Les groupes p-divisibles

ERTL Veronika

20 janvier 2010

Table des matières

0 Introduction

Dans ce texte on s'intéresse à quelques énoncés sur les *groupes p-divisibles* dûs à J.T. TATE. L'objectif est de démontrer que, sur un anneau de valuation discrète dont le corps de fractions est de caractéristique 0, un groupe p-divisible G est déterminé par son *module de Tate* $T_p(G)$ où, ce qui revient au même, par sa *fibre générique* G_η. Plus généralement :

Théorème 0.1 *Soit X un schéma intègre, noethérien et normal, dont la fibre générique η est de caractéristique 0. Soient G et H deux groupes p-divisibles sur X. Un homomorphisme $f_\eta : G_\eta \to H_\eta$ s'étend de façon unique en un homomorphisme $f : G \to H$.*

Ce mémoire est constitué en quatre parties :

D'abord, on examine l'action du groupe de Galois $\mathrm{Gal}(\overline{K}/K)$ sur la complétion C de la clôture algébrique $\overline{K}$ d'un corps local K de caractéristique mixte $(0, p)$. Les résultats principaux de ce chapitre sont les Théorèmes (1.3.1) et (1.3.2) :

On a $\mathrm{H}^0(K, C) \cong K$, et $\mathrm{H}^1(K, C)$ est un K-espace vectoriel de dimension 1.

Soit $\chi : \mathrm{Gal}(\overline{K}/K) \to K^\times$ un homomorphisme continu et $C(\chi)$ le corps C muni de l'action de $\mathrm{Gal}(\overline{K}/K)$ tordue par χ : $s.x = \chi(\gamma)(\gamma x)$, pour $\gamma \in \mathrm{Gal}(\overline{K}/K)$ et $x \in X$. Soit K_∞ l'extension de K déterminée par $\mathrm{Ker}(\chi)$. Supposons qu'il existe une extension finie K_0/K contenue dans K_∞ telle que K_∞/K_0 soit totalement ramifiée et $\mathrm{Gal}(K_\infty/K_0) \cong \mathbb{Z}_p$. Alors, $\mathrm{H}^0(K, C(\chi)) = 0$ et $\mathrm{H}^1(K, C(\chi)) = 0$.

Dans la seconde partie, on introduit la notion de *schéma en groupes fini et localement libre* et on fait quelques rappelles sur la *dualité de Cartier*, les *suites exactes courtes* et les *groupes connexes et étales*.

Dans la troisième partie, on définit les *groupes p-divisibles*. En appliquant les résultats généraux de la partie précédente, on discute leur rapport aux *groupes de Lie formels* et on définit le *module de Tate* $T_p(G)$ et le *co-module de Tate* $\Phi_p(G)$.

La dernière partie utilise les théorèmes du début afin d'obtenir des informations sur le module de Tate. On en déduit une *décomposition de Hodge-Tate* (Corollaire (4.1.2)) :

Il existe un isomorphisme canonique de $\mathrm{Gal}(\overline{K}/K)$-modules

$$\mathrm{Hom}\left(T_p(G), C\right) \cong t_{G^D}(C) \oplus t_G^*(C) \otimes_C C(-1),$$

où t_{G^D} est l'espace tangent du dual de G et t_G^* l'espace co-tangent de G à l'origine.

Cela permet de démontrer le théorème susmentionné au cas où X est le spectre d'un anneau intégralement clos, noethérien et intègre (Théorème (4.2.1) et Corollaire (4.2.1)) :

Soit R un anneau intègre, intégralement clos et noethérien de corps de fractions K de caractéristique 0. Pour deux groupes p-divisibles G et H sur R l'application de restriction

$$\mathrm{Hom}_R(G, H) \to \mathrm{Hom}_K(G \otimes_R K, H \otimes_R K)$$

est un isomorphisme. Mutatis mutandis, l'application

$$\mathrm{Hom}_R(G, H) \to \mathrm{Hom}_{\mathrm{Gal}(\overline{K}/K)}\left(T_p(G), T_p(H)\right)$$

est un isomorphisme.

1 Calcul de cohomologie galoisienne

Soit R un anneau de valuation discrète, complet et de caractéristique 0 ; on note k son corps résiduel supposé parfait de caractéristique $p > 0$. En outre, on note K le corps des fractions de R, $\overline{K}$ une clôture algébrique et v la valuation normalisée de K. Cette valuation s'étend à $\overline{K}$ et on note C la complétion de $\overline{K}$ pour la topologie définie par v.
Le corps C est algébriquement clos et la valeur absolue de $\overline{K}$ s'étend à C par continuité. Si π est une uniformisante de K et $x \in C$ on peut définir la valeur absolue de x par

$$|x| = |\pi|^{v(x)}$$

et $e = v(p)$ l'indice de ramification absolu de K.
Si L est un sous-corps de C contenant K et $\mathfrak{I}$ un idéal fractionaire de L, on pose $v(\mathfrak{I}) = \min\{v(x)|x \in \mathfrak{I}\}$.

1.1 Quelques extensions totalement ramifiées

Soient K_∞ une extension galoisienne de K, totalement ramifiée de groupe de Galois $\Gamma \cong \mathbb{Z}_p$ et K_n le sous-corps de K_∞ correspondant au sous-groupe $\Gamma(n) = p^n\,\mathbb{Z}_p$. L'extension K_n/K est cyclique de degré p^n. Remarquons qu'une telle extension existe, par exemple l'extension cyclotomique. Pour tout $n \in \mathbb{N} \cup \{\infty\}$ on note R_n l'anneau des entiers de K_n et $\mathfrak{m}_n$ son idéal maximal.
La différente relative d'une extension M/L est notée $\mathfrak{D}_{M/L}$.

Proposition 1.1.1 *Il existe $c \in \mathbb{R}$ tel que la valuation de la différente de K_n/K soit*

$$v(\mathfrak{D}_{K_n/K}) = en + c + p^{-n}a_n$$

où la suite $(a_n)_{n\in\mathbb{N}}$ est bornée.

Démonstration : Si L/K est une extension finie (ce qui est le cas de K_n/K) on a d'après [13, Proposition 4, p.72] $v_L(\mathfrak{D}_{L/K}) = \sum_{i=0}^{i=\infty}(\#G_i - 1)$, et donc

$$v_K(\mathfrak{D}_{L/K}) = \frac{1}{e_{L/K}}\sum_{i=0}^{i=\infty}(\#G_i - 1) = \frac{1}{e_{L/K}}\int_{-1}^{\infty}(\#G_y - 1)\,\mathrm{d}y$$

où G_i sont les groupes de ramification de $\mathrm{Gal}(L/K)$ et $e_{L/K}$ est l'indice de ramification relative. Par passage à la numérotation supérieure $G^x = G_{\psi(x)}$, c'est-à-dire en réalisant un changement de variables $y = \psi x$, où ψ est l'application réciproque de $\phi(y) = \int_0^y \frac{dt}{[G_0:G_t]}$ (et alors $\psi(x) = \int_0^x \left(G^0 : G^t\right) dt$), on obtient, puisque $dy = \psi'(x)dx = \left(G^0 : G^x\right) dx$,

$$v_K(\mathfrak{D}_{L/K}) = \frac{1}{e_{L/K}}\int_{-1}^{\infty}\left(1 - \frac{1}{\#G^x}\right)\#G^0\mathrm{d}x.$$

Si L/K est totalement ramifiée $\#G^0 = e_{L/K}$ et la formule se simplifie en

$$v_K(\mathfrak{D}_{L/K}) = \int_{-1}^{\infty}\left(1 - \frac{1}{\#G^x}\right)\mathrm{d}x.$$

Dans le cas de l'extension K_n/K, la définition de la numérotation supérieure donne $\mathrm{Gal}(K_n/K)^x = \mathrm{Gal}(K_\infty/K)^x$. Notons alors v_n le n-ième nombre de ramification supérieure, c'est-à-dire, le n-ième entier tel que $\mathrm{Gal}(K_\infty/K)^{v_n} \neq \mathrm{Gal}(K_\infty/K)^{v_n+1}$. Supposons que l'on a déjà prouvé que

$v_{n+1} - v_n = e$ pour n assez grand, disons $n \geq n_0$. Pour $n > n_0$ on a alors

$$\begin{aligned} v(\mathfrak{D}_{K_n/K}) &= (v_1 - v_0)\left(1 - \frac{1}{p^n}\right) + (v_2 - v_1)\left(1 - \frac{1}{p^{n-1}}\right) + \cdots + (v_{n_0} - v_{n_0-1})\left(1 - \frac{1}{p^{n-n_0+1}}\right) \\ &\quad + e\left(\left(1 - \frac{1}{p^{n-n_0}}\right) + \left((1 - \frac{1}{p^{n-n_0-1}}\right) + \cdots + (1-1)\right) \\ &= v_{n_0} - v_0 + \left((v_1 - v_0)\frac{1}{p^n} + (v_2 - v_1)\frac{1}{p^{n-1}} + \cdots + (v_{n_0} - v_{n_0-1})\frac{1}{p^{n-n_0+1}}\right) + \\ &\quad + e(n - n_0) - e\left(1 + \frac{1}{p} + \cdots + \frac{1}{p^{n-n_0}}\right) \\ &= en + \underbrace{v_{n_0} - v_0 - en_0 - e\frac{p}{p-1}}_{c} + \\ &\quad + p^{-n}\underbrace{\left(e\frac{p^{n_0+2}}{p-1} + (v_1 - v_0) + \frac{1}{p}(v_2 - v_1) + \cdots + \frac{1}{p^{n_0+1}}(v_{n_0} - v_{n_0-1})\right)}_{a_n}. \end{aligned}$$

Pour $n \leq n_0$, on pose par contre $a_n = p^n\left(v(\mathfrak{D}_{K_n/K}) - en - c\right)$. □

Pour compléter, il reste à montrer

Lemme 1.1.1 *Pour n assez grand, on a $v_{n+1} - v_n = e$.*

Démonstration : Comme K_∞/K est totalement ramifiée, on peut supposer le corps résiduel k algébriquement clos, cas auquel on peut toujours réduire le cas d'un k parfait par passage à la complétion de l'extension maximale non ramifiée de K. Dans ce cas, Serre montra dans [14] que l'on a une théorie du corps de classes qui fonctionne exactement comme dans le cas d'un corps résiduel fini : si L/K est une extension abélienne (nécessairement totalement ramifiée), l'isomorphisme de réciprocité

$$\rho : K^\times/N_{L/K}L^\times \cong \mathcal{O}_K^\times/N_{L/K}\mathcal{O}_L^\times \to \mathrm{Gal}(L/K),$$

où $N_{L/K}$ est la norme, donne d'après [13, Corollaire 3, p.235] une correspondance entre la filtration donnée par les $1 + \mathfrak{m}_K^n$ et la filtration par la ramification supérieure du groupe de Galois. Dans notre cas, cela fournit un épimorphisme continu

$$\rho : \mathcal{O}_K^\times \to \mathbb{Z}_p = \Gamma\,.$$

On dispose aussi du logarithme

$$\log : 1 + \pi^m\mathcal{O}_K \xrightarrow{\sim} \pi^m\mathcal{O}_K$$

si $m > \frac{e}{p-1}$. Composé avec l'application exponentielle, ρ induit un morphisme surjectif de groupes additifs

$$\tilde{\rho} : \pi^m\mathcal{O}_K \to p^l\,\mathbb{Z}_p \qquad \text{pour} \quad l \in \mathbb{N}\,\text{convenable.}$$

Soit $n_0 \in \mathbb{N}_{>m+e}$ tel qu'il existe $\alpha \in \mathcal{O}_K^\times$ avec $\tilde{\rho}(\pi^{n_0}\alpha) \notin p^{l+1}\,\mathbb{Z}_p$; alors $\tilde{\rho}(\pi^{n_0+j}\mathcal{O}_K) = p^{l+1}\,\mathbb{Z}_p$ pour $j \in \{1, 2, \ldots, e\}$ car avec $\pi^e = pu$, $u \in \mathcal{O}_K^\times$ on a

$$\tilde{\rho}(\pi^{n_0+j}) = \tilde{\rho}(pu\pi^{n_0+j-e}) \in p^{l+1}\,\mathbb{Z}_p$$

(ce qui a du sens, parce que $n_0 \geq m + e - 1$) mais

$$\tilde{\rho}(\pi^{n_0+e}\alpha) = \underbrace{\tilde{\rho}(\pi^{n_0}\alpha)}_{\notin p^{l+1}\,\mathbb{Z}_p}\underbrace{\tilde{\rho}(pu)}_{\in p\,\mathbb{Z}_p^\times} \notin p^{l+2}\,\mathbb{Z}_p\,.$$

Par récurrence, on obtient finalement

$$\tilde{\rho}(\pi^{n_0+j}\mathcal{O}_K) = p^i\,\mathbb{Z}_p$$

pour $j \in \{e(i-1)+1, e(i-1)+2, \ldots, ei\}$: on voit bien que les sauts de la ramification supérieure vérifient $v_n - v_{n-1} = e$ pour $n > n_0$. □

De cette proposition, on tire les corollaires suivants :

Corollaire 1.1.1 *$v(\mathfrak{D}_{K_{n+1}/K_n}) = e + p^{-n}b_n$ où $(b_n)_{n\in\mathbb{N}}$ est bornée.*

DÉMONSTRATION : On a $\mathfrak{D}_{K_{n+1}/K} = \mathfrak{D}_{K_{n+1}/K_n}.\mathfrak{D}_{K_n/K}$ d'où $v(\mathfrak{D}_{K_{n+1}/K_n}) = v(\mathfrak{D}_{K_{n+1}/K}) - v(\mathfrak{D}_{K_n/K})$. Donc $b_n = p^{-1}a_{n+1} - a_n$ est borné. □

Corollaire 1.1.2 *Il existe $a \in \mathbb{R}$ indépendant de n tel que pour tout $x \in K_{n+1}$ on a*

$$|\operatorname{Tr}_{K_{n+1}/K_n}(x)| \leq |p|^{1-ap^{-n}}|x|.$$

DÉMONSTRATION : Rappelons que $\mathfrak{m}_n$ désigne l'idéal maximal de l'anneau des entiers R_N de K_n. On a $\mathfrak{D}_{K_{n+1}/K_n} = \mathfrak{m}^d{}_{n+1}$ [13, V,§3, Lemme 3] avec $d = v_{K_{n+1}}(\mathfrak{D}_{K_{n+1}/K_n})$. Par conséquent, pour tout entier $i \geq 0$ on a

$$\operatorname{Tr}_{K_{n+1}/K_n}(\mathfrak{m}_{n+1}^i) = \mathfrak{m}^j{}_n,$$

avec $j = \left\lfloor \frac{i+d}{p} \right\rfloor$ [13, V, §3, Lemme 4]. En particulier pour $x \in \mathfrak{m}_{n+1}^i$, c'est-à-dire $i = v_{K_{n+1}}(x)$, on a

$$\begin{aligned}
v_{K_{n+1}}(\operatorname{Tr}_{K_{n+1}/K_n}(x)) &\geq p\left\lfloor \frac{i+d}{p} \right\rfloor \geq p\left(\frac{i+d}{p} - 1\right)\\
v_{K_{n+1}}(\operatorname{Tr}_{K_{n+1}/K_n}(x)) &\geq v_{K_{n+1}}(x) + d - p\\
p^{n+1}v(\operatorname{Tr}_{K_{n+1}/K_n}(x)) &\geq p^{n+1}v(x) + p^{n+1}v(\mathfrak{D}_{K_{n+1}/K_n}) - p\\
v(\operatorname{Tr}_{K_{n+1}/K_n}(x)) &\geq v(x) + \left(e + p^{-n}(b_n - 1)\right)
\end{aligned}$$

d'après le corollaire précédent. Comme la suite $(b_n)_{n\in\mathbb{N}}$ est bornée, on peut poser $a := -\frac{\inf_{n\in\mathbb{N}}(b_n-1)}{e}$ ce qui est indépendant de n et donne

$$\begin{aligned}
v(\operatorname{Tr}_{K_{n+1}/K_n}(x)) &\geq v(x) + e(1 - p^{-n}a)\\
|\operatorname{Tr}_{K_{n+1}/K_n}(x)| &\leq |p|^{1-ap^{-n}}|x|.
\end{aligned}$$

Quod erat demonstrandum. □

Corollaire 1.1.3 *Il existe $c \in \mathbb{R}$ indépendant de n tel que pour $x \in K_n$*

$$|\operatorname{Tr}_{K_n/K}(x)| \leq |p|^{n-c}|x|.$$

DÉMONSTRATION : Cela résulte immédiatement du Corollaire 2. En effet, on a $\operatorname{Tr}_{K_n/K} = \operatorname{Tr}_{K_1/K} \circ \operatorname{Tr}_{K_2/K_1} \circ \cdots \circ \operatorname{Tr}_{K_n/K_{n-1}}$ donc

$$\begin{aligned}
|\operatorname{Tr}_{K_n/K}(x)| &\leq |p|^{(1-a)+(1-ap^{-1})+\cdots+(1-ap^{-n+1})}|x|\\
&= |p|^{n-a(1+\cdots+p^{-n+1})}|x| \leq |p|^{n-c}|x|,
\end{aligned}$$

et l'énoncé est prouvé. □

On notera σ un générateur topologique du groupe Γ.

Lemme 1.1.2 *Il existe $c > 0$ indépendante de n telle que pour $x \in K_{n+1}$*

$$|x - p^{-1}\operatorname{Tr}_{K_{n+1}/Kn}(x)| \leq c|\sigma^{p^n}x - x|.$$

DÉMONSTRATION : Soit $\tau = \sigma^{p^n}$. Il définit un générateur de $\mathrm{Gal}(K_{n+1}/K_n)$. La trace de $x \in K_{n+1}$ sur K_n est alors donnée par $\operatorname{Tr}_{K_{n+1}/K_n}(x) = \sum_{i=0}^{p-1}\tau^i x$. Alors,

$$\begin{aligned}
px - \operatorname{Tr}_{K_{n+1}/K_n}(x) &= px - \sum_{i=0}^{p-1}\tau^i x = \sum_{i=0}^{p-1}(1-\tau^i)x\\
&= \sum_{i=1}^{p-1}\left(1 + \tau + \cdots + \tau^{i-1}\right)(1-\tau)x.
\end{aligned}$$

Puisque la valeur absolue $|\cdot|$ est ultramétrique l'égalité précédente donne

$$|px - \mathrm{Tr}_{K_{n+1}/K_n}(x)| \leq \max_{i=0}^{p-1} |\tau^i(1-\tau)x| = |(1-\tau)x|,$$

ce qui montre l'énoncé avec $c = p^{-1}$. □

On définit une fonction K-linéaire sur K_∞ à valeurs dans K notée t_K comme suit : pour $x \in K_n$ posons

$$t_K(x) = p^{-n} \mathrm{Tr}_{K_n/K}(x),$$

ce qui ne dépend pas du choix de n et définit un projecteur du K-espace vectoriel K_∞ sur son sous-K-espace vectoriel K.

Proposition 1.1.2 *Il existe une constante $d > 0$ telle que pour tout $x \in K_\infty$*

$$|x - t_K(x)| \leq d|\sigma x - x|.$$

DÉMONSTRATION : La preuve s'effectue par récurrence sur n. On va montrer l'inégalité

$$|x - t_K(x)| \leq c_n|\sigma x - x|$$

pour $x \in K_n$, avec

$$c_{n+1} = |p|^{-ap^{-n}} c_n,$$

où $a > 0$ est la constante du Corollaire 1.1.2.
Remarquons que la suite $(c_n)_{n\in\mathbb{N}}$ est croissante et bornée : on a

$$c_n = |p|^{-a(\sum_{i=1}^{n-1} p^{-i})} c_1 = \alpha^{a(\sum_{i=1}^{n-1} \frac{1}{p^i})} c_1 < \alpha^{a(\sum_{i=1}^{n} \frac{1}{p^i})} c_1 = c_{n+1} < \alpha^{a\frac{1}{1-\frac{1}{p}}} c_1$$

avec $\alpha > 1$. Donc, $d = |p|^{-a\frac{1}{1-\frac{1}{p}}} c_1$ donne alors le résultat voulu.
Pour $n = 1$ l'énoncé est fourni par le Lemme 1.1.2 et on prend c_1 égal au c de ce lemme. En supposant que l'énoncé est vrai pour n on a pour $x \in K_{n+1}$

$$\begin{aligned}
|\mathrm{Tr}_{K_{n+1}/K_n}(x) - pt_K(x)| &= |\mathrm{Tr}_{K_{n+1}/K_n}(x) - p \cdot p^{-(n+1)} \mathrm{Tr}_{K_{n+1}/K}(x)| \\
&= |\mathrm{Tr}_{K_{n+1}/K_n}(x) - p \cdot p^{-(n+1)} \mathrm{Tr}_{K_n/K} \mathrm{Tr}_{K_{n+1}/K_n}(x)| \\
&= |\mathrm{Tr}_{K_{n+1}/K_n}(x) - p^{-n} \mathrm{Tr}_{K_n/K} \mathrm{Tr}_{K_{n+1}/K_n}(x)| \\
&= |\mathrm{Tr}_{K_{n+1}/K_n}(x) - t_K(\mathrm{Tr}_{K_{n+1}/K_n}(x))| \\
&\leq c_n|\sigma \mathrm{Tr}_{K_{n+1}/K_n}(x) - \mathrm{Tr}_{K_{n+1}/K_n}(x)| \\
&= c_n|\mathrm{Tr}_{K_{n+1}/K_n}(\sigma x - x)| \\
&\leq c_n|p|^{1-ap^{-n}}|\sigma x - x|,
\end{aligned}$$

d'après le Corollaire 1.1.2 de la Proposition 1.1.1. En appliquant le Lemme 1.1.2 on obtient

$$\begin{aligned}
|x - t_K(x)| &= |\left(x - p^{-1}\mathrm{Tr}_{K_{n+1}/K_n}(x)\right) + \left(p^{-1}\mathrm{Tr}_{K_{n+1}/K_n}(x) - t_K(x)\right)| \\
&\leq \max\left(|(x - p^{-1}\mathrm{Tr}_{K_{n+1}/K_n}(x)|, |p|^{-ap^{-n}} c_n|\sigma x - x|\right) \\
&\leq \max\left(c_1|\sigma^{p^n} x - x|, |p|^{-ap^{-n}} c_n|\sigma x - x|\right) \\
&\leq \max(c_1, c_{n+1})\,|\sigma x - x| \\
&= c_{n+1}|\sigma x - x|,
\end{aligned}$$

et la récurrence complète donne l'énoncé. □

Remarque 1.1.1 La démonstration montre qu'en remplaçant K par K_n on obtient une inégalité correspondante avec *la même constante* d (car a est indépendant de n).

Soit maintenant X la complétion de K_∞ pour la topologie définie par la valuation v. C'est un espace de Banach sur lequel l'action de Γ est continue. On étudiera le Γ-espace X.

D'après la Proposition 1.1.2 l'opérateur t_K agit de façon continue sur K_∞ et s'étend par conséquent par continuité à X. Comme K est complet, on voit que $t_K(X) = K$ et que $X_0 := \mathrm{Ker}(t_K)$ est un sous-espace fermé de X.

Proposition 1.1.3 (a) *X est la somme directe de K et X_0.*
(b) *L'opérateur $\sigma - 1$ annule K tout en étant bijectif d'inverse continu sur X_0.*
(c) *Si $\lambda \in K^\times$ est congru à 1 modulo π et n'est pas une racine de l'unité, alors $\sigma - \lambda$ est bijectif d'inverse continu sur X.*

Démonstration : (a) Comme t_K est idempotent (c'est une projection), X est la somme directe de son noyau et son image :

$$X = K \oplus X_0.$$

(b) Pour tout n on pose

$$K_{n,0} = K_n \cap X_0$$

le sous-espace de K_n sur lequel la trace à K s'annule et on note $K_{\infty,0}$ leur réunion. Comme dans (a) on a

$$K_n = K \oplus K_{n,0} \qquad \text{pour} \quad n \in \mathbb{N} \cup \{\infty\},$$

et X_0 est par définition l'adhérence de $K_{\infty,0}$ dans X. Comme $\sigma - 1$ est injectif sur chacun des K-espaces vectoriels de dimension finie $K_{n,0}$, il est bijectif sur chacun d'eux, de même que sur leur réunion $K_{\infty,0}$. Si ϱ est son inverse, alors pour tout $y = (\sigma - 1)x \in K_{\infty,0}$, on a (d'après la Proposition 1.1.2)

$$|\varrho y - t_K(\varrho y)| = |\varrho y| \leq d|y|,$$

puisque $t_K(\varrho y) = 0$. En conséquence, ϱ s'étend par continuité à X_0 ce qui donne l'inverse continu voulu de $\sigma - 1$ sur X_0.
(c) On peut supposer que

$$|\lambda - 1|d < 1,$$

avec la constante d de (b). En effet, il existe toujours $n \in \mathbb{N}$ tel que $|\lambda^{p^n} - 1| < 1$. Comme d ne dépend pas de n et comme $\sigma - \lambda$ divise $\sigma^{p^n} - \lambda^{p^n}$, il suffit de remplacer K par K_n, σ par σ^{p^n} et λ par λ^{p^n} (ce qui est possible puisque par hypothèse $\lambda^{p^n} \neq 1$). Sur K, $\sigma - \lambda$ est bijectif car $1 - \lambda \neq 0$, λ n'étant pas une racine de l'unité. Et donc par (a) il suffit d'étudier son action sur X_0. On a l'équation d'opérateurs suivante

$$\varrho(\sigma - \lambda) = \varrho\left((\sigma - 1) - (\lambda - 1)\right) = 1 - (\lambda - 1)\varrho. \tag{1}$$

On obtient alors

$$|(\lambda - 1)\varrho y| \leq |\lambda - 1|d|y| < |y| \qquad \text{pour tout} \quad y \in X_0$$

ce qui montre que $1-(\lambda-1)\varrho$ est un automorphisme de X_0 dont l'inverse est une série géométrique. Alors, l'équation (1) implique que $\sigma - \lambda$ est continûment inversible sur X_0. □

On rappelle la définition des groupes de cohomologies continues. Soient G un groupe topologique, M un groupe topologique abélien muni d'une action additive et continue de G. Pour $n \in \mathbb{N}$, soit $C^n(G, M)$ le groupe de n-cochaînes continues de G à valeurs dans M, c'est-à-dire le groupe des fonctions continues sur G^n à valeurs dans M. De plus, on définit les opérateurs de bord $d_n : C^n(G, M) \to C^{n+1}(G, M)$ par les formules habituelles (voir [4, 1.1, p.10] et [13, VII, §2]). On obtient ainsi un complexe de groupes abéliens. On pose $\mathrm{Z}^n(G, M) = \mathrm{Ker}(d_n)$ le groupe de n-cocycles continus de G à valeurs dans M, $\mathrm{B}^n(G, M) = \mathrm{Im}(d_{n-1})$ si $n > 0$, respectivement $\mathrm{B}^0(H, M) = 0$, le groupe des n-cobords et finalement le $n^{\text{ième}}$ groupe de cohomologie continue, $\mathrm{H}^n(G, M) = \mathrm{Z}^n(G, M)/\mathrm{B}^n(G, M)$.
On a par exemple, $\mathrm{H}^0(G, M) = M^G$, car si $a \in M = C^0(G, M)$ et $\gamma \in G$, on a $d_0 a(\gamma) = (\gamma - 1)a$. En outre, $\mathrm{Z}^1(G, M) \cong \{f : G \to M \text{ continu } | f(gh) = f(g) + g \cdot f(h)\}$ et $\mathrm{B}^1(G, M) \cong \{f : G \to M \text{ continu } | \exists m \in M : f(g) = g(m) - m\}$, ce qui implique si G agit trivialement sur M on a $\mathrm{H}^1(G, M) = \mathrm{Hom}_{cont}(G, M)$.

Soit χ un caractère continu de Γ vers le groupe $K^\times$, alors on note $X(\chi)$ l'espace X muni de l'action tordue de Γ :

$$\gamma.x = \chi(\gamma)(\gamma x), \qquad \text{pour} \quad \gamma \in \Gamma, x \in X.$$

On étudie les groupes de cohomologie continue $\mathrm{H}^i(\Gamma, X)$ et $\mathrm{H}^i(\Gamma, X(\chi))$ pour les topologies canoniques de Γ et X.

On a alors

Proposition 1.1.4 (a) *$H^0(\Gamma, X) = K$, et $H^1(\Gamma, X)$ est un K-espace vectoriel de dimension* 1. (b) *Si $\chi(\Gamma)$ est infini, alors $H^0(\Gamma, X(\chi)) = H^1(\Gamma, X(\chi)) = 0$*

Démonstration : Soit, σ un générateur topologique de Γ et pour un caractère quelconque de Γ, soit $\lambda := \chi(\sigma^{-1})$. Si Y est un sous-espace fermé de X stable sous l'action de Γ, alors $\mathrm{H}^0(\Gamma, Y(\chi))$ est le noyau de $\sigma - \lambda$ sur Y. En effet, un élément y est dans $\mathrm{H}^0(\Gamma, Y(\chi))$ si et seulement si

$$y = \gamma.y = \chi(\gamma)(\gamma y) \qquad \text{pour tout} \qquad \gamma \in \Gamma\,.$$

Mais comme σ est un générateur topologique, c'est le cas si et seulement si

$$y = \sigma.y = \chi(\sigma)(\sigma y) = \lambda^{-1}\sigma(y),$$

c'est-à-dire,

$$(\sigma - \lambda)y = 0.$$

Par contre, $\mathrm{H}^1(\Gamma, Y(\chi))$ est un sous-groupe de conoyau de $\sigma - \lambda$ sur Y. En effet, comme un 1-cocycle est évidemment déterminé par sa valeur à σ, on a un plongement de $\mathrm{Z}^1(\Gamma, Y(\chi))$ dans Y :

$$f \mapsto f(\sigma),$$

et un élément f est dans $\mathrm{B}^1(\Gamma, Y(\chi))$ si et seulement s'il existe $y_0 \in Y$ tel que

$$f(\sigma) = \sigma(y_0) - \lambda(y_0).$$

En particulier, les deux groupes de cohomologie sont triviaux si $\sigma - \lambda$ est bijectif sur Y. Si χ est trivial, on a $\lambda = 1$ et $Y(\chi) = X_0$: la partie (b) de la Proposition 1.1.3 montre alors que $\mathrm{H}^0(\Gamma, X_0)$ et $\mathrm{H}^1(\Gamma, X_0)$ sont nuls. Par conséquent, l'égalité $X = K \oplus X_0$ de la partie (a) de la Proposition 1.1.3 implique

$$\mathrm{H}^0(\Gamma, X) = \mathrm{H}^0(\Gamma, K) = K \qquad \text{et}$$
$$\mathrm{H}^1(\Gamma, X) = \mathrm{H}^1(\Gamma, K) = \mathrm{Hom}(\Gamma, K)$$

un espace vectoriel de dimension 1 sur K.
Si $\chi(\Gamma)$ est infini, alors $\lambda = \chi(\sigma)$ n'est pas une racine de l'unité, puisque σ est un générateur topologique. On peut également supposer qu'il est congru à 1 car il existe un entier n tesl que $\chi(\sigma^{-p^n}) = \lambda^{p^n} \equiv 1 \mathrm{mod}\pi$ grâce à la continuité de l'action et si $\sigma^{p^n} - \lambda^{p^n}$ est bijectif $\sigma - \lambda$ l'est aussi. Donc, on peut appliquer la partie (c) de la proposition précédente, ce qui nous montre que $\sigma - \lambda$ est bijectif sur X et que $\mathrm{H}^0(\Gamma, X(\chi))$ et $\mathrm{H}^1(\Gamma, X(\chi))$ s'annulent. □

1.2 Des extensions finies de K_∞

On conserve les notations du paragraphe précédent, et on note L une extension finie de K_∞, $\mathcal{O}_L$ son anneau d'entiers et $\mathfrak{m}_L$ son idéal maximal ($\mathcal{O}_\infty$ et $\mathfrak{m}$ ont la même signification pour K_∞). Soit $\mathcal{H} = \mathrm{Gal}(\overline{K}/K_\infty)$.

Proposition 1.2.1 *On a $\mathrm{Tr}_{L/K_\infty}(\mathcal{O}_L) \supset \mathfrak{m}_\infty$.*

Démonstration : On peut d'abord supposer L/K_∞ galoisienne, car si L'/L est une extension finie, et si l'énoncé est vrai pour L'/K_∞, alors, par transitivité de la trace, il l'est pour L/K_∞. Il existe un entier n_0 et une extension finie galoisienne F/K_{n_0} telle que $L \simeq F \otimes_{K_{n_0}} K_\infty$: quitte à remplacer K par K_{n_0}, on peut supposer que $n_0 = 0$ et $L = FK_\infty$ avec F et K_∞ linéairement disjoints sur K. En particulier, on a $\mathrm{Gal}(F_n/K) \simeq \mathrm{Gal}(F/K) \times \mathrm{Gal}(K_n/K)$ pour tout $n \in \mathbb{N}$.

En posant $F_n = FK_n$, pour $n \in \mathbb{N} \cup \{\infty\}$, on a $F_\infty = L$.
Comme l'extension F/K est finie, il existe $h \in \mathbb{N}$ tel que $\mathrm{Gal}(F/K)^v = \{1\}$ pour tout $v \geq h$. Mais par ailleurs, on a

$$\mathrm{Gal}(F/K)^v = \mathrm{Gal}(F_n/K)^v / \left(\mathrm{Gal}(F_n/K)^v \cap \mathrm{Gal}(K_n/K)\right)$$

(parce que la numérotation supérieure passe au quotient). On a donc $\mathrm{Gal}(F_n/K)^v \subseteq \mathrm{Gal}(K_n/K)$, soit encore $\mathrm{Gal}(F_n/K)^v \cap \mathrm{Gal}(F/K) = \{1\}$ pour $v \geq h$. On a alors

$$\mathrm{Gal}(K_n/K)^v = \mathrm{Gal}(F_n/K)^v / \left(\mathrm{Gal}(F_n/K)^v \cap \mathrm{Gal}(F/K)\right) = \mathrm{Gal}(F_n/K)^v$$

pour tout $v \geq h$. Par conséquent,

$$\begin{aligned} v(\mathfrak{D}_{F_n/K_n}) &= v(\mathfrak{D}_{F_n/K}) - v(\mathfrak{D}_{K_n/K}) \\ &= \int_{-1}^{\infty} \left(\frac{1}{\#(\mathrm{Gal}(K_n/K)^v} - \frac{1}{\#(\mathrm{Gal}(F_n/K)^v} \right) \mathrm{d}v \\ &= \int_{-1}^{h} \left(\frac{1}{\#(\mathrm{Gal}(K_n/K)^v)} - \frac{1}{\#(\mathrm{Gal}(F_n/K)^v)} \right) \mathrm{d}v \\ &\leq \int_{-1}^{h} \frac{\mathrm{d}v}{\#(\mathrm{Gal}(K_n/K)^v)} \end{aligned}$$

Mais si les sauts de la filtration de $\mathrm{Gal}(K_\infty/K)^v$ sont $v_0 = -1 < v_1 < v_2 < \cdots < v_N \leq h < v_{N+1} < \cdots$, on a

$$\int_{-1}^{h} \frac{\mathrm{d}v}{\#(\mathrm{Gal}(K_n/K)^v)} = \frac{t_1 - t_0}{p^n} + \frac{t_2 - t_1}{p^{n-1}} + \cdots + \frac{h - t_N}{p^{n-N}} \leq \frac{(h+1)p^N}{p^n}$$

de sorte qu'on a bien $v(\mathfrak{D}_{F_n/K_n}) = p^{-n}\alpha_n$ où $(\alpha_n)_{n\in\mathbb{N}}$ est une suite bornée.
Soit $x \in \mathfrak{m}_{K_\infty}$. Il existe $m \in \mathbb{N}$ tel que $x \in K_m$. Si $n \geq m$, on peut écrire $xR_n = \mathfrak{m}_n^{j_n}$, avec $\lim\limits_{n\to\infty} j_n = \infty$ vu que K_∞/K est totalement ramifiée. Mais on sait ([13, p.91, Lemme 4]) que $\mathrm{Tr}_{F_n/K_n}(\mathfrak{m}_{F_n}^i) = \mathfrak{m}_n^j$ avec $j = \left\lfloor \frac{i + v_{F_n}(v(\mathfrak{D}_{F_n/K_n}))}{e_{F_n/K_n}} \right\rfloor$. Avec $i = 0$, cela donne

$$\mathrm{Tr}_{F_n/K_n}(\mathcal{O}_{F_n}) = \mathfrak{m}_n^j$$

avec $j \leq \left\lfloor v_{K_n}(v(\mathfrak{D}_{F_n/K_n}) \right\rfloor \leq \alpha_n + 1$. Comme $(\alpha_n)_{n\in\mathbb{N}}$ est bornée et $\lim\limits_{n\to\infty} j_n = \infty$, il existe $n \geq m$ tel que $j_n > \alpha_n + 1$. On a alors $x \in \mathrm{Tr}_{F_n/K_n}(\mathcal{O}_{F_n})$. □

Corollaire 1.2.1 *Soient L/K_∞ une extension finie galoisienne de groupe de Galois G et f une r-cochaîne de G à valeurs dans L, avec $r \geq 0$, et $c > 1$. Alors, il existe une $(r-1)$-cochaîne g de G dans L telle que*

$$|f - \delta g| \leq c|\delta f| \qquad \text{et} \qquad |g| \leq c|f|.$$

Remarque 1.2.1 Ici, $|f|$ signifie le maximum des valeurs absolues des valeurs de f. Une (-1)-cochaîne est un élément y de L et le cobord δy d'un tel y est la 0-cochaîne $\mathrm{Tr}_{L/K_\infty}(y)$.

Démonstration du Corollaire : En appliquant la proposition précédente, on trouve une (-1)-cochaîne $y \in L$ tel que $|y| \leq 1$ et $|\delta y| > c^{-1}$ (si on prend $y \in \mathcal{O}_L$ avec $\delta y = \mathrm{Tr}_{L/K_\infty}(y) \in \mathfrak{m}_\infty$ et $v(\delta y)$ assez petit, alors $v(y) \geq 0$ et $v(\delta y) > 0$, c'est-à-dire $|y| \leq 1$ et $c^{-1} < |\delta y| < 1$). On définit une $(r-1)$-cochaîne $y \cup f$ comme suit :

$$y \cup f = yf, \qquad \text{si} \qquad r = 0$$

$$(y \cup f)(s_1, \ldots, s_{r-1}) = (-1)^r \sum_{s_r \in G} s_1 s_2 \cdots s_r y \cdot f(s_1, s_2, \ldots, s_r), \qquad \text{si} \qquad r > 0.$$

On vérifie l'identité

$$(\delta y) f - \delta(y \cup f) = y \cup (\delta f),$$

dans laquelle on peut diviser par l'élément δy :

$$f - \delta g = (\delta y)^{-1}(y \cup \delta f), \qquad \text{avec} \qquad g = (\delta y)^{-1}(y \cup f).$$

Comme $|y| \leq 1$, $|(\delta y)^{-1}| < c$ et $|y \cup f| \leq |y|.|f|$, on a $|f - \delta g| \leq c|\delta f|$ et $|g| \leq c|f|$ comme exigé. □

Corollaire 1.2.2 *Le Corollaire 1.2.1 est encore valable si l'on remplace L par $\overline{K}$, G par $\mathcal{H}$ et si l'on considère des cochaînes continues par rapport à la topologie de Krull sur G et la topologie discrète sur $\overline{K}$ (pour $r = 0$ il faut alors remplacer la conclusion par : « il existe un élément $x \in K_\infty$ tel que $|f - x| \leq c|\delta f|$ »).*

Démonstration : Cet énoncé résulte du Corollaire 1.2.1, car une cochaîne continue de $\mathcal{H}$ à valeur dans $\overline{K}$ est induite par inflation d'une certaine extension finie galoisienne L/K (voir [15, Proposition 8]). □

Si on passe à la complétion C de $\overline{K}$, le groupe $\mathrm{H}^r(\mathcal{H}, C)$ est construit avec les cochaînes standard continues par rapport à la topologie de Krull sur $\mathcal{H}$ et la topologie de la valuation sur C.

Proposition 1.2.2 *On a $\mathrm{H}^0(\mathcal{H}, C) = X$ et $\mathrm{H}^r(\mathcal{H}, C) = 0$ pour $r > 0$.*

Démonstration : Supposons que l'on a la propriété suivante :

(∗) Pour toute cochaîne f sur H à valeurs dans C et pour tout $\epsilon > 0$, il existe une cochaîne h sur $\mathcal{H}$ à valeur dans $\overline{K}$ telle que $|f - h| < \epsilon$.

Soit f un cocycle sur $\mathcal{H}$ à valeurs dans C. Si $r = 0$, f est dans la complétion X de K_∞ d'après le Corollaire 1.2.2. Si $r > 0$, construisons par récurrence une suite de $(r-1)$-cochaînes $(g_\nu) \in C^{r-1}(\mathcal{H}, \overline{K})$ telle que

$$|g_{\nu+1} - g_\nu| \leq \frac{c^2}{2^\nu} \qquad \text{et} \qquad |f - \delta g_\nu| \leq \frac{c}{2^\nu} \qquad \text{pour tout} \quad \nu \in \mathbb{N}$$

avec une constante c convenable. Supposons $g_0, g_1, \ldots, g_\nu$ construites. On applique la propriété $(*)$ à $f - \delta g_\nu$ et $\epsilon = \frac{1}{2^{\nu+1}}$: il existe $h_\nu \in C^r(\mathcal{H}, \overline{K})$ telle que $|f - \delta g_\nu - h_\nu| < \frac{1}{2^{\nu+1}}$. D'après le Corollaire 1.2.2, il existe $\widetilde{g}_\nu \in C^{r-1}(\mathcal{H}, \overline{K})$ telle que $|h_\nu - \delta\widetilde{g}_\nu| < c|\delta h_\nu|$ et $|\widetilde{g}_\nu| \leq c|h_\nu|$. Posant maintenant $g_{\nu+1} := g_\nu + \widetilde{g}_\nu$, on a :

$$\begin{aligned} |f - \delta g_{\nu+1}| &= |f - \delta(g_\nu + \widetilde{g}_\nu)| \\ &= |f - \delta g_\nu - h_\nu + h_\nu - \delta\widetilde{g}_\nu| \\ &\leq \max\left(\underbrace{|f - \delta g_\nu - h_\nu|}_{<1/2^{\nu+1}}, \underbrace{|h_\nu - \delta\widetilde{g}_\nu|}_{<c|\delta h_\nu|} \right) < \frac{c}{2^{\nu+1}} \end{aligned}$$

(car $|\delta h_n u| = |\delta(\underbrace{h_\nu - (f - \delta g_\nu)}_{<1/2^{\nu+1}} + \underbrace{\delta f}_{=0 \text{ par hypothèse}} - \underbrace{\delta\delta g_\nu}_{0})| < \frac{1}{2^{\nu+1}}$). En plus, on a : $|g_{\nu+1} - g_\nu| = |\widetilde{g}_\nu| \leq c|h_\nu| = c|\underbrace{h_\nu - (f - \delta g_\nu)}_{<1/2^{\nu+1}} + \underbrace{f - \delta g_\nu}_{<c/2^\nu}| \leq \frac{c^2}{2^\nu}$. Après avoir construit cette suite convergente, on peut poser $g := \lim_{\nu\to\infty} g_\nu \in C^{r-1}(\mathcal{H}, C)$. Per constructionem, on a $|f - \delta g| = 0$ et donc effectivement $\mathrm{H}^r(\mathcal{H}, C) = 0$.

Il reste à prouver la propriété $(*)$. Remarquons que $C = \overline{K} + \pi^\nu \mathcal{O}_C$ pour tout $\nu \in \mathbb{N}$. Il existe donc des applications $\phi_\nu : C/\pi^\nu\mathcal{O}_C \to \overline{K}$ telles que $\psi_\nu\phi_\nu = \mathrm{id}_{C/\pi^\nu\mathcal{O}_C}$, où $\psi_\nu : C \to C/\pi^\nu\mathcal{O}_C$ est la projection canonique. Puisque $C/\pi^\nu\mathcal{O}_C$ est muni de la topologie discrète et ψ_ν continue, ϕ_ν l'est également. On pose maintenant

$$f_\nu = \phi_\nu\psi_\nu f : \mathcal{H}^r \to C \to C/\pi^\nu\mathcal{O}_C \to \overline{K},$$

ce qui définit bien une cochaîne continue de $\mathcal{H}$ à valeurs dans $\overline{K}$. Comme f et f_ν ont même image par la projection sur $C/\pi^\nu\mathcal{O}_C$ (en effet, $\psi_\nu f_\nu = \psi_\nu\phi_\nu\psi_\nu f = \psi_\nu f$), leurs valeurs ne diffèrent que par des éléments dans $\pi^\nu\mathcal{O}_C$ et cela implique

$$|f_\nu - f| \leq |\pi|^\nu \underset{\nu\to\infty}{\longrightarrow} 0$$

et on a fini. □

Maintenant, on est en mesure de démontrer les résultats principaux de ce chapitre.

1.3 L'action de $\mathrm{Gal}(\overline{K}/K)$ sur C

Comme le groupe de Galois de $\overline{K}/K$ agit par continuité sur C, on peut examiner les groupes de cohomologie $\mathrm{H}^r\left(\mathrm{Gal}(\overline{K}/K), C\right) =: \mathrm{H}^r(K, C)$.

Théorème 1.3.1 *On a* $\mathrm{H}^0(K, C) \cong K$, *et* $\mathrm{H}^1(K, C)$ *est un* K*-espace vectoriel de dimension* 1.

Démonstration : Soit K_∞/K une extension galoisienne infinie et totalement ramifiée de groupe de Galois isomorphe à $\mathbb{Z}_p$. On dispose d'un isomorphisme

$$\mathrm{H}^0(K, C) \cong \mathrm{H}^0\left(\mathrm{Gal}(\overline{K}/K)/\mathrm{Gal}(\overline{K}/K_\infty), C^{\mathrm{Gal}(\overline{K}/K_\infty)}\right).$$

Étant donné que $\mathrm{Gal}(\overline{K}/K)/\mathrm{Gal}(\overline{K}/K_\infty) \cong \mathrm{Gal}(K_\infty/K) = \Gamma$ et $C^{\mathrm{Gal}(\overline{K}/K_\infty)} = X$, la Proposition 1.1.4 (a) nous dit que $\mathrm{H}^0(K, C) \cong K$.
En outre, on dispose d'une suite exacte d'inflation-restriction (voir [13, p.126, Prop.5])

$$0 \to \mathrm{H}^1\left(\mathrm{Gal}(\overline{K}/K)/\mathrm{Gal}(\overline{K}/K_\infty), C^{\mathrm{Gal}(\overline{K}/K_\infty)}\right) \xrightarrow{\mathrm{Inf}} \mathrm{H}^1(K, C) \xrightarrow{\mathrm{Res}} \mathrm{H}^1\left(\mathrm{Gal}(\overline{K}/K_\infty), C\right).$$

D'après la Proposition 1.2.2, le groupe $\mathrm{H}^1\left(\mathrm{Gal}(\overline{K}/K_\infty), C\right)$ est nul, donc l'inflation est un isomorphisme. Mais on sait déjà (Proposition 1.1.4 (a)), que $\mathrm{H}^1\left(\mathrm{Gal}(\overline{K}/K)/\mathrm{Gal}(\overline{K}/K_\infty), C^{\mathrm{Gal}(\overline{K}/K_\infty)}\right)$ est un K-espace vectoriel de dimension 1 (car $\mathrm{Gal}(\overline{K}/K)/\mathrm{Gal}(\overline{K}/K_\infty) \cong \Gamma$ et $C^{\mathrm{Gal}(\overline{K}/K_\infty)} = X$). D'où l'énoncé. □

Soit maintenant $\chi : \mathrm{Gal}(\overline{K}/K) \to K^\times$ un homomorphisme continu (remarquons que les valeurs de χ sont des unités dans $\mathcal{O}_K$, parce que $\mathrm{Gal}(\overline{K}/K)$ est compact), et notons $C(\chi)$ le corps C muni de l'action tordue de $\mathrm{Gal}(\overline{K}/K)$: $\gamma.x = \chi(\gamma)(\gamma x)$, pour $\gamma \in \mathrm{Gal}(\overline{K}/K)$ et $x \in X$. Soit K_∞ l'extension de K déterminée par $\mathrm{Ker}(\chi)$.

Théorème 1.3.2 *Supposons qu'il existe une extension finie* K_0/K *contenue dans* K_∞ *telle que* K_∞/K_0 *soit totalement ramifiée et* $\mathrm{Gal}(K_\infty/K_0) \cong \mathbb{Z}_p$. *Alors,* $\mathrm{H}^0\left(K, C(\chi)\right) = 0$ *et* $\mathrm{H}^1\left(K, C(\chi)\right) = 0$.

Démonstration : Quitte à remplacer K par K_0, on peut supposer K_∞/K totalement ramifiée. La preuve s'effectue maintenant par une démonstration identique à celle du Théorème 1.3.1 sauf qu'il faut appliquer la partie (b) de la Proposition 1.1.4 au lieu de la partie (a). □

2 Schémas en groupes finis

On rappellera maintenant quelques faits sur des schémas en groupes finis.

2.1 Définition et exemples

Soit S un schéma. Un foncteur en groupes sur S est un cofoncteur F de la catégorie de schémas sur S dans la catégorie de groupes, c'est-à-dire la donnée, pour tout schéma X sur S, d'un groupe $F(X)$, et pour chaque S-morphisme $Y \to X$ d'un morphisme de groupes $F(X) \to F(Y)$.

Exemples. (a) Le schéma en groupes additif, $\mathbb{G}_a$: pour X sur S on pose

$$\mathbb{G}_a(X) = \text{groupe additif de} \quad \Gamma(X, \mathcal{O}_X);$$

(b) le schéma en groupes multiplicatif, $\mathbb{G}_m$: est donné par

$$\mathbb{G}_m(X) = \Gamma(X, \mathcal{O}_X)^\times,$$

c'est le cas $n = 1$ du
(c) schéma en groupes général linéaire, $\mathbb{GL}_n$:

$$\mathbb{GL}_n(X) = \text{matrices } n \times n \text{ invertibles à coefficients dans} \quad \Gamma(X, \mathcal{O}_X);$$

(d) le schéma en groupe spécial linéaire, $\mathbb{SL}_n$:

$$\mathbb{SL}_n(X) = \{A \in \mathbb{GL}_n(X) | \det(A) = 1\};$$

(e) les racines n-ièmes de l'unité, μ_n : pour X sur S on pose

$$\mu_n(X) = \{a \in \mathbb{G}_m(X) | a^n = 1\};$$

(f) si S est de caractéristique $p > 0$, on définit les racines p^r-ièmes de zéro, α_{p^r} :

$$\alpha_{p^r}(X) = \{a \in \mathbb{G}_a(X) | a^{p^r} = 0\};$$

comme $(a+b)^p = a^p + b^p$ dans $\Gamma(X, \mathcal{O}_X)$, $\alpha_{p^r}(X)$ est un sous-groupe de $\mathbb{G}_a(X)$;
(g) le foncteur de groupes constant, $\mathcal{H}$: soit H un groupe arbitraire. Pour X sur S on pose

$$\mathcal{H}(X) = H, \quad \text{et pour} \quad Y \to X, \quad \mathcal{H}(X) \xrightarrow{\text{id}} \mathcal{H}(Y).$$

Si F est représentable, disons par $G \xrightarrow{\tilde{\pi}} S$, alors on dit que G est un schéma en groupes. Le lemme de Yoneda traduit les axiomes de groupes en identités pour G sur S :
il existe un S-morphisme $\tilde{\mu} : G \times_S G \to G$, la *multiplication* qui satisfait l'associativité :

$$\tilde{\mu} \circ (\text{id} \times \tilde{\mu}) = \tilde{\mu} \circ (\tilde{\mu} \times \text{id}).$$

Il existe une section $\tilde{\varepsilon} : S \to G$, la *section unité*, pour le morphisme de structure $\tilde{\pi}$ telle que

$$\tilde{\mu} \circ (\tilde{\varepsilon} \times \text{id}) = \text{proj}_2 \qquad \text{et} \qquad \tilde{\mu} \circ (\text{id} \times \tilde{\varepsilon}) = \text{proj}_1 .$$

Il existe un S-morphisme $\tilde{\text{inv}} : G \to G$, l'*application inverse* :

$$\tilde{\mu} \circ (\text{id} \times \tilde{\text{inv}}) \circ \Delta = \tilde{\varepsilon} \circ \tilde{\pi} = \tilde{\mu} \circ (\tilde{\text{inv}} \times \text{id}) \circ \Delta,$$

où Δ est le morphisme diagonal.

Nous nous intéressons au cas où le schéma de base est affine (et commutatif) : $S = \text{Spec}(R)$, avec un anneau (abélien) R. Un groupe fini d'ordre n sur R est la donnée d'un schéma en groupe sur $\text{Spec}(R)$ qui est localement libre de rang n. Cela veut dire que G est défini par une R-algèbre A localement libre de rang n. Les applications $\tilde{\mu}$, $\tilde{\varepsilon}$ et $\tilde{\text{inv}}$ correspondent à des morphismes $\mu : A \to A \otimes A$ (la comultiplication, souvent notée Δ_A), $\varepsilon : A \to R$ (la co-unité, ε_A)

et un automorphisme inv : $A \to A$ (l'application antipodale, souvent notée S), satisfaisant aux conditions correspondantes :

$$(\mu \otimes \mathrm{id}) \circ \mu = (\mathrm{id} \otimes \mu) \circ \mu,$$
$$(\varepsilon \otimes \mathrm{id}) \circ \mu = \mathrm{id} \qquad \text{et} \qquad (\mathrm{id} \otimes \varepsilon) \circ \mu = \mathrm{id},$$
$$\mathrm{m} \circ (\mathrm{id} \otimes \mathrm{inv}) \circ \mu = \pi \circ \varepsilon = \mathrm{m} \circ (\mathrm{inv} \otimes \mathrm{id}) \circ \mu,$$

où m : $A \otimes A \to A$ définit la multiplication de A (souvent $\bigtriangledown$) et que π est le plongement de R dans A (souvent noté η).Un anneau A muni de ces structures s'appelle une *algèbre de Hopf*.

Exemples. (h) Soit Γ un groupe abstrait fini d'ordre n. Soit A l'anneau de fonctions sur Γ à valeurs dans R. On pose $\mu : A \to A \times A$, $(\mu f)(s,t) = f(st)$ et inv : $A \to A$, $(\mathrm{inv}\, f)(s) = f(s^{-1})$ et $\varepsilon : A \to R$, $(\varepsilon f) = f(1)$ On vérifie que les identités exigées sont satisfaites. Alors, $\Gamma = \mathrm{Spec}(A)$ est un groupe fini d'ordre n sur R.

(i) Les racines n-ième de l'unité $\mu_n = \mathrm{Spec}\,(R[X]/(X^n - 1))$ sont un groupe fini d'ordre n sur R avec $\mu(\overline{X}) = \overline{X} \otimes \overline{X}$. Pour une R-algèbre B on a :

$$\mu_n(B) = \mathrm{Hom}_R\,(R[X]/(X^n - 1), B) = \{b \in B | b^n = 1\}\,.$$

C'est un sous-groupe du R-schéma en groupes $\mathbb{G}_m = \mathrm{Spec}\left(R[X, X^{-1}]\right)$ avec $\mu(X) = X \otimes X$, $\mathrm{inv}(X) = X^{-1}$ et $\varepsilon(X) = 1$, on a

$$\mathbb{G}_m(B) = \mathrm{Hom}_R\left(R[X, X^{-1}], B\right) = B^\times,$$

plus précisément, on a une suite exacte $1 \to \mu_n \to \mathbb{G}_m \xrightarrow{n} \mathbb{G}_m$.

(j) Si R est de caractéristique $p > 0$ les racines p^r-ièmes de zéro, $\alpha_{p^r} = \mathrm{Spec}\left(R[X]/(X^{p^r})\right)$, forment un groupe fini sur R avec $\mu(X) = X \otimes 1 + 1 \otimes X$.

(k) Le groupe le plus général d'ordre 2 sur R dont l'algèbre affine est libre sur R est $\mathbf{G}_a^b = \mathrm{Spec}(R \oplus Rx) = \mathrm{Spec}(R[X]/(X^p + aX))$ pour $ab = 2$ et $x^2 + ax = 0$ avec $\mu(x) = x \otimes 1 + 1 \otimes x + bx \otimes x$. Pour une R-algèbre B on a $\mathbf{G}_a^b(B) = \left\{\beta \in B | \beta^2 + a\beta = 0\right\}$ et μ définit une multiplication sur $\mathbf{G}_a^b(B)$ par $\beta_1 * \beta_2 = \beta_1 + \beta_2 + b\beta_1\beta_2$ ($\beta_1 * \beta_2$ est encore dans $\mathbf{G}_a^b(B)$: $(\beta_1 + \beta_2 + b\beta_1\beta_2)^2 + a(\beta_1 + \beta_2 + b\beta_1\beta_2) = (b\beta_1\beta_2)^2 + 2\beta_1\beta_2 + 2b{\beta_1}^2\beta_2 + 2b\beta_1{\beta_2}^2 + ab\beta_1\beta_2 = 4\beta_1\beta_2 - 2ab\beta_1\beta_2 - 2ab\beta_1\beta_2 + a^2b^2\beta_1\beta_2 = \beta_1\beta_2(4 - 4 - 4 + 4) = 0$). Pour $a', b' \in R$, les groupes $\mathbf{G}_{a'}^{b'}$ et $\mathbf{G}_a^b$ sont isomorphes si et seulement s'il existe une unité $u \in R$ telle que $a' = ua$, $ub' = b$.

2.2 Dualité

A partir de maintenant, tous les groupes sont supposés commutatifs. Soit $G = \mathrm{Spec}(A)$ un schéma en groupes fini sur R et $m : A \otimes A \to A$, $\mu : A \to A \times A$ comme dans le paragraphe précédent. Le R-module

$$A^D := \mathrm{Hom}_{\mathbf{Mod}(R)}(A, R)$$

est de nouveau la R-algèbre d'un groupe fini sur R : on a les morphismes induits $\mu^D : A^D \otimes A^D \to A^D$, la multiplication d'algèbres, $\varepsilon^D : R \to A^D$, le plongement de $R = R^D$ dans A^D, $\pi^D : A^D \to R$, le co-unité et $\mathrm{inv}^D : A^D \to A^D$, l'inverse. On pose

$$G^D = \mathrm{Spec}(A^D)$$

et on vérifie facilement que $\mathrm{m}^D : A^D \to A^D \otimes A^D$ définit une multiplication sur G^D, ε^D définit une projection, π^D définit l'unité et inv^D l'inverse. Le schéma en groupes G^D est dit le *dual de Cartier* de G et bien sûr l'ordre de G et l'ordre de G^D sont égaux. On a également un isomorphisme canonique $(G^D)^D \cong G$.

Si T est un préschéma sur R, X et Y deux schémas, on considère le foncteur défini par

$$\mathcal{HOM}_{\mathrm{Spec}(R)}(X, Y)(T) = \mathrm{Hom}_T(X \times_R T, Y \times_R T) = \mathrm{Hom}_T(X, Y)$$

(les homomorphisme de schémas sur T de $X \times_R T$ vers $Y \times_R T$), alors on voit facilement que

$$G^D = \mathcal{HOM}_{\mathbf{SchGr}(R)}(G, \mathbb{G}_m),$$

où l'indice se réfère au sous-faisceau des homomorphismes de schémas en groupes. Maintenant, il est facile de décrire l'accouplement $G \times G^D \to \mathbb{G}_m$ de façon explicite : on rappelle que $\mathbb{G}_m = \mathrm{Spec}(R[X, X^{-1}])$ et on choisit un sous-ensemble ouvert U de $\mathrm{Spec}(R)$ trivialisant le faisceau localement libre $\mathcal{O}_G$. Soit $e_1, \ldots, e_n$ une base de $\mathcal{O}_G|_U$ et $e_1^D, \ldots, e_n^D$ la base duale de $\mathcal{O}_{G^D}|_U$. Alors l'application

$$R[X, X^{-1}]|U \to \mathcal{O}_G|U \otimes_{R|U} \mathcal{O}_{G^D}|U$$

est simplement donnée par

$$X \to \sum_{i=1}^{n} e_i \otimes e^D{}_i. \tag{2}$$

Remarquons que l'isomorphisme canonique

$$\mathcal{O}_{G^D} \otimes_R \mathcal{O}_G \xrightarrow{\sim} \mathcal{HOM}_R(\mathcal{O}_G, \mathcal{O}_G)$$

envoie l'élément $\sum e_i \otimes e_i^D$ sur le morphisme de modules trivial $\mathrm{id}_{\mathcal{O}_G}$. Donc, l'application (2) est bien canonique (en particulier, elle est indépendante du choix des e_i).

Exemples. (a) Le dual du groupe cyclique d'ordre n, $G = \underline{\mathbb{Z}/n\mathbb{Z}}$ est μ_n.
Décrivons l'accouplement de Cartier dans le cas $n = p$. On écrit $\underline{\mathbb{Z}/p\mathbb{Z}} = \mathrm{Spec}\,(R[Y]/(Y^p - Y))$, $\mu_p = \mathrm{Spec}\,(R[Z]/(Z^p - 1))$. Une base pour l'algèbre de $\underline{\mathbb{Z}/p\mathbb{Z}}$ est $\underline{1, Y, \ldots, Y^{p-1}}$; soit $f_0, \ldots, f_{p-1}$ la base duale (on peut montrer que $f_i = \frac{f_1^i}{i!}$). Si on considère l'application exponentielle $\exp(\xi) = 1 + \xi + \frac{\xi^2}{2!} + \cdots + \frac{\xi^{p-1}}{(p-1)!}$, alors $Z = \exp(f_1)$ et la dualité de Cartier est définie par

$$X \to \exp(Y \otimes \log Z).$$

(b) Si $G = \mathbf{G}_a^b$, alors le dual de Cartier est $G^D = \mathbf{G}_b^a$ et la combinaison de Cartier est

$$X \to 1 - Y \otimes Z.$$

2.3 Suites exactes courtes

Une suite

$$0 \to G' \xrightarrow{i} G \xrightarrow{j} G'' \to 0 \tag{3}$$

de groupes finis sur R est dite *exacte* si i est une immersion fermée identifiant G' au noyau de j (dans le sens catégorique), tandis que j est fidèlement plat. Si on dispose de j, il est facile de construire G' comme image inverse de la section unité de G''. Par contre, i étant donnée, il est plus délicat, bien que possible, de construire G''.

Si (3) est exact, les ordres m, m' et m'' de G, G' et G'' satisfont à la relation $m = m'm''$, ce qui résulte du lemme suivant :

Lemme 2.3.1 *Soient G un schéma en groupes fini sur R et N un sous-schéma en groupes plat. Alors, le quotient G/N existe, il est plat et fini sur R. On a*

$$\#(G) = \#(N)\#(G/N).$$

Si N est normal, alors G/N est un groupe fini sur R.

Démonstration (Esquisse, voir [12]) : Soit A_N l'algèbre de Hopf de N. Le groupe N est fini puisque A_N est un quotient du R-module A. Donc, N est propre sur R. Maintenant G est quasi-projectif parce qu'il est fini. En conséquence, un théorème de Grothendieck [6, Théorème 6.1] implique que G/N est représentable. Dans ce cas cependant, on sait construire G/N. Comme N est donné par un idéal quasi-cohérent $\mathfrak{J}$ de A, on peut considérer le R-sous-algèbre de A

$$A_{G/N} = \{x \in A | \mu(x) = x \otimes 1 \mod A \otimes \mathfrak{J}\} \tag{4}$$

et il est connu que le spectre de cette algèbre est précisément G/N.

Il reste à montrer que G/N est plat sur R et que le théorème de Lagrange est vrai. La définition (4) montre que le graphe de la relation d'équivalence en G induit par N est le produit fibré

$$\mathcal{R} = G \times_{G/N} G.$$

C'est un sous-schéma fermé de $G \times_R G$, et on a l'isomorphisme

$$N \times_R G \cong \mathcal{R} = G \times_{G/N} G.$$

Comme N est fidèlement plat sur R, il en est de même pour $\mathrm{proj}_2 : \mathcal{R} \to G$. Le diagramme cartésien

$$\begin{array}{ccc} \mathcal{R} & \xrightarrow{\mathrm{proj}_1} & G \\ {\scriptstyle \mathrm{proj}_2}\downarrow & & \downarrow{\scriptstyle \pi} \\ G & \xrightarrow[\pi]{} & G/N \end{array} \tag{5}$$

où π est la projection canonique, et sa symétrie montrent que proj_1 est aussi fidèlement plat. Maintenant $G \to G/N$ est surjective, par conséquent elle est dominée par un revêtement pour la topologie fpqc, supposé de la forme $X \xrightarrow{r} G \xrightarrow{\pi} G/N$ et $\pi \circ r$ fpqc. En réalisant une extension de base de (5) on obtient

$$\begin{array}{ccccc} \mathcal{R} \times_{G/N} X & \xrightarrow{\rho_1} & \mathcal{R} & \xrightarrow{\mathrm{proj}_1} & G \\ {\scriptstyle \rho_2}\downarrow & & {\scriptstyle \mathrm{proj}_2}\downarrow & & \downarrow{\scriptstyle \pi} \\ X & \xrightarrow[r]{} & G & \xrightarrow[\pi]{} & G/N \end{array} \tag{5'}$$

où ρ_2 (extension de base de proj_2) est fidèlement plate. Mais alors, le fpqc-morphisme $\pi \circ r$ l'est aussi. Donc par la descente fidèlement plate, π est fidèlement plat. Pour cette raison, G/N est plat sur R puisque G l'est.

Comptant les rangs dans l'isomorphisme

$$N \times_R G \cong G \times_{G/N} G$$

on trouve que

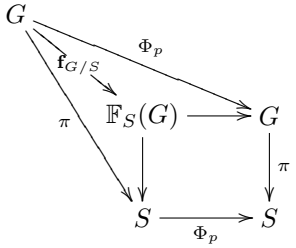
$$\#(N)\#(G) = \frac{\#(G)^2}{\#(G/N)}$$

comme exigé. De la description fonctorielle de G/N comme co-noyau de faisceaux, on déduit que G/N est un groupe si N est normal. □

Finalement, le dual d'une suite exacte courte de la forme (3) est exact.

2.4 Le morphisme de Frobenius

En caractéristique $p > 0$ on dispose du *morphisme de Frobenius*. Dans cette partie on va décrire comment il se présente en général. Soient S un schéma de caractéristique $p > 0$ et G un schéma en groupes fini sur S. On note $\Phi_p \colon G \to G$ le morphisme de schémas qui correspond à l'élévation à la puissance p-ième sur les sections. On a un diagramme commutatif



où le carré extérieur n'est pas cartésien tandis que le carré intérieur l'est. C'est-à-dire, $\mathbb{F}_S(G)$ est le produit fibré de G et S sur S et $\mathbf{f}_{G/S}$ est le morphisme induit par la projection π et Φ_p. On dit que le schéma $\mathbb{F}_S(G)$ est le *schéma en groupes de Frobenius* de G sur S et $\mathbf{f}_{G/S}$ est le *morphisme de Frobenius*. Le schéma $\mathbb{F}_S(G)$ est effectivement un schéma en groupes sur S parce qu'il est une extension de base, et le morphisme de Frobenius est un homomorphisme de schémas en groupes. Donc, cette construction commute avec produits et limites projectives. On se rend compte que

$$\mathcal{O}_{\mathbb{F}_S(G)} = \mathcal{O}_{G\,\varphi} \otimes_{\mathcal{O}_S} \mathcal{O}_S, \quad \text{où} \quad \varphi : \mathcal{O}_S \to \mathcal{O}_S\,,\ x \mapsto x^p,$$

et qu'au niveau de faisceaux, $\mathbf{f}_{G/S}$ est l'application

$$\mathbf{f} : \mathcal{O}_G \otimes_{\mathcal{O}_S} \mathcal{O}_S \to \mathcal{O}_G\,,\ a \otimes \lambda \mapsto a^p\lambda$$

Supposons maintenant $S = \mathrm{Spec}(R)$ où R est un anneau locale complet. Pour un schéma en groupes fini sur S, disons G, les différentielles $\Omega^1_{G/R}$ sont données par $A \otimes \mathfrak{m}_0/\mathfrak{m}_0^2$ via $1 \otimes \mu$ avec $A = \Gamma(G, \mathcal{O}_G)$ et $\mathfrak{m}_0 = \mathrm{Ker}\,\varepsilon$. Le quotient $\mathfrak{m}_0/\mathfrak{m}_0^2$ est l'espace tangent à l'origine de G et peut s'identifier à l'espace des différentielles invariantes $\omega_{G/R}$ de G. Le noyau de l'application $G\big(R[T]/(T^2)\big) \to G(R)$ s'identifie au dual de $\mathfrak{m}_0/\mathfrak{m}_0^2$. De ces remarques on déduit la proposition suivante :

Proposition 2.4.1 *Soient R un anneau local complet équicaractéristique de caractéristique $p > 0$ et G un schéma en groupes fini et connexe sur R. Alors, le noyau de $\mathbf{f}_{G/R}$ n'est que nul si G est trivial. De ce fait, si R est artinien, il existe un nombre entier $n > 0$ avec $G = \mathrm{Ker}\,\mathbf{f}^n_{G/R}$. Le plus petit entier n de cette forme est la* hauteur de Frobenius.

Démonstration : On examine le diagramme

$$\begin{array}{ccccc}
(\mathfrak{m}_0/\mathfrak{m}_0^2)^\vee & \longrightarrow & G(R[T]/T^2) & \longrightarrow & G(R) \\
\downarrow{\scriptstyle \mathbf{f}} & & \downarrow{\scriptstyle \mathbf{f}} & & \downarrow{\scriptstyle \mathbf{f}} \\
(\mathfrak{m}_0/\mathfrak{m}_0^2)^\vee_\varphi & \longrightarrow & \mathbb{F}_R(G)(R[T]/T^2) & \longrightarrow & \mathbb{F}_R(G)(R)
\end{array} \quad .$$

Comme $\mathbf{f}(a \otimes \lambda) = a^p\lambda$ et $p \geq 2$, la première application verticale s'annule. Si $\mathbf{f}$ est un monomorphisme, alors on trouve $\mathfrak{m}_0 = \mathfrak{m}_0^2$: cela implique que $\mathfrak{m}_0 = (0)$, c'est-à-dire, $G = S$ par le théorème de Krull.
Si R est artinien, la suite de noyaux $(\mathrm{Ker}\,\mathbf{f}^n_{G/R})_n$ finit par devenir stationnaire ; donc, elle s'arrête par G. □

2.5 Groupes connexes et étales

Dans ce paragraphe on suppose que R est un anneau local complet et noethérien.

Lemme 2.5.1 *Soit G un schéma en groupe affine sur R plat et de type fini. Alors, il existe une suite exacte (canonique)*

$$0 \to G^0 \xrightarrow{i} G \xrightarrow{j} G^{\mathrm{et}} \to 0,$$

où G^0 est affine et connexe sur R, plat et normal dans G et où G^{et} est étale fini sur R.

Démonstration : Soit G^0 la composante connexe de l'identité de G. Évidemment, G^0 est un sous-schéma en groupes de G connexe et normal. Soit A l'anneau des sections globales de G. C'est un produit de R-algèbres locales, parce que l'on peut relever les éléments idempotents (car R est complet). Soit A^{et} la sous-algèbre maximale séparable de A. Le schéma

$$G^{\mathrm{et}} := \mathrm{Spec}(A^{\mathrm{et}})$$

est un groupe fini et étale sur R. Si $e_0, \ldots, e_r$ sont les générateurs idempotents de A^{et}, $\varepsilon : A \to R$ s'annule en tous sauf un d'eux, disons $\varepsilon(e_0) = 1$. (On peut supposer le corps résiduel de R séparablement clos.) Mais grâce à cela on voit que

$$G^0 = \mathrm{Spec}\left(A/(\mathrm{Ker}\,\varepsilon \cap A^{\mathrm{et}})A\right) = \mathrm{Spec}(e_0 A),$$

et on voit que que G^0 est plat sur R. □

Si G est un groupe fini sur R, le groupe G^0 est

$$\mathrm{Spec}(A_{\mathfrak{m}_0})$$

où $\mathfrak{m}_0 = \mathrm{Ker}\,\varepsilon$. Autrement dit, l'anneau correspondant à G^0 est le quotient local de A à travers lequel la section de l'unité $\varepsilon : A \to R$ se factorise. L'application i est une immersion ouverte et fermée. Pour G variable, les foncteurs

$$G \mapsto G^0 \qquad \text{et} \qquad G \mapsto G^{\mathrm{et}}$$

sont exacts.

Le groupe G est *connexe* si

$$G = G^0.$$

Dans ce cas l'ordre de G est une puissance de la caractéristique du corps résiduel k de R, plus précisément, il est 1 si $\mathrm{char}(k) = 0$ et une puissance de p si $\mathrm{char}(k) = p > 0$. Plus généralement, on a :

Lemme 2.5.2 *Soit R un anneau local complet de corps résiduel séparablement clos (où plus généralement, un anneau local strictement hensélien) de caractéristique $p > 0$. Alors, tout schéma en groupes connexe et fini sur R est d'ordre p^t pour t convenable.*

Démonstration : Soient G un schéma en groupes connexe et fini sur R et $\overline{G} = G \times_R (R/\mathfrak{m}_R)$ sa fibre sur le point fermé. Le schéma $\overline{G}$ est forcément connexe, sinon on pourrait relever un idempotent non-trivial de $\mathcal{O}_{G^{\mathrm{et}}}$ (qui existe du fait que $R/\mathfrak{m}_R = (R/\mathfrak{m}_R)^{\mathrm{sep}}$) de $R/\mathfrak{m}_R$ vers R puisque R est complet par hypothèse. Par conséquent, G^{et} serait non-trivial, contradiction. Comme $\#(G) = \#(\overline{G})$ on peut se ramener au cas où R est un corps séparablement clos de caractéristique $p > 0$. La proposition (2.4.1) et une récurrence sur la hauteur de Frobenius de G permettent de supposer $G = \mathrm{Ker}\,\mathbf{f}_{G/R}$. Mais dans ce cas, l'algèbre de G est donnée par $R[x_1, \ldots, x_t]/(x_1^p, \ldots, x_t^p)$, d'où l'énoncé. □

Par contre, G est *étale* si

$$G = G^{\mathrm{et}}.$$

Le foncteur

$$G \mapsto G(\overline{k})$$

est une équivalence entre la catégorie de R-groupes étales d'ordre fini et celle des $\mathrm{Gal}(\overline{k}/k)$-modules finis où l'opération de $\mathrm{Gal}(\overline{k}/k)$ est continue. On dit que $\mathrm{Gal}(\overline{k}/k)$ est le groupe fondamental de R. Soit R_{et} une « extension maximale locale étale intègre »de R (c'est-à-dire, une extension maximale non-ramifiée de R, si R est un anneau de valuation discrète). Le groupe $\mathrm{Gal}(\overline{k}/k)$ agit sur R_{et} de l'unique façon compatible à son opération sur l'extension de corps résiduels k_{et}/k (le corps résiduel k_{et} de R_{et} une clôture séparable de k). Étant donné un $\mathrm{Gal}(\overline{k}/k)$-module Γ, le R-groupe étale fini correspondant est $\mathrm{Spec}(A)$ où A est l'anneau des fonctions $\Gamma \to R_{\mathrm{et}}$ commutant avec $\mathrm{Gal}(\overline{k}/k)$.

Dans le cas général - G non nécessairement étale - on a

$$G^{\mathrm{et}} = G(\overline{k}).$$

3 Les groupes p-divisibles

3.1 Définition

Soit p un nombre premier et $h \geq 0$ un nombre entier. Un *groupe p-divisible* sur un anneau (commutatif) R de hauteur h est un système inductif

$$G = (G_\nu, i_\nu)_{\nu \in \mathbb{N}}$$

où
(i) G_ν est un schéma en groupes fini d'ordre $p^{\nu h}$ sur R et
(ii) pour tout $\nu \in \mathbb{N}_0$, le morphisme $i_\nu : G_\nu \to G_{\nu+1}$ identifie G_ν avec le noyau de la multiplication par p^ν dans $G_{\nu+1}$, c'est-à-dire, la suite

$$0 \to G_\nu \xrightarrow{i_\nu} G_{\nu+1} \xrightarrow{p^\nu} G_{\nu+1}$$

est exacte.

Exemple. (a) Pour des groupes abéliens habituels, cela implique

$$G_\nu \cong (\mathbb{Z}/p^\nu \mathbb{Z})^h \quad \text{et} \quad G = \lim_{\nu \to \infty} G_\nu = (\mathbb{Q}_p/\mathbb{Z}_p)^h.$$

Un *homomorphisme de groupes p-divisibles* $f : G \to H$ est un système d'homomorphismes de groupes finis sur R

$$f_\nu : G_\nu \to H_\nu$$

qui sont compatibles avec les injections i_ν, c'est-à-dire tels que le diagramme

$$\begin{array}{ccc} G_\nu & \xrightarrow{f_\nu} & H_\nu \\ {\scriptstyle i_\nu}\downarrow & & \downarrow{\scriptstyle i_\nu} \\ G_{\nu+1} & \xrightarrow{f_{\nu+1}} & H_{\nu+1} \end{array}$$

commute pour tout $\nu \in \mathbb{N}$.

Proposition 3.1.1 *Un groupe p-divisible G sur R est un groupe de p-torsion commutatif sur R tel que la multiplication par p, $\mathbf{p} : G \to G$, soit une isogénie (un morphisme surjectif de noyau fini).*

Démonstration : Comme le système est inductif, on obtient des immersions fermées par itération des i_ν

$$i_{\nu+\mu-1} \circ \cdots \circ i_\nu =: i_{\nu,\mu} : G_\nu \to G_{\nu+\mu} \quad \text{pour tout } \nu \geq 0 \text{ et } \mu \geq 1,$$

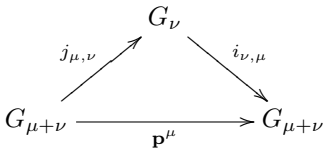
identifiant G_ν avec le noyau de la multiplication par p^ν dans tous les groupes $G_{\nu+\mu}$, car on a le diagramme suivant

$$\begin{array}{ccccccccc} 0 \longrightarrow & G_\nu & \xrightarrow{i_\nu} & G_{\nu+1} & \xrightarrow{i_{\nu+1}} & G_{\nu+2} & \xrightarrow{i_{\nu+1}} \cdots \xrightarrow{i_{\nu+\mu-1}} & G_{\nu+\mu} \\ & & & {\scriptstyle \mathbf{p}^\nu}\downarrow & & {\scriptstyle \mathbf{p}^\nu}\downarrow & & {\scriptstyle \mathbf{p}^\nu}\downarrow \\ & & & G_{\nu+1} & \xrightarrow{i_{\nu+1}} & G_{\nu+2} & \xrightarrow{i_{\nu+2}} \cdots \xrightarrow{i_{\nu+\mu-1}} & G_{\nu+\mu} \\ & & & & & {\scriptstyle \mathbf{p}}\downarrow & & {\scriptstyle \mathbf{p}^{\mu-1}}\downarrow \\ & & & & & G_{\nu+2} & \xrightarrow{i_{\nu+2}} \cdots \xrightarrow{i_{\nu+\mu-1}} & G_{\nu+\mu}. \end{array}$$

Donc, G_ν est le noyau de $\mathbf{p}^\nu$ sur $G = \varinjlim G_\nu$ et G est un groupe de p-torsion.
En échangeant les rôles de μ et ν, il en résulte que le morphisme

$$\mathbf{p}^\mu : G_{\mu+\nu} \to G_{\mu+\nu}$$

se factorise de façon canonique à travers G_ν



où $j_{\mu,\nu}$ est induit par $\mathbf{p}^\nu$ de façon unique. Maintenant, le noyau de $j_{\mu,\nu}$ est le noyau de p^μ. Comme l'ordre de $G_{\mu+\nu}$ est per definitionem le produit des ordres de G_μ et G_ν, on déduit du Lemme (2.3.1) une suite exacte

$$0 \to G_\nu \xrightarrow{i_{\mu,\nu}} G_{\mu+\nu} \xrightarrow{j_{\mu,\nu}} G_\nu \to 0. \tag{6}$$

Par conséquent, $\mathbf{p} : G \to G$ est une isogénie, cela veut dire, est surjective de noyau un schéma en groupe fini sur R. □

Exemples. (b) (C'est l'exemple motivant.) Soit X un schéma (abélien) de dimension d sur R. Si X_n dénote le noyau de la multiplication avec n, alors il est connu que X_n est un schéma en groupes fini sur R d'ordre n^{2d}. En conséquence, le système (X_{p^ν}, i_ν), où i_ν est l'inclusion, est un groupe p-divisible noté $X(p)$ de hauteur $h = 2d$. Il est dit le *groupe p-divisible du schéma abélien* X.

(c) D'une façon semblable, on construit d'autres groupes sur R : Prenant $X = \mathbb{G}_m$, on voit facilement que $\operatorname{Ker} p^\nu|_{\mathbb{G}_m} = \mu_{p^\nu}$. Les μ_{p^ν} forment un sytème inductif avec l'inclusion ordinaire et on obtient le groupe p-divisible de $\mathbb{G}_m$, $\mathbb{G}_m(p) = (\mu_{p^\nu}, i_{p^\nu})_\nu$, qui a hauteur 1.

3.2 Groupes formels

Soit R un anneau local complet (voire éventuellenment un corps ou un anneau local d'Artin), $\mathfrak{m}_R$ son idéal maximal. Par la suite, on restreindra la catégorie sur laquelle les foncteurs apparus sont définis.

Un schéma T sur R est dit *très fini*, si
(i) T est fini (donc affine) sur R, et
(ii) $\Gamma(T, \mathcal{O}_T)$ est un R-module de longueur finie.
Si R est artinien, (ii) résulte de (i).

Un *foncteur formel* F sur R est un co-foncteur de la catégorie de schémas très finis sur R vers la catégorie des ensembles et si les ensembles résultants ont une structure de groupes de manière fonctorielle, on parle de *foncteur formel en groupes* sur S. Bien sûr, tout R-foncteur ou R-foncteur en groupes F induit un foncteur formel $\hat{F}$, appelé la complétion formelle de F, par restriction aux R-schémas très finis.

Une R-algèbre A est dite *profinie*, si elle est la limite projective $\varprojlim A/\mathfrak{A}$ pour une famille d'idéaux $(\mathfrak{A})$ telle que $A/\mathfrak{A}$ soit très fini sur R. Remarquons que toute R-algèbre finie en tant que R-module est profinie, en particulier, R est profini, car $R = \lim_{\infty \leftarrow q} R/\mathfrak{m}_R^q$. Par contre, la R-algèbre $R[[X_1, \ldots, X_n]]$ n'est pas finie tout en étant profinie. En effet, soit

$$\mathfrak{J} = (X_1, \ldots, X_n) + \mathfrak{m}_R R[[X_1, \ldots, X_N]],$$

alors $R[[X_1, \ldots, X_n]]$ est la limite projective des $R[[X_1, \ldots, X_n]]/\mathfrak{J}^t$.

Toute R-algèbre profinie A définit un foncteur formel, dénommé le spectre formel $\operatorname{Spf} A$ de A par la formule

$$(\operatorname{Spf} A)(T) = \operatorname{Hom}_{R,\text{cont.}}(A, \Gamma(T, \mathcal{O}_T)),$$

où T est très fini sur R et où $\Gamma(T, \mathcal{O}_T)$ est muni de la topologie discrète. Par abus de notation, on peut le reécrire comme fonteur covariant sur la catégorie des R-algèbres très finies :

$$(\operatorname{Spf} A)(B) = \operatorname{Hom}_{R,\text{cont.}}(A, B).$$

Cette définition-ci mène à une extension aux R-algèbres profinies. Scilicet, pour B profinie, disons $B = \lim_{\infty \leftarrow \alpha} B/\mathfrak{B}_\alpha$, on pose

$$(\operatorname{Spf} A)(B) = \lim_{\infty \leftarrow \alpha} \operatorname{Hom}_{R,\text{cont.}}(A, B/\mathfrak{B}_\alpha).$$

Comme ces foncteurs formels sont des vrai foncteurs sur la catégorie de R-algèbres profinies, on est en mesure de définir les schémas formels :
Un *R-schéma (en groupes) formels* est un foncteur représentable de la catégorie de R-algèbres profinies vers la catégorie des ensembles (respectivement des groupes). Autrement dit, un R-schéma formel est de la forme $\mathrm{Spf}\, A$ pour une certaine R-algèbre A.

Si A est une R-algèbre finiment engendrée, on a le foncteur habituel représentable $\mathrm{Spec}\, A$ duquel on peut considérer la complétion $\widehat{\mathrm{Spec}\, A}$. Il est évident que celle-ci est représentable, c'est-à-dire, est un R-schéma formel $\mathrm{Spf}\, \hat{A}$ d'une certaine R-algèbre profinie $\hat{A}$: Soit

$$R[X_1, \ldots, X_m] \xrightarrow{\varphi} R[Y_1, \ldots, Y_n] \to A \to 0$$

une présentation de A. Puisque φ est donné par m polynômes en les Y_i (par changement linéaire de variables dans $R[X]$, on peut les supposer sans terme constant), φ reste défini si on remplace les anneaux de polynômes par des anneaux de séries formelles et on obtient une présentation pour $\hat{A} := \mathrm{Coker}\, \varphi$

$$R[[X_1, \ldots, X_m]] \xrightarrow{\varphi} R[[Y_1, \ldots, Y_n]] \to \hat{A} \to 0.$$

Si $\mathrm{Spf}\, A$ est un groupe formel, alors les co-multiplications induisent une comultiplication

$$\hat{\mu} : A \to A \hat{\otimes}_R A,$$

où le chapeau désigne le produit tensoriel complété. Plus précisément, si $A = \varprojlim A/\mathfrak{A}$, alors $A\hat{\otimes}_R A = \varprojlim (A/\mathfrak{A}) \otimes_R (A/\mathfrak{A})$ est une R-algèbre profinie. Cette co-multiplication est le co-produit dans la catégorie de R-algèbres profinies.

A. Grothendieck a fourni un critère de représentabilité dans [5] :

Théorème 3.2.1 *Un foncteur de la catégorie de R-algèbres profinies dans la catégorie des ensembles (respectivement des groupes) est représentable si et seulement s'il est exact à gauche.*

Examinons désormais le cas des groupes formels.

Proposition 3.2.1 *Tout groupe formel G sur R dispose d'une suite exacte canonique*

$$0 \to G^0 \to G \to G^{\mathrm{et}} \to 0$$

où G^0 est un sous-groupe formel connexe et normal de G et G^{et} est un groupe formel étale.

Démonstration : Écrivons $G = \mathrm{Spf}\, A$ et $A = \varprojlim A/\mathfrak{A}$. Comme dans la démonstration pour les schémas en groupes ordinaires (cf. Lemme (2.5.1)), on a les R-algèbres $(A/\mathfrak{A})^{\mathrm{et}}$ et par passage à la limite, on obtient A^{et}. On pose $G^{\mathrm{et}} = \mathrm{Spf}(A^{\mathrm{et}})$ avec une loi de groupe induite par celle de G de sorte que la surjection $G \to G^{\mathrm{et}}$ est un morphisme. Soit G^0 son noyau. L'anneau A des sections globales de G est un produit de R-algèbres locales, parce que l'on peut relever les éléments idempotents comme R est complet. Cela montre que G^0 est connexe. □

3.3 Groupes de Lie formels

Dans cette partie, on suppose R local complet, noethérien de corps résiduel k de caractéristique $p > 0$. On dit qu'un groupe formel Γ est lisse sur R, si Γ^0 est le spectre formel d'un anneau de séries entières. Un groupe formel lisse et connexe est un *groupe de Lie formel*, il est de la forme

$$\mathrm{Spf}(R[[X_1, \ldots, X_n]])$$

et l'entier n est sa dimension. L'isomorphisme

$$R[[X_1, \ldots, X_n]] \hat{\otimes}_R R[[Y_1, \ldots, Y_m]] \cong R[[S_1, \ldots, S_n, T_1, \ldots, T_m]],$$

avec $S_i = X_i \otimes 1$ et $T_i = 1 \otimes Y_i$ montre que pour décrire le structure d'un groupe de Lie formel $\mathrm{Spf}(R[[X_1, \ldots, X_n]])$, on a besoin d'une famille

$$f(Y, Z) = (f_i(Y, X))$$

de n séries entières en $2n$ variables Y_i, Z_j. Les axiomes imposés revient des axiomes de groupes :

$$\begin{aligned} &\text{(i)} && X = f(X,0) = f(0,X) \quad \text{(identité)};\\ &\text{(ii)} && f(X,f(Y,Z)) = f(f(X,Y),Z) \quad \text{(associativité)};\\ &\text{(iii)} && f(X,Y) = f(Y,X) \quad \text{(commutativité)}. \end{aligned}$$

L'existence de la loi de l'inverse est automatique.

On écrit $X * Y = f(X,Y)$. Les axiomes impliquent que

$$X * Y = X + Y + \text{(variables de degré} > 1).$$

Si $x_1, \ldots, x_n, y_1, \ldots, y_n$ sont des éléments (non-unités) d'une R-algèbre très finie B, alors la loi de groupes en $(\operatorname{Spf} A)(B)$ est donnée par $x * y = f(x,y) = x + y + \cdots$.

Considérons $\psi(X) = \underbrace{X * \cdots * X}_{p \text{ fois}}$. Cette expression détermine un morphisme

$$\psi : \mathcal{A} \to \mathcal{A},$$

où $\mathcal{A} = R[[X_1, \ldots, X_n]]$, correspondant à la multiplication par p dans Γ. Celui-ci est dit divisible si la multiplication par p, $\mathbf{p} : \Gamma \to \Gamma$, est une isogénie. Cela signifie que ψ fait de $\mathcal{A}$ un module libre de rang fini sur $\mathcal{A}$ même.

Appliquons la construction de l'Example (b) à Γ afin d'obtenir un groupe p-divisible

$$\Gamma(p) = (\Gamma_{p^\nu}, i_\nu)$$

de hauteur h sur R, où p^h est le degré de l'isogénie $\mathbf{p} : \Gamma \to \Gamma$. Le degré est en effet une puissance de p, car il coïncide avec l'ordre du R-groupe fini $\Gamma_p = \operatorname{Ker} p$, qui est connexe (voir Lemme (2.5.2)). Plus généralement, on a

$$(\Gamma(p))_\nu = \Gamma_{p^\nu} = \operatorname{Spec} A_\nu,$$

avec $A_\nu = \mathcal{A}/\mathfrak{J}_\nu$, où $\mathfrak{J}_\nu = \psi^\nu(\mathfrak{J}_0)\mathcal{A}$ est l'idéal de $\mathcal{A}$ engendré par les éléments $\psi^\nu(X_i)$, $1 \le i \le n$, en particulier, $\mathfrak{J}_0 = (X_1, \ldots, X_n)_{\mathcal{A}}$. Puisque les A_ν sont des anneaux locaux, tout $\Gamma(p)_\nu$ est connexe, c'est-à-dire, $\Gamma(p)$ est un groupe p-divisible connexe.

Lemme 3.3.1 *Soit R un anneau local complet et noethérien de corps résiduel k de caractéristique $p > 0$. Soit $\mathfrak{m}$ son idéal maximal, si bien qu'avec les notations qui précèdent $\mathfrak{m}\mathcal{A} + \mathfrak{J}_0 = \mathfrak{M}$ est l'idéal maximal de $\mathcal{A}$. Alors, les idéaux $\mathfrak{m}^\nu\mathcal{A} + \mathfrak{J}_\nu$ constituent un système fondamental de voisinages de 0 pour la topologie $\mathfrak{M}$-adique de $\mathcal{A}$.*

Démonstration : Le quotient $\mathcal{A}/(\mathfrak{m}^\nu\mathcal{A} + \mathfrak{J}_\nu) = A_\nu/\mathfrak{m}^\nu A_\nu$ est un anneau d'Artin (en effet, il est noethérien et tout idéal premier est maximal), les idéaux en question sont donc ouverts pour la topologie $\mathfrak{M}$-adique. D'autre part, ils sont aussi petits que l'on veut : il résulte des axiomes que

$$\psi(X_i) = pX_i + \text{(variables de degré} \ge 2),$$

et en conséquence,

$$\psi(\mathfrak{J}_0) \subset p\mathfrak{J}_0 + \mathfrak{J}_0^2 \subset (\mathfrak{m}\mathcal{A} + \mathfrak{J}_0)\mathfrak{J}_0 = \mathfrak{M}\mathfrak{J}_0,$$

car $p \in \mathfrak{m}\mathcal{A}$. Par récurrence on voit que

$$\mathfrak{J}_\nu = \psi^\nu(\mathfrak{J}_0)\mathcal{A} \subset \mathfrak{M}^\nu\mathfrak{J}_0.$$

Comme bien sûr $\mathfrak{m}^\nu\mathcal{A} \subset \mathfrak{M}$, on a

$$\mathfrak{m}^\nu\mathcal{A} + \mathfrak{J}_\nu \subset \mathfrak{M}^\nu$$

et cela conclut la démonstration. □

Proposition 3.3.1 *Soit R un anneau local complet et noethérien de corps résiduel k de caractéristique $p > 0$. Alors, le foncteur $\Gamma \mapsto \Gamma(p)$ est une équivalence entre la catégorie des groupes de Lie formels divisibles et commutatifs sur R et la catégorie des groupes p-divisibles connexes sur R.*

DÉMONSTRATION (esquisse, cf. les exposés $\mathrm{VII_A}$ et $\mathrm{VII_B}$ de Gabriel dans [2]) : Ayant un système fondamental de voisinages de 0 pour la topologie $\mathfrak{M}$-adique, l'anneau $\mathcal{A}$ est évidemment complet (pour la topologie $\mathfrak{M}$-adique). L'application

$$\mathcal{A} \to \lim_{\infty \leftarrow \nu} (\mathcal{A}/\mathfrak{J}_\nu) = \lim_{\infty \leftarrow \nu} (A_\nu)$$

est donc bijective. Si Γ et Γ' sont deux groupes de Lie formels correspondant à $\mathcal{A}$ et $\mathcal{A}'$, l'application $\mathrm{Hom}_R(\Gamma, \Gamma') \to \mathrm{Hom}_R(\Gamma(p), \Gamma'(p))$ induite par le foncteur en question est donc bijective. Autrement dit, le foncteur $\Gamma \to \Gamma(p)$ est pleinement fidèle.
Pour compléter la démonstration, il reste à montrer que tout groupe p-divisible connexe sur R est de la forme $\Gamma(p)$ à isomorphisme près, pour un groupe de Lie formel Γ sur R. Écrivons $G = (G_\nu, i_\nu)$ et $G_\nu = \mathrm{Spec}\, A_\nu$. Les inclusions $i_\nu : G_\nu \to G_{\nu+1}$ font de $(A_\nu)_\nu$ un syst'eme projectif. Posons alors

$$A = \lim_{\infty \leftarrow \nu} A_\nu.$$

La loi de groupes de G définit un morphisme $A \to A \hat{\otimes}_R A$ et si on réussit à montrer que A est isomorphe à $R[[X_1, \ldots, X_n]]$ pour $n \in \mathbb{N}$ convenable, on aura les propriétés exigées pour un groupe de Lie formel Γ. Ceci démontré, on voit que A est un module libre de rang fini sur A via ψ, ce qui veut dire que Γ est divisible et G est isomorphe à $\Gamma(p)$.
Afin de démontrer que A est une algèbre de séries entières sur R, on remarque d'abord que le R-module A est plat en tant que limite directe des R-modules A_ν qui sont plats parce que libres de type fini sur R (voir [7, pp.253-4]). Cela permet, grâce au lemme de Hensel de se ramener au cas où $R = k$ est un corps de caractéristique $p > 0$.
Dans ce cas, les limites directes de schémas en groupes finis et commutatifs d'ordre une puissance de p constituent une catégorie abélienne et un groupe p-divisible sur k est un objet dans cette catégorie sur lequel l'application $\mathbf{p}$ est une isogénie. Il existe un foncteur exact dans cette catégorie, qui associe à un schéma en groupe G son schéma en groupe de Frobenius $\mathbb{F}_k(G) =: G^{(p)}$ et qui conserve l'ordre des objets finis. À côté de cela, il existe des homomorphismes de foncteurs $\mathbf{f}$ (induit par le morphisme de Frobenius $\mathbf{f}_{G/k}$) et $\mathbf{V}$ (Verschiebung), tels que le diagramme suivant est commutatif pour tout G de la catégorie :

$$\begin{array}{ccc} G & \xrightarrow{\mathbf{p}} & G \\ & {\scriptstyle \mathbf{f}} \searrow \quad \nearrow {\scriptstyle \mathbf{V}} \quad \searrow {\scriptstyle \mathbf{f}} & \\ & G^{(p)} \xrightarrow{\mathbf{p}} G^{(p)} & \end{array} \tag{7}$$

(cf. [1, p.98], ou [2, exposé VII], ou [10, pp.18-19]). Si le groupe G est p-divisible de hauteur h, alors $\mathbb{F}_k(G)^{(p)}$ l'est aussi, et comme le morphisme $\mathbf{p}$ est surjectif (c'est une isogénie) de noyau d'ordre p^h, le diagramme montre que les morphismes $\mathbf{f}$ et $\mathbf{V}$ sont surjectifs d'ordre $\leq p^h$.
Retournons au groupe p-divisible connexe G sur k considéré plus haut. Pour tout ν soit H_ν le noyau de

$$\mathbf{f}^\nu : G \to \mathbb{F}_k(G)^{(p^\nu)}.$$

Par conséquent, on a $H_\nu = \mathrm{Ker}(\mathbf{f}^\nu) \subset \mathrm{Ker}(p^\nu) = G_\nu$ et puisque G_ν est fini et connexe et la suite (H_ν) strictement croissante (par rapport à l'inclusion), on a aussi $G_\nu \subset H_N$ pour $N \in \mathbb{N}$ assez grand dépendant de ν. Donc par passage aux limites, on obtient

$$A = \lim_{\infty \leftarrow \nu} A_\nu = \lim_{\infty \leftarrow \nu} B_\nu,$$

où $H_\nu = \mathrm{Spec}\, B_\nu$. Soient $\mathfrak{I}_\nu$ l'idéal d'augmentation de l'algèbre B_ν (dans ce cas, l'idéal maximal) et

$$\mathfrak{I} = \lim_{\infty \leftarrow \nu} \mathfrak{I}_\nu$$

l'idéal d'augmentation de A et soient $x_1, \ldots, x_n \in \mathfrak{I}$ dont les images canoniques forment une k-base de $\mathfrak{I}_1/\mathfrak{I}_1^2$. L'application $\mathfrak{I}_\nu/\mathfrak{I}_\nu^2 \to \mathfrak{I}_1/\mathfrak{I}_1^2$ est bijective. La surjectivité est claire et son noyau est nul, parce que H_1 est le noyau de $\mathbf{f}$ dans H_ν : le noyau de $\mathfrak{I}_\nu \to \mathfrak{I}_1$ est engendré par les

puissances p-ièmes des éléments de $\mathfrak{I}_\nu$ et il est donc dans $\mathfrak{I}_\nu^2$. Cela entraîne que les images des x_i dans B_ν engendrent $\mathfrak{I}_\nu$ pour tout ν. Considérons maintenant les homomorphismes

$$u_\nu : k[X_1, \ldots, X_n] \to B_\nu$$

envoyant X_i sur l'image de x_i dans B_ν. D'après ce qui précède, ils sont surjectifs. D'autre part, le noyau de u_ν contient les éléments $X_i^{p^\nu}$ car $\mathbf{f}^\nu$ tue H_ν, donc $x_i^{p^\nu}$ est nul dans B_ν. Mais si on applique $\mathbf{f}$ succesivement on voit que $\operatorname{rang}(B_\nu) = \operatorname{rang}(B_1)^\nu$ (puisque $\mathbf{f}$ est surjectif), et en appliquant la théorie des groupes finis tués par le morphisme de Frobenius, on voit que $\operatorname{rang}(B_1) = p^n$. D'emblée, on voit que l'idéal $(X_1^{p^\nu}, \ldots, X_n^{p^\nu})_{k[X]}$ est de codimension $p^{n\nu}$ dans $k[X] = k[X_1, \ldots, X_n]$. Comme $k[X_1, \ldots, X_n] \cong \operatorname{Im}(u_\nu) \oplus \ker(u_\nu)$, on a $\operatorname{codim} \operatorname{Ker}(u_\nu) = \dim \operatorname{Im}(u_\nu) = \operatorname{rang} B_\nu = p^{n\nu} = \operatorname{codim}(X_1^{p^\nu}, \ldots, X_n^{p^\nu})_k[X]$ et il en résulte que $(X_1^{p^\nu}, \ldots, X_n^{p^\nu})_{k[X]}$ est le noyau de u_ν. En conséquence, les u_ν induisent un isomorphisme

$$u : k[[X_1, \ldots, X_n]] \tilde{\to} A,$$

et on a fini. □

Soit maintenant $G = (G_\nu, i_\nu)$ un groupe p-divisible sur l'anneau local, complet et noethérien R. Les composantes connexes G_ν^0 déterminent un groupe p-divisible connexe G^0. Des suites canoniques

$$0 \to G_\nu^0 \to G_\nu \to G_\nu^{\text{et}} \to 0$$

on déduit une suite exacte

$$0 \to G^0 \to G \to G^{\text{et}} \to 0, \tag{8}$$

où G^{et} est un groupe p-divisible étale. La dimension du groupe de Lie formel correspondant à G^0 est par définition la dimension que G.

Lemme 3.3.2 *Soit $\mathcal{A}'$ une copie de $\mathcal{A}$ et $\varphi : \mathcal{A}' \to \mathcal{A}$ une application telle que $\mathcal{A}$ devient une $\mathcal{A}'$-algèbre via ϕ. Soient Ω et Ω' les modules de différentiels formels de $\mathcal{A}$ et $\mathcal{A}'$. En choissisant des bases de Ω et Ω', on obtient des éléments de base ϑ et ϑ' de $\Lambda^n\Omega$ et $\Lambda^n\Omega'$ respectivement. Soit $\mathrm{d}\varphi(\vartheta') = a\vartheta$, avec $a \in \mathcal{A}$. Alors, le discriminant de $\mathcal{A}$ sur $\mathcal{A}'$ est engendré par $\mathrm{N}_{\mathcal{A}/\mathcal{A}'}(a)$.*

Démonstration : La démonstration s'appuie sur l'existence d'une application trace $\mathrm{Tr} : \Lambda^n\Omega \to \Lambda^n\Omega'$ avec les propriétés suivantes :
(i) Tr est $\mathcal{A}'$-linéaire.
(ii) L'application $a \mapsto (\vartheta \mapsto \mathrm{Tr}(a\vartheta))$ établit un isomorphisme de $\mathcal{A}$-modules

$$\mathcal{A} \tilde{\to} \operatorname{Hom}_{\mathcal{A}'}(\Lambda^n\Omega, \Lambda^n\Omega').$$

(iii) Si $\vartheta \in \Omega'$ et $a \in \mathcal{A}$, alors

$$\mathrm{Tr}(a \cdot \mathrm{d}\varphi(\vartheta)) = (\mathrm{Tr}_{\mathcal{A}/\mathcal{A}'}(a))\vartheta.$$

Une telle application de trace existe chaque fois que $\mathcal{A} \cong \mathcal{A}' \cong R[[X_1, \ldots, X_n]]$ et que $\varphi : \mathcal{A}' \to \mathcal{A}$ est un morphisme de R-algèbres tel que $\mathcal{A}$ devient un $\mathcal{A}'$-module libre de rang fini. Pour plus de détails voir par exemple [8]. □

Proposition 3.3.2 *Le discriminant de A_ν sur R est engendré par $p^{n\nu p^{h\nu}}$, où $h = \mathrm{ht}(G)$ et $n = \dim(G)$.*

Démonstration : En général, pour un groupe fini $H = \operatorname{Spec} B$ sur R on dénote $\mathrm{disc}(H)$ le discriminant de B sur R. Si $0 \to H' \to H \to H'' \to 0$ est une suite exacte de groupes finis sur R d'ordres m', m et m'', alors par transitivité du discriminant on voit que

$$\mathrm{disc}(H) = \mathrm{disc}(H')^{m''} \cdot \mathrm{disc}(H'')^{m'}.$$

Bien sûr, $\mathrm{disc}(H) = (1)$ si H est étale. Comme on dispose pour un groupe p-divisible d'une suite exacte de la forme (8), ces deux faits permettent de se ramener au cas d'un groupe connexe $G \cong \Gamma(p)$, car

$$\mathrm{disc}(G_\nu) = \mathrm{disc}(G_\nu^0)^{p^{\nu h^0}} \cdot \mathrm{disc}(G_\nu^{\text{et}})^{p^{\nu h^{\text{et}}}} = \mathrm{disc}(G^0)^{m^0}.$$

D'après la démonstration de Proposition (3.3.1), on a alors $A_\nu = \mathcal{A}/\mathfrak{J}_\nu$. Comme on a déjà fait, on considère $\mathcal{A}$ comme $\mathcal{A}$-module libre de rang $p^{\nu h}$ via le morphisme d'algèbres $\varphi = \psi^\nu$. Pour éviter la confusion, on précise les notations : on considère $\mathcal{A}$ via φ comme algèbre sur une copie $\mathcal{A}'$ de $\mathcal{A}$. Avec l'idéal d'augmentation $\mathfrak{I}'$ de $\mathcal{A}'$ engendré par les X_i', on a

$$A_\nu = \mathcal{A}/\mathfrak{I}'.\mathcal{A}\ (= \mathcal{A}/\varphi(\mathfrak{I}')\mathcal{A})\,.$$

Par conséquent, il suffit de démontrer que le discriminant de $\mathcal{A}$ sur $\mathcal{A}'$ est engendré par la puissance de p en question.
On considère comme dans le lemme précédent les modules de différentielles formelles de $\mathcal{A}$ et $\mathcal{A}'$, qui sont des modules libres sur $\mathcal{A}$ et $\mathcal{A}'$ respectivement engendrés par les différentielles formelles $\mathrm{d}X_i$ et $\mathrm{d}X_i'$ pour $1 \leq i \leq n$. Le morphisme $\varphi : \mathcal{A}' \to \mathcal{A}$ induit une application $\mathcal{A}'$-linéaire $\mathrm{d}\varphi : \Omega' \to \Omega$. Le choix de bases de Ω et Ω' fournit des élément ϑ et ϑ' de $\Lambda^n\Omega$ et $\Lambda^n\Omega$. Soit $\mathrm{d}\varphi(\vartheta') = a\vartheta$ avec $a \in \mathcal{A}$. On va montrer que $a = p^{n\nu}$.
On peut choisir une base (ω_i) de Ω qui se compose de différentielles invariantes par translation, plus précisément, si la comultiplication

$$\mu : \mathcal{A} \to \mathcal{A}\hat{\otimes}_R\mathcal{A}$$

définit la structure de groupes formelle, alors $\mathrm{d}\mu : \Omega \to \Omega \oplus \Omega$ satisfait

$$\mathrm{d}\mu(\omega_i) = \omega_i \oplus \omega_i.$$

Pour la base correspondant (ω_i') dans la copie Ω' de Ω, on obtient l'égalité $\mathrm{d}\varphi(\omega_i') = p^\nu\omega_i$ par définition de φ (qui provient du morphisme $p^\nu : \Gamma \to \Gamma$). Donc, si on passe à $\Lambda^n\Omega$ et $\Lambda^n\Omega'$, on voit que $a = p^{n\nu}$. Puisque le rang de $\mathcal{A}$ sur $\mathcal{A}'$ est $p^\nu h$. On a $\mathrm{N}_{\mathcal{A}/\mathcal{A}'}(a) = a^{p^{h\nu}} = p^{n\nu p^{h\nu}}$ et l'énoncé de la proposition résulte du Lemme (3.3.2). □

3.4 Dualité pour les groupes p-divisibles

Soit $G = (G_\nu, i_\nu)$ un groupe p-divisible sur R. Pour tout ν note G_ν^D le dual de Cartier de G_ν. La suite exacte (6) avec $\mu = 1$ montre que l'on a des monomorphismes

$$j_\nu^D : G_\nu^D \to G_{\nu+1}^D,$$

où j_ν^D est le dual de l'application $j_{1,\nu} : G_{\nu+1} \to G_\nu$ induite par la multiplication par p. On a déjà vu que les G_ν^D sont des schémas en groupes des même ordres que les G_ν respectivement. C'est-à-dire, on a un système inductif

$$G^D = (G_\nu^D, j_\nu^D)_{\nu\geq 0}$$

tel que G_ν^D est un schéma en groupe fini sur R d'ordre $p^{\nu h}$. On a une suite exacte

$$0 \to G_\nu^D \xrightarrow{j_{1,\nu}^D} G_{\nu+1}^D \xrightarrow{i_{1,\nu}^D} G_1^D \to 0.$$

Et comme $p^\nu = j_{\nu,1}^D \cdot i_{1,\nu}^D$ on voit que $\mathrm{Ker}\, p^\nu = \mathrm{Ker}\, i_{1,\nu}^D = \mathrm{Im}\, j_{1,\nu}^D$, et la suite

$$0 \to G_\nu^D \xrightarrow{j_\nu^D} G_{\nu+1}^D \xrightarrow{p^\nu} G_{\nu+1}^D$$

est exacte. Donc, G^D est un groupe p-divisible, le *dual* de G. Comme G_ν et G_ν^D ont le même ordre pour tout ν, les groupes G et G^D ont la même hauteur. Si l'anneau de base R est complet, local et noethérien de caractéristique résiduelle $p > 0$ (comme dans la partie (3.3), de sorte que la dimension de G est définie), on a :

Proposition 3.4.1 *Soient n et n^D les dimensions de G et de son dual G^D. Alors, $n + n^D = h$, la hauteur de G et G^D.*

DÉMONSTRATION : La dimension et la hauteur de G ne changent pas si on réduit G modulo l'idéal maximal de R (voir démonstration de la Proposition (3.3.1). On peut donc se ramener au cas où $R = k$ est un corps de caractéristique $p > 0$. Du diagramme (7) on déduit que $\operatorname{Ker}\mathbf{V} \cong \operatorname{Ker}\mathbf{p}/\operatorname{Ker}\mathbf{f}$ et donc une suite exacte

$$0 \to \operatorname{Ker}\mathbf{f} \to \operatorname{Ker}\mathbf{p} \to \operatorname{Ker}\mathbf{V} \to 0.$$

Mais, $\operatorname{Ker}\mathbf{p} = G_1$ est d'ordre p^h et $\operatorname{Ker}\mathbf{f}$ est d'ordre p^n. En effet, $\mathbf{f}$ est injectif sur G^{et}, donc son noyau sur G est aussi son noyau sur la composante connexe G^0 et on peut identifier $\operatorname{Ker}\mathbf{f}$ avec un groupe de Lie formel de n paramètres. Une remarque dans la démonstration de la Proposition (3.3.1) montre que l'ordre de $\operatorname{Ker}\mathbf{f}$ est p^n. Puisque $\mathbf{f}$ et $\mathbf{V}$ sont en dualité par rapport à la dualité de Cartier, $\operatorname{Ker}\mathbf{V}$ est le dual de Cartier du co-noyau de l'application $\mathbf{f} : G_\nu^D \to \mathbb{F}_k(G^D) = \mathbb{F}_k(G)^D$. En conséquence, $\operatorname{Ker}\mathbf{V}$ est d'ordre p^{n^D}.Par la multiplicativité des ordres dans une suite exacte, on a alors $p^h = p^n \cdot p^{n^D}$, d'où l'énoncé. □

Exemples. (d) Pour le groupe p-divisible $\mathbb{G}_m(p)$, on a $h = n = 1$. Son dual est le groupe p-divisible étale $\mathbb{Q}_p/\mathbb{Z}_p$ pour lequel on a $h = 1$ et $n = 0$.

(e) Soit X un schéma abélien de dimension n sur R. Si le schéma dual X^D existe, on observe qu $(X(p))^D \cong X^D(p)$. Les groupes $X(p)$ et $X^D(p)$ sont de hauteur $2n$ et de dimension n. La partie connexe $X^0(p)$ de $X(p)$ est la complétion formelle de X le long de la section nulle et est de hauteur comprise entre n et $2n$. Par exemple, si X est une courbe elliptique ($n = 1$) alors la hauteur de $X(p)^0$ est 1 ou 2 selon que l'invariant de Hasse de $X(p)$ est non-nul ou nul.

3.5 Le module et le co-module de Tate

Soit R un anneau complet de valuation discrète de corps résiduel $k = R/\mathfrak{m}$ de caractéristique $p > 0$, et soit K le corps de faction de R. Soit L la completion d'une extension algébrique (pas forcément finie) de K. L'anneau des entiers $\mathcal{O}_L$ est un anneau de valuation, complet et de rang 1. Cependent, sa valuation n'est pas discrète en général.

Soit G un groupe p-divisible sur R. On définit le groupe $G(\mathcal{O}_L)$ de points de G à valeurs dans $\mathcal{O}_L$ par

$$G(\mathcal{O}_L) = \varprojlim_{\infty \leftarrow i} G(\mathcal{O}_L/\mathfrak{m}^i\mathcal{O}_L),$$

où $\mathfrak{m}$ est l'idéal maximal de R et où

$$G(\mathcal{O}_L/\mathfrak{m}^i\mathcal{O}_L) = \varprojlim_{\nu \to \infty} G_\nu(\mathcal{O}_L/\mathfrak{m}^i\mathcal{O}_L).$$

Évidemment, $G(\mathcal{O}_L)$ est un $\mathbb{Z}_p$-module. La définition des groupes p-divisibles implique que le groupe $G_\nu(\mathcal{O}_L/\mathfrak{m}^i\mathcal{O}_L)$ est le noyau de la multiplication par p^ν dans $G(\mathcal{O}_L/\mathfrak{m}^i\mathcal{O}_L)$. Par conséquent, le noyau de la multiplication par p^ν dans $G(\mathcal{O}_L)$ est $\varprojlim_{\infty \leftarrow i} G_\nu(\mathcal{O}_L/\mathfrak{m}^i\mathcal{O}_L) \cong G_\nu(\mathcal{O}_L)$, et le sous-groupe de torsion de $G(\mathcal{O}_L)$ est

$$G(\mathcal{O}_L)_{\text{tors}} \cong \varprojlim_{\nu \to \infty} G_\nu(\mathcal{O}_L).$$

Généralement, on ne peut donc pas échanger les deux limites. Par contre, si G est étale sur R, alors les applications $G_\nu(\mathcal{O}_L/\mathfrak{m}^{i+1}\mathcal{O}_L) \to G_\nu(\mathcal{O}_L/\mathfrak{m}^i\mathcal{O}_L)$ sont bijectives pour tout $i \in \mathbb{N}$. Maintenant, on voit facilement, que $G(\mathcal{O}_L)$ est une groupe de torsion si G est étale (on a $G(\mathcal{O}_L)_{\text{tors}} \cong \varprojlim_{\nu\to\infty} G_\nu(\mathcal{O}_L) \cong \varprojlim_{\nu\to\infty}\varprojlim_{\infty\leftarrow i} G_\nu(\mathcal{O}_L/\mathfrak{m}^i\mathcal{O}_L) = \varprojlim_{\infty\leftarrow i}\varprojlim_{\nu\to\infty} G_\nu(\mathcal{O}_L/\mathfrak{m}^i\mathcal{O}_L) = \varprojlim_{\infty\leftarrow i} G(\mathcal{O}_L/\mathfrak{m}^i\mathcal{O}_L) = G(\mathcal{O}_L)$).

En général, si $G_\nu = \operatorname{Spec} A_\nu$ et $A = \varprojlim_{\infty\leftarrow\nu} A_\nu$ et $A_\nu \cong A/\mathfrak{J}_\nu$, alors un point $x \in G(\mathcal{O}_L)$ peut s'identifier à un homomorphisme $A \to \mathcal{O}_L$ qui est continu pour la topologie de la valuation dans $\mathcal{O}_L$ et la topologie définie par les idéaux $\mathfrak{m}^i A + \mathfrak{J}_\nu$ dans A. En particulier, si G est connexe correspondant à un groupe de Lie formel Γ, tel que $A \cong R[[X_1, \ldots, X_n]]$, alors par le Lemme (3.3.1) et par ce que l'on a dit auparavant, $G(\mathcal{O}_L)$ est le groupe de points $x = (x_1, \ldots, x_n)$ de Γ à coordonnées x_i dans l'idéal maximal de $\mathcal{O}_L$. En particulier, si G est connexe, alors $G(\mathcal{O}_L)$ est un groupe analytique.

On considère maintenant la suite exacte (8), et soient A^{et} et A^0 les algèbres de G^{et} et G^0.

Proposition 3.5.1 *Si le corps résiduel k de R est parfait, alors l'application $G \to G^{\mathrm{et}}$ admet une section formelle et donc la suite*

$$0 \to G^0(\mathcal{O}_L) \to G(\mathcal{O}_L) \to G^{\mathrm{et}}(\mathcal{O}_L) \to 0$$

est exacte.

Démonstration : Si $R = k$, la suite exacte (8) est canoniquement scindée et par conséquence on a les identifications

$$A \cong A^0 \hat{\otimes}_R A^{\mathrm{et}} \cong A^{\mathrm{et}}[[X_1, \ldots, X_n]]$$

mais par plattitude de A sur R, on a les mêmes identités dans le cas général : grâce à cela la suite mentionnée est toujours scindée. En conséquence, la suite

$$0 \to G^0(\mathcal{O}_L) \to G(\mathcal{O}_L) \to G^{\mathrm{et}}(\mathcal{O}_L) \to 0$$

est exacte. □

Corollaire 3.5.1 *Si $x \in G(\mathcal{O}_L)$, alors il existe une extension L' de L et un élément $y \in G(\mathcal{O}_{L'})$, tel que $py = x$.*

Démonstration : D'après la proposition précédents, il suffit de prouver l'énoncé pour G^{et} et G^0 séparément. Pour la partie connexe, il est induit par le fait que l'application $\mathbf{p} : G^0 \to G^0$ fait de A^0 un A^0-module libre de rang fini, en particulier $\mathbf{p}$ est surjectif et donc on trouve un élément $y \in G^0(\mathcal{O}_{L'})$ avec cette propriété. Pour la partie étale, on peut encore supposer que $R = k$, et la surjectivité des application $G_{\nu+1} \xrightarrow{j_{1,\nu}} G_\nu$ induites par la multiplication par p donne le résultat voulu. □

Corollaire 3.5.2 *Si L est algébriquement clos, alors $G(\mathcal{O}_L)$ est divisible.*

Démonstration : La surjectivité de $\mathbf{p} : G(\mathcal{O}_L) \to G(\mathcal{O}_L)$ résulte du corollaire précédent. Comme son noyau est fini, on a la divisibilité de $G(\mathcal{O}_L)$. □

Désormais, on suppose que le corps résiduel k de R est parfait et la caractéristique de son corps de fractions K soit nulle. Cette dernière hypothèse est particulièrement importante pour la suite, car premièrement, elle permet de décrire $G(\mathcal{O}_L)$ localement comme $L^{\dim G}$ à travers une appication logarithme ; deuxièmement, les $G_\nu \times_R K$ sont automatiquement étales, donc $G_\nu(\mathcal{O}_L)$ (isomorphe $G_\nu(L)$ comme G_ν est fini est plat sur sur R) est isomorphe à $(\mathbb{Z}/p^\nu\mathbb{Z})^h$ pour L assez grand (dépendant de ν).

On va d'abord introduire le *logarithme*. L'*espace tangent de G* à l'origine est par définition l'espace tangent du groupe de Lie formel Γ correspondant à G^0 à l'origine. On note $t_G(L)$ ses points à coefficients dans L. Un tel point est une application R-linéaire $\tau : A^0 \to L$ telle que

$$\tau(fg) = f(0)\tau(g) + g(0)\tau(f) \quad \text{pour tout } f, g \in A^0 \cong R[[X_1, \ldots, X_n]],$$

où de façon équivalente, c'est une application R-linéaire de $\mathfrak{I}^0/(\mathfrak{I}^0)^2$ vers L où $\mathfrak{I}^0 = (X_1, \ldots, X_n)_{A^0}$ est l'idéal d'augmentation de A^0 (cette dernière est induite par la restriction de τ à $\mathfrak{I}^0$). Pour cette raison, $t_G(L)$ est un espace vectoriel de dimension $n = \dim G$ sur L. On définit l'application logarithme $\log : G(\mathcal{O}_L) \to t_G(L)$ par la formule

$$(\log x)(f) = \lim_{i \to \infty} \left(\frac{f(p^i x) - f(0)}{p^i} \right) \quad \text{pour } x \in G(\mathcal{O}_L) \text{ et } f \in A^0.$$

Remarquons que pour i grand, on a $p^i x \in G^0(\mathcal{O}_L)$, car $G^{\mathrm{et}}(\mathcal{O}_L)$ est de torsion. Mais il y a une autre définition. On peut identifier $\mathfrak{I}^0/(\mathfrak{I}^0)^2$ avec l'espace de formes différentielles ω sur Γ et définir pour $s \in G^0(\mathcal{O}_L)$

$$(\log x)(\omega) = \Omega(x),$$

où $\Omega(X) \in K[[X_1, \ldots, X_n]]$ est tel que $\Omega(0) = 0$ et $\mathrm{d}\Omega = \omega$ (voir [16]). L'application ainsi définie est bien-définie car Ω est unique par le Lemme de Poincaré Formel. Le logarithme est un

homomorphisme $\mathbb{Z}_p$-linéaire et un isomorphisme local. Autrement dit, si $c^{p-1} < |p|$, le logarithme fournit un isomorphisme entre le groupe de points $x = (x_i)$ dans $G^0(\mathcal{O}_L)$ avec $|x_i| \leq c$ pour tout $i \in \{1, \ldots, n\}$ et le groupe de points $\tau \in t_G(L)$ avec $|\tau(X_i)| \leq c$ pour tout i. On en déduit, que le noyau du logarithme est le sous-groupe de torsion de $G(\mathcal{O}_L)$ et que son co-noyau est de même un groupe de torsion. Pour résumer, on dispose d'un isomorphisme

$$G(\mathcal{O}_L) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \tilde{\to} t_G(L).$$

L'image de $G(\mathcal{O}_L)$ est contenue dans un $\mathcal{O}_L$-sous-module finiment engendré de $t_G(L)$ si la valuation de $\mathcal{O}_L$ est discrète, tandis que $\log G(\mathcal{O}_L) = t_G(L)$ si L est algébriquement clos.

Exemples. (f) Si $G = \mathbb{G}_m(p) = (\mu_{p^\nu}, i_\nu)$, alors $G(\mathcal{O}_L)$ est le groupe des unités congrues à 1 dans $\mathcal{O}_L$, comme sa hauteur est 1 (cf. exemple (b)) on a $t_G(L) = L$ et le logarithme est le logarithme p-adique habituel $\log_p$.

(g) Soit X un schéma abélien sur R et $G = X(p)$. On peut identifier $G(\mathcal{O}_L)$ avec le sous-groupe de $X(\mathcal{O}_L)$ qui consiste en les points x dont la réduction modulo l'idéal maximal de $\mathcal{O}_L$ est d'une puissance finie de p. Dans ce cas, on identifie $G^0(\mathcal{O}_L)$ au noyau de l'application de réduction. L'application logarithme fut étudiée dans le cas général par A. Mattuck [11], et pour les courbes elliptiques par E. Lutz [9].

On note $\overline{K}$ une clôture algébrique de K. Si X est un schéma en groupe commutatif ou un groupe formel sur R, on peut définir le *module de Tate* de X par

$$T_p(X) = \lim_{\infty \leftarrow \nu} \left(\mathrm{Ker}(X(\overline{K}) \xrightarrow{p^\nu} X(\overline{K}) \right).$$

Si $X = \lim_{\nu \to \infty} G_\nu = G$ est p-divisible, alors

$$T_p(G) = \lim_{\infty \leftarrow \nu} G_\nu(\overline{K}).$$

Dans ce cas, on peut aussi définir le *co-module de Tate* par

$$\Phi_p(G) = \lim_{\nu \to \infty} G_\nu(\overline{K}).$$

Comme on a supposé que la caractéristique de K est nulle, les $G_\nu \otimes_R K$ sont étales et par définition des groupes p-divisibles, on sait que $\Phi_p(G)$ et $T_p(G)$ sont des $\mathbb{Z}_p$-modules isomorphes à $(\mathbb{Q}_p/\mathbb{Z}_p)^h$ et $\mathbb{Z}_p^h$ respectivement (où h est la hauteur de G), sur lesquels l'action du groupe de Galois $\mathrm{Gal}(\overline{K}/K)$ est continue. On a des isomorphismes canoniques

$$\Phi_p(G) \cong T_p(G) \otimes_{\mathbb{Z}_p} (\mathbb{Q}_p/\mathbb{Z}_p) \quad \text{et} \quad T_p(G) \cong \mathrm{Hom}_{\mathbb{Z}_p}(\mathbb{Q}_p/\mathbb{Z}_p, \Phi_p(G)),$$

en conséquence, si on connaît $T_p(G)$ on connaît $\Phi_p(G)$ et vice versa. En outre, la connaissance d'un des deux équivaut à la connaissance de la fibre générique $G \otimes_R K$ du groupe p-divisible G. En effet, comme $G_\nu \otimes_R K$ est étale parce que K est de caractéristique nulle, il est déterminé par le module de Galois $(G_\nu \otimes_R K)(\overline{K})$, c'est-à-dire par $G_\nu(\overline{K})$. Cependant, on a $T_p(G)/p^\nu T_p(G) = G_\nu(\overline{K})$ per definitionem du module de Tate : le module de Tate détermine la fibre générique et vice versa.

Remarquons, que les applications $G_\nu(\mathcal{O}_L) \to G_\nu(L)$ sont bijectives, donc le co-module de Tate $\Phi_p(G)$ est le groupe de torsion de $G(\mathcal{O}_L)$ si L est une complétion de K.

Exemples. (h) Si $G = \mathbb{G}_m(p)$, alors $\Phi_p(\mathbb{G}_m(p)) = \lim_{\nu \to \infty} \mathrm{Ker}(\mathbb{G}_m(p) \xrightarrow{p^\nu} \mathbb{G}_m(p)) = \left\{ x \in \mathbb{G}_m(p)^\times | \exists \nu : x^{p^\nu} = 1 \right\}$ les racines de l'unité d'ordre une puissance de p dans $\overline{K}$. On note

$$\mathbb{Z}_p(1) = T_p(\mathbb{G}_m(p)).$$

Dans ce cadre, on définit aussi le caractère cyclotomique

$$\chi_{\mathrm{cycl}} : \mathrm{Gal}(\overline{K}/K) \to \mathbb{Z}_p^\times$$

par son action $\gamma(\zeta_{p^n}) = \zeta_{p^n}^{\chi_{\mathrm{cycl}}}$.

(i) Si X est un schéma abélien de dimension n sur R, et $G = X(p)$, alors $T_p(G) = T_p(X)$ est l'espace de la représentation p-adique de rang $h = 2n$ introduite par Weil.

4 Théorèmes sur les groupes p-divisibles

4.1 La décomposition de Hodge-Tate

Soit G un groupe p-divisible sur un anneau de valuation discrète R qui est complet et de caractéristique mixte. Rappelons que l'on note K le corps de fractions de R et C la complétion d'une clôture algébrique de K. Si G^D désigne le dual de G, la dualité de Cartier (voir sous-section (2.2)) entraîne

$$G_\nu^D(\mathcal{O}_C) \tilde{\to} \mathrm{Hom}_{\mathcal{O}_C}(G_\nu \otimes_R \mathcal{O}_C, \mathbb{G}_m \otimes_R \mathcal{O}_C) \quad \text{pour tout } \nu \in \mathbb{N}.$$

En passant à la limite projective quand $\nu \to \infty$, on obtient un isomorphisme

$$T_p(G^D) \tilde{\to} \mathrm{Hom}_{\mathcal{O}_C}\left(G\hat{\otimes}_R\mathcal{O}_C, \mathbb{G}_m(p)\hat{\otimes}_R\mathcal{O}_C\right)$$

où $\mathbb{G}_m(p)$ est le groupe p-divisible de $\mathbb{G}_m$. On en obtient des accouplement

$$T_p(G^D) \times G(\mathcal{O}_C) \to (\mathbb{G}_m(p))(\mathcal{O}_C) \cong U$$

et

$$T_p(G^D) \times t_G(C) \to t_{\mathbb{G}_m(p)}(C) \cong C,$$

où U dénote le groupe des unités congrues à 1 dans $\mathcal{O}_C$ (cf. example (f) de la sous-section (3.5)). Cet exemple montre aussi que les accouplements sont compatibles avec l'application logarithmique $\log : G(\mathcal{O}_C) \to t_G(C)$ introduite dans la partie (3.5) et le logarithme p-adique habituel $\log_p : U \to C$. Les noyaux de ces aplications logarithmes sont les groupes de torsion de leurs domaines de définition. Comme le logarithme est un isomorphisme local et C est algébriquement clos et $t_G(C)$ un espace vectoriel sur C, la propriété de divisibilité implique qu'elles sont surjectives. Ainsi on obtient un diagramme commutatif exact

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \Phi_p(G) & \longrightarrow & G(\mathcal{O}_C) & \xrightarrow{\log} & t_G(C) & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \alpha_0} & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \mathrm{d}\alpha} & & \\ 0 & \longrightarrow & \mathrm{Hom}_{\mathbb{Z}_p}(T_p(G^D), U_{\mathrm{tors}}) & \longrightarrow & \mathrm{Hom}_{\mathbb{Z}_p}(T_p(G^D), U) & \xrightarrow[\log_p]{} & \mathrm{Hom}_{\mathbb{Z}_p}(T_p(G^D), C) & \longrightarrow & 0, \end{array} \tag{9}$$

où $T_p(G^D)$ est libre de rang $h =$ hauteur de $G^D =$ hauteur de G sur $\mathbb{Z}_p$, où $U_{\mathrm{tors}} \cong \Phi_p(\mathbb{G}_m(p))$ est le groupe de racines de l'unité dans U (voir sous-section (3.5), exemple (c)). Les flèches verticales sont $\mathrm{Gal}(\overline{K}/K)$-équivariantes, l'action de $\mathrm{Gal}(\overline{K}/K)$ sur un homomorphisme f étant donnée par $(\gamma f)(x) = \gamma(f(\gamma^{-1}x))$. Celle de gauche est limite inductive de dualités parfaites et les autres des accouplements précédents.

Lemme 4.1.1 *Soit W un C-espace vectoriel muni d'une action semi-linéaire de $\mathrm{Gal}(\overline{K}/K)$, c'est-à-dire telle que $\gamma(cw) = \gamma(c)\gamma(w)$, pour $\gamma \in \mathrm{Gal}(\overline{K}/K)$, $c \in C$ et $w \in W$. Alors l'application C-linéaire*

$$W^{\mathrm{Gal}(\overline{K}/K)} \otimes_K C \to W$$

est injective.

Démonstration : Il s'agit de voir qu'un ensemble d'éléments $(w_i)_{i\in I} \in W^{\mathrm{Gal}(\overline{K}/K)}$ indépendant sur K est indépendant sur C. On considère une relation minimale non triviale $\sum_{i\in I} c_i w_i = 0$ avec $(c_i)_{i\in I} \in C$. Il faut montrer que tout les c_i sont nuls. Supposons que ce n'est pas vrai. Quitte à diviser la relation par un des coefficients non nuls, on peut supposer $c_{i_0} = 1$ pour un $i_0 \in I$. Si on applique les éléments $\gamma \in \mathrm{Gal}(\overline{K}/K)$ on obtient

$$0 = \gamma\left(\sum_{i\in I} c_i w_i\right) = \sum_{i\in I} \gamma(c_i)\gamma(w_i) = w_{i_0} + \sum_{i\in I-\{i_0\}} \gamma(c_i) w_i.$$

En formant la différence avec la somme initiale on a

$$0 = \sum_{i \in I - \{i_0\}} (\gamma(c_i) w_i - c_i w_i) = \sum_{i \in I - \{i_0\}} (\gamma(c_i) - c_i) w_i.$$

Cependant, la relation initiale était minimale et pour cela $\gamma(c_i) = c_i$ pour $i \in I - \{i_0\}$ et pour tout $\gamma \in \mathrm{Gal}(\overline{K}/K)$. Il en résulte que $c_i \in K$ pour tout $i \in I$, et donc $c_i = 0$ par hypothèse. □

Proposition 4.1.1 *Le morphisme α_0 est bijectif et α et $\mathrm{d}\alpha$ sont injectifs.*

DÉMONSTRATION : La preuve s'effectue en plusieurs étapes.
(1) *On montre d'abord que α_0 est bijectif.* En effet, on sait que $G_\nu^D(\overline{K}) = G_\nu^D(\mathcal{O}_C) = G_\nu^D(C)$. Comme K est de caractéristique 0, la dualité de Cartier fournit une dualité parfaite

$$G_\nu(C) \times G_\nu^D(C) \to \mathbb{G}_m(p)_\nu(C) \quad \text{pour tout } \nu \in \mathbb{N},$$

puisque $G_\nu \xrightarrow{\sim} \mathrm{Hom}(G_\nu^D, \mathbb{G}_m(p))$ et $G_\nu^D \xrightarrow{\sim} \mathrm{Hom}(G_\nu, \mathbb{G}_m(p))$. En passant à la limite inductive, on en déduit un isomorphisme

$$\lim_{\nu \to \infty} G_\nu(C) \to \lim_{\nu \to \infty} \mathrm{Hom}(G_\nu^D(C), \mathbb{G}_m(p)_\nu(C)) = \mathrm{Hom}(T_p(G^D), U_{\mathrm{tors}})$$

Remarquons que le passage à la limite projective fournit un isomorphisme $\mathrm{Gal}(\overline{K}/K)$-équivariant :

$$T_p(G) \cong \mathrm{Hom}\left(T_p(G^D), \mathbb{Z}_p(1)\right)$$

avec $\mathbb{Z}_p(1) = T_p(\mathbb{G}_m(p)) = \lim_{\infty \leftarrow \nu} \mu_{p^\nu}(\mathcal{O}_C)$.
(2) *Les ensembles* $\mathrm{Ker}\,\alpha$ *et* $\mathrm{Coker}\,\alpha$ *sont des espaces vectoriels sur $\mathbb{Q}_p$.* Par l'étape précédente, on a $\mathrm{Ker}\,\alpha_0 = \mathrm{Coker}\,\alpha_0 = 0$. En conséquence, le lemme de serpent appliqué au diagramme (9) montre que les noyaux (resp. les conoyaux) de α et $\mathrm{d}\alpha$ sont isomorphes. Comme $\mathrm{d}\alpha$ est C-linéaire et en particulier $\mathbb{Q}_p$-linéaire, ces quatres ensembles sont des espaces vectoriels sur $\mathbb{Q}_p$.
(3) *On a* $G(R) = G(\mathcal{O}_C)^{\mathrm{Gal}(\overline{K}/K)}$ *et* $t_G(K) = t_G(C)^{\mathrm{Gal}(\overline{K}/K)}$. On sait déjà que $K = \mathrm{H}^0(K, C) = C^{\mathrm{Gal}(\overline{K}/K)}$ par Théorème (1.3.1), ce qui implique $R = \mathcal{O}_C^{\mathrm{Gal}(\overline{K}/K)}$. D'où l'énoncé.
(4) *L'application α est injective sur $G(R)$.* D'après les étapes (3) et (2) le noyau de la restriction $\alpha|_{G(R)}$ est le $\mathbb{Q}_p$-espace vectoriel $(\mathrm{Ker}\,\alpha)^{\mathrm{Gal}(\overline{K}/K)}$ et par conséquent divisible par p de façon unique : la multiplication par p y est bijective. On traite d'abord le cas où G est connexe. On rappelle que la valuation de R est discrète. Si x est un point dans $G(R)$ dont toutes les coordonnées sont dans $\mathfrak{m}_R^i$, où $\mathfrak{m}_R$ est l'idéal maximal de R, alors les coordonnées de px sont dans $\mathfrak{m}_R^{i+1}$. Cela implique que $\bigcap p^\nu G(R) = 0$, G considéré comme groupe de Lie formel. On a donc $\mathrm{Ker}(\alpha) \cap G(R) = 0$. Pour le cas général, on utilise la fonctorialité du diagramme (9) avec $G^0 \to G$, où G^0 est la partie connexe de G, et le fait que $T_p(G^D) \to T_p((G^0)^D$ est surjectif. On voit alors que $\mathrm{Ker}\,\alpha \cap G^0(R) = 0$. Mais puisque $\mathrm{Ker}\,\alpha$ est un espace vectoriel donc sans torsion, et comme $G(R)/G^0(R)$ est de torsion, $\mathrm{Ker}\,\alpha \cap G(R) = 0$ et $\alpha|_{G(R)}$ est injectif.
(5) *Le morphisme* $\mathrm{d}\alpha$ *est injectif sur $t_G(K)$.* D'après le diagramme (9) et le point (4), $d\alpha$ est injectif sur $\log(G(R))$. Cela résulte de ce que ce dernier engendre le $\mathbb{Q}_p$-espace vectoriel $t_G(K)$.
(6) *L'application* $\mathrm{d}\alpha$ *est injective.* Il y a une factorisation de $\mathrm{d}\alpha$

$$t_G(C) \cong t_G(K) \otimes_K C \to \mathrm{Hom}_{\mathrm{Gal}(\overline{K}/K)}(T_p(G^D), C) \otimes_K C \to \mathrm{Hom}(T_p(G^D), C).$$

La flèche à gauche est injective par l'étape (5). Celle à droite l'est par le Lemme (4.1.1) comme $\mathrm{Hom}_{\mathrm{Gal}(\overline{K}/K)}(T_p(G^D), C) = \left(\mathrm{Hom}(T_p(G^D), C)\right)^{\mathrm{Gal}(\overline{K}/K)}$.
(7) *L'application α est injective.* Cela résulte immédiatement du raisonnement de l'étape (2). □

Théorème 4.1.1 *Les applications*

$$G(R) \xrightarrow{\alpha_R} \mathrm{Hom}_{\mathrm{Gal}(\overline{K}/K)}\left(T_p(G^D), U\right)$$

et

$$t_G(K) \xrightarrow{\mathrm{d}\alpha_R} \mathrm{Hom}_{\mathrm{Gal}(\overline{K}/K)}\left(T_p(G^D), C\right)$$

induites par α et par $\mathrm{d}\alpha$ *sont bijectives.*

DÉMONSTRATION : L'injectivité de ces applications fut montrée dans la Proposition (4.1.1). En outre, l'égalité $K = C^{\mathrm{Gal}[\overline{K}/K)}$ et le diagramme (9) montrent les inclusions

$$\mathrm{Coker}\,\alpha_R \subseteq (\mathrm{Coker}\,\alpha)^{\mathrm{Gal}(\overline{K}/K)} \quad \text{et} \quad \mathrm{Coker}\,\mathrm{d}\alpha_R \subseteq (\mathrm{Coker}\,\mathrm{d}\alpha)^{\mathrm{Gal}(\overline{K}/K)}.$$

Mais comme $\mathrm{Coker}\,\alpha$ et $\mathrm{Coker}\,\mathrm{d}\alpha$ sont isomorphes d'après le lemme du serpent dans le diagramme, on voit que l'application $\mathrm{Coker}\,\alpha_R \to \mathrm{Coker}\,\mathrm{d}\alpha_R$ est est injective. On peut donc se restreindre à montrer la surjectivité de $\mathrm{d}\alpha_R$. Cela revient à une question de dimensions car $\mathrm{d}\alpha_R$ est K-linéaire et injectif. On considère les C-espaces de dimension $h = \mathrm{ht}(G)$

$$\mathrm{Hom}\,(T_p(G), C) \quad \text{et} \quad \mathrm{Hom}\left(T_p(G^D), C\right)$$

sur lesquels $\mathrm{Gal}(\overline{K}/K)$ agit de façon semilinéaire. Posons

$$d^D = \dim_K \left(\mathrm{Hom}\left(T_p(G^D), C\right)^{\mathrm{Gal}(\overline{K}/K)}\right), \quad d = \dim_K \left(\mathrm{Hom}\,(T_p(G), C)^{\mathrm{Gal}(\overline{K}/K)}\right)$$

$$n = \dim G = \dim_K t_G(K), \quad n^D = \dim G^D = \dim_K t_{G^D}(K).$$

Par injectivité de $\mathrm{d}\alpha_R$ on connaît déjà les inégalités $n \leq d^D$ et $n^D \leq d$. Comme $n + n^D = h$ d'après la Proposition (3.4.1), il suffit de voir que $d + d^D \leq h$.
Comme vu dans l'étape (1) de la Proposition (4.1.1) $T_p(G) \cong \mathrm{Hom}\left(T_p(G^D), \mathbb{Z}_p(1)\right)$ et $T_p(G^D) \cong \mathrm{Hom}\,(T_p(G), \mathbb{Z}_p(1))$. En conséquence,

$$\mathrm{Hom}\left(T_p(G^D), C\right) = \mathrm{Hom}\,(\mathrm{Hom}(T_p(G), \mathbb{Z}_p(1)), C) = T_p(G) \otimes \mathrm{Hom}(\mathbb{Z}_p(1), C).$$

Par définition $\mathrm{Hom}(\mathbb{Z}_p(1), C)$ est isomorphe à $C(-1)$, le corps C muni de l'action de $\mathrm{Gal}(\overline{K}/K)$ tordue par le caractère cyclotomique inversé $\chi_{\mathrm{cycl}} : \mathrm{Gal}(\overline{K}/K) \to \mathbb{Z}_p^\times$. Ceci nous donne un accouplement $\mathrm{Gal}(\overline{K}/K)$-équivariant parfait canonique

$$\mathrm{Hom}\,(T_p(G), C) \times \mathrm{Hom}\left(T_p(G^D), C\right) \to C(-1). \tag{10}$$

D'après le Théorème (1.3.2), $C(-1)^{\mathrm{Gal}(\overline{K}/K)} = \mathrm{H}^0(\mathrm{Gal}(\overline{K}/K), C(-1)) = 0$. Étant donné que les espaces $\mathrm{Hom}\,(T_p(G), C)^{\mathrm{Gal}(\overline{K}/K)}$ et $\mathrm{Hom}\left(T_p(G^D), C\right)^{\mathrm{Gal}(\overline{K}/K)}$ sont accouplés dans $C(-1)^{\mathrm{Gal}(\overline{K}/K)}$, les sous-$C$-espaces vectoriels $\mathrm{Hom}\,(T_p(G), C)^{\mathrm{Gal}(\overline{K}/K)}\, C$ et $\mathrm{Hom}\left(T_p(G^D), C\right)^{\mathrm{Gal}(\overline{K}/K)}$ de $\mathrm{Hom}\,(T_p(G), C)$ et $\mathrm{Hom}\left(T_p(G^D), C\right)$ sont orthogonaux. D'autre part, leurs dimensions respectives sont d et d^D par le Lemme (4.1.1) : on a bien $d + d^D \leq h = \dim_C (\mathrm{Hom}(T_p(G), C)) = \dim_C \left(\mathrm{Hom}(T_p(G^D), C)\right)$ d'où le théorème. □

Corollaire 4.1.1 *Le* $\mathrm{Gal}(\overline{K}/K)$*-module* $T_p(G)$ *détermine la dimension* n *de* G*.*

DÉMONSTRATION : Le module de Tate $T_p(G)$ détermine la fibre générique $G \otimes_R K$. En outre, on sait que $G^D \otimes_R K = (G \otimes_R K)^D$. Donc, $T_p(G)$ détermine $G^D \otimes_R K$ et $T_p(G^D)$. Mais d'après le Théorème (4.1.1) on a$n = \dim_K (t_G(K)) = \dim_K \left(\mathrm{Hom}_{\mathrm{Gal}(\overline{K}/K)}(T_p(G^D), C)\right)$. □

Corollaire 4.1.2 (Décomposition de Hodge-Tate). *Le* $\mathrm{Gal}(\overline{K}/K)$*-module* $\mathrm{Hom}\,(T_p(G), C)$ *est canoniquement isomorphe à la somme directe*

$$t_{G^D}(C) \oplus t_G^*(C) \otimes_C C(-1),$$

où t_G^* *est l'espace co-tangent de* G *à l'origine.*

DÉMONSTRATION : Vide supra (discussion précédant la Proposition (4.1.1) que les applications $\mathrm{d}\alpha : t_G(C) \to \mathrm{Hom}(T_p(G^D), C)$ et $\mathrm{d}\alpha^D : t_{G^D}(C) \to \mathrm{Hom}(T_p(G), C)$ sont injectives. En outre, leurs images sont orthogonales sous l'accouplement (10) (preuve du Theoreme (4.2.1). Il en résulte une suite exacte

$$0 \to t_{G^D}(C) \xrightarrow{\mathrm{d}\alpha^D} \mathrm{Hom}(T_p(G), C) \to \mathrm{Hom}_C(t_G(C), C(-1)) = t_G^*(C) \otimes_C C(-1) \to 0.$$

L'énoncé est prouvé si on réussit à démontrer que cette suite est scindée de façon unique compatible avec l'action de $\mathrm{Gal}(\overline{K}/K)$. Comme $t_{G^D}(C)$ et $t_G(C)$ sont des C-espaces vectoriels de dimensions respectives n^D et n, la suite est de la forme

$$0 \to C^{n^D} \to \mathrm{Hom}(T_p(G), C) \to C(-1)^n \to 0.$$

Pour montrer que la suite est scindée, il s'agit de construire une section $\mathrm{Gal}(\overline{K}/K)$-équivariante. Appliquons le foncteur $\mathrm{Hom}_{C[\mathrm{Gal}(\overline{K}/K)]}(C(-1)^n, .)$:

$$\begin{aligned} 0 &\to \mathrm{Hom}_{C[\mathrm{Gal}(\overline{K}/K)]}(C(-1)^n, C^{n^D}) \to \mathrm{Hom}_{C[\mathrm{Gal}(\overline{K}/K)]}\left(C(-1)^n, \mathrm{Hom}(T_p(G), C)\right) \\ &\to \mathrm{Hom}_{C[\mathrm{Gal}(\overline{K}/K)]}(C(-1)^n, C(-1)^n) \to \mathrm{Ext}^1_{C[\mathrm{Gal}(\overline{K}/K)]}(C(-1)^n, C^{n^D}) \to \cdots, \end{aligned}$$

Mais $\mathrm{Hom}_C(C(-1)^n, C^{n^D})) \simeq C(1)^{nn^D}$: la suite exacte qui précède se reécrit

$$\begin{aligned} 0 &\to \mathrm{H}^0\left(\mathrm{Gal}(\overline{K}/K), C(1)^{nn^D}\right) \to \mathrm{H}^0\left(\mathrm{Gal}(\overline{K}/K), \mathrm{Hom}_C\left(C(-1)^n, \mathrm{Hom}(T_p(G), C)\right)\right) \\ &\to \mathrm{H}^0\left(\mathrm{Gal}(\overline{K}/K), \mathrm{Hom}_C(C(-1)^n, C(-1)^n)\right) \to \mathrm{H}^1\left(\mathrm{Gal}(\overline{K}/K), C(1)^{nn^D}\right) \to \cdots \end{aligned}$$

Mais d'après le Théorème (1.3.2) on a $\mathrm{H}^0\left(\mathrm{Gal}(\overline{K}/K), C(1)^{nn^D}\right) = \mathrm{H}^0(K, C(1))^{nn^D} = 0$ et $\mathrm{H}^1\left(\mathrm{Gal}(\overline{K}/K), C(1)^{nn^D}\right) = \mathrm{H}^1(K, C(1))^{nn^D} = 0$, donc

$$\mathrm{H}^0\left(\mathrm{Gal}(\overline{K}/K), \mathrm{Hom}_C\left(C(-1)^n, \mathrm{Hom}(T_p(G), C)\right)\right) \cong \mathrm{H}^0\left(\mathrm{Gal}(\overline{K}/K), \mathrm{Hom}_C(C(-1)^n, C(-1)^n)\right),$$

où

$$\mathrm{Hom}_{C[\mathrm{Gal}(\overline{K}/K)]}\left(C(-1)^n, \mathrm{Hom}(T_p(G), C)\right) \cong \mathrm{Hom}_{C[\mathrm{Gal}(\overline{K}/K)]}(C(-1)^n, C(-1)^n),$$

ce qui montre et l'existence et l'unicité d'un scindage. □

Remarque 4.1.1 Si $G = A(p)$ est un groupe p-divisible associé à un schéma abélien A sur R, la décomposition de Hodge-Tate prend la forme

$$\mathrm{H}^1(A \otimes_R \overline{K}, \mathbb{Q}_p) \otimes C \cong \mathrm{H}^1(A \otimes_R C, \Omega^0_{A \otimes_R C}) \oplus \mathrm{H}^0(A \otimes_R C, \Omega^1_{A \otimes_R C}) \otimes C(-1),$$

où la cohomologie à gauche est la cohomologie étale p-adique de A. En 1988, G. FALTINGS a démontré dans [3] une décomposition analogue (« de Hodge-Tate ») pour la cohomologie étale p-adique des variétés propres et lisses sur K.

4.2 La détermination d'un groupe p-divisible par son module de Tate

Théorème 4.2.1 *Soit R un anneau intègre, intégralement clos et noethérien de corps de fractions K de caractéristique 0. Soient G et H deux groupes p-divisibles sur X. Un morphisme $f : G \otimes_R K \to H \otimes_R K$ entre les fibres générique s'étend de façon unique en un morphisme $G \to H$.*

Comme on l'a vu lors de la preuve du Corollaire (4.1.1), ce théorème équivaut à :

Corollaire 4.2.1 *L'application $\mathrm{Hom}_R(G, H) \to \mathrm{Hom}_{\mathrm{Gal}(\overline{K}/K)}(T_p(G), T_p(H))$ est un isomorphisme.*

Un autre corollaire essentiel est le suivant.

Corollaire 4.2.2 *Soit $g : G \to H$ un morphisme dont la restriction $G \otimes_R K \to H \otimes_R K$ est un isomorphisme, alors g est un isomorphisme.*

Lemme 4.2.1 *Pour démontrer le théorème 4.1.2, on peut supposer que R est un anneau de valuation discrète complet, de caractéristique mixte $(0, p)$, à corps résiduel algébriquement clos.*

DÉMONSTRATION : Par normalité de R, on a $R = \bigcap_{\mathfrak{P} \text{ premier}, \mathrm{ht}(\mathfrak{P})=1} R_{\mathfrak{P}}$ et les $R_{\mathfrak{P}}$ sont des anneaux de valuation discrète. On peut donc déjà supposer que R est de valuation discrète. D'autre part, il existe une extension R' de R qui est un anneau complet de valuation discrète de corps résiduel k algébriquement clos tel que $R = R' \cap K$, ce qui permet de supposer R complet de corps résiduel k algébriquement clos. En outre, on peut supposer que k est de caractéristique p, car si $\mathrm{char}(k) \neq p$ alors aussi bien G que H sont étales et l'énoncé du théorème est trivial. On montre d'abord le Corollaire (4.2.2) directement de sorte qu'on puisse en déduire le théorème. □

DÉMONSTRATION DU COROLLAIRE (4.2.2) : Soient $G = (G_\nu)_\nu$ et $H = (H_\nu)_\nu$ et $(A_\nu)_\nu$, $(B_\nu)_\nu$ les algèbres de Hopf correspondantes. Par hypothèse, on dispose d'un système cohérent d'homomorphismes d'algèbres $u_\nu : B_\nu \to A_\nu$ dont les extensions $u_\nu \otimes \mathrm{id} : B_\nu \otimes_R K \to A_\nu \otimes_R K$ sont des isomorphismes. Puisque B_ν et A_ν sont libres sur R, les applications $B_\nu \to B_\nu \otimes_R K$ et $A_\nu \to A_\nu \otimes_R K$ sont injectives, les homomorphismes u_ν sont injectifs pour tout $\nu \in \mathbb{N}$. Il reste à prouver la surjectivité. Pour cela, on examine les discriminants de A_ν et B_ν - s'ils coïncident et sont non-nuls, u_ν est bijectif. D'après la Proposition (3.3.2) ces idéaux sont engendrés par une puissance de p qui ne depend que de la hauteur et de la dimension de G et de H respectivement. Mais la hauteur d'un groupe p-divisible est déterminée par sa fibre générique, de même que sa dimension comme mentionné dans la démonstration du Corollaire (4.1.1). Enfin, la bijectivité de $u_\nu \otimes \mathrm{id}$ entraîne l'égalité des deux déterminants. □

Pour prouver le théorème, on se servira de la proposition suivante.

Proposition 4.2.1 *Soit F un groupe p-divisible sur R et M un $\mathrm{Gal}(\overline{K}/K)$-sous-module de $T_p(F)$ et M un sous-$\mathbb{Z}_p$-module stable par $\mathrm{Gal}(\overline{K}/K)$ et facteur direct de $T_p(F)$. Alors il existe un groupe p-divisible Γ sur R et un homomorphisme $\phi : \Gamma \to F$ tel que ϕ induise un isomorphisme $T_p(\Gamma) \tilde{\to} M$.*

DÉMONSTRATION : Comme le sous-module $M \in T_p(F)$ est facteur direct, il correspond à un sous-groupe p-divisible fermé

$$E_* \in F \otimes_R K.$$

On note E l'adhérence de E_* dans F, qui est construite de la manière suivante : soient B_ν la R-algèbre affine de F_ν, $A_{*\nu}$ la K-algèbre affine de $E_{*\nu}$ et

$$u_\nu : B_\nu \otimes_R K \to A_{*\nu}$$

le morphisme correspondant à l'inclusion $E_{*\nu} \in F_\nu \otimes_R K$. Notons A_ν l'image de u_ν dans B_ν et posons

$$E_\nu := \mathrm{Spec}\, A_\nu.$$

Alors, pour tout ν, le schéma E_ν est un sous-groupe fermé de F_ν, et les inclusions $F_\nu \to F_{\nu+1}$ induisent des inclusions $E_\nu \to E_{\nu+1}$. Posons

$$E := \lim_{\nu \to \infty} E_\nu.$$

Bien que E ne soit pas forcément p-divisible et ne corresponde donc pas à nos exigences (vide infra), sa fibre générique $E \times_R K = E_*$ l'est. Les quotients E_{i+1}/E_i sont tués par p et p induit des homomorphismes

$$E_{i+\nu+1}/E_{i+1} \to E_{i+\nu}/E_i$$

qui sont des isomorphismes sur la fibre générique (en tant que groupes p-divisibles). Grâce à cela, tous les $D_i \otimes_R K$ (où D_i désigne l'algèbre affine de E_{i+1}/E_i) peuvent être identifiés. Par contre, les D_i forment une suite ascendante de R-réseaux dans une K-algèbre finie et séparable. Étant donné que R est noethérien, cette suite finit par devenir stationnaire et il existe un entier i_0 tel que $D_i = D_{i+1}$ pour $i \geq i_0$. Posons

$$\Gamma_\nu = E_{i_0+\nu}/E_{i_0}.$$

La multiplication par p^{i_0} induit un système cohérent d'homomorphismes $\Gamma_\nu \to E_\nu/E_0 = E_\nu$ qui sont des isomorphes sur la fibre générique. Si on réussit à démontrer que

$$\Gamma = \cup_{\nu \in \mathbb{N}} \Gamma_\nu$$

est p-divisible, on a alors fini, car par construction $T_p(\Gamma) \cong M$. Pour cela on factorise l'homomorphisme p^ν en $\Gamma_{\nu+1}$ comme suit

$$\begin{array}{ccccccc} \Gamma_{\nu+1} & = & E_{i_0+\nu+1}/E_{i_0} & \xrightarrow{p^\nu} & E_{i_0+\nu+1}/E_{i_0} & = & \Gamma_{\nu+1}\ , \\ & & \downarrow{\scriptstyle \alpha} & & \uparrow{\scriptstyle \gamma} & & \\ & & E_{i_0+\nu+1}/E_{i_0+\nu} & \xrightarrow{\beta} & E_{i_0+1}/E_{i_0} & & \end{array}$$

où α est la projection canonique, γ l'inclusion canonique et β est l'isomorphisme (grâce au choix de i_0) induit par p^ν. Par conséquent, le noyau de p^ν est $\mathrm{Ker}(\gamma \circ \beta \circ \alpha) = \mathrm{Ker}\,\alpha \cong E_\nu \cong \Gamma_\nu$, ce qui implique que Γ est p-divisible. □

L'exemple suivant dû à SERRE montre le fait mentionné que E n'est pas forcément p-divisible, autrement dit, que l'application ϕ n'est pas forcément une immersion fermée.

Exemple. Soit X une courbe elliptique sur R dont la réduction $\tilde{X}$ a un invariant de Hasse non nul. On suppose que les points d'ordre p sont rationnels. Alors, il existe deux tels points indépendants l'un de l'autre x et y, mais dont les points réduits par l'idéal maximal de R, $\tilde{x}$ et $\tilde{y}$ coïncident. Donc la suite

$$0 \to X \xrightarrow{\phi} (X/\mathbb{F}_p x) \times (X/\mathbb{F}_p y) \to \mathrm{Coker}\,\phi \to 0$$

est exacte sur K. Toutefois, ϕ n'est pas injectif sur R, parce que $\phi(\tilde{x}) = 0$. Le passage aux groupes p-divisibles associés fournit l'exemple voulu.

DÉMONSTRATION DU THÉORÈME (4.2.1) : On applique la proposition à $F = G \times H$ et M, le graphe de l'homomorphisme $T_p(G) \to T_p(H)$ correspondant à l'homomrphisme donné $f : G \otimes_R K \to H \otimes_R K$. Comme ce graphe est facteur directe dans $T_p(G \times H)$, on obtient un groupe p-divisible Γ sur R et un homomorphisme $\phi : \Gamma \to G \times H$ tel que sa composition avec la première projection induise un isomorphisme $T_p(\Gamma) \to T_p(G)$, et donc un isomorphisme sur les fibres génériques. D'après le Corollaire (4.2.2), $\mathrm{proj}_1 \circ \phi : \Gamma \to G$ est aussi un isomorphisme. En conséquence, $\mathrm{proj}_2 \circ \phi \circ (\mathrm{proj}_1 \circ \phi)^{-1} : G \to H$ est une extension homomorphe de f per constructionem de ϕ. L'unicité peut se voir sur les algèbres de Hopf : si on a des application $u_\nu, u'_\nu : B_\nu \to A_\nu$ qui coincïdent apres $\otimes K$, c'est que $u_\nu = v_\nu$. □

Il reste à démontrer le théorème initial.

DÉMONSTRATION DU THÉORÈME (0.1) : Pour un schéma X intègre, noethérien et normal dont la fibre générique est de caractéristique 0, il existe un recouvrement de voisinages ouverts du point générique, $X = \bigcup_{i \in I} U_i$, tel que les anneaux $\mathcal{O}_X(U_i)$ soient intègres, intégralement clos et noethériens de corps de fractions de caractéristique 0. Maintenant, on peut appliquer le théorème précédent aux homomorphismes restreints $f_\eta|_{U_i} : G_\eta|_{U_i} \to H_\eta|_{U_i}$. Donc, il existe des extensions uniques $f_i : G|_{U_i} \to H_{U_i}$ de f_η qui se recollent en $f : G \to H$ sur X. □

Références

[1] Cartier, P. : *Colloque sur la théorie des groupes algébriques.* Brussels, 1962.

[2] Demazure, M. et Grothendieck, A. : *Schémas en groupes.* Séminaire I.H.E.S., 1963-64.

[3] Faltings, G. : *p-adic Hodge theory.* J. Amer. Math. Soc., no.1, 1988.

[4] Fontaine, J.-M. : *Arithmétique des représentations Galoisiennes p-adiques.* Astérisque 295, Paris, 2004, pp.1-115.

[5] Grothendieck, A. : *Technique de descente et théorèmes d'existence en géométrie algébrique, II.* Séminaire Bourbaki, Exposé 195, 1960.

[6] Grothendieck, A. : *Technique de descente et théorèmes d'existence en géométrie algébrique, III.* Séminaire Bourbaki, Exposé 221, 1961.

[7] Hartshorne, R. : *Algebraic geometry.* Springer, Graduate Texts in Mathematics 52 : New York, 1977.

[8] Hartshorne, R. : *Residues and Duality.* Springer lecture notes 20, 1966.

[9] Lutz E. : *Les solutions de l'équation $y^2 = x^2 - Ax - B$ dans les corps p-adiques.* C. R. Acad. Sc. Paris, t. 203, 1936, pp.20-22.

[10] Manin, Yu.I. : *Theory of formal commutative groupes (translation).* Russian Math. Surveys, vol.18, pp.1-83, 1963.

[11] Mattuck, A. : *Abelian varieties over p-adic ground fields.* Annals of Math., Series 2, t. 62, 1955, pp. 92-119.

[12] Raynaud, M. : *Passage au quotient par une relation d'équivalence plate.* Proceedings of a conference on local fields, Driebergen, 1966. Springer-Verlag : Berlin, Heidelberg, New York, 1967, pp.78-85.

[13] Serre, J.-P. : *Corps locaux.* Hermann, Paris, 1968.

[14] Serre, J.-P. : *Sur les corps locaux à corps de restes algébriquement clos.* Bull. Soc. Math. de France 89, 1961, pp.105-154.

[15] Serre, J.-P. : *Cohomologie Galoisienne.* Springer lecture notes 5, 1964.

[16] Serre, J.-P. : *Lie algebras and Lie groups.* Benjamin : New York, 1965.

[17] Shatz, S.S. : *Group Schemes, Formal Groups, and p-Divisible Groups* in Arithmetic geometry, Cornell-Silverman, Springer-Verlag, 1986.

[18] Tate, J.T. : *p-divisible Groups.* Proceedings of a Conference on Local Fields, Driebergen, 1966. Springer-Verlag : Berlin, Heidelberg, New York, 1967, pp.158-183.