Invent. math. 81, 515-538 (1985)

Inventiones mathematicae
© Springer-Verlag 1985

Il n'y a pas de variété abélienne sur Z

Jean-Marc Fontaine

Institut Fourier, Laboratoire Associé au C.N.R.S., Université Scientifique et Médicale de Grenoble, B.P. 74, F-38402 Saint-Martin d'Hères, France

Conventions. Dans cet article, si A est un anneau commutatif,
- *une A-algèbre* est une A-algèbre associative, commutative et unitaire,
- *un groupe fini sur A* est un schéma en groupes commutatifs, fini et plat sur Spec A,
- si p est un nombre premier, *un p-groupe fini sur A* est un groupe fini sur A tué par une puissance de p.

Introduction

0.1. L'étude des représentations l-adiques associées aux courbes elliptiques avait conduit Serre à conjecturer quelle doit être l'action de l'inertie modérée sur la cohomologie étale l-adique ([Se2], n° 1.13); en démontrant cette conjecture pour le degré 1, Raynaud [R] a mis en évidence certaines propriétés de la fibre générique des groupes finis sur l'anneau des entiers d'un corps local de caractéristique 0.

Le but principal de cet article est d'établir une autre propriété de cette fibre générique; celle-ci signifie en gros que l'action de Galois est «très peu ramifiée». De façon précise, soit K un corps de caractéristique 0, complet pour une valuation discrète, à corps résiduel parfait k de caractéristique $p \neq 0$ et soit e l'indice de ramification absolu de K; soient $\bar{K}$ une clôture algébrique de K, $G = \mathrm{Gal}(\bar{K}/K)$, et, pour u réel $\geqq -1$, G^u les groupes de ramification en numérotation supérieure au sens de Serre ([Se1], chap. IV); posons enfin $G^{(u)} = G^{u-1}$.

Théorème A. *Soit n un entier $\geqq 1$ et soit J un groupe fini sur l'anneau des entiers $\mathfrak{O}_K$ de K, tué par p^n. Si $u > e\left(n + \dfrac{1}{p-1}\right)$, $G^{(u)}$ opère trivialement sur $J(\bar{K})$.*

Si L est le sous-corps de $\bar{K}$ engendré par les points de J à valeurs dans $\bar{K}$, ce théorème fournit une majoration de la différente $\mathfrak{D}_{L/K}$ de l'extension L/K. On a en effet:

Corollaire. *Soit v_0 la valuation de L normalisée par $v_0(p)=1$. Alors*

$$v_0(\mathfrak{D}_{L/K})<n+\frac{1}{p-1}.$$

Ce théorème et ce corollaire sont établis au §2 (Thm. 1) comme conséquences d'un résultat plus général qui est l'objet du §1 (Prop. 1.7):

Soit B une $\mathfrak{O}_K$-algèbre finie et plate, localement d'intersection complète; supposons qu'il existe $a\in\mathfrak{O}_K$ annulant $\Omega^1_{B/\mathfrak{O}_K}$ tel que $\Omega^1_{B/\mathfrak{O}_K}$ est un (B/a)-module localement libre. Soit alors S une $\mathfrak{O}_K$-algèbre finie et plate et I un idéal de S admettant des puissances divisées topologiquement nilpotentes; alors, pour tout homomorphisme (de $\mathfrak{O}_K$-algèbres) $u: B\to S/aI$, il existe un et un seul homomorphisme $\hat{u}: B\to S$ tel que u et $\hat{u}$ induisent le même homomorphisme de B dans S/I.

On en déduit que si L désigne le plus petit sous-corps de $\bar{K}$ qui contient les images de tous les $\mathfrak{O}_K$-homomorphismes de B dans $\bar{K}$ et si $H=\mathrm{Gal}(\bar{K}/L)$, alors $G^{(u)}\subset H$ dès que $u>e\left(v_0(a)+\frac{1}{p-1}\right)$.

0.2. On sait le rôle joué par les résultats de Raynaud dans diverses questions de géométrie arithmétique et, en particulier, dans la démonstration par Faltings [Fa] de la conjecture de Shafarevich.

Au §3, nous appliquons le théorème ci-dessus (ou, plus exactement, son corollaire) pour démontrer une autre conjecture de Shafarevich: *il n'existe pas de variété abélienne sur $\mathbb{Q}$, de dimension $g\geqq 1$, ayant bonne réduction partout* (et, par conséquent, il n'existe pas non plus de courbe de genre $g\geqq 1$, définie sur $\mathbb{Q}$, ayant bonne réduction partout, ce qui répond à une question posée par Shafarevich au Congrès de Stokholm ([Sh], voir aussi [Pa])).

Nous démontrons, en fait, un peu plus: soient E un corps de nombres, J un groupe fini tué par p sur l'anneau des entiers $\mathfrak{O}_E$ de E et F le sous-corps d'une clôture algébrique fixée $\bar{E}$ de E engendré par les points de J à valeurs dans $\bar{E}$. Si $m=[F:\mathbb{Q}]$ et si d_F est le discriminant du corps F, le corollaire ci-dessus fournit une majoration de $|d_F|^{1/m}$. Quand on la compare aux minorations fournies par la méthode d'Odlyzko-Poitou-Serre, on en déduit, pour certaines valeurs particulières de E et p, une majoration de m. Il en résulte que, dans cette situation, il n'existe qu'un nombre fini de classes d'isomorphismes de groupes finis tués par p sur $\mathfrak{O}_E$, «indécomposables»; quitte à restreindre un peu la liste des couples (E, p) que l'on regarde, il est alors facile de déterminer effectivement toutes ces classes (du moins si l'on veut bien utiliser les résultats de Raynaud). Par dévissage, on peut alors classifier les p-groupes finis sur $\mathfrak{O}_E$.

Nous montrons ainsi (§3, Thm. 4 et remarque b) du n° 3.4.5):

Théorème B. *Soit J un p-groupe fini sur $\mathfrak{O}_E$.*

i) *Si $E=\mathbb{Q}$ (resp. $\mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-3})$) et $p\in\{3, 5, 7, 11, 13, 17\}$ (resp. $p\in\{3, 5, 7\}$, $p\in\{5, 7\}$), alors J est somme directe d'un groupe constant* (i.e. *somme directe de groupes du type $\mathbb{Z}/p^n\mathbb{Z}$*) *et d'un groupe diagonalisable* (i.e. *somme directe de groupes du type $\boldsymbol{\mu}_{p^n}$*);

ii) *si $E=\mathbb{Q}$ et $p=2$ ou si $E=\mathbb{Q}(\sqrt{5})$ et $p=3$, J est extension d'un groupe constant par un groupe diagonalisable.*

En appliquant ce théorème au noyau de la multiplication par p^n (avec n suffisamment grand), on en déduit:

Corollaire. *Si* $E=\mathbb{Q}$, $\mathbb{Q}(\sqrt{-1})$, $\mathbb{Q}(\sqrt{-3})$ *ou* $\mathbb{Q}(\sqrt{5})$, *il n'existe pas de variété abélienne sur* E *de dimension* $\geqq 1$ *ayant bonne réduction partout.*

1. Groupes de ramification et majoration de la différente

Dans ce paragraphe, K est un corps complet pour une valuation discrète, à corps résiduel parfait k de caractéristique $p\neq 0$. On note v_K la valuation de K normalisée par $v_K(K^*)=\mathbb{Z}$, ainsi que son unique prolongement à toute extension algébrique de K.

Pour toute extension algébrique L de K, on note $\mathfrak{O}_L$ l'anneau de ses entiers, $\mathfrak{m}_L$ son idéal maximal, k_L son corps résiduel; si $\mathfrak{a}$ est un idéal principal de $\mathfrak{O}_L$, on note $v_K(\mathfrak{a})$ la valuation d'un générateur quelconque de $\mathfrak{a}$ (remarquons que si L/K est finie, tout idéal de $\mathfrak{O}_L$ est principal); si m est un nombre réel $\geqq 0$, on note $\mathfrak{a}_{L/K}^m$ l'idéal de $\mathfrak{O}_L$ formé des x vérifiant $v_K(x)\geqq m$.

1.1. Fixons quelques notations et rappelons quelques propriétés des groupes de ramification (cf. [Se1], Chap. IV; nous utilisons des définitions légèrement différentes de celles de Serre; voir la remarque (i) du n° 1.2 pour un dictionnaire entre celles-ci et celles-là).

Soit L une extension finie galoisienne de K et soit $G=\mathrm{Gal}(L/K)$. Pour tout $g\in G$, soit $\mathfrak{a}_g$ l'idéal de $\mathfrak{O}_L$ engendré par les $(g-1)x$, pour $x\in\mathfrak{O}_L$ et soit $\mathbf{i}_{L/K}(g)=v_K(\mathfrak{a}_g)$ (si $e_{L/K}$ est l'indice de ramification de l'extension L/K, $e_{L/K}\cdot\mathbf{i}_{L/K}(g)\in\mathbb{N}\cup\{+\infty\}$). Pour tout $i\in\mathbb{R}$, posons

$$G_{(i)}=\{g\in G\mid \mathbf{i}_{L/K}(g)\geqq i\}.$$

Alors les $G_{(i)}$ sont des sous-groupes invariants de G, on a $G_{(i')}\subset G_{(i)}$ si $i'\geqq i$, $G_{(i)}=G$ si $i\leqq 0$, $G_{(i)}=1$, pour i suffisamment grand.

Pour tout $i\in\mathbb{R}$, posons

$$\tilde{\varphi}_{L/K}(i)=\sum_{g\in G}\min\{i,\mathbf{i}_{L/K}(g)\}.$$

La fonction $\tilde{\varphi}_{L/K}\colon\mathbb{R}\to\mathbb{R}$ est linéaire par morceaux, strictement croissante, bijective. Pour tout $g\in G$, on pose

$$\mathbf{u}_{L/K}(g)=\tilde{\varphi}_{L/K}(\mathbf{i}_{L/K}(g))$$

(en convenant que $\mathbf{u}_{L/K}(1)=+\infty$), et, pour tout $u\in\mathbb{R}$,

$$G^{(u)}=\{g\in G\mid \mathbf{u}_{L/K}(g)\geqq u\}.$$

Si $\tilde{\psi}_{L/K}$ désigne la fonction réciproque de $\tilde{\varphi}_{L/K}$, et si $i,u\in\mathbb{R}$, on a

$$G^{(u)}=G_{(\tilde{\psi}_{L/K}(u))},\qquad G_{(i)}=G^{(\tilde{\varphi}_{L/K}(i))}$$

et

$$\tilde{\varphi}_{L/K}(i)=\int_0^i(G_{(x)}\colon 1)\,dx,\qquad \tilde{\psi}_{L/K}(u)=\int_0^u\frac{dy}{(G^{(y)}\colon 1)}.$$

Enfin, on pose

$$i_{L/K}=\sup_{g\neq 1}\mathbf{i}_{L/K}(g) \quad \text{et} \quad u_{L/K}=\sup_{g\neq 1}\mathbf{u}_{L/K}(g);$$

on voit que $i_{L/K}$ (resp. $u_{L/K}$) est le plus grand nombre réel i (resp. u) tel que $G_{(i)}\neq 1$ (resp. $G^{(u)}\neq 1$) et que $u_{L/K}=\tilde{\varphi}_{L/K}(i_{L/K})$.

1.2. Remarques. i) Si j et v sont des nombres réels $\geqq -1$, on a, avec les notations du chapitre IV de [Se1]:

$$G_j=G_{((j+1)/e_{L/K})}, \qquad G^v=G^{(v+1)}$$

et

$$\varphi_{L/K}(j)=\tilde{\varphi}_{L/K}((j+1)/e_{L/K})-1, \qquad \psi_{L/K}(v)=e_{L/K}\cdot\tilde{\psi}_{L/K}(v+1)-1.$$

ii) Si L' est une extension finie galoisienne de K contenant L et si $G'=\mathrm{Gal}(L'/K)$, pour tout $u\in\mathbb{R}$, l'image de $G'^{(u)}$ dans G est $G^{(u)}$ ([Se1], Prop. 14, p. 81); si $\bar{K}$ est une clôture séparable de K et si $G_K=\mathrm{Gal}(\bar{K}/K)$, on peut donc définir, pour tout $u\in\mathbb{R}$, le sous-groupe fermé $G_K^{(u)}$ de G_K par

$$G_K^{(u)}=\varprojlim \mathrm{Gal}(L/K)^{(u)},$$

pour L parcourant les extensions finies galoisiennes de K contenues dans $\bar{K}$.

Si L est l'une d'entre elles, $u_{L/K}$ est alors le plus petit nombre réel u tel que $G_K^{(u+\varepsilon)}\subset\mathrm{Gal}(\bar{K}/L)$, pour tout $\varepsilon>0$.

1.3. Proposition. *Soit L une extension finie galoisienne de K, et soit $\mathfrak{D}_{L/K}$ la différente de l'extension L/K. On a*

$$v_K(\mathfrak{D}_{L/K})=u_{L/K}-i_{L/K}.$$

Démonstration. On a ([Se1], Prop. 4, p. 72)

$$\begin{aligned} v_K(\mathfrak{D}_{L/K}) &= \sum_{g\neq 1}\mathbf{i}_{L/K}(g) \\ &= \sum_{g\in G}\min\{i_{L/K},\mathbf{i}_{L/K}(g)\}-i_{L/K}=\tilde{\varphi}_{L/K}(i_{L/K})-i_{L/K} \\ &= u_{L/K}-i_{L/K}. \end{aligned}$$

1.4. Soit L une extension finie galoisienne de K de groupe de Galois G et soit α un élément de $\mathfrak{O}_L$ tel que $\mathfrak{O}_L=\mathfrak{O}_K[\alpha]$ (un tel élément existe, cf. [Se1], Prop. 12, p. 66) et soit P le polynôme minimal de α sur K.

Proposition. *Conservons les notations ci-dessus et soit β un élément appartenant à une extension algébrique de K contenant L. Si l'on pose $i=\sup_{g\in G} v_K(\beta-g\alpha)$ et $u=v_K(P(\beta))$, alors*

$$u=\tilde{\varphi}_{L/K}(i) \quad \text{et} \quad i=\tilde{\psi}_{L/K}(u).$$

Démonstration. Comme $\mathfrak{O}_L=\mathfrak{O}_K[\alpha]$, $\mathbf{i}_{L/K}(g)=v_K((g-1)\alpha)$, pour tout $g\in G$. Quitte à remplacer β par un conjugué, on peut supposer que $i=v_K(\beta-\alpha)$. Pour tout $g\in G$, on a $\beta-g\alpha=(\beta-\alpha)-(g-1)\alpha$ et $v_K(\beta-g\alpha)=\min\{i,\mathbf{i}_{L/K}(g)\}$; comme $P(\beta)$

$=\prod_{g\in G}(\beta-g\alpha)$, on a $u=v_K(P(\beta))=\sum_{g\in G}\min\{i, \mathbf{i}_{L/K}(g)\}=\tilde{\varphi}_{L/K}(i)$, d'où aussi $i=\tilde{\psi}_{L/K}(u)$.

1.5. Proposition. *Soit L une extension finie galoisienne de K et soit m un nombre réel $\geqq 0$. Considérons la propriété*

$$(P_m)\begin{cases}\text{pour toute extension algébrique } E \text{ de } K, \text{ s'il existe}\\ \text{un homomorphisme (de } \mathfrak{O}_K\text{-algèbres) de } \mathfrak{O}_L \text{ dans}\\ \mathfrak{O}_E/\mathfrak{a}_{E/K}^m, \text{ alors il existe un } K\text{-plongement de } L \text{ dans } E.\end{cases}$$

Alors:

i) *si $m>u_{L/K}$, (P_m) est vraie:*
ii) *si (P_m) est vraie, $m>u_{L/K}-e_{L/K}^{-1}$.*

Démonstration. Choisissons α comme au n° 1.4.

Montrons (i):

Soient donc $m>u_{L/K}$, E une extension algébrique de K (que l'on peut supposer contenue dans une extension algébrique F de L) et

$$\eta: \mathfrak{O}_L \to \mathfrak{O}_E/\mathfrak{a}_{E/K}^m$$

un homomorphisme de $\mathfrak{O}_K$-algèbres. Soit β un relèvement dans $\mathfrak{O}_E$ de $\eta(\alpha)$. On a $v_K(P(\beta))\geqq m>u_{L/K}$, et, d'après la proposition précédente, si l'on pose $i=\sup_{g\in G} v_K(\beta-g\alpha)$, on a

$$i=\tilde{\psi}_{L/K}(v_K(P(\beta)))>\tilde{\psi}_{L/K}(u_{L/K})=i_{L/K}.$$

Il existe donc $g_0\in G$, tel que

$$v_K(\beta-g_0\alpha)>i_{L/K}=\sup_{g\neq 1} v_K((g-1)\alpha)=\sup_{g\neq 1} v_K((g-1)g_0\alpha).$$

D'après le lemme de Krasner (cf. par exemple, [L], p. 43), on a donc $g_0\alpha\in K(\beta)$, d'où $L=K(\alpha)=K(g_0\alpha)\subset K(\beta)\subset E$.

Montrons maintenant (ii):

Il suffit de vérifier que, pour $m=u_{L/K}-e_{L/K}^{-1}$, (P_m) n'est pas vraie. Si K' désigne l'extension maximale non ramifiée de K contenue dans L, on a $u_{L/K'}=u_{L/K}$ et $e_{L/K'}=e_{L/K}=[L:K']$ et on peut supposer L/K totalement ramifiée et choisir pour α une uniformisante de L; en particulier, P est un polynôme d'Eisenstein.

- Si $L=K$, il n'y a rien à démontrer;
- si L/K est modérément ramifiée, on a $u_{L/K}=1$; on voit que si E est une extension totalement ramifiée de K de degré $e_{L/K}-1$ et β une uniformisante de E, il existe un $\mathfrak{O}_K$-homomorphisme de $\mathfrak{O}_L$ dans $\mathfrak{O}_E/\mathfrak{a}_{E/K}^m$ qui envoie α sur l'image de β; il n'y a pourtant pas de K-plongement de L dans E;
- supposons enfin $e_{L/K}=[L:K]$ divisible par p; les $e_{L/K}\mathbf{i}_{L/K}(g)$, pour $g\in G$, $g\neq 1$, sont des entiers $\geqq 1$ et $p-1$ d'entre eux au moins sont $\geqq 2$; on en déduit que

$e_{L/K}m$ est un entier $>e_{L/K}$. Posons $e_{L/K}m=e_{L/K}r+s$, avec $r, s\in\mathbb{N}$, $0\leqq s<e_{L/K}$; on a $r\geqq 1$, avec l'inégalité stricte si $s=0$. Si l'on choisit $a\in K$ vérifiant $v_K(a)=r$, on en déduit que le polynôme $R=P-aX^s$ est encore un polynôme d'Eisenstein de degré $e_{L/K}$. Si l'on choisit une racine β de ce polynôme dans une extension algébrique convenable de L, le corps $E=K(\beta)$ est encore une extension totalement ramifiée de K, de degré $e_{L/K}=[L:K]$ et β est une uniformisante de E. On a $P(\beta)=a\beta^s$, donc $v_K(P(\beta))=v_K(a)+s/e_{L/K}=m$; il existe donc un homomorphisme de la $\mathfrak{O}_K$-algèbre $\mathfrak{O}_L$ dans $\mathfrak{O}_E/\mathfrak{a}_{E/K}^m$ qui envoie α sur l'image de β. S'il existait un K-plongement de L dans E, on aurait $L=E$, donc $\beta-g\alpha\in L$, pour tout g dans G, d'où $e_{L/K}\cdot v_K(\beta-g\alpha)\in\mathbb{Z}$. On aurait donc

$$e_{L/K}\cdot\tilde{\psi}_{L/K}(m)=e_{L/K}\cdot\tilde{\psi}_{L/K}(v_K(P(\beta)))$$
$$=(\text{Prop. 1.4})\ e_{L/K}\cdot\sup_{g\in G}v_K(\beta-g\alpha)\in\mathbb{Z}.$$

Un calcul simple montre que $e_{L/K}\cdot\tilde{\psi}_{L/K}(m)=e_{L/K}u_{L/K}-d^{-1}$, en notant d le cardinal de $G_{(i_{L/K})}$; comme $e_{L/K}u_{L/K}\in\mathbb{Z}$, ce n'est pas un entier, d'où une contradiction.

1.6. On suppose désormais K de caractéristique 0 et on note $e=v_K(p)$ l'indice de ramification absolu de K.

Soit S une $\mathfrak{O}_K$-algèbre finie et plate; elle s'identifie donc à un sous-anneau de $S_K=K\underset{\mathfrak{O}_K}{\otimes}S$. Rappelons que l'on dit qu'un idéal I de S est à *puissances divisées* si, pour tout $x\in I$ et tout $n\in\mathbb{N}$, l'élément $\gamma_n(x)=x^n/n!$ appartient à I; pour tout entier $m\geqq 1$, on note alors $I^{[m]}$ l'idéal de S engendré par les $\gamma_{n_1}(x_1)\cdot\gamma_{n_2}(x_2)\ldots\gamma_{n_r}(x_r)$, avec $x_1, x_2, \ldots, x_r\in I$ et $\sum n_j\geqq m$; c'est encore un idéal à puissances divisées de S; on dit que I est *à puissances divisées topologiquement nilpotentes* si $\bigcap I^{[m]}=0$.

Par exemple, si $S=\mathfrak{O}_L$, anneau des entiers d'une extension finie de K, l'idéal $\mathfrak{a}_{L/K}^m$ a des puissances divisées (resp. des puissances divisées topologiquement nilpotentes) si et seulement si $m\geqq e/(p-1)$ (resp. $m>e/(p-1)$).

1.7. Proposition. *Soit B une $\mathfrak{O}_K$-algèbre finie et plate, localement d'intersection complète. On suppose qu'il existe $a\in\mathfrak{O}_K$, annulant $\Omega^1_{B/\mathfrak{O}_K}$, tel que $\Omega^1_{B/\mathfrak{O}_K}$ est un (B/a)-module plat.*

i) *Si S est une $\mathfrak{O}_K$-algèbre finie et plate et si I est un idéal de S admettant des puissances divisées topologiquement nilpotentes, alors:*

a) *pour tout $\mathfrak{O}_K$-homomorphisme u de B dans S/aI, il existe un et un seul homomorphisme $\hat{u}: B\to S$ rendant le diagramme*

$$\begin{array}{ccc} B & \xrightarrow{u} & S/aI \\ \downarrow{\scriptstyle \hat{u}} & & \downarrow{\scriptstyle \text{proj. can.}} \\ S & \xrightarrow{\text{proj. can.}} & S/I \end{array}$$

commutatif;

b) *l'application canonique de l'ensemble des $\mathfrak{O}_K$-homomorphismes de B dans S dans celui des $\mathfrak{O}_K$-homomorphismes de B dans S/I est injective.*

ii) *La K-algèbre $B_K = K \otimes_{\mathfrak{O}_K} B$ est étale; si L est le plus petit sous-corps d'une clôture algébrique donnée $\bar{K}$ de K contenant les $u(B)$, pour u décrivant l'ensemble des $\mathfrak{O}_K$-homomorphismes de B dans $\bar{K}$, alors L/K* est galoisienne et $u_{L/K} \leqq v_K(a) + e/(p-1)$.

Démonstration.

• *Montrons d'abord le* (a) *de l'assertion* (i): il est clair que l'on peut supposer que B est un anneau local et que, si $\mathfrak{m}_B$ est son idéal maximal, $B/\mathfrak{m}_B = k$.

Alors $\Omega^1_{B/\mathfrak{O}_K}$ est un (B/a)-module libre. Soient $x_1, x_2, \ldots, x_h$ des éléments de $\mathfrak{m}_B$ qui relèvent une base de $\mathfrak{m}_B/(\mathfrak{m}_B^2 + \mathfrak{m}_K B)$; les dx_j engendrent $\Omega^1_{B/\mathfrak{O}_K}$. Si $b_1, b_2, \ldots, b_h \in B$ et si $\sum b_j dx_j = 0$, on voit (par exemple en regardant l'image de $\sum b_j dx_j$ dans le module des différentielles de $B/(\mathfrak{m}_B^2 + \mathfrak{m}_K B)$) que les $b_j \in \mathfrak{m}_B$; on en déduit que les dx_j forment une base du (B/a)-module libre $\Omega^1_{B/\mathfrak{O}_K}$.

Notons

$$\alpha : \mathfrak{O}_K[\![X_1, X_2, \ldots, X_h]\!] \to B$$

l'unique $\mathfrak{O}_K$-homomorphisme continu qui envoie X_j sur x_j; il nous permet d'identifier B au quotient de $\mathfrak{O}_K[\![X_1, X_2, \ldots, X_h]\!]$ par un idéal J. Comme B est fini d'intersection complète, il existe $P_1, P_2, \ldots, P_h \in \mathfrak{O}_K[\![X_1, X_2, \ldots, X_h]\!]$ tels que J soit l'idéal engendré par les P_j.

Pour tout i, $\sum_j \dfrac{\partial P_i}{\partial X_j}(x_1, x_2, \ldots, x_h) \cdot dx_j = 0$, ce qui implique que les $\dfrac{\partial P_i}{\partial X_j}(x_1, x_2, \ldots, x_h) \in aB$. Il existe donc des $p_{ij} \in B$ tels que $\dfrac{\partial P_i}{\partial X_j}(x_1, x_2, \ldots, x_h) = a p_{ij}$. Comme $a dx_j = 0$, pour tout j, il existe des $q_{li} \in B$ tels que

$$(q_{li})(a p_{ij}) = a I_h$$

(en notant I_h la matrice unité à h lignes et h colonnes). Comme B est un $\mathfrak{O}_K$-module libre, on peut diviser cette égalité par a et cela signifie que la matrice des p_{ij} est inversible dans B et que la matrice des q_{li} est son inverse.

Pour montrer l'assertion, il suffit de vérifier que, pour tout entier $n \geqq 1$, si $u : B \to S/aI^{[n]}$ est un $\mathfrak{O}_K$-homomorphisme, il existe un unique $\mathfrak{O}_K$-homomorphisme $u' : B \to S/aI^{[n+1]}$ tel que u et u' induisent le même homomorphisme de B dans $S/I^{[n]}$.

Si, pour tout i, u_i désigne un relèvement dans S de $u(x_i)$, cela revient à montrer que, si $u_1, u_2, \ldots, u_h$ sont des éléments de S vérifiant

$$P_i(u_1, u_2, \ldots, u_h) = a\lambda_i, \qquad \text{avec } \lambda_i \in I^{[n]}, \text{ pour tout } i,$$

alors il existe $\mu_1, \mu_2, \ldots, \mu_h \in I^{[n]}$, uniquement déterminés $\bmod I^{[n+1]}$ tels que $P_i(u_1 + \mu_1, u_2 + \mu_2, \ldots, u_h + \mu_h) \in aI^{[n+1]}$, pour tout i.

Pour tout $r = (r_1, r_2, \ldots, r_h) \in \mathbb{N}^h$ et tout $P \in \mathfrak{O}_K[\![X_1, X_2, \ldots, X_h]\!]$, posons

$$|r| = \sum r_j, \qquad \frac{\partial^r P}{\partial X^r} = \frac{\partial^{|r|} P}{\partial X_1^{r_1} \ldots \partial X_h^{r_h}} \quad \text{et} \quad \gamma_r(\mu) = \gamma_{r_1}(\mu_1) \ldots \gamma_{r_h}(\mu_h).$$

Comme les puissances divisées sont topologiquement nilpotentes, la série de Taylor converge et l'on a

$$P_i(u_1+\mu_1, \ldots, u_h+\mu_h) = a\lambda_i + \sum_j \frac{\partial P_i}{\partial X_j}(u_1, \ldots, u_h)\cdot \mu_j + R_j,$$

avec $R_j = \sum_{|r|\geqq 2} \frac{\partial^r P_i}{\partial X^r}(u_1, \ldots, u_h)\cdot \gamma_r(\mu)$.

Si $P\in J$, on a $\frac{\partial P}{\partial X_j}(x_1, \ldots, x_h)\in aB$, donc

$$\frac{\partial P}{\partial X_j}(X_1, \ldots, X_h)\in a\mathfrak{O}_K[\![X_1, \ldots, X_h]\!] + J;$$

par récurrence sur $|r|$, on en déduit que, si $|r|\geqq 1$ et si $P\in J$,

$$\frac{\partial^r P}{\partial X^r}(X_1, \ldots, X_h)\in a\mathfrak{O}_K[\![X_1, \ldots, X_h]\!] + J.$$

Il en résulte que

$$\frac{\partial^r P_i}{\partial X^r}(u_1, \ldots, u_h)\in aS + aI^{[n]} = aS;$$

si $|r|\geqq 2$, $\gamma_r(\mu)\in (I^{[n]})^{[2]}\subset I^{[n+1]}$ et $R_j\in aI^{[n+1]}$.

Si P_{ij} désigne un relèvement de p_{ij} dans $\mathfrak{O}_K[\![X_1, \ldots, X_h]\!]$, on a

$$\frac{\partial P_i}{\partial X_j}(x_1, \ldots, x_h) = aP_{ij}(x_1, \ldots, x_h),$$

donc $\frac{\partial P_i}{\partial X_j} = aP_{ij} + R_{ij}$, avec $R_{ij}\in J$, d'où

$$\frac{\partial P_i}{\partial X_j}(u_1, \ldots, u_h) \equiv aP_{ij}(u_1, \ldots, u_h) \bmod aI^{[n]}$$

et

$$\frac{\partial P_i}{\partial X_j}(u_1, \ldots, u_h)\cdot \mu_j \equiv aP_{ij}(u_1, \ldots, u_h)\,\mu_j \bmod aI^{[n+1]}$$

car $(I^{[n]})^2\subset I^{[n+1]}$. On a donc

$$P_i(u_1, \ldots, u_h) \equiv a(\lambda_i + \sum_j P_{ij}(u_1, \ldots, u_h)\cdot \mu_j) \bmod aI^{[n+1]};$$

comme S est plat sur $\mathfrak{O}_K$, les conditions que doivent vérifier les μ_j sont donc

$$\lambda_i + \sum_j \frac{\partial P_i}{\partial X_j}(u_1, \ldots, u_h)\cdot \mu_j \equiv 0 \bmod I^{[n+1]}, \qquad \text{pour tout } i.$$

Comme la matrice des $p_{ij} = \frac{\partial P_i}{\partial X_j}(x_1, \ldots, x_h)$ est inversible, la matrice des $\frac{\partial P_i}{\partial X_j}(u_1, \ldots, u_h)$ est inversible modulo $aI^{[n]}$; l'existence des $\mu_j\in I^{[n]}$ et leur unicité mod $I^{[n+1]}$ est alors évidente.

• *Le* (b) *de l'assertion* (i) résulte immédiatement du (a): si $\hat{u}$ et $\hat{v}$ sont deux $\mathfrak{O}_K$-homomorphismes de B dans S qui ont même réduction $u \bmod I$, l'unicité du relèvement de u implique $\hat{u}=\hat{v}$.

• *Montrons* (ii): comme B_K est finie sur K et comme $\Omega^1_{B_K/K}=K\bigotimes_{\mathfrak{O}_K}\Omega^1_{B/\mathfrak{O}_K}=0$, B_K est étale sur K. On peut donc écrire

$$B_K=\prod_{s=1}^{t} L_s,$$

où chaque L_s est une extension finie de K, que l'on peut supposer contenue dans $\bar{K}$; alors L est le composé des fermetures galoisiennes dans $\bar{K}$ des extensions L_s/K. Par suite L/K est galoisienne. Si a est une unité, $\Omega^1_{B/\mathfrak{O}_K}=0$, donc B est étale sur $\mathfrak{O}_K$, L/K est non ramifié et $u_{L/K}=0$.

Supposons donc que $a\in\mathfrak{m}_K$ et *montrons que, pour tout* $m\in\mathbb{R}$ *vérifiant* $m>v_K(a)+e/(p-1)$, L/K *vérifie* (P_m) (cf. n° 1.5).

Pour toute extension finie E de K, notons $J(E)$ l'ensemble des $\mathfrak{O}_K$-homomorphismes de B dans $\mathfrak{O}_E$. On voit que

$$\begin{aligned} J(E)&=\mathrm{Hom}_{\mathfrak{O}_K\text{-alg}}(B,\mathfrak{O}_E)=\mathrm{Hom}_{K\text{-alg}}(B_K,E)\\ &=\coprod_{s=1}^{t}\{K\text{-plongements de } L_s \text{ dans } E\}. \end{aligned}$$

Mais le nombre de K-plongements de L_s dans E est $\leqq$ au degré de l'extension L_s/K, avec l'égalité si et seulement si E contient un corps K-isomorphe à la fermeture galoisienne de L_s/K dans $\bar{K}$. On a donc

$$\sharp J(E)\leqq\sharp J(L),$$

avec l'égalité si et seulement s'il existe un K-plongement de L dans E. Il suffit donc de vérifier que, s'il existe un $\mathfrak{O}_K$-homomorphisme

$$\eta\colon \mathfrak{O}_L\to\mathfrak{O}_E/\mathfrak{a}^m_{E/K},$$

on a $\sharp J(E)\geqq\sharp J(L)$.

Mais $\mathfrak{a}^m_{E/K}=aI$, où I est un idéal à puissances divisées nilpotentes. On a donc une application

$$u\longmapsto u^\eta$$

de $J(L)$ dans $J(E)$: si $u\colon B\to\mathfrak{O}_L$, $u^\eta\colon B\to\mathfrak{O}_E$ est l'unique homomorphisme rendant le diagramme

$$\begin{array}{ccc} B & \xrightarrow{\eta\circ u} & \mathfrak{O}_E/aI \\ {\scriptstyle u^\eta}\downarrow & & \downarrow{\scriptstyle \text{proj. can.}} \\ \mathfrak{O}_E & \xrightarrow{\text{proj. can.}} & \mathfrak{O}_E/I \end{array}$$

commutatif. Il suffit maintenant de vérifier que cette application est injective.

Comme η induit un plongement du corps résiduel de L dans celui de E, il existe un K-plongement de l'extension maximale non ramifiée K' de K contenue dans L dans E; il est clair que l'on peut choisir ce plongement pour que η

soit un $\mathfrak{O}_{K'}$-homomorphisme. Soit alors α une uniformisante de $\mathfrak{O}_L$ et soit P le polynôme minimal de α sur K'; si $n=e_{L/K}=[L:K']$, on a

$$P=a_0+a_1X+\ldots+a_{n-1}X^{n-1}+X^n,$$

avec les $a_j\in\mathfrak{O}_{K'}$, vérifiant $v_K(a_j)\geqq 1$ et $v_K(a_0)=1$.

Si β désigne un relèvement dans $\mathfrak{O}_E$ de $\eta(\alpha)$, on doit avoir $P(\beta)\in aI$, donc, comme $a\in\mathfrak{m}_K$ et $I\subset\mathfrak{m}_E$, $v_K(P(\beta))>1$; on vérifie que ceci implique $v_K(\beta)=v_K(\alpha)=1/n$.

Si I' est le noyau de l'application composée

$$\mathfrak{O}_L\to\mathfrak{O}_E/aI\xrightarrow{\text{proj. can.}}\mathfrak{O}_E/I,$$

on a alors

$$I'=\{x\in\mathfrak{O}_L\mid v_K(x)\geqq m-v_K(a)\}$$

et I' est un idéal à puissances divisées topologiquement nilpotentes. Mais si $u,v\in J(L)$ et si $u^n=v^n$, on a $\eta\circ u\equiv\eta\circ v \bmod I$, donc $u\equiv v \bmod I'$, d'où $u=v$, d'après le (b) de l'assertion (i) et L/K vérifie bien (P_m).

D'après la Proposition 1.5, on a donc $m>u_{L/K}-n^{-1}$ si $m>v_K(a)+e/(p-1)$, d'où $u_{L/K}\leqq v_K(a)+e/(p-1)+1/n$.

- Si n est premier à p, L/K est modérément ramifiée et

$$u_{L/K}=1\leqq v_K(a)\leqq v_K(a)+e/(p-1).$$

- Supposons donc que p divise n. Alors, si $G=\mathrm{Gal}(L/K)$, $n\cdot\mathbf{i}_{L/K}(g)$ est entier pour tout $g\neq 1$ et l'ordre de $G_{(i)}$ est divisible par p si $i\leqq i_{L/K}$; on en déduit facilement que $nu_{L/K}$ doit être un entier divisible par p, donc aussi $n(p-1)u_{L/K}$. Comme on doit avoir

$$n(p-1)u_{L/K}\leqq n(p-1)v_K(a)+ne+p-1$$

et comme $n(p-1)v_K(a)+ne$ est un entier divisible par p, il faut $n(p-1)u_{L/K}\leqq n(p-1)v_K(a)+ne$, d'où $u_{L/K}\leqq v_K(a)+e/(p-1)$.

1.8. Corollaire. *Conservons les hypothèses et notations de la Proposition* 1.7 *et soit* $\mathfrak{D}_{L/K}$ *la différente de l'extension* L/K. *On a*

$$v_K(\mathfrak{D}_{L/K})<v_K(a)+e/(p-1).$$

Démonstration. C'est clair si L/K est non ramifiée. Sinon, on a $i_{L/K}>0$ et (Prop. 1.3)

$$v_K(\mathfrak{D}_{L/K})=u_{L/K}-i_{L/K}<u_{L/K}\leqq v_K(a)+e/(p-1).$$

1.9. Remarques. Conservons les hypothèses et notations de la Proposition 1.7.

i) Si $G_K=\mathrm{Gal}(\bar{K}/K)$, l'assertion (ii) signifie que, si $u>v_K(a)+e/(p-1)$, alors $G_K^{(u)}\subset\mathrm{Gal}(\bar{K}/L)$ (cf. rem. (ii) du n° 1.2).

ii) Soit $B^{\mathcal{N}}$ le normalisé de B dans B_K. Si $B_K=\prod_{s=1}^{t}L_s$, avec les L_s des extensions finies de K, on a $B^{\mathcal{N}}=\prod_{s=1}^{t}\mathfrak{O}_{L_s}$. Comme chaque L_s se plonge dans L, on a $v_K(\mathfrak{D}_{L_s/K})\leqq v_K(\mathfrak{D}_{L/K})<v_K(a)+e/(p-1)$. Comme $\mathfrak{D}_{L_s/K}$ est l'annulateur de

$\Omega^1_{\mathfrak{O}_{L_s}/\mathfrak{O}_K}$ ([Se1], Chap. III, Prop. 14), on en déduit que si c est un élément de $\mathfrak{O}_K$ vérifiant $v_K(c) \geqq e/(p-1)$, alors ac annule $\Omega^1_{B^{\mathscr{N}}/\mathfrak{O}_K}$.

2. Application aux p-groupes finis sur l'anneau des entiers d'un corps local

Dans ce paragraphe, K est toujours un corps de caractéristique 0, complet pour une valuation discrète, à corps résiduel parfait k de caractéristique $p \neq 0$. On note $e = v_K(p)$ l'indice de ramification absolu de K et $\bar{K}$ une clôture algébrique fixée de K.

2.1. Théorème 1. *Soit n un entier $\geqq 1$ et soit J un groupe fini sur $\mathfrak{O}_K$ tué par p^n. Soient H le noyau de l'action de $G_K = \mathrm{Gal}(\bar{K}/K)$ sur $J(\bar{K})$, $L = \bar{K}^H$, $\mathfrak{D}_{L/K}$ la différente de l'extension L/K. On a $G^{(u)} \subset H$ pour tout $u > e\left(n + \dfrac{1}{p-1}\right)$ et $v_K(\mathfrak{D}_{L/K}) < e\left(n + \dfrac{1}{p-1}\right)$.*

Démonstration. Il est clair que l'on peut supposer le corps résiduel k de K algébriquement clos.

Soit B l'algèbre affine de J et soit ω_J le module des différentielles invariantes de J; rappelons (cf., par exemple, [Fo], n° 4.3) que si m^* (resp. i_1^*, i_2^*): $B \to B \underset{\mathfrak{O}_K}{\otimes} B$ est le coproduit (resp. l'application $b \mapsto b \otimes 1$, l'application $b \mapsto 1 \otimes b$),

$$\omega_J = \{\omega \in \Omega^1_{B/\mathfrak{O}_K} \mid m^*\omega = i_1^*\omega + i_2^*\omega\}.$$

a) *Supposons d'abord que ω_J est un $(\mathfrak{O}_K/p^n)$-module libre.*

L'algèbre B est finie et plate sur $\mathfrak{O}_K$ par hypothèse. On sait (cf. par exemple, [De], Chap. II) que la fibre spéciale J_k de J est le produit direct d'un groupe étale $J_k^{\text{ét}}$ par un groupe connexe J_k^c, ce qui implique que son algèbre affine $B_k = k \underset{\mathfrak{O}_K}{\otimes} B$ est isomorphe à $(B_k^c)^{J_k^{\text{ét}}(k)}$, en notant B_k^c l'algèbre affine de J_k^c; on sait aussi (loc. cit.) qu'il existe des entiers h et $r_1, r_2, \ldots, r_h$ tels que $B_k^c \simeq k[X_1, \ldots, X_h]/(X_1^{p^{r_1}}, X_2^{p^{r_2}}, \ldots, X_h^{p^{r_h}})$; on en déduit que B_k est localement d'intersection complète, donc aussi B. On sait enfin (cf., par exemple, [Fo], n° 4.3) que $\Omega^1_{B/\mathfrak{O}_K}$ s'identifie à $B \underset{\mathfrak{O}_K}{\otimes} \Omega_J$; c'est donc un (B/p^n)-module libre.

On peut donc appliquer la Proposition 1.7 et son Corollaire 1.8 avec $a = p^n$ et le théorème en résulte.

b) Passons maintenant au cas général. D'après un résultat de Grothendieck (cf. [BBM] ou [I]), J peut se plonger dans un groupe de Barsotti-Tate Γ. On a alors $J(\bar{K}) \subset \Gamma_{p^n}(\bar{K})$ (en notant Γ_{p^n} le noyau de la multiplication par p^n dans Γ) et il suffit de prouver le résultat pour le groupe fini et plat Γ_{p^n}. Mais la suite exacte (pour la topologie *fppf*)

$$0 \longrightarrow \Gamma_{p^n} \longrightarrow \Gamma \xrightarrow{p^n} \Gamma \longrightarrow 0$$

induit une suite exacte

$$0 \longrightarrow \omega_\Gamma \xrightarrow{p^n} \omega_\Gamma \longrightarrow \omega_{\Gamma_{p^n}} \longrightarrow 0.$$

Comme ω_Γ est un $\mathfrak{O}_K$-module libre, $\omega_{\Gamma_{p^n}}$ est libre sur $\mathfrak{O}_K/p^n$ et on est ramené au cas (a).

2.2. Remarques. a) Nous n'allons utiliser le Théorème 1 que lorsque $e=n=1$. Dans ce cas, il n'est pas nécessaire d'utiliser l'existence d'un plongement dans un Barsotti-Tate; l'anneau $\mathfrak{O}_K/p$ est le corps résiduel k et le $(\mathfrak{O}_K/p)$-module ω_J est nécessairement libre.

b) Soit X un schéma propre et lisse sur $\mathfrak{O}_K$ et soit $\bar{X}=X\otimes\bar{K}$. Si $i, n\in\mathbb{N}$, soient $H_{n,i}$ le noyau de l'action de $G_K=\mathrm{Gal}(\bar{K}/K)$ sur $H^i(\bar{X}_{\text{ét}}, \mathbb{Z}/p^n\mathbb{Z})$, $L_{n,i}=\bar{K}^{H_{n,i}}$, $u_{n,i}=u_{L_{n,i}/K}$ et $d_{n,i}=v_K(\mathfrak{O}_{L_{n,i}/K})$. Le Théorème 1 montre que $u_{n,1}\leqq e\left(n+\frac{1}{p-1}\right)$ et $d_{n,1}<e\left(n+\frac{1}{p-1}\right)$; il me semble raisonnable de conjecturer que $u_{n,i}\leqq e\left(n+\frac{i}{p-1}\right)$ et $d_{n,i}<e\left(n+\frac{i}{p-1}\right)$.

c) Soit U un $\mathbb{Z}_p$-module libre de type fini muni d'une action linéaire et continue $\rho: G_K\to GL(U)$. Soient

$$H_n=\{g\in G \mid \rho(g)\equiv 1 \bmod p^n\}, \qquad L_n=\bar{K}^{H_n}, \qquad u_n=u_{L_n/K};$$

d'après un résultat de Sen (cf. [Sen]), il existe $c, c'\in\mathbb{R}$ tels que

$$e(n+c')\leqq u_n\leqq e(n+c), \qquad \text{pour tout } n.$$

Si U est le module de Tate d'un groupe de Barsotti-Tate Γ sur $\mathfrak{O}_K$, le Théorème 1 montre que l'on peut choisir $c=1/(p-1)$ (en particulier on peut choisir c indépendant de Γ). Si la conjecture ci-dessus est vraie et si $U=H^i(\bar{X}_{\text{ét}}, \mathbb{Z}_p)/\text{torsion}$, on peut choisir $c=i/(p-1)$ (en particulier, c ne devrait dépendre que de i et non de X).

3. Groupes finis et schemas abéliens sur $\mathbb{Z}$*

Dans ce paragraphe E est un corps de nombres et $\mathfrak{O}$ l'anneau de ses entiers.

3.1. Commençons par rappeler et/ou traduire dans ce contexte quelques-uns des résultats de Raynaud ([R], §2 et 3) sur les groupes finis sur les anneaux de valuation discrète.

3.1.1. Soit J un schéma fini et plat sur $\mathrm{Spec}\,\mathfrak{O}$ et soit N_E un sous-schéma (nécessairement fermé) de sa fibre générique $J_E=J\underset{\mathfrak{O}}{\otimes}E$. L'adhérence

---

* Le lecteur, uniquement intéressé par la démonstration de la non-existence de variétés abéliennes de dimension >0 sur $\mathbb{Q}$ ayant bonne réduction partout - et familier avec les dévissages de schémas en groupes commutatifs finis et plats, peut, au lieu de lire ce paragraphe

i) remarquer que si J est un 3-groupe fini sur $\mathbb{Z}$, et si L est le sous-corps de $\bar{\mathbb{Q}}$ engendré par les points d'ordre 3 de J, la majoration du discriminant de l'extension $L/\mathbb{Q}$ que l'on peut déduire du Théorème 1, comparée aux minorations de Diaz y Diaz, implique que $[L:\mathbb{Q}]\leqq 6$;

ii) en déduire, par un dévissage facile, que J est somme directe d'un groupe constant et d'un groupe diagonalisable;

iii) constater alors qu'une telle variété abélienne aurait «beaucoup trop» de points d'ordre une puissance de 3, rationnels sur $\mathbb{Q}$.

schématique N de N_E dans J est le plus petit sous-schéma fermé de J contenant N_E: si $J=\operatorname{Spec} B$, $J_E=\operatorname{Spec} B_E$, avec $B_E=B\underset{\mathfrak{O}}{\otimes}E$, et $N_E=\operatorname{Spec} B_E/I_E$, alors $N=\operatorname{Spec} B/I$, avec $I=I_E\cap B$ (on a utilisé la platitude pour identifier B à un sous-anneau de B_E); en particulier $B/I\to B_E/I_E$ est injectif, donc B/I est sans torsion et N est plat sur $\mathfrak{O}$; enfin N_E s'identifie à la fibre générique de N.

Si J est un groupe fini sur $\mathfrak{O}$ et N_E un sous-groupe de J_E, N est un sous-schéma en groupes fermé de J, fini et plat sur $\mathfrak{O}$, et le quotient J/N (pour la topologie *fppf*) *est représentable par un groupe fini sur $\mathfrak{O}$* (que l'on note encore J/N).

3.1.2. Soit $\mathscr{J}$ un groupe fini sur K et soient J et J' deux groupes finis sur $\mathfrak{O}$ qui prolongent $\mathscr{J}$ (i.e. dont la fibre générique s'identifie à $\mathscr{J}$, ce qui permet de considérer les algèbres affines de J et J' comme des sous-$\mathfrak{O}$-algèbres de l'algèbre affine $\mathscr{O}(\mathscr{J})$ de $\mathscr{J}$). On dit que J *domine* J' si $\mathscr{O}(J')\subset\mathscr{O}(J)$, ce qui revient à dire que l'identité sur la fibre générique se prolonge en un morphisme de J dans J'.

On a ainsi une relation d'ordre partiel sur les prolongements finis et plats de $\mathscr{J}$. Si J et J' sont deux tels prolongements de $\mathscr{J}$, *ils admettent une borne supérieure et une borne inférieure* [rappelons brièvement comment on les construit ([R], Prop. 2.2.2): on considère le produit $J\underset{\mathfrak{O}}{\times}J'$ et sa fibre générique $\mathscr{J}\underset{E}{\times}\mathscr{J}$; la borne supérieure de J et J' s'obtient en prenant l'adhérence schématique dans $J\underset{\mathfrak{O}}{\times}J'$ du noyau N_E du morphisme

$$\mathscr{J}\underset{E}{\times}\mathscr{J}\to\mathscr{J},$$

qui à (g,g') associe $g-g'$; la dualité de Cartier échange borne supérieure et borne inférieure].

3.1.3. Théorème 2. *Soit p un nombre premier tel que l'indice de ramification de chaque place $\mathfrak{p}$ de E au-dessus de p est $<p-1$. Alors*

i) *si $\mathscr{J}$ est un groupe fini sur E tué par une puissance de p, il admet au plus un prolongement fini et plat sur $\mathfrak{O}$;*

ii) *le foncteur «fibre générique» (de la catégorie des p-groupes finis sur $\mathfrak{O}$ dans celle des p-groupes finis sur E) est pleinement fidèle et son image essentielle est stable par sous-objet et quotient (en particulier, la catégorie des p-groupes finis sur $\mathfrak{O}$ est abélienne).*

Démonstration. Pour montrer i), il faut vérifier que si J et J' sont deux prolongements finis et plats de $\mathscr{J}$, on a $J=J'$. Grâce à 3.1.2, on peut supposer que $\mathscr{O}(J')\subset\mathscr{O}(J)$. Comme $\mathscr{O}(J)/\mathscr{O}(J')$ est un $\mathfrak{O}$-module de longueur finie, il suffit de vérifier que, pour tout idéal premier $\mathfrak{p}$ de $\mathfrak{O}$, on a $\mathscr{O}(J')\underset{\mathfrak{O}}{\otimes}\hat{\mathfrak{O}}_{\mathfrak{p}}=\mathscr{O}(J)\underset{\mathfrak{O}}{\otimes}\hat{\mathfrak{O}}_{\mathfrak{p}}$ (en notant $\hat{\mathfrak{O}}_{\mathfrak{p}}$ le complété du localisé en $\mathfrak{p}$ de $\mathfrak{O}$).

Il suffit donc de vérifier que, si $J_{\mathfrak{p}}$ est un p-groupe fini sur le corps des fractions $K_{\mathfrak{p}}$ de $\hat{\mathfrak{O}}_{\mathfrak{p}}$, admettant un prolongement fini et plat sur $\hat{\mathfrak{O}}_{\mathfrak{p}}$, ce prolongement est unique:

- si $\mathfrak{p}$ ne divise pas p, cela résulte de ce qu'un tel prolongement est nécessairement étale;
- si $\mathfrak{p}$ divise p, c'est un résultat de Raynaud ([R], Thm. 3.3.3). L'assertion ii) se déduit, par des arguments standards, de i) et de 3.1.1.

3.1.4. Remarques. a) Soit $\bar{E}$ une clôture algébrique de E; comme tout p-groupe fini sur E est étale, on voit que, sous les hypothèses du Théorème 2, tout p-groupe fini J sur $\mathfrak{O}$ est entièrement déterminé par la connaissance du module galoisien $J(\bar{E})$.

b) Pour un corps de nombres fixé E, il n'y a qu'un nombre fini de nombres premiers p qui ne vérifient pas les hypothèses du théorème (en particulier, pour $E=\mathbb{Q}$, il n'y a que $p=2$); pour chacun de ces p là, le Théorème 2 reste «presque» vrai: on peut montrer qu'il existe un entier r tel que, quels que soient les p-groupes finis J et J' sur $\mathfrak{O}$, le conoyau de l'homomorphisme injectif

$$\mathrm{Hom}_{\mathfrak{O}\text{-groupes}}(J, J') \to \mathrm{Hom}_{E\text{-groupes}}(J_E, J'_E)$$

est tué par p^r (par exemple, si la ramification en p est modérée, i.e. si les indices de ramification des $\mathfrak{p}$ divisant p sont tous premiers à p, il semble que l'on puisse choisir $r=1$).

3.2. Donnons maintenant un résultat local, également conséquence des travaux de Raynaud:

3.2.1. Proposition. *Soient k un corps algébriquement clos de caractéristique $p \neq 0$, $W=W(k)$ l'anneau des vecteurs de Witt à coefficients dans k, $K=\mathrm{Frac}\, W$, $\bar{K}$ une clôture algébrique fixée de K. Soient J_W un groupe fini tué par p sur W, H le noyau de l'action de $\mathrm{Gal}(\bar{K}/K)$ sur $J_W(\bar{K})$ et $L=\bar{K}^H$. On suppose que J_W contient un sous-groupe isomorphe à $\boldsymbol{\mu}_p$. On est dans l'un des cas suivants:*

i) *L/K est cyclique de degré $p-1$ et il existe des entiers r et s tels que $J_W \simeq (\mathbb{Z}/p\mathbb{Z})^r \otimes \boldsymbol{\mu}_p^s$;*

ii) *$[L:K]=p(p-1)$ et il existe des entiers r et s tels que J_W est une extension non triviale de $(\mathbb{Z}/p\mathbb{Z})^r$ par $\boldsymbol{\mu}_p^s$;*

iii) *L/K est cyclique de degré p^2-1;*

iv) *$[L:K] \geqq p^2(p-1)$.*

Démonstration. Soit $G=\mathrm{Gal}(\bar{K}/K)$. Commençons par rappeler la classification des $\mathbb{F}_p[G]$-modules simples: pour tout entier $h \geqq 1$, notons $\mathbb{F}_{p^h}$ l'unique sous-corps de k ayant p^h éléments; choisissons un élément π_h de $\bar{K}$ vérifiant $\pi_h^{p^h-1}=p$ et notons

$$\chi_h : G \to \mathbb{F}_{p^h}^*$$

le caractère de G dans $\mathbb{F}_{p^h}^*$ qui à g associe l'image de $g\pi_h/\pi_h$ dans le corps résiduel.

Soit M un $\mathbb{F}_p[G]$-module simple et soit $h=\dim_{\mathbb{F}_p} M$; alors $\mathrm{End}_{\mathbb{F}_p[G]}(M)$ est isomorphe à $\mathbb{F}_{p^h}$; si l'on choisit un tel isomorphisme, M devient un $\mathbb{F}_{p^h}$-espace vectoriel de dimension 1 et l'action de G sur M est donnée par une puissance du caractère χ_h; avec des conventions évidentes, on peut l'écrire

$$\chi_h^{i_0+pi_1+\ldots+p^{h-1}i_{h-1}},$$

avec $j \mapsto i_j$ une fonction de $\mathbf{Z}/h\mathbf{Z}$ dans $\mathbf{N}$ vérifiant $0 \leqq i_j \leqq p-1$ et les i_j pas tous égaux à $p-1$; changer l'isomorphisme de $\mathrm{End}_{\mathbf{F}_p[G]}(M)$ sur $\mathbf{F}_{p^h}$ revient à faire une permutation circulaire sur les i_j; la simplicité de M se traduit par le fait que la période de la fonction $j \mapsto i_j$ est exactement h.

3.2.2. Venons-en maintenant à la démonstration de la proposition pour $p \neq 2$. Ici encore, la catégorie des p-groupes finis sur W est abélienne ([R], Thm. 3.3.3 et Cor. 3.3.6); notons $(J_m)_{m=1,2,\ldots,t}$ une suite de Jordan-Hölder de J_W; alors $J_m(\bar{K})$ est un $\mathbf{F}_p[G]$-module simple; si l'on pose $h_m = \dim_{\mathbf{F}_p} J_m(\bar{K})$, l'action de G sur $J_m(\bar{K})$ est donc caractérisée, comme ci-dessus, par une fonction $i^m: \mathbf{Z}/h_m\mathbf{Z} \to \mathbf{N}$, de période exactement h_m, définie à permutation circulaire près, et, grâce à Raynaud ([R], Cor. 3.4.4), on sait que $i^m_j = i^m(j) \in \{0, 1\}$, pour tout j.

Pour tout m, notons L_m le sous-corps de $\bar{K}$ engendré sur K par les racines p-ièmes de l'unité et les points de $J_m(\bar{K})$; il est clair que L_m est une extension modérément ramifiée, donc cyclique, de K contenue dans L. Posons $d_m = [L_m : K]$.

3.2.2. Lemme. *Si $h_m \geqq 3$, alors $d_m > p^2(p-1)$.*

Démonstration. Posons $h = h_m$, $i = i^m$, $i_j = i^m_j$, $d = d_m$. Comme $\chi_1 = \chi_h^{1+p+p^2+\ldots+p^{h-1}}$, d est le plus petit entier $\geqq 1$ tel que $p^h - 1$ divise simultanément $d(1+p+\ldots+p^{h-1})$ et $d(i_0 + pi_1 + \ldots + p^{h-1} i_{h-1})$.

- s'il existe deux entiers consécutifs j et $j+1$ tels que $i_j = i_{j+1} = 0$, on peut, quitte à remplacer les i_j par une permutation circulaire, supposer que $i_{h-2} = i_{h-1} = 0$; on a donc

$$i_0 + pi_1 + \ldots + p^{h-1} i_{h-1} \leqq 1 + p + \ldots + p^{h-3} = (p^{h-2} - 1)/(p-1).$$

Comme les i_j ne sont pas tous nuls, le fait que $p^h - 1$ divise $d(i_0 + pi_1 + \ldots + p^{h-1} i_{h-1})$ implique $d(i_0 + pi_1 + \ldots + p^{h-1} i_{h-1}) \geqq p^h - 1$, d'où, a fortiori,

$$d \geqq (p^h - 1) \cdot (p-1)/(p^{h-2} - 1) > p^2(p-1).$$

- Sinon, comme la période de i est exactement h, il existe deux entiers consécutifs j et $j+1$ tels que $i_j = i_{j+1} = 1$, et, comme précédemment, on peut supposer $i_{h-2} = i_{h-1} = 1$; mais, si $p^h - 1$ divise $d(1+p+\ldots+p^{h-1})$ et $d(i_0 + pi_1 + \ldots + p^{h-1} i_{h-1})$, il divise aussi leur différence qui est de la forme $d(i'_0 + pi'_1 + \ldots + p^{h-1} i'_{h-1})$ avec $i'_j = 1 - i_j \in \{0, 1\}$ et $i'_{h-2} = i'_{h-1} = 0$; le même argument que ci-dessus montre que l'on a encore $d > p^2(p-1)$.

3.2.3. *Fin de la démonstration de la proposition pour $p \neq 2$*: Si l'un des h_m est $\geqq 3$, il résulte du lemme que l'on est dans le cas iv). On peut donc supposer tous les $h_m \leqq 2$.

a) Supposons que les h_m ne sont pas tous égaux à 1: si $h_m = 1$ (resp. 2), on voit que L_m/K est cyclique de degré $p-1$ (resp. p^2-1); si J_W est semi-simple, on en déduit que L/K est cyclique de degré p^2-1 et on est dans le cas iii); grâce à la pleine fidélité du foncteur «fibre générique» ([R], Cor. 3.3.6), si J_W n'est pas semi-simple, le $\mathbf{F}_p[G]$-module $J_W(\bar{K})$ ne l'est pas non plus et p divise $[L:K]$; comme p^2-1 divise aussi $[L:K]$, $p(p^2-1)$ divise $[L:K]$ et on est dans le cas iv).

b) Supposons enfin tous les h_m égaux à 1. Il n'y a que deux possibilités pour l'action de G sur $J_m(\bar{K})$

- ou bien elle est triviale et $J_m \simeq \mathbb{Z}/p\mathbb{Z}$,
- ou bien elle est donnée par χ_1 et $J_m \simeq \boldsymbol{\mu}_p$;

le semi-simplifié de J_W est donc isomorphe à

$$(\mathbb{Z}/p\mathbb{Z})^r \oplus \boldsymbol{\mu}_p^s,$$

pour des entiers r et s convenables.

Si J est semi-simple, on est dans le cas i); sinon, toujours grâce à la pleine fidélité du foncteur fibre générique, $[L: K] = p^u(p-1)$ avec u entier $\geqq 1$; si $u \geqq 2$, on est dans le cas iv); si $u = 1$, comme il n'y a pas d'extension non triviale, tuée par p, de $\mathbb{Z}/p\mathbb{Z}$ par lui-même, ni de $\boldsymbol{\mu}_p$ par lui-même, ni d'extension non triviale de $\boldsymbol{\mu}_p$ par $\mathbb{Z}/p\mathbb{Z}$, on est dans le cas ii).

3.2.4. *Démonstration de la proposition pour* $p=2$: soit J_W^c la composante connexe de l'élément-neutre de J_W; on a une suite exacte

$$0 \to J_W^c \to J_W \to J_W^{\text{ét}} \to 0$$

où $J_W^{\text{ét}}$ est un groupe fini étale tué par 2; il existe donc un entier r tel que $J_W^{\text{ét}} \simeq (\mathbb{Z}/2\mathbb{Z})^r$.

Soient H^c le noyau de l'action de $\mathrm{Gal}(\bar{K}/K)$ sur $J_W^c(\bar{K})$ et $L^c = \bar{K}^{H^c}$. Le même raisonnement que pour $p \neq 2$, appliqué à J_W^c, montre que l'on est dans l'un des cas suivants:

c_1) $L_c = K$ et il existe un entier s tel que $J_W^c \simeq \boldsymbol{\mu}_2^s$,
c_2) L_c/K est cyclique de degré $2^2 - 1 = 3$,
c_3) $[L_c: K] \geqq 2^2(2-1) = 4$.

Si on est dans le cas c_3), comme $L_c \subset L$, on a iv).

Si on est dans le cas c_2), on a iii) ou iv) suivant que l'action de $\mathrm{Gal}(\bar{K}/K)$ sur $J_W(\bar{K})$ est ou non semi-simple.

Si on est dans le cas c_1) et si la suite exacte (de modules galoisiens)

$$0 \to J_W^c(\bar{K}) \to J_W(\bar{K}) \to J_W^{\text{ét}}(\bar{K}) \to 0$$

n'est pas scindée, on est dans le cas ii) où le cas iv).

Reste le cas c_1) avec la suite exacte ci-dessus scindée. Si l'on note J_K^c (resp. J_K, $J_K^{\text{ét}}$) la fibre générique de J_W^c (resp. J_W, $J_W^{\text{ét}}$), cela implique que la suite exacte

$$0 \to J_K^c \to J_K \to J_K^{\text{ét}} \to 0$$

est scindée. Le choix d'un scindage $\eta: J_K^{\text{ét}} \to J_K$ permet d'identifier $J_K^{\text{ét}}$ à un sous-groupe de J_K; soit N l'adhérence schématique de ce sous-groupe dans J_W; comme $J_W^{\text{ét}}$ est le prolongement minimal de $J_K^{\text{ét}}$, l'identité sur $J_K^{\text{ét}}$ se prolonge en un morphisme de $J_W^{\text{ét}}$ dans $N \subset J_W$; ceci définit un scindage de la suite exacte

$$0 \to J_W^c \to J_W \to J_W^{\text{ét}} \to 0$$

et on est dans le cas i).

3.3. Donnons maintenant la traduction globale du Théorème 1.

3.3.1. Théorème 3. *Soient p un nombre premier, n un entier $\geqq 1$, et $\bar{E}$ une clôture algébrique de E. Soient J un groupe fini sur $\mathfrak{O}$ tué par p^n, H le noyau de l'action de $\mathrm{Gal}(\bar{E}/E)$ sur $J(\bar{E})$ et $F=\bar{E}^H$. Pour tout idéal premier $\mathfrak{p}$ de $\mathfrak{O}$, soient $e_\mathfrak{p}$ l'indice de ramification absolu de $\mathfrak{p}$ et $r_\mathfrak{p}$ l'exposant de $\mathfrak{p}$ dans l'idéal discriminant de l'extension F/E. On a:*

i) $r_\mathfrak{p}=0$ *si* $\mathfrak{p}$ *ne divise pas* p;

ii) $r_\mathfrak{p}<[F:E]\cdot e_\mathfrak{p}\cdot\left(n+\dfrac{1}{p-1}\right)$ *si* $\mathfrak{p}$ *divise* p.

Démonstration. La première assertion est claire puisque tout groupe fini sur $\hat{\mathfrak{O}}_\mathfrak{p}$ (séparé complété de $\mathfrak{O}$ pour la topologie $\mathfrak{p}$-adique), tué par un entier premier à la caractéristique résiduelle, est étale.

Supposons donc que $\mathfrak{p}$ divise p et soient $\mathfrak{P}_1, \mathfrak{P}_2, \ldots, \mathfrak{P}_g$ les idéaux premiers de F au-dessus de $\mathfrak{p}$. Avec des conventions évidentes, soit $\hat{\mathfrak{P}}_1^m$ la différente de l'extension $F_{\mathfrak{P}_1}/E_\mathfrak{p}$. Si e est l'indice de ramification de cette extension, le Théorème 1 du n° 2.1 nous dit que $m<ee_\mathfrak{p}\cdot(n+1/(p-1))$. Comme les $\mathfrak{P}_i$ sont conjugués par Galois, pour tout i, $\hat{\mathfrak{P}}_i^m$ est la différente de l'extension $F_{\mathfrak{P}_i}/E_\mathfrak{p}$. La différente de l'extension F/E est le produit des différentes locales et la contribution des places au-dessus de $\mathfrak{p}$ est

$$(\mathfrak{P}_1\,\mathfrak{P}_2\ldots\mathfrak{P}_g)^m.$$

La contribution de $\mathfrak{p}$ dans l'idéal discriminant de F/E est donc $N_{F/E}((\mathfrak{P}_1\,\mathfrak{P}_2\ldots\mathfrak{P}_g)^m)=\mathfrak{p}^{mfg}$, en notant f le degré de l'extension résiduelle de $F_{\mathfrak{P}_1}/E_\mathfrak{p}$. On a donc

$$r_\mathfrak{p}=\mathrm{mfg}=\mathrm{efg}\cdot(m/e)=[F:E]\cdot(m/e)<[F:E]\cdot e_\mathfrak{p}\cdot(n+1/(p-1)).$$

3.3.2. Corollaire. *Si d_E* (resp. d_F) *désigne le discriminant du corps E* (resp. F), *on a:*

$$|d_F|^{1/[F:\mathbb{Q}]}<|d_E|^{1/[E:\mathbb{Q}]}\cdot p^{n+\frac{1}{p-1}}.$$

Démonstration. Notons $\mathfrak{d}_{F/\mathbb{Q}}$ (resp. $\mathfrak{d}_{E/\mathbb{Q}}$, $\mathfrak{d}_{F/E}$) l'idéal discriminant de l'extension $F/\mathbb{Q}$ (resp. $E/\mathbb{Q}$, F/E).

Soit $(p)=\prod_{i=1}^{h}\mathfrak{p}_i^{e_i}$ la décomposition de l'idéal de $\mathfrak{O}$ engendré par p en puissances d'idéaux premiers distincts. Soient f_i le degré de l'extension résiduelle $E_{\mathfrak{p}_i}/\mathbb{Q}_p$ et $r_i=r_{\mathfrak{p}_i}$ l'exposant de $\mathfrak{p}_i$ dans $\mathfrak{d}_{F/E}$.

On a $\mathfrak{d}_{F/E}=\prod_{i=1}^{h}\mathfrak{p}_i^{r_i}$ et $N_{E/\mathbb{Q}}(\mathfrak{d}_{F/E})=(p)^r$, avec $r=\sum f_i r_i$. Comme, pour tout i, $r_i<[F:E]\cdot e_i\cdot(n+1/(p-1))$, on a

$$\begin{aligned}r&<[F:E]\cdot(\textstyle\sum f_i e_i)\cdot(n+1/(p-1))\\&=[F:E]\cdot[E:\mathbb{Q}]\cdot(n+1/(p-1))=[F:\mathbb{Q}]\cdot(n+1/(p-1)).\end{aligned}$$

Comme

$$\mathfrak{d}_{F/\mathbb{Q}}=\mathfrak{d}_{E/\mathbb{Q}}^{[F:E]}\cdot N_{E/\mathbb{Q}}(\mathfrak{d}_{F/E}),$$

on a

$$|d_F|^{1/[F:\mathbb{Q}]}=|d_E|^{1/[E:\mathbb{Q}]}\cdot p^{r/[F:\mathbb{Q}]},$$

et l'inégalité cherchée en résulte.

3.3.3. Remarque. La même méthode fournit une majoration du discriminant du corps F engendré par les points d'ordre p^n d'une variété abélienne semi-stable sur E ayant bonne réduction en dehors d'un ensemble fini S de places finies de E ne divisant pas p (majoration ne dépendant que de p, n, E et S, en particulier indépendante de la dimension de la variété): le critère galoisien de réduction semi-stable ([SGA 7I], Exp. IX, Cor. 3.5.2) implique en effet que l'action de l'inertie est modérée en toutes les places de mauvaise réduction qui ne divisent pas p.

3.4. Nous sommes maintenant en mesure de prouver que, pour certaines valeurs particulières de E et p les seuls p-groupes finis qui existent sur $\mathfrak{O}$ sont «ceux que l'on pense».

Choisissons une clôture algébrique $\bar{\mathbb{Q}}$ de $\mathbb{Q}$ contenant E et notons

$$\chi: \mathrm{Gal}(\bar{\mathbb{Q}}/E) \to \mathbb{Z}_p$$

le caractère donnant l'action sur les racines de l'unité d'ordre une puissance de p.

Disons qu'un p-groupe fini J sur $\mathfrak{O}$ est *constant* (resp. *diagonalisable*) s'il est isomorphe à une somme directe de $\mathbb{Z}/p^a\mathbb{Z}$ (resp. μ_{p^a}), avec a variable dans $\mathbb{N}$. Il résulte du Théorème 2 que, si tous les indices de ramification absolus des idéaux premiers de $\mathfrak{O}$ au-dessus de p sont $<p-1$, un p-groupe fini J sur $\mathfrak{O}$ est constant (resp. diagonalisable) si et seulement si $\mathrm{Gal}(\bar{\mathbb{Q}}/E)$ opère trivialement (resp. à travers χ) sur $J(\bar{\mathbb{Q}})$.

3.4.1. Théorème 4. *Soit J un p-groupe fini sur $\mathfrak{O}$.*

i) *Si $E=\mathbb{Q}$* (resp. $\mathbb{Q}(\sqrt{-1})$, $\mathbb{Q}(\sqrt{-3})$) *et $p\in\{3, 5, 7, 11, 13, 17\}$* (resp. $p\in\{3, 5, 7\}$, $p\in\{5, 7\}$), *alors J est somme directe d'un groupe constant et d'un groupe diagonalisable;*

ii) *si $E=\mathbb{Q}(\sqrt{5})$ et $p=3$, J est extension d'un groupe constant par un groupe diagonalisable.*

3.4.2. Commençons par établir un lemme:

Lemme. *Supposons J tué par p et soit F le sous-corps de $\bar{\mathbb{Q}}$ engendré par les points de $J(\bar{\mathbb{Q}})$. Alors $F\subset E(\sqrt[p]{1})$, sauf peut-être lorsque $E=\mathbb{Q}(\sqrt{5})$ et $p=3$ auquel cas, si η désigne une unité fondamentale de E, $F\subset E(\sqrt[3]{1}, \sqrt[3]{\eta})$.*

Démonstration. Posons $F_0=E(\sqrt[p]{1})$. On peut supposer que J contient un sous-groupe isomorphe à μ_p et on a alors $F_0\subset F$.

Lorsque $E\neq\mathbb{Q}$, notons ι l'unique automorphisme non trivial de E et J_ι le groupe fini sur $\mathfrak{O}$ déduit de J par l'extension des scalaires $\iota: \mathfrak{O}\to\mathfrak{O}$; quitte à remplacer J par $J\oplus J_\iota$, on peut supposer $F/\mathbb{Q}$ galoisienne.

Posons $n=[F:\mathbb{Q}]$, $n_0=[F:E]$, $n_0'=[F:F_0]$, $a=[E:\mathbb{Q}]\in\{1, 2\}$; on a $n=an_0$ et $n_0=(p-1)\cdot n_0'$. Soient d_E (resp. d_F) le discriminant de E (resp. F) et $\delta_E=|d_E|^{1/a}$. D'après le Corollaire 3.3.2, on a

$$|d_F|^{1/n}<\delta_E\cdot p^{p/(p-1)}.$$

Le corps F est totalement imaginaire et les minorations de discriminants obtenues par Diaz y Diaz suivant la méthode d'Odlyzko-Poitou-Serre ([DD], Table 1) donnent

- pour $E=\mathbb{Q}$, si p vaut respectivement 3, 5, 7, 11, 13, 17 alors $n\leqq 6$, 12, 18, 50, 88, 574, donc $n'_0\leqq 3$, 3, 3, 5, 7, 35;
- pour $E=\mathbb{Q}(\sqrt{-1})$, si p vaut respectivement 3, 5, 7, $n\leqq 22$, 64, 316, donc $n'_0\leqq 5$, 8, 26;
- pour $E=\mathbb{Q}(\sqrt{-3})$, si p vaut respectivement 5, 7, alors $n\leqq 38$, 108, donc $n'_0\leqq 4$, 9;
- pour $E=\mathbb{Q}(\sqrt{5})$ et $p=3$, $n\leqq 28$, donc $n'_0\leqq 7$.

Notons e l'indice de ramification absolu d'une place quelconque $\mathfrak{P}$ de F au-dessus de p et posons $e=(p-1)\cdot e'$. Dans tous les cas considérés, $E/\mathbb{Q}$ est non ramifiée en p, donc e divise n_0 et e' est un entier divisant n'_0. Comme $n'_0<60$, l'extension galoisienne F/F_0 est résoluble; comme, dans tous les cas considérés, F_0 est principal (cf. [Ma], p. 230 et 234), *il suffit de montrer que* $e'=1$ sauf peut-être si $E=\mathbb{Q}(\sqrt{5})$ et $p=3$, auquel cas $F=E(\sqrt[3]{1}, \sqrt[3]{\eta})$.

La Proposition 3.2 montre que $e'\in\{1, p, p+1\}$ ou $e'\geqq p^2$; les bornes pour n'_0, donc *a fortiori* pour e', interdisent $e'\geqq p^2$; elles laissent a priori possible $e'=p$ comme $e'=p+1$ pour chacun des sept couples (E, p) suivant:

$$(\mathbb{Q}, 3),\quad (\mathbb{Q}, 17),\quad (\mathbb{Q}(\sqrt{-1}), 3),\quad (\mathbb{Q}(\sqrt{-1}), 5)$$
$$(\mathbb{Q}(\sqrt{-1}), 7),\quad (\mathbb{Q}(\sqrt{-3}), 7),\quad (\mathbb{Q}(\sqrt{5}), 3).$$

Si l'on avait $e'=p+1$, l'extension F/E serait non ramifiée en dehors de p, modérément ramifiée en les places au-dessus de p et on aurait $|d_F|^{1/n}<\delta_E\cdot p$. Dans ces sept cas, les tables de Diaz y Diaz nous donnent

$$n\leqq 2, 116, 8, 20, 50, 32, 78, \text{ donc } n'_0\leqq 1, 7, 2, 2, 4, 2, 6 \text{ qui est } <p+1;$$

le cas $e'=p+1$ est donc impossible.

Reste le cas $e'=p$. *Montrons d'abord qu'alors nécessairement* $n'_0=p$:

- on ne peut avoir $n'_0=2p$, car sinon le groupe d'inertie $G_{\mathfrak{P}}$ de $\mathrm{Gal}(F/F_0)$ en $\mathfrak{P}$ serait l'unique p-sous-groupe de Sylow de ce groupe d'ordre $2p$ et serait invariant, donc $F^{G_{\mathfrak{P}}}/F_0$ serait une extension quadratique partout non ramifiée;
- les majorations de n'_0 ne laissent plus alors que la possibilité $n'_0=p$, sauf pour $(\mathbb{Q}(\sqrt{-1}), 7)$ où $n'_0=3p=21$ est *a priori* possible; mais le même argument s'applique: il n'y a, à isomorphisme près, que deux groupes d'ordre 21 et chacun d'eux n'a qu'un seul 7-sous-groupe de Sylow.

Supposons donc $e'=p$ d'où $e=p\cdot(p-1)$. L'extension F/E est donc de degré $p\cdot(p-1)$ totalement ramifiée en toutes les places au-dessus de p.

Soit $\mathfrak{p}$ l'une d'entre elles, et soient k une clôture algébrique du corps résiduel de $\mathfrak{O}_{\mathfrak{p}}$, $W=W(k)$ et $J_W=W\underset{\mathfrak{O}}{\otimes}J$. La Proposition 3.2.1 nous montre que J_W est une extension non triviale d'un $(\mathbf{Z}/p\mathbf{Z})^r$ par un μ_p^s; le fait que F/E est totalement ramifiée implique que $J_{\mathfrak{p}}=\hat{\mathfrak{O}}_{\mathfrak{p}}\underset{\mathfrak{O}}{\otimes}J$ aussi. En regardant l'action de Galois sur une telle extension, on voit que F est de la forme

$$F=E(\sqrt[p]{1}, \sqrt[p]{u}),$$

où u est un élément de E qui n'est pas une puissance p-ième; il est clair que l'on peut choisir u entier, divisible par aucune puissance p-ième d'un élément premier de l'anneau principal $\mathfrak{O}$.

Montrons que u doit être une unité en vérifiant que c'est une unité en toute place finie λ de E:

- si λ ne divise par p, cela résulte de ce que F/E doit être non ramifiée en λ;
- si λ divise p, cela se voit, soit directement en étudiant les extensions de $\mathbb{Z}/p\mathbb{Z}$ par $\boldsymbol{\mu}_p$ sur un anneau de valuation discrète, soit en remarquant que si u n'était pas une unité, le discriminant de l'extension ne satisferait pas la majoration du corollaire au Théorème 1.

Mais si $E \neq \mathbb{Q}(\sqrt{5})$, les unités de E sont les racines de l'unité contenues dans E; elles sont toutes d'ordre premier à p et sont donc des puissances p-ièmes. Si $e'=p$, on a donc nécessairement $E=\mathbb{Q}(\sqrt{5})$ et $p=3$; dans ce cas, u est au signe près une puissance de η, et, si $F \neq E(\sqrt[3]{1})$, on a $F=E(\sqrt[3]{1}, \sqrt[3]{\eta})$.

3.4.3. Montrons maintenant le théorème:

1ère étape. Tout p-groupe fini sur $\mathfrak{O}$, extension d'un groupe constant par un groupe constant, est constant: si E' désigne le corps engendré par les points à valeurs dans $\bar{\mathbb{Q}}$ d'un tel groupe J, E'/E est résoluble puisque $\mathrm{Gal}(E'/E)$ est un p-groupe; elle est non ramifiée partout puisque, pour tout idéal premier $\mathfrak{p}$ de $\mathfrak{O}$, tout groupe fini sur $\hat{\mathfrak{O}}_{\mathfrak{p}}$ extension d'un groupe étale par un groupe étale est encore étale; donc $E'=E$, $\mathrm{Gal}(\bar{\mathbb{Q}}/E)$ opère trivialement sur $J(\bar{\mathbb{Q}})$ et J est constant.

2e étape. Tout p-groupe fini sur $\mathfrak{O}$ extension d'un groupe diagonalisable par un groupe diagonalisable est diagonalisable: il suffit d'appliquer la première étape au groupe dual.

3e étape. Dans la catégorie des groupes finis sur $\mathfrak{O}$ tués par p, il n'y a pas d'extension non triviale de $\boldsymbol{\mu}_p$ par $\mathbb{Z}/p\mathbb{Z}$: il suffit de vérifier que si l'on a une suite exacte

$$0 \to \mathbb{Z}/p\mathbb{Z} \to J \to \boldsymbol{\mu}_p \to 0,$$

telle que la suite exacte de groupes abéliens

$$0 \to \mathbb{Z}/p\mathbb{Z} \to J(\bar{\mathbb{Q}}) \to \boldsymbol{\mu}_p(\bar{\mathbb{Q}}) \to 0$$

est scindée, cette dernière est aussi scindée en tant que suite exacte de modules galoisiens; il suffit pour cela de vérifier que, si F' est le corps engendré par les points de $J(\bar{\mathbb{Q}})$, on a $F'=E(\sqrt[p]{1})$. Lorsque $E \neq \mathbb{Q}(\sqrt{5})$, il suffit d'appliquer le Lemme 3.4.2; lorsque $E=\mathbb{Q}(\sqrt{5})$, si ce n'était pas le cas, on aurait $F'=F=E(\sqrt[3]{1}, \sqrt[3]{\eta})$ et l'extension $F'/E(\sqrt[3]{1})$ serait ramifiée en les $\mathfrak{p}$ au-dessus de p, ce qui contredit le fait qu'il n'existe pas d'extension non triviale de $\boldsymbol{\mu}_3$ par $\mathbb{Z}/3\mathbb{Z}$ sur $\hat{\mathfrak{O}}_{\mathfrak{p}}$.

4e étape. Si $E \neq \mathbb{Q}(\sqrt{5})$, dans la catégorie des groupes finis sur $\mathfrak{O}$ tués par p, il n'y a pas d'extension non triviale de $\mathbb{Z}/p\mathbb{Z}$ par $\boldsymbol{\mu}_p$: même démonstration que pour la 3e étape.

5e étape. Les seuls objets simples de la catégorie des p-groupes finis sur $\mathfrak{O}$ sont $\mathbf{Z}/p\mathbf{Z}$ et $\boldsymbol{\mu}_p$: soit χ_1 le caractère, à valeurs dans $\mathbf{F}_p^*$, donnant l'action de $\mathrm{Gal}(\bar{\mathbf{Q}}/E)$ sur les racines p-ièmes de l'unité. Si J est un p-groupe fini sur $\mathfrak{O}$, simple, J est tué par p, et, avec les notations du Lemme 3.4.2, l'action de $\mathrm{Gal}(\bar{\mathbf{Q}}/E)$ sur $J(\bar{\mathbf{Q}})$ se factorise à travers $\mathrm{Gal}(F/E)$; comme $J(\bar{\mathbf{Q}})$ doit être un $\mathbf{F}_p[\mathrm{Gal}(F/E)]$-module simple et comme ou bien $F=E(\sqrt[p]{1})$, ou bien F est une p-extension de $E(\sqrt[p]{1})$, $J(\bar{\mathbf{Q}})$ est un $\mathbf{F}_p$-vectoriel de dimension 1 sur lequel l'action de Galois est donnée par χ_1^i où $i\in\{0,1,\ldots,p-2\}$. D'après le résultat de Raynaud rappelé au n° 3.2, on doit avoir $i=0$ ou $i=1$; l'unicité du prolongement (Thm. 2) implique que dans le premier cas $J\simeq\mathbf{Z}/p\mathbf{Z}$, dans le second $J\simeq\boldsymbol{\mu}_p$.

6e étape. Montrons (i): soit J un p-groupe fini sur $\mathfrak{O}$ et posons

$$V_0=\{x\in J(\bar{\mathbf{Q}})\mid gx=x,\ \text{pour tout } g\in\mathrm{Gal}(\bar{\mathbf{Q}}/E)\}$$

et

$$V_1=\{x\in J(\bar{\mathbf{Q}})\mid gx=\chi(g)x,\ \text{pour tout } g\in\mathrm{Gal}(\bar{\mathbf{Q}}/E)\}.$$

Il est clair que $V_0\oplus V_1$ s'injecte dans $J(\bar{\mathbf{Q}})$ et que ce qu'il s'agit de prouver c'est que $V_0\oplus V_1=J(\bar{\mathbf{Q}})$, auquel cas nous dirons que J est admissible. Il est clair que la catégorie des J qui sont admissibles est stable par sous-objet, quotient et somme directe.

Supposons qu'il existe des p-groupes finis sur $\mathfrak{O}$, non admissibles et choisissons-en un, J, tel que l'ordre de $J(\bar{\mathbf{Q}})$ est minimal. Soit J' un sous-groupe de J tel que J/J' est simple; on a $J'=J'_0\oplus J'_1$, avec J'_0 constant et J'_1 diagonalisable; si on avait $J'_0\neq 0$ et $J'_1\neq 0$, J/J'_0 et J/J'_1 seraient admissibles, donc aussi J qui s'injecte dans $J/J'_0\oplus J/J'_1$.

Si $J'_0=0$, $J'=J'_1$ est diagonalisable; comme $J/J'=J''$ est simple, $J''\simeq\boldsymbol{\mu}_p$ ou $J''\simeq\mathbf{Z}/p\mathbf{Z}$; dans le premier cas J, extension d'un groupe diagonalisable par un groupe diagonalisable serait diagonalisable donc admissible; dans le second cas, on aurait une suite exacte

$$0\to J'(\bar{\mathbf{Q}})\to J(\bar{\mathbf{Q}})\to\mathbf{Z}/p\mathbf{Z}\to 0;$$

soit u un relèvement dans $J(\bar{\mathbf{Q}})$ d'un générateur de $\mathbf{Z}/p\mathbf{Z}$; on a $pu=v\in J'(\bar{\mathbf{Q}})$ et, pour tout $g\in\mathrm{Gal}(\bar{\mathbf{Q}}/E)$, il existe $w_g\in J'(\bar{\mathbf{Q}})$ tel que $gu=u+w_g$; on a donc $\chi(g)v=gv=g(pu)=pu+pw_g$, donc $(\chi(g)-1)\cdot v=pw_g$; en choisissant g tel que $\chi(g)-1$ soit une unité p-adique, on en déduit que $v\in p\cdot J'(\bar{\mathbf{Q}})$, ce qui revient à dire que l'on peut choisir u pour que $pu=0$, ou encore que la suite

$$0\to J'(\bar{\mathbf{Q}})_p\to J(\bar{\mathbf{Q}})_p\to\mathbf{Z}/p\mathbf{Z}\to 0$$

est encore exacte. Mais, d'après la 4e étape cette suite est scindée, donc a fortiori la suite

$$0\to J'(\bar{\mathbf{Q}})\to J(\bar{\mathbf{Q}})\to\mathbf{Z}/p\mathbf{Z}\to 0$$

et J est admissible.

Il reste à examiner le cas où $J'_1=0$, donc $J'=J'_0$ est constant; il se traite exactement comme le cas précédent en utilisant la 1ère étape à la place de la 2e et la 3e à la place de la 4e.

7e étape. Preuve de (ii): on procède par récurrence sur la longueur du p-groupe fini J. Si celle-ci est 1, cela résulte de la première étape. Si elle est $\geqq 2$, soit J' un sous-groupe de J tel que J/J' est simple; on a alors une suite exacte

$$0 \to J'_1 \to J' \to J'_0 \to 0$$

avec J'_1 diagonalisable et J'_0 constant. Deux cas peuvent se présenter:

- ou bien $J/J' \simeq \mathbb{Z}/p\mathbb{Z}$: alors J/J'_1 est une extension du groupe constant $\mathbb{Z}/p\mathbb{Z}$ par le groupe constant J'_0 et est un groupe constant; donc J est extension du groupe constant J/J'_1 par le groupe diagonalisable J'_1.

- Ou bien $J/J' \simeq \boldsymbol{\mu}_p$: on montre comme au n° précédent que la suite exacte

$$0 \to J'_0 \to J/J'_1 \to \boldsymbol{\mu}_p \to 0$$

est scindée et J/J'_1 contient un sous-groupe J'' isomorphe à $\boldsymbol{\mu}_p$; l'image réciproque $\hat{J}''$ de J'' dans J, extension de $\boldsymbol{\mu}_p$ par un groupe diagonalisable, est diagonalisable; et J est extension du groupe constant J'_0 par le groupe diagonalisable $\hat{J}''$.

3.4.4. Corollaire 1. *Si E et p sont comme dans le Théorème* 4, *tout groupe p-divisible (ou de Barsotti-Tate) sur $\mathfrak{O}$ est isomorphe à une somme directe de copies de $\mathbb{Q}_p/\mathbb{Z}_p$ et de copies de $\boldsymbol{\mu}_{p^\infty}$, sauf peut-être pour $E=\mathbb{Q}(\sqrt{5})$ auquel cas tout groupe 3-divisible sur $\mathfrak{O}$ est extension d'une somme de copies de $\mathbb{Q}_3/\mathbb{Z}_3$ par une somme de copies de $\boldsymbol{\mu}_{3^\infty}$.*

C'est clair!

3.4.5. Remarques. a) Pour $E=\mathbb{Q}(\sqrt{5})$, on peut préciser l'énoncé précédent: il est facile de voir que, pour tout nombre premier $l \neq 2$, il existe, à isomorphisme près, un et un seul groupe l-divisible Γ^l sur $\mathbb{Q}(\sqrt{5})$ tel que $\Gamma^l(\bar{\mathbb{Q}})$ s'identifie au sous-groupe de l-torsion de $\bar{\mathbb{Q}}^*/U$ (en notant U le groupe des unités de $\mathbb{Q}(\sqrt{5})$). On peut montrer que tout groupe 3-divisible sur $\mathfrak{O}$ est isogène à une somme directe de copies de $\mathbb{Q}_3/\mathbb{Z}_3$, $\boldsymbol{\mu}_{3^\infty}$ et Γ^3.

b) En appliquant la Proposition 3.2.1 et le Théorème 3, un raisonnement analogue à celui utilisé pour prouver le Théorème 4 montre que tout 2-groupe fini sur $\mathbb{Z}$ est extension d'un groupe constant par un groupe diagonalisable. En se fatigant un peu plus, le même type de méthodes devrait permettre de montrer que ce résultat reste vrai si l'on remplace $\mathbb{Z}$ par l'anneau des entiers de quelques extensions quadratiques de $\mathbb{Q}$.

3.4.6. Corollaire 2. *Sur $E=\mathbb{Q}$, $\mathbb{Q}(\sqrt{-1})$, $\mathbb{Q}(\sqrt{-3})$ ou $\mathbb{Q}(\sqrt{5})$, il n'existe pas de variété abélienne de dimension $\geqq 1$ ayant bonne réduction partout.*

Démonstration. Soit A une telle variété et g sa dimension. Son modèle de Néron $\mathscr{A}$ est un schéma abélien sur $\mathfrak{O}$.

Si $E=\mathbb{Q}$, $\mathbb{Q}(\sqrt{-1})$ ou $\mathbb{Q}(\sqrt{-3})$, choisissons un nombre premier p comme dans le Théorème 4. Le système des $(\mathscr{A}_{p^n})_{n\in\mathbb{N}}$ est un groupe p-divisible sur $\mathfrak{O}$ de dimension g; comme $\mathbb{Q}_p/\mathbb{Z}_p$ est de dimension 0 et μ_{p^∞} de dimension 1,

$$(\mathscr{A}_{p^n})_{n\in\mathbb{N}} \simeq (\mathbb{Q}_p/\mathbb{Z}_p)^g \oplus (\mu_{p^\infty})^g.$$

En particulier, $\mathscr{A}(E)$ a une infinité de points de p-torsion; ceci est impossible pour toutes sortes de raisons, la plus simple étant peut-être que, si l'on choisit un idéal premier $\mathfrak{L}$ de $\mathfrak{O}$, premier à p, de corps résiduel k, le groupe des points de p-torsion de $A(E)$ s'envoie injectivement dans le groupe fini $A(k)$.

Si $E=\mathbf{Q}(\sqrt{5})$, on voit que, pour tout n, A possède un sous-groupe Γ_n, défini sur E, isomorphe à $(\mu_{3^n})^g$ et que $(A/\Gamma_n)(E)$ contient un sous-groupe isomorphe à $(\mathbf{Z}/3^n\mathbf{Z})^g$; il en est de même du groupe des points à valeurs dans $\mathbf{F}_2$ du modèle de Néron de A/Γ_n, ce qui, pour n suffisamment grand, contredit les bornes de Weil.

3.4.7. Remarques. a) Le même type de méthodes devrait permettre de montrer qu'il n'existe pas de variétés abéliennes semi-stables, de dimension $\geqq 1$, sur $\mathbf{Q}$ ayant bonne réduction en-dehors de 2 (ou de 3? ou de 5?).

b) J.-F. Mestre a montré [Me] que, si A est une variété abélienne sur $\mathbf{Q}$ de dimension $g\geqq 1$ dont la fonction L vérifie les conjectures standard [Se3], alors son conducteur est $>10^g$; en particulier, A ne peut pas être semi-stable avec bonne réduction en dehors de 2, ou de 3, ou de 5, ou de 7.

c) En revanche, la courbe elliptique $X_0(11)$ est semi-stable sur $\mathbf{Q}$, avec bonne réduction en dehors de 11; on peut d'ailleurs montrer, qu'à isogénie près, c'est la seule courbe elliptique semi-stable sur $\mathbf{Q}$ ayant bonne réduction en dehors de 11.

d) En outre, il existe des courbes elliptiques sur $\mathbf{Q}$ qui ne sont pas semi-stables et qui ont bonne réduction en dehors de 2; leur liste se trouve dans [AnIV] (Table 4) et $X_0(32)$ est celle qui a le plus petit conducteur.

Bibliographie

[AnIV] Birch, B.J., Kuyk, W.: Modular functions of one variable IV, Antwerp. Lect. Notes Math. vol. 476. Berlin-Heidelberg-New York: Springer 1975

[BBM] Berthelot, P., Breen, L., Messing, W.: Théorie de Dieudonné cristalline, II. Lect. Notes Math. vol. 930. Berlin-Heidelberg-New York: Springer 1982

[De] Demazure, M.: Lecture on p-divisible groups. Lect. Notes Math. vol. 302. Berlin-Heidelberg-New York: Springer 1972

[DD] Diaz y Diaz, F.: Tables minorant la racine n-ième du discriminant d'un corps de degré n. Publ. Math. d'Orsay. Orsay: Université d'Orsay 1980

[Fa] Faltings, G.: Endlichkeitssätze für abelsche Varietäten über Zahlkörpern. Invent. Math. **73**, 349–366 (1983)

[Fo] Fontaine, J.M.: Formes différentielles et modules de Tate des variétés abéliennes sur les corps locaux. Invent. Math. **65**, 379–409 (1982)

[I] Illusie, L.: Déformations de groupes de Barsotti-Tate. In: Séminaire sur les pinceaux arithmétiques: La conjecture de Mordell (L. Szpiro, ed.), pp. 151–198. Astérisque, vol. 127. Paris: Soc. Math. Fr. 1985

[L] Lang, S.: Algebraic number theory. Reading, MA: Addison Wesley 1970

[Ma] Masley, J.M.: Where are number fields with small class number?. In: Number theory Carbondale 1979. Proceedings, pp. 221–224, Lect. Notes Math. vol. 751. Berlin-Heidelberg-New York: Springer 1979

[Me] Mestre, J.-F.: Formules explicites et minorations de conducteurs de variétés algébriques. Compos. Math. (à paraître)

[Pa] Paršin, A.N.: Quelques conjectures de finitude en géométrie diophantienne. Actes du Congrès Int. Math. Nice, vol. 1, pp. 467–471. Paris: Gauthier-Villars 1971

[R] Raynaud, M.: Schémas en groupes de type $(p, \ldots, p)$. Bull. Soc. Math. Fr. **102**, 241–280 (1974)
[Sen] Sen, S.: Ramification in p-adic Lie extensions. Invent. Math. **17**, 44–50 (1972)
[Se1] Serre, J.-P.: Corps locaux. 2° édition, Paris: Hermann 1968
[Se2] Serre, J.-P.: Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. Invent. Math. **15**, 259–331 (1972)
[Se3] Serre, J.-P.: Facteurs locaux des fonctions zêta des variétés algébriques (définitions et conjectures). Séminaire Delange-Pisot-Poitou (Théorie des nombres), N° 19. Paris: Université de Paris 1969–1970
[Sh] Shafarevich, I.: Communication au Congrès de Stockholm, 1962 (English translation) Algebraic Number Fields. Am. Math. Soc. Trans. **31**, 25–39 (1963)
[SGA7I] Grothendieck, A.: Groupes de monodromie en géométrie algébrique. Lect. Notes Math. vol. 288. Berlin-Heidelberg-New York: Springer 1972

Oblatum 15-IV-1985

Addendum

Ajouté le 1° *juin* 1985: Je reçois une lettre d'A.N. Parshin qui me signale que V.A. Abrashkin vient aussi de prouver qu'il n'y a pas de variété abélienne sur $\mathbf{Q}$ (et sur quelques extensions finies de $\mathbf{Q}$) de dimension $d>0$ ayant bonne réduction partout (pour $d=2,3$, il l'avait fait, il y a longtemps déjà, cf. V.A. Abrashkin, *p-divisible groups over* **Z**, Math. USSR Izvestija **11**, 937–956 (1977)).

Sa démonstration repose aussi sur la majoration de la différente de l'extension L/K du théorème 1: il l'obtient seulement pour $e=n=1$, en utilisant la classification des p-groupes finis sur $\mathfrak{O}_K$ par leurs «systèmes finis de Honda» (cf. J.-M. Fontaine, *Groupes finis commutatifs sur les vecteurs de Witt*, C.R. Acad. Sci. Paris **280**, 1423–1425 (1975)).

Mais dans ce cas $(e=n=1)$ et toujours d'après Parshin, Abrashkin fait beaucoup mieux: avec les notations du §2, il caractérise les représentations de G_K à valeurs dans les espaces vectoriels de dimension finie sur $\mathbf{F}_p$ qui sont de la forme $J(\bar{K})$, avec J groupe fini tué par p sur $\mathfrak{O}_K$; si $p\neq 2$, ce sont celles qui vérifient

i) la conjecture de Serre, i.e. le théorème de Raynaud ([*R*], cor. 3.4.4) utilisé dans la démonstration de la proposition 3.2,

ii) la majoration de la différente donnée dans le théorème 1.