

COURS DE JEAN-PIERRE SERRE

JEAN-PIERRE SERRE

EVA BAYER (réd.)

Groupes linéaires modulo p et Points d'ordre fini des variétés abéliennes

Cours de Jean-Pierre Serre, tome 7 (1986)

http://www.numdam.org/item?id=CJPS_1986__7_

© Bibliothèque de l'IHP, 2015, tous droits réservés.

L'accès aux archives de la collection « Cours de Jean-Pierre Serre » implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Notes numérisées par l'IHP et diffusées par le programme
Numérisation de documents anciens mathématiques
<http://www.numdam.org/>

- 4 FEV. 2000

Groupes linéaires modulo p
et
Points d'ordre fini des variétés abéliennes

Jean - Pierre SERRE

Cours au Collège de France, janvier - mars 1986

notes de Eva BAYER

N° Cote : PB 929.9 al
Institut Henri Poincaré BIBLIOTHÈQUE 11, rue P.-et-M.-Curie 75231 PARIS CEDEX 05
N° Inventaire : 28658B

- 1771 -

Groupes linguistiques

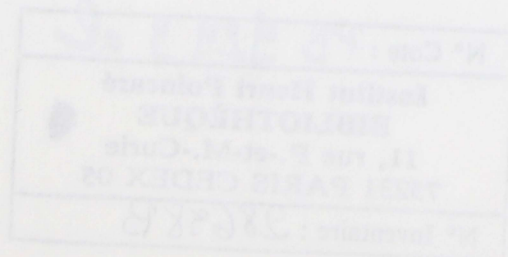
et

Point de vue de la syntaxe

Don - 1971

Centre de Recherches de France - janvier - mai 1971

Centre de Recherches



Annuaire du Collège de France

Résumé des cours de 1985-1986

I. SCIENCES MATHÉMATIQUES, PHYSIQUES ET NATURELLES

Algèbre et géométrie

M. Jean-Pierre SERRE, membre de l'Institut
(Académie des Sciences), professeur

Le cours a continué celui de l'année précédente, consacré aux représentations 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 $\mathbb{Q}$, de clôture algébrique $\bar{K}$; on note G_K le groupe de Galois $\text{Gal}(\bar{K}/K)$.

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 $\mathbb{Z}_\ell$ -module libre de rang $2n$. Le groupe G_K opère sur T_ℓ par une représentation

$$\rho_\ell : G_K \rightarrow \text{Aut}(T_\ell) \cong \text{GL}_{2n}(\mathbb{Z}_\ell).$$

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

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

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 $\rho : G_K \rightarrow \prod_\ell G_{K,\ell}$ 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 Z_ℓ^* des homothéties. Notons $c(\ell)$ l'indice de $Z_\ell^* \cap G_{K,\ell}$ dans Z_ℓ^* . 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 $c \geq 1$ tel que le groupe $\rho(G_K)$ contienne toutes les homothéties de $\hat{Z}^* = \prod_\ell Z_\ell^*$ qui sont des puissances c -ièmes.*

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

pour tout entier $m \geq 1$, il existe $s_m \in G_K$ tel que $s_m(x) = m^c x$ pour tout $x \in A(\bar{K})$ 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 $\mathrm{GSp}(T_\ell, e_\ell)$ des similitudes symplectiques de T_ℓ relativement à e_ℓ .

THÉOREME 3 - Faisons les hypothèses suivantes :

- (i) L'anneau $\text{End}(A)$ des $\bar{K}$ -endomorphismes de A est réduit à $\mathbb{Z}$;
- (ii) La dimension n de A est impaire, ou égale à 2, ou à 6.

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

Pour $n = 1$, cela revient à dire que $\rho(G_K)$ est ouvert dans le produit des $\text{GL}(T_\ell)$: 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 $A(\bar{K})$, le sous-groupe de torsion de $A(\bar{K})$. Si $x \in A(\bar{K})$, posons :

$N(x)$ = ordre de x ;

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

THÉOREME 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 :

$$d(x) \geq C(\epsilon, A, K) \cdot N(x)^{2-\epsilon} \quad \text{pour tout } x \in A(\bar{K})_r$$

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 $\text{GL}(T_\ell/\ell T_\ell) \cong \text{GL}_{2n}(\mathbb{F}_\ell)$ 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 GL_{2n} , défini sur $\mathbb{F}_\ell$, qui jouit des propriétés suivantes :

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

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 $\mathbb{Q}$. Ce tore contient le groupe G_m des homothéties.

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

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 $(G_\ell^{\mathrm{alg}})^\circ$ 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 $\mathrm{GL}_N(\mathbb{F}_\ell)$:

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

Si k est un corps, tout sous-groupe fini de $\mathrm{GL}_N(k)$, d'ordre premier à la caractéristique de k , contient un sous-groupe abélien d'indice $\leq c_1(N)$, où $c_1(N)$ ne dépend que de N . C'est là un théorème classique de C. Jordan (du moins lorsque $k = \mathbb{C}$, cas auquel on se ramène sans difficulté). On a reproduit la démonstration qu'en avait donnée FROBENIUS en 1911 (*Ges. Abh.*, III, n° 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 $\mathrm{GL}_N(\mathbb{F}_\ell)$ engendrés par leurs éléments d'ordre ℓ

Supposons $\ell \geq N$. Soit G un sous-groupe de $\mathrm{GL}_N(\mathbb{F}_\ell)$, 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 GL_N , défini sur $\mathbb{F}_\ell$, et isomorphe au groupe additif G_a . Soit G^{alg} le sous-groupe algébrique de GL_N engendré par les $G_a(x)$, pour $x \in G_u$. Le groupe $G^{\mathrm{alg}}(\mathbb{F}_\ell)$ des $\mathbb{F}_\ell$ -points de G^{alg} contient évidemment G^+ ; d'après un théorème de V. Nori, on a :

$$G^+ = G^{\mathrm{alg}}(\mathbb{F}_\ell)^+ \quad \text{si } \ell \geq c_2(N)$$

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 $G_K(\ell)^{\text{alg}}$. D'autre part, la théorie abélienne permet de définir un certain sous-tore de GL_N qui commute à $G_K(\ell)^{\text{alg}}$; le groupe réductif connexe H_ℓ engendré par ce tore et par $G_K(\ell)^{\text{alg}}$ 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.

Groupes linéaires modulo p

et

Points d'ordre fini des variétés abéliennes

Jean - Pierre SERRE

Cours au Collège de France, janvier - mars 1986

notes de Eva BAYER

Table des Matières

Résumé du Cours p. 1

1^{ère} Partie - Sous-groupes de $GL_n(\mathbb{F}_p)$... p. 5

Théorème de Jordan ... p. 5

Inertie modérée (rigidité de Raynaud) ... p. 20

Caractérisation des variétés abéliennes de type CM ... p. 28

Sous-groupes de $GL_n(\mathbb{F}_p)$ engendrés

par des f -éléments - - - p. 37

Variante du théorème de Bézout ... p. 44

Semi-simplicité et nullité de H^1 ... p. 63

Références ... p. 70

2^{ème} Partie - Variétés abéliennes ... p. 71

Tors de Hodge ... p. 81

Orbites - - - p. 84

Le produit des G_2 ... p. 86

Le produit des $G_{2^{\infty}}$... p. 89

Egalité des rangs - - - p. 100

Le cas $\text{End } A = \mathbb{Z}$ et le groupe $GS\mathbb{P}_{2n}$... p. 103

Compléments ... p. 109

1^{ère} partie

- $G \subset GL_n(\mathbb{F}_p)$, n fixe, p variable $\rightarrow \infty$
- $GL_n(\mathbb{F}_p)$ contient:
- sous-groupes abéliens
 - sous-groupes indépendants de p (provenant de $GL_n(\mathbb{Z})$: ce sont les plus difficiles à classer)
 - sous-groupes "algébriques" $SL_n(\mathbb{F}_p)$, $Sp_n(\mathbb{F}_p)$

Thm "de Jordan" (1878)

G sous-groupe de $GL_n(\mathbb{K})$, $\mathbb{K}$ corps.

Si l'ordre de G est premier à $p = \text{car}(\mathbb{K})$, alors G contient un sous-groupe abélien normal A tel que $|G/A| \leq c(n)$, où $c(n)$ dépend seulement de n .

(e.g. $c(2) = 60$)

Thm (Nori; versions plus faibles de Matthews, Vaserstein, Weisfeiler)

G engendré par ses éléments d'ordre p
(engendré par ses p -Sylow : équiv.)

Alors, il existe $c_2(n)$ tel que si $p > c_2(n)$, on a $[G^{\text{alg}}(\mathbb{F}_p) : G] \leq c_3(n)$

G^{alg} : sous-groupe algébrique engendré par g^t , $g \in G$ d'ordre p , t indéterminée
($g = 1 + u$, $u^p = 0$, $g^t = 1 + tu + \binom{t}{2} u^2 + \dots$)

$G \subset G^{\text{alg}}$, $G = G^{\text{alg}}(\mathbb{F}_p)^+$: sous-groupe engendré par les p -éléments.

2

Le théorème de Nori a d'autres applications que celles données dans ce cours :

① Il existe $c_3(n)$ tel que si $p > c_3(n)$ et si $G \subset GL(V)$, V ev. $/\mathbb{F}_p$ de dim n , action de G sur V semi-simple, alors $H^1(G, V) = 0$.

② Soit Γ un sous-groupe de $SL_n(\mathbb{Z})$, Γ Zariski-dense dans SL_n . Alors, l'adhérence de Γ dans $SL_n(\hat{\mathbb{Z}})$ est ouverte. En particulier, $\Gamma \rightarrow SL_n(\mathbb{Z}/p\mathbb{Z})$ est surjectif pour presque tout p .

2^{ème} partie du cours.

Groupes de Galois des points d'ordre fini de variétés abéliennes.

A variété abélienne, $\dim A = n \geq 1$.

K corps de nombres (corps de fct, corps fini)

A défini sur K . Soit m entier ≥ 1 , et

A_m : points de division par m , i.e.

$A_m = \text{Ker}(m: A(\bar{K}) \rightarrow A(\bar{K}))$, où

$\bar{K}$: clôture algébrique de K .

$G_m = \text{image de } \text{Gal}(\bar{K}/K) \text{ dans } \text{Aut}(A_m) = GL_{2n}(\mathbb{Z}/m\mathbb{Z})$.

G_m est "gros", "presque égal au groupe des points d'un certain groupe algébrique"

- $m = l, l^2, \dots$ G_{l^∞} : "fait"
- G_l , l variable $\rightarrow$ on combine.

Résultats

Après extension finie de K , pour l assez grand, on définira un tore $T_l \subset GL_{2n} / \mathbb{F}_l$, et un groupe semi-simple $S_l \subset GL_{2n}$ qui commutent entre eux, $H_l = T_l \cdot S_l$ groupe réductif.

- ① $G_l \subset H_l(\mathbb{F}_l)$ avec indice borne' $\leq c(A, K)$ (indépendant de l).
 $G_l \supset S_l(\mathbb{F}_l)^+$
 image $(\tilde{S}_l(\mathbb{F}_l) \rightarrow S_l(\mathbb{F}_l))$
- ② T_l est indépendant de l
 (le même que le tore l -adique de G_{pro})
 $T_l \subset [\text{centre}(\text{End}(A) \otimes \mathbb{F}_l)]^*$
- ③ rang S_l indépendant de l (et égal au rang l -adique).

Cas particulier:

Si $\text{End}_{\mathbb{F}} A = \mathbb{Z}$, et si $\dim A$ est impair, ou 2, ou 6, alors
 $T = G_m$, $S_l = Sp_{2n}$, $H_l = CSp_{2n}$
 (similitudes symplectiques) ($= GSp_{2n}$ not. standard)
 et $G_l = H_l(\mathbb{F}_l)$ si l est grand.

$\Rightarrow$ Image de $\text{Gal}(\bar{K}/K)$ dans

$\prod_l CSp_{2n}(\mathbb{Q}_l)$ est ouverte pour la topologie adélique.

Si la polarisation est de degré 1, ouverte dans

$$\prod_e \text{CS}_{p_{2n}}(\mathbb{Z}_e).$$

Thm:

Il y a équivalence entre:

① $S_e = 1$ pour une infinité de l

② $|G_e|$ est premier à l pour une infinité de l

③ A est de type CM.

Faltings: Commutant de H_e dans $\text{End}(A_e)$
est $\text{End}(A) \otimes \mathbb{F}_e$ (l grand)

Si x est un point d'ordre l premier,
l'ordre de l'orbite de x dans $\text{Gal}(\bar{K}/K)$
est $\geq \text{cte. } l^2$ (si A ss facteur de
type CM).

Corollaire:

$$G_e \cap (\text{homothéties de } A_e) = G_e \cap G_m(\mathbb{F}_e)$$

$$G_m \hookrightarrow GL_{2n}$$

T_e contient G_m

Donc l'indice de $G_e \cap G_m(\mathbb{F}_e)$ dans $\mathbb{F}_e^*$
est borné (quand l varie)

Question: Est-ce que G_e contient $G_m(\mathbb{F}_e)$ pour
 l assez grand?

Pour tout $i \geq 1$, on a $H^i(G_e, A_e) = 0$ si $l \geq c(A, K, i)$
(ste spectrale) $H^i(G_e, \bigotimes_r A_e \bigotimes_s \hat{A}_e) = 0$ l gd, $r \neq s$.

1^{ère} partie : Sous-groupes de $GL_n(\mathbb{F}_p)$

① Le théorème de Jordan

Thm :

$G \subset GL_n(\mathbb{C})$, G fini :

Il existe $A \subset G$ abélien normal
tel que $[G:A] \leq c(n)$, où $c(n)$
ne dépend que de n .

("normal" n'est pas sérieux : $A' \subset G$
 $[G:A'] \leq c'(n)$, A' abélien

$A = \bigcap g A' g^{-1}$, g él. de G opérant
trivialement sur G/A'

$[G:A] \leq c'(n)!$, A abélien normal.)

Le théorème s'étend à tout corps k ,
 $|G|$ non divisible par $\text{car}(k)$:

a.) Si $\text{car}(k)=0$, on peut supposer k
de type fini sur $\mathbb{Q}$, donc plongable
dans $\mathbb{C}$.

b.) Si $\text{car}(k)=p$, on peut le supposer
parfait, k corps résiduel de
 $\Lambda = W(k)$: anneau de valuation discrète
complet, de corps résiduel k .

$$G \subset GL_n(k)$$



réd. mod p

$$GL_n(\Lambda)$$

G peut se remonter dans $GL_n(\Lambda)$ 6

$k = \Lambda/p\Lambda$, on remonte dans $\Lambda/p^2\Lambda$

$$0 \rightarrow M_n(k) \rightarrow GL_n(\Lambda/p^2\Lambda) \rightarrow GL_n(\Lambda/p\Lambda) \rightarrow 0$$

obstruction dans $H^2(G, M_n(k)) = 0$.

Comme le corps des fractions de Λ est de car. 0, on applique a.).

Reformulation:

Pour chaque n , il n'y a qu'un nombre fini ($\bar{a}$ conj. près) de sous-groupes finis de $PGL_n(\mathbb{C})$ qui sont irréductibles et primitifs.

$\tilde{G}$: image réciproque de G dans $SL_n(\mathbb{C})$
repr. de $\tilde{G}$ dans $\mathbb{C}$ n'est pas
l'induite d'une représentation de $d' < n$.

Jordan usuel $\Rightarrow$ reformulation:

Soit G un tel groupe, $\tilde{G}$ comme ci-dessus.

Par Jordan, $\exists A \subset \tilde{G}$ abélien normal,
 $[\tilde{G} : A] \leq c(n)$.

On décompose $\mathbb{C}^n$ en sous-espaces propres pour A , et $\tilde{G}$ les permute transitivement
 $\Rightarrow$ un seul tel sous-espace propre
 $\Leftrightarrow A \subset$ homothéties.

$$\tilde{G}/A \twoheadrightarrow G \Rightarrow |G| \leq c(n).$$

"Jordan constructif":

Liste des sous-groupes irréductibles primitifs de $\text{PGL}_n(\mathbb{C})$

$n = 1$

1

$n = 2$

A_4, S_4, A_5

$c(2) = 60$

. . .

$n = 7$ voir Feit, Congrès de Nice 1970.

Meilleur $c(n)$ connu donné par Weisfeiler, en utilisant la classification des groupes finis simples.

Sous-groupes primitifs irréductibles de PGL_n sont en nombre fini.

Thm Feit-Thompson: Si p divise l'ordre d'un tel groupe, alors $p \leq 2n+1$.
($G_{168} \subset \text{PGL}_3$: borne optimale).

1^{ère} démonstration

(Zassenhaus, Kazdan-Margulis).

Thm:

G groupe de Lie réel, il existe un
voisinage U de l'élément neutre tel que
pour tout sous-groupe discret Γ de
 G , le sous-groupe de Γ engendré
par $\Gamma \cap U$ est nilpotent.

(Forme plus forte: Raghunathan, Discrete Subgroups ...)

(Même énoncé excepté que $\Gamma \cap U$ est contenu dans $\exp(\mathfrak{z})$, où $\mathfrak{z} \in \text{Lie } G$, $\mathfrak{z}$ nilpotente.

Démonstration:

$$(x, y) \longmapsto [x, y] = x y x^{-1} y^{-1}$$

$G \times G \longrightarrow G$ au voisinage de l'élément neutre.

x_i, y_i

coord. centrées
à l'origine

$$(x, y)_j = \sum \alpha_{\alpha} \beta_{\beta} x^{\alpha} y^{\beta}$$

α, β multiindices

$$|\alpha| \geq 1, |\beta| \geq 1$$

$$|x| = \sup |x_i|$$

$$|[x, y]| \leq c |x| \cdot |y| \quad \text{avec } c \text{ convenable.}$$

Quitte à changer de coordonnées, on peut supposer que $|[x, y]| \leq |x| \cdot |y|$ dans un voisinage U convenable, U relativement compact, $|x| \leq 1$ dans U .

$$\Gamma \cap U \quad \text{fini} \quad = \quad 1 = \gamma_0, \gamma_1, \dots, \gamma_N$$

$$|\gamma_i| \leq |\gamma_j| \quad \text{si } i < j$$

$$[\gamma_i, \gamma_j] = \gamma_{k(i,j)} \quad i, j \geq 1.$$

Γ_i sous-groupe engendré par $\{1, \dots, \gamma_i\}$
opère trivialement sur Γ_j / Γ_{j-1}

$\Rightarrow$ le groupe engendré par $\Gamma \cap U$ est nilpotent.

Il suffit de démontrer le thm de Jordan avec $GL_n(\mathbb{C})$ remplacé par $U_n(\mathbb{C})$, groupe unitaire.

On applique à $U_n(\mathbb{C})$ le thm précédent, V v.g. de 1, tel que si $G \subset U_n(\mathbb{C})$ fini, le sous-groupe H engendré par $V \cap G$ est nilpotent.

$$[G : H] \leq \text{vol}(U_n(\mathbb{C})) / \text{vol}(W),$$

où $W \cdot W \subset V$, W symétrique, car si $g \in G$, $g' \in G$ sont des repr. distincts mod H , alors $gW \cap g'W = \emptyset$.

$N \subset G$ d'indice $\leq c_1(n)$, N nilpotent

Thm (Blichfeld)

Tout sous-groupe nilpotent de $GL_n(\mathbb{C})$ est "monomial" : l'espace est somme directe de droites stables (permutées) par le groupe
 $\Leftrightarrow$ il existe dans le groupe unitaire un tore normalisé par le groupe.

$$[N : \underbrace{N \cap T}_{\text{abélien}}] \leq n!$$

2^{ème} démonstration du thm de Jordan

Frobenius (1911) Vol 3, inspirée par Bieberbach (1911), voir aussi Schur (1911).

$E = \mathbb{C}^n$ métrique usuelle

espace de Hilbert / $\mathbb{C}$ de dim finie $= n$.

A opérateur, $A \in \text{End}(E)$, A^* son adjoint. On pose :

$$n(A) = \text{Tr}(AA^*) = \sum |a_{ij}|^2$$

$$(a_{ij}) : \text{matrice de } A \text{ p.r. base orthonormale } e_i \\ = \sum_{i=1}^n \|A e_i\|^2$$

Si A est normal (i.e. $AA^* = A^*A$),

on peut choisir e_i : vecteurs propres de A
valeurs propres a_i , alors

$$n(A) = \sum |a_i|^2.$$

On a $n(UA) = n(AU) = n(A)$ si U est unitaire

A normal de valeurs propres a_i ,

$$\sup_{i < j} |a_i - a_j|^2 \leq 2n(A)$$

$$i < j \quad |a_i - a_j|^2 \leq 2|a_i|^2 + 2|a_j|^2 \leq 2n(A)$$

B un autre opérateur

$$n(AB - BA) \leq \sup_{i < j} |a_i - a_j|^2 n(B)$$

$$\parallel \leq 2n(A)n(B)$$

$$\sum |(a_i - a_j)b_{ij}|^2$$

Si U et V unitaires,

$$n(1 - UVU^{-1}V^{-1}) \leq 2n(1-U)n(1-V) :$$

$$\begin{aligned} n(VU - UV) &= n(-(1-U)(1-V) + (1-V)(1-U)) \\ &\leq 2n(1-U)n(1-V) \end{aligned}$$

Lemme:

Soient U et V unitaires, avec

$$C = UVU^{-1}V^{-1}.$$

On suppose

① U et C commutent

② $n(1-V) < 4$

Alors $C = 1$.

① $\iff$ ①' : U et VUV^{-1} commutent.

Supposons $U \neq VUV^{-1}$, et montrons

$$n(1-V) \geq 4.$$

Exemple: $U = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, $V = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

$$VUV^{-1} = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$n(1-V) = n \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} = 4.$$

Soit Λ = Spectre de U (= celui de VUV^{-1})

$$E_{\lambda, \mu} = \{x \text{ t.q. } Ux = \lambda x, VUV^{-1}x = \mu x\}$$

$$E = \bigoplus_{\substack{\text{orth} \\ (\lambda, \mu) \\ \lambda, \mu \in \Lambda}} E_{\lambda, \mu}$$

Il y a au moins 2 couples (λ, μ) , $\lambda \neq \mu$, tels que $E_{\lambda, \mu} \neq 0$.

Il y a au moins un tel couple. S'il n'y en avait qu'un, la multiplicité de λ ne serait pas la même dans U et dans VUV^{-1} : celle de λ dans U serait égale à celle de VUV^{-1} augmentée de $\dim E_{\lambda, \mu}$.

Soient $(\lambda_1, \mu_1), (\lambda_2, \mu_2)$ deux tels couples.

Choisissons e_1 unitaire $\in E_{\lambda_1, \mu_1}$

e_2 " E_{λ_2, μ_2}

e_1 vecteur propre de U pour λ_1

Ve_1 VUV^{-1} λ_1

$$\Rightarrow Ve_1 \in \bigoplus E_{\nu, \lambda_1} \perp E_{\lambda_1, \mu_1}$$

donc $Ve_1 \perp e_1$, $Ve_2 \perp e_2$

$$\begin{aligned} n(1-V) &\geq \|(1-V)e_1\|^2 + \|(1-V)e_2\|^2 \\ &\geq 2+2 = 4. \end{aligned}$$

Lemme:

Si G fini $\subset U_n(\mathbb{C})$, si $U, V \in G$

tels que $n(1-U) < \frac{1}{2}$, $n(1-V) < 4$,

alors U et V commutent.

On en déduit que le sous-groupe engendré par les U t.q. $n(1-U) < \frac{1}{2}$ est commutatif et normal, et on verra que son indice est

$$\leq c(n) = (\sqrt{8n} + 1)^{2n^2} + (\sqrt{8n} - 1)^{2n^2}$$

Démonstration du thm de Jordan :

Si n entier ≥ 1 , $\exists c(n)$ t.q. si $G \subset GL_n(k)$
 G fini, k corps, ordre de G premier à $\text{car}(k)$,
 alors G contient un sous-groupe abélien
 normal d'indice $\leq c(n)$.

Il suffit de le prouver pour $k = \mathbb{C}$,
 la même constante vaut pour tout k .

Preuve de Bieberbach - Frobenius,

$$G \subset U_n(\mathbb{C}), \quad n(A) = \text{Tr}(AA^*) = \sum |a_{ij}|^2.$$

On a montré ① et ② :

$$\textcircled{1} \quad \text{Si } U, V \text{ unitaires, } n(1 - UVU^{-1}V^{-1}) \leq 2n(1 - U)n(1 - V).$$

$$\textcircled{2} \quad \text{Si } A, B \text{ unitaires, } C = ABA^{-1}B^{-1} \\ \text{si } A \text{ et } B \text{ commutent et si} \\ n(1 - B) < 4, \text{ alors } C = 1.$$

$$\textcircled{3} \quad \text{Si } A, B \in G, \quad G \text{ sous-groupe fini} \\ \text{de } U_n(\mathbb{C}), \text{ et si } n(1 - A) < \frac{1}{2} \\ \text{et } n(1 - B) < 4, \text{ alors } A \text{ et } B \\ \text{commutent.}$$

Démonstration de ③ :

$$\text{Soit } k = 2n(1 - A), \quad k < 1, \quad C_0 = B \\ C_1 = ABA^{-1}B^{-1}, \quad C_2 = AC_1A^{-1}C_1^{-1}, \dots, \\ C_m = AC_{m-1}A^{-1}C_{m-1}^{-1}, \dots$$

$$n(1 - B) < 4, \quad n(1 - C_1) < 4k, \dots$$

$$n(1 - C_m) < 4k^m, \text{ d'où } n(1 - C_m) \rightarrow 0,$$

$$\text{donc } C_m = 1 \text{ pour un } m.$$

On applique (2) à A et C_{n-2} ; le C correspondant est C_{n-1} . Le fait que $C_n = 1$ signifie que A et C_{n-1} commutent.

On a $n(1 - C_{n-2}) < 4$, donc $C_{n-1} = 1$.

On continue : $C_1 = 1$.

(4) Soit A le sous-groupe de G engendré par les $u \in G$ tels que $n(1-u) < \frac{1}{2}$.

Alors A est abélien et normal dans G .

(5) On a $[G:A] \leq (\sqrt{8n} + 1)^{2n^2} - (\sqrt{8n} - 1)^{2n^2}$.

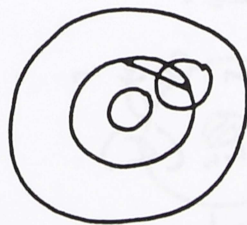
Soient $P_1, \dots, P_N$ des représentants des classes de G/A .

$$n(P_i - P_j) \geq \frac{1}{2} \quad \text{si } i \neq j$$

"

$$n(1 - P_i^{-1} P_j)$$

$$\begin{array}{c} P_1 \quad \quad P_2 \\ \hline \geq \frac{1}{2} \end{array}$$



$$n(U) = n(1) = n$$

grand rayon : $R = \sqrt{n} + \frac{1}{2\sqrt{2}}$

$$r = \sqrt{n} - \frac{1}{2\sqrt{2}}$$

Volume couronne : $S_n (R^{2n^2} - r^{2n^2})$

Vol. boule de rayon $\frac{1}{2\sqrt{2}}$:

$$S_n \left(\frac{1}{2\sqrt{2}} \right)^{n^2}$$

$$N \leq \frac{\left(\sqrt{n} + \frac{1}{2\sqrt{2}}\right)^{2n^2} - \left(\sqrt{n} - \frac{1}{2\sqrt{2}}\right)^{2n^2}}{\left(\frac{1}{2\sqrt{2}}\right)^{2n^2}}$$

$$N \leq (\sqrt{8n} + 1)^{2n^2} - (\sqrt{8n} - 1)^{2n^2}.$$

$c(n)$ = plus petit entier $N \geq 1$ tel que tout sous-groupe fini de $GL_n(\mathbb{C})$ contient un sous-groupe abélien normal d'indice $\leq N$.

e.g. $c(1)=1$, $c(2)=60$, ... $c(7)$ connu.

$$\log c(n) \ll n^2 \log n$$

Blichfeldt : $\log c(n) \ll n^2 / \log n$

Weisfeiler (preprint) en utilisant la classification des groupes finis simples:

$$\log c(n) \ll n \log n$$

optimal: $S_n \subset GL_n(\mathbb{C})$.

$$c(n) \leq n! n^{a \log n + b} \quad a, b \text{ const. univ.}$$

(il ne donne pas la valeur de a, b , qui doivent être difficiles à déterminer).

Compléments

α_i : valeurs propres de A unitaire

$$n(1-A) = \sum |1-\alpha_i|^2$$



$\text{amp}(A)$ = longueur du plus petit arc de cercle contenant toutes les valeurs propres de A .

$$A, B \text{ unitaires, } \operatorname{amp}(A) \leq \delta_A$$

$$\operatorname{amp}(B) \leq \delta_B$$

$$\text{Alors, } \operatorname{amp}(AB) \leq \delta_A + \delta_B$$

$$A, B \text{ unitaires, } \operatorname{amp}(A) \leq \delta < \pi$$

$$\text{alors } \operatorname{amp}(ABA^{-1}B^{-1}) \leq 2\delta_A$$

$$A, B \text{ unitaires, } \operatorname{amp}(A) = \delta < \frac{\pi}{3},$$

$$\chi(1 - ABA^{-1}B^{-1}) < k \chi(1 - B)$$

$$\text{où } k = 4 \sin^2 \frac{\delta}{2} < 1$$

$$\left(\sup |a_i - a_j| : \right)$$



$$A, B \text{ unitaires, } A \text{ commute à } ABA^{-1}B^{-1} \neq 1,$$

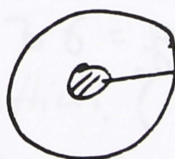
$$\text{alors } \operatorname{amp}(B) \geq \pi$$

(i.e. $0 \in \text{env. convexe du spectre de } B$).

$$\text{Si } A, B \in G \text{ fini, } \operatorname{amp}(A) < \frac{\pi}{3}, \operatorname{amp}(B) < \pi,$$

$$\text{alors } A \text{ et } B \text{ commutent.}$$

(même démo,



$$\operatorname{amp}() \leq \pi/6$$

$$c(n) \leq \frac{\operatorname{vol} U_n}{\operatorname{vol} \text{ boule}}$$

Variante du thm de Jordan

(se démontre en se ramenant à Jordan)

$$G \text{ fini} \subset GL_n(k), \quad \operatorname{car}(k) = p > 0$$

Soit G^+ le s/g de G engendré par les p -Sylow de G

Thm:

Il existe dans G/G^+ un sous-groupe abélien normal d'indice $\leq c(n)$.

Lemme:

Il existe un s/g H de G d'ordre premier $\bar{a} \ p$, tel que $H \twoheadrightarrow G/G^+$.

Démonstration du Lemme:

Soit P un p sous-groupe de Sylow de G .
On a $P \subset G^+$. Soit $N = N_G(P)$ le normalisateur de P dans G . Alors $N \rightarrow G/G^+$ est surjectif.

Soit $g \in G$, gPg^{-1} est un p -Sylow de G^+ , donc de la forme $\gamma P \gamma^{-1}$, $\gamma \in G^+$.

$$gPg^{-1} = \gamma P \gamma^{-1} \iff \gamma^{-1}g \in N.$$

$\delta = \gamma^{-1}g$, on a $g = \delta \gamma$ avec $\gamma \in G^+$, $\delta \in N$ (lemme de Frattini).

$$\text{On a } 1 \longrightarrow \underbrace{P}_{p\text{-groupe}} \longrightarrow N \longrightarrow \underbrace{N/P}_{\substack{\text{d'ordre premier} \\ \bar{a} \ p}} \longrightarrow 1$$

se scinde.

On peut écrire $N = PH$ avec $H \cong N/P$ d'ordre premier $\bar{a} \ p$.

Comme $P \rightarrow G/G^+$ est trivial, on a $H \twoheadrightarrow G/G^+$.

Le lemme entraîne le thm.

(Tits : variante de Brauer et Feit.

n, α exp. de p dans l'ordre de $G = \alpha$.
 Il existe A d'indice $c(n, \alpha) = c(n, \alpha, p)$
 Utilise Jordan)

Autre variante de Jordan: $/\mathbb{Q}$

Soit L un s/g alg. de $GL_n / \mathbb{Q}$

Soit L^0 sa composante neutre.

Alors le g. fini L/L^0 possède un s/g. abélien normal d'indice $\leq c(n)$.

Contient Jordan, mais sa démonstration utilise Jordan.

Thm:

Il existe un s/g fini H de L tel que

$H \rightarrow L/L^0$ soit surjectif

(Borel - Serre CMH 64, 1964)

Lemme "à la Frattini" :

Si C est un s/g de Cartan de L^0 et

N son normalisateur dans L , alors $N \twoheadrightarrow L/L^0$.

$g \in L$, $g C g^{-1}$ Cartan de L^0

"
 $\gamma C \gamma^{-1}$ $\gamma \in L^0$ etc.

$N^0 = C$ $N/N^0 \twoheadrightarrow L/L^0$

N^0 nilpotent, on se ramène au cas commutatif.

(marche sur un corps alg. clos quelconque)

Ordre de H divisible par les mêmes nombres

premiers que L/L^0 .

Supposons $L^0 = T$ tore, $G = L/L^0$

$$1 \rightarrow T \rightarrow L \rightarrow G \rightarrow 1$$

$d = |G|$, $u \in H^2(G, T)$ corr. à L , $du = 0$.

$$1 \rightarrow T_d \rightarrow T \xrightarrow{d} T \rightarrow 1$$

$$H^2(G, T_d) \rightarrow H^2(G, T) \xrightarrow{d} H^2(G, T)$$

$$\begin{array}{ccc} \cup & & \cup \\ \downarrow & \longrightarrow & \downarrow \\ \cup & & \cup \end{array} \longrightarrow 0$$

$$1 \rightarrow T_d \rightarrow H \rightarrow G \rightarrow 1$$

$$\begin{array}{ccccc} & \downarrow & & \downarrow & \\ 1 \rightarrow & T & \rightarrow & L & \rightarrow G \rightarrow 1 \end{array}$$

$(Q$ ne peut pas borner $|H|)$

Marche aussi sur un corps non alg. clos:

e.g. k parfait, L/L^0 k -groupe fin:

on veut relever en H fin: stable par Galois:

c'est possible.

(2) Inertie modérée (rigidité de Raynaud)

K corps local, car. résiduelle $p > 0$.

k : corps résiduel, suppose' parfait
(fini dans toutes les applications)

$\bar{K}$: clôture alg. de K

$\bar{k}$: corps résiduel de $\bar{K}$.

$$1 \longrightarrow \underbrace{I}_{\text{g. d'inertie}} \longrightarrow \text{Gal}(\bar{K}/K) \longrightarrow \text{Gal}(\bar{k}/k) \longrightarrow 1$$

I_w : plus gd pro- p s/g de I
inertie "sauvage"

$I/I_w = I_t$: g. d'inertie modérée,
d'ordre premier à p

($I = I_w \cdot I_t$ semi-direct, non canonique)

Structure de I_t

$$I_t = \varprojlim_{\substack{n \\ (n,p)=1}} \mu_n(\bar{k})$$

$\mu_n(\bar{k})$: gp. des racines n ièmes de 1 ds $\bar{k}$

π : uniformisante

K'/K finie, galoisienne, $G(K'/K)$

On a $I(K'/K) \rightarrow \mu_n$, définie ainsi:

Si π' : unif. de K' , $s \in I$

$s\pi'/\pi'$ entier de K'

$\equiv$ racine de 1 mod π'

cette racine de 1 est indép. du choix de π' .

q puissance de p , $\mathbb{F}_q \subset \bar{\mathbb{K}}$

$$n = q - 1, \quad \mu_n(\bar{\mathbb{K}}) = \mathbb{F}_q^*$$

$$I_t = \varprojlim_{p^n} \mathbb{F}_{p^n}^*$$

homomorphisme de transition: normes.

Soit $\rho: \text{Gal}(\bar{\mathbb{K}}/\mathbb{K}) \rightarrow \text{GL}(V)$

V : ev. sur $\bar{\mathbb{K}}$

repr. continue à image finie

Soit $\rho|_I$ sa restriction à I .

I_w pro- p -gp, agit par matrices unipotentes, trivialement sur les facteurs simples, d'où il existe une suite de composition de V (p.r. $\rho|_I$) telle que I_w opère trivialement sur les facteurs simples.

Si $\rho|_I$ est semi-simple, alors I_w opère trivialement.

D'où une repr. $\rho|_{I_t}: I_t \rightarrow \text{GL}(V)$.

C'est une somme directe de repr. de degré 1 donnée par les caractères

$$\chi_\alpha: I_t \rightarrow \bar{\mathbb{K}}^*$$

associés à la représentation.

$$\chi: \mathbb{F}_{p^m}^\times \longrightarrow \overline{\mathbb{K}}^\times$$

On a $\chi(x) = x^{i(\chi)}$

où $i(\chi) \in \mathbb{Z}/(p^m-1)\mathbb{Z}$

$$i(\chi) = i_0 + i_1 p + \dots + i_{m-1} p^{m-1}$$

avec $0 \leq i_j \leq p-1$

et $(i_0, \dots, i_{m-1}) \neq (p-1, \dots, p-1)$.

$$\mathbb{F}_{p^m} \longrightarrow \overline{\mathbb{K}}$$

$$x \longmapsto x \quad (1, 0, \dots, 0)$$

$$x \longmapsto x^p \quad (0, 1, \dots, 0)$$

...

$$x \longmapsto x^{p^{m-1}} \quad (0, \dots, 1)$$

$$\text{amp}(\chi) = \sup(i_0, \dots, i_{m-1}) \geq 0$$

$$\leq p-1.$$

$$\mathbb{F}_{p^2}^\times \xrightarrow{\text{norme}} \mathbb{F}_p^\times \xrightarrow{\chi} \overline{\mathbb{K}}^\times$$

$$x \longmapsto x^i$$

$$x \longmapsto x^{p+1} \longmapsto x^{i+p^i}$$

$$(i, i), \quad \text{amp} = i$$

Théorème de rigidité'

Supposons ρ triviale sur I_w , et supposons que tous les caractères de I_t définis par ρ soient d'amplitude $\leq \delta$, où δ est un entier $< p-1$.

(on dit ^{alors} que ρ est une représentation d'amplitude $\leq \delta$)

Soit $A \in GL(V)$. Supposons que les $s \in I_t$ tels que $\rho(s)$ commute à A forment un s/g d'indice $< \frac{p-1}{\delta}$ dans I_t .

Alors les $\rho(s)$, $s \in I_t$, commutent à A .

Même énoncé' avec "commute à A " remplacé par "fixe un vecteur donné de V ".

Démonstration:

On se ramène à une représentation

$\rho: \mathbb{F}_{p^n}^\times \rightarrow GL(V)$ dont tous les caractères sont d'amplitude $\leq \delta$.

Mise sous forme diagonale, elle fait intervenir des caractères $\chi_1, \dots, \chi_d$
 $d = \dim(V)$.

Si $(a_{ij}) =$ matrice de A

$s \in \mathbb{F}_{p^n}^\times$, $\rho(s)$ commute à A

$$a_{ij}(\chi_i(s) - \chi_j(s)) = 0$$

1^{er} cas:

pour tout i, j t.q. $a_{ij} \neq 0$, on a

$\chi_i = \chi_j$. Alors tous les $\rho(s)$ commutent à A .

Il existe i, j avec $a_{ij} \neq 0$, $\chi_i \neq \chi_j$.

Alors l'ensemble des s t.q. $p(s)$ commute à A est contenu dans l'ensemble des solutions de l'équation $\chi_i(s) = \chi_j(s)$.

Soit $\chi = \chi_i$, $\chi' = \chi_j$.

$$\chi(s) = \chi'(s)$$

$$\chi(s) = s^{i_0 + p i_1 + \dots + p^{n-1} i_{n-1}} \quad i_\alpha, i'_\alpha \leq \delta.$$

$$\chi'(s) = s^{i'_0 + p i'_1 + \dots + p^{n-1} i'_{n-1}}$$

$$s \in \mathbb{F}_{p^n}^\times, \text{ équation en } s \text{ de degré} \\ \leq \delta(1 + p + \dots + p^{n-1})$$

$$\text{donc l'ordre du centralisateur de } A \\ \text{est } \leq \delta \frac{p^n - 1}{p - 1}$$

$$\text{Donc l'indice est } \geq \frac{p^n - 1}{\delta} - \text{contradiction.}$$

Application aux variétés abéliennes

Soit A une variété abélienne sur K ayant bonne réduction.

Supposons $\text{car}(K) = 0$, et soit $e = v(p)$ l'indice de ramification absolu de K .

Soit $V = \text{Ker}(p: A(K) \rightarrow A(K))$ en.

sur $\mathbb{F}_p$ de $\dim 2g$, où $g = \dim(A)$.

Thm (Raynaud)

L'action de $\text{Gal}(\bar{K}/K)$ sur le semi-
simplifié de V p.r. à l'action de I
est d'amplitude $\leq e$.

(Corriger définition de l'amplitude:
 eu. V sur $k' \subset \bar{k}$ ss-corps,
 on regarde $V \otimes \bar{k}$) .

$A[p]$ schéma des points de division par p ,
 schéma en groupes fini, tue' par p , plat
 (Bull. SMF ~ 1974) .

$e=1$ et $\dim(A)=1$

cas ordinaire: action d'inertie $\begin{pmatrix} x & 0 \\ 0 & 1 \end{pmatrix}$

$$\mathbb{F}_p^\times \longrightarrow GL_2(\mathbb{F}_p)$$

$$x \longmapsto \begin{pmatrix} x & 0 \\ 0 & 1 \end{pmatrix}$$

$$\text{caractères} \rightarrow \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

supersingulière :

$$\mathbb{F}_{p^2}^\times \longrightarrow GL_2(\mathbb{F}_p)$$

$$x \longmapsto \begin{pmatrix} x & 0 \\ 0 & x^p \end{pmatrix}$$

$$\text{caractères} \rightarrow \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

On travaille dans H_1

Conjecture:

Si on est dans H_r , l'amplitude est
 $\leq r.e$

(Fontaine - Messing: vrai pour p
 assez grand (?)) .

20/1/86

Inertie modérée

$$\mathbb{F}_p^* \longrightarrow \mathbb{F}_p^* \quad x \mapsto x^{i_0 + p i_1 + \dots + i_{n-1} p^{n-1}}$$

caractères

$0 \leq i_j \leq p-1$

$$(i_0, \dots, i_{n-1}) \neq (p-1, \dots, p-1)$$

$$\text{amp}(x) = \sup(i_j)$$

K corps local, O_K anneau des entiers de K

car $K = \bar{K} = 0$, G schéma en groupes sur O_K

$G(\bar{K})$: espace vectoriel sur $\mathbb{F}_p$ de dim. n

$G_K = \text{Gal}(\bar{K}/K)$ opère sur $G(\bar{K})$, et donne

$$G_K \longrightarrow \text{GL}_n(\mathbb{F}_p).$$

Thm (Raynaud):

$e = v(p)$: indice de ramification absolue de K

Les caractères de l'inertie modérée intervenant dans une telle représentation ont une amplitude $\leq e$.

Cas utile ensuite : $e=1$.

Complément:

On suppose de plus $e=1$, $p \geq 3$. Soit I l'image dans $\text{GL}_n(\mathbb{F}_p)$ du groupe d'inertie de $\text{Gal}(\bar{K}/K)$. Alors I n'a pas de quotient d'ordre p .

$$1 \longrightarrow I_w \longrightarrow I \longrightarrow I_t \longrightarrow 1$$

sauvage modérée

(produit semi-direct)

I^n : higher ram. gps, $n \text{ réel} \geq 0$.

Thm (Fontaine): $I^{\frac{1}{p-1}} = \{1\}$.

Si J est un groupe d'inertie cyclique d'ordre p ,
alors $J \neq \{1\}$. D'où contradiction avec le th. de Fontaine.

Corollaire:

I est engendré par ses s/g modérés.

Tors d'inertie

$\mathbb{F}_{p^n}^\times$: gp de $\mathbb{F}_p$ -points du tore $T_n / \mathbb{F}_p$
"repr. de gp. mult. de $\mathbb{F}_{p^n}^\times = T_n(\mathbb{F}_p)$
où $T_n = \text{Res}_{\mathbb{F}_{p^n}/\mathbb{F}_p}(\mathbb{G}_m)$

$$(i.e. \quad T_n(A) = (\mathbb{F}_{p^n} \otimes A)^\times)$$

Donnée $\mathbb{F}_{p^n}^\times \rightarrow GL(V)$, on veut
prolonger à $T_n \rightarrow GL(V)$
(de groupes alg.)

1^{ère} étape: $k \supset \mathbb{F}_{p^n}$ et $\dim V = 1$.

$T_n / \mathbb{F}_p$, caract. $\cong \mathbb{Z}_{w_1} \times \dots \times \mathbb{Z}_{w_n}$ (n fois)

base de prolongements $\mathbb{F}_{p^n} \subset k$
(action naturelle de Gal).

Théorème de rigidité'

Représentation ρ de $\mathbb{F}_{p^n}^\times$ d'amplitude $\leq \delta$ dans $GL(V)$. Soit A un élément de $End(V)$. Alors les $x \in \mathbb{F}_{p^n}^\times$ tels que $\rho(x)$ commute à A forment un s/g qui est soit $\mathbb{F}_{p^n}^\times$, soit d'indice $\geq \frac{p-1}{\delta}$.

Situation de tout à l'heure:

$$e=1, \quad p \geq 3, \quad \rho: I \rightarrow GL(V)$$

Chaque $I = I_w \cdot I_t \rightarrow$ tore env. de I_t

Gp. alg. engendré' résoluble, u. tore

($p \geq n$, n ds GL_n) U : prendre exp $\rightarrow \mathbb{F}_p$.

③ Variété abélienne / k : corps de nombres.

$n = \dim(A) \geq 1$, l premier.

$$A_\ell = \text{Ker}(A(K) \rightarrow A(K)) \simeq \mathbb{F}_\ell^{2n}$$

$G_\ell =$ image de $\text{Gal}(\bar{K}/K)$ dans $\text{Aut}(A_\ell)$

Théorème:

S'il existe une infinité de l tels que

$|G_\ell|$ soit premier à l , alors A est de type CM.

(Il est bien connu que si A est de type CM, alors $|G_\ell|$ est premier à l sauf éventuellement pour un nombre fini de l).

Jordan

Rigidité de l'inertie modérée

thm de Faltings:

pour l assez grand, le commutant de G_l dans $\text{End}(A_l)$ est $\text{End}_K(A) \otimes \mathbb{Z}/l\mathbb{Z}$.

Type CM: "Suffisamment d'endomorphismes".

Soit $\Lambda = \mathbb{Q} \otimes \text{End}_{\bar{K}}(A)$: semi-simple

$\text{rang} :=$ dimension d'une sous-algèbre commutative semi-simple qui est son propre commutant

$=$ rang du groupe multiplicatif de Λ comme groupe algébrique.

$\text{rg } M_n = n$

Le rang est invariant par extension des scalaires.

CM $\iff \text{rg } \Lambda = 2n$

$\iff$ il y a une algèbre commutative semi-simple (étale) $M \subset \Lambda$

telle que V_l soit un

$\mathbb{Q}_l \otimes M$ -module libre de rang 1 (pour un l , ou pour tout l).

$\iff$ le groupe de Mumford-Tate de A est un tore

$\Leftrightarrow A/\bar{K}$ est produit de variétés abéliennes simples qui sont de type CM au sens de Shimura - Tanigama.

Si on savait que G_ℓ est commutatif, on aurait fini par Faltings.

Soit L l'ensemble des ℓ tels que $|G_\ell|$ est premier à ℓ .

Jordan $\Rightarrow \exists c$ tel que $\forall \ell \in L$, il existe un sous-groupe abélien normal H_ℓ de G_ℓ d'indice $\leq c$

Pour tout $\ell \in L$, choisissons H_ℓ abélien normal d'indice minimum.

$$[G_\ell : H_\ell] \leq c$$

$$\phi_\ell := G_\ell / H_\ell.$$

$$\text{Gal}(\bar{K}/K) \twoheadrightarrow G_\ell \twoheadrightarrow \phi_\ell$$

Donc $\phi_\ell = \text{Gal}(K'_\ell/K)$, K'_ℓ/K gal.

$$[K'_\ell : K] \leq c$$

Théorème (Hermite)

Les extensions d'un corps de nombres d'un degré donné et non ramifiées en dehors d'un nombre fini de places sont en nombre fini.

K'_l/K ne peut être ramifié qu'en

- a.) les places de K où A a mauvaise réduction
- b.) les places de K au-dessus de l .

a.) est un ensemble fini fixe

(en fait, quitte à étendre les scalaires par une extension finie de K , A a bonne réduction partout: En effet, par une telle extension on peut supposer A semi-stable. Par un théorème de Grothendieck, l'inertie agit par des unipotents. $\forall$ place de K , I_v agit sur A_v . Cette action est triviale Serre-Tate (Néron) s'il existe une infinité de l tels que l'action soit triviale, alors on a bonne réduction.

b.) pour l assez grand, on verra que ces places n'existent pas.

Lemme:

Si $l \in L$ est assez grand, l'extension K'/K est non ramifiée aux places de K divisant l

(vrai si $l > c+1$

l non ramifié dans K)

Soit v place de K au-dessus de l
 $\bar{v}$ " $\bar{K}$ "

On suppose $e_v = 1$.

Soit $I_{\bar{v}}$ le groupe d'inertie associé à $G_{\bar{v}}$.

Lemme $\Leftrightarrow I_{\bar{v}} \subset H_{\bar{v}}$

Montrons que $I_{\bar{v}}$ commute à $H_{\bar{v}}$ si $l > c$.

D'abord, $I_{\bar{v}} \cap H_{\bar{v}}$ commute à $H_{\bar{v}}$.

L'indice dans $I_{\bar{v}}$ de $I_{\bar{v}} \cap H_{\bar{v}}$ est $\leq c$.

Soit $M \in H_{\bar{v}}$.

Le sous-groupe de $I_{\bar{v}}$ formé des éléments commutant à M est d'indice $\leq c < l-1$.

Par rigidité (et $\delta=1$) tout $I_{\bar{v}}$ commute à M . Donc $I_{\bar{v}}$ commute à $H_{\bar{v}}$.

$H_{\bar{v}}$ abélien normal

$I_{\bar{v}}$ cyclique, commute à $H_{\bar{v}}$.

Deux conjugués quelconques de $I_{\bar{v}}$ commutent entre eux.

Démonstration:

Soyent I_1, I_2 deux tels s/g.

Soit $M \in I_2$. Soit I_1' le s/g des $x \in I_1$ qui commutent à M .

On a $H_{\bar{v}} \cap I_1 \subset I_1'$, car

$H_{\bar{v}}$ commute à I_2 .

Or, l'indice de $H_{\bar{v}} \cap I_1$ dans I_1 est $\leq c$.

Par rigidité, tous les éléments de I_1 commutent à M .

Le s/g engendré par H_ℓ et les $I_{\bar{v}}$ est abélien normal, et contient H_ℓ , il est donc égal à H_ℓ (par minimalité de l'indice)

Bornons-nous aux $\ell > c+1$, $\ell \nmid \text{disc}(K)$.

L'extension K'_ℓ/K est ramifiée au plus en des places de mauvaise réduction, et son degré est $\leq c$.

Ces extensions sont en nombre fini. On peut donc trouver K'/K fini qui contient tous les K'_ℓ .

Par changement de base de K à K' , les G_ℓ sont remplacés par des s/g G'_ℓ et l'on a $G'_\ell \subset H_\ell$.

En particulier les G'_ℓ sont abéliens.

Donc: quitte à remplacer K par K' , les G_ℓ sont abéliens.

Le commutant d'un groupe abélien est une algèbre semi-simple de rang $2n$.

Donc par Faltings, A est de type CM.

Analogie sur les corps de fonctions
(pas besoin de Raynaud).

K corps des fonctions rationnelles d'une courbe/ $\mathbb{F}_q$
 A variété abélienne / K .

CM = ?

Variété abélienne de type CM en car $p > 0$:

① $\mathbb{Q} \otimes \text{End}_{\bar{K}} A$ de rang $2n$, $n = \dim A$

② (Oort, Grothendieck)

A provient "presque" d'une variété sur $\mathbb{F}_q$.

Quitte à faire une extension finie des scalaires, et une isogénie (radicielle),
 A est définissable sur un corps fini.

(Ce n'est pas toujours vrai sans faire d'isogénie :

E courbe elliptique supersingulière

$$\rightarrow E \times E \rightarrow A \rightarrow 0$$

rad. de
 $d^0 p$
appl. tangente

noyau droite donnée.

droite de pente transcendante

$\rightarrow A_t$. Pas défini sur un corps fini).

réf. : Oort, J. pure appl. Algebra (1973), t.3, 399-408.

[Il n'y a pas de définition du groupe de Mumford-Tate en caract. $p > 0$,
mais il devrait y en avoir une : problème "cristallin" !]

Théorème :

Si les G_ℓ sont d'ordre premier à ℓ
pour une infinité de ℓ , alors A est
de type CM.

$H_\ell \subset G_\ell$ s/g abélien normal d'indice minimum
 $[G_\ell : H_\ell] \leq c$, $\phi_\ell = G_\ell / H_\ell$.

L'extension K'/K corr. à ϕ_ℓ ne peut être
 ramifiée qu'aux places de mauvaise réduction
 ($\ell \neq \text{car } K = p$).

En fait (comme avant) on montre que quitte
 à agrandir K , il y a bonne réduction
 partout.

Si K est donné, S ensemble fini de places
 de K , et m un entier premier à p ,
 il n'y a qu'un nombre fini d'extensions
 galoisiennes de K de degré m non
 ramifiées en dehors de S :

$$\pi_{\text{geom}} \longrightarrow \pi_1 \longrightarrow \text{Gal}(\mathbb{F}_\ell/\mathbb{F}_\ell) \longrightarrow 0, \quad \ell = \mathbb{F}_q$$

Même argument: quitte à agrandir K ,
 tous les G_ℓ ($\ell \in L$) deviennent abéliens.

De là, CM:

(1) Analogie en car p du thm de
 Faltings sur le commutant:

$$\text{End}_K A \otimes \mathbb{F}_\ell = \text{comm}(G_\ell) \quad \ell \text{ gdc}$$

$$\text{Gal}(\bar{K}/K) \rightarrow \text{Gal}(\bar{k}/k) = \hat{\mathbb{Z}} \xrightarrow{\varphi_\ell} G_\ell \quad (k = \mathbb{F}_q)$$

les repr. φ_ℓ sont les mêmes que celles données par la variété abélienne / $\mathbb{F}_q$ donnée par une fibre.

repr. ℓ_ℓ triviales sur le groupe fondamental géométrique : Oort " K/k -trace".

On peut supposer $= 0$.

Néron-Lang: pp. des points rat. sur $K\bar{k}$ de A est de type fini.

Or, les A_ℓ sont faits de points rationnels sur $K\bar{k}$ — contradiction.

Sous-groupes de $GL_n(\mathbb{F}_p)$ engendrés par leurs p -éléments (p -Sylow)

- M. Nori (en préparation)
- Matthews - Vaserstein - Weisfeiler
- Weisfeiler

On suppose $p \geq n$ (et même $p \geq 2n$).

Si $x \in GL_n(k)$, car $k = \mathbb{F}_p$, est d'ordre une puissance de p , alors $x = 1$ ou x est d'ordre p , et $x = \exp(y)$, $y^p = 0$ (forme de Jordan).

A un tel x on attachera

$$\psi_x : G_a \rightarrow GL_n$$

$$\psi_x(t) = \exp_p(ty)$$

Si G est un groupe fini, p fixé, G^+ le s/g de G engendré par les p -Sylow (p -élé). G/G^+ plus grand quotient de G d'ordre premier à p .

Si $G = G^+$, le groupe algébrique engendré par les $\psi_x(G_a)$, $x \in G$ d'ordre p , est noté G^{alg} .

Théorème (Nori) $k = \mathbb{F}_p$

Il existe une constante $c_1(n)$ dépendant de n mais non de p , telle que

$$G^{\text{alg}}(\mathbb{F}_p)^+ = G \quad \text{si} \quad p \geq c_1(n)$$

Cas où l'action de G est semi-simple est plus facile, et donne $c(n)$ effectif.

Exponentielles

Soit p un nombre premier, et A une algèbre associative sur $\mathbb{F}_p$. Soit $x \in A$ nilpotent, $x^r = 0$ avec

$$r \leq p \quad (\text{i.e. } x^p = 0)$$

$$\text{Alors } e^x = 1 + x + \frac{x^2}{2!} + \dots + \frac{x^{p-1}}{(p-1)!}$$

est défini, inversible d'inverse e^{-x} .

Si $x, y \in A$ et si $x^i y^j = 0$ dis que

$i+j \geq p$, et si $xy = yx$, alors

$$(x+y)^p = 0, \quad x^p = y^p = 0, \quad \text{et } e^{x+y} = e^x e^y$$

Corollaire :

Si $x_i \in A$, $i=1, \dots, m$ commutent et si

$$x_i^{r_i} = 0 \quad r_i \geq 1, \quad \sum_i (r_i - 1) + 1 \leq p, \quad \text{alors}$$

$$\left(\sum x_i \right)^p = 0, \quad \text{et } e^{\sum x_i} = e^{x_1} \dots e^{x_n}$$

$$(x_1^i x_2^j \neq 0 \Rightarrow r_1 \geq i+1, r_2 \geq j+1, \text{ donc}$$

$$i+j+2-1 > p - \text{contradiction})$$

Si $x^r = y^r = 0$, $p > 2r-1$, x et y commutent, alors $e^x e^y = e^{x+y}$.

$$A = \text{End}(V) \simeq M_n(k)$$

$$V \text{ ev. sur } k, \quad \text{car}(k) = p, \quad \dim(V) = n$$

Si x est nilpotent dans A , on a $x^n = 0$.

Si $p \geq n$, e^x est défini. C'est un élément

unipotent de $GL_n(k)$.

$\text{Exp} : x \mapsto e^x$ et $u \mapsto \log u$ donnent des bijections réciproques des nilpotents et unipotents

Lemme :

Si $p \geq 2n-1$, et si $x \in M_n(k)$ est nilpotent,
alors

$$\text{ad}(x) : y \mapsto [x, y] = xy - yx$$

(endom. de $M_n(k)$)

est tel que $\text{ad}(x)^p = 0$, et l'on a

$$e^x y e^{-x} = e^{\text{ad}(x)} y$$

pour tout $y \in M_n(k)$.

$$\text{ad}(x) : \text{End}(V) \rightarrow \text{End}(V), \quad \text{ad}(x) = L_x - R_x$$

$$\text{ou } L_x y = xy, \quad R_x y = yx$$

$$L_x \text{ et } R_x \text{ commutent, } L_x^n = 0, \quad R_x^n = 0$$

("nilpotents" par n) comme $p \geq 2n-1$,

$$(L_x - R_x)^p = 0, \text{ et}$$

$$e^{\text{ad}(x)} = e^{L_x} e^{-R_x}, \text{ donc}$$

$$\begin{aligned} e^{\text{ad}(x)} y &= e^{L_x} \left(y - yx + y \frac{x^2}{2} - \dots \right) \\ &= (1 + x + \dots) y (1 - x + \dots) \\ &= e^x y e^{-x}. \end{aligned}$$

Autre point de vue :

$$\text{remarquons que } \text{End}(V) = V \otimes V^*$$

$$V_1, \dots, V_k \quad x_i \in \text{End}(V_i) \text{ nilpotents}$$

$$\text{Supposons } \sum (\dim(V_i) - 1) + 1 \leq p$$

$$\text{alors } x = \sum x_i \otimes 1 \otimes \dots \otimes 1 \in \text{End}(V_1 \otimes \dots \otimes V_k)$$

est "nilpotente" par p . On a $e^x = e^{x_1} \otimes \dots \otimes e^{x_k}$.

Lemme:

Supposons $p \geq 2n-1$. Soit $x \in \text{End}(V)$ nilpotent, et
soient $W_2 \subset W_1 \subset \text{End}(V)$ des s/esp. vect. tels que
 $[x, W_1] \subset W_2$, i.e. $\text{ad}(x)W_1 \subset W_2$.

Alors W_1, W_2 sont stables par

$$y \mapsto e^x y e^{-x}$$

et $e^x y e^{-x} \equiv y \pmod{W_2} \quad \forall y \in W_1$

$$e^x y e^{-x} = e^{\text{ad}(x)} y = y + \text{ad}(x)y + \frac{1}{2} \text{ad}(x)^2 y + \dots$$

Si $y \in W_1$, $\equiv y \pmod{W_2}$

Exemple: $p=2, n=2$

$$x = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \quad W_1 = W_2 = \left\{ \begin{pmatrix} \lambda & 0 \\ \mu & \lambda \end{pmatrix}, \lambda, \mu \in \mathbb{k} \right\}$$

$$[x, W_1] \subset W_1, \text{ mais } e^x = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

et W_1 n'est pas stable par conjugaison par e^x

$$e^x \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} e^{-x} = \begin{pmatrix} * \\ * \end{pmatrix} \notin W_1$$

La construction de G_{alg}

V ev. de dim n sur $\mathbb{k}$, $\mathbb{k}$ de car p

Hyp: $p \geq 2n-1$

Soit G un s/g de $GL(V)$ eng. par ses élt's unipotents (i.e. $x^p = 1$).

Soit G_u l'ensemble des éléments unipotents de G .

Si $x \in G_u$, on a $x = \exp(X)$, $\log x = X$ nilpotent dans $\text{End}(V)$.

$$\exp(tX) = 1 + tX + \dots$$

est "indéterminée"

D'où un homomorphisme

$$S_x: G_a \rightarrow GL(V)$$

vu comme groupe algébrique sur k .

Par définition, G^{alg} est le plus petit s/g algébrique de $GL(V)$ contenant les images de S_x (i.e. engendré par les "s/g à un paramètre" $\text{Im } S_x$).

Problème:

Comparer G et $G^{alg}(k) = \text{pts rationnels}$, en supposant que G est k -stable.

(G est " k -stable" $\iff \forall x \in G_a \ \forall \lambda \in k$
on a $x^\lambda \in G$).

L'algèbre de Lie de G^{alg}

Soit $\mathfrak{g} = \text{Lie } G^{alg}$ l'algèbre de Lie
 $\mathfrak{g} \subset \text{End}(V)$

Soit $\mathfrak{a}$ le k -s/esp. vect. de $\text{End}(V)$
engendré par les $\log(x)$, $x \in G_a$.

Lemme:

On a $\mathfrak{a} \subset \mathfrak{g}$, et $[\mathfrak{a}, \mathfrak{a}] = [\mathfrak{g}, \mathfrak{g}]$

Remarque: Pas d'exemple connu où $\mathfrak{a} \neq \mathfrak{g}$.

$$\frac{d}{dt} (e^{tX})_{t=0} = X$$

$$X = \log x$$

Théorème:

On a $\mathcal{O} = \mathcal{O}_f$ dans chacun des cas suivants:

- ① $G = G_u$ (tout élément de G est unipotent)
- ② L'action de G sur V est semi-simple

Principe de ①:

G est contenu à conj. près dans le groupe unipotent triangulaire supérieur.

$p \geq n$: $\exp$ et $\log$ donnent des isomorphismes

réciproques: unipotents $\longleftrightarrow$ alg. de Lie correspondante,

$\mathfrak{sl}_g \longleftrightarrow \mathbb{F}_p \text{ sl}_{\mathfrak{alg}}$ de Lie

$$\mathcal{O} = k \cdot \log(G) \quad G^{\text{alg}} = \exp(\mathcal{O})$$

② $\Rightarrow$ ②': G^{alg} est un groupe algébrique semi-simple.

Propriétés de G^{alg} :

- G^{alg} est connexe
- n'a aucun quotient (même sur $\bar{k}$) qui soit G_m

Le radical de G^{alg} est unipotent

$G^{\text{alg}}/\text{rad} = \text{semi-simple}$

L'action de G^{alg} est semi-simple $\Rightarrow$ ②'

Lemme:

Si la car. du corps est $> \text{rang} + 1$, l'algèbre de Lie $\mathcal{O}_f$ d'un groupe semi-simple est telle que $[\mathcal{O}_f, \mathcal{O}_f] = \mathcal{O}_f$.

Classification: les contre exemples sont PSL_n ,
 $p|n$. Centre de SL_n est μ_n . SL_p de $\text{rg } p-1$
 Contre-ex minimal: PSL_2 en $\text{car } 2$ ($\text{rg } 1$)

$$G^{\text{alg}} \subset SL_n$$

semi-simple

$$\text{rg } G^{\text{alg}} \leq n-1$$

$$p > n, \text{ car } p \geq 2n-1$$

Etude des alg. de Lie en $\text{car } p$:

- Dieudonné Vol II

- Jacobson

De ce lemme résulte: $[\alpha, \alpha] = [\alpha, \sigma] = \sigma$

$$\Rightarrow \alpha > \sigma \Rightarrow \alpha = \sigma.$$

Tits: $G = \tilde{G}/C \subset \text{étale} \Rightarrow \text{alg. de Lie} =$
 non étale - liste.

Question: Est-il vrai que $\sigma = \alpha$? (si $p > 2n-1$)

Théorème:

Il existe une constante $c_2(n) \geq 2n-1$ telle que si

$k = \mathbb{F}_p$, $p \geq c_2(n)$, et si $G \subset GL_n(\mathbb{F}_p)$ est
 semi-simple et engendré par ses p -éléments,

alors

$$G = G^{\text{alg}}(\mathbb{F}_p)^+$$

s/g de $G^{\text{alg}}(\mathbb{F}_p)$ engendré par ses p -éléments
 (semi-simple: représentation semi-simple).

On trouvera $c_2(n)$ effectif (mais pas bon).

Lemme

① Soit $F \in \mathbb{F}_q[X_1, \dots, X_N]$, $F \neq 0$

Soit $d = \deg F$

Alors le nombre de $(x_1, \dots, x_N) \in \mathbb{F}_q^N$ tels
que $F(x_1, \dots, x_N) = 0$ est $\leq d \cdot q^{N-1}$.

Démonstration:

par récurrence sur $N+d$

Si $N+d=1$, $N=1$ et $d=0$: OK

Sinon, 2 cas: ou bien F est divisible par
un facteur linéaire $X_1 - a$, $a \in \mathbb{F}_q$

$$F = (X_1 - a)G(X_1, \dots, X_N), \quad \deg G = d-1$$

nombre de solutions $\leq q^{N-1} + (d-1)$

Sinon, $\forall a \in \mathbb{F}_q$, $F(a, X_2, \dots, X_N) \neq 0$ et
de degré $\leq d$.

Pour chaque a , il y a au plus dq^{N-2}
solutions en $X_2, \dots, X_N$.

② Variante du thm de Bézout

Dans l'espace projectif $\mathbb{P}^N$, soient
 $V_1, \dots, V_N$ des hypersurfaces de degrés
 $m_1, \dots, m_N$

Alors le nombre de points d'intersection
isolés des V_i est $\leq m_1 \dots m_N$

Famille $\bar{a}$ un paramètre de V_i^t

t.q. $V_i^0 = V_i$,

t générique: intersections isolés

Fulton: Intersection theory

Théorème:

Soient $S_1, \dots, S_d$ des hypersurfaces de $\mathbb{P}^N$
de degrés $m_1, \dots, m_d$ et soient V_α les
composantes irréductibles de $S_1 \cap \dots \cap S_d$.

Alors

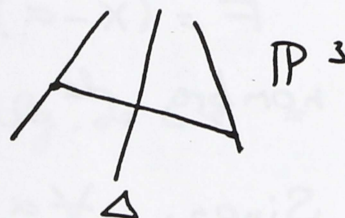
$$\sum \deg(V_\alpha) \leq m_1 \dots m_d$$

On se ramène à variétés linéaires, sauf une.

$$S_1 \cap S_2 \quad (S_1 \times S_2) \cap \Delta \quad (\text{diagonale})$$

$$\mathbb{P}^N * \mathbb{P}^N = \mathbb{P}^{2N+1} \quad \text{"joint"}$$

$$(S_1 * S_2) \cdot \Delta = S_1 \cap S_2$$

Théorème:

Soit $f: \text{Aff}^N \rightarrow \text{Aff}^M$ déf. sur $\mathbb{F}_q$
donné par M polynômes $f_1, \dots, f_M$
de degrés $\leq d$.

On suppose que l'application tangente à f
en $(0, \dots, 0)$ est injective.

Alors,

$$|\text{Im}(f: \mathbb{F}_q^N \rightarrow \mathbb{F}_q^M)| \geq$$

$$\geq q^N \left(1 - \frac{(d-1)N}{q}\right) / d^N$$

Corollaire:

Si q est grand par rapport à d, N
image $\geq c \cdot q^N$ avec $c = c(d, N)$.

Démonstration:

On se ramène à $M = N$.

En effet, on peut choisir les coordonnées pour que

$$\det \frac{\partial f_i}{\partial x_j} (0, \dots, 0) \neq 0 \quad \begin{matrix} i = 1, \dots, N \\ j = 1, \dots, N \end{matrix}$$

$$\text{Aff}^N \rightarrow \text{Aff}^M \xrightarrow{\text{proj}} \text{Aff}^N$$


Soit $J = \det \left(\frac{\partial f_i}{\partial x_j} \right)$ le polynôme Jacobien de f .

Soit $\Omega \subset \mathbb{F}_{q^N}$ l'ensemble des x avec $J(x) \neq 0$.
 $\deg(J) \leq N(d-1)$.

D'après le 1^{er} lemme,

$$|\mathbb{F}_{q^N} - \Omega| \leq N(d-1)q^{N-1}$$

$$\begin{aligned} \text{Donc } |\Omega| &\geq q^N - N(d-1)q^{N-1} \\ &= q^N \left(1 - \frac{N(d-1)}{q} \right) \end{aligned}$$

Les fibres de $f: \Omega \rightarrow \mathbb{F}_{q^N}$ ont au plus d^N éléments.

$$(a_1, \dots, a_N) \in \mathbb{F}_{q^N}$$

$$f_1(x_1, \dots, x_N) = a_1$$

$$\vdots$$

$$f_N(x_1, \dots, x_N) = a_N$$

$$|f(\Omega)| \geq |\Omega|/d^N$$

Lemme:

Soit G un groupe algébrique linéaire connexe / $\mathbb{F}_q$
dont aucun quotient $\neq 1$ n'est un tore

$\Leftrightarrow$ rad est unipotent

$\Leftrightarrow$ ext. d'un groupe semi-simple par un groupe unipotent

Alors $|G(\mathbb{F}_q)| \leq q^{\dim G}$

O. se ramène au cas semi-simple.

$|G(\mathbb{F}_q)|$ ne change pas par isogénie.

O. se ramène à G simplement connexe, simple.
Chevalley déployé:

$$G(\mathbb{F}_q) = q^N \prod_{i=1}^{\text{rg } G} \left(1 - \frac{1}{q^{a_i}}\right) \quad N = \dim G$$

non déployé: formule similaire avec "1" remplacé par racine de 1.

Par exemple, G spécial unitaire:

$$|G(\mathbb{F}_q)| = q^N \underbrace{\left(1 - \frac{1}{q^2}\right) \left(1 + \frac{1}{q^3}\right) \dots}_{< 1}$$

orth: facile, 1 seul + compensé par $1 - \frac{1}{q^2}$

D

orth triunitaire

E_6

Variante plus facile:

$$q^N \left(1 - \frac{1}{q^2}\right)^{\text{rg}} \leq |G(\mathbb{F}_q)| \leq q^N \left(1 + \frac{1}{q^2}\right)^{\text{rang}}$$

Idee de la démonstration de Nori :

$\alpha = \sigma_f$ donc il ex. base x_α de σ_f formée
de $\log x_\alpha$, $x_\alpha \in G$, $N = \dim \sigma_f$,

$$|G^{\text{alg}}(\mathbb{F}_p)| \leq p^N.$$

Théorème (= Lemme p. 41)

Soit $G \subset GL_n(\mathbb{F}_p)$ engendré par des éléments x
tels que $x^p = 1$.

Soient α le sous-espace de $M_n(\mathbb{F}_p)$ engendré
par les $\log(x)$, $x \in G$, $x^p = 1$, et
 $\sigma_f = \text{Lie}(G^{\text{alg}})$.

On suppose $p \geq 2n - 1$.

Alors $[\alpha, \alpha] = [\sigma_f, \sigma_f]$.

Corollaire:

Si G agit de façon semi-simple sur $\mathbb{F}_p^n$,
alors $\alpha = \sigma_f$.

Démonstration:

$V = \mathbb{F}_p^n$. Si $W \subset V$, il y a équivalence
entre: (sans supposer $p \geq 2n - 1$)

(i) $GW = W$

(ii) $\alpha W \subset W$

(iii) $G^{\text{alg}} W = W$

(iv) $\sigma_f W \subset W$

Si $W_2 \subset W_1$, il y a équivalence entre:

G agit trivialement sur W_1/W_2 $\alpha W_1 \subset W_2$
 G^{alg} " " $\leftrightarrow \sigma_f W_1 \subset W_2$

$\text{End}(V) = V \otimes V^*$. Action sur $\text{End}(V)$ est du type précédent si: $p \geq 2n-1$.
 s/espace de $\text{End}(V)$ $W_2 \subset W_1 \subset \text{End}(V)$

- ① $\alpha \in \text{End}(V)$ est stable par G (tr. de str.)
 $\Rightarrow$ stable par G^{alg} et $[\sigma_f, \alpha] \subset \alpha$
- ② Puisque $\text{ad}(\alpha)$ applique α dans $[\alpha, \alpha]$,
 $\text{ad}(\sigma_f)$ fait de même: $[\alpha, \sigma_f] \subset [\alpha, \alpha]$.
- ③ Puisque $\text{ad}(\sigma_f)$ applique α dans $[\alpha, \alpha]$,
 on a $[\sigma_f, \sigma_f] \subset [\alpha, \alpha]$
 D'où égalité.

($X \in \text{End}(V)$, prendre X' avec même inv. tens. que X)

Théorème :

Soit $G \subset \text{GL}_n(\mathbb{F}_p)$ engendré par ses p -éléments.
 Supposons $\alpha = \sigma_f$ (avec les notations précédentes)
 alors l'indice de G dans $G^{\text{alg}}(\mathbb{F}_p)$ est $\leq n^{6n^2}$.

Corollaire:

Si $p > n^{6n^2}$, on a $G = G^{\text{alg}}(\mathbb{F}_p)^+$.

Démonstration:

1.) Si $p \leq 2n^5$, l'énoncé est trivial car
 $|G^{\text{alg}}(\mathbb{F}_p)| \leq p^{n^2}$.

$n=1$ ok, $n \geq 2$: $p < n^6$ ok.

2.) On peut donc supposer $p > 2n^5$.

Soit $N = \dim \sigma_f$, on a $N \leq n^2$.

Soit $x_1, \dots, x_N$ une base de $\sigma_f = \alpha$,
 formée d'éléments $\log x_i$, $x_i \in G_n$.

On a $|G^{\text{alg}}(\mathbb{F}_p)| \leq p^N.$

G contient $\{x_1^{n_1}, \dots, x_N^{n_N}, 0 \leq n_i \leq p-1\}$

" $\exp(n_1 x_1) \dots \exp(n_N x_N)$

$f: \text{Aff}^N \rightarrow M_n = \text{Aff}^{n^2}$

$f(t_1, \dots, t_N) = \exp(t_1 x_1) \dots \exp(t_N x_N)$

On a $|G| \geq |\text{Im } f|$

Application tangente à l'origine:

$df(1, 0, \dots, 0) = x_1$

donc injective.

$df(0, \dots, 1) = x_N$

Degrés des composantes de f :

$\leq N(n-1) < n^3 = d$

Borne de la semaine dernière :

$|\text{Im } f| \geq p^N \left(1 - \frac{N(d-1)}{p}\right) / d^N$

$|\text{Im } f| \geq p^N \left(1 - \frac{n^5}{p}\right) / n^{3n^2}$

$p \geq 2n^5 \quad \geq p^N / 2n^{3n^2}$

Donc l'indice de G est $\leq 2n^{3n^2} \leq n^{6n^2}$

Démonstration du corollaire:

$p \geq n^{6n^2}$. Posons $H = G^{\text{alg}}(\mathbb{F}_p)^+$

à voir : $G = H$. $G \subset H$ est clair.

D'après le thm, $[H:G] \leq n^{6n^2}$

Lemme:

Si $H \geq G$ avec indice $< p$, p premier, et si H est engendré par ses p -éléments, alors $H = G$.

H/G , tout p -élément de H opère trivialement, donc $\in G \Rightarrow H = G$.

$$\text{Si } p \geq n^{6n^2} \Rightarrow p > n^{6n^2} !$$

Si G^{alg} est semi-simple, le revêtement universel $\tilde{G}^{\text{alg}}$ est défini, et $G^{\text{alg}}(\mathbb{F}_p)^+$ est l'image de $\tilde{G}^{\text{alg}}(\mathbb{F}_p) \rightarrow G^{\text{alg}}(\mathbb{F}_p)$.

$G^{\text{alg}}(\mathbb{F}_p)$ est engendré par ses p -éléments (bien connu, voir notes de Steinberg :

Lectures on Chevalley groups, Yale.

On se ramène aux groupes de rang 1, puis on regarde SL_2 et SU_2 à la main).

$$1 \rightarrow \underbrace{C}_{\substack{\text{de dim } 0 \\ \text{centre, de type multiplicatif}}} \rightarrow \tilde{G}^{\text{alg}} \rightarrow G^{\text{alg}} \rightarrow 1$$

$$1 \rightarrow \mu_n \rightarrow SL_n \rightarrow PSL_n = PGL_n \rightarrow 1$$

$$1 \rightarrow C(\mathbb{F}_p) \rightarrow \tilde{G}^{\text{alg}}(\mathbb{F}_p) \rightarrow G^{\text{alg}}(\mathbb{F}_p) \rightarrow \underbrace{H'(\mathbb{F}_p, C)}_{\substack{\text{divise l'ordre} \\ \text{de } C, \text{ donc} \\ \text{est premier à } p}}$$

Exemples numériques:

$$n=2 \Rightarrow G=(1), \quad G^{\text{alg}}=1$$

$$G=SL_2(\mathbb{F}_p) \Rightarrow G^{\text{alg}}=SL_2$$

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \text{ engendrent } SL_2.$$

Exemples où $G^{\text{alg}}(\mathbb{F}_p)^+ \neq G$

1.) J_1 1^{er} groupe de Janko, ordre 175560.

Contenu dans $G_2(\mathbb{F}_{11}) \subset GL_7(\mathbb{F}_{11})$

$p=11$. J_1 est engendré par ses 11-éléments.

$J_1^{\text{alg}} \stackrel{?}{=} G_2$: automorphismes des octaves de Cayley, dim 14.

$$\text{Ordre de } G_2(\mathbb{F}_{11}) = 11^6 \cdot (11^2 - 1)(11^6 - 1)$$

$$= 3,766 \dots 10^{14}$$

$$\text{Indice} \sim 2 \cdot 10^9$$

2.) A_7 repr. naturelle de $d^{\circ}7$, laisse fixe $(1, \dots, 1) \rightarrow$ on obtient repr. de $d^{\circ}6 \bmod 7$: $k = \mathbb{F}_7 \leadsto d^{\circ}5$

$$D \subset H = \{ \sum x_i = 0 \}$$

eng. $(1, \dots, 1)$

H/D de dim 5

Forme quadratique invariante $\sum x_i^2$

$$SO_5(\mathbb{F}_7)$$

$$B_2 = C_2 : SO_5 = Sp_4.$$

$$2A_7 = \tilde{A}_7 \subset Sp_4(\mathbb{F}_7) \subset GL_4, \quad \tilde{A}_7^{\text{alg}} \stackrel{?}{=} Sp_4$$

$$\text{indice } 54880$$

Groupe semi-simples en caractéristique p

On va s'intéresser aux s/g alg. G de GL_n en car p , sous les hypothèses:

- 1.) G est un groupe semi-simple, et son action est semi-simple.
- 2.) G est engendré par des s/g à 1 paramètre de type exp, i.e. de la forme

$$t \mapsto \exp(tX)$$

où X nilpotente, $X^p = 0$.

On va démontrer l'existence d'une constante c_3 telle que si $p > c_3(n)$, un tel G est "comme en car. 0".

Supposons corps de base algébriquement clos de car p .

Contre-exemple si 2.) n'est pas vérifiée:

$n=4$, p quelconque.

Si m entier ≥ 1 , s/g G de SL_4 formé des matrices

$$\begin{pmatrix} a & b & & 0 \\ c & d & & 0 \\ & & a^m & b^m \\ 0 & & c^m & d^m \end{pmatrix}$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2$$

$$G = SL_2$$

Il y a une infinité de tels groupes non isom. On ne peut pas relever en car 0.

exp:
$$\begin{pmatrix} 1 & t & & \\ 0 & 1 & & \\ & & 1 & t^{p^n} \\ & & 0 & 1 \end{pmatrix}$$

$$G_0 \subset G \xrightarrow{p} GL_n$$

$$t \mapsto \exp(tX_0) \exp(t^p X_1) \dots \exp(t^{p^n} X_n)$$

$$X_i^{p^n} = 0 \quad X_i \text{ commutent entre eux}$$

2.) $X_i = 0$ si $i \geq 1 \iff p(t)$ pol. de $d^0 < p$
 Sur les pts rationnels, le gpe précédent donne

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

s/q semi-simple de GL_n , en car 0

On va montrer que si $p \geq c_3(n)$, la "réduction mod p " d'un tel gpe vérifie

(1) et (2), et irréductible $\rightarrow$ irréductible,
 et on obtient ainsi tous les gp. satisfaisant à (1) et (2) à conjugaison près.

Remarque:

L'ensemble des tels G (à conj. près) est fini.

Problème:

Peut-on prendre $c_3(n) = n$?

rep. irréd / $\mathbb{Q}$, $\mathbb{Z}[\frac{1}{N}]$ N convenable
ou réduit mod p , $p > N$.

Simplement convexe associé $\rightarrow$ forme sur $\mathbb{Z}$
"réseau admissible" $\mathbb{Z}$ -structure

$$S: G_{\mathbb{Z}} \rightarrow GL_n / \mathbb{Z}.$$

Remarque 1:

Si une repr. en car 0 est irréductible, elle le reste mod p pour p assez grand :
 $G(\mathbb{Q})$ irréductible. Im $G(\mathbb{Q})$ dans $M_n(\mathbb{Q})$
engendre $M_n(\mathbb{Q})$. Donc $\exists g_i \in G(\mathbb{Q})$,
 $1 \leq i \leq n^2$ tels que $S(g_i)$ forment une
base de $M_n(\mathbb{Q})$. Reste vrai mod p
pour p assez grand.

Remarque 2:

$G \subset GL_n$ semi-simples en car. 0 sont en
nombre fini.

1.) $\text{rg } G \leq n-1$, car $G \subset SL_n$.
par classification, nombre fini de G
possibles.

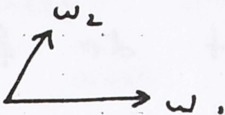
2.) Réduction au cas G simple, et représentation
irréductible.

Classification des irréductibles par leur plus
haut poids (poids dominant).

$$P_+ = \left\{ \lambda = \sum_{i=1}^l m_i w_i \mid m_i \geq 0, w_1, \dots, w_l \text{ poids fond.}, l = \text{rang.} \right\}$$

V_λ irréd. $\leftrightarrow \lambda$
 $\dim(V_\lambda)$: polynôme en m .
 $\rightarrow \infty$ sur le monoïde des λ .

Exemple: SL_3 (duale)



$$\dim V_\lambda = \frac{(m_1+1)(m_2+1)(m_1+m_2+2)}{2}$$

3 racines.

Représentations irréductibles en car p des groupes semi-simples

Classées par les mêmes $\lambda \in P_+$
à chaque $\lambda \rightarrow V_\lambda$ irréd. ($V_{\lambda,p}$ irréd.)

$G > \underset{T \cdot U}{B}$ Borel T tore, U unipotent.

Si V repr. irréd. de G , il y a une unique droite de V stable par B , et l'action de B sur cette droite se fait par un caractère

$$B \rightarrow T \xrightarrow{\lambda} \mathbb{G}_m$$

(en toute car.)

En général, $V_{\lambda,p}$ est "plus petite" que $V_\lambda \bmod p$. Plus précisément,

$$V_\lambda \bmod p = V_{\lambda,p} + ?$$

(ste J-H)

Définition:

λ est p-restreinte si les coefficients m_i sont $\leq p-1$:

$$\lambda = \sum_{i=1}^l m_i w_i \quad m_i \text{ entiers } \geq 0$$

Tout λ s'écrit de façon unique

$$\lambda = \sum_{\alpha=0}^{\infty} p^{\alpha} \lambda_{\alpha}$$

où les λ_{α} sont p-restreintes, et 0 pour α grand.

Remarque:

$$V_{p^{\alpha} \lambda} = (V_{\lambda})^{(p^{\alpha})}$$

$$S: G \rightarrow GL_n \xrightarrow{\text{Frob } p^{\alpha}} GL_n$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \begin{pmatrix} a^{p^{\alpha}} & b^{p^{\alpha}} \\ c^{p^{\alpha}} & d^{p^{\alpha}} \end{pmatrix}$$

Théorème (Steinberg):

Si $\lambda = \sum p^{\alpha} \lambda_{\alpha}$ λ_{α} p-restreint
alors

$$V_{\lambda} = \bigotimes_{\alpha} (V_{\lambda_{\alpha}})^{(p^{\alpha})}$$

Repr. de G sera dite restreinte, si elle est somme directe de V_{λ} avec λ p-restreint.

(Les repr. en nombre infini en car p proviennent de cette construction).

Lemme:

Si $p \geq n$, tout G satisfaisant $\bar{a}$ (1)
et (2) est du type p -restreint

Tout V_λ intervenant dans la repr. est

$$\lambda = \sum m_i w_i \quad \text{avec} \quad 0 \leq m_i \leq p-1$$

On a aussi $m_i \leq n-1$:

Lemme:

Si $\lambda = \sum m_i w_i$ est p -restreint, on a
 $m_i + 1 \leq \dim V_{\lambda, p}$ pour tout i .

On se ramène au cas de SL_2 .

$$SL_2 \longrightarrow G \xrightarrow{\quad \beta \quad} \text{Aut}(V_{\lambda, p})$$

G s. connexe

Restr. $\bar{a}$ SL_2 contient un vecteur propre
 pour le s/g de Borel de SL_2 avec
 $\exp m_i$

$$T_{SL_2} \rightarrow T_G$$

Un seul poids fondamental.

Si m est tel que $0 \leq m \leq p-1$, la
 repr. de SL_2 (en car p) de poids
 dominant $m w_1$, w_1 pds f. de SL_2 ,
 est la repr. $\text{Sym}^m(V_{w_1})$

V_{w_1} = repr. de $d^{\circ}z$ naturelle de SL_2 ,
 d'où $\dim V_{m w_1} = m+1$.

$$x, y \quad \{x^n, x^{n-1}y, \dots, y^n\} = \text{Sym}^n$$

$\bar{\alpha}$ voir : elle est irréductible si $n \leq p-1$

(si $n = p$: $\{x^p, x^{p-1}y, \dots, y^p\}$, et $\{x^p, y^p\}$ est stable $\rightarrow$ pas irréd.)

On passe d'un module $\bar{\alpha}$ à l'autre par $\begin{pmatrix} 1 & \\ & 0 \end{pmatrix}$ dérivée non nulle grâce à l'hypothèse.

Soit repr. irréd. $\lambda \quad m_i \leq p-1, m_i \leq n-1$

En car 0 : Soit S_n l'ensemble fini des (G, ρ) , G semi-simple, irréd. $\bar{\alpha}$ poids dominant coeff. $\leq n-1$

Si $p > c_4(n)$, les réductions mod p de ces repr. sont irréductibles.

Si λ int. G mod p , la repr. en car 0 a la même réduction mod $p \rightarrow$ c'est elle.

Effectivité :

Critère d'irréductibilité pour la réduction mod p de V_λ (Verma, Humphreys, Jantzen)

$$\text{Si } \sum (m_i + 1) c_i \leq p$$

c_i : coeff. de la plus grande racine du dual (G simple)

$\Rightarrow V_{\lambda, p}$ est la réduction mod p de V_λ

Représentation de Steinberg :

$$(p-1)(w_1 + \dots + w_\ell) \rightarrow \text{irréd. deg } p$$

On peut améliorer $c_3(n)$, $\sim n^2$ (probablement n).

17/2/86

Rappels:

- $G \subset GL_n / k$ car p , $p \geq n$, alg. dos tel que
- ① G semi-simple (en part. connexe) agissant de façon semi-simple.
 - ② G engendré par des $s/g \simeq G_a$ donnés par $t \mapsto \exp(tX)$, X nilpotente.

Nous avons vu qu'il existe une constante $c_3(n)$ telle que si $p \geq c_3(n)$ et si G satisfait à ①, ②, alors G provient par réduction mod p d'un groupe analogue en car 0.

Groupes de Chevalley / $\mathbb{Z}$, simplement connexe
Les repr. lin. sont aussi définies sur $\mathbb{Q}$ et même sur $\mathbb{Z}$.

$c_3(n)$ choisi tel que les réductions mod p des repr. irréd. de G de degré $\leq n$ sont irréductibles.

Engendrés par $t \in G_a$, $S(t) = \sum a_m t^m$, $\deg \leq n$.

G de rang $< n$ simplement connexe / k
 $S: G \rightarrow GL_n$.

Théorème: Si $p \geq c_3(n)$, se relève.

$V(\lambda)$, avec λ poids dominant p -restreint.
(i.e. $\lambda = \sum c_i w_i$ avec $0 \leq c_i \leq p-1$)

②: p -restreint $\Rightarrow c_i \leq n-1$.

$\dim V(\lambda)_p = \dim V(\lambda)_0$: se relève.

En fait, on a $c_3(n) = n$, mais ce ne sera pas démontré dans le cours. de toutes façons, on n'arrive pas à estimer toutes les constantes.

Finitude (à conj. près) indépendante de p ,
géométrique (on met ensemble les formes) des G

Définition:

Soit $G \subset GL(V)$, et N entier ≥ 0 .

Soit $T^i V = \otimes^i V$, $T_N = \bigoplus_{i=0}^N T^i V$

et soit T_N^G le sous-espace de T_N fixé par G . Soit G_N le sous-groupe alg. de $GL(V)$ fixant T_N^G .

On dit que G est défini par ses invariants tensoriels de poids $\leq N$ si: $G_N = G$.

Théorème:

Pour tout n , il existe $c_4(n)$ et $c_5(n)$ telles
que, si $G \subset GL_n / k$, car $k = p$,
 $p \geq c_4(n)$ et satisfaisant ① et
② (sur la clôture algébrique), alors
 G est défini par ses invariants tensoriels
de degré $\leq c_5(n)$.

Chevalley: Tout groupe alg. lin. est le stabilisateur d'une droite dans une somme directe d'espaces tensoriels $\otimes^i V \otimes^j V^*$
(cf. Demazure - Gabriel)

Gp. semi-simple: $\subset SL$. Alors on peut éliminer V

$$O_n \text{ a } V^* \simeq \wedge^n V, \quad n = \dim V$$

G_p semi-simple stabilise une droite $\Rightarrow$ il la fixe.

En car 0, pour chaque G semi-simple il existe un N correspondant. Fixons $G \hookrightarrow GL_n$, car 0.

(/ $\mathbb{Q}$). Fixons une base e_α des tenseurs invariants de poids $\leq N$.

Pour presque tout p , la réduction mod p de G est le fixateur des $e_\alpha \pmod{p}$.

$\tilde{G}/\mathbb{Z}$ fixateur des e_α : schéma en groupes de type fini. Par EGA IV : la réduction mod p de $\tilde{G}$ est le fixateur des $e_\alpha \pmod{p}$ pour p assez grand. Mais $\tilde{G}/\mathbb{Q} = G/\mathbb{Q}$.

Donc $\tilde{G} = G \pmod{p}$, p assez grand ($\geq c_4(n)$)
 $c_5(n)$ constante choisie en car 0.

Soit Norm_G le normalisateur de G dans GL_n .

$\text{Norm}_G/G \hookrightarrow GL_M$, M borné en fct de n :
 $M \leq c_6(n)$.

Sous-espace des tenseurs invariants de poids $\leq c_5(n)$: $W = T_{c_5(n)}^G$

Norm_G opère sur W , G opère trivialement
 On a donc une représentation fidèle

$$\text{Norm}_G/G \longrightarrow GL_W.$$

Théorème analogue :

Il existe $c_7(n)$, $c_8(n)$ telles que si $p \geq c_7(n)$

et G vérifie ①, ②, alors l'idéal des
pol. $f(a_{ij})$ définissant $G \subset M_n$ est
engendré par ses éléments de degré $\leq c_g(n)$.

On avait $G \subset GL_n(\mathbb{F}_p)$ engendré par ses
 p -éléments, semi-simple. On lui a associé
 G^{alg} semi-simple. Alors G^{alg} est aussi
 le groupe des élé de GL_n qui fixe
 les invariants tensoriels de degré borné
 de G .

Il existe un nombre fini de polynômes à
 coefficients dans $\mathbb{Z}$ en les a_{ij} tels que
 G soit géométriquement conjugué à un
 groupe définissable par une partie de
 ces polynômes.

Semi-simplicité et nullité de H^1 .

(pas utilisé dans la suite du cours)

car $p > 0$.

Théorème 1 :

Soit G semi-simple de rang $\leq n-1$, et soit

$$\rho: G \rightarrow GL(V)$$

$\dim(V) \leq n$, une repr. lin. de G

satisfaisant à ① et ②.

Alors si $c \geq c_g(n)$, $H^1(G, V) = 0$.

Démonstration:

On peut supposer p absolument irréductible. Le cas $p = 1$ est trivial: $H^1(G, 1) = \text{Hom}(G, G_a) = 0$.

Supposons $p \neq 1$, p irréductible, réduction mod p d'une représentation de car 0.

$H^1(G, V) = 0$ en car 0 (bien connu, car semi-simple) $\nrightarrow$ idem en car. p assez grand?

On le fait un peu autrement:

$$\alpha \in H^1(G, V) \leadsto 0 \rightarrow V \rightarrow E_\alpha \rightarrow 1 \rightarrow 0,$$

$$(\text{car } \text{Ext}_1^G(V_1, V_2) = H^1(G, \text{Hom}(V_1, V_2)))$$

Lie G opère sur la situation.

En car 0, on a un élément de Casimir:

$$C = \sum \alpha_{ij} X_i X_j$$

forme quadratique en les élé de l'algèbre de Lie ($\in$ centre de l'alg. env. U_{alg}).

On montre que C agit sur toute repr. irréd.

V_λ ($\lambda \rightarrow$ Casimir) par un scalaire $\neq 0$.

Pour p assez grand, C donne sur V un scalaire non nul mod p .

Le noyau de C dans E_α est un supplémentaire de 1 stable par G .

(remarque de Raynaud: $V \rtimes G \twoheadrightarrow G$,
 $H^1(G, V) = 0 \Leftrightarrow$ tous conjugués)

Question. $c_g(n) = n+1$?

On en déduit la semi-simplicité des représentations :

Théorème 2 :

Si $p \geq c_{10}(n)$, G semi-simple de rang $< n$,
toute représentation linéaire

$$\rho: G \rightarrow GL_n$$

en car p dont les poids sont p -restreints
(dans les quotients de Jordan - Hölder)
est semi-simple.

Question: peut-on supprimer l'hypothèse
sur les poids ?

A voir: Si V_1 et V_2 sont des repr. irréd.
de G p -restreintes, $\dim V_1 + \dim V_2 \leq n$,
 $p \geq c_{10}(n)$, alors $\text{Ext}_G^1(V_1, V_2) = 0$
 $\text{Ext}_G^1(V_1, V_2) = H^1(G, \text{Hom}(V_1, V_2))$, et
 $\dim(\text{Hom}(V_1, V_2)) \leq n^2$: on applique le
théorème précédent avec $c_{10}(n) = c_9(n^2)$.

Théorème 3 (Nori) :

Il existe $c_{11}(n)$ tel que si $p > c_{11}(n)$ et si
 $G \subset GL(V)$, V espace vectoriel $/\mathbb{F}_p$, $\dim V = n$,
 V un G -module semi-simple, alors
 $H^1(G, V) = 0$.

Supposons $p \geq n$.

Soit G^+ le sous-groupe de G engendré par
les p -Sylow de G .

Alors:

- 1.) G^+ est un s/g normal de G d'indice premier à p
- 2.) G^+ opère de façon semi-simple sur V .

Fait général:

Si G opère de façon semi-simple sur V de dim finie, alors tout s/g normal H de G opère de façon semi-simple. V simple, W sous H -module simple

$$\sum_{\substack{W \text{ H-mod} \\ \text{simple}}} W \subset V \quad \text{stable par } G$$

on en extrait une somme directe.

- 3.) $H^1(G, V) \rightarrow H^1(G^+, V)$ est injectif (résulte de ce que l'indice est premier à p).

Conclusion: On peut remplacer G par G^+ : on peut donc supposer G engendré par ses p -éléments.

On a attaché à G une "enveloppe algébrique" G_{alg} qui est un groupe semi-simple (au sens algébrique) contenu dans GL_n , vu comme groupe algébrique $/\mathbb{F}_p$.

- 1.) Par définition, G_{alg} est engendré par les groupes à 1 paramètre $t \mapsto \exp(tx)$, où x parcourt les log des p -élé de G .

2.) G^{alg} est semi-simple, et $\bar{\alpha}$ action semi-simple

3.) $[G^{\text{alg}}(\mathbb{F}_p) : G] \leq c(n)$.

si $p \geq c_j(n)$, on sait que $H^1(G^{\text{alg}}, V) = 0$.

Soit $\alpha \in H^1(G, V)$. Soit

$$0 \rightarrow V \rightarrow E_\alpha \rightarrow \mathbb{F}_p \rightarrow 0$$

l'extension correspondante.

(Si on savait que E_α est un G^{alg} -module, on aurait fini).

On peut supposer que V ne contient pas la représentation $\pm$. En effet,

$$H^1(G, \mathbb{F}_p) = \text{Hom}(G, \mathbb{Z}/p\mathbb{Z})$$

Si p est grand, $G = G^{\text{alg}}(\mathbb{F}_p)^+$: quotient de $\bar{G}(\mathbb{F}_p)$. Mais si $p \geq 5$, $\bar{G}(\mathbb{F}_p)$ est égal à son groupe dérivé, donc n'a pas d'homomorphisme dans $\mathbb{Z}/p\mathbb{Z}$: donc

$$H^1(G, \mathbb{F}_p) = 0.$$

Soit $\tilde{G}^{\text{alg}}$ l'enveloppe algébrique de G vu comme s/g de $GL(E_\alpha)$.

Soient $\mathfrak{o}_f$ ($\tilde{\mathfrak{o}}_f$) l'alg. de Lie de G^{alg} ($\tilde{G}^{\text{alg}}$)
 α ($\tilde{\alpha}$) le $\mathbb{F}_p$ -ev. engendré par les
 log dans $\text{End}(V)$ (resp. dans $\text{End}(E_\alpha)$)
 des p -éléments de G .

$$\begin{array}{ccc} \alpha & \subset & \mathfrak{o}_f \\ \uparrow & & \uparrow \\ \tilde{\alpha} & \subset & \tilde{\mathfrak{o}}_f \end{array}$$

On a un: si p est assez grand, $\alpha = \sigma_f$

$$([\sigma_f, \sigma_f] = [\alpha, \alpha] \text{ si } p \geq 2n-1,$$

$$\sigma_f = [\sigma_f, \sigma_f] \text{ si } p \geq 3, \text{ donc } \sigma_f = \alpha).$$

Le même argument montre que $[\tilde{\sigma}_f, \tilde{\sigma}_f] \subset \tilde{\alpha}$.

Montrons que $\tilde{\sigma}_f = [\tilde{\sigma}_f, \tilde{\sigma}_f]$:

$$0 \rightarrow W \rightarrow \tilde{\sigma}_f \rightarrow \sigma_f \rightarrow 0$$

$$\text{On a } W = [\sigma_f, W]$$

W est semi-simple, p -restreinte, et ne contient pas 1 .

Thm: En car p , si $V(\lambda)$ est repr. irréd. p -restreinte
 $V(\lambda)$ est un module irréd. sur l'algèbre de Lie
du groupe.

$$\text{D'où } \tilde{\alpha} = \tilde{\sigma}_f.$$

Par ce qu'on a déjà vu (applique' $\tilde{\alpha}$ $n+1$ au lieu de n) l'indice de G dans $G^{\text{alg}}(\mathbb{F}_p)$ est $\leq c_{12}(n)$.

$$\text{Soit } w = \dim(W)$$

$$1 \rightarrow W \rightarrow \tilde{G}^{\text{alg}} \xrightarrow{\text{proj}} G^{\text{alg}} \rightarrow 1$$

$$|\tilde{G}^{\text{alg}}(\mathbb{F}_p)| = p^w |G^{\text{alg}}(\mathbb{F}_p)|$$

$$N = \dim G^{\text{alg}} = \dim \sigma_f \geq p^w p^N \left(1 - \frac{1}{p^2}\right)^n \gg p^{N+w}$$

(au choix: $\geq \frac{1}{2} p^{N+w}$ si p assez grand)

$$|G| \leq |G^{\text{alg}}(\mathbb{F}_p)| \leq p^N$$

$$\text{Si } p \text{ assez grand, } c_{12}(n) p^N \geq \frac{1}{2} p^{N+w}$$

$$\Rightarrow w=0 \text{ si } p \text{ assez grand.}$$

Donc $\tilde{G}^{\text{alg}} \rightarrow G^{\text{alg}} \rightarrow 1$ est une isogénie

Mais il n'y a pas d'isogénie inseparable
car $p > n$, donc $\tilde{G}^{\text{alg}}$ est semi-simple.

On a déjà vu que ceci entraîne

$$H^1(\tilde{G}^{\text{alg}}, V) = 0$$

donc E_λ est scindée sur $\tilde{G}^{\text{alg}}$, donc
aussi sur G .

Références

Théorème de Jordan

- G.F.FROBENIUS, Ges.Abh., Springer-Verlag, 1968, III, 403-506.
- C.CURTIS et I.REINER, Representation theory ..., 1ere éd., 258-262.
- R.BRAUER et W.FEIT, An analog of Jordan's theorem ..., Ann.of Math. 84 (1966), 119-131.
- H.BASS, Theorems of Jordan and Burnside ..., J.of Algebra 82 (1983), 245-254.

Inertie et groupes de type $(p, \dots, p)$

- J-P.SERRE, Propriétés galoisiennes ..., Inv.Math.15 (1972), 259-331.
- M.RAYNAUD, Schémas en groupes de type $(p, \dots, p)$, Bull.SMF. 102 (1974), 241-280.
- J-M.FONTAINE, Il n'y a pas de variété abélienne sur $\mathbb{Z}$, Inv.Math. 81 (1985), 515-538.

Théorème de Bézout

- W.FULTON, Intersection Theory, Springer-Verlag, 1984 (p.148 et 223)

Enveloppes algébriques des sous-groupes de $GL_n(\mathbb{F}_p)$

- M.V.NORI, On subgroups of $SL_n(\mathbb{Z})$ and $SL_n(\mathbb{F}_p)$, 1983, non publié (une nouvelle version est en cours de rédaction).
- C.MATTHEWS, L.VASERSTEIN et B.WEISFELLER, Congruence properties of Zariski-dense subgroups, Proc.LMS 48 (1984), 514-532.
- B.WEISFELLER, Strong approximation for Zariski-dense subgroups, Ann.of Math. 120 (1984), 271-315.
- B.WEISFELLER, On the size and structure of finite linear groups, 1984, non encore publié.

Représentations linéaires des groupes semi-simples en caract. p

- A.BOREL et al, Seminar on Algebraic Groups..., Lect.Notes 131, Springer-Verlag, 1970.
- J.E.HUMPHREYS, Ordinary and Modular Representations of Chevalley Groups, Lect.Notes 528, Springer-Verlag, 1976.
- C.W.CURTIS et al, Representation Theory of Groups of Lie-type, Santa Cruz Conf., AMS Proc.Symp.Pure M. 37 (1980), Part IV.

K corps de nombres, A variété ab. / K , $\dim A = n$.

$$A_\ell = A[\ell] = \text{Ker}(\ell: A(K) \rightarrow A(K)) \cong (\mathbb{Z}/\ell\mathbb{Z})^{2n}.$$

$G_K = \text{Gal}(\bar{K}/K)$, G_K opère sur A_ℓ .

$$G_\ell = \text{Im}(G_K \rightarrow \text{Aut}(A_\ell) \cong \text{GL}_{2n}(\mathbb{F}_\ell))$$

"Pour tout n assez grand" signifie: A et K sont fixés.

On va définir, pour ℓ assez grand, un s/g alg. réductif connexe $\underline{H}_\ell \subset \text{GL}_{2n}/\mathbb{F}_\ell$.

Un groupe réductif connexe est: tore. semi-simple qui commutent entre eux, et dont l'intersection est un groupe fini contenu dans le centre du semi-simple.

Tore: composante neutre du centre

Semi-simple: groupe dérivé

$$\text{(e.g. } \text{GL}_n = \mathbb{G}_m \cdot \text{SL}_n, \text{ } \text{GSp}_{2n} = \mathbb{G}_m \cdot \text{Sp}_{2n})$$

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

Définition de $\underline{S}_\ell$:

Rappelons d'abord un théorème de Faltings:

Thm (Faltings):

Si ℓ est assez grand, on a:

- ① G agit de façon semi-simple sur A_ℓ .
- ② Le commutant de cette représentation est $\mathbb{F}_\ell \otimes \text{End}(A)$

Soit $\ell \geq 2n$, et ℓ assez grand pour ①

Soit G_ℓ^+ le s/g de G_ℓ engendré par les ℓ -éléments

On définit $\underline{S}_\ell$ par:

$$\underline{S}_\ell = (G_\ell^+)^{\text{alg}} = \{g. \text{ engendre' par } e^{tx}, x \in \log(\ell\text{-élé' de } G_\ell)\}.$$

G_ℓ^+ opère de façon semi-simple. $\underline{S}_\ell$ aussi.

Donc $\underline{S}_\ell$ est semi-simple, et agit de façon semi-simple, et est engendré par des exponentielles.

Remarque: La borne du thm de Faltings n'est pas effective.

Extension finie K' de K : remplace G_ℓ par $G_\ell' \subset G_\ell$ d'indice $\leq [K':K]$.

D'où $G_\ell'^+ = G_\ell^+$ si $\ell > [K':K]$, $\underline{S}_\ell' = \underline{S}_\ell$.

Étendre les scalaires ne modifie qu'un nombre fini de $\underline{S}_\ell$.

Le tore $\underline{S}_\ell$

Cas particulier: Si $\text{End}_{\bar{K}} A = \mathbb{Z}$, alors $\underline{S}_\ell$: homothéties G_m .

Choisissons K assez grand pour que

$$\text{End}_{\bar{K}} A = \text{End}_K A.$$

$$\text{Centre}(\mathbb{Q} \otimes \text{End} A) = L = \prod L_j$$

L est une $\mathbb{Q}$ -algèbre commutative étale.

T_L = "tore des éléments invariants de L " = $\prod T_{L_j}$
tore sur $\mathbb{Q}$.

On définira un sous-tore C de T_L défini sur $\mathbb{Q}$.

$$V_{\ell \infty} A = (\text{module de Tate de } A \text{ en } \ell) \otimes \mathbb{Q}_\ell.$$

$L_\ell = L \otimes \mathbb{Q}_\ell$ opère sur $V_{\ell \infty} A$.

$V_{\ell \infty} A$ est un module projectif de type fini sur L_ℓ . D'où un module libre de rang 1 sur L_ℓ , $\det_{V_\ell} (V_{\ell \infty} A)$. On en déduit un homomorphisme

$$G_K \rightarrow L_\ell^*$$

donnant l'action de G_K sur ce module.

On obtient ainsi une famille (l variable) de repr. ab. de G_K , elles sont "compatibles" (Frob. $\in L$, indép. de l).

Propriété de "Hodge - Tate"

Donc cette famille peut être décrite comme dans Mc Gill "Abelian l -adic representations".

Taniyama - Weil :

$$\begin{array}{c} S_m \text{ attaché à } K \\ \cup \\ T_K \longrightarrow T_m \text{ tore} \end{array}$$

$G_K \rightarrow L_\ell^*$ sont "associés" (Mc Grel)
à un homomorphisme $T_K \xrightarrow{\varphi} T_L$.

D'où un sous-tore $\varphi(T_K)$ de T_L

$\pi: T_L \rightarrow T_L$ isogénie
(action sur le det)

Si L est un corps, $\pi(x) = x^d$

$\pi(x) = x^{d'}$, où $d = \text{rang}_{L_\ell} V_{\ell \infty} A$.

Définition de C : sous-tore de T_L tel que son image par π soit $\varphi(T_K)$

Exemple:

Courbe elliptique $\bar{a}$ mult. compl. par $L = \mathbb{Q}(\sqrt{d})$.

$L \subset K$. Identification par l'action sur espace tgl.

Dans ce cas, $\Psi: T_K \rightarrow T_L$ est $N_{K/L} = \text{norme}: K^* \rightarrow L^*$
et $\pi = \text{id}$, $C = T_L$.

Définition directe de Ψ :

Soit $\text{Lie}(A)$ l'algèbre de Lie de A sur K .
C'est un $K-L$ bimodule. $\det_L \text{Lie } A$ est un
module de rang 1 sur L . Tout $\alpha \in K^*$
définit un automorphisme de $\det_L \text{Lie } A$
 $\alpha \mapsto \det_L (\alpha: \text{Lie } A \rightarrow \text{Lie } A)$ c'est Ψ .
 $K^* \rightarrow L^*$

$T_{L,\ell}$ est défini: (tore associé à l'action de
 $\mathbb{F}_\ell \otimes \mathbb{Q}_L$ sur A_ℓ , (où $\sigma_L = L \cap \text{End } A$: ordre de L)

$\underline{C}_\ell \subset T_{L,\ell}$. Donc $\underline{C}_\ell$ commute à G_ℓ
donc à G_ℓ^+ , donc à $\underline{S}_\ell$.

Donc on peut définir le groupe réductif
connexe $\underline{H}_\ell = \underline{C}_\ell \cdot \underline{S}_\ell$.

Théorème:

Pour ℓ assez grand, $\underline{H}_\ell$ est engendré par $\underline{S}_\ell$
et par les différents tores d'inertie modérée en

Supposons ℓ assez grand pour que:

- 1.) A a bonne réduction en ℓ
- 2.) ℓ non ramifié dans K .

Soit w une place de $\overline{K}$ divisant l .

$$w \mapsto I_w \subset G_l$$

"

produit semi-direct de "modéré" et "sauvage".

On a défini un tore $/\mathbb{F}_l$ contenant l'inertie modérée et qui est son "enveloppe".

$(\mathbb{H}_l / \mathbb{S}_l$ tore engendré par les tores d'inertie).

Exemple:

Courbe elliptique $\bar{a}$ mult. compl. par $L = \mathbb{Q}(\sqrt{-d})$

$\mathbb{H}_l = T_{L, l}$ l décompose dans L :

tores d'inertie: $\begin{pmatrix} * & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & * \end{pmatrix}$.

Conjecture:

$\mathbb{H}_l$ est engendré par les tores d'inertie (l grand)

Théorème 1:

Pour l assez grand, G_l normalise $\mathbb{H}_l$
et l'ordre de $G_l / G_l \cap \mathbb{H}_l(\mathbb{F}_l)$ est borné
quand l varie.

1' : Si K est assez grand, alors pour tout l assez grand on a:

$G_l \subset \mathbb{H}_l(\mathbb{F}_l)$ avec indice borné pour l variable.

Démonstration:

Que G_l normalise $\mathbb{H}_l$ est clair.

G_l normalise $\mathbb{S}_l$, et G_l normalise G_l^+ donc $\mathbb{S}_l$.

Dès que tous les end. de A sont $/K$, G_l centralise $\mathbb{S}_l$.

Supposons K assez grand pour que tous les end. soient définis sur K . Soit $\underline{N}_\ell$ le normalisateur de $\underline{S}_\ell$ dans $GL_{2n}/\mathbb{F}_\ell$. $G_\ell \subset \underline{N}_\ell(\mathbb{F}_\ell)$.

$G_\ell \rightarrow \underline{N}_\ell/\underline{S}_\ell(\mathbb{F}_\ell)$. Soit G'_ℓ l'image.

$G'_\ell = G_\ell / G_\ell \cap \underline{S}_\ell(\mathbb{F}_\ell)$, $|G'_\ell|$ est premier à ℓ .

Il existe un entier k ne dépendant que de n tel que, si W est le sous-espace de

$$\bigoplus_{i=1}^k T^i(A_\ell)$$

formé des éléments invariants par $\underline{S}_\ell$, alors

$\underline{S}_\ell$ est le fixateur de W , et $\underline{N}_\ell/\underline{S}_\ell \hookrightarrow GL_W$.

En particulier, $\dim W$ est borné par une constante ne dépendant que de n .

D'où $G'_\ell \hookrightarrow GL_W(\mathbb{F}_\ell) = \text{Aut}(W)$.

Soit J_ℓ un s/g abélien normal de G'_ℓ d'indice minimum. Par Jordan, on a $[G'_\ell : J_\ell] \leq c$ (ne dépendant que de n).

On va montrer que si ℓ est assez grand, les groupes d'inertie dans G'_ℓ des places au-dessus de ℓ sont contenues dans J_ℓ .

Soit I un tel groupe d'inertie. On va montrer que I commute à J_ℓ . Soit $x \in J_\ell$. Le s/g I_x des éléments de I commutant à x est d'indice au plus c (car I_x contient $I \cap J_\ell$). Le groupe I est un groupe d'inertie modérée d'amplitude $\leq k$ (thm de Raynaud). Par le thm de

rigidité de l'inertie, si l'indice est $< \frac{l-1}{k}$, alors I commute à x . Donc I commute à J_ℓ .

On utilise le même argument pour prouver que si I et I' sont deux groupes d'inertie différents, I et I' commutent (car s/g d'indice $< c$ de I : $I \cap J$ commute à I').

Alors J_ℓ et les I engendrent un s/g abélien normal, donc égal à J_ℓ .

Considérons l'extension K_ℓ/k de groupe de Galois G'_ℓ/J_ℓ

$$G_k \rightarrow G_\ell \rightarrow G'_\ell \rightarrow G'_\ell/J_\ell$$

cette extension est de degré $\leq c$ borné, et est ramifiée au plus aux places de mauvaise réduction de A . (pas ramifiée en l par l'argument précédent). Par Hermite, il n'y a qu'un nombre fini de tels corps. On étend K de telle sorte que le nouveau K contienne les K_ℓ . Ceci fait (pour l grand) on a G'_ℓ abélien.

A montrer (quitte à étendre K): G'_ℓ est contenu dans le s/g alg. de $\underline{N}_\ell/\underline{S}_\ell$ engendré par les tores d'inertie en l , qui est un tore. A vérifier: les tores d'inertie normalisent $\underline{S}_\ell$ (si l assez grand). Il suffit de voir qu'un tel tore normalise W .

Le groupe d'inertie le fait. Amplitude $\leq k$,
 $l-1 > k \Rightarrow$ le tore d'inertie stabilise les
 mêmes sous-espaces que le groupe d'inertie.
 Les tores en quot. sont $\subset \underline{N}_\ell$. Leurs
 images dans $\underline{N}_\ell / \underline{S}_\ell$ sont des tores qui
 commutent entre eux. En effet, c'est vrai
 pour les s/g d'inertie et ampl. $\leq k$ suffit
 ($l-1 > k$). Soit $\underline{X}_\ell$ le sous-tore de
 $\underline{N}_\ell / \underline{S}_\ell$ engendré par les tores d'inertie.

A montrer: quitte à faire une extension finie
 de K , on a : $G'_\ell \subset \underline{X}_\ell(\mathbb{F}_\ell)$.

On peut supposer K assez grand pour que
 A ait réduction semi-stable sur K . En les
 places de mauvaise réduction de A , l'action
 de l'inertie est unipotente.

v place à mauvaise réduction de A , $l \neq p_v$
 Action de l'inertie en v sur $V_{\ell \infty} A$ ou sur
 A_ℓ se fait par des éléments de valeur
 propre 1.

$\Rightarrow$ pas d'inertie dans G'_ℓ pour les places
 de mauvaise réduction $\neq l$. Celle en l
 est contenue dans $G'_\ell \cap \underline{X}_\ell(\mathbb{F}_\ell)$. Donc
 l'extension abélienne de K de groupe de
 Galois

$$G'_\ell / (G'_\ell \cap \underline{X}_\ell(\mathbb{F}_\ell))$$

est non ramifiée partout, donc contenue
 dans le corps de classes absolu de K .

Quitte à étendre K , on a :

$$G'_\ell \subset \underline{X}_\ell(\mathbb{F}_\ell)$$

$$1 \longrightarrow \underline{S}_\ell \longrightarrow \underline{N}_\ell \longrightarrow \underline{N}_\ell / \underline{S}_\ell \longrightarrow 1$$

$\bigcup$
 $\underline{X}_\ell$ eng. par les images
des tores d'inertie

Soit $\underline{H}'_\ell$ l'image réciproque de $\underline{X}_\ell$ dans $\underline{N}_\ell$.

$$1 \longrightarrow \underline{S}_\ell \longrightarrow \underline{H}'_\ell \longrightarrow \underline{X}_\ell \longrightarrow 1$$

donc $\underline{H}'_\ell$ est réductif connexe de groupe dérivé $\underline{S}_\ell$.

$$\underline{H}'_\ell = \underline{C}'_\ell \cdot \underline{S}_\ell, \quad \underline{C}'_\ell \text{ comp. neutre du centre.}$$

La projection $\underline{H}'_\ell \rightarrow \underline{X}_\ell$ donne une isogénie $\underline{C}'_\ell \rightarrow \underline{X}_\ell$.

A montrer : $\underline{C}'_\ell = \underline{C}_\ell$ pour ℓ assez grand, et donc, $\underline{H}'_\ell = \underline{H}_\ell$.

D'abord, $\underline{C}'_\ell$ est un sous-tore du tore $T_{L,\ell}$.

1.) $\underline{C}'_\ell$ commute à G_ℓ , car $\underline{C}'_\ell \subset$ centre de $\underline{H}'_\ell$.

$\underline{C}'_\ell \subset$ "groupe multiplicatif" de $\mathbb{F}_\ell \otimes \text{End } A$.

2.) $\underline{C}'_\ell$ commute à $\text{End } A$, car les tores d'inertie, $\underline{S}_\ell, \dots$ commutent à $\mathbb{F}_\ell \otimes \text{End } A$.

$$1.) \text{ et } 2.) \Rightarrow \underline{C}'_\ell \subset T_{L,\ell}$$

$$\begin{array}{ccc} \underline{C}_\ell & & \\ \underline{C}'_\ell & \subset T_{L,\ell} & \xrightarrow{\pi} T_{L,\ell} \\ & & \pi(x) = x^d \end{array}$$

Il suffit de prouver $\pi(\underline{C}_\ell) = \pi(\underline{C}'_\ell)$.
C'est vrai par la "théorie abélienne".

$$\pi(C_\ell) = \varphi(T_K)_\ell$$

$\pi(C'_\ell)$: engendré par les tores d'inertie
(système de repr. abélienne ℓ -adique, deux
tores mod ℓ suivants coïncident: $\varphi: T_K \rightarrow \dots$
et celui engendré par les tores d'inertie en les
places $|\ell$).

[Si on n'est pas convaincu, on peut définir $H \overset{\text{comme}}{=} H']$

$$1 \rightarrow \underline{S}_\ell(\mathbb{F}_\ell) \rightarrow \underline{H}_\ell(\mathbb{F}_\ell) \rightarrow (\underline{H}_\ell / \underline{S}_\ell)(\mathbb{F}_\ell) \rightarrow 1$$

exacte:
Lang)

$$\bigcup_{G_\ell^+} \text{indice borne'} \subset \bigcup_{G_\ell} \text{indice borne'} \quad \underline{X}_\ell(\mathbb{F}_\ell)$$

Il suffit de voir que l'indice de G_ℓ' dans
 $\underline{X}_\ell(\mathbb{F}_\ell)$ est borné.

$$\det_L : \underline{X}_\ell \rightarrow \pi(C_\ell) \subset I_{L,\ell}$$

isogénie de degré borné.

$$\underbrace{C_\ell \rightarrow \underline{X}_\ell \rightarrow \pi(C_\ell)}_{\text{borne'}}$$

image de Galois est d'indice borné dans
les points rationnels du tor image.

Remarque:

En fait, il y a $c(n)$ tel que

$$|G_\ell / G_\ell \cap \underline{H}_\ell(\mathbb{F}_\ell)| \leq c(n)$$

pour tout ℓ assez grand (dépendant de
 A, K).

$$[\underline{H}_\ell(\mathbb{F}_\ell) : G_\ell] \leq c(n) \quad \text{pour } \ell \text{ grand}$$

$$n=1 \quad (\text{courbe elliptique}) \quad |G_\ell / G_\ell \cap \underline{H}_\ell(\mathbb{F}_\ell)| < 2$$

$$\ell \text{ grand, } \underline{H}_\ell(\mathbb{F}_\ell) = G_\ell.$$

Rappel :

$$\underline{H}_\ell = \underline{C}_\ell \cdot \underline{S}_\ell \subset GL_n / \mathbb{F}_\ell$$

Th : pour k assez grand, on a : $G_\ell \subset \underline{H}_\ell(\mathbb{F}_\ell)$ avec indice borné (pour ℓ assez grand dép. de k).

$$G_\ell^+ = \text{image de } \tilde{S}_\ell(\mathbb{F}_\ell) \rightarrow \underline{S}_\ell(\mathbb{F}_\ell) = \underline{S}_\ell(\mathbb{F}_\ell)^+$$

où $\tilde{S}_\ell$: rev. univ. de $\underline{S}_\ell$

pour ℓ assez grand

$\underline{S}_\ell(\mathbb{F}_\ell)^+$: son groupe dérivé, et c'est le groupe dérivé de $\underline{H}_\ell(\mathbb{F}_\ell)$

$$\underline{H} = \underline{C} \cdot \underline{S} / \mathbb{F}_\ell \quad \ell \geq 5$$

groupe dérivé de $\underline{H}(\mathbb{F}_\ell) =$ groupe dérivé de $\underline{S}(\mathbb{F}_\ell) =$
 $=$ image de $\tilde{S}(\mathbb{F}_\ell) \rightarrow \underline{S}(\mathbb{F}_\ell)$

à montrer : le groupe dérivé de $\underline{H}(\mathbb{F}_\ell)$ est contenu dans l'image de $\tilde{S}(\mathbb{F}_\ell) \rightarrow \underline{S}(\mathbb{F}_\ell)$

$\tilde{H} = \underline{C} \times \tilde{S} \rightarrow \underline{H}$ isogénie centrale, $x, y \in \underline{H}(\mathbb{F}_\ell)$

$$\tilde{x}, \tilde{y} \in \tilde{H}(\mathbb{F}_\ell) \rightarrow x, y$$

$[\tilde{x}, \tilde{y}] \in \tilde{H}(\mathbb{F}_\ell)$, en fait dans $\tilde{H}(\mathbb{F}_\ell)$

$$- \quad - \quad - \quad \tilde{S}(\mathbb{F}_\ell)$$

$$\underline{H} \times \underline{H} \rightarrow \underline{H}$$

$$(x, y) \mapsto [x, y]$$

se factorise par $\underline{H} \times \underline{H} \rightarrow \tilde{S} \rightarrow \underline{H}$

$\underline{G}_\ell^+ = \underline{S}_\ell(\mathbb{F}_\ell)^+$ est le groupe dérivé de $\underline{G}_\ell$

Tore de Hodge V dim $2n$ $V = V_1 \oplus V_2$

$\dim V_i = n$, $G_m \times G_m$ opère par :

$$(\lambda, \mu) \quad \lambda \text{ sur } V_1, \mu \text{ sur } V_2.$$

$$\begin{pmatrix} \gamma & & 0 \\ & \gamma & \\ 0 & & \gamma \end{pmatrix}$$

$\frac{1}{2}$ -tore de Hodge: G_m λ sur V_1
1 sur V_2

$$\begin{pmatrix} \gamma & & 0 \\ & \gamma & \\ 0 & & \gamma \end{pmatrix}$$

Un s/g alg. H de GL_{2n} "contient géométriquement" un tore de Hodge si après extension des scalaires il en contient un. Même définition pour les $\frac{1}{2}$ -tores.

Th:

Si ℓ est assez grand, tout tore d'inertie en ℓ contient géométriquement un $\frac{1}{2}$ -tore de Hodge, et est engendré par des $\frac{1}{2}$ -tores de Hodge.

Th:

Le groupe $\subseteq_\ell$ contient les homothéties G_m

Th:

Le groupe H_ℓ contient géométriquement un tore de Hodge.

Il suffit de démontrer le 1^{er} thm (Bogomolov a montré que $\subseteq$ contient G_m).

Conditions sur ℓ : ℓ non ramifié dans K ,

A a bonne réduction en ℓ ,

$\ell \geq 3$, ℓ premier au degré d'une polarisation que l'on a choisie sur A .

$\mathbb{F}_{\ell^N}^* \xrightarrow{\cong} \text{caractères dans } \mathbb{F}_{\ell^N}^*$

$$\chi_1, \dots, \chi_N \quad x \mapsto x^{\ell^i}$$

les caractères qui interviennent sont du type

$$\prod \chi_i^{\epsilon_i} \quad \epsilon_i = 0 \text{ ou } 1.$$

$$A_{\ell} \times A_{\ell} \rightarrow \mu_{\ell} \quad (\cong \mathbb{Z}/\ell\mathbb{Z})$$

De l'existence de cette forme symplectique sur A_{ℓ} il résulte que les $2n$ caractères $\psi_1, \dots, \psi_{2n}$ donnant l'action de $\mathbb{F}_{\ell^n}^*$ sur A_{ℓ} peuvent être indexés de telle sorte que $\psi_1 \psi_2 = \chi = \psi_3 \psi_4 = \dots = \psi_{n-1} \psi_n$ où $\chi = \text{caractère cyclotomique} = \chi_1 \dots \chi_N$.

On a associé à ces données un tore de dim N

$$G_n \times \dots \times G_n \quad N \text{ fois}$$

$$\underline{\chi}_1, \dots, \underline{\chi}_n \quad \text{base de ses caractères.}$$

Autre propriété de $\mathbb{H}_{\ell}$:

Le commutant de $\mathbb{H}_{\ell}$ (dans sa représentation sur A_{ℓ}) est $\mathbb{F}_{\ell} \otimes \text{End } A$ (l'grand)

Pour G_{ℓ} , l'énoncé analogue est un thm de Faltings.

Le commutant de $\mathbb{H}_{\ell} \subset \mathbb{F}_{\ell} \otimes \text{End}(A)$.

Mais on a vu que $\text{End}(A)$ commute

$$\text{à } \mathbb{H}_{\ell}$$

Exercice: Il y a équivalence entre:

① A est de type CM

② $S_{\ell} = (1)$ pour ℓ assez grand

$S_{\ell} = (1)$ pour une infinité de ℓ .

Théorème :

Il existe une constante $c \geq 1$ (dépendant de A, K) telle que G_ℓ contienne les puissances c -ièmes des homothéties.

G_ℓ d'indice borné dans $\mathbb{H}_\ell(\mathbb{F}_\ell) > \mathbb{F}_\ell^*$

Théorème :

Si A n'a pas de facteur (à isogénie près) de type CM ($\neq (1)$), il existe une constante $c > 0$ telle que pour tout point de A d'ordre premier ℓ , on ait

$$|G_\ell \cdot x| \geq c \ell^2.$$

On peut supposer que A soit simple, et non de type CM.

Lemme : ℓ grand.

La représentation de S_ℓ dans A_ℓ ne contient pas la représentation unité.

Admettons ce lemme. Alors le sous-espace de A_ℓ fixé par G_ℓ^+ est réduit à 0.

Donc pour tout $x \in A_\ell$, $x \neq 0$, il existe un élément s d'ordre ℓ de G_ℓ^+ qui ne fixe pas x .

$G_\ell \cdot x$ contient tous les transformés du type $\lambda s^i x$, $\lambda \in (\mathbb{F}_\ell^*)^\ell$, $0 \leq i \leq \ell-1$ tous distincts :

$$\lambda s^i x = \lambda' s^{i'} x \quad s^{i-i'} x = (\lambda'/\lambda) x$$

$s^{i-i'}$ unipotent $\Leftrightarrow$ valeurs propres = 1, donc

$$\lambda' = \lambda \quad s^{i-i'} x = x \Rightarrow i = i'.$$

Démonstration du lemme:

$\mathbb{Q} \otimes \text{End } A = D$, corps gauche de centre L .

$$[D:L] = d^2, \quad [L:\mathbb{Q}] = \lambda, \quad n = \dim A$$

$$D_\ell \simeq M_d(L_\ell) \quad (\text{réduction mod } \ell \text{ d'un ordre de } D)$$

$$\text{Commutant de } \underline{H}_\ell = \underline{C}_\ell \cdot S_\ell$$

On montre que V_ℓ est un $\mathbb{Q}_\ell \otimes L$ -module libre de rang $2n/\lambda$, et que A_ℓ est un L_ℓ -module libre de rang $2n/\lambda$.

$$\text{Sur } \mathbb{F}_\ell, L_\ell \text{ devient } \underbrace{\overline{\mathbb{F}_\ell} \times \dots \times \overline{\mathbb{F}_\ell}}_{\lambda \text{ fois}}$$

$$\overline{A}_\ell = A_\ell \otimes \overline{\mathbb{F}_\ell} = \bigoplus_{i=1}^{\lambda} V_i \quad \dim V_i = \frac{2n}{\lambda}$$

V_i stables par $\underline{C}_\ell$ (qui agit par homothéties) et par $\underline{S}_\ell$.

De plus, le commutant (dans V_i) de $\underline{S}_\ell$ est $\simeq M_d$. Donc la repr. de $\underline{S}_\ell$ ds V_i est somme de d repr. irréd. isomorphes entre elles. Supposons qu'il existe i t.q. cette représentation irréductible soit 1. Alors $\dim V_i = d$, d'où $2n = \lambda d$.

Mais ceci entraîne que A est de type CM. Soit F un s/corps commutatif maximal de D contenant L . $[F:L] = d$, donc

$$[F:\mathbb{Q}] = \lambda d = 2n, \text{ ce qui entraîne CM.}$$

Lemme: Si K est assez grand, le groupe G_ℓ est engendré par $G_\ell^+ = [G_\ell : G_\ell]$ et par les s/g d'inertie en ℓ .

Soit G_ℓ' le s/g engendré par les groupes d'inertie en ℓ et G_ℓ^+ : $G_\ell \rightarrow G_\ell/G_\ell'$ abélien, et correspond à une extension de K non ramifiée, abélienne.

On remplace K par une extension contenant le corps de classes absolu de K .

Propriété (*): Pour tout ℓ assez grand, la conclusion du lemme est vrai.

Si (*) est vraie, et si K' est une extension finie de K , on a $G_\ell' = G_\ell$ pour ℓ grand.

Théorème:

Si (*) est vérifiée, l'image de $G_K = \text{Gal}(\bar{K}/K)$ dans $\prod_\ell G_\ell$ est ouverte.

Cette image décrit l'action de $\text{Gal}(\bar{K}/K)$ sur les points de A d'ordre sans facteur carré.
"Presque indépendant" de G_ℓ .

Corollaire:

Si A n'a pas de facteur de type CM, et si x est un point de A d'ordre N sans facteur carré, on a:

$$|G_K x| \geq c_\varepsilon N^{2-\varepsilon} \quad \text{pour tout } \varepsilon > 0.$$

où $c_\varepsilon > 0$ ne dépend que de ε, A, K

(peut être remplacé par $c N^{2-c'/\log \log N}$).

$$N = \ell_1 \dots \ell_k \quad |G_K x| \geq \frac{1}{c_\varepsilon} \prod |G_{\ell_i} x_i|$$

$$x = x_1 + \dots + x_k$$

$$\geq \prod \ell_i^2 / c^k$$

$k = w(N)$: nombre de facteurs premiers

$$>> N^2 / c^{w(N)}$$

$$c^{u(N)} \ll N^\varepsilon \quad \text{pour tout } \varepsilon > 0 \\ \ll N^{c/\log \log N}$$

A démontrer :

Il existe l_0 (dépend de A, k) tel que si $l_1, \dots, l_k$ sont distincts, et $> l_0$, alors l'homomorphisme

$$G_k \rightarrow G_{l_1} \times \dots \times G_{l_k}$$

est surjectif.

Ceci entraîne que $G_k \xrightarrow{\varphi} \prod G_{l_i}$ est surjectif.

Lemme de Goursat :

$H \subset G_1 \times G_2$ tel que $\text{pr}_1 H = G_1$, $\text{pr}_2 H = G_2$

(N_1, N_2, φ) N_1 s/g distingué de G_1

N_2 " " " G_2

$$\varphi: G_1/N_1 \xrightarrow{\sim} G_2/N_2$$

$\leadsto H = H(N_1, N_2, \varphi)$: l'ensemble des couples

(g_1, g_2) tels que $\varphi(\bar{g}_1) = \bar{g}_2$ où

$\bar{g}_i$: image de g_i mod N_i

Assertion: tout H ayant cette propriété est obtenue de façon unique à partir d'un triplet (N_1, N_2, φ) ,

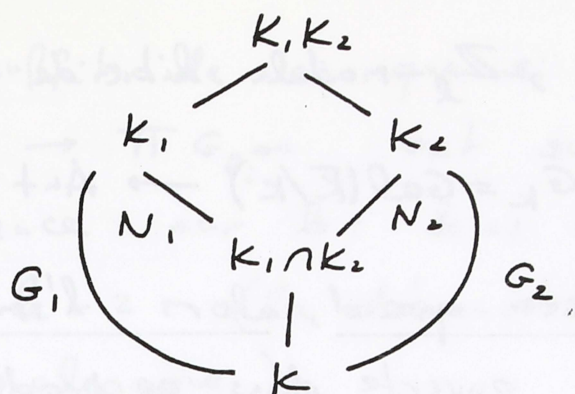
à savoir : $N_1 = H \cap G_1$, $G_1 = G \times \{1\}$

$$N_2 = H \cap G_2.$$

Par récurrence sur k :

Prelevons $k=2$

$$G_{l_1} \times G_{l_2} \supset H = \text{image de } G_k.$$



$$N_1 = H \cap G_{\ell_1}, \quad N_2 = H \cap G_{\ell_2}$$

$$G_K \rightarrow G_{\ell_1}/N_1 \xrightarrow{\sim} G_{\ell_2}/N_2 = \phi$$

à montrer: $\phi = (1)$.

Choisissons un quotient simple Σ de ϕ .

G_{ℓ_1} est engendré par le groupe d'inertie en ℓ_1 ,
et $G_{\ell_1}^+ = \text{dérivé}$.

Un groupe d'inertie en ℓ_1 a une image triviale dans ϕ .

ℓ_0 tel que tout $\ell \geq \ell_0$ est non ramifié dans K
et A a bonne réduction en ℓ .

Alors, Σ est non abélien, quotient de G_{ℓ_1} et
de G_{ℓ_2} . Montrons que ce n'est pas possible:

$$\mathfrak{S}_{\ell}(\mathbb{F}_{\ell}) \rightarrow G_{\ell_1}^+ \xrightarrow{\text{sur}} \Sigma \quad \ell \geq 5$$

donc Σ est "de Lie en car ℓ "

= (simple, simpl. connexe $(\mathbb{F}_{\ell^N})$ / centre

Si $\ell, \ell' \geq 5$, $\ell \neq \ell'$: aucun gp simple
de Lie de car ℓ n'est isom. à
de car ℓ' (Artin)

Exceptions: $SL_2(\mathbb{F}_4) = A_5 = PSL_2(\mathbb{F}_5)$,

$SL_3(\mathbb{F}_2) = PSL_2(\mathbb{F}_7)$, et 1 ou 2 autres)

Le même argument marche quand il y a plus
de 2 facteurs.

$T_\ell = T_\ell A = \varprojlim A_{\ell^n}$, $\mathbb{Z}_\ell$ -module libre de rang $2n$.

G_{ℓ^∞} = image de $G_K = \text{Gal}(K/k) \rightarrow \text{Aut}(T_\ell)$.

Th 1: Si K est assez grand, alors l'image de $G_K \rightarrow \prod_\ell G_{\ell^\infty}$ est ouverte dans ce produit.

Th 1': Il existe une suite croissante de corps K , de réunion $\bar{K}$, telle que pour chacun d'eux $G_K \rightarrow \prod_\ell G_{\ell^\infty}$ soit surjectif.

Les extensions de K données par les points de ℓ^∞ -division sont "presque" disjointes, quand ℓ varie.

(contre-exemple au Th 1 lorsque K n'est pas assez grand: A = courbe elliptique à m.c. par $\mathbb{Q}(\sqrt{d})$, $\mathbb{Q}(\sqrt{d}) \not\subset K$)

Rappel:

*2) Si K est assez grand, alors pour presque tout ℓ le groupe G_ℓ est engendré par les groupes d'inertie en les places de K divisant ℓ , et G_ℓ^+ (s/g engendré par les ℓ -éléments).

1^{ère} étape de la démonstration:

Soit K comme ci-dessus. Montrons qu'il existe $\ell_0 = \ell(A, K)$ tel que

$G_K \rightarrow \prod_{\ell \geq \ell_0} G_{\ell^\infty}$ est surjectif.

Il suffit de voir que si $l_0 \leq l_1 < \dots < l_k$,

$G_k \rightarrow \prod G_{l_i, \infty}$ est surjectif.

Réurrence sur k : $k=1$ est trivial. Faisons-le pour $k=2$ (la démonstration est la même pour k quelconque).

Propriétés de l_0 : assez grand pour que si $l \geq l_0$, on ait

- A a bonne réduction en l
- $(*_l)$ est vraie
- $G_l^+ = \underline{S}_l(\mathbb{F}_l)^+$
- $l_0 \geq 5$.

Alors, $G_k \rightarrow G_{l_1, \infty} \times G_{l_2, \infty}$ est surjectif.

Par le lemme de Goursat il suffit de démontrer qu'il n'existe pas d'homomorphisme $G_k \rightarrow \phi$, $\phi \neq \{1\}$, qui se factorise à la fois par $G_{l_1, \infty}$ et par $G_{l_2, \infty}$. On peut supposer ϕ fini, simple.

Trois cas:

a.) $\phi = \mathbb{Z}/l\mathbb{Z}$, $l \neq l_1$

$$1 \rightarrow \underbrace{G(l_1)}_{\text{pro } l\text{-groupe}} \longrightarrow G_{l_1, \infty} \longrightarrow G_{l_1} \longrightarrow 1$$

$$\begin{array}{ccc} & G_{l_1} & \\ & \nearrow & \searrow \\ G_{l_1, \infty} & \xrightarrow{\text{surj.}} & \phi \end{array}$$

groupe d'inertie en $l_1 \rightarrow 1$ en $G_{l_2, \infty}$,
donc en ϕ .

le groupe $G_l^+ = [G_l^+, G_l^+]$, donc $\rightarrow 1$.

b.) $l \neq l_2$, même preuve

c.) ϕ simple non abélien

$$\begin{array}{ccc} & G(l_1) & \\ \nearrow & & \searrow \\ G_{l_1, \infty} & \longrightarrow & \phi \end{array}$$

ϕ est du type Lie de car. l_1

— " ————— l_2

impossible si $l_1, l_2 \geq 5$

2^{ème} étape

Soit $\mathcal{A}$ l'image de G_k dans $\prod_{l < l_0} G_{l, \infty}$

$\mathcal{A}$ est ouvert dans $\prod_{l < l_0} G_{l, \infty}$

$$\mathcal{B} = \prod_{l \geq l_0} G_{l, \infty}$$

$$G_k \longrightarrow \mathcal{A} \times \mathcal{B} \quad \text{proj. surjectives}$$

Par Goursat, il suffit de prouver que si

$G_k \rightarrow \phi$, ϕ profini, se factorise par $\mathcal{A}$ et $\mathcal{B}$,
alors ϕ est fini.

$|\mathcal{A}|$ n'est divisible que par un nombre fini de nombres premiers, donc idem pour ϕ

$$|\phi| = \prod_{l \leq M} l^{\psi(l)}$$

$$\psi(l) \in \{0, 1, 2, \dots, \infty\}.$$

A montrer: $\psi(l) \neq \infty$ pour tout l .

Lemme:

Si $l > M$, l'image dans ϕ de $G_{l\infty}$, ou
comme s/q de $B = \prod_{l \geq l_0} G_{l\infty}$, est triviale.

$$G(l) \subset G_{l\infty} \longrightarrow \phi$$

pro l -gpe :
 image triviale
 ds ϕ

inertie en $l \rightarrow 1$ dans ϕ

$G_l^+ \rightarrow 1$, car eng. par l -éléments

ϕ est quotient de $\pi \subset \prod_{l < l_0} G_{l\infty}$, donc
 " " " $\prod_{l_0 < l < M} G_{l\infty}$.

Si $l < l_0$, l'exposant de l dans $\prod_{l_0 \leq l \leq M} G_{l\infty}$
 est fini.

Si $l > l_0$, l'exposant de l dans π est fini.
 Donc l'exposant de l dans ϕ est fini.

$G_{l\infty}$ contient "beaucoup" d'homothéties:

$G_{l\infty} \cap \mathbb{Z}_l^*$ (homothéties de $T_l A$) est
 ouvert dans $\mathbb{Z}_l^*$

Soit $e(l)$ l'indice de $G_{l\infty} \cap \mathbb{Z}_l^*$ dans $\mathbb{Z}_l^*$.

Conjecture: $e(l) = 1$ pour l assez grand.

Théorème 2: $e(l)$ est borné quand l varie.

Equivalent: il existe une constante $c \geq 1$ telle que
 toute homothétie qui est une puissance c ième
 appartient à $G_{l\infty}$, et même:

Corollaire :

Tout élément de $\hat{Z}^* = \prod_{\ell} Z_{\ell}^*$ qui est une puissance c -ième, appartient à G_{∞}
 (où G_{∞} est l'image de G_k dans $\prod G_{\ell^{\infty}}$).

(suffit à échauffer, par un argument bien connu de Lang, que toute courbe de genre ≥ 2 sur une variété abélienne ne contient qu'un nombre fini de points de torsion. Ceci a été démontré par Raynaud d'une autre façon.)

Th :

Si A n'a pas de facteur ($\neq 0$) de type CM,
 on a, pour tout $\varepsilon > 0$:

$$|G_k x| \geq c \cdot N(x)^{2-\varepsilon}$$

pour tout $x \in A(\bar{K})$ d'ordre fini $N(x)$,

où $c = c(A, K, \varepsilon) > 0$.

On peut le remplacer par $c' N(x)^{2-c''/\log \log N(x)}$
 (même démonstration que la dernière fois).

$G_{\ell^{\infty}}$ ouvert d'un $\underline{H}_{\ell^{\infty}}(\mathbb{Q}_{\ell})$, où
 $\underline{H}$ est un groupe réductif connexe,
 $\underline{H} = \underline{C}_{\ell^{\infty}} \cdot \underline{S}_{\ell^{\infty}}$,

$\underline{C}$ est un tore qui provient par extension des scalaires $\mathbb{Q}_{\ell}/\mathbb{Q}$ d'un tore $\underline{C}$ sur $\mathbb{Q}$.

$C \subset T_L$, où $L = \text{centre de } \mathbb{Q} \otimes \text{End } A$

(e.g. $\text{End } A = \mathbb{Z}$, $L = \mathbb{Q}$, $T_L = G_m$, $C = G_m$).

$C(\mathbb{Z}_\ell)$ a un sens pour presque tout ℓ .
 $c(\ell) = \text{indice de } G_{\ell^\infty} \cap C(\mathbb{Z}_\ell) \text{ dans } C(\mathbb{Z}_\ell)$
 $< \infty$.

Th 2* : $c(\ell)$ est borné quand ℓ varie

$\Rightarrow$ Th 2, car $C > G_m$, et $C(\mathbb{Z}_\ell) > \mathbb{Z}_\ell^*$.

(Il est faux que $c(\ell) = 1$ pour ℓ grand.

e.g. considérer 4 courbes elliptiques à m.c. par $\mathbb{Q}(\sqrt{-a})$, $\mathbb{Q}(\sqrt{-b})$, $\mathbb{Q}(\sqrt{-c})$ et $\mathbb{Q}(\sqrt{-abc})$, a, b, c premiers ≥ 2

$A =$ produit de ces 4 courbes : alors $c(\ell) \geq 2$.

Démonstration des Th 2 (2^*) en supposant $\text{End } A = \mathbb{Z}$.

Choisissons une polarisation sur A , et supposons ℓ premier au degré de cette polarisation.

Donne une forme alternée sur $T_\ell A$ non dégénérée sur $\mathbb{Z}_\ell$.

$$s \in G_K, \quad s x \cdot s y = \chi_{\ell^\infty}(s) x \cdot y$$

$$G_{\ell^\infty} \subset G \text{Sp}_{2n}(\mathbb{Z}_\ell).$$

Définition : $Y \subset \text{Sp}_{2n}(\mathbb{Z}_\ell)$. Un élé $y \in \text{Sp}_{2n}(\mathbb{Z}_\ell)$ appartient à Y si et seulement si il existe $u \in \mathbb{Z}_\ell^*$ tel que $u \cdot y \in G_{\ell^\infty}$.

$U = \mathbb{Z}_\ell^* \cap G_{\ell^\infty}$ d'indice $c(\ell)$ dans $\mathbb{Z}_\ell^*$.
 y donnée, "son u " est bien déterminée mod U .

$y \mapsto u$ d'où un hom. $\lambda: Y \rightarrow \mathbb{Z}_\ell^*/U$.

Cet homomorphisme est surjectif si l est grand.

En effet, si $u \in \mathbb{Z}_l^*$,

$$\chi_{l^\infty} : G_K \rightarrow \mathbb{Z}_l^* \quad \text{est surjectif}$$

donc il existe un $s \in G_K$ avec $\chi_{l^\infty}(s) = u^2$

un tel $s \rightarrow x \in G_{l^\infty}$.

$$G_{Sp_{2n}} \xrightarrow{N} G_m \quad \text{fact. de similitude}$$

$$\text{On a } N(x) = u^2$$

Si $y = u^{-1}x$, $N(y) = u^{-2} \cdot u^2 = 1$, donc

$y \in Sp_{2n}(\mathbb{Z}_l)$, $y \in Y$, et $y \mapsto u$.

Je suis donc ramené à montrer:

(1) $Y^{(ab)}$ est d'ordre borné quand l varie.

Soit Y_l l'image de Y par l'homomorphisme $Sp_{2n}(\mathbb{Z}_l) \rightarrow Sp_{2n}(\mathbb{F}_l)$, réduction mod l .

(2) Supposons $l \geq 3$. Pour qu'un élément $z \in Sp_{2n}(\mathbb{F}_l)$ appartienne à Y_l , il faut et il suffit qu'il existe $v \in \mathbb{F}_l^*$ avec $vz \in G_l$.

Notons $y \mapsto \bar{y}$ la réduction mod l . Si

$$z = \bar{y}, \quad u \cdot y = x \in G_{l^\infty}, \quad \bar{u} \cdot \bar{y} = \bar{x} \in G_l.$$

Inversement, supposons qu'on ait $v \in \mathbb{F}_l^*$, $vz \in G_l$.

$$N(vz) = v^2 \in \mathbb{F}_l^{*2}. \quad \text{Il existe un } x \in G_{l^\infty}$$

$$\text{avec } \bar{x} = vz, \quad Nx = \lambda, \quad \bar{\lambda} = v^2. \quad \text{Donc}$$

$$\lambda = u^2, \quad \text{avec } \bar{u} = v. \quad y = u^{-1}x, \quad Ny = 1$$

$$\bar{y} = v^{-1}vz = z.$$

(3) Y_l contient G_l^+

car G_l^+ étant engendré par les l -éléments,

et étant son groupe dérivé, est contenu dans

$$\mathrm{Sp}_n(\mathbb{F}_\ell).$$

l'gd, $G_\ell^+ = \underline{S}(\mathbb{F}_\ell)^+ = \text{image de } \underline{\tilde{S}}(\mathbb{F}_\ell) \rightarrow \underline{S}(\mathbb{F}_\ell)$
 $\underline{\tilde{S}}$: revêtement universel de $\underline{S}$.

$$\underline{S} \subset \mathrm{Sp}_n / \mathbb{F}_\ell \quad (\text{faible})$$

$$G_\ell \subset \underline{H}_\ell(\mathbb{F}_\ell), \quad \underline{H}_\ell = G_m \cdot \underline{S}_\ell \quad (\text{car } \mathrm{End} = \mathbb{Z})$$

$$Y_\ell \subset \underline{H}_\ell(\mathbb{F}_\ell) \cap \mathrm{Sp}_{2n}(\mathbb{F}_\ell)$$

$$\text{Soit } \underline{S}' = \underline{H}_\ell \cap \mathrm{Sp}_{2n} / \mathbb{F}_\ell$$

$$(4) \quad \text{On a } S_\ell' = \{\pm 1\} \cdot S_\ell$$

$$\lambda \cdot x, \quad N(\lambda x) = 1, \quad N\lambda = \lambda^2 = 1 \Rightarrow \lambda = \pm 1.$$

$$Y_\ell^\circ = Y_\ell \cap \underline{S}_\ell(\mathbb{F}_\ell)$$

$$(5) \quad Y_\ell^\circ \text{ est d'indice } \leq 2 \text{ dans } Y_\ell.$$

$$G_\ell^+ \subset Y_\ell^\circ \subset \underline{S}_\ell(\mathbb{F}_\ell)$$

l'indice de G_ℓ^+ dans $\underline{S}_\ell(\mathbb{F}_\ell)$ est borné.

$$(\leq 2^{rg}, \text{ donc } \leq 2^n).$$

$$(6) \quad \text{L'indice de } G_\ell^+ \text{ dans } Y_\ell \text{ est borné}$$

$$\text{Si } \ell \text{ est grand, } (G_\ell^+)^{ab} = 1$$

$$(7) \quad Y_\ell^{ab} \text{ est d'ordre borné.}$$

$$1 \rightarrow \underbrace{Y(\ell)} \rightarrow Y \rightarrow Y_\ell \rightarrow 1$$

noyau de la
réduction mod ℓ = pro ℓ -groupe

On veut prouver que si ℓ est assez grand, $Y^{ab} \rightarrow Y_\ell^{ab}$ est un isom.

(i.e. $Y(\ell) \subset \text{groupe dérivé de } Y$).

Il suffit de prouver :

$$(8) \quad \text{il n'y a pas d'homomorphisme}$$

97
 $f: Y(l) \rightarrow \mathbb{Z}/l$ invariant par Y ,
 -dire $f(yzy^{-1}) = f(z) \quad \forall y \in Y(l)$.

$Y(l)$ en définissant:
 $\{y \in Y \mid y \equiv 1 \pmod{l^N}\} \}_{N=1,2,\dots}$
 $Y(l^2) \supset \dots \supset Y(l^N) \supset \dots$
 $V_N = Y(l^N) / Y(l^{N+1}) \hookrightarrow \text{Sp}_{2n}(\mathbb{F}_l)$

$$\cap$$

 $u \mapsto u \pmod{l} \quad \text{SL}_{2n}(\mathbb{F}_l)$
 $\text{sl}_{2n}/\mathbb{F}_l$

uniques, donc compatibles avec l'action
 ramené à prouver:

l grand, il n'existe pas de sous-espace
 de $\text{sl}_{2n}/\mathbb{F}_l$, et de forme
 non nulle $f: \underline{V} \rightarrow \mathbb{F}_l$ tels que:
 - est stable par conjugaison par Y_l .
 $f(yzy^{-1}) = f(z) \quad y \in Y_l, z \in \underline{V}$.

l est grand, l'action de G_l^+ par
 conjugaison sur $\text{sl}_{2n}/\mathbb{F}_l$ est semi-simple
 ne contient pas la représentation unité.
 $\mathfrak{u} = \text{scal} \oplus \text{sl}_{2n}$

(9) $\Rightarrow \dots \Rightarrow (1)$.

à démontrer (10)

me échoue avec $\tilde{S}_l$ (ou S_l , c'est
 pareil)

98
 dans A_l
 semi-simple, et
 fidèle.

et de repr.
 d'une alg. de

est "l-restreinte"

r. semi-simple
 sauf pour
 ablement

te', commuterait
 contredirait

à $\tilde{S}_l(\mathbb{F}_l)$

tre $\times$ semi-sim

nothétiques

tant aux

et de $\det_L :=$
 rec $u, y \in G_{l^{\infty}}$.

Les pages 97 et 98 se superposent dans le document original.

① il suffit de prouver γ^{ab} d'ordre borné 99
 $\gamma^{ab} \rightarrow C(\mathbb{Z}_\ell)/U$, $U = C(\mathbb{Z}_\ell) \cap G_{\ell^\infty}$

avec indice borné (théorie abélienne).

sl $\leftrightarrow$ matrices commutant à $\text{End } A$ et
 de trace 0/L.

Aujourd'hui on va démontrer 2 énoncés:

l'an dernier, on a défini $G_{\ell\infty}$ et son enveloppe algébrique

$\underline{H}_{\ell\infty}$, groupe réductif / $\mathbb{Q}_{\ell}$

cette année, G_{ℓ} et son enveloppe algébrique $\underline{H}_{\ell} / \mathbb{F}_{\ell}$

1.) Les rangs de tous les $\underline{H}_{\ell\infty}$ et $\underline{H}_{\ell}$ sont les mêmes (et sont indépendants de ℓ)

2.) Si $\text{End } A = \mathbb{Z}$ et si $\dim A = 2, 6$ ou impair, alors $G_{\ell\infty} = \text{GSp}_{2n}$ pour ℓ grand, et $G_{\ell} \subset \prod G_{\ell\infty}$ est ouvert dans le groupe adélique de GSp_{2n} .

Le rang de $\underline{H}_{\ell\infty}$ est indépendant de ℓ .

$N = 2n$, $H \subset \text{GL}_N$, H réductif connexe

$$\text{GL}_N \rightarrow \text{Aff}_*^N$$

Aff_*^N : espace des polynômes unitaires $X^N + a_1 X^{N-1} + \dots + a_N$ avec a_N inversible.

$$\text{cl} : \text{GL}_N \rightarrow \text{Aff}_*^N$$

$x \mapsto$ polynôme caractéristique de x .

L'image de H par cl est une sous-variété fermée de Aff_*^N définie sur $\mathbb{Q}$, de $\dim =$ rang de H .

Si H est un tore, cl est un morphisme fini.

Si $T \subset H$ est un tore maximal, alors

$$\text{cl}(T) = \text{cl}(H).$$

Si $h_i \in H$ sont zariski-denses, alors $\text{cl}(H)$ est l'adhérence (de zariski) des $\text{cl}(h_i)$.

$\mathcal{A}(\mathcal{H}_{\ell\infty}) = \text{Zariski-adh\u00e9rence des } \mathcal{A}(\text{Frob}_v),$
 v bonne r\u00e9d, $v \notin S$ fini.

Remarque:

$\mathcal{H}_{\ell\infty} = C \cdot S_{\ell\infty}$, S semi-simple, C tore / $\mathbb{Q}$.
 $C \subset GL_N$

Les groupes $\mathcal{H}$ r\u00e9ductifs convexes \u00e0 tore central C fix\u00e9 sont en nombre fini (a conjugaison g\u00e9om\u00e9trique pr\u00e8s).

En particulier, les vari\u00e9t\u00e9s $\mathcal{A}(\mathcal{H})$ possibles (pour C fix\u00e9) sont en nombre fini: $V_1, \dots, V_k$.
 On suppose que $\mathcal{A}(\mathcal{H}_{\ell\infty}) = V_1$ pour tout ℓ .
 $r = \dim V_1 = \text{rang}$ (V_i irr\u00e9d).

Supposons ℓ assez grand. $\mathcal{H}_{\ell} = \underline{C}_{\ell} \cdot \underline{S}_{\ell}$,
 S_{ℓ} semi-simple commutant \u00e0 $\underline{C}_{\ell}$ engendr\u00e9 par des exponentielles, et op\u00e9rant de fa\u00e7on semi-simple.
 En fait, si ℓ est assez grand, un tel $\mathcal{H}_{\ell}$ provient g\u00e9om\u00e9triquement par r\u00e9duction mod ℓ d'un groupe analogue en $\text{car } 0$.

$V_{i,\ell} = \text{r\u00e9d. mod } \ell \text{ de } V_i$

Si ℓ est assez grand, $\mathcal{A}(\mathcal{H}_{\ell}) = V_{i,\ell}$, ℓ

A monter: $i_{\ell} = 1$ pour tout ℓ

1\u00e8re \u00e9tape: $\mathcal{A}(\mathcal{H}_{\ell}) \supset V_{1,\ell}$ pour ℓ assez grand.

Soit J l'ensemble des i tels que $V_i \not\subset V_1$.

Si $i \in J$, $V_1 \cap V_i$ est une sous-vari\u00e9t\u00e9 de V_1 de dimension $\leq r-1$, $r = \dim V_1$.

On choisit une place v dont le Frobenius σ_v satisfait : $\mathcal{d}(\sigma_v) \notin \bigcup_{i \in J} V_i(\mathbb{Q})$

(possible car les Frob. sont Zariski-denses).

Donc pour l assez grand, $\sigma_v \bmod l \in H_l(\mathbb{F}_l)$

satisfait : $\mathcal{d}(\sigma_v) \notin V_i(\mathbb{F}_l)$, $i \in J$.

donc $\mathcal{d}(\underline{H}_l) \neq V_{i,l}$, $i \in J$,

donc $V_{1,l} \subset \mathcal{d}(\underline{H}_l)$.

Ceci entraîne : $\text{rang } \underline{H}_l \geq r = \dim V_1$
pour l grand.

2^{ème} étape. Montrer que $\text{rang } \underline{H}_l \geq r+1$ est impossible.

Avec la 1^{ère} étape, ça entraînera $\mathcal{d}(\underline{H}_l) = V_{1,l}$.

Démonstration de la 2^{ème} étape.

$G_l \subset_{\text{borné}} \underline{H}_l(\mathbb{F}_l)$

$\mathcal{d}(G_l) \subset \text{Aff}_{2n}^{\text{sym}}(\mathbb{F}_l)$.

On va estimer $|\mathcal{d}(G_l)|$ de 2 façons différentes.
1^{ère} estimation:

On choisit un tore maximal (H) de $\underline{H}_l$,
défini $/\mathbb{F}_l$.

Lemme:

Si T est un tore $/\mathbb{F}_l$ de dimension s ,

$$|T_l(\mathbb{F}_l)| \geq l^s \left(1 - \frac{1}{l}\right)^s = (l-1)^s.$$

"

$\prod (l - \varepsilon_i)$

racines de 1

$$|(H)(\mathbb{F}_l)| \geq c_n l^{n+1} \gg l^{r+1}$$

(e.g. $c_n = (\frac{1}{2})$)

$s \leq 2n$, $(1 - \frac{1}{l})^{2n} \geq (\frac{1}{2})^{2n}$, c_n ne dépend que de n

$$|G_\ell \cap \bigoplus (\mathbb{F}_\ell)| \geq c' |\bigoplus (\mathbb{F}_\ell)| \gg \ell^{r+1} \quad \ell \rightarrow \infty$$

Si $T \subset GL_N$, l'application

$$d: T \rightarrow \text{Aff}_n^N$$

est de degré au plus $N!$

$$|d(G_\ell)| \geq |d(G_\ell \cap \bigoplus (\mathbb{F}_\ell))| \geq \frac{1}{(2n)!} |G_\ell \cap \bigoplus (\mathbb{F}_\ell)| \gg \ell^{r+1}$$

$$(a) \quad |d(G_\ell)| \gg \ell^{r+1}$$

G_ℓ = réduction modulo ℓ de G_{ℓ^∞} .

$$\text{Si } x \in G_{\ell^\infty}, d(x) \in V_1(\mathbb{Q})$$

d'où $d(G_\ell) \subset V_1(\mathbb{F}_\ell)$ pour presque tout ℓ .

$$|V_\ell(\mathbb{F}_\ell)| \leq \ell^r \quad \text{car } \dim V_1 = r.$$

d'où $|d(G_\ell)| \leq \ell^r$, contradiction.

2.) Supposons $\text{End } A = \mathbb{Z}$. Soit $n = \dim A$

Appelons r le rang commun des groupes

$$\underline{H}_{\ell^\infty}, \underline{H}_\ell.$$

$$\underline{H}_{\ell^\infty} = \mathbb{G}_m \cdot \underline{S}_{\ell^\infty}, \quad \underline{H}_\ell = \mathbb{G}_m \cdot \underline{S}_\ell.$$

$$\underline{H}_{\ell^\infty} \subset GSp_{2n}, \quad \underline{S}_{\ell^\infty} \subset Sp_{2n}$$

de même mod ℓ .

$$1.) \quad r \leq n+1$$

On avait vu que si $r = n+1$, alors

$$\underline{S}_{\ell^\infty} = Sp_{2n} \quad \text{pour tout } \ell$$

$$\underline{H}_{\ell^\infty} = GSp_{2n}$$

$$(S \subset Sp_{2n}, \text{rg } S = \text{rg } Sp_{2n})$$

Faltings + $\text{End } A = \mathbb{Z}$: S et Sp_{2n} ont le même commutateur: les scalaires).

Borel - de Siebenthal (voir oeuvres de Borel vol. 1, et Bourbaki Lie $\mathfrak{g}$).

Si $S_1 \subset S_2 \subset GL_N$ sont semi-simples de cor 0 et ont même rang, même commutant, alors $S_1 = S_2$.

Borel et de Siebenthal donnent une description des groupes semi-simples de même rang.

Si $S_1 \neq S_2$, il existe un s_2 non central dans S_2 qui commute à S_1 .

2.) Si $r = n+1$, $S_{\ell\infty} = Sp_{2n}$ pour tout ℓ

$H_{\ell\infty} = GSp_{2n}$ pour tout ℓ

(corollaire: si $S_{\ell\infty} = Sp_{2n}$ pour un ℓ , alors c'est vrai pour tout ℓ .)

On a montré: si $n=2,6$ ou impair et si:

$\text{End } A = \mathbb{Z}$, alors $r = n+1$, $H_{\ell\infty} = GSp_{2n}$.

Reste à montrer:

Théorème:

Si $\text{End } A = \mathbb{Z}$ et $r = n+1$, alors

a.) $G_{\ell\infty} = GSp_{2n}(\mathbb{Z}_{\ell})$ ℓ grand

b.) Image de G_K dans $\prod G_{\ell\infty}$ est ouverte dans le groupe adélique de GSp_{2n}

c.) $G_{\ell} = GSp_{2n}(\mathbb{F}_{\ell})$ pour ℓ grand

d.) $\underline{H}_{\ell} = GSp_{2n} / \mathbb{F}_{\ell}$.

On prouve d'abord que $\underline{H}_{\ell} = GSp_{2n} / \mathbb{F}_{\ell}$

(ℓ grand). On en déduit que pour ℓ grand

$G_{\ell} = GSp_{2n}(\mathbb{F}_{\ell})$. D'où $G_{\ell\infty} = GSp_{2n}(\mathbb{Z}_{\ell})$.

et b.) résulte du thm de la fois précédente.

On se donne une polarisation sur A . Elle fournit 105
 une forme symplectique qui n'est pas nécessairement
 non dégénérée mod l pour tout l . Il y a (au moins)
 deux façons de résoudre ce problème: on remplace
 A par une variété isogène, munie d'une
 polarisation principale, ou bien on prend l
 assez grand pour que la forme soit non
 dégénérée mod l .

A voir: $\underline{S}_l = Sp_{2n}/F_l$, l grand.

$\underline{S}_l \subset Sp_{2n}/F_l$ l grand

$(G_l^+ \subset Sp_{2n}/F_l)$

$\underline{S}_l \subset Sp_{2n}/F_l$ semi-simples, même commutant
 (Lunottéties) même rang.

Le théorème de Borel-^{de} Siebenthal est vrai
 en $\text{car} \geq 5$, mais il est faux en $\text{car. } 2, 3$.

Contre-exemple: en $\text{car } 2$

$SO_{2n} \not\subset Sp_{2n}$ $n \geq 2$, SO_{2n} abs. irréd.

$\parallel$
 C_n

Sp_{2n} aussi:

même rang

$\text{car } 3$: $A_2 \subset G_2$ plongement bizarre.

G.M. Seitz "Maximal subgroups of classical
 algebraic groups".

$T \subset S$ S semi-simple, $T \subset S' \subset S$ à décrire.

Racines: R , $\alpha \in R$ U_α s/g à un paramètre

$S = \langle T, U_\alpha \rangle$

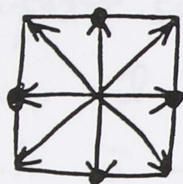
$$S' = \langle T, U_\alpha, \alpha \in R' \rangle \quad R' \subset R.$$

$$1.) \quad \alpha \in R' \Rightarrow -\alpha \in R'$$

R' système de racines de S' , $R' \subset R$.

$$2.) \quad \text{En car } \geq 5, \text{ si } \alpha, \beta \in R' \text{ et } \alpha + \beta \in R, \\ \text{alors } \alpha + \beta \in R'.$$

Sp_4

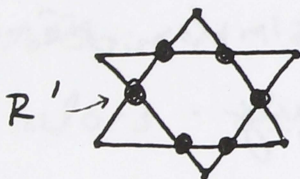


racines courtes ne satisfont pas 2.)

Racines longues sat. 2.)

$Sp_2 \times Sp_2 \subset Sp_4$ donc racines longues

G_2



R' ^(racines courtes) ne vérifie pas 2.)

et est impossible en car $\neq 7$.

$$x_\alpha(t) \in U_\alpha$$

$$[x_\alpha(t), x_\beta(t')] = x_\beta(t) \cdot x_\alpha(t') - x_{\alpha+\beta}(\dots) x_{\alpha+\beta}(\dots)$$

$\uparrow$
 $t \cdot t'$

$$\gamma = \pm 1, \pm 2, \pm 3$$

Si car $\neq 2, 3$, on est obligé d'avoir $\alpha + \beta$.

$$\Gamma \text{ s/g de } \mathbb{Z}R, \quad R'_\Gamma = \Gamma \cap R$$

En faisant varier Γ , on trouve tous les systèmes satisfaisant 1.) et 2.)

$$\text{On a donc } \underline{S}_\ell = Sp_{2n} / \mathbb{F}_\ell.$$

Pour ℓ grand, on avait vu que G_ℓ contient l'image de $\tilde{S}_\ell(\mathbb{F}_\ell) \rightarrow \underline{S}_\ell(\mathbb{F}_\ell)$

Ici $\underline{S}_\ell = \tilde{S}_\ell = Sp_{2n}$. Donc $G_\ell \supset Sp_{2n}(\mathbb{F}_\ell)$,
l'grand.

$$1 \rightarrow \mathrm{Sp}_{2n}(\mathbb{F}_\ell) \rightarrow \underset{\substack{\cup \\ G_\ell}}{\mathrm{GSp}_{2n}(\mathbb{F}_\ell)} \xrightarrow{N} \mathbb{F}_\ell^\times \rightarrow 1$$

107

$N: G_\ell \rightarrow \mathbb{F}_\ell^\times$ caractère cyclotomique
surjectif.

Donc: $G_\ell = \mathrm{GSp}_{2n}(\mathbb{F}_\ell)$.

Théorème:

Si $\ell \geq 5$, tout sous-groupe fermé de $\mathrm{Sp}_{2n}(\mathbb{Z}_\ell)$
ayant pour réduction mod ℓ le groupe $\mathrm{Sp}_{2n}(\mathbb{F}_\ell)$
est égal à $\mathrm{Sp}_{2n}(\mathbb{Z}_\ell)$.

(Serait faux pour $\ell=2,3$, $n=1$. Voir McGill et correction).

Avant de démontrer ce théorème, montrons qu'il entraîne l'énoncé avec GSp .

On applique le théorème à l'adhérence H du groupe dérivé de G_{ℓ^∞} . Ce groupe est contenu dans $\mathrm{Sp}_{2n}(\mathbb{Z}_\ell)$, et son image mod ℓ est le groupe dérivé de G_ℓ , i. e. $\mathrm{Sp}_{2n}(\mathbb{F}_\ell)$.

D'où $H = \mathrm{Sp}_{2n}(\mathbb{Z}_\ell)$. On conclut comme tout à l'heure: $N: G_{\ell^\infty} \rightarrow \mathbb{Z}_\ell^\times$ est surjectif (caractère cyclotomique).

Démonstration du théorème:

$S = \mathrm{Sp}_{2n}(\mathbb{Z}_\ell)$, $H \subset S$ donne.

$$S \supset S_1 \supset \dots \supset S_m \supset \dots$$

$$\text{ou } S_m = \{s \in S \mid s \equiv 1 \pmod{\ell^m}\}.$$

$$S/S_1 = \text{Sp}_{2n}(\mathbb{F}_\ell)$$

S_i/S_{i+1} s'identifie à l'algèbre de Lie $\text{sp}_{2n}(\mathbb{F}_\ell)$
de Sp_{2n} sur $\mathbb{F}_\ell$:

$$s = 1 + \ell^i x, \quad s \in S_i \mapsto x \bmod \ell \in \mathfrak{p}_{2n}$$

A monter: $\mathbb{H} \rightarrow S/S_i$ est surjectif $\forall i$

Par récurrence sur i :

Il suffira de voir que $\mathbb{H}/S_{i+1}$ contient S_i/S_{i+1} .
Fabriquer dans $\mathbb{H}$ $1 + \ell^i x \bmod S_{i+1}$
pour x quelconque $\in \text{sp}_{2n}(\mathbb{F}_\ell)$

(Tits: il suffit de le voir pour un seul x ,
car action irréductible.)

("avec Tits") Dans l'algèbre de Lie de Sp_{2n} ,
a.T. il y a au moins un $x \neq 0$, $x^2 = 0$.

("sans Tits") L'algèbre de Lie de Sp_{2n} est
s.T. engendrée $/\mathbb{F}_\ell$ par des x , $x^2 = 0$
(vrai même si $\text{car} = 2$).

(a.T.) $x = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$

(s.T.) e.g. SL_2 : $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

$$\exp(x) = 1 + x \in \text{Sp}_{2n}(\mathbb{F}_\ell)$$

Il existe $s = 1 + t \in \mathbb{H}$ avec $t \equiv x \bmod \ell$

$$s^\ell = 1 + \ell t + \frac{\ell(\ell-1)}{2} t^2 + \dots + \ell t^{\ell-1} + t^\ell$$

$$t^2 \equiv 0 \bmod \ell$$

$$t^\ell \equiv 0 \bmod \ell^2 \quad \text{si } \ell \geq 5$$

$$s^l \equiv 1 + lt \pmod{S_2}.$$

$$s^{l^2} \equiv 1 + l^2 t \pmod{S_3}, \text{ etc.}$$

Conjecture :

H_{l^∞} = groupe de Mumford-Tate $/\mathbb{Q}_l$

$\underline{H}_l$ = réduction mod l de M.T.

Démontrables (?) :

① G_{l^∞} contient l'image de
 $\tilde{S}_{l^\infty}(\mathbb{Z}_l) \rightarrow S_{l^\infty}(\mathbb{Z}_l)$ (l assez grand)

et $\underline{S}_l$ est la réduction mod l de $\underline{S}_{l^\infty}$

$$\begin{array}{c} \tilde{S}_l^\infty(\mathbb{Z}_l) \\ \downarrow \\ G_{l^\infty} \cap S_{l^\infty}(\mathbb{Z}_l). \end{array}$$

l'image inverse est ~~contenue dans~~ un
compact maximal "superspécial" dans la
terminologie de Bruhat-Tits.

② Extension des résultats aux corps de type
fini sur $\mathbb{Q}$:

les résultats sont ^{très} probablement exactement
 les mêmes que sur $\mathbb{Q}$.

On a utilisé :

- Hermite: il n'y a qu'un nombre fini
 d'extensions de degré donné, et
 non ramifiées en dehors d'un ensemble fini
 fixe'.

- Théorème de finitude du corps de classes:
extension abélienne maximale non ramifiée partout
de degré fini (Katz-Lang).

③ Corps de fonctions d'une variable sur un
corps fini.

($l \neq$ caractéristique)

On définit $\mathbb{H}_{l,\infty}$: enveloppe algébrique de
Galois.

Il n'est plus vrai en général que $G_{l,\infty} \subset \mathbb{H}_{l,\infty}$
soit ouvert, à cause de la partie abélienne

$$\mathbb{H}_{l,\infty} = C \cdot \underline{S} \quad \text{proj. de } \underline{S} \text{ ouverte}$$

$$\begin{array}{ccc} \text{proj. dans } C : & \hat{\mathbb{Z}} & \rightarrow C(\mathbb{Q}_l) \\ G_k \xrightarrow{\text{degré}} \mathbb{Z} & & \text{action sur } \overline{\mathbb{F}_q} \end{array}$$

(s/g de $\mathbb{Z}_l^*$ engendré par les puissances de p
mod l , on définit G_l^+ , C_l
mais G_l n'est pas d'indice borné dans $\mathbb{H}_l$ (A

Fin du Cours