1}\tau^2$, on pose l'idéal premier non nul $\mathfrak{p} := (T)$ de A et on note $I_{\mathfrak{p}}$ le groupe d'inertie de Gal_F en $\mathfrak{p}$.

Commençons par remarquer que $\mathfrak{p}$ est le seul idéal premier non nul de A pour lequel ϕ ait une mauvaise réduction, on a $j_\phi = \frac{-1}{T^{q-1}}$ et donc $v_{\mathfrak{p}}(j_\phi) = -(q-1)$ et en particulier $\mathrm{PGCD}(v_{\mathfrak{p}}(j_\phi); q) = 1$.

Lemme 6.1 :
Pour tout idéal non nul $\mathfrak{a}$ de A, le caractère $\det \circ \overline{\rho}_{\phi,\mathfrak{a}} : \mathrm{Gal}_F \longrightarrow (A/\mathfrak{a})^\times$ est surjectif et non ramifié en tout idéal premier non nul $\mathfrak{p}$ de A ne divisant pas $\mathfrak{a}$.

Preuve :
Soit $\mathfrak{a}$ un idéal non nul de A.
Par la proposition 4.8 (puisque $d - 1 = q - 2$ et par transitivité du PGCD), on a $\det \circ \overline{\rho}_{\phi,\mathfrak{a}}$ qui est surjectif.

Considérons $\psi : A \longrightarrow F\{\tau\}$ le module de Drinfeld de rang 1 défini par $\psi_T := T - (-T^{q-1})\tau = T + T^{q-1}\tau$.
Par le corollaire 4.6 à la page 322 de [Ham93], on a $\det \circ \rho_\phi = \rho_\psi$ et donc en particulier $\det \circ \overline{\rho}_{\phi,\mathfrak{a}} = \overline{\rho}_{\psi,\mathfrak{a}}$.

De plus, on a $T \cdot \psi_T \cdot T^{-1} = T + \tau$ et donc ψ est isomorphe au module de Carlitz. Donc quitte à remplacer ψ par un module de Drinfeld qui lui est isomorphe, on peut supposer que ψ est le module de Carlitz.

Soit $\mathfrak{a}$ un idéal non nul de A.
La proposition 2.2 et le théorème 2.3 respectivement à la page 81 et 82 de [Hay74], on a $\overline{\rho}_{\psi,\mathfrak{a}}$ qui est surjective et non ramifiée en tout idéal premier non nul $\mathfrak{p}$ de A ne divisant pas $\mathfrak{a}$. Finalement, on a bien que le caractère $\det \circ \overline{\rho}_{\phi,\mathfrak{a}} : \mathrm{Gal}_F \longrightarrow (A/\mathfrak{a})^\times$ est surjectif et non ramifié en tout idéal premier non nul $\mathfrak{p}$ de A ne divisant pas $\mathfrak{a}$ (puisque $\det \circ \overline{\rho}_{\phi,\mathfrak{a}} = \overline{\rho}_{\psi,\mathfrak{a}}$).

■

Lemme 6.2 :
Pour tout idéal premier non nul λ de A, $\overline{\rho}_{\phi,\lambda}$ est irréductible.

Preuve :
Raisonnons par l'absurde en supposant que $\overline{\rho}_{\phi,\lambda}$ est réductible pour un certain idéal premier non nul λ de A :

* Supposons tout d'abord que $\lambda = \mathfrak{p} = (T)$:
  Pour tout $c \in \mathbb{F}_q^\times$, ϕ a une bonne réduction en l'idéal premier $(T-c)$ et par le lemme 4.11 on a $P_{\phi,(T-c)}(x) = x^2 - x + (T-c)$. Ainsi, $\overline{\rho}_{\phi,\mathfrak{p}}(\mathrm{Gal}_F) \subseteq \mathrm{GL}_2(\mathbb{F}_\mathfrak{p})$ contient un élément dont le polynôme caractéristique est $x^2 - x - c \in \mathbb{F}_\mathfrak{p}[x] = \mathbb{F}_q[x]$ (l'élément en question étant l'image de Frob_{T-c} par $\overline{\rho}_{\phi,\mathfrak{p}}$ et en utilisant la proposition 4.7).
  Or, puisque $\overline{\rho}_{\phi,\lambda}$ est réductible, on obtient que le polynôme $x^2 - x - c$ est réductible dans $\mathbb{F}_q[x]$ pour tout $c \in \mathbb{F}_q$. Mais lorsque q est pair cela n'est pas possible car $\mathbb{F}_q$ possède une extension quadratique qui est donnée par un polynôme irréductible de degré 2 dans $\mathbb{F}_q$ et pour q impair, on aurait $(-1)^2 - 4 \times (-c) = 1 + 4c$ qui serait un carré dans $\mathbb{F}_q$ pour tout $c \in \mathbb{F}_q$, ce qui n'est pas possible puisque $c \longmapsto 1 + 4c$ est un isomorphisme dans $\mathbb{F}_q$ (car 4 est premier avec q puisque $q \neq 2$) et tous les éléments de $\mathbb{F}_q$ ne sont pas des carrés. Ainsi, on a $\lambda \neq (T)$.

* Quitte à conjuguer $\overline{\rho}_{\phi,\lambda}$, on peut supposer que $\overline{\rho}_{\phi,\lambda}$ est de la forme (4.9) avec $\chi_1, \chi_2 : \mathrm{Gal}_F \longrightarrow \mathbb{F}_\lambda^\times$ deux caractères.
  Puisque ϕ a une bonne réduction en dehors de $\mathfrak{p}$, les caractères χ_1 et χ_2 sont tous les deux non ramifiés en tout idéal premier non nul de A excepté peut-être en $\mathfrak{p}$ et λ (comme mentionné au début de la sous-partie III.1). En appliquant le premier point de la proposition 4.6 (avec $\mathfrak{a} := \lambda$ et en utilisant le fait que $\lambda \neq \mathfrak{p}$), on trouve que l'un des caractères χ_1 ou χ_2 est non ramifié en $\mathfrak{p}$. Or, par le lemme 6.1, $\det \circ \overline{\rho}_{\phi,\lambda} = \chi_1\chi_2$ est non ramifié en $\mathfrak{p}$ et donc χ_1 et χ_2 sont tous les deux non ramifiés en $\mathfrak{p}$. De plus, comme $\overline{\rho}_{\phi,\lambda}$ est réductible et que ϕ a une bonne réduction en λ, la proposition 4.5 implique que χ_1 ou χ_2 est non ramifié en λ.
  Nous avons vérifié que χ_1 et χ_2 satisfont deux points du lemme 4.14 avec $n := 1$, donc par le lemme 4.15, il existe $\zeta \in \mathbb{F}_\lambda^\times$ tel que $P_{\phi,\mathfrak{q}}(\zeta^{\deg(\mathfrak{q})}) = 0$ dans $\mathbb{F}_\lambda$ pour tout idéal premier non nul $\mathfrak{q}$ de A différent de $\mathfrak{p}$ et λ.

Nous pouvons désormais achever la preuve :

* Supposons que $q > 3$ ou $\deg(\lambda) > 1$.
  Il existe deux éléments distincts $c_1, c_2 \in \mathbb{F}_q^\times$ tels que $\lambda \notin \{(T-c_1); (T-c_2)\}$. En utilisant le lemme 4.11, on a :
  $$c_1 - c_2 = P_{\phi,(T-c_1)}(\zeta) - P_{\phi,(T-c_2)}(\zeta) \equiv 0 + 0 \equiv 0 \ [\lambda],$$
  ce qui contredit le fait que c_1 et c_2 sont des éléments distincts de $\mathbb{F}_q$.

* Supposons enfin que $q = 3$ et $\deg(\lambda) = 1$.
  On a $\lambda = (T-b)$ pour un certain $b \in \mathbb{F}_3^\times$ et $\mathbb{F}_\lambda \cong \mathbb{F}_3$. En définissant l'idéal premier non nul $\mathfrak{q} := (T^2+T+2)$ de A, on a $\zeta^{\deg(\mathfrak{q})} = 1$ (car $\mathrm{Card}(\mathbb{F}_\lambda^\times) = 2 = \deg(\mathfrak{q})$) et par conséquent, $P_{\phi,\mathfrak{q}}(1) \equiv 0 \ [\lambda]$. Par le lemme 4.13, on a $P_{\phi,\mathfrak{q}}(x) = x^2 + 2x + \left(T^2 + T + 2\right)$ et ainsi :
  $$0 \equiv P_{\phi,\mathfrak{q}}(1) \equiv 1^2 + 2 \times 1 + b^2 + b + 2 \equiv b^2 + b + 2 \ [\lambda].$$
  On aboutit alors à $b^2 + b + 2 = 0$ car $b \in \mathbb{F}_3$, ce qui est contradictoire avec le fait que $x^2 + x + 2$ est irréductible dans $\mathbb{F}_3[x]$ (car $0, 1$ et 2 ne sont pas des racines du polynôme).

Finalement, on en déduit que $\overline{\rho}_{\phi,\lambda}$ est irréductible pour tout idéal premier non nul λ de A.

■

Lemme 6.3 :
Pour tout idéal premier non nul λ de A, on a $\rho_{\phi,\lambda}(\mathrm{Gal}_F) = \mathrm{GL}_2(A_\lambda)$.

Preuve :
Soient λ un idéal premier non nul de A et $G := \rho_{\phi,\lambda}(\mathrm{Gal}_F) \subseteq \mathrm{GL}_2(A_\lambda)$.

* En utilisant le lemme 6.1 successivement avec $\mathfrak{a} := \lambda^i$ pour tout $i \in \mathbb{N}^*$ on trouve (système projectif) que $\det(G) = A_\lambda^\times$.

* De plus, puisque $\mathrm{PGCD}(v_\mathfrak{p}(j_\phi); q) = 1$, le troisième point de la proposition 4.6 implique que $\overline{\rho}_{\phi,\lambda}(I_\mathfrak{p})$ (et donc aussi $\overline{\rho}_{\phi,\lambda}(\mathrm{Gal}_F)$ par inclusion) contient un sous-groupe de cardinal $N(\lambda)$. Par le lemme 6.2, $\overline{\rho}_{\phi,\lambda}(\mathrm{Gal}_F)$ agit de manière irréductible sur $\mathbb{F}_\lambda^2$ et la proposition 4.2 nous donne $\mathrm{SL}_2(\mathbb{F}_\lambda) \subseteq \overline{\rho}_{\phi,\lambda}(\mathrm{Gal}_F)$. Enfin, en adjoignant à ce résultat le fait que $\det(G) = A_\lambda^\times$, on en déduit que l'image de G modulo λ est $\mathrm{GL}_2(\mathbb{F}_\lambda)$ tout entier. En effet, en notant G_λ l'image de G modulo λ, on a $\det(G_\lambda) = \mathbb{F}_\lambda^\times$ et $\mathrm{SL}_2(\mathbb{F}_\lambda) \subseteq G_\lambda$, d'où le diagramme commutatif suivant (par le théorème de factorisation des morphismes) :

$$\begin{array}{ccc} G_\lambda & \xrightarrow{f := \det|_{G_\lambda}} & \mathbb{F}_\lambda^\times \\ \downarrow & \nearrow & \\ G_\lambda / \mathrm{SL}_2(\mathbb{F}_\lambda) & & \end{array}$$

On a alors $G_\lambda / \mathrm{Ker}(f) \cong \mathbb{F}_\lambda^\times$ par le premier théorème d'isomorphisme et comme les groupes en jeu sont finis on a également que $\mathrm{Card}(G_\lambda) = \mathrm{Card}(\mathrm{Ker}(f))\,\mathrm{Card}(\mathbb{F}_\lambda^\times)$. Or, $\mathrm{SL}_2(\mathbb{F}_\lambda) \subseteq \mathrm{Ker}(f)$, d'où la majoration $\mathrm{Card}(\mathrm{SL}_2(\mathbb{F}_\lambda)) \leq \mathrm{Card}(\mathrm{Ker}(f))$, d'où :

$$\mathrm{Card}(G_\lambda) \geq \mathrm{Card}(\mathrm{SL}_2(\mathbb{F}_\lambda)) \times \mathrm{Card}(\mathbb{F}_\lambda^\times) = \mathrm{Card}(\mathrm{GL}_2(\mathbb{F}_\lambda)).$$

Or, comme G_λ est un sous-groupe de $\mathrm{GL}_2(\mathbb{F}_\lambda)$, on a bien que $G_\lambda = \mathrm{GL}_2(\mathbb{F}_\lambda)$.

* Fixons nous désormais un générateur π de l'idéal λ et considérons P un p-Sylow de $\overline{\rho}_{\phi,\lambda^2}(I_\mathfrak{p})$ (avec p le nombre premier divisant q).
Puisque $\mathrm{PGCD}(v_\mathfrak{p}(j_\phi); q) = 1$ et par le deuxième point de la proposition 4.6, on trouve que le cardinal de P est divisible par $N(\lambda)^2$. De plus, un p-Sylow de $\mathrm{GL}_2(\mathbb{F}_\lambda)$ a pour cardinal $N(\lambda)$ puisque :

$$\mathrm{Card}(\mathrm{GL}_2(\mathbb{F}_\lambda)) = \prod_{k=0}^{1} \left(q^{2\deg(\lambda)} - q^{k\deg(\lambda)}\right) = q^{\deg(\lambda)} \underbrace{\left(q^{2\deg(\lambda)} - 1\right)\left(q^{\deg(\lambda)} - 1\right)}_{\text{non divisible par } p}.$$

On en conclut donc qu'il existe $g \in P$ tel que $g \equiv I_2 + \pi B \ \left[\lambda^2\right]$ avec $B \in M_2(A_\lambda)$ tel que $B \not\equiv 0\ [\lambda]$.

Quitte à conjuguer la représentation $\overline{\rho}_{\phi,\lambda^2}$, on peut assumer grâce au premier point de la proposition 4.6 que :

$$\overline{\rho}_{\phi,\lambda^2}(I_\mathfrak{p}) \subseteq \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix},\ a \in (A/\lambda^2)^\times,\ b \in A/\lambda^2 \text{ et } c \in \mathbb{F}_q^\times \right\}.$$

Ainsi, on a

$$P \subseteq \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix},\ a \in (A/\lambda^2)^\times, a \equiv 1\ [\lambda] \text{ et } b \in A/\lambda^2 \right\}$$

et donc B modulo λ est de la forme $\begin{pmatrix} * & * \\ 0 & 0 \end{pmatrix}$. Enfin, puisque $B \not\equiv 0\ [\lambda]$, on en déduit que B modulo λ n'est pas une matrice scalaire.

Nous avons donc vérifié ici les hypothèses de la proposition 4.1 avec $q > 2$, d'où $G = \mathrm{GL}_2(A_\lambda)$.

■

Nous pouvons désormais démontrer le résultat voulu :
En posant $G := \rho_\phi(\mathrm{Gal}_F)$ un sous-groupe fermé de $\mathrm{GL}_2(\widehat{A})$ (car ρ_ϕ est un représentation continue et Gal_F est un groupe compact), on a $\det(G) = \widehat{A}^\times$ par le théorème 4.2 (avec $d := q-1$), il nous reste donc à montrer que $\mathrm{SL}_2(\widehat{A})$ est un sous-groupe de G. Pour cela, utilisons le théorème 4.1 avec $q > 2$:

* Pour tout idéal premier non nul λ de A, $\mathrm{SL}_2(A_\lambda)$ est un sous-groupe de $G_\lambda := \rho_{\phi,\lambda}(\mathrm{Gal}_F)$ par le lemme 6.3, ce qui nous donne la première hypothèse du théorème 4.1.

* Soient λ_1 et λ_2 deux idéaux premiers non nuls distincts de A de norme strictement plus grande que 3.
Le troisième point de la proposition 4.6 nous donne que $\overline{\rho}_{\phi,\lambda_1\lambda_2}(I_\mathfrak{p})$ contient un sous-groupe de cardinal $N(\lambda_1)N(\lambda_2)$. En particulier, G modulo $\lambda_1\lambda_2$ a un sous-groupe de cardinal $N(\lambda_1)N(\lambda_2)$, ce qui nous donne la deuxième hypothèse du théorème 4.1.

* Soient λ_1 et λ_2 deux idéaux premiers non nuls distincts de A de norme égale à 2.
Le troisième point de la proposition 4.6 nous donne que $\overline{\rho}_{\phi,\lambda_1\lambda_2}(I_\mathfrak{p})$ contient un sous-groupe conjugué dans $\mathrm{GL}_2(A_{\lambda_1\lambda_2})$ à $\left\{\begin{pmatrix}1 & b\\ 0 & 1\end{pmatrix},\ b \in A_{\lambda_1\lambda_2}\right\}$. En particulier, l'intersection de G modulo $\lambda_1\lambda_2$ avec $\mathrm{SL}_2(A_{\lambda_1\lambda_2})$ contient un sous-groupe conjugué dans $\mathrm{GL}_2(A_{\lambda_1\lambda_2})$ à $\left\{\begin{pmatrix}1 & b\\ 0 & 1\end{pmatrix},\ b \in A_{\lambda_1\lambda_2}\right\}$, ce qui nous donne la troisième hypothèse du théorème 4.1.

* Enfin, on considère le cas où $q = 3$ et $\mathfrak{a} = (T)(T-1)(T-2)$. Puisque l'on a $\det(G) = \widehat{A}^\times$, alors en particulier on a que le déterminant de G modulo $\mathfrak{a}$ est égal à $A_\mathfrak{a}^\times$ tout entier (car les idéaux composant $\mathfrak{a}$ sont deux à deux premiers entre eux). Finalement, on a bien vérifié la dernière hypothèse du théorème 4.1.

En utilisant le théorème 4.1 avec $q > 2$, on en déduit que $\mathrm{SL}_2(\widehat{A}) = D(G) \subseteq G$ et puisque l'on a également $\det(G) = \widehat{A}^\times$ (par le théorème 4.2), on en déduit que $G = \rho_\phi(\mathrm{Gal}_F) = \mathrm{GL}_2(\widehat{A})$. En effet, on a que $\mathrm{SL}_2(\widehat{A}) \subsetneq G \subseteq \mathrm{GL}_2(\widehat{A})$ et par le premier théorème d'isomorphisme appliqué aux morphismes de groupes det et $f := \det|_G$, on a $\mathrm{GL}_2(\widehat{A})/\mathrm{SL}_2(\widehat{A}) \cong \widehat{A}^\times$ (dont les classes seront notées $\overline{N}$ pour $N \in \mathrm{GL}_2(\widehat{A})$) ainsi que $G/\mathrm{SL}_2(\widehat{A}) \cong \widehat{A}^\times$ (dont les classes seront notées $\overline{\overline{N}}$ pour $N \in G$).

Soit $M \in \mathrm{GL}_2(\widehat{A})$.
On a $\det\left(\overline{M}\right) \in \widehat{A}^\times$, donc il existe $\overline{\overline{N}} \in G/\mathrm{SL}_2(\widehat{A})$ tel que $\det\left(\overline{M}\right) = \det\left(\overline{\overline{N}}\right)$. Or, il existe $N \in G$ tel que $\det(M) = \det(N)$ et par conséquent, $\det\left(MN^{-1}\right) = 1$ et ainsi $MN^{-1} \in \mathrm{SL}_2(\widehat{A}) \subseteq G$. Finalement, on a que $M = \underbrace{\left(MN^{-1}\right)}_{\in G}\underbrace{N}_{\in G} \in G$, c'est-à-dire $\mathrm{GL}_2(\widehat{A}) \subseteq G$ et par conséquent on a bien que $G = \mathrm{GL}_2(\widehat{A})$.

II Le cas $q = 2$

Dans toute cette partie, on suppose que $q = 2$, on considère $\phi : A \longrightarrow F\{\tau\}$ le module de Drinfeld défini par $\phi_T := T + T^3\tau + \left(T^2+T+1\right)\tau^2$, on pose l'idéal premier non nul $\mathfrak{p} := \left(T^2+T+1\right)$ de A et on note $I_\mathfrak{p}$ le groupe d'inertie de Gal_F en $\mathfrak{p}$.

Commençons par remarquer que $\det\left(\rho_\phi(\mathrm{Gal}_F)\right) = \widehat{A}^\times$ par le théorème 4.2 (car $q = 2$), $\mathfrak{p}$ est le seul idéal premier non nul de A pour lequel ϕ ait une mauvaise réduction et ϕ a une réduction stable de rang 1 en $\mathfrak{p}$. Enfin, on a $j_\phi = \frac{(T^3)^{q+1}}{T^2+T+1} = \frac{T^9}{T^2+T+1}$ et donc $v_\mathfrak{p}\left(j_\phi\right) = -1$.

Lemme 6.4 :
Le morphisme $\mathrm{Gal}_F \longrightarrow \mathrm{GL}_2(\widehat{A})/D\left(\mathrm{GL}_2(\widehat{A})\right)$ obtenu en composant ρ_ϕ avec la projection sur $D\left(\mathrm{GL}_2(\widehat{A})\right)$ est surjectif.

Preuve :
Il suffit d'appliquer la proposition 5.1 puisque $v_\infty(j_\phi) = -7 \leq -5$.

■

Lemme 6.5 :
Pour tout idéal premier non nul λ de A, on a $\overline{\rho}_{\phi,\lambda}(\mathrm{Gal}_F) = \mathrm{GL}_2(\mathbb{F}_\lambda)$.

Preuve :
Raisonnons par l'absurde en supposant que $\overline{\rho}_{\phi,\lambda}(\mathrm{Gal}_F) \neq \mathrm{GL}_2(\mathbb{F}_\lambda)$ pour un idéal premier non nul λ de A.
Par le troisième point de la proposition 4.6 (car $\mathrm{PGCD}(v_\mathfrak{p}(j_\phi); q) = \mathrm{PGCD}(-1; 2) = 1$ et $e = 0$) on trouve que $\overline{\rho}_{\phi,\lambda}(I_\mathfrak{p})$ contient un sous-groupe de cardinal $N(\lambda)$. De plus, par la proposition 4.2, la représentation $\overline{\rho}_{\phi,\lambda}$ est réductible. En effet, s'il était irréductible, alors $\overline{\rho}_{\phi,\lambda}(\mathrm{Gal}_F)$ contiendrait $\mathrm{SL}_2(\mathbb{F}_\lambda)$ et donc devrait être $\mathrm{GL}_2(\mathbb{F}_\lambda)$ par surjectivité du déterminant (d'après la proposition 4.8) ce qui contredit l'hypothèse faite sur $\overline{\rho}_{\phi,\lambda}(\mathrm{Gal}_F)$.

Quitte à conjuguer $\overline{\rho}_{\phi,\lambda}$, on peut supposer que :

$$\forall \sigma \in \mathrm{Gal}_F,\ \overline{\rho}_{\phi,\lambda}(\sigma) = \begin{pmatrix} \chi_1(\sigma) & * \\ 0 & \chi_2(\sigma) \end{pmatrix},$$

où $\chi_1, \chi_2 : \mathrm{Gal}_F \longrightarrow \mathbb{F}_\lambda^\times$ sont des caractères.

Supposons que $\deg(\lambda) = 1$, c'est-à-dire que $\lambda = (T + i)$ pour $i \in \mathbb{F}_2$.
Les éléments non nuls de $\phi[\lambda]$ sont les racines du polynôme $Q(x) := (T^2 + T + 1)x^3 + T^3x + (T + i) \in A[x]$ (qui est séparable). On a $\chi_1 = 1$ puisque $\mathbb{F}_\lambda^\times = \mathbb{F}_2^\times$ et donc il existe un élément non nul de $\phi[\lambda]$ appartenant à F (car une droite est fixe par l'action de Gal_F tout entier), en particulier, $Q(x)$ a une racine dans F. Ainsi, l'image de $Q(x)$ dans $\mathbb{F}_\mathfrak{q}$ a une racine dans $\mathbb{F}_\mathfrak{q}$ pour tout idéal premier non nul $\mathfrak{q} \neq \left(T^2 + T + 1\right)$ de A. Cependant, un calcul montre que $Q(x)$ est irréductible modulo $\mathfrak{q}$ pour un certain $\mathfrak{q} \in \left\{(T + 1); \left(T^3 + T + 1\right)\right\}$ (qu'on choisit en fonction de la valeur de i).

Ainsi, on a $\deg(\lambda) > 1$ et puisque ϕ a une bonne réduction en dehors de $\mathfrak{p}$, on a que χ_1 et χ_2 sont non ramifiés en tout idéal premier non nul de A excepté peut-être en $\mathfrak{p}$ et λ (par le petit paragraphe au début de la sous-partie III.1). Or, lorsque $\lambda = \mathfrak{p}$, le premier point de la proposition 4.6 et le fait que $\mathbb{F}_q^\times = \left\{\overline{1}\right\}$ impliquent que χ_1 ou χ_2 est non ramifié en $\mathfrak{p}$. De même lorsque $\lambda \neq \mathfrak{p}$, le premier point de la proposition 4.6 et le fait que $\mathbb{F}_q^\times = \left\{\overline{1}\right\}$ impliquent que χ_1 et χ_2 sont non ramifiés en $\mathfrak{p}$. De plus, ϕ a une bonne réduction en λ et la proposition 4.5 ainsi que la réductibilité de $\overline{\rho}_{\phi,\lambda}$ impliquent que χ_1 ou χ_2 est non ramifié en λ.

Nous avons donc vérifié les deux points du lemme 4.14 avec $n := 1$, donc par le lemme 4.15, il existe $\zeta \in \mathbb{F}_\lambda^\times$ tel que $P_{\phi,\mathfrak{q}}\left(\zeta^{\deg(\mathfrak{q})}\right) = 0$ dans $\mathbb{F}_\lambda$ pour tout idéal premier non nul $\mathfrak{q} \neq \lambda$ de A où ϕ a une bonne réduction. Or, comme $\deg(\lambda) > 1$, $P_{\phi,(T)}(x)$ et $P_{\phi,(T+1)}(x)$ ont une racine commune modulo λ et donc leur résultat r est divisible par λ. Cependant, grâce au lemme 4.12, on a une expression de $P_{\phi,(T)}(x)$ et $P_{\phi,(T+1)}(x)$ et on trouve que $r = T + 1$. Ainsi, on a $r = T + 1 \equiv 0\ [\lambda]$, ce qui est contradictoire avec le fait que $\deg(\lambda) > 1$.

Finalement, on obtient que pour tout idéal premier non nul λ de A, $\overline{\rho}_{\phi,\lambda} = \mathrm{GL}_2(\mathbb{F}_\lambda)$.

■

Lemme 6.6 :
Pour tout idéal premier non nul λ de A, on a $\rho_{\phi,\lambda}(\mathrm{Gal}_F) = \mathrm{GL}_2(A_\lambda)$.

Preuve :
Soit λ un idéal premier non nul de A.
Notons $G := \rho_{\phi,\lambda}(\mathrm{Gal}_F)$ qui est sous-groupe fermé de $\mathrm{GL}_2(A_\lambda)$ (car $\rho_{\phi,\lambda}$ est un représentation continue et Gal_F est un groupe compact) et montrons le lemme en appliquant la proposition 4.1.

On a $\det(G) = A_\lambda^\times$ puisque $\det(\rho_\phi(\mathrm{Gal}_F)) = \widehat{A}^\times$ (par le théorème 4.2 puisque $q = 2$). De plus, par le lemme 6.5, l'image de G modulo λ est égale à $\mathrm{GL}_2(\mathbb{F}_\lambda)$. On a donc vérifié les deux premières hypothèses de la proposition 4.1.

Raisonnons désormais par disjonction de cas :

* Supposons que $\deg(\lambda) > 1$ (et donc $\mathrm{Card}(\mathbb{F}_\lambda) > 2$).
Par le premier point de la proposition 4.6, $\overline{\rho}_{\phi,\lambda^2}(I_\mathfrak{p})$ a un sous-groupe de cardinal $N(\lambda)^2$ qui est conjugué dans $\mathrm{GL}_2(A/\lambda^2)$ à un sous-groupe de $\left\{\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix},\ a \in (A/\lambda^2)^\times \text{ et } b \in A/\lambda^2\right\}$. En se donnant une uniformisante π de A_λ, on trouve donc que G contient une matrice de la forme $I_2 + \pi B$ avec $B \in \mathcal{M}_2(A_\lambda)$ et B n'est pas une matrice scalaire modulo λ. En effet, l'élément $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \mathrm{GL}_2(A/\lambda^2)$ se relève en un élément $I_2 + \pi B$ de $\mathrm{GL}_2(A_\lambda)$ tel que B modulo λ n'est pas une matrice scalaire (car le coefficient en haut à droite est non nul modulo λ).
La troisième hypothèse étant vérifiée, la proposition 4.1 nous donne alors que $G = \mathrm{GL}_2(A_\lambda)$.

* On peut donc désormais supposer que $\deg(\lambda) = 1$ (et donc $\mathbb{F}_\lambda = \mathbb{F}_2$).
Puisque $\lambda \neq \mathfrak{p}$ et que $\mathrm{PGCD}(v_\mathfrak{p}(j_\phi); q) = 1$, le troisième point de la proposition 4.6 nous donne que pour tout $i \in \mathbb{N}^*$, $\overline{\rho}_{\phi,\lambda^i}(I_\mathfrak{p})$ contient un sous-groupe qui est conjugué dans $\mathrm{GL}_2(A/\lambda^i)$ à $\left\{\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix},\ b \in A/\lambda^i\right\}$.
En utilisant le fait que G est fermé, on obtient que G a un élément qui est conjugué dans $\mathrm{GL}_2(A_\lambda)$ à une matrice de la forme $\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$ avec $b \not\equiv 0\ [\lambda]$. En particulier, G possède un élément de déterminant 1 dont l'image modulo λ est d'ordre 2.

  Montons que $\overline{G} := \overline{\rho}_{\phi,\lambda^2}(\mathrm{Gal}_F)$ est égal à $\mathrm{GL}_2(A/\lambda^2)$ et pour cela, posons S le sous-groupe de $\mathrm{SL}_2(A/\lambda^2)$ qui est l'image réciproque de $D\left(\mathrm{GL}_2(\mathbb{F}_\lambda)\right)$ par qui est la réduction modulo λ.
  Puisque $\mathbb{F}_\lambda = \mathbb{F}_2$, on a $\mathrm{Card}(S) = 2^3 \times 3$ (par le premier théorème d'isomorphisme appliqué à la réduction modulo λ) et $[\mathrm{GL}_2(A/\lambda^2) : S] = 2^2 = 4$. De plus le quotient $\mathrm{GL}_2(\mathbb{F}_\lambda)/D\left(\mathrm{GL}_2(\mathbb{F}_\lambda)\right)$ est abélien (car de cardinal plus petit que 6) et donc l'application quotient $\overline{G} \longrightarrow \mathrm{GL}_2(\mathbb{F}_\lambda)/D\left(\mathrm{GL}_2(\mathbb{F}_\lambda)\right)$ est surjective par la proposition 5.1. En particulier, on a $\left[\mathrm{GL}_2(A/\lambda^2) : \overline{G}\right] = \left[S : S \cap \overline{G}\right]$ (par le deuxième théorème d'isomorphisme). Or, on sait que $\overline{G}$ contient une matrice g qui est conjugué dans $\mathrm{GL}_2(A/\lambda)$ à $\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$ pour un certain $b \not\equiv 0\ [\lambda]$. De plus, g n'est pas stable sous l'action de conjugaison par $\overline{G}$ puisque l'image de $\overline{G}$ modulo λ est $\mathrm{GL}_2(\mathbb{F}_\lambda)$. Ainsi, $\mathrm{Card}\left(S \cap \overline{G}\right)$ est divisible par 4. On a également que le groupe $S \cap \overline{G}$ contient un élément d'ordre 3 puisque l'image de $\overline{G}$ modulo λ est $\mathrm{GL}_2(\mathbb{F}_\lambda) = \mathrm{GL}_2(\mathbb{F}_2)$ et $[\mathrm{GL}_2(A/\lambda^2) : S] = 2^2$.

  Enfin, puisque $\mathrm{Card}(S) = 2^3 \times 3 = 12$, on trouve que $\left[\mathrm{GL}_2(A/\lambda^2) : \overline{G}\right] = \left[S : S \cap \overline{G}\right]$ est égal à 1 ou 2 (car $S \cap \overline{G}$ est d'ordre au moins 12 par ce qui précède est divise 24 par le théorème de Lagrange). Or, si $\left[\mathrm{GL}_2(A/\lambda^2) : \overline{G}\right] = 2$, on aurait que $\overline{G}$ serait un sous-groupe distingué de $\mathrm{GL}_2(A/\lambda^2)$ qui posséderait un quotient abélien non trivial, ce qui contredirait la proposition 5.1. Ainsi, $\left[\mathrm{GL}_2(A/\lambda^2) : \overline{G}\right] = 1$ et donc $\overline{G} = \mathrm{GL}_2(A/\lambda^2)$.

Finalement, nous avons vérifié toutes les hypothèses de la proposition 4.1 (avec $\mathrm{Card}(\mathbb{F}_\lambda) = 2$), donc on en conclut que $G = \mathrm{GL}_2(A_\lambda)$.

■

Lemme 6.7 :
On a l'inclusion $D\left(\mathrm{GL}_2(\widehat{A})\right) \subseteq \rho_\phi(\mathrm{Gal}_F)$.

Preuve :
Posons $G := \rho_\phi(\mathrm{Gal}_F)$ qui est sous-groupe fermé de $\mathrm{GL}_2(\widehat{A})$ (car ρ_ϕ est un représentation continue et Gal_F est un groupe compact).
Montrons que G vérifie les hypothèses du théorème 4.1 :

* Par le lemme 6.6, le groupe $G_\lambda := \rho_{\phi,\lambda}(\mathrm{Gal}_F)$ est égal à $\mathrm{GL}_2(A_\lambda)$ pour tout idéal premier non nul λ de A, donc $\mathrm{SL}_2(A_\lambda) \subseteq G_\lambda$. Nous avons donc vérifiés la première hypothèse du théorème 4.1.

* Soient λ_1 et λ_2 deux idéaux premiers non nuls de A distincts tels que $\deg(\lambda_1) = \deg(\lambda_2) \geq 2$.
Par le troisième point de la proposition 4.6, $\overline{\rho}_{\phi,\lambda_1\lambda_2}(I_\mathfrak{p}) \subseteq \overline{\rho}_{\phi,\lambda_1\lambda_2}(\mathrm{Gal}_F)$ contient un sous-groupe d'ordre $N(\lambda_1)N(\lambda_2) = N(\lambda_1)^2$. On a ainsi vérifié la deuxième hypothèse du théorème 4.1.

* Soient λ_1 et λ_2 deux idéaux premiers non nuls de A distincts tels que $\deg(\lambda_1) = \deg(\lambda_2) = 1$.
On a $\mathfrak{p} \notin \{\lambda_1; \lambda_2\}$ et pour tout $i \in \mathbb{N}^*$, le troisième point de la proposition 4.6 implique que $\overline{\rho}_{\phi,\lambda_1^i\lambda_2^i}(I_\mathfrak{p}) \subseteq \overline{\rho}_{\phi,\lambda_1^i\lambda_2^i}(\mathrm{Gal}_F)$ contient un sous-groupe qui est conjugué dans $\mathrm{GL}_2(A/(\lambda_1^i\lambda_2^i))$ à $\left\{\begin{pmatrix}1 & b\\ 0 & 1\end{pmatrix},\ b \in A/(\lambda_1^i\lambda_2^i)\right\}$. Ainsi, le sous-groupe fermé $G_{\lambda_1\lambda_2} := \rho_{\phi,\lambda_1\lambda_2}(\mathrm{Gal}_F)$ contient un sous-groupe qui est conjugué dans $\mathrm{GL}_2(A/(\lambda_1\lambda_2))$ à $\left\{\begin{pmatrix}1 & b\\ 0 & 1\end{pmatrix},\ b \in A/(\lambda_1\lambda_2)\right\}$. Ainsi, le groupe $G_{\lambda_1\lambda_2} \cap \mathrm{SL}_2(A_{\lambda_1\lambda_2})$ contient un sous-groupe qui est conjugué dans $\mathrm{GL}_2(A_{\lambda_1\lambda_2})$ à $\left\{\begin{pmatrix}1 & b\\ 0 & 1\end{pmatrix},\ b \in A_{\lambda_1\lambda_2}\right\}$ et on a donc vérifié la troisième hypothèse du théorème 4.1.

* Enfin, pour λ_1 et λ_2 les deux idéaux premiers non nuls de A distincts tels que $\deg(\lambda_1) = \deg(\lambda_2) = 1$ et $\mathfrak{a} = \lambda_1\lambda_2$, on a directement que $\det(\rho_{\phi,\mathfrak{a}}(\mathrm{Gal}_F)) = A_\mathfrak{a}^\times$ puisque $\det(\rho_\phi(\mathrm{Gal}_F)) = \widehat{A}^\times$ (par le théorème 4.2).

Finalement, on a donc vérifié toutes les hypothèses du théorème 4.1 et on en déduit que $D(G) = D\left(\mathrm{GL}_2(\widehat{A})\right)$ et donc $D\left(\mathrm{GL}_2(\widehat{A})\right) \subseteq \rho_\phi(\mathrm{Gal}_F)$.

■

Nous pouvons maintenant donner la preuve du théorème 0.4 dans le cas où $q = 2$:
Par le lemme 6.4, on a que le morphisme $\mathrm{Gal}_F \longrightarrow \mathrm{GL}_2(\widehat{A})/D\left(\mathrm{GL}_2(\widehat{A})\right)$ obtenu en composant ρ_ϕ avec la projection sur $D\left(\mathrm{GL}_2(\widehat{A})\right)$ est surjectif et par le lemme 6.7 on a $D\left(\mathrm{GL}_2(\widehat{A})\right) \subseteq \rho_\phi(\mathrm{Gal}_F)$, on obtient donc que $\rho_\phi(\mathrm{Gal}_F) = \mathrm{GL}_2(\widehat{A})$.

En effet, on a en toute généralité que $\rho_\phi(\mathrm{Gal}_F) \subseteq \mathrm{GL}_2(\widehat{A})$ donc il nous suffit de montrer l'inclusion réciproque. Pour $g \in \mathrm{GL}_2(\widehat{A})$, en notant π la projection canonique de $\mathrm{GL}_2(\widehat{A})$ dans $\mathrm{GL}_2(\widehat{A})/D\left(\mathrm{GL}_2(\widehat{A})\right)$, on a

$$\pi\left(\rho_\phi(\mathrm{Gal}_F)\right) = \mathrm{GL}_2(\widehat{A})/D\left(\mathrm{GL}_2(\widehat{A})\right),$$

donc il existe un élément $h \in \rho_\phi(\mathrm{Gal}_F)$ tel que $\pi(h) = \pi(g)$. Par conséquent, on a $h^{-1}g \in D\left(\mathrm{GL}_2(\widehat{A})\right)$ et donc :

$$g = h\left(h^{-1}g\right) \in \rho_\phi(\mathrm{Gal}_F)D\left(\mathrm{GL}_2(\widehat{A})\right).$$

Or, on a $D\left(\mathrm{GL}_2(\widehat{A})\right) \subseteq \rho_\phi(\mathrm{Gal}_F)$ et donc on a $g \in \rho_\phi(\mathrm{Gal}_F)$, c'est-à-dire $\mathrm{GL}_2(\widehat{A}) \subseteq \rho_\phi(\mathrm{Gal}_F)$.

Finalement, on obtient par double inclusion que $\rho_\phi(\mathrm{Gal}_F) = \mathrm{GL}_2(\widehat{A})$ et donc la représentation ρ_ϕ est surjective.

Annexe A

Groupe de Galois absolu

Dans cet annexe on donne des résultats de base (sans démonstration) sur le groupe de Galois absolu. On commencera tout d'abord par rappeler des résultats dans le cas fini dans la partie I qui nous serviront dans la partie II lorsque nous définirons le groupe de Galois absolu et que nous le verrons comme une limite projective.

I Rappels sur les extensions galoisiennes finies

Le but de cette première partie est de donner des rappels sur les extensions finies galoisiennes. On ne donnera donc pas de preuves et on suppose connues les notions de décomposition d'idéaux, d'indice de ramification, de degré résiduel, de corps résiduels ainsi que la théorie de Galois dans le cas des extensions finies. Nous commencerons par donner des généralités en sous-partie I.1 avant de parler de substitution du Frobenius en sous-partie I.2.

I.1 Généralités

Dans toute cette sous-partie on considère une extension de corps $\mathbb{L}/\mathbb{K}$ finie de degré n et galoisienne de groupe de Galois $\mathrm{Gal}(\mathbb{L}/\mathbb{K})$. On se donne également un anneau B noethérien intégralement clos et de corps des fractions $\mathbb{K}$, C la fermeture intégrale de B dans $\mathbb{L}$ (c'est-à-dire l'ensemble des éléments de $\mathbb{L}$ qui sont entiers sur B) que l'on suppose être un B-module de type fini ainsi que $\mathfrak{p}$ un idéal premier non nul de B.

Proposition A.1 :
Le groupe $\mathrm{Gal}(\mathbb{L}/\mathbb{K})$ agit transitivement sur l'ensemble des idéaux premiers $\mathfrak{P}$ de C au-dessus de $\mathfrak{p}$.

Corollaire A.1 :
Soit $\mathfrak{P}$ un idéal premier de C au-dessus de $\mathfrak{p}$.
Les entiers $e_{\mathfrak{P}}$ et $f_{\mathfrak{P}}$ ne dépendent que de $\mathfrak{p}$.
En particulier, si on les note $e_{\mathfrak{p}}$, $f_{\mathfrak{p}}$ ainsi que $g_{\mathfrak{p}}$ le nombre d'idéaux premiers $\mathfrak{P}$ au-dessus de $\mathfrak{p}$, alors on a $n = e_{\mathfrak{p}} f_{\mathfrak{p}} g_{\mathfrak{p}}$.

Définition A.1 : Groupe de décomposition de $\mathfrak{P}$:
On considère $\mathfrak{P}$ un idéal premier de C au-dessus de $\mathfrak{p}$.
On appelle **groupe de décomposition** de $\mathfrak{P}$ le sous-groupe de $\mathrm{Gal}(\mathbb{L}/\mathbb{K})$ formé des éléments σ tels que $\sigma(\mathfrak{P}) = \mathfrak{P}$ et on le note $D_{\mathfrak{P}}(\mathbb{L}/\mathbb{K})$.

Remarques :

* Si $\mathfrak{P}'$ est un autre idéal premier de C au-dessus de $\mathfrak{p}$, alors la proposition A.1 montre que $D_{\mathfrak{P}'}(\mathbb{L}/\mathbb{K})$ est conjugué à $D_{\mathfrak{P}}(\mathbb{L}/\mathbb{K})$.
* Pour $\mathfrak{P}$ un idéal premier de C au-dessus de $\mathfrak{p}$, l'indice de $D_{\mathfrak{P}}(\mathbb{L}/\mathbb{K})$ dans $\mathrm{Gal}(\mathbb{L}/\mathbb{K})$ est égal à $g_{\mathfrak{p}}$.

Désormais on fixe $\mathfrak{P}$ un idéal premier de C au-dessus de $\mathfrak{p}$.
Par la correspondance de Galois dans le cas fini, le groupe $D_{\mathfrak{P}}(\mathbb{L}/\mathbb{K})$ correspond à une extension $\mathbb{K}_D/\mathbb{K}$ contenue dans $\mathbb{L}$ et cette extension n'est galoisienne que si $D_{\mathfrak{P}}(\mathbb{L}/\mathbb{K})$ est distingué dans $\mathrm{Gal}(\mathbb{L}/\mathbb{K})$. On a alors par la correspondance de Galois dans le cas fini que :

$$[\mathbb{K}_D : \mathbb{K}] = g_{\mathfrak{p}},\ [\mathbb{L} : \mathbb{K}_D] = e_{\mathfrak{p}} f_{\mathfrak{p}} \text{ et } \mathrm{Gal}(\mathbb{L}/\mathbb{K}_D) = D_{\mathfrak{P}}(\mathbb{L}/\mathbb{K}).$$

Désormais, on considère également $\mathbb{M}$ un corps intermédiaire entre $\mathbb{K}$ et $\mathbb{L}$ et on note $C_{\mathbb{M}} := \mathbb{M} \cap C$ la fermeture intégrale de B dans $\mathbb{M}$, $\mathfrak{P}_{\mathbb{M}} := \mathfrak{P} \cap C_{\mathbb{M}}$ et $\overline{M} := C_{\mathbb{M}}/\mathfrak{P}_{\mathbb{M}}$ le corps résiduel (en particulier les définitions précédentes s'appliquent à $\mathbb{K}$ et $\mathbb{L}$).

Pour $\sigma \in D_{\mathfrak{P}}(\mathbb{L}/\mathbb{K})$, σ définit par passage au quotient un $\overline{\mathbb{K}}$-automorphisme $\overline{\sigma}$ de $\overline{\mathbb{L}}$ et on obtient alors un morphisme $\varepsilon_{\mathfrak{P}} : D_{\mathfrak{P}}(\mathbb{L}/\mathbb{K}) \longrightarrow \mathrm{Gal}\left(\overline{\mathbb{L}}/\overline{\mathbb{K}}\right)$.

Définition A.2 : Groupe d'inertie de $\mathfrak{P}$:
On considère $\mathfrak{P}$ un idéal premier de C au-dessus de $\mathfrak{p}$.
On appelle **groupe d'inertie** de $\mathfrak{P}$ le noyau de $\varepsilon_{\mathfrak{P}}$ et on le note $I_{\mathfrak{P}}(\mathbb{L}/\mathbb{K})$.

Toujours par la correspondance de Galois dans le cas fini, il correspond à $I_{\mathfrak{P}}(\mathbb{L}/\mathbb{K})$ une extension galoisienne $\mathbb{K}_I/\mathbb{K}_D$ de groupe de Galois $D_{\mathfrak{P}}(\mathbb{L}/\mathbb{K})/I_{\mathfrak{P}}(\mathbb{L}/\mathbb{K})$ et on a $\mathrm{Gal}(\mathbb{L}/\mathbb{K}_I) = I_{\mathfrak{P}}(\mathbb{L}/\mathbb{K})$.

Remarque :
Le groupe de Galois $\mathrm{Gal}\left(\overline{\mathbb{L}}/\overline{\mathbb{K}}\right)$ est un groupe engendré par le Frobenius $\mathrm{Frob}_q : x \longmapsto x^q$ et tout élément de $D_{\mathfrak{P}}(\mathbb{L}/\mathbb{K})$ qui s'envoie sur Frob_q via $\varepsilon_{\mathfrak{P}}$ est appelé **élément de Frobenius en $\mathfrak{P}$** et se note $\mathrm{Frob}_{\mathfrak{P}}$. De plus, lorsque l'extension $\mathbb{L}/\mathbb{K}$ est non ramifiée, $\mathrm{Frob}_{\mathfrak{P}}$ est défini de manière unique et pour tout $\sigma \in \mathrm{Gal}(\mathbb{L}/\mathbb{K})$ on a $\mathrm{Frob}_{\sigma(\mathfrak{P})} = \sigma\,\mathrm{Frob}_{\mathfrak{P}}\,\sigma^{-1}$ et donc l'ensemble des $\mathrm{Frob}_{\mathfrak{P}}$ défini une classe de conjugaison dans $\mathrm{Gal}(\mathbb{L}/\mathbb{K})$ appelée **classe de conjugaison du Frobenius en $\mathfrak{p}$**.

Proposition A.2 :
L'extension résiduelle $\overline{\mathbb{L}}/\overline{\mathbb{K}}$ est quasi-galoisienne (c'est-à-dire normale) et le morphisme $\varepsilon_{\mathfrak{P}}$ donne une isomorphisme de $D_{\mathfrak{P}}(\mathbb{L}/\mathbb{K})/I_{\mathfrak{P}}(\mathbb{L}/\mathbb{K})$ dans $\mathrm{Gal}\left(\overline{\mathbb{L}}/\overline{\mathbb{K}}\right)$.

Désormais, on note $\overline{\mathbb{L}}_s$ la plus grande extension séparable de $\overline{\mathbb{K}}$ contenue dans $\overline{\mathbb{L}}$.
Par ce qui précède, l'extension $\overline{\mathbb{L}}_s/\overline{\mathbb{K}}$ est galoisienne de groupe de Galois $D_{\mathfrak{P}}(\mathbb{L}/\mathbb{K})/I_{\mathfrak{P}}(\mathbb{L}/\mathbb{K})$ et on pose :

$$f_0 := \left[\overline{\mathbb{L}}_s : \overline{\mathbb{K}}\right] \text{ et } p^s = \left[\overline{L} : \overline{L}_s\right].$$

Proposition A.3 :
Soient w, w_I, w_D et v les valuations discrètes définies respectivement par les idéaux $\mathfrak{P}$, $\mathfrak{P}_I$, $\mathfrak{P}_D$ et $\mathfrak{p}$.

- On a $[\mathbb{L} : \mathbb{K}_I] = ep^s$, $[\mathbb{K}_I : \mathbb{K}_D] = f_0$ et $[\mathbb{K}_D : \mathbb{K}] = g$;
- La valuation w prolonge w_T avec l'indice e et w_I et w_D prolongent v avec l'indice 1 ;
- On a $\overline{K}_I = \overline{L}_s$, $\overline{\mathbb{K}}_D = \overline{\mathbb{K}}$.
  En particulier, on a $\left[\overline{\mathbb{L}} : \overline{\mathbb{K}}_I\right] = p^s$, $\left[\overline{\mathbb{K}}_I : \overline{\mathbb{K}}_D\right] = f_0$ et $\left[\overline{\mathbb{K}}_D : \overline{K}\right] = 1$.

Corollaire A.2 :
Si $\overline{\mathbb{L}}/\overline{\mathbb{K}}$ est séparable, alors c'est une extension galoisienne de groupe de Galois $D_{\mathfrak{P}}(\mathbb{L}/\mathbb{K})/I_{\mathfrak{P}}(\mathbb{L}/\mathbb{K})$ et on a $\overline{\mathbb{K}}_I = \overline{L}$, $[\mathbb{L} : \mathbb{K}_I] = e$, $[\mathbb{K}_I : \mathbb{K}_D] = f$ et $[\mathbb{K}_D : \mathbb{K}] = g$.

Remarque :
L'extension résiduelle $\overline{\mathbb{L}}/\overline{\mathbb{K}}$ est séparable lorsque $\overline{\mathbb{K}}$ est un corps parfait ou lorsque l'ordre du groupe d'inertie $I_{\mathfrak{P}}(\mathbb{L}/\mathbb{K})$ est premier à la caractéristique du corps résiduel $\overline{\mathbb{K}}$.

De même, les groupes $D_{\mathfrak{P}}(\mathbb{L}/\mathbb{M})$ et $I_{\mathfrak{P}}(\mathbb{L}/\mathbb{M})$ sont bien définis et lorsque $\mathbb{M}/\mathbb{K}$ est galoisienne, les groupes $D_{\mathfrak{P}}(\mathbb{M}/\mathbb{K})$ et $I_{\mathfrak{P}}(\mathbb{M}/\mathbb{K})$ sont biens définis et on a la proposition suivante :

Proposition A.4 :

* On a $D_{\mathfrak{P}}(\mathbb{L}/\mathbb{M}) = D_{\mathfrak{P}}(\mathbb{L}/\mathbb{K}) \cap \mathrm{Gal}(\mathbb{L}/\mathbb{M})$ et $I_{\mathfrak{P}}(\mathbb{L}/\mathbb{M}) = I_{\mathfrak{P}}(\mathbb{L}/\mathbb{K}) \cap \mathrm{Gal}(\mathbb{L}/\mathbb{M})$;
* Si $\mathbb{M}/\mathbb{K}$ est galoisienne, alors le diagramme suivant est commutatif et ses lignes et colonnes sont exactes :

$$\begin{array}{ccccccccc}
 & & 1 & & 1 & & 1 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & I_{\mathfrak{P}}(\mathbb{L}/\mathbb{M}) & \longrightarrow & I_{\mathfrak{P}}(\mathbb{L}/\mathbb{K}) & \longrightarrow & I_{\mathfrak{P}}(\mathbb{M}/\mathbb{K}) & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & D_{\mathfrak{P}}(\mathbb{L}/\mathbb{M}) & \longrightarrow & D_{\mathfrak{P}}(\mathbb{L}/\mathbb{K}) & \longrightarrow & D_{\mathfrak{P}}(\mathbb{M}/\mathbb{K}) & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & \mathrm{Gal}\left(\overline{\mathbb{L}}/\overline{\mathbb{M}}\right) & \longrightarrow & \mathrm{Gal}\left(\overline{\mathbb{L}}/\overline{\mathbb{K}}\right) & \longrightarrow & \mathrm{Gal}\left(\overline{\mathbb{M}}/\overline{\mathbb{K}}\right) & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 1 & & 1 & & 1 & &
\end{array}$$

Remarque :
Lorsque l'on veut étudier les groupes de décomposition ou d'inertie au-dessus de $\mathfrak{p}$, on peut s'il l'on veut, remplacer B par l'anneau de valuation discrète $B_{\mathfrak{p}}$ (et cette réduction au cas local peut être poussée plus loin car on peut même remplacer $B_{\mathfrak{p}}$ par son complété).

I.2 Substitution du Frobenius

Dans toute cette sous-partie, on considère $\mathbb{L}/\mathbb{K}$ une extension galoisienne, B un anneau de Dedekind de corps des fractions $\mathbb{K}$, C sa fermeture intégrale dans $\mathbb{L}$ ainsi que $\mathfrak{P}$ un idéal premier non nul de C et $\mathfrak{p} := \mathfrak{P} \cap B$.

Supposons que $\mathbb{L}/\mathbb{K}$ soit non ramifiée en $\mathfrak{P}$ et que $B/\mathfrak{p}$ soit un corps fini à q éléments.
Le groupe d'inertie $I_{\mathfrak{P}}(\mathbb{L}/\mathbb{K})$ est alors réduit à l'identité et le groupe de décomposition $D_{\mathfrak{P}}(\mathbb{L}/\mathbb{K})$ s'identifie au groupe de Galois de l'extension résiduelle $\overline{L}/\overline{\mathbb{K}}$. Or, puisque $\overline{\mathbb{K}} = \mathbb{F}_q$, ce groupe de Galois est un groupe cyclique engendré par le Frobenius. On considère alors $s_{\mathfrak{P}}$ l'élément de $D_{\mathfrak{P}}(\mathbb{L}/\mathbb{K})$ correspondant à ce générateur et il est caractérisé par la propriété suivante :

$$\forall c \in C,\ \ s_{\mathfrak{P}}(c) \equiv c^q\ [\mathfrak{P}].$$

Définition A.3 : Substitution de Frobenius de $\mathfrak{P}$:
On appelle **substitution de Frobenius de $\mathfrak{P}$** l'élément $s_{\mathfrak{P}}$.

Remarques :

* Cette substitution du Frobenius correspond à l'élément de Frobenius en $\mathfrak{P}$ dont nous avons parlé dans la partie précédente et il est unique car l'extension est non ramifiée.
* La définition de la substitution de Frobenius de $\mathfrak{P}$ montre que c'est un générateur du groupe de décomposition de $\mathfrak{P}$, son ordre est égal à $f_{\mathfrak{P}}$ et on le note souvent $(\mathfrak{P}, \mathbb{L}/\mathbb{K})$.

Proposition A.5 :
Soient $\mathbb{M}$ un sous-corps de $\mathbb{L}$ contenant $\mathbb{K}$ et $\mathfrak{P}_{\mathbb{M}} := \mathfrak{P} \cap \mathbb{M}$.

* On a $(\mathfrak{P}, \mathbb{L}/\mathbb{M}) = (\mathfrak{P}, \mathbb{L}/\mathbb{K})^f$ avec $f := \left[\overline{M} : \overline{K}\right]$;
* Si $\mathbb{M}$ est galoisienne sur $\mathbb{K}$, alors l'image de $(\mathfrak{P}, \mathbb{L}/\mathbb{K})$ dans $\mathrm{Gal}(\mathbb{M}/\mathbb{K})$ est égale à $(\mathfrak{P}_{\mathbb{M}}, \mathbb{M}/\mathbb{K})$.

Pour finir, remarquons que pour $\sigma \in \mathrm{Gal}(\mathbb{L}/\mathbb{K})$ on a (par transport de structure) la formule :

$$(\sigma(\mathfrak{P}), \mathbb{L}/\mathbb{K}) = \sigma(\mathfrak{P}, \mathbb{L}/\mathbb{K})\sigma^{-1}.$$

En particulier, si $\mathrm{Gal}(\mathbb{L}/\mathbb{K})$ est abélien, alors $(\mathfrak{P}, \mathbb{L}/\mathbb{K})$ ne dépend que de $\mathfrak{p}$ et on l'appelle **symbole d'Artin de $\mathfrak{p}$** et on le note $(\mathfrak{p}, \mathbb{L}/\mathbb{K})$. On définit par linéarité le symbole d'Artin de tout idéal $\mathfrak{a}$ de B ne contenant aucun idéal $\mathfrak{p}$ ramifié et on le note encore $(\mathfrak{a}, \mathbb{L}/\mathbb{K})$.

II Notion de groupe de Galois absolu

Nous pouvons désormais discuter du groupe de Galois absolu d'une extension de corps ainsi que de son sous-groupe d'inertie en utilisant les propriétés évoquées dans la partie I.

Dans toute cette partie, on considère $\mathbb{K}$ un corps local complet pour une place $\mathfrak{p}$ et on note k son corps résiduel.

Définition A.4 : Groupe de Galois absolu :
On appelle **groupe de Galois absolu** le groupe $\mathrm{Gal}_{\mathbb{K}} := \mathrm{Gal}\left(\mathbb{K}^{sep}/\mathbb{K}\right)$.

On remarquera que l'extension $\mathbb{K}^{sep}/\mathbb{K}$ est bien une extension galoisienne mais cependant elle n'est pas nécessairement finie. Ainsi, le groupe $\mathrm{Gal}_{\mathbb{K}}$ est potentiellement de cardinal infini mais ce n'est pas un obstacle insurmontable comme on le verra ci-dessous.

De même que dans le cas fini, on peut définir le sous-groupe de décomposition et d'inertie du groupe de Galois absolu. En effet, on peut définir le groupe de décomposition d'un idéal de manière similaire et l'application de réduction est surjective et appelle sous-groupe d'inertie son noyau.

Proposition A.6 :
On a l'isomorphisme suivant :

$$\mathrm{Gal}\left(\mathbb{K}^{sep}/\mathbb{K}\right) \cong \varprojlim_{\substack{\mathbb{L} \\ [\mathbb{L}:\mathbb{K}]<+\infty}} \mathrm{Gal}(\mathbb{L}/\mathbb{K}),$$

où la limite projective porte sur les corps intermédaires $\mathbb{L}$ contenus dans $\mathbb{K}^{sep}$ et contenant $\mathbb{K}$ tels que l'extension $\mathbb{L}/\mathbb{K}$ soit de degré fini.

On remarque alors que $\mathrm{Gal}\left(\mathbb{K}^{sep}/\mathbb{K}\right)$ est alors muni de la topologie profinie et qu'en particulier son sous-groupe d'inertie (noté simplement $I_{\mathfrak{p}}$) est fermé (car noyau d'une application continue).

En prenant la limite projective dans les suites exactes données en proposition A.4 on obtient la proposition suivante :

Proposition A.7 :

- On a l'isomorphisme :

$$I_{\mathfrak{p}} \cong \varprojlim_{\substack{\mathbb{L} \\ [\mathbb{L}:\mathbb{K}]<+\infty}} I_{\mathfrak{p}}(\mathbb{L}/\mathbb{K});$$

- On a la suite exacte courte :

$$0 \longrightarrow I_{\mathfrak{p}} \longrightarrow \mathrm{Gal}_{\mathbb{K}} \longrightarrow \mathrm{Gal}_k \longrightarrow 0.$$

Remarque :
De manière générale, on peut relever le morphisme de Frobenius du groupe de Galois absolu Gal_k en un élément du groupe de Galois absolu $\mathrm{Gal}_{\mathbb{K}}$ mais à un élément du groupe d'inertie près. Or, lorsque l'extension est non-ramifiée, le groupe d'inertie agit trivialement et il est alors possible de parler du morphisme de Frobenius dans $\mathrm{Gal}_{\mathbb{K}}$.

Bibliographie

[Bre16] Florian Breuer.
« Explicit Drinfeld moduli schemes and Abhyankar's generalized iteration conjecture ». English.
In : J. Number Theory 160 (2016), p. 432-450. ISSN : 0022-314X. DOI : 10.1016/j.jnt.2015.08.021.

[CG18] Philippe Caldero et Jérôme Germoni.
Nouvelles histoires hédonistes de groupes et de géométries. Tome 2. French. 2nd edition. T. 122.
Math. Devenir. Paris : Calvage et Mounet, 2018. ISBN : 978-2-9163-5267-1.

[Con] Keith Conrad. Galois groups of cubics ans quartics in all characteristics.
URL : https://kconrad.math.uconn.edu/blurbs/galoistheory/cubicquarticallchar.pdf.

[Ent21] Alexei Entin.
« Monodromy of hyperplane sections of curves and decomposition statistics over finite fields ». English.
In : Int. Math. Res. Not. 2021.14 (2021), p. 10409-10441. ISSN : 1073-7928.
DOI : 10.1093/imrn/rnz120.

[Gek08] Ernst-Ulrich Gekeler. « Frobenius distributions of Drinfeld modules over finite fields ». English.
In : Trans. Am. Math. Soc. 360.4 (2008), p. 1695-1721. ISSN : 0002-9947.
DOI : 10.1090/S0002-9947-07-04558-8.

[Gek16] Ernst-Ulrich Gekeler. « The Galois image of twisted Carlitz modules ». English.
In : J. Number Theory 163 (2016), p. 316-330. ISSN : 0022-314X. DOI : 10.1016/j.jnt.2015.11.021.

[Gos96] David Goss. Basic structures of function field arithmetic. English. T. 35.
Ergeb. Math. Grenzgeb., 3. Folge. Berlin : Springer, 1996. ISBN : 3-540-61087-1.

[Gro66] A. Grothendieck. « Éléments de géométrie algébrique. IV : Étude locale des schémas et des morphismes de schémas. (Troisième partie). Rédigé avec la colloboration de J. Dieudonné ». French.
In : Publ. Math., Inst. Hautes Étud. Sci. 28 (1966), p. 1-255. ISSN : 0073-8301.
DOI : 10.1007/BF02684343. URL : https://eudml.org/doc/103860.

[Ham93] Yoshinori Hamahata. « Tensor products of Drinfeld modules and v-adic representations ». English.
In : Manuscr. Math. 79.3-4 (1993), p. 307-327. ISSN : 0025-2611. DOI : 10.1007/BF02568348.
URL : https://eudml.org/doc/155844.

[Hay74] David R. Hayes. « Explicit class field theory for rational function fields ». English.
In : Trans. Am. Math. Soc. 189 (1974), p. 77-91. ISSN : 0002-9947. DOI : 10.2307/1996848.

[Jon10] Nathan Jones. « Almost all elliptic curves are Serre curves ». English.
In : Trans. Am. Math. Soc. 362.3 (2010), p. 1547-1570. ISSN : 0002-9947.
DOI : 10.1090/S0002-9947-09-04804-1.

[Pap23] Mihran Papikian. Drinfeld modules. English. T. 296. Grad. Texts Math. Cham : Springer, 2023.
ISBN : 978-3-031-19706-2 ; 978-3-031-19709-3 ; 978-3-031-19707-9. DOI : 10.1007/978-3-031-19707-9.

[PR09a] Richard Pink et Egon Rütsche.
« Adelic openness for Drinfeld modules in generic characteristic ». English.
In : J. Number Theory 129.4 (2009), p. 882-907. ISSN : 0022-314X. DOI : 10.1016/j.jnt.2008.12.002.

[PR09b] Richard Pink et Egon Rütsche.
« Image of the group ring of the Galois representation associated to Drinfeld modules ». English.
In : J. Number Theory 129.4 (2009), p. 866-881. ISSN : 0022-314X. DOI : 10.1016/j.jnt.2008.12.003.

[Rib76] Kenneth A. Ribet.
« Galois action on division points of Abelian varieties with real multiplications ». English.
In : Am. J. Math. 98 (1976), p. 751-804. ISSN : 0002-9327. DOI : 10.2307/2373815.

[Rob00] Alain M. Robert. A course in p-adic analysis. English. T. 198. Grad. Texts Math.
New York, NY : Springer, 2000. ISBN : 0-387-98669-3.

[Rom21] Jean-Étienne Rombaldi. Mathématiques pour l'agrégation. Algèbre et géométrie. French.
Deuxième édition. De Boeck Supérieur, 2021. ISBN : 978-2-80733220-1.

[Ros03] Michael Rosen. « Formal Drinfeld modules. » English. In : J. Number Theory 103.2 (2003), p. 234-256.
ISSN : 0022-314X. DOI : 10.1016/S0022-314X(03)00111-2.

[Ser04] Jean-Pierre Serre. Corps locaux. French. 4th corrected ed.
Paris : Hermann, Éditeurs des Sciences et des Arts, 2004. ISBN : 2-7056-1296-3.

[Ser72] Jean-Pierre Serre. « Galois properties of points of finite order of elliptic curves ». French.
In : Invent. Math. 15 (1972), p. 259-331. ISSN : 0020-9910. DOI : 10.1007/BF01405086.
URL : https://eudml.org/doc/142133.

[Ser03] Jean-Pierre Serre. « On a theorem of Jordan ». English.
In : Bull. Am. Math. Soc., New Ser. 40.4 (2003), p. 429-440. ISSN : 0273-0979.
DOI : 10.1090/S0273-0979-03-00992-3.

[Wil09] Robert A. Wilson. The finite simple groups. English. T. 251. Grad. Texts Math.
London : Springer, 2009. ISBN : 978-1-84800-987-5 ; 978-1-84800-988-2.
DOI : 10.1007/978-1-84800-988-2.

[Zyw25] David Zywina. Drinfeld modules with maximal Galois action. 2025. arXiv : 2502.01030 [math.NT].
URL : https://arxiv.org/abs/2502.01030.

[Zyw11] David Zywina. Drinfeld modules with maximal Galois action on their torsion points.
Preprint, arXiv :1110.4365 [math.NT] (2011). 2011. URL : https://arxiv.org/abs/1110.4365.