BULLETIN DE LA S. M. F.

MICHEL RAYNAUD

Schémas en groupes de type $(p, \ldots, p)$

Bulletin de la S. M. F., tome 102 (1974), p. 241-280

<http://www.numdam.org/item?id=BSMF_1974__102__241_0>

Bull. Soc. math. France,
102, 1974, p. 241-280.

SCHÉMAS EN GROUPES DE TYPE $(p, \ldots, p)$

PAR

MICHEL RAYNAUD

RÉSUMÉ. — Soient p un nombre premier, et S un schéma. Un S-schéma en groupe G de type $(p, \ldots, p)$ est un S-schéma en groupes fini plat et de présentation finie, commutatif et annulé par p. OORT et TATE ont classifié les groupes G de rang p. On donne ici une classification analogue pour certains schémas en groupe de type $(p, \ldots, p)$: les schémas en F-vectoriels, où F est un corps extension finie du corps premier $\mathbf{Z}/p\mathbf{Z}$.

Lorsque S est le spectre d'un anneau de valuation discrète R, strictement hensélien, de corps des fractions K de caractéristique zéro et de corps résiduel de caractéristique p, tout K-schéma en groupes de type $(p, \ldots, p)$ admet une suite de Jordan-Hölder, dont les quotients successifs sont des schémas en vectoriels; il en est de même des R-schémas en groupes de type $(p, \ldots, p)$ si R n'est pas trop ramifié, et l'on peut préciser les représentations du groupe de Galois $\mathrm{Gal}(\overline{K}/K)$ qui correspondent aux R-schémas en groupes simples.

Soient p un nombre premier, et S un schéma. Un S-schéma en groupes G est dit de type $(p, \ldots, p)$, s'il est fini, plat, de présentation finie sur S, commutatif et annulé par l'élévation à la puissance p-ième. Le groupe multiplicatif du corps premier $\mathbf{Z}/p\mathbf{Z}$ opère alors de façon naturelle sur G. Lorsque G est de rang p, cette action donne une décomposition de l'idéal d'augmentation du faisceau d'algèbres du S-schéma G en une somme directe de faisceaux inversibles sur S, et a permis à OORT et TATE de classifier les schémas en groupes de rang p [10].

Plus généralement, on peut obtenir une classification analogue de certains groupes de type $(p, \ldots, p)$ qui sont munis d'une action du groupe multiplicatif des éléments non nuls d'une extension finie F de $\mathbf{Z}/p\mathbf{Z}$. On est ainsi amené à étudier en détail les schémas en F-vectoriels, ce qui fait l'objet du paragraphe 1.

Supposons maintenant que S est le spectre d'un anneau de valuation discrète R, strictement hensélien, de corps résiduel de caractéristique p, et de corps des fractions K de caractéristique zéro. L'intérêt des schémas

en F-vectoriels provient du fait que tout K-schéma en groupes de type $(p, \ldots, p)$ possède une suite de composition dont les quotients successifs sont isomorphes à des schémas en F-vectoriels; de plus, si R n'est pas trop ramifié, le même résultat vaut pour les R-schémas en groupes de type $(p, \ldots, p)$. Ces énoncés sont démontrés au paragraphe 3, et utilisent des propriétés élémentaires de l'opération d'adhérence schématique rassemblés au paragraphe 2.

Les schémas en F-vectoriels sur K correspondent à certaines représentations modérées du groupe de Galois de $\overline{K}/K$, et l'on peut préciser celles qui proviennent de R-schémas en groupes (3.4.3). Par contre, la considération des schémas en F-vectoriels n'apporte aucune lumière quant à l'action sauvage du groupe de Galois, sauf dans les questions qui se prêtent bien au dévissage. On en donne un exemple au paragraphe 4, en étudiant les caractères du groupe de Galois qui correspondent à la puissance extérieure maximale d'un R-schéma en groupes de type $(p, \ldots, p)$. Par une méthode totalement différente, on étudie également la puissance extérieure maximale d'un groupe p-divisible.

Enfin, on a regroupé en appendice quelques résultats sur la différente d'un schéma en groupes fini, plat, commutatif, ainsi qu'une jolie formule de traces que m'a communiquée A. DOUADY.

Cet article doit beaucoup à J.-P. SERRE qui m'a incité à étudier les schémas en F-vectoriels, qui a prévu la forme des caractères du groupe de Galois, et qui a exercé une pression suffisante, pendant trois ans, pour que ce travail voit le jour.

Table des matières

1. **Schémas en F-vectoriels** Pages
   1.1. Caractères fondamentaux de F 243
   1.2. Schémas en F-vectoriels 244
   1.3. Un exemple 249
   1.4. Classification des schémas en F-vectoriels 253
   1.5. Remarques et exemples 257
2. **Adhérence schématique sur un anneau de valuation discrète**
   2.1. L'opération adhérence schématique 259
   2.2. Relation d'ordre sur les prolongements 260
   2.3. Application : compléments à un théorème de Tate 261
3. **Schémas en groupes fini et action du groupe de Galois**
   3.1. Structure du groupe de Galois modérément ramifié 263
   3.2. Dévissage d'un groupe de type $(p, \ldots, p)$ 264

3.3. Prolongements des schémas en F-vectoriels..... 265
3.4. Action du groupe de Galois sur un schéma en F-vectoriels..... 269
4. **Déterminants**
4.1. Cas des groupes de type $(p, \ldots, p)$..... 271
4.2. Cas des groupes p-divisibles..... 272
APPENDICE : *Trace et différente*..... 274
BIBLIOGRAPHIE..... 279

1. Schémas en F-vectoriels

Dans toute la suite, p désigne un nombre premier.

Soient r un entier $\geqq 1$, $q = p^r$, F un corps fini à q éléments, et F^* le groupe multiplicatif des éléments non nuls de F.

Pour tout entier $n \geqq 1$, tout schéma S, on note $(\mu_n)_S$, ou simplement μ_n, le S-schéma en groupes des racines n-ièmes de l'unité.

1.1. CARACTÈRES FONDAMENTAUX DE F. — Soient $\bar{\mathbf{Q}}$ une clôture algébrique du corps $\mathbf{Q}$ des nombres rationnels, C le sous-corps de $\bar{\mathbf{Q}}$ engendré par les racines $(q-1)$-ièmes de l'unité, D' la fermeture intégrale de $\mathbf{Z}$ dans C, $\mathfrak{p}$ une place de D' au-dessus de p. Notons U l'ouvert de Spec (D') obtenu en rendant $(q-1)$ inversible, et en enlevant les points au-dessus de (p) autres que $(\mathfrak{p})$; U est donc le spectre d'un certain anneau de Dedekind D.

On note μ le groupe des racines $(q-1)$-ième de l'unité contenues dans D; le groupe $\mu = \mu_{q-1}(D)$ est cyclique d'ordre $q-1$. Soit M le groupe des caractères χ de F^* à valeurs dans μ. On prolonge chaque caractère χ à F tout entier en posant $\chi(0) = 0$.

Soit $k(\mathfrak{p})$ le corps résiduel de D en $\mathfrak{p}$; c'est un corps à q éléments, donc isomorphe (non canoniquement) à F.

DÉFINITION 1.1.1. — *Un caractère χ de F^*, à valeurs dans D, est fondamental si l'application composée*

$$F \xrightarrow{\chi} D \xrightarrow{\text{can}} k(\mathfrak{p})$$

est un morphisme de corps (i.e. est additive).

(*N. B.* — Cette terminologie diffère légèrement de celle de [12], p. 267.)

Si χ est un caractère fondamental, les autres caractères fondamentaux sont de la forme χ^{p^h}. Comme, par ailleurs, on a $\chi^{p^r} = \chi$, nous sommes

amenés à noter les caractères fondamentaux χ_i, où i parcourt un espace principal homogène sous $\mathbf{Z}/r\mathbf{Z}$, de façon que l'on ait $\chi_i^p = \chi_{i+1}$ pour tout i.

Si maintenant χ est un caractère quelconque de F^*, il s'écrit sous la forme

$$\chi = \prod_i \chi_i^{n_i}, \qquad 0 \leqq n_i \leqq p-1. \tag{1}$$

Cette écriture « p-adique » est unique, sauf si $\chi = 1$ qui correspond à $n_i = 0$ pour tout i, mais aussi à $n_i = p-1$ pour tout i.

REMARQUE 1.1.2. — Si $\mathfrak{p}'$ est une autre place de D' au-dessus de p, et si $\sigma \in \mathrm{Gal}(C/\mathbf{Q}) = (\mathbf{Z}/(q-1)\mathbf{Z})^*$ est tel que $\sigma(\mathfrak{p}) = \mathfrak{p}'$, les caractères de F^* à valeurs dans D', qui sont fondamentaux en $\mathfrak{p}'$, sont ceux de la forme $\sigma \circ \chi_i$. En particulier, tout caractère primitif de F^* est fondamental en une place de D' au-dessus de p, et une seule.

1.2. SCHÉMAS EN F-VECTORIELS. — Soit S un schéma.

DÉFINITION 1.2.1. — *Un S-foncteur V en F-vectoriels est un foncteur contravariant :*

$$V : (\mathrm{Sch}/S)^0 \to (F\text{-}vectoriels),$$

défini sur la catégorie des S-schémas, à valeurs dans les espaces vectoriels sur le corps F.

Si V est représentable, nous dirons que V est un S-schéma en F-vectoriels (comme d'habitude, on identifie un schéma au foncteur qu'il représente). Un foncteur V en F-vectoriels définit *ipso facto* un foncteur en groupes commutatifs G annulé par p. On suppose désormais que V est un S-schéma en F-vectoriels, fini, plat et de présentation finie sur S. Soit G' le dual de Cartier du schéma en groupes G, sous-jacent à V. Alors $G' = \mathbf{Hom}_{\mathrm{gr}}(G, G_m)$ est canoniquement muni d'une structure F-vectorielle grâce à l'action de F sur le premier facteur. Plus précisément, pour tout S-schéma T, tout $\lambda \in F$ et tout $u \in G'(T) = \mathrm{Hom}(G_T, (G_m)_T)$, λu est l'homomorphisme de G_T dans $(G_m)_T$ tel que $(\lambda u)(x) = u(\lambda x)$ pour tout T-schéma X et tout $x \in G(X)$. Nous dirons que G', muni de la structure F-vectorielle précédente, est le schéma en F-vectoriels V', dual de V. Dorénavant, nous désignons par la même lettre un foncteur en F-vectoriels et le foncteur en groupes sous-jacent.

Soient $\mathscr{A}$ la bigèbre de G, $c : \mathscr{A} \to \mathscr{A} \otimes_S \mathscr{A}$ sa comultiplication, et $d : \mathscr{A} \otimes_S \mathscr{A} \to \mathscr{A}$ sa multiplication. Pour tout entier $n \geqq 0$, nous notons

$$c_n : \mathscr{A} \to \underbrace{\mathscr{A} \otimes \ldots \otimes \mathscr{A}}_{n \text{ facteurs}} \quad \text{et} \quad d_n : \underbrace{\mathscr{A} \otimes \ldots \otimes \mathscr{A}}_{n \text{ facteurs}} \to \mathscr{A}$$

la comultiplication et la multiplication itérée. La bigèbre duale $\mathscr{A}' = \mathbf{Hom}_{\mathscr{O}_S}(\mathscr{A}, \mathscr{O}_S)$ est une bigèbre du groupe dual G' de G; sa multiplication d' est la transposée ${}^t c$ de c et sa comultiplication c' est la transposée ${}^t d$ de d. On note $\mathscr{I}$ (resp. $\mathscr{I}'$) l'idéal d'augmentation de $\mathscr{A}$ (resp. $\mathscr{A}'$); $\mathscr{I}$ et $\mathscr{I}'$ sont en dualité par la restriction de l'accouplement canonique entre $\mathscr{A}$ et $\mathscr{A}'$.

La structure de foncteur en F-vectoriels sur G équivaut à la donnée, pour tout $\lambda \in F$, d'un endomorphisme de bigèbre $[\lambda] : \mathscr{A} \to \mathscr{A}$. Ces endomorphismes satisfont aux conditions suivantes :

$$[1] = \mathrm{id}_{\mathscr{A}},$$

(2) $$[\lambda] \circ [\mu] = [\lambda\mu] \quad \text{pour tout } \lambda \text{ et } \mu \quad \text{dans } F,$$

(3) $$d \circ ([\lambda] \otimes [\mu]) \circ c = [\lambda + \mu] \quad \text{pour tout } \lambda \text{ et } \mu \quad \text{dans } F.$$

La dernière condition traduit la distributivité de l'opération de F vis-à-vis de l'addition de F.

Par transposition, les endomorphismes $[\lambda]' = {}^t[\lambda]$ de la bigèbre $\mathscr{A}'$ définissent la structure vectorielle du dual G' de G.

Pour écrire commodément les endomorphismes $[\lambda]$, nous allons faire sur le schéma S l'hypothèse suivante :

($\star$) *S est un schéma au-dessus de* Spec $(D) = U$ (*notations de 1.1.*).

Nous notons encore χ le caractère de F^* à valeurs dans $\mu_{q-1}(S)$, composé de $\chi : F^* \to \mu$ et du morphisme canonique $\mu \subset D \to \Gamma(\mathscr{O}_S)$.

Exemples. — (*a*) Si S est le spectre d'un anneau local hensélien dont le corps résiduel contient un sous-corps à q éléments, S peut-être muni d'une structure de U-schéma.

(*b*) Plus généralement, si $S/p\,S$ est connexe et si $(\mu_{q-1})_S$ est isomorphe à un groupe constant, S peut être muni d'une structure de U-schéma.

Ceci étant, commençons par traduire les formules (2) qui expriment que F^* opère sur la bigèbre $\mathscr{A}$. Pour tout $\chi \in M$, les endomorphismes

$$i_\chi = \frac{1}{q-1} \sum_{\lambda \in F^*} \chi^{-1}(\lambda)[\lambda]$$

du $\mathcal{O}_S$-module $\mathscr{A}$ forment une famille d'idempotents orthogonaux qui respectent l'idéal d'augmentation $\mathscr{I}$, donc définissent une décomposition canonique de $\mathscr{I}$:

$$\mathscr{I} = \otimes_{\chi \in M} \mathscr{I}_\chi,$$

où $\mathscr{I}_\chi = i_\chi(\mathscr{I})$. Pour tout ouvert V de S, $\Gamma(V, \mathscr{I}_\chi)$ est alors l'ensemble des $a \in \Gamma(V, \mathscr{I})$ tels que $[\lambda]a = \chi(\lambda)a$ pour tout $\lambda \in F^*$. On a de même une décomposition $\mathscr{I}' = \otimes_{\chi \in M} \mathscr{I}'_\chi$ duale de la précédente. Comme les $[\lambda]$ sont des endomorphismes de bigèbres, cette décomposition fait de $\mathscr{A}$ une bigèbre graduée de type M (*cf.* BOURBAKI, A, III, p. 149). On note, pour tout couple de caractères χ', χ'' de M :

$$(4) \qquad \begin{cases} c_{\chi',\chi''} : \mathscr{I}_{\chi'\chi''} \to \mathscr{I}_{\chi'} \otimes \mathscr{I}_{\chi''}, \\ d_{\chi',\chi''} : \mathscr{I}_{\chi'} \otimes \mathscr{I}_{\chi''} \to \mathscr{I}_{\chi'\chi''}, \end{cases}$$

les applications $\mathcal{O}_S$-linéaires déduites respectivement de la comultiplication c et de la multiplication d de $\mathscr{A}$. Plus généralement, pour toute suite $\chi_1, \ldots, \chi_n$ d'éléments de M, on déduit de c_n et d_n des applications canoniques

$$(5) \qquad \begin{cases} c_{\chi_1,\ldots,\chi_n} : \mathscr{I}_{\chi_1\ldots\chi_n} \to \mathscr{I}_{\chi_1} \otimes \ldots \otimes \mathscr{I}_{\chi_n}, \\ d_{\chi_1,\ldots,\chi_n} : \mathscr{I}_{\chi_1} \otimes \ldots \otimes \mathscr{I}_{\chi_n} \to \mathscr{I}_{\chi_1\ldots\chi_n}. \end{cases}$$

Ces dernières peuvent se calculer de proche en proche, à partir du cas $n = 2$ (formules (4)) grâce aux formules d'associativité suivantes : si

$$\chi' = \chi'_1 \ldots \chi'_n \qquad \text{et} \qquad \chi'' = \chi''_1 \ldots \chi''_m,$$

on a

$$(6) \qquad \begin{cases} c_{\chi'_1,\ldots,\chi'_n,\chi''_1,\ldots,\chi''_m} = (c_{\chi'_1,\ldots,\chi'_n} \otimes c_{\chi''_1,\ldots,\chi''_m}) \circ c_{\chi',\chi''}, \\ d_{\chi'_1,\ldots,\chi'_n,\chi''_1,\ldots,\chi''_m} = d_{\chi',\chi''} \circ (d_{\chi'_1,\ldots,\chi'_n} \otimes d_{\chi''_1,\ldots,\chi''_m}). \end{cases}$$

Désormais nous faisons sur G l'hypothèse supplémentaire :

(★★) *Chacun des faisceaux $\mathscr{I}_\chi$ est un $\mathcal{O}_S$ module inversible.*

Il en résulte que le rang de la $\mathcal{O}_S$-algèbre $\mathscr{A}$ est constant et égal à q. On a la réciproque partielle suivante :

PROPOSITION 1.2.2. — *Soit G un S-schéma en F-vectoriels défini par une $\mathcal{O}_S$-bigèbre de rang q. Supposons S connexe et qu'il existe $s \in S$ tel que la fibre de G au-dessus de s soit étale ou de type multiplicatif (cas certainement réalisé si S est intègre et de corps des fractions de caractéristique zéro). Alors chacun des faisceaux $\mathscr{I}_\chi$ est un $\mathcal{O}_S$-module inversible.*

En effet, $\mathscr{I}_\chi$, étant un facteur direct du $\mathcal{O}_S$-module $\mathscr{A}$, est localement libre; il est de rang constant car S est connexe. Il suffit donc de voir qu'il est de rang 1 au-dessus du point s. Or, quitte éventuellement à remplacer G par son dual et s par un point géométrique $\bar{s}$ au-dessus de s, on est ramené au cas où G est un groupe étale constant sur un corps k. Comme G est un schéma en F-vectoriels, de rang q, $G(k)$ est un F-vectoriel de rang 1, et $\mathscr{A}$ est isomorphe à la bigèbre des fonctions sur F à valeurs dans k. La proposition est alors immédiate, et sera d'ailleurs explicitée au numéro suivant.

REMARQUE 1.2.3. — Soit k un corps contenant F. Alors le groupe additif $(G_a)_k$ est un schéma en F-vectoriels, et il en est de même du noyau $(\alpha_p)_k$ du morphisme de Frobenius dans G_a. Considérons alors le schéma en F-vectoriels, produit de r copies de $(\alpha_p)_k$. Il est de rang q, mais les faisceaux $\mathscr{I}_\chi$ correspondants ne sont pas de rang 1, pour $r > 1$.

Pour toute suite $\chi_1, \ldots, \chi_n$ d'éléments de M, l'application composée

$$d_{\chi_1, \ldots, \chi_n} \circ c_{\chi_1, \ldots, \chi_n}$$

est un endomorphisme $\mathcal{O}_S$-linéaire du faisceau inversible $\mathscr{I}_{\chi_1, \ldots, \chi_n}$, donc s'identifie canoniquement à un élément $w_{\chi_1, \ldots, \chi_n}$ de $\Gamma(S, \mathcal{O}_S)$. On déduit de (6) une formule d'associativité pour les w :

$$w_{\chi_1', \ldots, \chi_n', \chi_1'', \ldots, \chi_n''} = w_{\chi', \chi''} w_{\chi_1', \ldots, \chi_n'} w_{\chi_1'', \ldots, \chi_n''}, \tag{7}$$

avec

$$\chi' = \chi_1' \ldots \chi_n' \qquad \text{et} \qquad \chi'' = \chi_1'' \ldots \chi_n''.$$

Nous allons maintenant traduire la formule (3), et montrer qu'elle permet de calculer les coefficients $w_{\chi', \chi''}$ (donc aussi les $w_{\chi_1, \ldots, \chi_n}$ d'après (7)) qui s'avèrent être des constantes de structure indépendantes du schéma en F-vectoriels G.

En considérant la restriction de (3) à $\mathscr{I}_\chi$, on trouve $\forall \chi \in M$ et $\forall \lambda$ et $\mu \in F^*$:

$$\chi(\lambda+\mu) = \chi(\lambda)+\chi(\mu)+\textstyle\sum_{\chi'\chi''=\chi} \chi'(\lambda)\chi''(\mu) w_{\chi', \chi''}. \tag{8}$$

Fixons un couple de caractères χ_1, χ_2 tel que $\chi_1 \chi_2 = \chi$. Multiplions les deux membres de (8) par $\chi_1^{-1}(\lambda)\chi_2^{-1}(\mu)$, et sommons sur λ et μ. On obtient :

$$\sum_{\lambda,\,\mu \in F^*} \chi_1^{-1}(\lambda)\chi_2^{-1}(\mu)\chi(\lambda+\mu) = \sum_{\lambda,\,\mu \in F^*} (\chi_2(\lambda\mu^{-1}) + \chi_1(\mu\lambda^{-1})) + (q-1)^2 w_{\chi_1,\chi_2}.$$

Dans le premier membre, on peut se borner aux couples (λ, μ) de $F^* \times F^*$ tels que $\lambda+\mu \neq 0$. Posant alors $\lambda = \nu u$, $\mu = \nu v$, avec $u+v = 1$ et $\nu \in F^*$, il vient

$$(9) \qquad (q-1) w_{\chi_1,\chi_2} = \sum_{u+v=1} \chi_1^{-1}(u)\chi_2^{-1}(v) - \sum_{g \in F^*} (\chi_1(g) + \chi_2(g)).$$

Premier cas : χ_1 et $\chi_2 \neq 1$. Alors

$$(10) \qquad w_{\chi_1,\chi_2} = \frac{1}{q-1}\left(\sum_{u+v=1} \chi_1^{-1}(u)\chi_2^{-1}(v)\right) = \frac{\chi_1\chi_2(-1)}{q-1}\left(\sum_{u+v+1=0} \chi_1^{-1}(u)\chi_2^{-1}(v)\right) = \frac{(\chi_1\chi_2)(-1)}{q-1} j(\chi_1^{-1}, \chi_2^{-1}),$$

où $j(\chi', \chi'')$ désigne la *somme de Jacobi* relative aux caractères χ' et χ'' (*cf.* [14], p. 500).

Deuxième cas : $\chi_1 = 1$, $\chi_2 = \chi \neq 1$. Alors

$$(10\,bis) \qquad w_{1,\chi} = w_{\chi,1} = \frac{1}{q-1}\left(\sum_{u+v=1,\,u\neq 0} \chi^{-1}(v) - (q-1)\right) = -\frac{q}{q-1}.$$

Troisième cas : $\chi_1 = \chi_2 = 1$. Alors

$$(10\,ter) \qquad w_{1,1} = \frac{1}{q-1}(q-2-2(q-1)) = -\frac{q}{q-1}.$$

Dorénavant, nous adoptons pour un caractère $\chi \in M$ son unique écriture p-adique $\chi = \prod_i \chi_i^{a_i}$ avec $0 \leqq a_i \leqq p-1$ et les a_i non tous nuls.

Posons

$$(11) \qquad \begin{cases} c_\chi = c_{\underbrace{\chi_1,\ldots,\chi_1}_{a_1},\ldots,\underbrace{\chi_r,\ldots,\chi_r}_{a_r}}, \\ d_\chi = d_{\underbrace{\chi_1,\ldots,\chi_1}_{a_1},\ldots,\underbrace{\chi_r,\ldots,\chi_r}_{a_r}}, \\ w_\chi = d_\chi \circ c_\chi = w_{\underbrace{\chi_1,\ldots,\chi_1}_{a_1},\ldots,\underbrace{\chi_r,\ldots,\chi_r}_{a_r}}. \end{cases}$$

Pour tout caractère fondamental χ_i posons

$$(11\,bis)\qquad \begin{cases} c_i = c_{\underbrace{\chi_i, \ldots, \chi_i}_{p}}, \\ d_i = d_{\underbrace{\chi_i, \ldots, \chi_i}_{p}}, \\ w_i = d_i \circ c_i = w_{\underbrace{\chi_i, \ldots, \chi_i}_{p}}, \end{cases}$$

(notons que la bigèbre de G étant commutative, c_χ, d_χ, w_χ ne dépendent pas, à isomorphisme canonique près, de l'indexation des caractères fondamentaux).

Pour étudier plus en détail la bigèbre $\mathscr{A}$ du schéma en F-vectoriels G, il est essentiel de savoir si $w_{\chi', \chi''}$ est inversible ou non. Il suffit de faire le calcul dans D, ce qui nous ramène au problème des valuations p-adiques des coefficients w, question classique d'arithmétique sur les sommes de Gauss (*cf.* [8], p. 90). Néanmoins, nous allons retrouver ces valuations par une étude du schéma en groupes constant défini par le groupe additif F^+ de F ainsi que son dual de Cartier. Ces calculs nous seront utiles pour la classification des schémas en F-vectoriels faite dans 1.4.

1.3. Un exemple. — Soient G le schéma en groupes constant sur D défini par F^+, et G' son dual de Cartier qui est un groupe diagonalisable.

La bigèbre A de G est la bigèbre des fonctions sur F^+, à valeurs dans D. Comme D module, elle possède une base canonique formée des fonctions caractéristiques ε_a des parties à un élément $\{a\}$ de F^+. On a

$$\varepsilon_a \varepsilon_b = 0 \quad \text{si} \quad a \neq b \quad \text{et} \quad \varepsilon_a^2 = \varepsilon_a.$$

La comultiplication envoie ε_a sur $\sum_{a' + a'' = a} \varepsilon_{a'} \otimes \varepsilon_{a''}$. L'idéal d'augmentation I est engendré par les ε_a, $a \neq 0$.

Le schéma en groupes G est de manière naturelle un foncteur en F-vectoriels. L'endomorphisme $[\lambda]$ de la bigèbre A associé à $\lambda \in F$ envoie ε_a sur la fonction caractéristique de l'image réciproque de a par l'homothétie de rapport λ. En particulier, I_χ est engendré par $\varepsilon_\chi = \sum_{a \in F^+} \chi(a)\, \varepsilon_a$. On a donc

$$(12)\qquad \varepsilon_{\chi'} \varepsilon_{\chi''} = \varepsilon_{\chi' \chi''}$$

et par suite

$$c(\varepsilon_\chi) = \varepsilon_\chi \otimes 1 + 1 \otimes \varepsilon_\chi + \sum_{\chi' \chi'' = \chi} w_{\chi', \chi''}\, \varepsilon_{\chi'} \otimes \varepsilon_{\chi''}.$$

Le schéma en groupes G', dual de G, a une bigèbre A' égale à la bigèbre sur D du groupe fini F^+ ([4], p. 3). Si $\mathbf{a}$ ($a \in F^+$) est la base canonique de A', on a donc

$$\mathbf{ab} = \mathbf{c} \qquad \text{avec} \quad c = a+b$$

et

$$c'(\mathbf{a}) = \mathbf{a} \otimes \mathbf{a}.$$

L'idéal d'augmentation I' de A' est formé des éléments $\sum t_a \mathbf{a}$ tels que $\sum t_a = 0$. La base $(\mathbf{a})$ ($a \in F^+$) est la base duale de (ε_a).

Pour tout $\lambda \in F$, on a $[\lambda]' \mathbf{a} = \mathbf{b}$ avec $b = \lambda a$, et I'_χ est engendré par

$$e_\chi = \sum \chi^{-1}(a)\mathbf{a} \qquad \text{si} \quad \chi \neq 1$$

et par

$$e_1 = \sum \mathbf{a} - q\mathbf{o} \qquad \text{si} \quad \chi = 1.$$

La base (e_χ) de I' est en dualité avec la base $(\varepsilon_\chi (q-1))$ de I. Par transposition, on déduit alors de (12) les formules

$$(12\,bis) \qquad \begin{cases} e_{\chi'} e_{\chi''} = (q-1)\, w_{\chi',\chi''} e_{\chi'\chi''}, \\ c'(e_\chi) = e_\chi \otimes 1 + 1 \otimes e_\chi + \dfrac{1}{q-1} \sum_{\chi'\chi''=\chi} e_{\chi'} \otimes e_{\chi''}. \end{cases}$$

Pour pouvoir comparer G et G', introduisons la sous-C-extension $\tilde{C}$ de $\overline{\mathbf{Q}}$ engendrée par les racines p-ièmes de l'unité, et soit $\tilde{D}$ la fermeture intégrale de D dans $\tilde{C}$. Notons ψ un caractère non trivial de F^+ à valeurs dans $\mu_p(\tilde{D})$. Alors ψ permet de définir un D-morphisme de schémas en F-vectoriels

$$G_D \to G'_D$$

qui envoie $a \in F^+$ sur $a\psi$; $F^+ \to \mu_p(\tilde{D})$, considéré comme élément de

$$G'(D) = \mathrm{Hom}_{\mathrm{gr}}(F^+, \tilde{D}^*).$$

Ce morphisme correspond à un morphisme de bigèbres

$$A' \otimes_D \tilde{D} \xrightarrow{u} A \otimes_D \tilde{D},$$
$$\mathbf{a} \to \sum_{\lambda \in F} \psi(\lambda a)\varepsilon_\lambda.$$

On a alors : $u(e_\chi) = g(\chi)\,\varepsilon_\chi$ avec

$$(13) \qquad \begin{cases} g(1) = -q, \\ g(\chi) = \sum_{a \in F} \chi^{-1}(a)\psi(a) \qquad \text{pour} \quad \chi \neq 1, \end{cases}$$

i.e. $g(\chi)$ est la *somme de Gauss* relative au caractère multiplicatif χ^{-1} et au caractère additif ψ).

En comparant avec les formules (12) et (12 *bis*), on trouve

$$w_{\chi', \chi''} = \frac{1}{q-1} \frac{g(\chi')g(\chi'')}{g(\chi'\chi'')}.$$

On déduit alors de (7) :

$$(14) \qquad w_{\chi_1, \ldots, \chi_n} = \frac{1}{(q-1)^{n-1}} \frac{g(\chi_1)\ldots g(\chi_n)}{g(\chi_1 \ldots \chi_n)}.$$

Notons encore les formules suivantes, conséquences des propriétés élémentaires des sommes de Gauss :

Pour $\chi \neq 1$, on a $g(\chi)g(\chi^{-1}) = q\chi(-1)$ (*cf.* [14], p. 501).

Par suite, si chacun des χ_j est différent de 1, on a

$$(15) \qquad w_{\chi_1, \ldots, \chi_n} w_{\chi_1^{-1}, \ldots, \chi_1^{-1}} = \left(\frac{q}{(q-1)^2}\right)^{n-1}.$$

Si l'on prend pour caractère additif ψ le composé de la trace $F \to \mathbf{Z}/p\mathbf{Z}$ et d'un caractère non trivial de $\mathbf{Z}/p\mathbf{Z}$ à valeurs dans $\mu_p(\tilde{D})$, on a

$$g(\chi^p) = g(\chi) \quad ([8], \text{p. } 93).$$

Par suite

$$(16) \qquad w_{\chi_1^p, \ldots, \chi_n^p} = w_{\chi_1, \ldots, \chi_n}.$$

Il résulte de cette dernière formule que les $w_{\chi_1, \ldots, \chi_n}$ se trouvent dans le sous-anneau D_1 de D formé des éléments invariants par le Frobenius de $\mathrm{Gal}(C/\mathbf{Q})$.

Étudions maintenant le groupe diagonalisable $G' \otimes_D k$, où $k = k(\mathfrak{p})$ est le corps résiduel en $\mathfrak{p}$. L'action de F sur G' respecte l'idéal d'augmentation I', donc définit par passage au quotient une action sur I'/I'^2 et aussi $\mathrm{Hom}_D(I'/I'^2, k)$ qui n'est autre que l'algèbre de Lie $\overline{L}$ de $G' \otimes_D k$. Par ailleurs, pour tout D-schéma T, on a

$$G'(T) = \mathrm{Hom}_{\mathrm{gr}}(F^+, \Gamma(T, \mathcal{O}_T^*)).$$

Prenant pour T l'algèbre des nombres duaux sur k, on en déduit que $\bar{L}$ est canoniquement isomorphe à $\mathrm{Hom}_{gr}(F^+, k^+)$. Or, si $h : F^+ \to k^+$ est un homomorphisme tel que $h(1) = 1$, h est un vecteur propre de $\bar{L}$, pour l'action de F^*, si, et seulement si, h est multiplicatif, donc provient d'un morphisme de corps $F \to k$. On voit ainsi que les caractères de F^* qui interviennent dans l'action de F^* sur $\bar{L}$, donc aussi sur I'/I'^2, sont les r-caractères fondamentaux χ_i. Autrement dit, $(I'/I'^2) \otimes_D k$ admet pour base les images $\bar{e}_i$ des éléments $e_i = e_{\chi_i}$. Comme $G' \otimes_D k$ est un groupe radiciel de hauteur 1 (isomorphe à μ_p^r), la k-algèbre $A' \otimes_D k$ est engendrée par les $\bar{e}_i$, liés par les seules relations $(\bar{e}_i)^p = 0$.

D'après (16), w_i, défini en (11 *bis*), ne dépend pas de i. On pose

$$w = w_i. \tag{17}$$

PROPOSITION 1.3.1.

1° *Soit* $\chi \in M$ *et* $\chi = \prod_i \chi_i^{a_i}$ *son écriture p-adique. Alors* w_χ *est un élément inversible de* D_1, *et l'on a*

$$w_\chi \equiv a_1! \ldots a_r! \pmod{p}.$$

2° *On a* $w \equiv p! \pmod{p^2}$ *et* $w = pu$, *où* u *est une unité de* D_1 *telle que* $u \equiv -1 \pmod{p}$.

Démonstration. — Il résulte déjà de (15) que w_χ et w sont inversibles dans le localisé de D_1 en (p). Par ailleurs, les considérations précédentes montrent que l'on a

$$\prod_i e_i^{a_i} \neq 0 \pmod{p} \qquad \text{et} \qquad e_i^p = 0 \pmod{p}.$$

En comparant avec (12 *bis*), on trouve que w_χ est une unité de D_1 tandis que $w \equiv 0 \pmod{p}$. Soient

$$\chi' = \prod_i \chi_i^{a_i'} \qquad \text{et} \qquad \chi'' = \prod_i \chi_i^{a_i''}$$

des caractères dont le produit $\chi' \chi''$ soit un caractère fondamental χ_i. Il existe alors un indice j pour lequel on a $a_j' + a_j'' \geqq p$, et par suite $w_{\chi', \chi''} \equiv 0 \pmod{p}$. Il résulte de (12) que l'on a

$$c(\varepsilon_{\chi_i}) \equiv 1 \otimes \varepsilon_{\chi_i} + \varepsilon_{\chi_i} \otimes 1 \pmod{p}.$$

Plus généralement, pour tout entier $n > 0$, le coproduit itéré c_n est tel que

$$c_n(\varepsilon_{\chi_i}) \equiv \varepsilon_{\chi_i} \otimes 1 \otimes \ldots \otimes 1 + \ldots + 1 \otimes \ldots \otimes 1 \otimes \varepsilon_{\chi_i} \pmod{p}.$$

Prenons $n = \sum_i a_i$, et calculons $c_n(\varepsilon_\chi) = c_n(\prod_i \varepsilon_{\chi_i}^{a_i})$ (12). Comme c_n est un morphisme d'algèbres, on trouve que le coefficient de $\varepsilon_{\chi_1}^{\otimes a_1} \otimes \ldots \otimes \varepsilon_{\chi_r}^{\otimes a_r}$ dans $c_n(\varepsilon_\chi)$ est congru à $a_1! \ldots a_r! \pmod p$. Par ailleurs, compte tenu de (12) et des définitions, ce coefficient est aussi égal à w_χ. De même, en calculant le coefficient de $\varepsilon_{\chi_i}^{\otimes p}$ dans le développement de $c_p(\varepsilon_{\chi_i}^p)$, on trouve $w \equiv p! \pmod{p^2}$. La dernière assertion de la proposition résulte de la congruence $(p-1)! \equiv -1 \pmod p$.

1.4. CLASSIFICATION DES SCHÉMAS EN F-VECTORIELS. — Soient de nouveau S un D-schéma, et G un S-schéma en F-vectoriels vérifiant ($\star\star$). Nous allons cesser de traiter symétriquement le point de vue algèbre et cogèbre, et utiliser la proposition 2 pour écrire simplement la multiplication dans l'algèbre $\mathscr{A}$ de G.

Notons $\mathscr{S}$ l'algèbre symétrique du $\mathscr{O}_S$-module $\oplus_i \mathscr{I}_{\chi_i}$. Alors $\mathscr{S}$ est somme directe des $\mathscr{O}_S$-modules inversibles « monômes » en les $\mathscr{I}_{\chi_i}$:

$$\mathscr{S} = \oplus_{n_i \geq 0} \prod_i \mathscr{I}_{\chi_i}^{n_i}.$$

On note can : $\mathscr{I}_{\chi_1}^{\otimes n_1} \otimes \ldots \otimes \mathscr{I}_{\chi_r}^{\otimes n_r} \xrightarrow{\sim} \prod_i \mathscr{I}_{\chi_i}^{n_i}$ l'isomorphisme canonique.

Soient $\chi \in M$, et $\chi = \prod_i \chi_i^{a_i}$ son écriture p-adique. On reprend les formules (11) et (11 *bis*) en posant

$$(18) \qquad \begin{cases} \bar{c}_\chi = (\text{can}) \circ c_\chi & : \ \mathscr{I}_\chi \to \prod_i \mathscr{I}_{\chi_i}^{a_i}, \\ \bar{d}_\chi = (d_\chi) \circ (\text{can})^{-1} & : \ \prod_i \mathscr{I}_{\chi_i}^{a_i} \to \mathscr{I}_\chi, \\ \bar{c}_i = (\text{can}) \circ c_i & : \ \mathscr{I}_{\chi_{i+1}} \to \mathscr{I}_{\chi_i}^p, \\ \bar{d}_i = (d_i) \circ (\text{can})^{-1} & : \ \mathscr{I}_{\chi_i}^p \to \mathscr{I}_{\chi_{i+1}}. \end{cases}$$

On a donc $\bar{c}_i \bar{d}_i = w$ et $\bar{c}_\chi \bar{d}_\chi = w_\chi$, de sorte que $\bar{d}_\chi$ et $\bar{c}_\chi$ sont des isomorphismes (prop. 1.3.1).

Considérons alors le $\mathscr{O}_S$-module localement libre de rang q :

$$\otimes_{0 \leq a_i \leq p-1} \prod_i \mathscr{I}_{\chi_i}^{a_i} = \mathscr{O}_S \otimes (\otimes_{0 \leq a_i \leq p-1} \prod_i \mathscr{I}_{\chi_i}^{a_i}) \qquad \text{(et les } a_i \text{ non tous nuls).}$$

Grâce aux isomorphismes $\bar{d}_\chi$ on transporte sur ce module la structure de bigèbre de $\mathscr{A}$.

On peut alors expliciter la multiplication de la façon suivante : si

$$\chi' = \prod \chi_i^{a_i'} \qquad \text{et} \qquad \chi'' = \prod \chi_i^{a_i''}$$

sont deux caractères tels que $a'_i + a''_i \leqq p-1$, pour tout i, la multiplication de $\prod_i \mathscr{I}_{\chi_i}^{a'_i}$ et de $\prod_i \mathscr{I}_{\chi_i}^{a''_i}$ est donnée par l'isomorphisme canonique

$$(\prod_i \mathscr{I}_{\chi_i}^{a'_i}) \otimes (\prod_i \mathscr{I}_{\chi_i}^{a''_i}) \xrightarrow{\sim} \prod_i \mathscr{I}_{\chi_i}^{a'_i + a''_i}, \tag{19}$$

tandis que l'élévation à la puissance p-ième est donnée sur les générateurs $\mathscr{I}_{\chi_i}$ par l'application

$$\bar{d}_i : \mathscr{I}_{\chi_i}^{p} \to \mathscr{I}_{\chi_{i+1}}. \tag{19 bis}$$

Explicitons maintenant la structure de cogèbre. Il nous suffit de décrire l'application

$$c_{\chi', \chi''} : \mathscr{I}_{\chi_i} \to (\prod_j \mathscr{I}_{\chi_j}^{a'_j}) \otimes (\prod_j \mathscr{I}_{\chi_j}^{a''_j})$$

pour tout i et tout couple de caractères $\chi' = \prod_j \chi_j^{a'_j}$ et $\chi'' = \prod_j \chi_j^{a''_j}$ tels que $\chi' \chi'' = \chi_i$. Notons qu'il existe un unique entier h, $0 < h \leqq r$ tel que l'on ait

$$\begin{cases} a'_{i-h} + a''_{i-h} = p, \\ a'_{i-k} + a''_{i-k} = p-1 \quad \text{pour} \quad 0 < k < h, \\ a'_j = a''_j = 0 \quad \text{sinon.} \end{cases} \tag{20}$$

Considérons alors l'application donnée par la comultiplication itérée :

$$\mathscr{I}_{\chi_i} \to \mathscr{I}_{\chi_{i-h}}^{\otimes p} \otimes \mathscr{I}_{\chi_{i-h+1}}^{\otimes p-1} \otimes \ldots \otimes \mathscr{I}_{\chi_{i-1}}^{\otimes p-1}.$$

En utilisant les règles d'associativité (6), on peut la calculer de deux façons différentes de sorte que le diagramme ci-dessous est commutatif :

$$\begin{array}{ccccc} & & \mathscr{I}_{\chi_{i-1}}^{\otimes p} \xrightarrow{\sim} \mathscr{I}_{\chi_{i-1}} \otimes \mathscr{I}_{\chi_{i-1}}^{\otimes p-1} \xrightarrow{c_{i-2} \otimes id} \mathscr{I}_{\chi_{i-2}}^{\otimes p} \otimes \mathscr{I}_{\chi_{i-1}}^{\otimes p-1} \to \ldots & & \\ & \overset{c_{i-1}}{\nearrow} & & & \to \mathscr{I}_{\chi_{i-h}}^{\otimes p} \otimes \mathscr{I}_{\chi_{i-h+1}}^{\otimes p-1} \otimes \ldots \otimes \mathscr{I}_{\chi_{i-1}}^{p-1} \\ \mathscr{I}_{\chi_i} & & & & \| \\ & \underset{c_{\chi', \chi''}}{\searrow} & & & \\ & & \mathscr{I}_{\chi'} \otimes \mathscr{I}_{\chi''} \xrightarrow[c_{\chi'} \otimes c_{\chi''}]{} (\mathscr{I}_{\chi_{i-h}}^{\otimes a'_{i-h}} \otimes \ldots \otimes \mathscr{I}_{\chi_{i-1}}^{\otimes a'_{i-1}}) \otimes (\mathscr{I}_{\chi_{i-h}}^{\otimes a''_{i-h}} \otimes \ldots \otimes \mathscr{I}_{\chi_{i-1}}^{\otimes a''_{i-1}}) & & \end{array}$$

Comme $c_{\chi'}$ et $c_{\chi''}$ sont inversibles, on voit que $c_{\chi', \chi''}$ est déterminé en fonction des c_j. Utilisant les isomorphismes d_χ, on peut écrire symboliquement

$$c_{\chi', \chi''} = \frac{\bar{c}_{i-h} \cdots \bar{c}_{i-1}}{w_{\chi'} w_{\chi''}}. \tag{21}$$

THÉORÈME 1.4.1. — *Soit S un D-schéma. L'application*

$$G \mapsto (\mathscr{I}_{\chi_i},\ \bar{c}_i : \mathscr{I}_{\chi_{i+1}} \to \mathscr{I}_{\chi_i}^p,\ \bar{d}_i : \mathscr{I}_{\chi_i}^p \to \mathscr{I}_{\chi_{i+1}})$$

définit une bijection entre les classes d'isomorphismes de S-schémas en F-vectoriels G vérifiant $(\star\star)$ et les classes d'isomorphismes des systèmes formés de r $\mathscr{O}_S$-modules inversibles $\mathscr{L}_i$ et de r-couples d'applications $\mathscr{O}_S$-linéaires :

$$(22) \qquad \begin{cases} \bar{c}_i : & \mathscr{L}_{i+1} \to \mathscr{L}_i^p = \mathscr{L}_i^{\otimes p}, \\ \bar{d}_i : & \mathscr{L}_i^p \to \mathscr{L}_{i+1} \end{cases}$$

tels que $\bar{d}_i \circ \bar{c}_i = w\,\mathrm{id}_{\mathscr{L}_{i+1}}$ pour tout i.

Démonstration. — Compte tenu de ce qui précède, il reste à montrer comment on construit un schéma en F-vectoriels G à partir des données $(\mathscr{L}_i, \bar{c}_i, \bar{d}_i)$.

Pour ce faire, considérons l'algèbre symétrique $\mathscr{S}$ de $\oplus_i \mathscr{L}_i$:

$$\mathscr{S} = \oplus_{a_i \geq 0} (\prod_i \mathscr{L}_i^{a_i}).$$

Considérons le $\mathscr{O}_S$-module localement libre de rang q :

$$\mathscr{A} = \oplus_{0 \leq a_i \leq p-1} (\prod_i \mathscr{L}_i^{a_i}) = \mathscr{O}_S \oplus (\oplus_{\chi \in M} \mathscr{I}_\chi),$$

où, pour tout $\chi = \prod_i \chi_i^{a_i}$, on a posé $\mathscr{I}_\chi = \prod_i \mathscr{L}_i^{a_i}$. On munit $\mathscr{A}$ de la structure de $\mathscr{O}_S$-algèbre commutative définie par les formules (19) et (19 *bis*). Alors l'algèbre $\mathscr{A}$ est engendrée par les faisceaux $\mathscr{I}_{\chi_i}$, de sorte qu'il existe au plus une structure de bigèbre sur $\mathscr{A}$, pour laquelle la comultiplication c vérifie (21). Nous allons voir que cette bigèbre existe effectivement et que, munie de sa graduation de type M, elle correspond à un S-schéma en F-vectoriels G. On aura ainsi décrit une application inverse de celle considérée dans le théorème 1.4.1.

L'existence du S-schéma, G ayant les propriétés requises, devient un problème de nature locale sur S, ce qui nous ramène au cas où S est affine et les $\mathscr{L}_i$ libres. Il nous suffit alors de vérifier l'existence de G dans le cas « universel » où $S = \mathrm{Spec}\,(E)$, E étant le quotient de l'anneaux de polynômes $D[U_1, \ldots, U_r, V_1, \ldots, V_r]$ par l'idéal engendré par les éléments $U_i V_i - w$. Notons u_i (resp. v_i) l'image de U_i (resp. V_i) dans E.

Nous sommes amenés à étudier la E-algèbre libre « universelle »

$$A = E[X_1, \ldots, X_r]/\mathfrak{a},$$

où $\mathfrak{a}$ est l'idéal engendré par les éléments $X_i^p - v_i X_{i+1}$.

Notons que E est une D-algèbre intègre, dans laquelle p n'est pas diviseur de zéro. Il nous suffiit donc de vérifier les propriétés de la comultiplication c après localisation par (p).

Soit E' la E-algèbre finie libre $E[T]/(T^{q-1} - v_1^{p^{r-1}} v_2^{p^{r-2}} \dots v_r)$. Comme E' est fidèlement plate sur E, il suffit de vérifier les propriétés de c au-dessus de $E'_{(p)}$. En fait, on va prouver le lemme plus précis suivant :

LEMME 1.4.2. — *Soit* $S' = \mathrm{Spec}(E')$, *et soit* H *le* S'*-schéma en F-vectoriels constant défini par* F^+. *Alors il existe un* S'*-morphisme de schémas en F-vectoriels*

$$H \to G_{S'}$$

qui est un isomorphisme au-dessus de $S'_{(p)}$.

Considérons le système d'équations

$$T_i^p = v_i T_{i+1}. \tag{23}$$

Par élimination de $T_2, \dots, T_r$, on déduit de (23) que T_1 satisfait à l'équation

$$T_1^q = v_1^{p^{r-1}} v_2^{p^{r-2}} \dots v_r T_1. \tag{24}$$

L'image t_1 de T dans E' est solution de (24). Comme $u_i v_i = w$, où w est le produit d'une unité par p, t_1 est non diviseur de zéro dans E', et les v_i sont inversibles dans $E'_{(p)}$. Il est immédiat de vérifier que les équations (23) admettent une unique solution dans E' de la forme $(t_1, \dots, t_r)$ et que les t_i sont inversibles dans $E'_{(p)}$.

Soit B la bigèbre de H. Il résulte de (12) que l'algèbre sous-jacente à B est engendrée par les ε_{χ_i} liés par les relations $\varepsilon_{\chi_i}^p = \varepsilon_{\chi_{i+1}}$. Vu le choix des t_i, il existe donc un morphisme d'algèbres

$$\alpha : \quad A' = A \otimes_E E' \to B$$

qui envoie X_i sur $t_i \varepsilon_{\chi_i}$ pour tout i, et α est un isomorphisme au-dessus de $E'_{(p)}$.

Soient $\chi' = \prod_i \chi_i^{a'_i}$ et $\chi'' = \prod_i \chi_i^{a''_i}$ deux caractères tels que $\chi' \chi'' = \chi_i$ et vérifiant les conditions (20). On a alors

$$\begin{aligned}
&(\alpha \otimes \alpha)[(\textstyle\prod_j X_j^{a''_j}) \otimes (\prod_j X_j^{a'_j})] \\
&\quad = (\textstyle\prod_j t_j^{a'_j + a''_j})(\varepsilon_{\chi'} \otimes \varepsilon_{\chi''}) \\
&\quad = t_{i-h}^p t_{i-h+1}^{p-1} \dots t_{i-1}^{p-1} (\varepsilon_{\chi'} \otimes \varepsilon_{\chi''}) \quad \text{d'après (20)} \\
&\quad = v_{i-h} \dots v_{i-1} t_i (\varepsilon_{\chi'} \otimes \varepsilon_{\chi''}) \quad \text{d'après (23).}
\end{aligned}$$

Par définition de c, et d'après (21), la composante de $c(X_i)$ suivant $(\prod_j X_j^{a'_j}) \otimes (\prod_j X_j^{a''_j})$ est égale à $(u_{i-h} \dots u_{i-1})/w_{\chi'} w_{\chi''}$. Par suite, la composante de $(\alpha \otimes \alpha) \circ c(X_i)$ suivant $\varepsilon_{\chi'} \otimes \varepsilon_{\chi''}$ est égale à

$$\frac{u_{i-h} \dots u_{i-1} v_{i-h} \dots v_{i-1}}{w_{\chi'} w_{\chi''}} t_i = \frac{w^h}{w_{\chi'} w_{\chi''}} t_i.$$

Par ailleurs, si on note c_H la comultiplication dans B, il résulte de (12) et de (21) que l'on a

$$(c_H)_{\chi', \chi''} \varepsilon_{\chi_i} = w_{\chi', \chi''} \varepsilon_{\chi'} \otimes \varepsilon_{\chi''} = \frac{w^h}{w_{\chi'} w_{\chi''}} \varepsilon_{\chi'} \otimes \varepsilon_{\chi''}.$$

Il en résulte que $c_H \circ \alpha(X_i)$ et $(\alpha \otimes \alpha) \circ c(X_i)$ ont même composante suivant $\varepsilon_{\chi'} \otimes \varepsilon_{\chi''}$. Comme α est injectif, on voit, finalement que c se prolonge en une comultiplication sur A, pour laquelle α est un morphisme de bigèbres compatible avec l'action de F.

1.5. REMARQUES ET EXEMPLES. — Soit S un D-schéma qui est le spectre d'un anneau local R. Tout $\mathcal{O}_S$-module inversible est alors libre, et le théorème 1.4.1 et la formule (21) donnent le résultat suivant :

COROLLAIRE 1.5.1. — *Un S-schéma en F-vectoriels G vérifiant* (★★) *équivaut à la donnée de r couples* (γ_i, δ_i) *d'éléments de R tels que* $\gamma_i \delta_i = w$ *pour tout i. De plus, G admet pour système d'équations* $X_i^p = \delta_i X_{i+1}$, *et la comultiplication est donnée par la formule*

$$c(X_i) = X_i \otimes 1 + 1 \otimes X_i + \sum_{\chi'\chi'' = \chi_i} \frac{\gamma_{i-h} \cdots \gamma_{i-1}}{w_{\chi'} w_{\chi''}} (\prod_j X_j^{a'_j}) \otimes (\prod_j X_j^{a''_j}),$$

où l'on a posé $\chi' = \prod_j \chi_j^{a'_j}$, $\chi'' = \prod_j \chi_j^{a''_j}$, *et où h est défini par les conditions* (20).

De plus, des familles de couples (γ_i, δ_i) *et* (γ'_i, δ'_i), *tels que* $\gamma_i \delta_i = \gamma'_i \delta'_i = w$ *our tout i, définissent des schémas en F-vectoriels isomorphes si, et seulement si, il existe une famille d'unités* u_i *de R telle que*

$$\delta'_i = u_i^p \delta_i u_{i+1}^{-1} \qquad et \qquad \gamma_i = u_i^p \gamma'_i u_{i+1}^{-1} \quad pour\ tout\ i.$$

Supposons plus précisément que R est un anneau de valuation discrète strictement hensélien, de corps des fractions de caractéristique 0 et de corps résiduel de caractéristique p. Soient π une uniformisante, et v la

valuation sur R normalisée par $v(\pi) = 1$. Notons $e = v(p)$ l'indice de ramification absolue.

COROLLAIRE 1.5.2. — *Il existe une bijection canonique entre les R-schémas en F-vectoriels de rang q et les familles de r entiers n, telles que $0 \leqq n_i \leqq e$ pour tout i.*

En effet, reprenant les notations du corollaire 1.5.1, à un schéma en F-vectoriels G, défini par les r-couples (γ_i, δ_i), tels que $\gamma^i \delta_i = w$, on fait correspondre la famille d'entiers $n_i = v(\delta_i)$. Il reste à voir que si α_i est une famille de r unités de R, le R-schéma en F-vectoriels, défini par les couples $(\gamma'_i = \alpha_i \gamma_i, \delta'_i = \alpha_i^{-1} \delta_i)$, est isomorphe à G. D'après le corollaire 1.5.1, il nous faut trouver une famille de r unités u_i de R telle que

$$\delta'_i u_{i+1} = \delta_i u_i^p \quad \text{pour tout } i.$$

Par élimination, on trouve que u_i doit être solution de l'équation

$$u_i^{q-1} = (\alpha_i)^{p^{r-1}} (\alpha_{i+1})^{p^{r-2}} \dots \alpha_{i+r-1}.$$

Cette équation admet une solution puisque R est strictement hensélien.

REMARQUES :

1.5.3. Si un S-schéma en F-vectoriels G est défini par un système $(\mathscr{L}_i, \bar{c}_i, \bar{d}_i)$ du type considéré dans le théorème 1.4.1, on vérifie que le dual de Cartier G' de G est le schéma en F-vectoriels défini par le système $(\mathscr{L}'_i, \bar{c}'_i, \bar{d}'_i)$, où $\mathscr{L}'_i$ est le $\mathscr{O}_S$-module inversible dual de $\mathscr{L}_i$, et $\bar{c}'_i$ (resp. $\bar{d}'_i$) est le transposé de $\bar{d}_i$ (resp. $\bar{c}_i$).

1.5.4. Soit S un schéma local complet de caractéristique résiduelle p. Alors, avec les notations du corollaire 1.5.1, on peut montrer que la famille de couples (γ_i, δ_i) définit un S-schéma en groupes isomorphe au noyau de l'élévation à la puissance p-ième dans un S-groupe p-divisible [13], si, et seulement si, pour tout i, l'un des coefficients γ_i ou δ_i est une unité. C'est toujours le cas si S est le spectre d'un anneau de valuation discrète, d'inégales caractéristiques, absolument non ramifié.

1.5.5. Rappelons que l'on a défini D_1 comme étant le sous-anneau de D formé des invariants sous le Frobenius de $\mathrm{Gal}(C/\mathbf{Q})$, et que D_1 contient les coefficients w et w_χ. Soient alors S un schéma au-dessus de D_1, et $(\mathscr{L}_i, \bar{c}_i, \bar{d}_i)$ un système sur S du type considéré dans le théorème 1.4.1. Ce système définit donc, au-dessus de $S \otimes_{D_1} D$, un schéma en F-vectoriels.

Comme w et les w_χ sont dans D_1, la bigèbre de ce schéma en F-vectoriels est déjà définie sur S, et correspond à un S-schéma en groupes fini, commutatif G, localement libre de rang q. La bigèbre de G est une bigèbre graduée par le groupe M des caractères de F^*. Cette graduation définit canoniquement une action du groupe de type multiplicatif $(F^*)'$, dual de Cartier du groupe constant F^*. Comme $(F^*)'$ n'est pas en général constant sur D_1, G n'est pas nécessairement un S-schéma en F-vectoriels. Il est néanmoins facile d'interpréter les S-schémas en groupes ainsi obtenus. En effet, pour tout S-schéma en anneaux $\mathbf{A}$, on a la notion de schéma en $\mathbf{A}$-modules. Ainsi, les schémas en F-vectoriels sont les schémas en $\mathbf{A}$-modules, où l'on prend pour $\mathbf{A}$ le schéma en anneaux, constant, associé au corps F. Or, au-dessus de D_1, il existe un schéma en anneau $\mathbf{E}$, qui est une « forme » du précédent, et qui est caractérisé par le fait que son groupe des unités est isomorphe au dual de Cartier de F^*. Sa bigèbre de groupe est définie au-dessus de D_1 par les équations (12); pour tout D_1-schéma T, $\mathbf{E}(T)$ est égal à l'ensemble des morphismes (non nécessairement unitaires) du monoïde multiplicatif de F dans le monoïde multiplicatif de $\Gamma(T, \mathcal{O}_T)$. Ceci étant, les systèmes $(\mathscr{L}_i, \bar{c}_i, \bar{d}_i)$ classent les S-schémas en modules sur $\mathbf{E}$, qui vérifient $(\star\star)$.

2. Adhérence schématique sur un anneau de valuation discrète

Dans ce paragraphe et les deux suivants, on considère un anneau de valuation discrète R, de corps des fractions K, de corps résiduel k de caractéristique p. On désigne par π une uniformisante de R, et par v la valuation normalisée ($v(\pi) = 1$). Dans le cas d'inégales caractéristiques, on désigne par $e = v(p)$ l'indice de ramification absolue de R.

2.1. L'OPÉRATION « ADHÉRENCE SCHÉMATIQUE ». — Soient $\mathscr{X}$ un R-schéma de type fini, $X = \mathscr{X} \otimes_R K$ sa fibre générique, JY un sous-schéma fermé de X. On appelle adhérence schématique de Y dans $\mathscr{X}$, le plus petit sous-schéma fermé $\mathscr{Y}$ de $\mathscr{X}$ qui contient Y. Comme Y est fermé dans X, on a $Y = \mathscr{Y} \otimes_R K$. Soit $\mathscr{U}$ un ouvert affine de $\mathscr{X}$ d'anneau $\mathscr{A}$, de sorte que $U = X \cap \mathscr{U}$ a pour anneau $A = \mathscr{A} \otimes_R K$. Si $Y \cap U$ est défini par l'idéal I de A, $\mathscr{Y} \cap \mathscr{U}$ est défini par l'idéal $\mathscr{I}$ de $\mathscr{A}$, image réciproque de I. En particulier, l'application $\mathscr{A}/\mathscr{I} \to A/I$ est injective, donc $\mathscr{A}/\mathscr{I}$ est sans torsion, et $\mathscr{Y}$ est plat sur R (*cf.* [5], p. 33). Il en résulte que la formation de l'adhérence schématique commute aux produits fibrés sur R et, par suite, si $\mathscr{X}$ est un R-schéma en groupes et Y un sous-schéma en

groupes de X, alors $\mathscr{Y}$ est un sous-schéma en groupes fermé de $\mathscr{X}$, plat sur R. Si de plus $\mathscr{X}$ est fini sur R, il en est de même de $\mathscr{Y}$, et le quotient $\mathscr{X}/\mathscr{Y}$ (pour la topologie *fppf*) est représentable par un schéma fini sur R.

2.2. RELATIONS D'ORDRE SUR LES PROLONGEMENTS. — Soit G un K-schéma en groupes, fini, commutatif, et soient $\mathscr{G}$ et $\mathscr{G}'$ des R-schémas en groupes finis et plats (nécessairement commutatifs) qui prolongent G. Dans la suite, on identifie les fibres génériques de $\mathscr{G}$ et $\mathscr{G}'$ avec G.

DÉFINITION 2.2.1. — *On dit que $\mathscr{G}$ domine $\mathscr{G}'$, et on écrit $\mathscr{G} \geqq \mathscr{G}'$ s'il existe un R-morphisme $u : \mathscr{G} \to \mathscr{G}'$ qui prolonge l'identité de G.*

Si un tel u existe, il est unique, et c'est un morphisme de R-schémas en groupes. Si l'on identifie les anneaux $\mathscr{A}$ et $\mathscr{A}'$ de $\mathscr{G}$ et $\mathscr{G}'$ à des sous-anneaux de l'anneau A de G, on a $\mathscr{G} \geqq \mathscr{G}'$ si, et seulement si, $\mathscr{A}' \subset \mathscr{A}$. On définit ainsi une relation d'ordre partiel sur les classes d'isomorphismes de prolongements de G qui sont finis et plats sur R.

PROPOSITION 2.2.2. — *Soient $\mathscr{G}$ et $\mathscr{G}'$ des prolongements finis et plats d'un K-schéma en groupes commutatif G. Alors $\mathscr{G}$ et $\mathscr{G}'$ possèdent une borne supérieure et une borne inférieure.*

Démonstration. — Considérons le produit $\mathscr{G} \times_R \mathscr{G}'$, sa fibre générique $G \times_K G$, et le noyau N du morphisme

$$G \times_K G \to G,$$
$$(g, g') \mapsto g - g'.$$

Soit $\mathscr{N}$ l'adhérence schématique de N dans $\mathscr{G} \times_R \mathscr{G}'$, et considérons le diagramme

$$\begin{array}{ccccc} & & & \xrightarrow{p_1} & \mathscr{G} \\ & \overset{i}{} & & \nearrow & \\ \mathscr{N} & \to & \mathscr{G} \times_R \mathscr{G}' & & \\ & & & \searrow & \\ & & & \xrightarrow{p_2} & \mathscr{G}' \end{array}$$

Les applications $p_1 \circ i$ et $p_2 \circ i$ donnent le même isomorphisme sur la fibre générique, donc $\mathscr{N}$ est un prolongement fini et plat de G qui domine $\mathscr{G}$ et $\mathscr{G}'$. On vérifie immédiatement que $\mathscr{N}$ est une borne supérieure de $\mathscr{G}$ et $\mathscr{G}'$.

Par dualité de Cartier, on échange les rôles des bornes supérieures et des bornes inférieures.

COROLLAIRE 2.2.3. — *Soit G un K-schéma en groupes, fini, commutatif, qui possède un prolongement sur R fini et plat.*

1° *Si G est étale (resp. de type multiplicatif), l'ensemble des prolongements finis et plats de G possède un maximum (resp. un minimum).*

2° *Si K est de caractéristique zéro, les prolongements finis et plats de G possèdent un maximum et un minimum.*

L'assertion 2° est un cas particulier du 1°. Les deux assertions du 1° s'échangent par dualité de Cartier. Examinons le cas où G est étale de K-algèbre A. Si $\mathscr{G}$ est un prolongement de G sur R, fini et plat, sa R-algèbre est contenue dans la fermeture intégrale de R dans A, qui est finie sur A. L'existence d'un maximum parmi les prolongements de G résulte de là et de la proposition 2.2.2.

2.3. APPLICATION : COMPLÉMENT A UN THÉORÈME DE TATE. — Supposons R d'inégales caractéristiques, de caractéristique résiduelle p. Dans [13] (p. 180), TATE a montré que si $\mathscr{G} = (\mathscr{G}_n)_{n\geqq 0}$ et $\mathscr{H} = (\mathscr{H}_n)_{n\geqq 0}$ sont des groupes p-divisibles définis sur R, tout morphisme entre les fibres génériques de $\mathscr{G}$ et $\mathscr{H}$ se prolonge de manière unique en un morphisme entre $\mathscr{G}$ et $\mathscr{H}$. Nous allons donner un critère d'existence d'un prolongement d'un groupe p-divisible de K à R.

PROPOSITION 2.3.1. — *Soit $G = (G_n)_{n\geqq 0}$ un groupe p-divisible défini sur K. Supposons que, pour tout $n \geqq 0$, G_n se prolonge en un R-schéma en groupes fini et plat. Alors G se prolonge en un R-groupe p-divisible $\mathscr{G}$, unique à isomorphisme près.*

Démonstration. — L'unicité du prolongement résulte du théorème de Tate. Prouvons l'existence. Pour tout $n \geqq 0$, on note $\mathscr{G}(n)$ un prolongement fini et plat sur R du groupe G_n.

(*a*) Pour tout $n \geqq 0$, on peut supposer que l'inclusion $G_n \subsetneq G_{n+1}$ se prolonge en un R-morphisme $\mathscr{G}(n) \to \mathscr{G}(n+1)$.

En effet, procédant par récurrence croissante sur n, il suffit de montrer que l'on peut modifier $\mathscr{G}(n+1)$ en un autre prolongement $\overline{\mathscr{G}(n+1)}$ de $\mathscr{G}(n+1)$ de G_{n+1}, de façon que l'inclusion $i_n : G_n \to G_{n+1}$ se prolonge en un R-morphisme

$$\mathscr{G}(n) \to \overline{\mathscr{G}(n+1)}.$$

Par dualité de Cartier, on obtient des R-groupes $\mathscr{G}(n)'$ et $\mathscr{G}(n+1)'$ et un épimorphisme $i'_n : G'_{n+1} \to G'_n$. Notons $\overline{(\mathscr{G}(n+1))'}$ l'adhérence schéma-

tique dans $\mathscr{G}(n+1)' \times_R \mathscr{G}(n)'$ du graphe de i'_n. On obtient ainsi un autre prolongement de G'_{n+1} et la projection canonique $\overline{(\mathscr{G}(n+1))'} \to (\mathscr{G}(n))'$ donne, par dualité, l'application cherchée $\mathscr{G}(n) \to \overline{\mathscr{G}(n+1)}$.

(*b*) Pour tout n, G_n est filtré par les sous-groupes G_i, $i \leqq n$, et les quotients successifs sont isomorphes à G_1. Prenant les adhérences schématiques des G_i dans $\mathscr{G}(n)$, on obtient une filtration de $\mathscr{G}(n)$ par des R-sous-schémas en groupes fermés et plats $\mathscr{G}(n)_i$ et les quotients successifs $\mathscr{G}(n)_i/\mathscr{G}(n)_{i-1} = \mathscr{G}^i_{(n)}$, $1 \leqq i \leqq n$, sont des prolongements de G_1 sur R.

Pour tout n et tout $i < n$, les morphismes $\mathscr{G}(n) \to \mathscr{G}(n+1)$ construits dans (*a*), induisent des morphismes $\mathscr{G}(n)_i \to \mathscr{G}(n+1)_i$ et, par passage au quotient, des morphismes

$$(\star) \qquad \mathscr{G}^i_{(n)} \to \mathscr{G}^i_{(n+1)}.$$

Autrement dit, pour i fixé, la suite des $\mathscr{G}^i_{(n)}$ est décroissante.

(*c*) L'élévation à la puissance p-ième dans $\mathscr{G}(n)$, induit sur la fibre générique des épimorphismes $G_i \to G_{i-1}$ pour $1 \leqq i \leqq n$, donc induit des applications $\mathscr{G}(n)_i - \mathscr{G}(n)_{i-1}$ et, par passage au quotient, définit des morphismes

$$(\star\star) \qquad \mathscr{G}^i_{(n)} \to \mathscr{G}^{i-1}_{(n)}.$$

Pour n fixé, les $\mathscr{G}^i_{(n)}$ forment donc une suite croissante de prolongements de G_1.

(*d*) Pour i fixé, il résulte du corollaire 2.2.3, que la suite décroissante $(\star)$ est stationnaire pour n assez grand. Notons $\mathscr{G}^i$ la valeur stationnaire.

Par ailleurs, pour tout n, on a, d'après $(\star\star)$, $\mathscr{G}^i_{(n)} \geqq \mathscr{G}^{i-1}_{(n)}$. Il en résulte que la suite des $\mathscr{G}^i$ est croissante, donc stationnaire pour $i \geqq i_0$, toujours d'après le corollaire 2.2.3.

(*e*) Pour établir la proposition 2.3.1, il est loisible de remplacer $\mathscr{G}(n)$ par $\mathscr{G}(n)/\mathscr{G}(n)_{i_0}$ pour tout n, donc on peut supposer $i_0 = 1$. Alors, pour tout i, l'application $(\star\star)$ $\mathscr{G}^i_{(n)} \to \mathscr{G}^{i-1}_{(n)}$ est un isomorphisme pour n assez grand. Par dévissage, on en déduit que, pour i et j *fixés* et n assez grand, la ligne horizontale du diagramme ci-dessous est exacte.

$$(\star\star\star) \qquad \begin{array}{ccccccccc} & & & & & & \mathscr{G}(n)_{i+j} & & \\ & & & & & \overset{p^i}{\nearrow} & \uparrow & & \\ 0 & \to & \mathscr{G}(n)_i & \subsetneq & \mathscr{G}(n)_{i+j} & \to & \mathscr{G}(n)_j & \to & 0 \end{array}$$

Cela étant, pour tout n, notons $\mathscr{G}_n$ la valeur stationnaire de la suite décroissante

$$\mathscr{G}(n) \to \mathscr{G}(n+1)_n \to \ldots \to \mathscr{G}(n+r)_n \ldots .$$

On déduit alors de (★★★) que, dans le diagramme ci-dessous, la ligne horizontale est exacte

$$\begin{array}{ccccccccc} & & & & & & \mathscr{G}_{i+j} & & \\ & & & & & \overset{p^i}{\nearrow} & \downarrow & & \\ 0 & \to & \mathscr{G}_i & \to & \mathscr{G}_{i+j} & \to & \mathscr{G}_j & \to & 0. \end{array}$$

Ceci prouve bien que $\mathscr{G} = (\mathscr{G}_i)$ est un R-groupe p-divisible, qui prolonge G.

3. Schémas en groupes finis et action du groupe de Galois

3.1. Structure du groupe de Galois modérément ramifié. — Ce numéro est directement issu de [12] (paragraphe 1).

Supposons que l'anneau de valuation discrète R soit strictement hensélien, et soit $\overline{K}$ une clôture séparable de K. Le groupe de Galois $\mathrm{Gal}(\overline{K}/K)$ coïncide donc avec le groupe d'inertie I.

Rappelons que l'on a une suite exacte canonique de groupes profinis :

$$0 \to I_p \to \mathrm{Gal}(\overline{K}/K) \to I_t \to 0,$$

où I_t est d'ordre premier à p, et correspond à l'inertie modérée, tandis que I_p est un pro-p-groupe correspondant à l'inertie sauvagement ramifiée.

Plus précisément, pour tout entier n, premier à p, il existe une unique sous-extension K_n de $\overline{K}$, de degré n sur K. Elle est galoisienne, et on a un isomorphisme canonique

$$i_n : \quad \mathrm{Gal}(K_n/K) \xrightarrow{\sim} \mu_n(K)$$

tel que, si v' désigne la valuation normalisée de K_n, on a, pour tout $x' \in K_n$ et tout $\sigma \in \mathrm{Gal}(K_n/K)$:

$$\sigma_{x'} = x'(i_n(\sigma))^{v'(x')}(1+u') \qquad \text{avec} \quad v'(u') \geqq 1.$$

Si m divise n, le diagramme suivant est commutatif :

$$\begin{array}{ccc} \mathrm{Gal}(K_n/K) & \xrightarrow{i_n} & \mu_n(K) \quad \omega \\ {\scriptstyle \mathrm{can}}\downarrow & & \downarrow{\scriptstyle \varphi_{n,m}} \quad \downarrow \\ \mathrm{Gal}(K_m/K) & \xrightarrow{i_m} & \mu_m(K) \quad \omega^{n/m}. \end{array}$$

Ainsi, le groupe d'inertie modérée I_t s'identifie à $\varprojlim_{(n,p)=1} \mu_n(K)$. Les isomorphismes canoniques $\mu_n(K) \xrightarrow{\sim} \mu_n(k)$, pour $(n, p) = 1$, suggèrent un autre système cofinal de quotients finis de I_t. En effet, désignons par k_q le sous-corps fini de k ayant $q = p^h$ éléments. Les racines de l'unité contenues dans k sont celles de ses sous-corps finis, et $k_q^* = \mu_{q-1}(k)$. Il en résulte que I_t s'identifie aussi à $\varprojlim_{q=p^h} k_q^*$. Dans cette nouvelle description si $q' = q^{r'}$, l'application de transition $k_{q'}^* \to k_q^*$ est la norme

$$\mathrm{Norme}_{k_{q'}/k_q}(x') = x'^{(1+q+\ldots+q^{r'-1})} = x'^{(q^{r'}-1)/(q-1)} = x'^{(q'-1)/(q-1)}$$

On note

$$j : I_t \xrightarrow{\sim} \varprojlim k_q^* = \varprojlim \mu_{q-1}(k)$$

l'identification canonique, et

$$j_q : I_t \to \mu_{q-1}(k) \xrightarrow[\sim]{\mathrm{can}} \mu_{q-1}(K)$$

la surjection canonique.

3.2. DÉVISSAGE D'UN GROUPE DE TYPE $(p, \ldots, p)$. — Suppososn R hensélien, et soit G un K-schéma en groupes commutatif, étale et annulé par p. Alors $G(\overline{K})$ est un espace vectoriel V de dimension finie sur le corps premier $\mathbf{F}_p$, et le groupe de Galois $\mathrm{Gal}(\overline{K}/K)$ opère linéairement sur V. Réciproquement, si V est un espace vectoriel de dimension finie sur $\mathbf{F}_p$, muni d'une représentation $\rho : \mathrm{Gal}(\overline{K}/K) \to \mathrm{Aut}(V)$, il lui correspond un K-schéma en groupes étale, commutatif, annulé par p.

Supposons qur G soit un K-schéma en groupes simple, de sorte que ρ est une représen ation simple de $\mathrm{Gal}(\overline{K}/K)$, et considérons la restriction de ρ au pro-p-groupe I_p de l'inertie sauvage, qui est invariant dans $\mathrm{Gal}(\overline{K}/K)$. Comme V est un espace vectoriel non nul sur $\mathbf{F}_p$, le sous-espace V^{I_p} des invariants sous I_p est non nul ([11], p. 146), et il est stable

par ρ. Comme ρ est simple, on en déduit que I_p opère trivialement sur V, donc que la représentation ρ est modérément ramifiée.

Supposons de plus R strictement hensélien, alors ρ provient d'une représentation (notée encore ρ) du groupe commutatif I_t. Considérons le commutant de ρ dans Aut (V) qui est un corps F, nécessairement fini. Comme I_t est commutatif, $\rho(I_t)$ est contenu dans le commutant de ρ, donc est formé d'homothéties du F-vectoriel V. Enfin, comme ρ est simple, V est nécessairement de dimension 1 sur F. On voit donc que le K-schéma en groupes correspondant à ρ est un K-schéma en F-vectoriels vérifiant la condition (★★) du paragraphe 1.2 (prop. 1.2.2).

PROPOSITION 3.2.1. — *Supposons R strictement hensélien. Soit G un K-schéma en groupes commutatif, fini, annulé par une puissance de p. On suppose G étale ou de type multiplicatif. Soit G_i, $i \in I$, la famille des quotients successifs d'une suite de Jordan-Hölder de G. Alors, pour chaque i, il existe un corps fini F_i, de caractéristique p, tel que G_i soit un K-schéma en F_i-vectoriels vérifiant* (★★).

Par dévissage, on voit que chacun des groupes G_i est annulé par p. Le cas étale résulte donc des considérations précédentes, et le cas de type multiplicatif s'en déduit par dualité.

3.3. PROLONGEMENTS DES SCHÉMAS EN F-VECTORIELS. — Soit maintenant $\mathscr{G}$ un R-schéma en groupes fini et plat, dont la fibre générique G est un schéma en F-vectoriels. En général, les opérations de F sur G ne s'étendent pas à $\mathscr{G}$. Mais si G est étale (resp. de type multiplicatif), parmi les divers prolongements possibles de G sur R, il en existe un $\mathscr{G}^+$ (resp. $\mathscr{G}^-$) qui est maximal (resp. minimal) (cor. 2.2.3). Et il est formel de vérifier que tout automorphisme de G se prolonge à $\mathscr{G}^+$ et $\mathscr{G}^-$. En particulier, la structure de schéma en F-vectoriels s'étend à $\mathscr{G}^+$ et $\mathscr{G}^-$. D'où le résultat suivant :

PROPOSITION 3.3.1. — *Supposons R d'inégales caractéristiques, et soit $\mathscr{G}$ un R-schéma en groupes fini et plat, dont la fibre générique G est un schéma en F-vectoriels. Alors la structure de schéma en F-vectoriels de G s'étend au prolongement maximal $\mathscr{G}^+$ et au prolongement minimal $\mathscr{G}^-$ de G.*

Les propositions 3.3.1 et 3.3.2 nous serviront au numéro suivant, pour obtenir des informations sur l'action du groupe de Galois sur $G(\bar{K})$. Auparavant, nous allons étudier les divers prolongements de G sur R qui possèdent une structure F-vectorielle.

Dans la suite de ce numéro, on suppose R d'inégales caractéristiques, et on désigne par F un corps ayant $q = p^r$ éléments. Soit $\mathscr{G}$ un R-schéma en F-vectoriels, de rang q, de fibre générique G. D'après le corollaire 1.5.1, le R-groupe $\mathscr{G}$ admet des équations de la forme

$$X_i^p = \delta_i X_{i+1}, \tag{1}$$

où i parcourt un espace principal homogène sous $\mathbf{Z}/r\,\mathbf{Z}$ et où les δ_i sont des éléments de R qui vérifient, pour tout i :

$$0 \leqq v(\delta_i) \leqq e = v(p). \tag{2}$$

Tout autre R-schéma en F-vectoriels $\mathscr{G}'$, qui prolonge G, a des équations analogues

$$X_i'^p = \delta_i' X_{i+1}' \quad \text{pour tout } i, \tag{1'}$$

$$0 \leqq v(\delta_i') \leqq e \quad \text{pour tout } i. \tag{2'}$$

De plus, il existe des éléments α_i de K^*, tels que l'isomorphisme de schémas en F-vectoriels $\mathscr{G} \times_R K \xrightarrow{\sim} \mathscr{G}' \times_R K$ des fibres génériques soit donné par des équations de la forme

$$X_i' = \alpha_i X_i \quad \text{pour tout } i. \tag{3}$$

On en déduit des relations de compatibilité entre les δ_i, δ_i' et les α_i :

$$\delta_i' = \alpha_i^p \delta_i \alpha_{i+1}^{-1} \quad \text{pour tout } i. \tag{4}$$

En particulier, pour que l'on ait $\mathscr{G} \geqq \mathscr{G}'$, il faut et il suffit que l'on ait

$$v(\alpha_i) \geqq 0 \quad \text{pour tout } i. \tag{5}$$

Supposons $\mathscr{G} \geqq \mathscr{G}'$, et examinons les divers cas possibles :

(*a*) L'un des α_j n'est pas une unité (i.e. on a $\mathscr{G} > \mathscr{G}'$). Alors il existe i tel que $v(\alpha_i) \geqq 1$ soit maximal parmi les $v(\alpha_j)$. On a, d'après (4), $v(\delta_i') \geqq p-1$. Comparant avec (2'), on trouve $e \geqq p-1$.

Par suite, si $e < p-1$, on a nécessairement $\mathscr{G} = \mathscr{G}'$. Compte tenu du corollaire 2.2.3, on peut appliquer ce résultat avec $\mathscr{G} = \mathscr{G}^+$ et $\mathscr{G}' = \mathscr{G}'^-$. On en déduit qu'il existe au plus un R-schéma en groupes fini et plat qui prolonge G.

(*b*) Les α_j n'ont pas tous la même valuation. Alors il existe i tel que $v(\alpha_i) > v(\alpha_{i+1})$. On a alors, d'après (4), $v(\delta_i') \geqq p$, donc $e \geqq p$ (d'après (2')). Réciproquement, si on a $v(\delta_i') \geqq p$, on peut prendre $\alpha_i = \pi$ et $\alpha_j = 1$

pour $j \neq i$, et obtenir ainsi un prolongement $\mathscr{G} > \mathscr{G}'$, pour lequel on a

$$\sum_j v(\delta'_j) > \sum_j v(\delta_j).$$

(*c*) Les α_j ont même valuation > 0, et l'on a $v(\delta'_j) \leqq p-1$, pour tout j. Alors, d'après (4), on a nécessairement $v(\alpha_j) = 1$ pour tout j, $v(\delta_j) = 0$ pour tout j, et $v(\delta'_j) = p-1$ pour tout j, et donc

$$\sum_j v(\delta'_j) > \sum_j v(\delta_j).$$

La condition $v(\delta_j) = 0$ pour tout j entraîne que $\mathscr{G}$ est étale; si, de plus, $e = p-1$, la condition $v(\delta'_j) = p-1$ entraîne que $\mathscr{G}'$ est de type multiplicatif.

Par récurrence décroissante sur $\sum_j v(\delta_j)$, les raisonnements précédents entraînent l'assertion 1° de la proposition suivante :

PROPOSITION 3.3.2. — *Soit G un K-schéma en F-vectoriels, de rang q, qui admet un prolongement $\mathscr{G}$ sur R fini et plat.*

1° *Le prolongement maximal $\mathscr{G}^+$ de G est caractérisé sur les équations de type* (1) *par les conditions suivantes :*

(*a*) $v(\delta_i) \leqq p-1$ *pour tout* i.

(*b*) $\exists\, i$ *avec* $v(\delta_i) < p-1$.

2° *Si $e < p-1$, $\mathscr{G}$ est, à isomorphisme près, l'unique prolongement de G sur R et c'est un schéma en F-vectoriels.*

3° *Si $e = p-1$, si G est simple et R hensélien, alors, ou bien $\mathscr{G}$ est l'unique prolongement de G, ou bien il existe deux prolongements de G, l'un étale, l'autre de type multiplicatif. Dans tous les cas, ces prolongements sont des schémas en F-vectoriels.*

Démonstration. — Il reste à prouver les 2° et 3°. On a prouvé le 2° dans l'analyse du cas (*a*) ci-dessus. Reste à établir le 3°. Considérons les schémas en F-vectoriels maximal et minimal $\mathscr{G}^+$ et $\mathscr{G}^-$ qui prolongent G. Supposons $\mathscr{G}^+ \neq \mathscr{G}^-$. Alors, d'après l'analyse des cas (*a*), (*b*) et (*c*) ci-dessus, $\mathscr{G}^+$ est étale et $\mathscr{G}^-$ est de type multiplicatif. Il reste à voir que $\mathscr{G} = \mathscr{G}^+$ ou $\mathscr{G}^-$. Comme $\mathscr{G}^+$ est étale, que R est hensélien et que G est simple, $\mathscr{G} \otimes_R k$ est aussi un schéma en groupes simple. Par suite, si le morphisme canonique $u : \mathscr{G}^+ \to \mathscr{G}^-$ n'est pas un isomorphisme, $u \otimes_R k$ est nul. Montrons que $\mathscr{G}$ est de type multiplicatif lorsque $u \otimes_R k = 0$. Pour établir ce point, on peut supposer S strictement hensélien et, par dévissage, on

se ramène au cas où G est de rang p. Mais alors $\mathscr{G}$ est un R-schéma en F_p-vectoriels, et comme il n'est pas étale, il est de type multiplicatif.

THÉORÈME 3.3.3. — *Supposons R d'inégales caractéristiques et $e < p-1$. Alors tout K-schéma en groupes fini, commutatif G, annulé par une puissance de p, admet au plus un prolongement fini et plat sur R.*

Démonstration. — Compte tenu de la proposition 2.2.2, il suffit de montrer que tout morphisme $u : \mathscr{G} \to \mathscr{G}'$, entre deux prolongements de G, qui est l'identité sur la fibre générique, est un isomorphisme. Par dévissage (prop. 3.2.1), on se ramène au cas où G est un schéma en F-vectoriels. Le fait que u soit un isomorphisme résulte alors de l'assertion du 2° de la proposition 3.3.2.

REMARQUES :

3.3.4. Les amateurs de cristaux constateront avec plaisir que la condition $e < p-1$ équivaut au fait que l'idéal maximal de R est un idéal à puissances divisées.

3.3.5. Supposons que $e = p-1$, et soit G un K-schéma en groupes-fini, commutatif, annulé par une puissance de p, qui admet un prolon, gement sur R fini et plat. Soit $u : \mathscr{G}^+ \to \mathscr{G}^-$ le morphisme canonique entre les prolongements maximal et minimal. Notons $\mathscr{G}^+_{\mathrm{bi}}$ (resp. $\mathscr{G}^-_{\mathrm{bi}}$) la composante biconnexe de $\mathscr{G}^+$ (resp. $\mathscr{G}^-$) (c'est-à-dire le quotient de la composante neutre par le plus grand sous-groupe de type multiplicatif). Alors il résulte de l'assertion du 3° de la proposition 3.3.2 que u induit un isomorphisme $\mathscr{G}^+_{\mathrm{bi}} \xrightarrow{\sim} \mathscr{G}^-_{\mathrm{bi}}$. Plus généralement la composante biconnexe $\mathscr{G}_{\mathrm{bi}}$ ne dépend pas du prolongement $\mathscr{G}$ de G.

COROLLAIRE 3.3.6. — *Supposons $e < p-1$, et soient $\mathscr{G}$ et $\mathscr{H}$ des R-schémas en groupes commutatifs, finis et plats, annulés par une puissance de p. Notons G et H leurs fibres génériques.*

1° *Tout morphisme de G dans H se prolonge de manière unique en un R-morphisme $u : \mathscr{G} \to \mathscr{H}$. De plus,* Ker (u) *et* Coker (u) *sont plats sur R.*

2° *L'application naturelle* $\mathrm{Ext}_{R-\mathrm{gr}}(\mathscr{G}, \mathscr{H}) \to \mathrm{Ext}_{K-\mathrm{gr}}(G, H)$ *est injective.*

COROLLAIRE 3.3.7. — *Supposons R strictement hensélien, et $e \leqq p-1$. Soit $\mathscr{G}$ un R-schéma en groupes commutatif, fini et plat, annulé par une puissance de p. Alors $\mathscr{G}$ possède une suite de composition $\mathscr{G}_i$ dont les quotients successifs $\mathscr{G}_i/\mathscr{G}_{i+1}$ admettent des structures vectorielles sur des corps F_i convenables.*

3.4. ACTION DU GROUPE DE GALOIS SUR UN SCHÉMA EN F-VECTORIELS. — Supposons R strictement hensélien, d'inégales caractéristiques.

Soit G un K-schéma en F-vectoriels, de rang q, donné par l'équation

$$X_i^p = \delta_i X_{i+1} \quad \text{avec} \quad \delta_i \in K^* \quad \text{pour tout } i. \tag{1}$$

Par élimination des X_j, $j \neq i$, on en déduit que les points de G dans $\overline{K}$, correspondent aux valeurs de X_i qui sont solutions de l'équation

$$X_i^q = a_i X_i \quad \text{avec} \quad a_i = \delta_i^{p^{r-1}} \delta_{i+1}^{p^{r-2}} \dots \delta_{i+r-1}. \tag{6}$$

Le groupe G est donc trivialisé par l'extension modérée L de K de degré $q-1$. Par suite, l'action du groupe de Galois I_t sur le F-vectoriel $G(L)$ de dimension 1 est décrite par un caractère de la forme

$$I_t \xrightarrow{j_q} \mu_{q-1}(K) \xrightarrow{\psi} F_q^*. \tag{7}$$

Rappelons que la coordonnée X_i est associée au caractère fondamental χ_i (*cf.* § 1), et par suite, l'action de F sur $G(L)$, provenant de la structure de schéma en F-vectoriels, est donnée par la formule

$$\lambda x = \chi_i(\lambda) x \quad \text{pour tout } x \quad \text{dans } G(L) \quad \text{et tout} \quad \lambda \text{ dans } F. \tag{8}$$

Par ailleurs, si l'on note v' la valuation normalisée de L, les racines non nulles de (6) ont pour valuation

$$\frac{v'(a_i)}{q-1} = v(a_i) = p^{r-1} v(\delta_i) + \dots + v(\delta_{i+r-1}).$$

Compte tenu des rappels sur l'action du groupe de Galois modéré faits au n° 3.1, pour tout $\sigma \in I_t$ et toute racine non nulle x de (6), on a

$$\sigma(x) = j_q(\sigma)^{v(a_i)} x. \tag{9}$$

Pour tout i, notons $\psi_i : \mu_{q-1}(K) \to F^*$ l'application inverse de χ_i (de sorte que $\psi_i^p = \psi_{i-1}$). Il résulte alors de (8) et (9) qu'un élément σ de I_t opère sur le F-vectoriel $G(L)$ par l'homothétie de rapport

$$\psi_i(j_q(\sigma))^{v(a_i)}.$$

Or $\psi_i^{v(a_i)} = \psi_{i+1}^{v(\delta_i)} \dots \psi_{i+r}^{v(\delta_{i+r-1})}$. On a donc prouvé le résultat suivant :

THÉORÈME 3.4.1. — *Supposons R strictement hensélien, d'inégales caractéristiques. Soit G un K-schéma en F-vectoriels, d'équations* (1). *Alors*

le groupe de Galois Gal $(\overline{K}/K)$ *opère par homothéties sur le F-vectoriel* $G(\overline{K})$ *à travers le caractère*

$$I_t \xrightarrow{j_q} \mu_{q-1}(K) \xrightarrow{\psi} F^* \qquad \text{avec} \quad \psi = \psi_{i+1}^{v(\delta_i)} \dots \psi_{i+r}^{v(\delta_{i+r-1})}.$$

REMARQUE 3.4.2. — Pour que la représentation de Gal $(\overline{K}/K)$ dans $G(\overline{K})$ soit simple, il faut et il suffit que les composés de ψ avec les divers automorphismes de F soient distincts. Il revient au même de demander que la suite des $v(\delta_j)$ ne soit pas invariante par une puissance de la permutation circulaire $j \mapsto j+1$ autre que l'identité.

THÉORÈME 3.4.3. — *Supposons R strictement hensélien, d'inégales caractéristiques. Soit G un K-schéma en F-vectoriels associé à un caractère $\psi : \mu_{q-1}(K) \to F^*$. Pour que G se prolonge en un R-schéma en groupes fini et plat, il faut et il suffit que ψ puisse s'écrire sous la forme*

$$\psi = \psi_{i+1}^{n_i} \dots \psi_{i+r}^{n_{i+r-1}} \qquad \text{avec} \quad 0 \leqq n_j \leqq e \text{ pour tout } j.$$

Démonstration. — Si G admet un prolongement sur R fini et plat $\mathscr{G}$, on peut supposer que la structure F-vectorielle de G s'étend à $\mathscr{G}$ (prop. 3.3.2). Alors $\mathscr{G}$ admet des équations du type 1°, les conditions du 2° étant les seules restrictions imposées aux coefficients δ_i. Le théorème 3.4.3 en résulte, compte tenu du théorème 3.4.1.

Combinant 3.2.1 avec 3.4.3, on obtient le résultat suivant :

COROLLAIRE 3.4.4. — *Soit G un K-schéma en groupes fini, commutatif, annulé par une puissance de p et qui se prolonge en un R-schéma en groupes fini et plat. Soit H un quotient de Jordan-Hölder de G. Alors H est un schéma en F-vectoriels, pour un corps fini convenable F. Si F à p^r éléments, le caractère $\psi : I_t \to F^*$, qui décrit l'action du groupe de Galois* Gal $(\overline{K}/K)$ *sur le F-vectoriel $G_i(\overline{K})$ est alors de la forme*

$$\psi = \psi_{i+1}^{n_1} \dots \psi_{i+r}^{n_r} \qquad \text{avec} \quad 0 \leqq n_j \leqq e \text{ pour tout } j.$$

REMARQUES :

3.4.5. Le corollaire 3.4.4 est le résultat annoncé dans [12] (1.13). Il a d'abord été prouvé par SERRE dans le cas des sous-groupes finis d'un

groupe formel de dimension 1 (*loc. cit.* 1.9 et 1.10). SERRE à ensuite conjecturé le résultat dans le cas général.

3.4.6. Faut-il souligner que le théorème 3.4.1 et le corollaire 3.4.4 ne nous apprennent rien pour $e \geqq p-1$? Par contre, il résulte de 3.4.3 que si $e \geqq p-1$, tout K-schéma en F-vectoriels fini, se prolonge en un R-schéma en groupes fini.

3.4.7. La situation est très différente en égale caractéristique p, où l'on peut montrer que tout K-schéma en groupes, commutatif, fini, annulé par une puissance de p, se prolonge en un R-schéma en groupes fini et plat (d'après B. MAZUR et M. ARTIN).

Exemple. — Supposons R strictement hensélien, absolument non ramifié, et soit $\mathscr{E}$ une R-courbe elliptique dont la fibre spéciale est d'invariant de Hasse nul. Soient $\mathscr{G}$ le noyau de l'élévation à la puissance p-ième dans $\mathscr{E}$, et G la fibre générique de $\mathscr{G}$. Alors $\mathscr{G}$ est un R-schéma en groupe fini et plat, de rang $q = p^2$.

(*a*) G est un schéma en groupe simple, sinon il contiendrait un sous-schéma en groupe H de rang p, dont l'adhérence schématique dans $\mathscr{G}$ serait étale ou de type multiplicatif, en contradiction avec le fait que $\mathscr{E} \otimes_R k$ est d'invariant de Hasse nul.

(*b*) G, étant simple, est un groupe F-vectoriel (prop. 3.2.1) où F est un corps à q éléments. Mais alors $\mathscr{G}$ lui-même est un R-schéma en groupes F-vectoriels (prop. 3.3.2). Il admet une équation de la forme $X^{p^2} = p\,X$, et le caractère $\psi : \mu_{q-1}(K) \to F^*$, qui définit la représentation de $\mathrm{Gal}(\overline{K}/K)$ dans F^*, est l'un des caractères ψ_i.

4. Déterminants

Dans ce paragraphe, on suppose R strictement hensélien, d'inégales caractéristiques.

4.1. CAS DES GROUPES DE TYPE $(p, \ldots, p)$. — Soit $\mathscr{G}$ un R-schéma en groupes, fini, plat, commutatif et annulé par p. Notons G sa fibre générique, qui est un K-schéma en groupes étale, et soit p^h son rang. On peut considérer la puissance extérieure maximale de G : $\det(G) = \bigwedge^h G$, qui est un groupe étale de rang p. On se propose d'étudier l'action du groupe de Galois $\mathrm{Gal}(\overline{K}/K)$ sur $\det(G)$.

Supposons d'abord que $\mathscr{G}$ est un R-schéma en F-vectoriels, décrit par les équations (1) de 3.3. Alors $q = p^r = p^h$. On sait (th. 3.4.1) que l'action du groupe de Galois $\mathrm{Gal}(\overline{K}/K)$ sur $G(\overline{K})$ est donné par le caractère $\psi \circ j_q$ avec

$$\psi = \psi_{i+1}^{v(\delta_i)} \dots \psi_{i+r}^{v(\delta_{i+r-1})}.$$

L'action sur $\det(G)$ est donc décrite par le caractère

$$\mathrm{Norme}_{F/\mathbf{F}_p}(\psi) = (\psi_{i+1} \dots \psi_{i+r})^{v(\delta_i)+\dots+(v\delta_{i+r-1})} : \mu_{q-1}(K) \to \mathbf{F}_p^*.$$

En fait, si on compose $\psi_{i+1} \dots \psi_{i+r}$ avec le morphisme canonique $I_t \to \mu_{q-1}(K)$, on trouve le caractère

$$\tau_p : \; I_t \xrightarrow{j_p} \mu_{p-1}(K) \xrightarrow[\sim]{\text{can}} \mathbf{F}_p^*.$$

D'autre part, des équations (1) de l'algèbre de $\mathscr{G}$, on déduit que la différente $\mathfrak{D}_{\mathscr{G}/R}$ de $\mathscr{G}$ au-dessus de R est engendrée par $\prod_i \delta_i$; *a fortiori*, il en est de même de la différente absolue $\overline{\mathfrak{D}}(\mathscr{G})$ de $\mathscr{G}$ (appendice, déf. 8). Finalement, on voit que l'action de $\mathrm{Gal}(\overline{K}/K)$ sur le déterminant de la fibre générique d'un R-schéma en F-vectoriels est donnée par le caractère modéré $\tau_p^{v(\overline{\mathfrak{D}}(\mathscr{G}))}$. Par dévissage (cor. 3.3.7), on en déduit le résultat suivant :

THÉORÈME 4.1.1. — *Soit G la fibre générique d'un R-schéma en groupes $\mathscr{G}$, fini, plat, commutatif, annulé par p. Supposons $e \leqq p-1$. Alors l'action de* $\mathrm{Gal}(\overline{K}/K)$ *sur* $\det(G)$ *est donnée par le caractère modéré $\tau_p^{v(\overline{\mathfrak{D}}(\mathscr{G}))}$.*

REMARQUE 4.1.2. — On peut penser que la conclusion du théorème reste vraie sans restriction sur e. On peut le déduire du numéro suivant, lorsque $\mathscr{G}$ est le noyau de l'élévation à la puissance p-ième dans un R-groupe p-divisible.

4.2. CAS DES GROUPES p-DIVISIBLES. — Soit $T(\mu_{p^\infty})$ le module de Tate des racines de l'unité de $\overline{K}$, d'ordre une puissance de p, et soit

$$\tau : \; \mathrm{Gal}(\overline{K}/K) \to \mathbf{Z}_p^*$$

le caractère de la représentation du groupe de Galois $\mathrm{Gal}(\overline{K}/K)$ dans $T(\mu_{p^\infty})$.

THÉORÈME 4.2.1. — *Soit X un R-groupe p-divisible de hauteur h et de dimension d. Notons $T(X)$ le module de Tate des points d'ordre fini*

de $X \otimes_R K$. *Alors le caractère de la représentation du groupe de Galois* $\mathrm{Gal}(\overline{K}/K)$ *dans* $\det(T(X)) = \bigwedge^h T(X)$ *est égal à* τ^d.

REMARQUE 4.2.2. — En utilisant les décompositions de Hodge-Tate, TATE avait montré que la représentation du groupe de Galois dans $\bigwedge^h T(X)$ coïncide avec celle de τ^d sur un sous-groupe ouvert de $\mathrm{Gal}(\overline{K}/K)$.

Pour démontrer le théorème, nous allons utiliser une méthode de déformation et le fait que le théorème est évident dans le cas où X est de type ordinaire, c'est-à-dire est extension d'un groupe étale par un groupe de type multiplicatif.

On peut supposer R complet, ce qui ne modifie pas le groupe de Galois $\mathrm{Gal}(\overline{K}/K)$ et, par dévissage sur X, on peut supposer que $\overline{X} = X \otimes_R k$ est connexe.

Soit $\mathcal{O}$ l'anneau local complet d'une déformation verselle sur R, du groupe p-divisible $\overline{X}$. D'après les travaux de LAZARD, CARTIER, GROTHENDIECK (*cf.* [2]), il n'y a pas d'obstruction infinitésimale à relever un groupe p-divisible, donc $\mathcal{O}$ est une R-algèbre de séries formelles. Soit $S = \mathrm{Spec}(\mathcal{O})$, qui est donc un schéma régulier, et notons $\mathscr{X}$ le S-groupe p-divisible universel relatif au problème de déformation considéré.

LEMME 4.2.3. — *Soient* k *un corps de caractéristique* $p > 0$ *et* X *un* k*-groupe* p*-divisible connexe. Alors* $\overline{X}$ *peut être déformé en un groupe* p*-divisible sur* $k[[T]]$, *qui est de type ordinaire au-dessus du point générique.*

Admettons un instant ce lemme, et prouvons le théorème. Soit x le point générique de $\overline{S} = S \otimes_R k$. Il résulte du lemme que $\mathscr{X}$ est de type ordinaire au-dessus du point x. Par ailleurs, la dimension du groupe p-divisible $\overline{X}$ se conserve par déformation en caractéristique p, donc $\mathscr{X} \otimes_S k(x)$ est encore de dimension d. Soient alors $\tilde{S}$ un hensélisé strict de S en x, et $\tilde{\mathscr{X}}$ l'image réciproque de $\mathscr{X}$ sur S. Il résulte des remarques précédentes que $\tilde{\mathscr{X}}$ est extension d'un groupe étale isomorphe à $(\mathbf{Q}_p/\mathbf{Z}_p)^{h-d}$ par un groupe de type multiplicatif isomorphe à $(\mu_{p^\infty})^d$. Par suite, le module galoisien $\bigwedge^h T(\mathscr{X}) \otimes T(\mu_{p^\infty})^{\otimes -d}$, défini sur S est non ramifié au point x. Comme il est aussi non ramifié aux points de $S \otimes_R K$ qui sont de caractéristique zéro, il est non ramifié en tous les points de codimension $\leqq 1$ de S. D'après le théorème de pureté de Zariski-Nagata ([6], p. 118), il est non ramifié sur S. Par restriction à une section convenable

de S au-dessus de R, on conclut que $\Lambda^h T(X) \otimes T(\mu_{p^\infty})^{\otimes -d}$ est non ramifié sur R, d'où le théorème, puisque R est strictement hensélien.

Démonstration du lemme. — Nous allons utiliser la théorie des courbes typiques de Cartier. La littérature sur le sujet est bien incomplète; le lecteur pourra consulter [1], [2], et surtout [9], dont nous nous sommes largement inspirés.

Pour tout anneau L, notons $W(L)$ l'anneau des vecteurs de Witt, à coordonnées dans L, et $A(L)$ l'anneau $W(L)[[V, F]]$, décrit dans [9].

Soit $\overline{X}$ un groupe p-divisible connexe, de dimension d, défini sur un corps k de caractéristique $p > 0$. Soit $\overline{T}$ le $A(k)$ module de ses courbes typiques. Notons $\bar{e}_1, \ldots, \bar{e}_d$ une base du k-espace vectoriel $\overline{T}/V\overline{T} \simeq \mathrm{Lie}(\overline{X})$ et $\overline{m}_1, \ldots, \overline{m}_d$ des relèvements des e_i dans $\overline{T}$. Il existe alors des éléments $\overline{Q}_{ij}$, $1 \leqq i, j \leqq d$, de $W(k)[[V]]$, uniquement déterminés, tels que $F(\overline{m}_i) = \sum_j Q_{ij} \overline{m}_j$ dans $\overline{T}$.

Soient $L = k[[T]]$, et $m_1, \ldots, m_d$ la base canonique de $A(L)^d$. Choisissons des relèvements quelconques Q_{ij}, $0 \leqq i, j \leqq d$, des $\overline{Q}_{ij}$ dans $W(L)[[V]]$, et notons T le $A(L)$-module quotient de $A(L)^d$ par le sous-module engendré par les éléments $\mathrm{F}\, m_i - \sum_j Q_{ij} m_j$, pour $i = 1, \ldots, d$ Alors T est le module des courbes typiques d'un groupe formel X sur $L = k[[T]]$ qui relève $\overline{X}$. De plus, la p-algèbre de Lie de X est isomorphe au L-module libre de rang d égal à T/VT, et l'opération de puissance p-ième provient par passage au quotient de l'action de F. Comme les relèvements Q_{ij} des $\overline{Q}_{ij}$ sont arbitraires, il n'y a pas de mérite à les choisir de façon que l'opération de puissance p-ième sur $\mathrm{Lie}(X) \otimes_{k[[T]]} k((T))$ soit injective, de sorte que $\mathrm{Lie}(X)$ soit une p-algèbre de Lie génériquement de type multiplicatif, d'où le lemme.

APPENDICE

Trace et différente

Soient $S = \mathrm{Spec}(R)$ un schéma affine, G un S-schéma en groupes fini, commutatif, localement libre de rang n. Notons A sa bigèbre, c sa comultiplication, d sa multiplication, A' la bigèbre du dual de Cartier G' de G, et $\langle\ ,\ \rangle$ l'accouplement naturel entre A et A'.

Pour nous y reconnaître, nous considérons A comme une algèbre de fonctions sur G, et A' comme une algèbre de mesures sur G, la multiplication devenant la convolution $\star$. On note 1 l'élément unité de A et δ celui de A'.

Par transposition, on définit une action de A sur A', et une action de A' sur A. Plus précisément, pour $f \in A$ et $\mu \in A'$, on définit $f\mu \in A'$ par

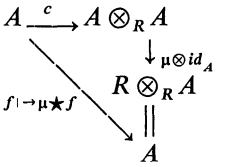
$$\langle g, f\mu \rangle = \langle fg, \mu \rangle \quad \text{pour tout } g \in A,$$

[on obtient ainsi l'action naturelle de A sur $A' = \mathrm{Hom}_R(A, R')$], et l'on définit $\mu \star f \in A$ par

$$\langle \mu \star f, \nu \rangle = \langle f, \mu \star \nu \rangle \quad \text{pour tout } \nu \in A',$$

[on obtient ainsi l'action naturelle de A' sur $A = \mathrm{Hom}_R(A', R)$].

LEMME 1. — *Soit $\mu \in A'$. On a un diagramme commutatif*

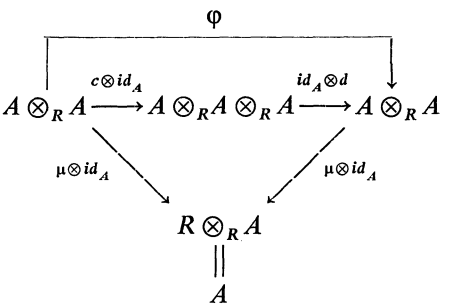


En effet, l'application $f \mapsto \mu \star f$ est la transposée de l'application $\nu \mapsto \mu \star \nu$ et cette dernière est la composée des applications $\nu \mapsto \mu \otimes \nu$ et $\mu \otimes \nu \mapsto \mu \star \nu$. La commutativité du diagramme en résulte par transposition.

LEMME 2. — *Soit $\mu \in A'$. Les conditions suivantes sont équivalentes :*

1° *La mesure μ sur G est invariante par translations.*

2° *Le diagramme suivant est commutatif :*



3° *Pour toute fonction* $f \in A$, *on a* $\mu \star f = \langle f, \mu \rangle 1$.

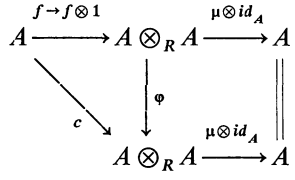
4° *Pour toute mesure* $\nu \in A'$, *on a* $\mu \star \nu = \langle 1, \nu \rangle \mu$.

Démonstration. — L'application φ n'est autre que le comorphisme de la translation universelle

$$G \times_S G \to G \times_S G,$$
$$(g, g') \mapsto (gg', g')$$

d'où l'équivalence des 1° et 2°.

Prouvons que 2° $\Leftrightarrow$ 3°. Considérons le diagramme



Le triangle de gauche est commutatif; sur la première ligne on a $(\mu \otimes \mathrm{id}_A)(f \otimes 1) = \langle \mu, f \rangle 1$; d'après le lemme 1,

$$(\mu \otimes \mathrm{id}_A) \circ c(f) = \mu \star f.$$

Si le 2° est vérifié, le carré de droite est commutatif, d'où 2° $\Rightarrow$ 3°. Réciproquement, si le 3° est vérifié, en utilisant la linéarité de φ par rapport au facteur de droite de $A \otimes_R A$, on trouve que le carré de droite est commutatif, donc 3° $\Rightarrow$ 2°.

Enfin, pour tout $\nu \in A'$ et tout $f \in A$, on a

$$\langle \mu \star \nu - \langle 1, \nu \rangle \mu, f \rangle = \langle \mu \star f - \langle \mu, f \rangle 1, \nu \rangle$$

d'où l'équivalence des 3° et 4°.

Voici une première application, qui relie la trace dans G à la trace dans G'. La démonstration m'a été communiquée par A. DOUADY.

PROPOSITION 3. — *Notons* $\theta \in A'$ *la trace dans la R-algèbre* A, *et notons* $\tau \in A$ *la trace dans la R-algèbre* A'. *Alors on a*

$$\langle \tau, \theta \rangle = n = \mathrm{rang}(G).$$

Démonstration. — La trace θ est évidemment une mesure invariante sur G. D'où

$$\begin{aligned}\langle \tau, \theta \rangle &= \text{trace de l'application } \mu \mapsto \theta \star \mu \\ &= \text{trace de l'application } \mu \mapsto \langle 1, \mu \rangle \theta \\ &= \langle 1, \theta \rangle = n.\end{aligned}$$

LEMME 4. — *Soit $f \in A$. Les conditions suivantes sont équivalentes :*

1° *on a $c(f) = 1 \otimes f$.*

2° *pour tout $\mu \in A'$, on a $\mu \star f = \langle \mu, 1 \rangle f$.*

De plus, les seuls éléments de A qui satisfont à ces conditions sont ceux de la forme $\lambda 1$, $\lambda \in R$.

Démonstration. — Soit $\nu \in A'$. On a

$$\begin{aligned}\langle \mu \star f - \langle \mu, 1 \rangle f, \nu \rangle &= \langle f, \mu \star \nu \rangle - \langle \mu, 1 \rangle \langle f, \nu \rangle \\ &= \langle c(f) - 1 \otimes f, \mu \otimes \nu \rangle,\end{aligned}$$

d'où l'équivalence des 1° et 2°.

Par ailleurs, il est clair que les éléments $\lambda 1$, $\lambda \in R$ vérifient la condition du 1°. Montrons que ce sont les seuls. Soient I l'idéal d'augmentation de A, et

$$a = \lambda 1 + i \in A = R \oplus I.$$

On a

$$c(a) = \lambda 1 + i \otimes 1 + 1 \otimes i + j \qquad \text{avec} \quad j \in I \otimes_R I.$$

Par suite, si $c(a) = 1 \otimes a$, on a $i = 0$.

Revenons aux mesures invariantes sur G. Comme G' est localement intersection complète au-dessus de S (par exemple, parce que G' est un sous-schéma en groupes d'un groupe lisse), il résulte de la dualité pour les faisceaux cohérents ([7], III, § 6 et 7), que le A'-module $A = \mathrm{Hom}(A', R)$ est localement isomorphe au A'-module A'. On déduit alors du lemme 4 que les éléments $\theta \in A'$ tels que $\mu \star \theta = \langle \mu, 1 \rangle \theta$ pour tout $\mu \in A'$ (c'est-à-dire les mesures invariantes sur G d'après le lemme 2), forment un R-module inversible D, facteur direct de A'.

DÉFINITION 5. — *Une mesure de Haar sur G est une base de D, c'est-à-dire une mesure invariante sur G, qui induit une mesure non nulle sur chaque fibre de G.*

Vu ce qui précède, G possède localement sur S une mesure de Haar, et deux mesures de Haar sur G diffèrent par multiplication par une unité de R.

LEMME 5. — *Supposons que R soit un corps k, et soit $f \in A$. Il existe un plus petit sous-espace vectoriel E de A, contenant f et stable par les translations de G. De plus :*

1° *si ε_i est une base de A et si $c(f) = \sum_i \varepsilon_i \otimes a_i$, E est le sous-espace de A engendré par les a_i.*

2° *on a $E = \{ \nu \star f \}$, $\nu \in A'$.*

Démonstration. — La description de E donnée dans le 1° est classique (*cf.* [6], p. 404). On a alors les équivalences suivantes :

$$\begin{aligned} \langle \mu, e \rangle = 0, \quad \forall e \in E \quad &\Leftrightarrow \quad \langle \mu \otimes \nu, c(f) \rangle = 0, \quad \forall \nu \in A' \\ &\Leftrightarrow \quad \langle \mu \star \nu, f \rangle \quad = 0, \quad \forall \nu \in A' \\ &\Leftrightarrow \quad \langle \mu, \nu \star f \rangle \quad = 0, \quad \forall \nu \in A', \end{aligned}$$

d'où l'équivalence de 1° et 2°.

LEMME 6. — *Si μ est une mesure de Haar sur G, μ est une base du A-module A'.*

Démonstration. — On peut supposer que R est un corps k, et il nous faut montrer que si $f \in A$ est tel que $f\mu = 0$, alors $f = 0$. On a $\langle f\mu, g \rangle = 0$ pour tout $g \in A$, soit encore $\langle \mu, fg \rangle = 0$. Donc l'orthogonal $\mu^\perp$ de μ contient l'idéal fA de A. Comme μ est une mesure invariante non nulle, $\mu^\perp$ est stable par les translations de G. Or le saturé par translations d'un idéal non nul est égal à A, donc $fA = 0$, et par suite $f = 0$.

LEMME 7. — *Soit D (resp. D') la droite des mesures invariantes sur G (resp. G'). La restriction à $D \times D'$ de l'accouplement $\langle \ , \ \rangle$ est non dégénérée.*

Démonstration. — On peut supposer que R est un corps k. Soit μ (resp. h) une mesure de Haar sur G (resp. G'). Pour tout $f \in A$, on a

$$\langle h, f\mu \rangle = \langle hf, \mu \rangle.$$

D'après le lemme 2, appliqué à la mesure invariante h sur G', on a $hf = \langle \delta, f \rangle h$ et donc $\langle h, f\mu \rangle = \langle \delta, f \rangle \langle h, \mu \rangle$. Comme μ est une base du A-module A' (lemme 6), on ne peut pas avoir $\langle h, f\mu \rangle = 0$ pour tout $f \in A'$, donc $\langle h, \mu \rangle \neq 0$.

Application à la différente. — Considérons le A-module inversible A', et soit $\theta \in A'$ la trace sur R de la R-algèbre A. Alors θ est une mesure invariante sur G, de sorte que si μ est une mesure de Haar sur G, il existe $\lambda \in R$ tel que $\theta = \lambda\mu$. Par ailleurs, soit $\mathfrak{D}$ l'idéal de A égal à la différente de la R-algèbre A. C'est un idéal invariant par les translations de G, donc provenant d'un idéal $\overline{\mathfrak{D}}$ de R.

DÉFINITION 8. — *Nous appellerons l'idéal $\overline{\mathfrak{D}}$ la différente absolue de G.*

D'après le lemme 6, la mesure de Haar μ est une base du A-module A'. La théorie de la dualité pour les R-algèbres finies, localement intersection complète (*cf.* [13], p. 165) montre alors que $\mathfrak{D} = \lambda A$, avec $\theta = \lambda\mu$. Par suite on a $\overline{\mathfrak{D}} = \lambda R$. De façon plus intrinsèque, si D est la droite des mesures invariantes sur G, et si $u : R \to D$ est l'application R-linéaire qui envoie $1 =$ sur θ, par dualité des R-modules inversibles, on obtient une application

$$v : \quad D^{\otimes -1} \to R$$

dont l'image est précisément l'idéal $\overline{\mathfrak{D}}$. On déduit alors du lemme 7 et de la proposition 3 le résultat suivant :

PROPOSITION 9. — *Soit $\overline{\mathfrak{D}}$ la différente absolue de G et $\overline{\mathfrak{D}'}$ la différente absolue de G'. Alors $\overline{\mathfrak{D}}\,\overline{\mathfrak{D}'}$ est l'idéal de R engendré par le rang n du schéma en groupes G.*

BIBLIOGRAPHIE

[1] CARTIER (P.). — Groupes formels associés aux anneaux de Witt généralisés, *C. R. Acad. Sc. Paris*, t. 265, 1967, série A, p. 49-52; et Modules associés à un groupe formel commutatif; Courbes typiques, *C. R. Acad. Sc. Paris*, t. 265, 1967, série A, p. 129-132.

[2] CARTIER (P.). — Relèvement des groupes formels commutatifs, *Séminaire Bourbaki*, 1968/69, n° 359, p. 217-230. — Berlin, Springer-Verlag, 1971 (*Lecture Notes in Mathematics*, 179).

[3] DEMAZURE (M.) et GROTHENDIECK (A.). — *Schémas en groupes*, I, Séminaire de géométrie algébrique, 1962-1964 (SGA 3). — Berlin, Springer-Verlag, 1970 (*Lecture Notes in Mathematics*, 151).

[4] DEMAZURE (M.) et GROTHENDIECK (A.). — *Schémas en groupes*, II, Séminaire de géométrie algébrique, 1962-1964 (SGA 3). — Berlin, Springer-Verlag, 1970 (*Lecture Notes in Mathematics*, 152).

[5] GROTHENDIECK (A.). — *Éléments de géométrie algébrique*, IV, 2e partie. — Paris, Presses universitaires de France, 1965 (*Institut des Hautes Études Scientifiques. Publications mathématiques*, 24).

[6] GROTHENDIECK (A.). — *Cohomologie locale des faisceaux cohérents et théorèmes de Lefschetz locaux et globaux*, Séminaire de géométrie algébrique, 1962 (SGA 2). — Amsterdam, North-Holland publishing Company, 1968 (*Advanced Studies in pure Mathematics*, 2).

[7] HARTSHORNE (R.). — *Residues and duality*. — Berlin, Springer-Verlag, 1966 (*Lecture Notes in Mathematics*, 20).

[8] LANG (S.). — *Algebraic number theory*. — Reading, Addison-Wesley publishing Company, 1970 (*Addison-Wesley Series in Mathematics*).

[9] MUMFORD (D.). — Bi-extensions of formal groups, « *Algebraic geometry* », p. 307-322. — London, Oxford University Press, 1969 (*Tata Institute of fundamental Research. Studies in Mathematics*, 4).

[10] OORT (F.) and TATE (J.). — Group schemes of prime order, *Ann. scient. Éc. Norm. Sup.*, 4e série, t. 3, 1970, p. 1-21.

[11] SERRE (J.-P.). — *Corps locaux*. — Paris, Hermann, 1962 (*Act. scient. et ind.*, 1296; *Publ. Inst. Math. Univ. Nancago*, 8).

[12] SERRE (J.-P.). — Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, *Invent. Math.*, Berlin, t. 15, 1972, p. 259-331.

[13] TATE (J.). — p-divisible groups, « *Proceedings of a conference on local fields* » [Driebergen, 1966], p. 158-183. — Berlin, Springer-Verlag, 1967.

[14] WEIL (A.). — Numbers of solutions of equations in finite fields, *Bull. Amer. math. Soc.*, t. 55, 1949, p. 497-508.

(Texte reçu le 20 février 1974.)

Michel RAYNAUD,
Les Bruyères,
91, rue du Colonel-Fabien,
92160 Antony.