[Dans le cours de 1985-1986, on montrera que ces propriétés entraînent la suivante :

(d) *L'image de* $G_K \to \prod_\ell (\mathbf{G}_m \cdot \mathbf{Sp}_{2n})(\mathbf{Q}_\ell)$ *est ouverte pour la topologie adélique.*]

La propriété End (A) = $\mathbf{Z}$, à elle seule, n'est pas suffisante pour entraîner (a), (b), (c) : il existe un contre-exemple de MUMFORD pour $n = 4$. On peut toutefois démontrer le résultat suivant :

2.2.8. *Supposons que* End (A) = $\mathbf{Z}$ *et que* n *soit impair* (ou $n = 2$, ou $n = 6$). *Alors les propriétés* (a), (b), (c) *ci-dessus sont vraies ; on a*

$$G_\ell^{alg} = \mathbf{G}_m \cdot \mathbf{Sp}_{2n}$$

pour tout ℓ.

(Un énoncé analogue avait déjà été démontré par K. RIBET pour le groupe de MUMFORD-TATE.)

2.3. *Indications sur les démonstrations*

Au moyen du théorème d'irréductibilité de Hilbert, on se ramène au cas où le corps de base K est un corps de nombres algébriques. On dispose alors de trois types de renseignements sur les G_ℓ et les G_ℓ^{alg} :

(i) la théorie générale des représentations ℓ-adiques abéliennes, appliquée à une puissance extérieure convenable de V_ℓ, permet d'étudier le groupe C_ℓ (tout comme dans le cas des variétés abéliennes de type *CM*) ;

(ii) les groupes d'inertie en les places de K divisant ℓ fournissent des sous-tores à 1 paramètre de G_ℓ^{alg} (définis sur une extension convenable de $\mathbf{Q}_\ell$) qui n'ont que deux poids, le poids « 0 » et le poids « 1 », avec multiplicité n chacun ; de tels sous-tores restreignent considérablement la structure du groupe S_ℓ ;

(iii) les places de K ne divisant pas ℓ, et où A a bonne réduction, donnent des « tores de Frobenius » qui sont essentiellement indépendants de ℓ, et ont des propriétés très particulières (dues notamment aux pentes des polygones de Newton, comme l'a remarqué Y. ZARHIN).

En combinant ces informations à 2.2.2. (FALTINGS), on prouve 2.2.1., 2.2.3., 2.2.4. et 2.2.7. La démonstration de 2.2.8. est plus délicate ; elle utilise notamment la classification des représentations « minuscules » des groupes simples.

Signalons également que certains des résultats ci-dessus (par exemple 2.2.2., 2.2.3., 2.2.4., 2.2.5. et 2.2.7.) sont vrais lorsque le corps de base K est une extension de type fini d'un corps fini.

SÉMINAIRES

D. BERTRAND, *Variétés abéliennes, groupes de Galois et transcendance* (2 exposés).

136.

Résumé des cours de 1985–1986

Annuaire du Collège de France (1986), 95–99

Le cours a continué celui de l'année précédente, consacré aux représenta-
1 tions ℓ-adiques associées aux variétés abéliennes. Il s'est surtout attaché à la « variation avec ℓ » des groupes de Galois considérés.

1. *Notations*

K est une extension finie de $\mathbf{Q}$, de clôture algébrique $\overline{K}$; on note G_K le groupe de Galois Gal $(\overline{K}/K)$.

A est une variété abélienne sur K, de dimension $n \geq 1$.

Pour tout nombre premier ℓ, T_ℓ est le module de Tate de A relativement à ℓ ; c'est un $\mathbf{Z}_\ell$-module libre de rang $2n$. Le groupe G_K opère sur T_ℓ par une représentation

$$\rho_\ell : G_K \to \mathrm{Aut}\,(T_\ell) \simeq \mathbf{GL}_{2n}(\mathbf{Z}_\ell).$$

L'image de cette représentation est notée $G_{K,\ell}$; le groupe $G_{K,\ell}$ est le groupe de Galois des « points de ℓ^∞-division » de A.

La famille des ρ_ℓ, pour ℓ premier, définit un homomorphisme

$$\rho : G_K \to \prod_\ell G_{K,\ell} \subset \prod_\ell \mathrm{Aut}\,(T_\ell).$$

Le groupe $\rho(G_K)$ est le groupe de Galois des points de torsion de A.

2. *Résultats*

2.1. *Indépendance des* ρ_ℓ

Disons que les représentations ρ_ℓ sont *indépendantes sur* K si l'homomorphisme $\rho : G_K \to \prod_\ell G_{K,\ell}$ est *surjectif*, i.e. si $\rho(G_K)$ est égal au produit des $G_{K,\ell}$.

THÉORÈME 1 - *Il existe une extension finie* K′ *de* K *telle que les* ρ_ℓ *soient indépendantes sur* K′.

(Bien entendu, K′ dépend de la variété abélienne A considérée.)

Ce résultat peut se reformuler de la manière suivante :

THÉORÈME 1′ - *Si* K *est assez grand,* $\rho(G_K)$ *est un sous-groupe ouvert du produit des* $G_{K,\ell}$.

2.2. *Homothéties*

On sait (BOGOMOLOV) que $G_{K,\ell}$ contient un sous-groupe ouvert du groupe $\mathbf{Z}_\ell^*$ des homothéties. Notons $c(\ell)$ l'indice de $\mathbf{Z}_\ell^* \cap G_{K,\ell}$ dans $\mathbf{Z}_\ell^*$. D'après une conjecture de S. Lang, on devrait avoir $c(\ell) = 1$ pour ℓ assez grand. On peut prouver le résultat plus faible suivant (d'ailleurs suffisant pour les applications que Lang avait en vue) :

THÉORÈME 2 - *Les entiers* $c(\ell)$ *restent bornés quand* ℓ *varie.*

Vu le th. 1, ce résultat équivaut à :

THÉORÈME 2′ - *Il existe un entier* $c \geqslant 1$ *tel que le groupe* $\rho(G_K)$ *contienne toutes les homothéties de* $\hat{\mathbf{Z}}^* = \prod_\ell \mathbf{Z}_\ell^*$ *qui sont des puissances* c*-ièmes.*

Une autre façon d'énoncer le th. 2′ consiste à dire qu'il existe un entier $c \geqslant 1$ ayant la propriété suivante :

pour tout entier $m \geqslant 1$, *il existe* $s_m \in G_K$ *tel que* $s_m(x) = m^c x$ *pour tout* $x \in A(\overline{K})$ *d'ordre fini premier à* m.

2.3. *Comparaison avec le groupe des similitudes symplectiques*

Choisissons une polarisation e sur A, ce qui munit chacun des T_ℓ d'une forme alternée e_ℓ à discriminant $\neq 0$ (et même à discriminant inversible, si ℓ est assez grand). Le groupe de Galois $G_{K,\ell}$ est contenu dans le groupe $\mathbf{GSp}(T_\ell, e_\ell)$ des similitudes symplectiques de T_ℓ relativement à e_ℓ.

THÉORÈME 3 - *Faisons les hypothèses suivantes :*

(i) *L'anneau* End (A) *des* $\overline{K}$*-endomorphismes de* A *est réduit à* $\mathbf{Z}$;

(ii) *La dimension* n *de* A *est impaire, ou égale à* 2, *ou à* 6.

Alors $G_{K,\ell}$ *est ouvert dans* $\mathbf{GSp}(T_\ell, e_\ell)$ *pour tout* ℓ, *et est égal à* $\mathbf{GSp}(T_\ell, e_\ell)$ *pour tout* ℓ *assez grand.*

En combinant ce résultat avec le th.1, on obtient :

COROLLAIRE - *Si* (i) *et* (ii) *sont satisfaites,* $\rho(G_K)$ *est un sous-groupe ouvert du produit des* $\mathbf{GSp}(T_\ell, e_\ell)$.

Pour $n = 1$, cela revient à dire que $\rho(G_K)$ est ouvert dans le produit des $\mathbf{GL}(T_\ell)$: on retrouve une propriété des courbes elliptiques sans multiplications complexes qui avait fait l'objet du cours de 1970-1971 (voir aussi *Invent. Math.* 15 (1972), 259-331).

2.4. *Orbites des points de torsion de* A

Soit $A(\overline{K})_t$ le sous-groupe de torsion de $A(\overline{K})$. Si $x \in A(\overline{K})_t$, posons :

$N(x)$ = ordre de x ;

$d(x) = |G_K \cdot x|$ = nombre de conjugués de x sur K.

THÉORÈME 4 - *Supposons que* A *ne contienne aucune sous-variété abélienne* $\neq 0$ *de type* CM. *Alors, pour tout* $\epsilon > 0$, *il existe une constante* $C(\epsilon, A, K) > 0$ *telle que :*

$$d(x) \geqslant C(\epsilon, A, K) \cdot N(x)^{2-\epsilon} \quad \textit{pour tout } x \in A(\overline{K})_t.$$

Lorsque A contient une sous-variété abélienne $\neq 0$ de type CM, cet énoncé reste vrai à condition d'y remplacer l'exposant $2 - \epsilon$ par $1 - \epsilon$: cela résulte du th. 2′.

2.5. *Groupes de Galois des points de division par* ℓ

Soit $G_K(\ell)$ l'image de $G_{K,\ell}$ dans $\mathbf{GL}(T_\ell/\ell T_\ell) \simeq \mathbf{GL}_{2n}(\mathbf{F}_\ell)$ par réduction modulo ℓ. L'un des principaux résultats du cours a été de montrer que $G_K(\ell)$ est « presque algébrique ». De façon plus précise, on construit, pour tout ℓ assez grand, un *sous-groupe réductif connexe* H_ℓ de $\mathbf{GL}_{2n}$, défini sur $\mathbf{F}_\ell$, qui jouit des propriétés suivantes :

2.5.1. Quitte à remplacer K par une extension finie, $G_K(\ell)$ est contenu dans $H_\ell(\mathbf{F}_\ell)$, et son indice est borné quand ℓ varie. Pour ℓ assez grand, $G_K(\ell)$ contient le groupe dérivé de $H_\ell(\mathbf{F}_\ell)$.

2.5.2. Le rang de H_ℓ est indépendant de ℓ, et est égal au rang de l'algèbre de Lie du groupe ℓ-adique $G_{K,\ell}$.

2.5.3. La composante neutre du centre de H_ℓ est un tore « indépendant de ℓ » : il s'obtient par réduction (mod ℓ) à partir d'un tore défini sur $\mathbf{Q}$. Ce tore contient le groupe $\mathbf{G}_m$ des homothéties.

2.5.4. La représentation linéaire de degré $2n$ de H_ℓ définie par le plongement $H_\ell \to \mathbf{GL}_{2n}$ est semi-simple ; son commutant est $\mathbf{F}_\ell \otimes \mathrm{End}\,(A)$.

Remarque. Il devrait être possible de préciser (2.5.2) et (2.5.3) en montrant que H_ℓ est la réduction (mod ℓ) de la composante neutre $(G_\ell^{alg})^\circ$ de l'enveloppe algébrique du groupe ℓ-adique $G_{K,\ell}$ (du moins pour ℓ assez grand). Cela n'a pas été fait dans le cours.

3. *Ingrédients des démonstrations*

Il y a d'abord ceux déjà utilisés dans l'étude ℓ-adique, pour ℓ fixé : théorèmes de Faltings, tores de Frobenius, théorie abélienne, et propriétés des groupes d'inertie en les places de K divisant ℓ.

On a également besoin de renseignements sur les sous-groupes de $\mathbf{GL}_N(\mathbf{F}_\ell)$:

3.1. *Sous-groupes d'ordre premier à la caractéristique*

Si k est un corps, *tout sous-groupe fini de* $\mathbf{GL}_N(k)$, *d'ordre premier à la caractéristique de* k, *contient un sous-groupe abélien d'indice* $\leqslant c_1(N)$, où $c_1(N)$ ne dépend que de N. C'est là un théorème classique de C. Jordan (du moins lorsque $k = \mathbf{C}$, cas auquel on se ramène sans difficulté). On a reproduit la démonstration qu'en avait donnée FROBENIUS en 1911 (*Ges. Abh.*, III, n^{os} 87-88). Cette démonstration donne pour $\log c_1(N)$ une majoration de l'ordre de $N^2 \log N$; d'après un résultat récent de B. WEISFEILER (basé sur la classification des groupes finis simples) on peut remplacer $N^2 \log N$ par $N \log N$, ce qui est essentiellement optimal.

3.2. *Sous-groupes de* $\mathbf{GL}_N(\mathbf{F}_\ell)$ *engendrés par leurs éléments d'ordre* ℓ

Supposons $\ell \geqslant N$. Soit G un sous-groupe de $\mathbf{GL}_N(\mathbf{F}_\ell)$, soit G_u l'ensemble des éléments de G d'ordre ℓ, et soit G^+ le sous-groupe de G engendré par G_u (ou, ce qui revient au même, le plus petit sous-groupe normal de G d'indice premier à ℓ). Si $x \in G_u$, on peut écrire x sous la forme $\exp(X)$, avec $X^\ell = 0$; les $\exp(tX)$ forment un sous-groupe algébrique $G_a(x)$ de $\mathbf{GL}_N$, défini sur $\mathbf{F}_\ell$, et isomorphe au groupe additif $\mathbf{G}_a$. Soit G^{alg} le sous-groupe algébrique de $\mathbf{GL}_N$ engendré par les $G_a(x)$, pour $x \in G_u$. Le groupe $G^{alg}(\mathbf{F}_\ell)$ des $\mathbf{F}_\ell$-points de G^{alg} contient évidemment G^+ ; *d'après un théorème de V. Nori, on a* :

$$G^+ = G^{alg}(\mathbf{F}_\ell)^+ \quad \textit{si } \ell \geqslant c_2(N)$$

où $c_2(N)$ *ne dépend que de* N. Ce résultat est particulièrement utile lorsque G agit de façon semi-simple sur $\mathbf{F}_\ell^N$, car le groupe G^{alg} est alors semi-simple, et peut se relever en caractéristique 0 si $c_2(N)$ est bien choisi.

On applique ceci avec $N = 2n$, le groupe G étant le groupe de Galois $G_K(\ell)$. D'après un théorème de Faltings, l'action de ce groupe sur $\mathbf{F}_\ell^N$ est semi-simple si ℓ est assez grand, d'où d'après (3.2) un groupe semi-simple $G_K(\ell)^{alg}$. D'autre part, la théorie abélienne permet de définir un certain sous-tore de $\mathbf{GL}_N$ qui commute à $G_K(\ell)^{alg}$; le groupe réductif connexe H_ℓ engendré par ce tore et par $G_K(\ell)^{alg}$ est celui qui intervient dans (2.5). Une fois le groupe H_ℓ défini, il faut prouver qu'il a les propriétés (2.5.1) à (2.5.4). En fait, c'est (2.5.1) qui est le point essentiel ; on le traite en utilisant les théorèmes de Jordan et de Nori cités ci-dessus, ainsi que le théorème de structure des groupes d'inertie en les places de K divisant ℓ dû à Raynaud. De là, on passe aux théorèmes 1, 2, 3 et 4.

137.

Lettre à Marie-France Vignéras du 10/2/1986

Chère Marie-France,

Comme convenu, voici un résumé de la suite de mon cours.

1. Groupes semi-simples en caractéristique $p > 0$ (suite)

Je te rappelle où on en était arrivé : on se place sur un corps k algébriquement clos de caractéristique $p > 0$ et on s'intéresse aux sous-groupes algébriques G de $\mathbf{GL}_n$ satisfaisant aux deux conditions suivantes :

(1) G est un groupe semi-simple, et son action sur $V = k^n$ est semi-simple ;

(2) G est engendré par des sous-groupes (additifs) à un paramètre qui sont de type exponentiel.

On a démontré que, si $p \geq c_3(n)$ (où $c_i(n)$ désigne une constante ne dépendant que de n), un tel groupe *s'obtient par réduction* mod p *à partir d'un groupe de caractéristique* 0 satisfaisant à (1) ; et aussi que, inversement, tout groupe de caractéristique 0 satisfaisant à (1) se réduit mod p en un groupe satisfaisant à (1) et (2). (Je n'ai pas énoncé explicitement cette réciproque, mais elle résultait de la démonstration.)

2 [Je me suis à peu près convaincu que l'on peut prendre $c_3(n) = n$, qui est optimal comme le montre le cas de $\mathbf{SL}_n$. Mais je ne compte pas donner la démonstration dans le cours ; cela m'entraînerait trop loin. Pour les applications que j'ai en vue, la valeur exacte de $c_3(n)$ n'a pas d'importance.]

Le résultat ci-dessus entraîne que les *types* (à conjugaison près) des groupes G considérés *sont en nombre fini*, et "ne dépendent pas de p". Ce principe sera très utile dans la suite. Il entraîne par exemple ceci :

3 **Théorème** – *Il existe $c_4(n)$ et $c_5(n)$ tels que, si $p \geq c_4(n)$, tout groupe G du type ci-dessus soit caractérisé par ses invariants tensoriels de poids $\leq c_5(n)$.*

(Si m est un entier ≥ 0, je dis que G est "caractérisé par ses invariants tensoriels de poids $\leq m$" si, pour tout $g \in \mathbf{GL}_V$ qui n'appartient pas à G, il existe un élément d'un $\otimes^q V$, fixé par G mais pas par g, avec $0 \leq q \leq m$. En d'autres termes, G est le *fixateur* des tenseurs de poids $\leq m$ fixés par G.)

Démonstration – On se place d'abord en caractéristique 0. On a un nombre fini de groupes semi-simples à regarder. On sait (c'est bien connu, et d'ailleurs facile) que chacun d'eux est déterminé par ses invariants tensoriels ; et, pour chacun d'eux, un nombre fini de tels invariants suffit. On peut donc choisir un $c_5(n)$ tels que tout G de caractéristique 0 soit caractérisé par ses invariants tensoriels de poids $\leq c_5(n)$. Ceci fait, on choisit pour chaque G une base de ces invariants, et on réduit mod p pour des p assez grands pour que ça ait un sens. Le schéma en groupes fixant ces invariants est de type fini (sur $\mathbf{Z}$, si l'on veut) et coïncide avec le groupe considéré sur $\mathbf{Q}$. Il coïncide donc aussi avec lui en réduction mod p, pourvu que p soit assez grand. Pour chaque G, il n'y a donc qu'un nombre fini de p à éviter ; d'où mon $c_4(n)$.

Je te dis tout de suite à quoi me servira ce résultat ; lorsque j'ai (en caractéristique p) un groupe G satisfaisant à (1) et (2), je m'intéresserai à son *normalisateur* N dans $\mathbf{GL}_V$ et j'aurai envie de plonger le quotient N/G dans un $\mathbf{GL}_W$ avec un W aussi explicite que possible. Or le théorème ci-dessus dit que je peux le faire en prenant pour W le sous-espace de $\bigoplus_i \otimes^i V$ ($i \leq c_5(n)$) fixé par G : en effet, N laisse évidemment stable W, et y opère par l'intermédiaire de N/G ; de plus, le théorème garantit que cette action est fidèle. Et le fait que cette action soit induite par une action tensorielle me sera utile (voir n° 3).

Il y a ici une philosophie que j'ai la flemme de détailler, mais qui dit ceci : si je pars d'un sous-groupe G de $\mathbf{GL}_n(\mathbf{F}_p)$ comme je l'ai fait jusqu'ici, le groupe G^{alg} qui lui est associé (d'après Nori) n'est autre que le groupe des éléments de $\mathbf{GL}_n$ qui fixe les *invariants tensoriels de petit degré* de G.

2. Semi-simplicité et nullité du H^1

(Les résultats de cette section ne seront pas utilisés dans la suite, mais ils s'insèrent naturellement ici.)

Les deux premiers énoncés sont "géométriques" : on se place sur un corps k de caractéristique $p > 0$ que l'on peut supposer algébriquement clos.

Théorème A – *Si $G \subset \mathbf{GL}_n$ satisfait à* (1) *et* (2), *et si $p \geq c_6(n)$, on a*

$$H^1(G, V) = 0 \,, \quad \text{où } V = k^n.$$

(Il s'agit du 1er groupe de cohomologie de G à coefficients dans V, la cohomologie étant définie par des cochaînes "morphiques" sur G. Formulation équivalente :

$\mathrm{Ext}^1_G(\mathbf{1}, V) = 0$, où $\mathbf{1}$ désigne la représentation unité de G.)

Démonstration – Par dévissage on peut supposer V irréductible. Si $V = \mathbf{1}$, on a $H^1(G, \mathbf{1}) = \mathrm{Hom}(G, \mathbf{G}_a) = 0$. On peut donc supposer V irréductible $\neq \mathbf{1}$. Si p est assez grand, on sait que cette représentation est réduction mod p d'une représentation de caractéristique 0. Or dans cette dernière l'opérateur de Casimir (induit par l'action de l'algèbre de Lie) est $\neq 0$. Il le reste donc (mod p) pour presque tout p. Or, dès qu'il est $\neq 0$, il entraîne la nullité de $H^1(G, V)$ par un argument standard. (Par exemple, on représente une classe de cohomologie par une extension $0 \to V \to E \to \mathbf{1} \to 0$ de G-modules, et on doit voir que cette extension est scindée. Or l'élément de Casimir opère sur E, est 0 sur $\mathbf{1}$, et est un scalaire $\lambda \neq 0$ sur V : son noyau dans E donne donc un scindage de E.) Il n'y a donc qu'un nombre fini de p à exclure, d'où le théorème A.

Remarque – La meilleure valeur de $c_6(n)$ semble être $c_6(n) = n + 1$.

Voici une variante du théorème A :

Théorème B – *Soit $\rho : G \to \mathbf{GL}_n$ une représentation linéaire en caractéristique p d'un groupe semi-simple G. Supposons que :*

(a) *les poids intervenant dans ρ sont p-restreints ;*

(b) $p \geq c_7(n)$.

Alors ρ est semi-simple.

(Il se peut que la condition (a) soit inutile : je n'ai pas regardé.)

Démonstration – Il suffit de voir que, si V_1 et V_2 sont deux représentations de G satisfaisant à (a) et $\dim V_1 + \dim V_2 \leq n$, alors $\mathrm{Ext}^1_G(V_1, V_2) = 0$ si $p \geq c_7(n)$. Or on peut récrire $\mathrm{Ext}^1_G(V_1, V_2)$ comme $H^1(G, W)$, où $W = V_1^* \otimes V_2$. On applique alors le théorème A à la représentation W.

(Je m'aperçois que, dans mes énoncés, je suppose tantôt que G est *contenu* dans le $\mathbf{GL}_n$ considéré, tantôt qu'on a une représentation de G dans $\mathbf{GL}_n$, non nécessairement fidèle. Excuse-moi ! On passe sans difficulté d'un type d'énoncé à l'autre, mais dans mon cours, il me faudra choisir, hélas.)

Voici maintenant un théorème de Nori, que j'avais énoncé dans mon 1er cours :

Théorème C – *Soit G un sous-groupe de $\mathbf{GL}_n(\mathbf{F}_p)$, opérant de façon semi-simple.*

On a alors :

$$H^1(G, \mathbf{F}_p^n) = 0 \quad si \quad p \geq c_8(n).$$

Démonstration – Soit G^+ le sous-groupe de G engendré par ses p-éléments. C'est un sous-groupe distingué de G, d'indice premier à p. Il en résulte que G^+ opère de façon semi-simple sur $\mathbf{F}_p^n$ ("lemme de Clifford") et que $H^1(G, \mathbf{F}_p^n)$ se plonge dans le groupe $H^1(G^+, \mathbf{F}_p^n)$. On est ainsi ramené à prouver la nullité de ce dernier groupe, i.e. *on est ramené au cas où G est engendré par ses p-éléments.* On introduit alors l'enveloppe algébrique G^{alg} de G, que je noterai simplement $\underline{G}$ pour éviter des exposants. On sait que (si p est assez grand) G est égal à $\underline{G}(\mathbf{F}_p)^+$. Le théorème A montre que $H^1(\underline{G}, V) = 0$, où $V = \mathbf{F}_p^n$, et on a envie de passer de là à la nullité de $H^1(G, V)$. Ce n'est pas tout à fait évident, et je n'ai rien trouvé de mieux que le fourbi suivant :

Tout d'abord, on peut supposer que V ne contient pas la représentation unité (car $H^1(G, \mathbf{1}) = \mathrm{Hom}(G, \mathbf{Z}/p\mathbf{Z}) = 0$ si p est assez grand). Ceci fait, considère une extension

$$0 \longrightarrow V \longrightarrow E \longrightarrow \mathbf{1} \longrightarrow 0$$

associée à une classe de cohomologie donnée dans $H^1(G, V)$. Il nous faut prouver que cette extension est scindée. *A priori*, le groupe G n'opère pas sur E (s'il opérait, on appliquerait le théorème A, et on aurait gagné). On va le forcer à opérer. Pour cela, on regarde l'enveloppe algébrique de G *dans* $\mathbf{GL}_E$, ce qui a un sens, puisque G est engendré par ses p-éléments. Appelons $\widetilde{\underline{G}}$ cette enveloppe, et $\widetilde{\mathfrak{g}}$ son algèbre de Lie ; on a une projection naturelle $\widetilde{\mathfrak{g}} \to \mathfrak{g}$, où $\mathfrak{g} = \mathrm{Lie}(\underline{G})$, et le noyau de cette projection s'identifie à un sous-$\underline{G}$-module W de V. J'ai supposé que V ne contient aucun sous-module irréductible trivial ; comme l'action de $\underline{G}$ sur V est p-restreinte, il en résulte que l'on a $[\mathfrak{g}, W] = W$ pour tout $W \subset V$ stable par $\underline{G}$. De ceci, et de la suite exacte

$$0 \longrightarrow W \longrightarrow \widetilde{\mathfrak{g}} \longrightarrow \mathfrak{g} \longrightarrow 0,$$

on déduit que W est contenu dans $[\widetilde{\mathfrak{g}}, \widetilde{\mathfrak{g}}]$; comme $[\mathfrak{g}, \mathfrak{g}] = \mathfrak{g}$, *cela entraîne* $\widetilde{\mathfrak{g}} = [\widetilde{\mathfrak{g}}, \widetilde{\mathfrak{g}}]$. Or on a vu dans un cours antérieur que cette relation entraîne "$\mathfrak{g} = \mathfrak{a}$" dans $\mathbf{GL}_E$, et aussi que (pour p assez grand) l'indice de G dans $\widetilde{\underline{G}}(\mathbf{F}_p)$ est borné par $c_9(n)$. Or, si W est de dimension w, et si $\underline{G}$ est de dimension N, l'ordre de $\widetilde{\underline{G}}(\mathbf{F}_p)$ est $\geq c_{10}(n) p^{N+w}$, c'est facile à voir. Comme l'ordre de G est $\leq p^N$, ceci n'est possible (pour p assez grand) que si $w = 0$. Mais alors $\underline{G}$ et $\widetilde{\underline{G}}$ ont même dimension et la

projection $\widetilde{\underline{G}} \to \underline{G}$ est une isogénie (on peut même voir que c'est un isomorphisme). En particulier $\widetilde{\underline{G}}$ est semi-simple et son H^1 à valeurs dans V est 0 d'après le théorème A, si p est assez grand. L'extension E est donc $\widetilde{\underline{G}}$-scindée, donc *a fortiori* G-scindée, cqfd.

Remarques - 1) Cette démonstration n'est pas tout à fait celle de Nori.

2) Je n'ai aucune idée de la valeur optimum de $c_8(n)$, et je préfère ne pas faire de conjecture à ce sujet : je manque d'exemples.

3. Les groupes de Galois des points de division par ℓ : algébricité

Après ces 10 ou 12 cours de préliminaires, j'en viens enfin aux théorèmes principaux. Ce n'est pas trop tôt !

On se donne une variété abélienne A de dimension $n \geq 1$ sur un corps de nombres K. Pour tout ℓ, on note G_ℓ le groupe de Galois des points de division par ℓ. C'est un sous-groupe de $\mathrm{Aut}(A_\ell) \simeq \mathbf{GL}_2(\mathbf{F}_\ell)$, avec des notations évidentes. On se propose de montrer que *le groupe G_ℓ n'est "pas très différent" du groupe des $\mathbf{F}_\ell$-points d'un certain groupe réductif connexe $\underline{H}_\ell \subset \mathbf{GL}_{2n}$.* (Conjecturalement, on devrait pouvoir prendre pour $\underline{H}_\ell$ la réduction mod ℓ du groupe de Mumford-Tate. Mais ce n'est pas du tout comme cela qu'on va le définir.)

Définition des $\underline{H}_\ell$

Comme tout groupe réductif connexe qui se respecte, $\underline{H}_\ell$ s'écrit de façon unique :

$$\underline{H}_\ell = \underline{C}_\ell \cdot \underline{S}_\ell,$$

où $\underline{C}_\ell$ est un tore, et $\underline{S}_\ell$ un groupe semi-simple, ces deux groupes commutant l'un avec l'autre. Il revient donc au même de définir $\underline{H}_\ell$ ou de définir séparément $\underline{C}_\ell$ et $\underline{S}_\ell$. C'est ce que je vais faire :

a) *Définition de $\underline{S}_\ell$*

On applique la théorie de Nori au sous-groupe G_ℓ^+ de G_ℓ engendré par les ℓ-éléments de G_ℓ ; autrement dit, on définit $\underline{S}_\ell$ comme l'enveloppe algébrique de G_ℓ^+. Pour ℓ assez grand, on sait que G_ℓ agit de façon semi-simple (théorème de Faltings) ; cela entraîne que $\underline{S}_\ell$ est semi-simple.

Il est bon de noter que la définition de $\underline{S}_\ell$ dépend du choix du corps de base K (ce qui peut paraître aberrant à première vue). Mais, si l'on étend les scalaires de K à une extension finie K' de degré d, le groupe G_ℓ est remplacé par un sous-groupe d'indice $\leq d$, et il en résulte que, si $\ell > d$, le groupe G_ℓ^+ *ne change pas*, non plus bien sûr que $\underline{S}_\ell$. Donc, après extension finie des scalaires, *les $\underline{S}_\ell$ restent les mêmes, à un nombre fini d'exceptions près.*

b) *Définition de $\underline{C}_\ell$*

On suppose K assez grand pour que tout $\overline{K}$-endomorphisme de A soit défini sur K. Soit L le centre de $\mathbf{Q} \otimes \mathrm{End}(A)$, et soit $L = \prod L_j$ sa décomposition en produit de corps. Cette décomposition de L induit une décomposition de A, à isogénie près :

$$A = \prod A_j.$$

Je poserai $d_j = 2.\dim(A_j)/[L_j : \mathbf{Q}]$. Il est facile de voir que d_j est un entier. Plus précisément, les modules de Tate $V_\ell(A_j)$ sont des $\mathbf{Q}_\ell \otimes L_j$-modules libres de rang d_j. Je noterai d la famille des d_j.

Soit $T_L = \prod T_{L_j}$ le tore sur $\mathbf{Q}$ qui représente les éléments inversibles de L. Si $x = (x_j)$ est un point de T_L, je noterai x^d le point $(x_j^{d_j})$. L'application $x \mapsto x^d$ est une isogénie $\delta : T_L \to T_L$.

Il me faut maintenant faire intervenir un système de représentations ℓ-adiques *abéliennes*, celui défini par le "déterminant relatif à L". Plus précisément, on a pour chaque ℓ une représentation

$$f_\ell : \mathrm{Gal}(\overline{K}/K) \longrightarrow (\mathbf{Q}_\ell \otimes L)^* = T_L(\mathbf{Q}_\ell)$$

qui donne l'action de $\mathrm{Gal}(\overline{K}/K)$ sur le $\mathbf{Q}_\ell \otimes L$-module libre de rang 1 $\det_{\mathbf{Q}_\ell \otimes L} V_\ell(A)$. (Cela a un sens car $V_\ell(A)$ est un $\mathbf{Q}_\ell \otimes L$-module projectif : sa j-ème composante est libre de rang d_j.) On vérifie de façon essentiellement standard (i.e. comme dans le cas de la multiplication complexe) que c'est là une représentation rationnelle au sens de mon bouquin à McGill ; elle est associée à une représentation (définie sur $\mathbf{Q}$) $f : S_{\mathrm{m}} \to T_L$, où S_{m} est l'un des tores ainsi notés dans McGill. Je noterai C le sous-tore de T_L caractérisé par la propriété suivante : *l'image de C par l'isogénie $\delta : T_L \to T_L$ définie plus haut est la composante neutre de $f(S_{\mathrm{m}})$.* Par construction, C est un sous-tore de T_L, défini sur $\mathbf{Q}$. (Si j'étais plus courageux, je te donnerais une description explicite directe de C, en termes de l'action de L sur l'espace tangent à A (i.e. à la Shimura) ; c'est un exercice embêtant, qu'il faudra bien que je fasse un de ces jours.)

Pourquoi ai-je défini ce C un peu baroque ? Parce que c'est lui qui définit les $\underline{C}_\ell$ que je voulais ! En effet, $\mathrm{End}(A)$ agit sur les A_ℓ, et on peut parler de la réduction (mod ℓ) du tore T_L, ainsi que de son sous-tore C, du moins pour presque tout ℓ. Ce sont des sous-groupes algébriques (sous-tores) de $\mathbf{GL}_{2n/\mathbf{F}_\ell}$, que je noterai $T_{L,\ell}$ et $\underline{C}_\ell$ respectivement.

Note que les éléments de G_ℓ *commutent* aux endomorphismes de A. Il en est donc de même de mon groupe $\underline{S}_\ell$, et on en conclut que *les groupes* $\underline{C}_\ell$ *et* $\underline{S}_\ell$ *commutent*. J'ai donc bien le droit de définir le groupe réductif connexe $\underline{H}_\ell$ par la formule :

$$\underline{H}_\ell = \underline{C}_\ell \cdot \underline{S}_\ell.$$

(*Exemples* – Si $\mathrm{End}(A)$ est réduit à $\mathbf{Z}$, le groupe $\underline{C}_\ell$ est simplement le groupe $\mathbf{G}_m$ des homothéties ; la partie intéressante de $\underline{H}_\ell$ est alors $\underline{S}_\ell$. Par contre, si A est de type CM, on a $\underline{S}_\ell = \{1\}$ et $\underline{H}_\ell = \underline{C}_\ell$.)

Maintenant que j'ai défini les $\underline{H}_\ell$, je peux énoncer le théorème principal n° 1 :

Théorème 1 – *Quitte à remplacer K par une extension finie, on a :*

(i) *Pour tout ℓ assez grand, G_ℓ est contenu dans le groupe $\underline{H}_\ell(\mathbf{F}_\ell)$ des $\mathbf{F}_\ell$-points de $\underline{H}_\ell$.*

(ii) *L'indice de G_ℓ dans $\underline{H}_\ell(\mathbf{F}_\ell)$ reste borné quand ℓ varie.*

Une remarque avant de commencer la démonstration : dans tout ce qui suit, on se borne à des ℓ suffisamment grands pour que toutes les inégalités du genre $\ell \geq c_i(2n)$ des cours précédents soient satisfaites. Je ne le redirai pas à chaque fois.

Démonstration de (i)

D'abord G_ℓ normalise G_ℓ^+ donc aussi $\underline{S}_\ell$. On a donc

$$G_\ell \subset \underline{N}_\ell(\mathbf{F}_\ell),$$

où $\underline{N}_\ell$ est le normalisateur de $\underline{S}_\ell$ dans $\mathbf{GL}_{2n}$. On est ainsi conduit à regarder l'image de G_ℓ dans le groupe $(\underline{N}_\ell/\underline{S}_\ell)(\mathbf{F}_\ell)$ Notons G'_ℓ cette image ; c'est un groupe d'ordre premier à ℓ. Or, d'après ce qu'on a vu au début, le groupe $\underline{N}_\ell/\underline{S}_\ell$ peut se représenter (grâce à une action tensorielle) dans un certain groupe linéaire $\mathbf{GL}_W$, où $\dim W$ est borné en fonction de n uniquement. Choisissons un sous-groupe abélien normal J_ℓ de G'_ℓ d'indice minimum ("J" est pour "Jordan"). D'après le

théorème de Jordan, on a $(G'_\ell : J_\ell) \leq c$, où c ne depend que de n. Si de plus ℓ est non ramifié dans K (ce qui n'exclut qu'un nombre fini de ℓ) et si I_v est un groupe d'inertie modérée dans G'_ℓ relativement à une place v divisant ℓ, le
7 plongement $I_v \to \mathbf{GL}_W$ ne fait intervenir que des caractères d'amplitude bornée par une constante ne dépendant que de n. (cela résulte de la construction de W au moyen de tenseurs de poids bornés). Or $I_v \cap J_\ell$ est d'indice $\leq c$ dans I_v. On en conclut par le *théorème de rigidité* des tores d'inertie que, si ℓ est assez grand, le groupe I_v commute à J_ℓ ; et, par le même raisonnement, que deux groupes I_v relatifs à des v distincts commutent entre eux. Le groupe engendré par J_ℓ et les I_v est alors abélien normal dans G'_ℓ ; comme J_ℓ a été choisi d'indice minimum, cela entraîne $I_v \subset J_\ell$ pour tout v. Considérons alors les homomorphismes

$$\mathrm{Gal}(\overline{K}/K) \longrightarrow G_\ell \longrightarrow G'_\ell \longrightarrow G'_\ell/J_\ell.$$

Ils correspondent à des extensions K'_ℓ/K, de groupe de Galois G'_ℓ/J_ℓ, qui sont de degré borné (par c) et qui sont non ramifiées en dehors des places de mauvaise réduction de A (en effet elles ne sont pas ramifiées en ℓ). Ces extensions sont donc en nombre fini (Hermite). Si l'on remplace K par une extension finie les contenant, les G'_ℓ sont remplacés par des sous-groupes des J_ℓ, i.e. deviennent abéliens.

On est donc ramené *au cas où les groupes G'_ℓ sont abéliens*. J'ai besoin d'un peu mieux : je désire que les G'_ℓ soient contenus dans un *tore* de $\underline{N}_\ell/\underline{S}_\ell$ rationnel sur $\mathbf{F}_\ell$. Pour cela, le plus commode est d'utiliser les "tores d'inertie" associés aux places v divisant ℓ. Il n'est pas difficile de voir que ces tores *normalisent* $\underline{S}$ (par exemple parce qu'ils normalisent son algèbre de Lie – ou bien parce qu'ils laissent stable le sous-espace W des tenseurs fixés par $\underline{S}$), donc définissent des tores du quotient $\underline{N}_\ell/\underline{S}_\ell$. Et l'argument de rigidité utilisé plus haut montre que ces tores commutent entre eux, donc engendrent un sous-tore de $\underline{N}_\ell/\underline{S}_\ell$ que je noterai $\underline{X}'_\ell$. Je dis que, quitte à augmenter K, on a $G'_\ell \subset \underline{X}'_\ell(\mathbf{F}_\ell)$ pour ℓ assez grand. En effet, je peux supposer que A est semi-stable sur K ; cela entraîne que l'inertie en les places de K à mauvaise réduction est unipotente, donc d'image triviale dans G'_ℓ (qui est d'ordre premier à ℓ, je le rappelle). Si je note G''_ℓ l'intersection de G'_ℓ et de $\underline{X}'_\ell(\mathbf{F}_\ell)$, il en résulte que l'extension K''_ℓ de K de groupe de Galois G'_ℓ/G''_ℓ est *non ramifié partout*. Il n'y a alors qu'à remplacer K par son corps de classes absolu pour "détruire" toutes ces extensions, i.e. pour se ramener *au cas où G'_ℓ est contenu dans $\underline{X}'_\ell(\mathbf{F}_\ell)$*.

Soit $\underline{X}_\ell$ l'image réciproque dans $\underline{N}_\ell$ du tore $\underline{X}'_\ell$ de $\underline{N}_\ell/\underline{S}_\ell$. C'est un groupe

réductif connexe de groupe dérivé $\underline{S}_\ell$. On peut donc l'écrire de façon unique

$$\underline{X}_\ell = \underline{D}_\ell \cdot \underline{S}_\ell,$$

où $\underline{D}_\ell$ est un tore, commutant à $\underline{S}_\ell$; et la projection $\underline{D}_\ell \to \underline{X}'_\ell$ est une isogénie.

Puisque G'_ℓ est contenu dans $\underline{X}'_\ell(\mathbf{F}_\ell)$, G_ℓ est contenu dans $\underline{X}_\ell(\mathbf{F}_\ell)$ (en effet G_ℓ est en tout cas contenu dans $\underline{X}_\ell(\overline{\mathbf{F}}_\ell)$, et G_ℓ est formé de points rationnels sur $\mathbf{F}_\ell$). On aura donc prouvé (i) *si l'on montre que le tore $\underline{D}_\ell$ coïncide avec le tore $\underline{C}_\ell$ défini* (si péniblement) *au* § 3.

La première chose à faire, c'est de démontrer que *le tore $\underline{D}_\ell$ est contenu dans le tore $T_{L,\ell}$* (celui défini par l'action du centre L de $\mathrm{End}(A)$, réduit mod ℓ). On utilise pour cela le théorème de Faltings qui dit que, pour ℓ grand, le commutant de G_ℓ est $\mathbf{F}_\ell \otimes \mathrm{End}(A)$. Comme $\underline{D}_\ell$ commute à G_ℓ, ce théorème entraîne que $\underline{D}_\ell$ est contenu dans "le groupe multiplicatif de $\mathbf{F}_\ell \otimes \mathrm{End}(A)$". Mais d'autre part $\underline{D}_\ell$ commute à $\mathbf{F}_\ell \otimes \mathrm{End}(A)$; en effet il est contenu dans le groupe engendré par $\underline{S}_\ell$ (qui commute évidemment à $\mathrm{End}(A)$) et par les tores d'inertie aux places divisant ℓ qui commutent tout autant. Ces deux propriétés de $\underline{D}_\ell$ entraînent bien qu'il est contenu dans le tore $T_{L,\ell}$.

On est maintenant mieux placé pour prouver l'identité de $\underline{D}_\ell$ et de $\underline{C}_\ell$. En effet, tous deux sont des sous-tores de $T_{L,\ell}$, et il suffit de voir que leurs images par l'isogénie

$$\delta : T_{L,\ell} \longrightarrow T_{L,\ell}$$

coïncident.

Or ces images sont faciles à déterminer :

– celle de $\underline{D}_\ell$ est le sous-tore de $T_{L,\ell}$ engendré par les tores d'inertie en ℓ, pour la représentation $\det_L V_\ell(A)$ réduite mod ℓ ;

– celle de $\underline{C}_\ell$ est par construction l'image du tore T_{m} de McGill réduit mod ℓ.

L'égalité des deux résulte alors de ce qui est fait dans McGill, convenablement interprété (il faudrait détailler... mais il n'y a aucune difficulté de principe : on connaît vraiment bien les représentations abéliennes !).

Ceci achève la démonstration de (i).

Démonstration de (ii)

Ce n'est pas difficile. Tout d'abord, on sait par la première partie du cours que G_ℓ^+ est d'indice borné dans $\underline{S}_\ell(\mathbf{F}_\ell)$. Utilisant la suite exacte

$$\{1\} \longrightarrow \underline{S}_\ell(\mathbf{F}_\ell) \longrightarrow \underline{H}_\ell(\mathbf{F}_\ell) \longrightarrow (\underline{H}_\ell/\underline{S}_\ell)(\mathbf{F}_\ell) \longrightarrow \{1\},$$

on est ramené à prouver que l'image de G_ℓ dans $(\underline{H}_\ell/\underline{S}_\ell)(\mathbf{F}_\ell)$ est d'indice borné. C'est là une question "abélienne", donc facile ! On peut par exemple la traiter en utilisant le déterminant relatif à L, qui donne une isogénie

$$\det_L : \underline{H}_\ell/\underline{S}_\ell \longrightarrow \delta(\underline{C}_\ell) \subset T_{L,\ell}.$$

La théorie abélienne (McGill) montre que l'image de G_ℓ dans les points rationnels de $\delta(\underline{C}_\ell)$ est d'indice borné ; comme l'isogénie ci-desus est également de degré borné (facile), on obtient ce que l'on veut.

(Autre possibilité : utiliser les tores d'inertie, qui contiennent beaucoup de points rationnels provenant de G_ℓ.)

Remarques

1) La démonstration ci-dessus fournit une autre définition du groupe $\underline{H}_\ell$: c'est le groupe algébrique engendré par $\underline{S}_\ell$ et par les tores d'inertie relatifs aux places divisant ℓ. (Conjecturalement, les tores d'inertie devraient suffire à engendrer $\underline{H}_\ell$, mais je ne vois pas comment le démontrer. On avait rencontré une situation analogue dans le cas ℓ-adique.)

2) Il est naturel de se demander si (ii) peut être renforcé en :

(ii ?) - *On a $G_\ell = \underline{H}_\ell(\mathbf{F}_\ell)$ pour ℓ assez grand.*

La réponse est "non". L'assertion (ii ?) peut être fausse même dans le cas CM, j'en ai donné des exemples il y a longtemps (et Ken en a donné d'autres).

3) Le théorème 1 n'est utile que si l'on montre que les groupes $\underline{H}_\ell$ sont "assez gros", en un sens convenable. Ce sera l'objet des n$^{\mathrm{os}}$ 6 et 7.

4) J'aurais dû énoncer explicitement dans le théorème que *le commutant de $\underline{H}_\ell$ (dans $\mathrm{End}(A) = M_{2n}(\mathbf{F}_\ell)$) est* $\mathbf{F}_\ell \otimes \mathrm{End}(A)$ si ℓ est assez grand. En effet, on sait que c'est vrai pour G_ℓ d'après Faltings ; le commutant en question est donc contenu dans $\mathbf{F}_\ell \otimes \mathrm{End}(A)$. Et d'autre part, les éléments de $\underline{H}_\ell(\mathbf{F}_\ell)$ commutent à $\mathrm{End}(A)$, on l'a vu en cours de démonstration.

En particulier, si $\mathrm{End}(A) = \mathbf{Z}$, *la représentation* $\underline{S}_\ell \to \mathbf{GL}_{2n}$ *est absolument simple.*

5) Plus généralement, si $(i.j)$ est un couple d'entiers donné, les invariants tensoriels de type (i,j) de G_ℓ et de $\underline{H}_\ell$ *sont les mêmes*, pour ℓ assez grand (le "assez grand" dépend bien sûr du couple (i,j) choisi). En effet, tout invariant tensoriel de type (i,j) de G_ℓ est invariant par $\underline{S}_\ell$ si ℓ est assez grand (petit lemme sur les exponentielles), et aussi par les tores d'inertie (rigidité).

5. Le groupe des homothéties

Lemme – *Le tore C du* § 3 b) *contient le groupe* $\mathbf{G}_m$ *des homothéties.*

Si j'avais décrit C explicitement, ce serait évident (du moins je l'espère...). Comme je ne l'ai pas fait, il me faut utiliser la théorie ℓ-adique exposée l'an dernier. Celle-ci montre que l'enveloppe algébrique du groupe de Galois ℓ-adique G_{ℓ^∞} a pour composante neutre un groupe réductif donc le centralisateur connexe est le tore $C_{\mathbf{Q}_\ell}$. Or cette composante contient les homothéties (Bogomolov – et Deligne). Donc C contient $\mathbf{G}_m$.

Une fois ce lemme prouvé, on voit que $\underline{H}_\ell$ contient $\mathbf{G}_{m/\mathbf{F}_\ell}$ pour ℓ assez grand. Vu le théorème 1, cela entraîne :

Théorème – *Il existe une constante c telle que le groupe G_ℓ contienne un sous-groupe d'indice $\leq c$ du groupe $\mathbf{F}_\ell^*$ des homothéties.*

(Précisons que c dépend de A et de K.)

J'aimerais bien démontrer *que G_ℓ contient $\mathbf{F}_\ell^*$ tout entier pour ℓ assez grand*, mais je n'y suis pas parvenu. Ça a pourtant l'air abordable – et c'est vrai dans des tas de cas particuliers. C'est vexant !

6. Le rang du groupe $\underline{H}_\ell$

Soit $\underline{H}_{\ell^\infty}$ l'enveloppe algébrique du groupe ℓ-adique G_{ℓ^∞}. On a vu dans le cours de l'an dernier que $\underline{H}_{\ell^\infty}$ a un *rang* r qui est indépendant de ℓ.

Théorème 2 – *Le rang de $\underline{H}_\ell$ est égal à r pour ℓ assez grand.*

Démonstration

On utilise l'application cl : $\mathbf{GL}_{2n} - \mathbf{Aff}_*^{2n}$ qui avait déjà servi l'an dernier, dans le cas ℓ-adique. Je te rappelle ce que c'est :

$\mathbf{Aff}_*^{2n}$ est l'espace affine de dimension $2n$ privé de l'hyperplan "dernière coordonnée $= 0$" : ses points sont des vecteurs $(a_1, \ldots, a_{2n})$ avec a_{2n} inversible ;

cl est le morphisme de $\mathbf{GL}_{2n}$ dans $\mathbf{Aff}_*^{2n}$ qui attache à toute matrice inversible les coefficients de son polynôme caractéristique.

On avait vu que, si H est un sous-groupe réductif connexe de $\mathbf{GL}_{2n}$, $\mathrm{cl}(H)$ est une sous-variété irréductible fermée de $\mathbf{Aff}_*^{2n}$, définie sur $\mathbf{Q}$, et de dimension égale au rang de H. (On voyait ça en remplaçant H par un tore maximal.)

On va appliquer ça à la fois en caractéristique 0 et en caractéristique $\ell > 0$. On s'intéresse d'abord (en caractéristique 0) à des groupes réductifs du type $C.\Sigma$, où C est mon tore usuel, et Σ est semi-simple commutant à C. A conjugaison près (dans une clôture algébrique), il n'y a qu'un nombre fini de tels groupes, d'où, par cl, un nombre fini de sous-variétés[(*)] $P_1, \ldots, P_h$ de $\mathbf{Aff}_*^{2n}$, de dimensions $r_1, \ldots, r_h$. La variété $\mathrm{cl}(\underline{H}_{\ell^\infty})$ est égale à l'une d'elles, disons P_1 (on sait en effet que $\mathrm{cl}(\underline{H}_{\ell^\infty})$ est indépendante de ℓ) ; on peut d'ailleurs caractériser P_1 directement : c'est l'adhérence pour la topologie de Zariski des points de $\mathbf{Aff}_*^{2n}(\mathbf{Q})$ attachés aux *endomorphismes de Frobenius* des réductions de A, on l'a vu. En particulier, on a $r = r_1$.

Il faut maintenant passer de là au rang des groupes $\underline{H}_\ell$, en caractéristique ℓ. On va utiliser le fait suivant : si ℓ est assez grand, $\underline{H}_\ell$ *est la réduction* (mod ℓ) *d'un groupe réductif connexe du type $C.\Sigma$ ci-dessus.* J'avais dit ça (et je l'avais démontré) pour le groupe semi-simple $\underline{S}_\ell$, mais c'est aussi vrai (il faut un petit argument supplémentaire) pour le groupe $\underline{H}_\ell = \underline{C}_\ell \cdot \underline{S}_\ell$. Il en résulte que, toujours pour ℓ assez grand, la variété $\mathrm{cl}(\underline{H}_\ell)$ *est la réduction* (mod ℓ) *de l'une des variétés P_i introduites ci-dessus.* Le théorème 2 sera prouvé (et même précisé !) si je montre que $\mathrm{cl}(\underline{H}_\ell) = P_{1/\mathbf{F}_\ell}$ pour tout ℓ assez grand. (Autrement dit, $\underline{H}_\ell$ et $\underline{H}_{\ell^\infty}$ ont "le même" tore maximal.)

Je choisis d'abord une place v de K ayant la propriété que la classe $\mathrm{cl}(\sigma_v)$ de son Frobenius ne se trouve dans aucune des sous-variétés $P_1 \cap P_j$ distinctes de P_1 ; un tel v existe grâce à la propriété de densité que j'ai rappelée. Par réduction (mod ℓ) , on aura la même propriété pour presque tout ℓ (en effet, si un point n'est pas dans une sous-variété, il n'y est pas non plus mod ℓ, sauf pour un nombre fini de valeurs de ℓ). Pour ces ℓ là on est sûr que $\mathrm{cl}(\underline{H}_\ell)$ contient P_1 (ce qui montre

(*) la lettre P correspond à "polynôme"

déjà que le rang de $\underline{H}_\ell$ est $\geq r$).

Il faut maintenant prouver que $\mathrm{cl}(\underline{H}_\ell)$ n'est pas plus grand que P_1 ou, ce qui revient au même, que le rang de $\underline{H}_\ell$ est $\leq r$. (Ça devrait être trivial : on se dit que le rang ne peut pas augmenter par réduction mod ℓ !) Suppose que ce ne soit pas le cas, et que ce rang soit $\geq r+1$. Je vais d'abord prouver que *le nombre d'éléments de* $\mathrm{cl}(G_\ell)$ *est* $\gg \ell^{r+1}$ (i.e. $\geq c\ell^{r+1}$, où c est un nombre > 0 indépendant de ℓ). Cela se fait ainsi : on choisit un tore maximal Θ de $\underline{H}_\ell$ rationnel sur $\mathbf{F}_\ell$, et on remarque que $|\Theta(\mathbf{F}_\ell)| \gg \ell^{r+1}$; comme G_ℓ est d'indice borné dans $\underline{H}_\ell(\mathbf{F}_\ell)$, l'indice de $G_\ell \cap \Theta(\mathbf{F}_\ell)$ dans $\Theta(\mathbf{F}_\ell)$ est borné, et l'on a $|G_\ell \cap \Theta(\mathbf{F}_\ell)| \gg \ell^{r+1}$. D'autre part, le morphisme $\mathrm{cl} : \Theta \to \mathbf{Aff}^{2n}_*$ est un morphisme fini dont le degré est borné par exemple par $(2n)!$! On a donc bien :

$$|\mathrm{cl}(G_\ell)| \geq |\mathrm{cl}(G_\ell \cap \Theta(\mathbf{F}_\ell))| \geq |G_\ell \cap \Theta(\mathbf{F}_\ell)|/(2n)! \gg \ell^{r+1}.$$

Mais d'autre part $\mathrm{cl}(G_\ell)$ est simplement la réduction (mod ℓ) de $\mathrm{cl}(G_{\ell^\infty})$, donc est contenu dans $P_1(\mathbf{F}_\ell)$. Puisque P_1 est une variété de dimension r, son nombre de points (mod ℓ) est $\ll \ell^r$. Contradiction !

Remarque.– On devrait pouvoir simplifier cette démonstration. Intuitivement, un petit rang signifie "beaucoup de relations multiplicatives entre les valeurs propres des Frobenius" et l'on sait en outre que ces relations sont engendrées par celles à petits coefficients. Cela devrait suffire à montrer que ces relations se voient aussi bien en caractéristique ℓ qu'en caractéristique 0. (J'ai essayé de rédiger une démonstration basée sur ce principe, mais je me suis embourbé.)

7. Où l'on trouve le groupe symplectique

Dans cette section, on s'intéresse *au cas où* $\mathrm{End}(A) = \mathbf{Z}$ (il s'agit des $\overline{K}$-endomorphismes). Le groupe C est alors réduit à $\mathbf{G}_m$ (homothéties), et les groupes $\underline{S}_\ell$ sont absolument irréductibles pour ℓ grand.

Le rang commun r des groupes $\underline{H}_{\ell^\infty}$ (cf. n° 6) est $\leq n+1$, du fait que ces groupes sont contenus dans le groupe des similitudes symplectiques $\mathbf{GSp}_{2n} = \mathbf{G}_m.\mathbf{Sp}_{2n}$. On a vu dans le cours de l'an dernier que *l'on a* $r = n+1$ *si et seulement si* $\underline{H}_{\ell^\infty} = \mathbf{GSp}_{2n/\mathbf{Q}_\ell}$ pour tout ℓ. Et l'on a vu aussi que $r = n+1$ dès que n est impair (ou $n = 2, 6$ – mais pas $n = 4$). On va maintenant obtenir un résultat bien plus précis :

Théorème 3 – *Supposons* $\mathrm{End}(A) = \mathbf{Z}$ *et* $r = n+1$. *Alors* :

(a) $G_\ell = \mathbf{GSp}_{2n}(\mathbf{F}_\ell)$ *pour* ℓ *grand,*

(b) $G_{\ell^\infty} = \mathbf{GSp}_{2n}(\mathbf{Z}_\ell)$ *pour* ℓ *grand.*

(c) *l'image de* $\mathrm{Gal}(\overline{K}/K)$ *dans le produit restreint* $\prod'_\ell \mathbf{GSp}_{2n}(\mathbf{Q}_\ell)$ *est ouverte* (pour la topologie adélique).

Remarques

1) En fait, l'assertion (c) entraîne (a) et (b). Mais on démontrera d'abord (a), puis (b), et on en déduira (c).

2) Quitte à étendre le corps de base, et à faire une isogénie (ce qui ne change rien), on peut supposer que A admet une polarisation de degré 1. On a alors $G_{\ell^\infty} \subset \mathbf{GSp}_{2n}(\mathbf{Z}_\ell)$ pour tout ℓ, et l'assertion (c) prend la forme plus parlante suivante :

(c') *L'image de* $\mathrm{Gal}(\overline{K}/K)$ *dans* $\prod_\ell \mathbf{GSp}_{2n}(\mathbf{Z}_\ell)$ *est ouverte* (donc d'indice fini), *pour la topologie produit.*

Le théorème 3 entraîne évidemment :

Corollaire – *Si* $\mathrm{End}(A) = \mathbf{Z}$ *et si* n *est impair ou égal à* 2 *ou* 6, *les assertions* (a), (b), (c) *ci-dessus sont vraies.*

Dans le cas $n = 1$, on retrouve le théorème que j'avais publié dans *Invent. Math.* **15** (1972).

Démonstration

Je suppose que A admet une polarisation de degré 1 (cf. Remarque 2 ci-dessus), ce qui entraîne $G_{\ell^\infty} \subset \mathbf{GSp}_{2n}(\mathbf{Z}_\ell)$ pour tout ℓ et *a fortiori* $G_\ell \subset \mathbf{GSp}_{2n}(\mathbf{F}_\ell)$.

Démonstration de (a)

Le groupe G_ℓ^+ est contenu dans $\mathbf{GSp}_{2n}(\mathbf{F}_\ell)$, et est engendré par des ℓ-éléments : il est donc contenu dans $\mathbf{Sp}_{2n}(\mathbf{F}_\ell)$, et on en déduit (pour $\ell \geq 4n$, par exemple) que le groupe semi-simple $\underline{S}_\ell$ est contenu dans $\mathbf{Sp}_{2n/\mathbf{F}_\ell}$. Pour ℓ assez grand, $\underline{S}_\ell$ jouit donc des deux propriétés suivantes :

(1) C'est un sous-groupe semi-simple absolument irréductible du groupe $\mathbf{Sp}_{2n/\mathbf{F}_\ell}$.

(2) Son rang est n (d'après le théorème 2 et l'hypothèse $r = n+1$).

Or les propriétés (1) et (2) *entraînent* $\underline{S}_\ell = \mathbf{Sp}_{2n/\mathbf{F}_\ell}$, du moins pour $\ell \neq 2$ (pour $\ell = 2$, $\underline{S}_\ell$ pourrait être égal à un groupe orthogonal $\mathbf{SO}_{2n/\mathbf{F}_\ell}$, groupe qui jouit manifestement des propriétés (1) et (2) pour $n \geq 2$). C'est une question de systèmes de racines, que j'avais expliquée l'an dernier – et je viens d'avoir la chance de recevoir un preprint de G.M. Seitz (Mem. AMS **365**, p. 278), où c'est explicitement démontré (et c'est de là que je tire le contre-exemple pour $\ell = 2$, qui m'avait d'abord échappé, oh honte).

Ceci dit, il résulte de ce qui a été fait au début du cours que $G_\ell^+ = \mathbf{Sp}_{2n}(\mathbf{F}_\ell)^+ = \mathbf{Sp}_{2n}(\mathbf{F}_\ell)$ pour ℓ grand. Ainsi, G_ℓ contient $\mathbf{Sp}_{2n}(\mathbf{F}_\ell)$. On regarde alors la suite exacte :

$$(*) \qquad \{1\} \longrightarrow \mathbf{Sp}_{2n} \longrightarrow \mathbf{GSp}_{2n} \xrightarrow{c} \mathbf{G}_m \longrightarrow \{1\},$$

où c est l'homomorphisme qui attache à toute similitude son multiplicateur. Sur $\mathbf{F}_\ell$, cette suite exacte donne :

$$\{1\} \longrightarrow \mathbf{Sp}_{2n}(\mathbf{F}_\ell) \longrightarrow \mathbf{GSp}_{2n}(\mathbf{F}_\ell) \xrightarrow{c} \mathbf{F}_\ell^* \longrightarrow \{1\}.$$

De plus, on sait que le composé $\mathrm{Gal}(\overline{K}/K) \to G_\ell^+ \xrightarrow{c} \mathbf{F}_\ell^*$ n'est autre que le ℓ-ème caractère cyclotomique, i.e. celui qui donne l'action de $\mathrm{Gal}(\overline{K}/K)$ sur μ_ℓ. Si ℓ est assez grand, ce caractère est surjectif. Comne G_ℓ contient $\mathbf{Sp}_{2n}(\mathbf{F}_\ell)$, on a donc bien $G_\ell = \mathbf{GSp}_{2n}(\mathbf{F}_\ell)$.

Démonstration de (b)

On travaille avec un ℓ fixé, et l'on utilise le lemme suivant :

Lemme 1 – *Supposons $\ell \geq 5$. Soit X un sous-groupe fermé de $\mathbf{Sp}_{2n}(\mathbf{Z}_\ell)$ ayant pour image $\mathbf{Sp}_{2n}(\mathbf{F}_\ell)$ par réduction* (mod ℓ). *Alors X est égal à $\mathbf{Sp}_{2n}(\mathbf{Z}_\ell)$.*

Pour $n = 1$, la démonstration est faite dans McGill, p. IV-23 à IV-24. Cette démonstration repose essentiellement sur le fait que l'algèbre de Lie de $\mathbf{SL}_2$ est engendrée (linéairement) par des matrices u telles que $u^2 = 0$. Or ce fait se généralise à $\mathbf{Sp}_{2n}$, pour n quelconque. D'où le résultat, par la même démonstration. (Peut-être y a-t-il une référence dans la littérature qui m'éviterait de refaire la démonstration ?)

On applique ce lemme au groupe $X =$ adhérence du groupe dérivé de G_{ℓ^∞}. Il est clair que X est contenu dans $\mathbf{Sp}_{2n}(\mathbf{Z}_\ell)$. D'autre part, si ℓ est assez grand, G_{ℓ^∞} se projette sur $\mathbf{GSp}_{2n}(\mathbf{F}_\ell)$, donc X se projette sur le groupe dérivé de $\mathbf{GSp}_{2n}(\mathbf{F}_\ell)$ qui n'est autre que $\mathbf{Sp}_{2n}(\mathbf{F}_\ell)$ (pour $\ell \geq 5$, ici encore). Vu le lemme, on en conclut que X est égal à $\mathbf{GSp}_{2n}(\mathbf{Z}_\ell)$. La démonstration de (b) se termine comme dans le cas (a), en utilisant la suite exacte

$$\{1\} \longrightarrow \mathbf{Sp}_{2n}(\mathbf{Z}_\ell) \longrightarrow \mathbf{GSp}_{2n}(\mathbf{Z}_\ell) \xrightarrow{c} \mathbf{Z}_\ell^* \longrightarrow \{1\}$$

combinée avec le fait que l'image de $\chi_\ell : \mathrm{Gal}(\overline{K}/K) \to G_{\ell^\infty} \xrightarrow{c} \mathbf{Z}_\ell^*$ est $\mathbf{Z}_\ell^*$ tout entier, pour ℓ grand.

Démonstration de (c)

Ici encore, on imite ce qui est fait dans McGill, p. IV-18 à IV-27. Utilisant de nouveau un groupe dérivé, ainsi que la suite exacte $(*)$ de la page précédente, on se ramène à prouver l'énoncé suivant :

Lemme 2 – *Soit X un sous-groupe fermé de $\prod_\ell \mathbf{Sp}_{2n}(\mathbf{Z}_\ell)$. Supposons que, pour tout ℓ* (resp. *pour presque tout ℓ*), *la projection*

$$X \longrightarrow \mathbf{Sp}_{2n}(\mathbf{Z}_\ell)$$

ait une image ouverte (resp. *soit surjective*). *Alors X est ouvert.*

La démonstration utilise les propriétés suivantes des groupes $\Sigma_\ell = \mathbf{Sp}_{2n}(\mathbf{F}_\ell)/\{\pm 1\}$:

(1) Aucun sous-groupe propre de $\mathbf{Sp}_{2n}(\mathbf{F}_\ell)$ ne s'applique sur Σ_ℓ. Facile !

(2) A part les trois cas : $n = 1$, $\ell = 2$ ou 3 et $n = 2$, $\ell = 2$, le groupe Σ_ℓ est un groupe *simple non abélien*. Classique !

(3) Si ℓ est assez grand (e.g. $\ell > 2n$), Σ_ℓ *n'intervient dans aucun des $\Sigma_{\ell'}$ pour $\ell' \neq \ell$.*

(On dit qu'un groupe simple Σ *intervient* dans un groupe G si Σ est isomorphe à un quotient d'un sous-groupe de G.)

Voici une façon possible de prouver (3) : on remarque que, pour $\ell > 2n$, tout ℓ-sous-groupe de $\mathbf{GL}_{2n}(\mathbf{F}_{\ell'})$, avec $\ell' \neq \ell$, est *abélien* (décomposer en somme de représentations irréductibles, et noter que toute représentation irréductible d'un ℓ-groupe est de degré 1 ou $\geq \ell$). Si donc Σ_ℓ intervenait dans un $\Sigma_{\ell'}$, son ℓ-groupe de Sylow serait abélien, ce qui n'est pas le cas (sauf pour $n = 1$, cas que l'on traite directement, cf. McGill).

Une fois armé de ces propriétés, on démontre le lemme 2 tout simplement en recopiant la démonstration donnée pour $n = 1$ dans McGill, p. IV-24 à IV-27. Je n'ai pas envie d'en dire plus.

8. Compléments

Les théorèmes 1, 2 et 3 constituent les résultats principaux du cours. Suivant le temps qu'il me restera (et mon énergie), je donnerai ou non les compléments suivants :

8.1 – *Généralisation aux corps K de type fini sur $\mathbf{Q}$*

Sauf erreur, *tous* les énoncés restent valables dans cette situation plus générale. La seule différence dans les démonstrations réside dans l'endroit où j'utilisais le théorème de finitude de Hermite (et aussi, un peu, dans l'emploi des tores d'inertie). Lorsque K est de type fini sur $\mathbf{Q}$, il faut faire un peu plus attention, mais Raynaud m'a convaincu que ça marchait quand même. On verra bien.

8.2 – *Transposition aux corps de fonctions en caractéristique $p > 0$*

Les énoncés sont un peu modifiés, du fait, par exemple, que G_{ℓ^∞} n'est plus un sous-groupe *ouvert* de son enveloppe algébrique.

Toutefois, c'est uniquement la partie abélienne qui "ne se remplit pas" : le reste se remplit comme en caractéristique 0. Par exemple, dans la situation(*) du théorème 3, on trouve que l'image de $\mathrm{Gal}(\overline{K}, K)$ dans $\prod_\ell \mathbf{GSp}_{2n}(\mathbf{Z}_\ell)$ contient un sous-groupe ouvert du produit des $\mathbf{Sp}_{2n}(\mathbf{Z}_\ell)$; par contre son image dans $\prod_\ell \mathbf{Z}_\ell^*$ par l'homomorphisme c est loin d'être ouverte : elle est isomorphe à $\widehat{\mathbf{Z}}$.

Quant aux démonstrations, elles sont plutôt plus simples qu'en caractéristique 0 car il n'y a plus lieu de faire intervenir des tores d'inertie : il n'y a plus de places au-dessus de ℓ !

8.3 – *Exemples numériques*

J'aimerais bien faire en genre 2 ce que j'avais fait pour le genre 1, i.e. partir de courbes de genre 2 explicites, et tâcher de dire à partir de quand le groupe de Galois correspondant G_ℓ devient égal à $\mathbf{GSp}_4(\mathbf{F}_\ell)$. Dans ce genre de question, les

(*) Attention ! Je ne sais pas si le *corollaire* au théorème 3 reste vrai en caractéristique p. Il y a des difficultés car on n'a plus de "tores de Hodge".

8 tores d'inertie jouent certainement un rôle essentiel : on devrait s'en tirer en les utilisant, et en calculant sur machine un très petit nombre de Frobenius (Mestre m'en a fourni quelques tables que je n'ai pas commencé à exploiter).

Voila. Je crois que c'est à peu près tout(*).

(*) Peut-être donnerai-je aussi la démonstration du théorème de Matthews-Vaserstein-Weisfeiler et Nori : si Γ est un sous-groupe Zariski dense de type fini de $\mathbf{Sp}_{2n}(\mathbf{Q})$, son adhérence dans le groupe adélique $\prod'_\ell \mathbf{Sp}_{2n}(\mathbf{Q}_\ell)$ est ouverte, i.e. Γ a la proprieté d'"approximation forte". La démonstration est analogue à celle des théorèmes 1, 2 , 3 ci-dessus, mais nettement plus facile.

138.

Lettre à Ken Ribet du 7/3/1986

Cher Ken.

J'ai envie de te raconter les démonstrations de quelques résultats que je suis en train d'exposer dans mon cours, et qui ne figurent pas dans ma lettre à Marie-France du 10 février.

1. Indépendance des groupes de Galois ℓ-adiques

Les notations sont celles de ma lettre à Marie-France,§ 3 : je note G_ℓ le groupe de Galois des points de division par ℓ. Comme il me faut aussi parler du groupe ℓ-adique correspondant, je note ce dernier G_{ℓ^∞} : ce n'est pas très commode, mais je n'ai rien trouvé de mieux.

1 **Théorème** – *Si K est assez grand, l'image de*

$$G_K \longrightarrow \prod_\ell G_{\ell^\infty} \qquad (\text{où } G_K = \mathrm{Gal}(\overline{K}/K))$$

est un sous-groupe ouvert du produit des G_{ℓ^∞}.

(On a envie de formuler ça en disant que les extensions de K engendrées par les points de ℓ^∞-division sont *presque* linéairement disjointes, si K est assez grand.)

Corollaire – *Si K est assez grand, l'image de $G_K \to \prod_\ell G_\ell$ est ouverte.*

Bien entendu, ceci n'est vrai que si K est assez grand : l'exemple des courbes elliptiques à multiplication complexe par $\mathbf{Q}(\sqrt{-d})$, avec $\sqrt{-d} \notin K$, le montre.

On peut si l'on veut reformuler le théorème en disant qu'il existe une *suite* de corps K arbitrairement grands (i.e. de réunion $\overline{K}$) telle que, pour chacun d'eux, $G_K \to \prod_\ell G_{\ell^\infty}$ soit *surjectif*.

1.1. *Une propriété préliminaire des G_ℓ*

Considérons la propriété suivante de G_ℓ :

(1_ℓ) – *Le groupe G_ℓ est engendré par G_ℓ^+ et par les groupes d'inertie en les places de $\overline{K}$ divisant ℓ.*

Je te rappelle que G_ℓ^+ est par définition le sous-groupe de G_ℓ engendré par les éléments d'ordre une puissance de ℓ. Pour ℓ assez grand, on sait que c'est aussi $\mathbf{S}_\ell(\mathbf{F}_\ell)^+$, image de $\widetilde{\mathbf{S}}_\ell(\mathbf{F}_\ell) \to \mathbf{S}_\ell(\mathbf{F}_\ell)$, cf. lettre à Marie-France.

Proposition – *Si K est assez grand, la propriété (1_ℓ) est vraie pour tout ℓ assez grand.*

(Le "assez grand" relatif à ℓ dépend du corps K choisi.)

Appelle G'_ℓ le sous-groupe de G_ℓ engendré par G_ℓ^+ et par les sous-groupes d'inertie en les places divisant ℓ. Il est facile de voir que, lorsqu'on remplace K par une extension finie, on ne change qu'un nombre fini des G'_ℓ (car il en est ainsi de G_ℓ^+, ainsi que des groupes d'inertie). D'autre part, on a :

Lemme – *Pour ℓ assez grand, G_ℓ^+ est égal à son propre groupe dérivé, et c'est*
2 *aussi le groupe dérivé de G_ℓ, ainsi que de $\mathbf{H}_\ell(\mathbf{F}_\ell)$.*

C'est là une propriété générale des groupes réductifs (facile).

Ceci dit, supposons que A soit semi-stable sur K. Notons K_ℓ l'extension de K correspondant au groupe quotient G_ℓ/G'_ℓ. Cette extension est abélienne, non ramifiée au-dessus de ℓ, et non ramifiée aux places de mauvaise réduction (car les groupes d'inertie correspondants sont unipotents, donc tombent dans G_ℓ^+). Donc K_ℓ est contenue dans le corps de classes absolu K' de K. En remplaçant K par K', on gagne.

1.2. *Démonstration du théorème*

On suppose à partir de maintenant que K est assez grand pour que l'on ait (1_ℓ) pour tout ℓ assez grand. On se propose de montrer que cela entraîne que $G_K \to \prod_\ell G_{\ell^\infty}$ a une image *ouverte*.

On va d'abord prouver l'indépendance des G_{ℓ^∞} pour ℓ assez grand. En d'autres termes :

Lemme 1.2.1 – *Il existe ℓ_0* (dépendant de K) *tel que l'homomorphisme*

$$G_K \longrightarrow \prod_{\ell \geq \ell_0} G_{\ell^\infty}$$

soit surjectif.

Il revient au même de prouver l'existence d'un ℓ_0, tel que, si $\ell_1 < \ldots < \ell_k$ sont des nombres premiers $\geq \ell_0$, l'homomorphisme

$$G_K \longrightarrow G_{\ell_1^\infty} \times \ldots \times G_{\ell_k^\infty}$$

soit surjectif.

On prendra pour ℓ_0 un nombre premier ≥ 5 tel que, pour tout $\ell \geq \ell_0$, on ait les propriétés agréables suivantes :

- A a bonne réduction en les places divisant ℓ,
- (1_ℓ) est vrai,
- G_ℓ^+ est égal à $\mathbf{S}_\ell(\mathbf{F}_\ell)^+$.

Pour prouver la propriété de surjectivité ci-dessus, on raisonnera par récurrence sur k. Je me borne à donner l'argument pour $k = 2$: le cas général n'est pas plus difficile.

D'après le "lemme de Goursat", tout revient à prouver qu'il n'existe pas d'homomorphisme surjectif $f : G_K \to X$, où X est un groupe profini $\neq \{1\}$, qui se factorise à la fois par $G_K \to G_{\ell_1^\infty}$ et par $G_K \to G_{\ell_2^\infty}$. On peut de plus supposer que X est un *groupe fini simple*. Il y a alors diverses possibilités à distinguer :

(a) X est isomorphe à $\mathbf{Z}/\ell\mathbf{Z}$, où ℓ est un nombre premier $\neq \ell_1$. Soit $G(\ell_1)$ le noyau de $G_{\ell_1^\infty} \to G_{\ell_1}$; c'est un pro-ℓ_1-groupe. Son image dans X est donc triviale, i.e. l'homomorphisme $G_{\ell_1^\infty} \to X$ se factorise par G_{ℓ_1}. Mais G_{ℓ_1} est engendré par les groupes d'inertie en ℓ_1 dont l'image dans X est triviale (l'inertie en ℓ_1 ayant une image triviale dans $G_{\ell_2^\infty}$) et par $G_{\ell_1}^+$ qui est égal à son dérivé. Contradiction.

(b) Même argument, si $X \simeq \mathbf{Z}/\ell\mathbf{Z}$ avec $\ell \neq \ell_2$.

(c) X est simple non abélien.

Les mêmes arguments que ci-dessus montrent que $G_{\ell_i^\infty} \to X$ se factorise en $G_{\ell_i} \to X$, et que $G_{\ell_i}^+ \to X$ est surjectif. Il en résulte que X est un quotient simple non abélien de $\widetilde{\mathbf{S}}_{\ell_i}(\mathbf{F}_{\ell_i})$, autrement dit, c'est un groupe simple "de Lie de caractéristique ℓ_i", pour $i = 1, 2$. Mais il est connu que, si l'on se borne aux caractéristiques ≥ 5, il n'y a aucun isomorphisme exceptionnel entre groupes simples de caractéristiques différentes (du genre $\mathbf{SL}_3(\mathbf{F}_2) = \mathbf{PSL}_2(\mathbf{F}_7)$, par exemple) : même les ordres de ces groupes sont différents ! D'où encore une contradiction, ce qui achève la démonstration du lemme 1.2.1.

Fin de la démonstration du théorème

On choisit un ℓ_0 auquel on puisse appliquer 1.2.1, et on note A l'image de G_K dans $\prod_{\ell < \ell_0} G_{\ell^\infty}$. Un argument élémentaire montre que A est ouvert dans ce produit.

Si l'on pose

$$B = \prod_{\ell \geq \ell_0} G_{\ell^\infty},$$

on a un homomorphisme $G_K \to A \times B$ dont les deux projections sont surjectives, et l'on est ramené ici encore à un "lemme de Goursat". Autrement dit, on doit prouver que si l'on a un homomorphisme surjectif $G \to X$ qui se factorise à la fois par $G_K \to A$ et par $G_K \to B$, alors X est *fini*.

Notons d'abord que l'ordre (profini) de X n'est divisible que par les nombres premiers divisant $|A|$, lesquels sont en nombre fini. On peut donc choisir un entier $M \geq \ell_0$ tel que

$$|X| = \prod_{\ell \leq M} \ell^{x(\ell)}, \quad \text{avec } x(\ell) \in \{0, 1, 2, \ldots, \infty\},$$

et tout revient à voir que les exposants $x(\ell)$ sont finis.

Pour cela, on commence par prouver que, si $\ell > M$, *l'image de* G_{ℓ^∞} (vu comme sous-groupe de B) *dans* X *est triviale*. En effet, comme ℓ ne divise pas $|X|$, cette image se factorise par G_ℓ ; mais les groupes d'inertie en ℓ ont une image triviale dans X (du fait que X est quotient de A), et il en est de même de G_ℓ^+, qui est engendré par des éléments d'ordre ℓ. Il résulte de là que l'homomorphisme surjectif $B \to X$ se factorise par un produit fini partiel :

$$\prod_{\ell_0 \leq \ell \leq M} G_\ell \longrightarrow X.$$

Mais, si $\ell < \ell_0$, l'exposant de ℓ dans l'ordre de ce produit partiel est fini. On a donc $x(\ell) \neq \infty$ pour tout $\ell < \ell_0$. D'autre part, puisque X est quotient de A, on a aussi $x(\ell) \neq \infty$ pour tout $\ell \geq \ell_0$. Ceci suffit à prouver que $x(\ell)$ est fini pour tout ℓ, donc que X est fini, ce qui achève la démonstration du théorème.

2. Où l'on montre que G_{ℓ^∞} contient "beaucoup" d'homothéties

On sait (Bogomolov) que G_{ℓ^∞} contient un sous-groupe *ouvert* du groupe $\mathbf{Z}_\ell^*$ des homothéties. Appelle $e(\ell)$ l'indice dans $\mathbf{Z}_\ell^*$ du groupe $G_{\ell^\infty} \cap \mathbf{Z}_\ell^*$. Je me propose de démontrer :

Théorème – *Quand* ℓ *varie, les* $e(\ell)$ *restent bornés.*

Vu le § 1, ce théorème entraîne le suivant :

Théorème – *Il existe une constante $c = c(K, A) \geq 1$ telle que l'image de $G_K \to \prod_\ell G_{\ell^\infty}$ contienne toutes les homothéties qui sont des puissances c-ièmes.*

Ces théorèmes sont moins bons que ce que l'on conjecture d'habitude, à savoir que $e(\ell) = 1$ pour ℓ assez grand, ou encore que l'image de G_K contient un sous-groupe *ouvert* du groupe des homothéties. Ils sont cependant suffisamment bons pour les applications aux courbes contenant une infinité de points de torsion, à la Lang.

Pour la *démonstration* de ces théorèmes, il est commode de prouver un peu plus. Je te rappelle que l'adhérence (pour la topologie de Zariski) de G_{ℓ^∞} est un certain groupe réductif connexe produit d'un tore C essentiellement indépendant de ℓ par un groupe semi-simple. De façon plus précise, le tore C se déduit par le changement de base $\mathbf{Q} \to \mathbf{Q}_\ell$ d'un certain sous-tore C_0 du tore T_L attaché au centre L de $\mathbf{Q} \otimes \mathrm{End}\, A$. On peut parler des "points de C à valeurs dans $\mathbf{Z}_\ell$", qui forment un groupe que je noterai $C(\mathbf{Z}_\ell)$. (Disons en tout cas que cela a un sens pour presque tout ℓ, par exemple en choisissant un modèle de C_0 sur $\mathbf{Z}$.) Appelons $c(\ell)$ l'indice de $C(\mathbf{Z}_\ell) \cap G_{\ell^\infty}$ dans $C(\mathbf{Z}_\ell)$. L'énoncé plus fort que je désire démontrer est :

Théorème – *Quand ℓ varie, les $c(\ell)$ restent bornés.*

(Comme $e(\ell)$ est $\leq c(\ell)$, c'est bien un résultat plus fort que celui portant simplement sur les homothéties.)

2.1. *Démonstration du théorème lorsque* $\mathrm{End}\, A = \mathbf{Z}$

(J'expose d'abord ce cas particulier, qui est plus simple que le cas général, mais contient pourtant l'argument essentiel.)

L'énoncé ne concerne que les ℓ assez grands. On peut en particulier supposer que ℓ ne divise pas le degré d'une polarisation de A, ce qui fait que G_{ℓ^∞} est contenu dans le groupe $\mathbf{GSp}_{2n}(\mathbf{Z}_\ell)$ des similitudes symplectiques. On note

$$N : \mathbf{GSp}_{2n} \longrightarrow \mathbf{G}_m$$

l'homomorphisme "norme", qui attache à toute similitude symplectique son multiplicateur.

On va associer au groupe G_{ℓ^∞} un certain sous-groupe Y de $\mathbf{Sp}_{2n}(\mathbf{Z}_\ell)$ défini de la façon suivante :

Pour qu'un élément y de $\mathbf{Sp}_{2n}(\mathbf{Z}_\ell)$ appartienne a Y, il faut et il suffit qu'il existe une homothétie $u \in \mathbf{Z}_\ell^*$, telle que $uy \in G_{\ell^\infty}$.

(On peut voir Y comme une espèce de "projection" de G_{ℓ^∞} sur le facteur $\mathbf{Sp}_{2n}$ du groupe $\mathbf{GSp}_{2n}$; ce n'est pas une vraie projection du fait que $\mathbf{GSp}_{2n}$ n'est pas le produit de $\mathbf{G}_m$ par $\mathbf{Sp}_{2n}$, mais il ne s'en faut pas de beaucoup : c'est vrai à un facteur 2 près, ce qui n'est pas gênant pour ce qu'on veut faire.)

Notons d'autre part U le groupe $G_{\ell^\infty} \cap \mathbf{Z}_\ell^*$, qui est d'indice $e(\ell)$ dans $\mathbf{Z}_\ell^*$. Notons que, si y appartient à Y, l'homothétie u correspondante est *bien déterminée* mod U. L'application $y \mapsto u$ définit donc un homomorphisme

$$\lambda : Y \longrightarrow \mathbf{Z}_\ell^*/U.$$

Cet homomorphisme est surjectif si ℓ est grand. En effet, on sait que l'homomorphisme composé $G_K \to \mathbf{GSp}_{2n}(\mathbf{Z}_\ell) \xrightarrow{N} \mathbf{Z}_\ell^*$ est égal au caractère cyclotomique, donc est surjectif. Ceci entraîne que, pour tout $u \in \mathbf{Z}_\ell^*$, il existe $x \in G_{\ell^\infty}$ tel que $N(x) = u^2$; si l'on pose $y = u^{-1}x$, on a $y \in Y$ et $\lambda(y) \equiv u \pmod U$, ce qui prouve la surjectivité de λ.

Il résulte de ceci que Y *a un quotient abélien d'ordre* $e(\ell)$.

Si je note Y^{ab} le plus grand quotient abélien de Y (qui est un groupe fini), je suis donc ramené à prouver ceci :

(1) *L'ordre de Y^{ab} est borné quand ℓ varie.*

C'est de cet énoncé qu'on va maintenant s'occuper.

La première chose à faire est de déterminer l'image Y_ℓ de Y par l'opération "réduction modulo ℓ". C'est évidemment un sous-groupe de $\mathbf{Sp}_{2n}(\mathbf{F}_\ell)$. On peut le caractériser ainsi :

(2) *Supposons $\ell \geq 3$. Pour qu'un élément z de $\mathbf{Sp}_{2n}(\mathbf{F}_\ell)$ appartienne à Y_ℓ, il faut et il suffit qu'il existe $v \in \mathbf{F}_\ell^*$ tel que $vz \in G_\ell$.*

Il est clair que tout élément de Y_ℓ a la propriété en question. Inversement, supposons que z et v soient comme dans (2). Puisque vz appartient à G_ℓ, je peux choisir un x dans G_{ℓ^∞} tel que l'on ait

$$\overline{x} = vz$$

(je conviens de noter $\overline{x}$ la réduction (mod ℓ) d'une matrice).

Si $w = N(x)$, on a $\overline{w} = N(vz) = v^2$, donc w est un carré (mod ℓ), donc w est un carré dans $\mathbf{Z}_\ell^*$. Je peux écrire $w = u^2$, avec $u \in \mathbf{Z}_\ell^*$, et je peux même choisir u de telle sorte que $\overline{u} = v$. L'élément $y = u^{-1}x$ appartient alors à Y, et il est clair que $\overline{y} = z$, cqfd.

(3) *Le groupe Y_ℓ contient G_ℓ^+*

Comme G_ℓ^+ est contenu dans $\mathbf{GSp}_{2n}(\mathbf{F}_\ell)$, et est engendré par les ℓ-éléments, il est contenu dans $\mathbf{Sp}_{2n}(\mathbf{F}_\ell)$. Le critère (2) s'applique alors avec $v = 1$.

Il faut maintenant prouver que Y_ℓ ne déborde pas trop de G_ℓ^+. Pour cela, on rappelle que G_ℓ est contenu (avec indice borné) dans $\mathbf{H}_\ell(\mathbf{F}_\ell)$, où $\mathbf{H}_\ell$ est un certain groupe réductif connexe qui a été défini dans les exposés antérieurs. Du fait que $\mathrm{End}\, A = \mathbf{Z}$, la composante neutre du centre de $\mathbf{H}_\ell$ est simplement le groupe $\mathbf{G}_m$ des homothéties. Le groupe dérivé $\mathbf{S}_\ell$ de $\mathbf{H}_\ell$ est un groupe semi-simple, contenu dans $\mathbf{Sp}_{2n/\mathbf{F}_\ell}$. Posons :

$$\mathbf{S}'_\ell = \mathbf{H}_\ell \cap \mathbf{Sp}_{2n/\mathbf{F}_\ell}.$$

(4) *L'indice de $\mathbf{S}_\ell$ dans $\mathbf{S}'_\ell$ est ≤ 2.*

Cela résulte de ce que $\mathbf{G}_m \cap \mathbf{Sp}_{2n/\mathbf{F}_\ell}$ est d'ordre 2.

Posons alors :

$$Y_\ell^0 = Y_\ell \cap \mathbf{S}_\ell(\mathbf{F}_\ell).$$

Comme Y_ℓ est évidemment contenu dans $\mathbf{S}'_\ell(\mathbf{F}_\ell)$, on déduit de (4) :

(5) *L'indice de Y_ℓ^0 dans Y_ℓ est ≤ 2.*

On a d'autre part :

$$G_\ell^+ \subset Y_\ell^0 \subset \mathbf{S}_\ell(\mathbf{F}_\ell),$$

et l'on sait aussi que, si ℓ est assez grand, G_ℓ^+ est égal à $\mathbf{S}_\ell(\mathbf{F}_\ell)^+$, image de $\widetilde{\mathbf{S}}_\ell(\mathbf{F}_\ell)$ dans $\mathbf{S}_\ell(\mathbf{F}_\ell)$. Pour de tels ℓ, l'indice de G_ℓ^+ dans $\mathbf{S}_\ell(\mathbf{F}_\ell)$ est donc majoré par l'ordre du groupe fondamental de $\mathbf{S}_\ell$, ordre que l'on peut majorer de façon uniforme (une borne grossière est $2n$, où $n = \dim A$). De ceci, et de (5), résulte :

(6) *L'indice de G_ℓ^+ dans Y_ℓ est borné* (quand ℓ varie).

Comme le groupe G_ℓ^+ est égal à son dérivé (pour ℓ grand), ceci entraîne :

(7) *L'ordre de Y_ℓ^{ab} est borné.*

Notons alors $Y(\ell)$ le noyau de la projection $Y \to Y_\ell$, i.e. l'ensemble des $y \in Y$ tels que $y \equiv 1$ (mod ℓ). C'est un pro-ℓ-groupe. Si je montre que son image dans Y^{ab} est triviale, cela prouvera que $Y^{ab} \to Y_\ell^{ab}$ est un isomorphisme, et (1) résultera de (7). Or l'image de $Y(\ell)$ dans Y^{ab} est un ℓ-groupe. En décomposant ce groupe en morceaux, je suis donc ramené à prouver l'énoncé suivant (pour ℓ assez grand) :

(8) *Il n'existe pas d'homomorphisme surjectif $f : Y(\ell) \to \mathbf{Z}/\ell\mathbf{Z}$ qui soit Y-invariant, i.e. tel que*

$$f(yzy^{-1}) = f(z) \quad \textit{si } y \in Y,\ z \in Y(\ell).$$

(Formulation équivalente : $Y(\ell)$ est contenu dans le groupe dérivé de Y.)

On va utiliser la *filtration* naturelle du groupe $Y(\ell)$. Si N est un entier ≥ 1, notons $Y(\ell^N)$ le sous-groupe de Y formé des éléments qui sont congrus à 1 (mod ℓ^N). On obtient ainsi

$$Y(\ell) \supset Y(\ell^2) \supset \ldots \supset Y(\ell^N) \supset \ldots.$$

Les quotients successifs $Y(\ell^N)/Y(\ell^{N+1})$ s'identifient à des $\mathbf{F}_\ell$ sous-espaces vectoriels $\mathbf{v}_N$ de l'algèbre de Lie $\mathfrak{sl}_{2n/\mathbf{F}_\ell}$ (et même de l'algèbre de Lie $\mathfrak{sp}_{2n/\mathbf{F}_\ell}$, mais $\mathfrak{sl}$ me suffit) ; l'identification se fait comme d'habitude : à un élément $y = 1 + \ell^N x$ de $Y(\ell^N)$, on associe la réduction (mod ℓ) de x. Cette identification est compatible avec l'action de Y par conjugaison ; bien entendu Y opère sur les $\mathbf{v}_N$ à travers l'homomorphisme $Y \to Y_\ell$ de réduction (mod ℓ).

Par un petit dévissage, on voit que (8) résultera de :

(9) *Il n'existe pas de sous-espace vectoriel $\mathbf{v}$ de $\mathfrak{sl}_{2n/\mathbf{F}_\ell}$ stable par Y_ℓ et muni d'une forme linéaire $f : \mathbf{v} \to \mathbf{Z}/\ell\mathbf{Z}$ surjective telle que*

$$f(yvy^{-1} = f(v) \quad \textit{si } v \in \mathbf{v} \textit{ et } y \in Y_\ell.$$

Comme Y_ℓ contient G_ℓ^+, il suffira de prouver ceci :

(10) *Si ℓ est assez grand, l'action de G_ℓ^+ par conjugaison sur $\mathfrak{sl}_{2n/\mathbf{F}_\ell}$ est semi-simple et ne contient pas la représentation unité.*

Comme l'action de G_ℓ^+ provient de celle de $\widetilde{S}_\ell(\mathbf{F}_\ell)$, on déduit (10) de :

(11) *L'action de $\widetilde{\mathbf{S}}_\ell$ sur $\mathfrak{sl}_{2n}$ par conjugaison est semi-simple, ℓ-restreinte, et ne contient pas la représentation unité* (ℓ grand).

C'est une pure question de groupes semi-simples. On a un groupe semi-simple qui agit sur un espace vectoriel par une représentation ℓ-restreinte absolument

irréductible (cette dernière propriété provenant de Faltings, qui nous donne le commutant de $\widetilde{\mathbf{S}}_\ell$). Il s'agit d'en déduire (11), si ℓ est assez grand par rapport à la dimension de la représentation. (Si la représentation est de degré $2n$, l'inégalité $\ell > 4n^2$ devrait suffire, mais peu importe.) Seule la semi-simplicité de l'action n'est
3 pas évidente. On la démontre par exemple en remontant en caractéristique 0, où elle est évidemment vraie, et en remarquant que, du coup, elle reste vraie pour ℓ assez grand.

Cela achève la démonstration dans le cas $\mathrm{End}\, A = \mathbf{Z}$, ouf !

2.2. *Démonstration du théorème dans le cas général*

On rappelle que L désigne le centre de $\mathbf{Q} \otimes \mathrm{End}\, A$. Le déterminant d'un L-automorphisme x (ou $\mathbf{Q}_\ell \otimes L$-automorphisme) est noté $N(x)$; même notation modulo ℓ. (Dans une rédaction détaillée, il me faudra être plus précis, et introduire l'ordre de L qui opère sur A, sa réduction (mod ℓ), etc. Je m'en dispense ici : ce genre d'ennuis ne concerne qu'un nombre fini de ℓ.)

La restriction de N à T_L est une isogénie (notée π dans le début du cours) ; en particulier, NC est un sous-tore de T_L.

On reprend pas à pas la démonstration du n° 2.1. La première chose à faire est de donner la définition de Y :

C'est l'ensemble des automorphismes y du module de Tate $T_\ell = A_{\ell^\infty}$ jouissant des deux propriétés suivantes :

(a) *il existe $u \in C(\mathbf{Z}_\ell)$ tel que $uy \in G_{\ell^\infty}$* ;

(b) *on a $N(y) = 1$.*

(Noter que (a) entraîne que y commute à $\mathbf{Q} \otimes \mathrm{End}\, A$, et en particulier à L ; cela permet de parler de $N(y)$.)

Si $U = C(\mathbf{Z}_\ell) \cap G_{\ell^\infty}$, on a comme précédemment un homomorphisme

$$\lambda : Y \longrightarrow C(\mathbf{Z}_\ell)/U.$$

De plus, cet homomorphisme est *presque surjectif*, i.e. son conoyau est d'ordre borné. En effet, la théorie abélienne (McGill !) montre que le sous-groupe de $C(\mathbf{Z}_\ell)$ formé des éléments du type $N(x)$, avec $x \in G_{\ell^\infty}$, est d'indice borné, et le résultat s'en déduit aussitôt. Imitant 2.1, on voit qu'on est ramené à prouver :

(1) *L'ordre de Y^{ab} est borné* (quand ℓ varie).

On reprend les mêmes arguments que dans 2.1. On prouve d'abord que la réduction Y_ℓ de Y (mod ℓ) est contenue (à un groupe d'ordre borné près) dans le groupe $\mathbf{S}(\mathbf{F}_\ell)$, et contient le groupe $\mathbf{S}(\mathbf{F}_\ell)^+$. D'où l'analogue de (7), i.e. le fait que Y_ℓ^{ab} est borné. Ceci fait, il reste à généraliser (9) et (10), ce qui se fait exactement de la même manière. On utilise le fait que les éléments de Y commutent à $\mathbf{Q} \otimes \mathrm{End}\, A$: donc les éléments des espaces vectoriels $\mathbf{v}_N$ commutent aussi à $\mathrm{End}\, A$. On est finalement ramené à montrer que l'action de $\mathbf{S}_\ell$ sur les $\mathbf{v}_N$ ne contient pas la représentation unité. Or, si $\mathbf{S}_\ell$ fixait un sous-espace $\mathbf{w} \neq 0$ de l'un des $\mathbf{v}_N$, celui-ci serait contenu dans $\mathbf{F}_\ell \otimes \mathrm{End}\, A$ (théorème de Faltings) ; mais, étant contenu dans un $\mathbf{v}_N$, il commuterait à $\mathbf{F}_\ell \otimes \mathrm{End}\, A$, i.e. il serait contenu dans le centre de $\mathbf{F}_\ell \otimes \mathrm{End}\, A$, que l'on a envie de noter L_ℓ. Mais Y est formé d'éléments de déterminant 1 ; donc $\mathbf{v}_N$ est formé d'éléments de trace 0 (relativement à L_ℓ), et tout élément de L_ℓ de trace 0 relativement à L_ℓ est réduit à 0. Contradiction.

(Je me rends bien compte du caractère incomplet de cette démonstration. Mais les détails manquants ne présentent pas de difficultés sérieuses : on a simplement besoin d'un peu de théorie abélienne, à la McGill.)