JEAN-PIERRE SERRE
J.-F. BOUTOT (réd.)
J. OESTERLÉ (réd.)

Groupes de Galois et représentations ℓ-adiques

Cours de Jean-Pierre Serre, tome 5 (1984)
<http://www.numdam.org/item?id=CJPS_1984__5_>

ANNUAIRE

DU

COLLÈGE DE FRANCE
1984-1985

Algèbre et géométrie

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

RÉSUMÉ
DES COURS ET TRAVAUX

85e année

PARIS

11, place Marcelin-Berthelot (Ve)

I. SCIENCES MATHÉMATIQUES, PHYSIQUES ET NATURELLES

Algèbre et géométrie

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

Les résultats récents de G. FALTINGS (*Invent. Math.* 73 (1983), 349-366) permettent de comprendre un peu mieux les propriétés des représentations ℓ-adiques, notamment dans le cas des variétés abéliennes. Le cours en a exploré deux aspects :

1) critère effectif permettant de reconnaître l'isomorphisme de deux représentations ;

2) détermination des enveloppes algébriques des groupes de Galois ℓ-adiques.

Un troisième aspect, celui de la « variation des groupes de Galois avec ℓ » fera l'objet du cours de 1985-1986.

1. *Critère effectif d'isomorphisme. Corps quartiques et isogénies*

1.1. *Le groupe déviation* $\tilde{G}$ (FALTINGS, *loc. cit.*, § 6)

Soient $\rho_1 : G \to \mathbf{GL}(V_1)$ et $\rho_2 : G \to \mathbf{GL}(V_2)$ deux représentations linéaires d'un groupe G dans des $\mathbf{Q}_\ell$-espaces vectoriels V_1 et V_2 de dimension $d < \infty$. Supposons que, pour $i = 1, 2$, ρ_i soit semi-simple et que $\rho_i(G)$ laisse stable un $\mathbf{Z}_\ell$-réseau de V_i. Soit $\mathrm{Tr}\,\rho_i$ le caractère de ρ_i. Les fonctions $\mathrm{Tr}\,\rho_1$ et $\mathrm{Tr}\,\rho_2$ sont

à valeurs dans $\mathbf{Z}_\ell$. Supposons que ces fonctions soient distinctes, i.e. que ρ_1 et ρ_2 ne soient *pas isomorphes*. Soit ℓ^α la plus grande puissance de ℓ telle que :

$$\mathrm{Tr}\ \rho_2(s) \equiv \mathrm{Tr}\ \rho_1(s) \pmod{\ell^\alpha} \quad \text{pour tout } s \in G.$$

Notons M la sous-$\mathbf{Z}_\ell$-algèbre de End $(V_1) \times$ End (V_2) engendrée par les $(\rho_1(s), \rho_2(s))$ pour $s \in G$. Si $m = (m_1, m_2)$ est un élément de M, posons :

$$\theta(m) = \ell^{-\alpha}(\mathrm{Tr}\ (m_2) - \mathrm{Tr}\ (m_1)).$$

La forme linéaire $\theta : M \to \mathbf{Z}_\ell$ est surjective. Par réduction (mod ℓ) elle définit une forme linéaire non nulle :

$$t : M/\ell M \to \mathbf{Z}/\ell\mathbf{Z}.$$

Si s est un élément de G, et $\bar{s}$ son image dans $M/\ell M$, on a :

$$t(\bar{s}) \equiv \ell^{-\alpha}(\mathrm{Tr}\ \rho_2(s) - \mathrm{Tr}\ \rho_1(s)) \pmod{\ell}.$$

On notera $\bar{G}$ le sous-groupe de $(M/\ell M)^*$ formé des $\bar{s}$, pour s parcourant G. C'est un quotient fini de G, d'ordre $< \ell^{2d^2}$. Le couple formé par $\bar{G}$ et l'application $t : \bar{G} \to \mathbf{Z}/\ell\mathbf{Z}$ mesure en quelque sorte la « *déviation* » entre ρ_2 et ρ_1. L'intérêt de $(\bar{G}, t)$ est que c'est un objet « fini » (alors que G lui-même, en pratique, est infini). Cela permet souvent de dresser la liste des $(\bar{G}, t)$ possibles sans connaître ρ_1 ni ρ_2 (ni α). Supposons par exemple que cette liste soit formée de :

$$(\bar{G}_1, t_1), \ldots, (\bar{G}_h, t_h).$$

Pour tout j $(1 \leqslant j \leqslant h)$, on peut alors choisir un élément $s_j \in G$ tel que $t_j(\bar{s}_j) \neq 0$. L'ensemble $\{s_1, \ldots, s_h\}$ ainsi obtenu jouit de la propriété suivante :

(1) *Si* $\mathrm{Tr}\ \rho_2(s_j) = \mathrm{Tr}\ \rho_1(s_j)$ *pour* $j = 1, \ldots, h$, *les représentations* ρ_1 *et* ρ_2 *sont isomorphes* (i.e. l'égalité des caractères de ρ_1 et ρ_2 peut se tester sur $\{s_1, \ldots, s_h\}$.

Sinon, en effet, il existerait un indice j tel que le couple $(\bar{G}, t)$ associé à (ρ_1, ρ_2) soit isomorphe à $(\bar{G}_j, t_j)$, ce qui entraînerait :

$$\mathrm{Tr}\ \rho_2(s_j) \not\equiv \mathrm{Tr}\ \rho_1(s_j) \pmod{\ell^{\alpha+1}},$$

et contredirait l'hypothèse faite.

1.2. *Le cas* $\ell = d = 2$

Supposons que $\ell = 2$ et $d = 2$, de sorte que l'on puisse réaliser ρ_1 et ρ_2 comme des représentations de G dans $\mathbf{GL}_2(\mathbf{Z}_2)$. Faisons les hypothèses suivantes :

(i) $\det \rho_2 = \det \rho_1$;

(ii) les deux homomorphismes de G dans $\mathbf{GL}_2(\mathbf{Z}/2\mathbf{Z}) = \mathfrak{S}_3$, obtenus en réduisant ρ_1 et ρ_2 modulo 2, sont surjectifs et coïncident.

On peut alors déterminer $(\tilde{G}, t)$. On trouve que $\tilde{G}$ *est isomorphe, soit à* $\mathfrak{S}_4 \times \{\pm 1\}$, *soit à* $\mathfrak{S}_4$, *soit à* $\mathfrak{S}_3 \times \{\pm 1\}$, *et que* $t : \tilde{G} \to \mathbf{Z}/2\mathbf{Z}$ *vaut* 0 *sur les éléments de* $\tilde{G}$ *d'ordre* $\leqslant 3$, *et* 1 *sur les autres.*

1.3. *Courbes elliptiques*

Soient E_1 et E_2 deux courbes elliptiques sur **Q**. Soit S un ensemble fini de nombres premiers tel que $2 \in S$ et que les E_i aient bonne réduction en dehors de S. Soit $G = G_S$ le groupe de Galois de la plus grande extension algébrique de **Q** non ramifiée en dehors de S, et soient ρ_1 et ρ_2 les représentations 2-adiques de G associées à E_1 et E_2. Supposons que les points d'ordre 2 de E_i $(i = 1, 2)$ engendrent une extension K de **Q**, de groupe de Galois $\mathfrak{S}_3$, qui soit indépendante de i.

Toutes les conditions du n° 1.2 sont alors satisfaites. Si ρ_1 et ρ_2 ne sont pas isomorphes (i.e., d'après FALTINGS, si E_1 et E_2 ne sont pas **Q**-isogènes), on en déduit un groupe déviation $\tilde{G}$ de type $\mathfrak{S}_4 \times \{\pm 1\}$, $\mathfrak{S}_4$ ou $\mathfrak{S}_3 \times \{\pm 1\}$, d'où une extension galoisienne $\tilde{K}/\mathbf{Q}$ contenant K et de groupe de Galois $\tilde{G}$. Connaissant S, on peut déterminer explicitement les extensions $\tilde{K}/\mathbf{Q}$ qui sont *a priori* possibles : cela se fait, soit par la théorie du corps de classes, soit par des méthodes de géométrie des nombres. Si $\tilde{K}_1, \ldots, \tilde{K}_h$ désignent les extensions en question, on choisit pour tout $j = 1, \ldots, h$ un nombre premier p_j dont la substitution de Frobenius $\tilde{s}_j$ dans $\tilde{K}_j/\mathbf{Q}$ est d'ordre > 3. On peut alors appliquer le critère (1) du n° 1.1, et l'on en déduit :

(2) *Pour que les courbes* E_1 *et* E_2 *soient isogènes sur* **Q**, *il suffit que les traces des endomorphismes de Frobenius de* E_1 *et* E_2 *soient les mêmes pour les nombres premiers* $p_1, \ldots, p_h$.

(Ou, de façon plus concrète : il suffit que E_1 et E_2 aient le même nombre de points modulo $p_1, \ldots, p_h$.)

1.4. *Exemples d'applications du critère* (2)

(a) *Le cas de* 5077

Ce cas a été traité par J.-F. MESTRE (*C.R. Acad. Sci. Paris*, 300 (1985), 509-512). Les deux courbes E_1 et E_2 dont on veut prouver l'isogénie ont pour conducteur le nombre premier 5077. La première est l'unique « courbe de Weil » de ce conducteur. La seconde est définie par l'équation

$$y^2 + y = x^3 - 7x + 6.$$

Toutes deux ont bonne réduction supersingulière en 2, la trace de l'endomorphisme de Frobenius étant -2. De là, et d'un résultat de HONDA-HILL, on déduit que, si ces courbes ne sont pas isogènes, le groupe $\tilde{G}$ qui leur est associé est de type $\mathfrak{S}_4$ et le corps $\tilde{K}$ correspondant est non ramifié sur K. Or on constate qu'il n'y a que trois corps $\tilde{K}_1, \tilde{K}_2, \tilde{K}_3$ ayant ces propriétés, et que

l'on peut prendre pour p_1, p_2, p_3 les nombres premiers 5, 5 et 11. Comme les traces des endomorphismes de Frobenius de E_1 et E_2 sont les mêmes en 5 et en 11, on en déduit bien que E_1 *et* E_2 *sont isogènes* (donc, en fait, isomorphes).

(b) *Le cas de* 11

Il s'agit de prouver que *toute courbe elliptique sur* **Q** *de conducteur* 11 *est isogène à la courbe* $y^2 - y = x^3 - x^2$, résultat déjà démontré par M. AGRAWAL, J. COATES, D. HUNT et A. van der POORTEN, par des calculs sur machine, utilisant la théorie de BAKER. On applique pour cela le critère (2), en prenant pour E_1 la courbe donnée de conducteur 11, et pour E_2 celle des trois courbes de WEIL de conducteur 11 ou 11^2 qui a même réduction en 2 que E_1. On montre comme ci-dessus que le groupe $\bar{G}$ associé à E_1 et E_2 (supposées non isogènes) est de type $\mathfrak{S}_4$ et que l'extension $\bar{K}/K$ correspondante n'est ramifiée qu'au-dessus de 11. Or on vérifie facilement qu'une telle extension n'existe pas (son discriminant contredirait les bornes d'ODLYZKO). D'où l'isogénie de E_1 et E_2, et l'on en déduit aussitôt le résultat cherché.

2. *Représentations l-adiques attachées aux variétés abéliennes*

2.1. *Notations*

K est une extension de type fini de **Q** ;

$\overline{K}$ est une clôture algébrique de K ;

G_K est le groupe de Galois Gal $(\overline{K}/K)$;

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

ℓ est un nombre premier ;

$T_\ell = T_\ell(A)$ est le module de Tate de A relativement à ℓ ; c'est un $\mathbf{Z}_\ell$-module libre de rang $2n$;

$V_\ell = \mathbf{Q} \otimes T_\ell$; c'est un $\mathbf{Q}_\ell$-espace vectoriel de dimension $2n$, sur lequel opère G_K ;

$\rho_\ell : G_K \to \mathrm{Aut}\,(V_\ell)$ est la représentation ℓ-adique correspondante ;

G_ℓ est l'image de ρ_ℓ ; c'est un sous-groupe compact de Aut (V_ℓ) ;

$\mathfrak{g}_\ell$ est l'algèbre de Lie de G_ℓ ; on a $\mathfrak{g}_\ell \subset \mathrm{End}\,(V_\ell)$;

G_ℓ^{alg} est l'adhérence de G_ℓ pour la topologie de Zariski ; c'est un $\mathbf{Q}_\ell$-sous-groupe algébrique du groupe linéaire $\mathbf{GL}_{V_\ell} \simeq \mathbf{GL}_{2n}$.

2.2. *Structure de* G_ℓ^{alg}

2.2.1. (BOGOMOLOV). *Le groupe* G_ℓ *est un sous-groupe ouvert* (pour la topologie ℓ-adique) *du groupe des* $\mathbf{Q}_\ell$*-points de* G_ℓ^{alg}.

Ce résultat peut aussi se formuler en disant que l'algèbre de Lie du groupe G_ℓ^{alg} est égale à $\mathfrak{g}_\ell$, ou encore que $\mathfrak{g}_\ell$ est une sous-algèbre *algébrique* de End (V_ℓ).

2.2.2. (FALTINGS). *Le groupe* G_ℓ^{alg} *est réductif, et son commutant dans* End (V_ℓ) *est égal à* $\mathbf{Q}_\ell \otimes \mathrm{End}_K(A)$. En particulier, $\mathfrak{g}_\ell$ est une algèbre de Lie réductive, de commutant égal à $\mathbf{Q}_\ell \otimes \mathrm{End}(A)$.

On conjecture que G_ℓ^{alg} est « indépendant de ℓ » (pour A et K fixés), et plus précisément que sa composante neutre $(G_\ell^{alg})^\circ$ se déduit du « groupe de Mumford-Tate » par extension des scalaires de $\mathbf{Q}$ à $\mathbf{Q}_\ell$. L'un des buts du cours a été de démontrer un certain nombre de résultats partiels dans cette direction :

2.2.3. *Le groupe fini* $G_\ell^{alg}/(G_\ell^{alg})^\circ$ *est indépendant de* ℓ. De façon plus précise, le noyau de l'homomorphisme surjectif

$$G_K \to G_\ell \to G_\ell^{alg}/(G_\ell^{alg})^\circ$$

est indépendant de ℓ.

2.2.4. *Le rang de* G_ℓ^{alg} (dimension d'un sous-tore maximal) *est indépendant de* ℓ.

Ecrivons le groupe réductif connexe $(G_\ell^{alg})^\circ$ sous forme standard :

$$(G_\ell^{alg})^\circ = C_\ell \cdot S_\ell$$

où C_ℓ est un tore central (composante neutre du centre), et S_ℓ un groupe semi-simple (groupe dérivé). On a sur C_ℓ et S_ℓ les renseignements suivants :

2.2.5. (BOGOMOLOV). *Le groupe* C_ℓ *est indépendant de* ℓ, en ce sens qu'il provient par extension des scalaires d'un sous-tore de $\mathbf{GL}_{2n}$ défini sur $\mathbf{Q}$; *il contient le groupe* $\mathbf{G}_m$ *des homothéties.*

2.2.6. (FALTINGS). *On a* $C_\ell = \mathbf{G}_m$ *si* End $(A) = \mathbf{Z}$. *On a* $S_\ell = \{1\}$ *si et seulement si* A *est de type CM.*

Toute polarisation de A munit V_ℓ d'une forme alternée non dégénérée qui est invariante, à un facteur près, par l'action de G_K. On en conclut que G_ℓ^{alg} est contenu dans le groupe $\mathbf{G}_m \cdot \mathbf{Sp}_{2n}$ des *similitudes symplectiques,* et en particulier que l'on a $S_\ell \subset \mathbf{Sp}_{2n}$. On s'intéresse au cas où il y a égalité. Tout d'abord :

2.2.7. *Les propriétés suivantes sont équivalentes* :

(a) $S_\ell = \mathbf{Sp}_{2n}$ *pour un* ℓ ;

(b) $S_\ell = \mathbf{Sp}_{2n}$ *pour tout* ℓ ;

(c) End $(A) = \mathbf{Z}$ *et* rang $(G_\ell^{alg}) = 1 + n$.

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

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

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

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

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

pour tout ℓ.

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

2.3. *Indications sur les démonstrations*

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

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

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

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

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

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

Séminaires

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

Publications

J.-P. Serre, *Autour du théorème de Mordell-Weil,* I *et* II, notes de cours rédigées par Michel Waldschmidt, Publ. Math. Univ. Paris VI, 2 vol., 1984, 176 p. + 202 p.

— *L'invariant de Witt de la forme* Tr (x^2), Comm. Math. Helv. 59 (1984), 651-676.

Missions

Exposés

— *ℓ-adic representations,* Düsseldorf, septembre 1984 ;

— *Corps quartiques et isogénies de courbes elliptiques,* Bordeaux, novembre 1984 ;

— *Courbes elliptiques sur* **Q**, Genève, janvier 1985 ;

— **C** *est algébriquement clos,* E.N.S.J.F., Montrouge, janvier 1985 ;

— *Curves over finite fields* (2 exposés), Singapour, février 1985 ;

— *On Faltings' proof of Mordell conjecture,* Singapour, février 1985 ;

— *The Ramanujan function*, Singapour, février 1985 ;

— $\Delta = b^2 - 4ac$, Singapour, février 1985 ;

— *Curves of genus two*, Brighton, février 1985 ;

— *Subgroups of* $\mathbf{GL}_n(\mathbf{F}_p)$, Queen Mary College, Londres, février 1985 ;

— *Nombres de points des courbes algébriques sur les corps finis* (3 exposés), Les Plans-sur-Bex, mars 1985 ;

— « 5077 », Harvard, mai 1985 ;

— *Sur la lacunarité des puissances de êta,* Bordeaux, mai 1985 ;

— *On the quadratic forms of type* Tr (x^2), Oberwolfach, juin 1985 ;

— *Propriétés galoisiennes des points d'ordre fini des variétés abéliennes*, Besançon, juin 1985.

Groupe de Galois

et

Représentations l-adiques

—

Collège de France 1984

Notes Boutot — Oesterlé

Groupes de Galois et Représentations ℓ-adiques

Jean-Pierre Serre

Cours au Collège de France, octobre-décembre 1984

Notes par J-F. Boutot et J. Oesterlé

J.P. SERRE – 8.10.84 Représentations ℓ-adiques. (Cours n°1)

Plan du cours

1. Courbes elliptiques. Résultats

K corps de nombres (plus gen. de t.f. / $\mathbb{Q}$)

E courbe elliptique / K = var. abel. de dim 1.

$n \geq 1$ $\quad E_n = E_n(\bar{K}) = \mathrm{Ker}\{ n : E(\bar{K}) \to E(\bar{K}) \}$

$\simeq \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ pas canoniquement

$G = \mathrm{Gal}(\bar{K}/K)$ opère sur E_n, $G \to \mathrm{Aut}(E_n) \simeq GL_2(\mathbb{Z}/n\mathbb{Z})$

G_n = image de $G \to GL_2$.

n puissance de ℓ, ℓ premier fixé $\quad n = \ell, \ell^2, \ldots$

d'où $G \to GL_2(\mathbb{Z}_\ell)$ $\quad$ image $= G_{\ell^\infty}$

et $G \to GL_2(\hat{\mathbb{Z}}) = \prod_\ell (GL_2(\mathbb{Z}_\ell))$ $\quad$ image $= G_\infty$

Th 1. Si E n'a pas de mult. complexe (i.e. $\mathrm{End}_{\bar{K}} E = \mathbb{Z}$), G_∞ est ouvert (⇔ d'indice fini) dans $GL_2(\hat{\mathbb{Z}})$.

Cor 1) pour tout ℓ, G_{ℓ^∞} est ouvert dans $GL_2(\mathbb{Z}_\ell)$.

2) pour presque tout ℓ, $G_{\ell^\infty} = GL_2(\mathbb{Z}_\ell)$.

3) $\quad$, $G_\ell = GL_2(\mathbb{Z}/\ell\mathbb{Z})$

Rem 1) et 3) ⇒ 2)

Le théorème se démontre facilement maintenant avec Faltings

(Faltings)

Th 2. Si E, E' sont deux courbes elliptiques /K à rep. ℓ-adiques isomorphes, alors E et E' sont isogènes sur K.

$G \to GL_2(\mathbb{Z}_\ell) \to GL_2(\mathbb{Q}_\ell)$ est la rep. ℓ-adique

on dit qu'elles sont "isomorphes" si elles sont conjuguées

Il fut vrai pour un ℓ $\Rightarrow$ pour tout ℓ.

Ces résultats posent des questions d'effectivité. J'ai fait le travail sur $\mathbb{Q}$.

$E/\mathbb{Q}$, sans m.c., et soit S l'ensemble (fini) des p en lesquels E a mauvaise réduction (= ens des div premiers du discriminant)

Posons $N = N_E = \prod_{p \in S} p$ (pas très différent du conducteur)

[on pourrait aussi prendre N = conducteur].

Th 3. Il existe des constantes absolues, effectiv. calculables, c_1 et c_2 telles que :

(1) Si $\ell \geq N^{c_1}$, alors $G_\ell = GL_2(\mathbb{Z}/\ell\mathbb{Z})$ et $G_{\ell^\infty} = GL_2(\mathbb{Z}_\ell)$

(2)$_R$ Si $\ell \geq c_2 \log N$ et si GRH vraie, alors idem.

Rem c_2 est explicite, mais très gros.

c_1 : le Cebotarev effectif n'a jamais été fait sans GRH.

—

Il existe aussi une version effective du théorème 2.

Soit S un ensemble fini de places de K en dehors desquelles les deux courbes ont bonne réduction. Si $v \notin S$, les réductions mod v de E et E' sont définies $\tilde{E}_v$ et $\tilde{E}'_v$. Soit $k(v)$ le corps résiduel $|k(v)| = Nv$. On a la formule de Hasse

$$\tilde{E}_v(k_v) = 1 + Nv - a_v \qquad a_v = \text{trace du Frobenius de } \tilde{E}_v$$

rep l-adiques de E et E' sont isomorphes

$\Updownarrow$

$a_v = a'_v$ pour tout $v \notin S$.

$\Updownarrow$

$|\tilde{E}_v(k_v)| = |\tilde{E}'(k_v)|$ pour tout $v \notin S$.

car les Frobenius sont denses dans le gr. de Galois et les rep. sont semi-simples.

Faltings a montré que pour tout $v \notin S$ peut-être remplacé par quelque d'effectif.

4. En fait, si $K = \mathbb{Q}$, $N = \prod_{p \in S} p$, il suffit de vérifier que $a_p = a'_p$ pour $p \notin S$ et $p \leq N^{c_3}$.

et sous GRH $p \leq c_4 (\log N)^2$.

c_3 et c_4 sont absolus grands !! inutilisables

Cependant on fera un <u>exemple</u> totalement explicite pour $N = 5077$ (courbe de Mestre) ; on s'en tire avec $p < 100$.

Les spécialistes de transcendance s'intéressent au $x \in E(\bar{K})$ point d'ordre fini $n \geq 1$, au nombre des conjugués (gal/K) de $x\} = c(x$ E et K sont fixés.

Th 5. 1) Si E a de la mult. complexe $c(x) \geq c_{E,K} \dfrac{n}{\sqrt{\log\log n}}$.

2) Sinon, $c(x) \geq c'_{E,K}\, n^2$.

En tout cas toujours $\geq n^{1-\varepsilon}$. On essaiera aussi de le démontrer pour les sociétés abéliennes. Masser a des résultats dans ce sens avec des exposants plus faibles.

Pourquoi $\sqrt{\log\log n}$? Il y a m.c. par un corps imag quad $\mathbb{Q}(\sqrt{-d}) \cap K$

l dit discret soit | inerte $\mathbb{F}_{l^2}$ opère sur E_l
| décomposé $\mathbb{F}_l \times \mathbb{F}_l$ opère sur E_l, alors

$E_l \simeq \mathbb{Z}/n$ droits stables par Galois. Donc x a au plus $l-1$ conjugués $= l\left(1-\frac{1}{l}\right)$.

Prenons $n = l_1 \cdots l_k$, l_i décomposés $l_1 < l_2 < \cdots < X$ donné.

Alors $c(x) \gtrsim n \prod \left(1-\frac{1}{l_i}\right)$

$\log n = \sum \log l_i \sim \frac{1}{2} X$

$-\log \prod \left(1-\frac{1}{l_i}\right) = \sum \frac{1}{l_i} + c + O(1)$ 1/2 des premiers sont décomposés

$= \frac{1}{2} \log\log X + c' + O(1)$

$\dfrac{n}{\prod \left(1-\frac{1}{l_i}\right)} \sim c'' \sqrt{\log X} \overset{14}{\sim} c''' \sqrt{\log\log n}$.

Remarque. Sur $\mathbb{Q}$ et pour $\ell > 37$ tous les exemples connus ont groupe de Galois GL_2.

Sinon ce sera le nom d'un s/g de Cartan non déployé d'ordre $2(\ell^2-1)$ la courbe modulaire correspondant à ce s/g soit X_ℓ a-t-elle d'autres pts rationnels sur $\mathbb{Q}$ que les pointes et les pts à mult. complexe (tout à fait possible qu'il y en ait avec gros coefficients ?

(2) Variétés abéliennes et représentations ℓ-adiques.

A var. ab / K corps de nombres. On a encore A_n, A_ℓ, ...

rep ℓ-adique $G \longrightarrow GL_{2g}$ $\quad \mathbb{Z}/n\mathbb{Z}$, $\mathbb{F}_\ell$, $\mathbb{Z}_\ell$, $\hat{\mathbb{Z}}$ $\quad g = \dim A$

On s'intéresse à G_{ℓ^∞} = image de $G = Gal(\overline{K}/K)$ dans $GL_{2g}(\mathbb{Q}_\ell)$

(Bogomolov)

Th G_{ℓ^∞} est ouvert dans son adhérence Zariski.

Plus précisément soit H_ℓ le plus petit s/g alg de GL_{2g}, défini sur $\mathbb{Q}_\ell$, dont le groupe des $\mathbb{Q}_\ell$ points contienne G_{ℓ^∞}.
Alors G_{ℓ^∞} est ouvert dans $H_\ell(\mathbb{Q}_\ell)$, i.e. a même algèbre de Lie.
Il y a des conjectures sur H_ℓ (cf texte), peut-être fausses.
Cong la plus forte H_ℓ est indépendant de ℓ = "Mumford-Tate".

On sait que H_ℓ est un groupe réductif, soit H_ℓ° la comp neutre.

Indépendance de ℓ : * H_ℓ / H_ℓ° est indépendant de ℓ.

$H_\ell^\circ = T_\ell \cdot S_\ell$ $\quad T_\ell$ = composante neutre du centre de H_ℓ°

S_ℓ = groupe dérivé de H_ℓ°

$T_\ell \cap S_\ell$ est fini.

* T_ℓ est indépendant de ℓ (provient de T sur $\mathbb{Q}$) et contient le gr G_m de Tamat.
* rang S_ℓ est indép. de ℓ
* la rep. du groupe de Cartan de H_ℓ° est indép. de ℓ.
* (Faltings) le commutant de H_ℓ° est $(\mathrm{End}_{\bar{K}} A) \otimes \mathbb{Q}_\ell$.

C'est une combinaison de méthodes de Zarhin, Faltings.

Pour aller plus loin on peut faire l'hypothèse $\mathrm{End}_{\bar{K}} A = \mathbb{Z}$, alors $T_\ell = G_m$.

Th (modulo vérifications) Si $g = 1, 2, 3$, impair. Alors $S_\ell \simeq Sp_{2g}$.

Rem. pour $g = 4$, il y a deux possibilités (Mumford)

$Sp_8 \subset GL_8$ ou (après extension des scalaires) $SL_2 \times SL_2 \times SL_2 \subset GL_8$.

(3) Propriétés des repns. mod. ℓ.

A var ab /K $\dim A = g$ $G_\ell \subset GL_{2g}(\overline{\mathbb{F}_\ell})$

ou s'inté ens à $\mathbb{Q}$ caractéristique avec ℓ.

Th Pour chaque ℓ assez grand il existe (on définit comment) un s/g algébrique H_ℓ de GL_{2g} (sur $\overline{\mathbb{F}_\ell}$) avec les propriétés :

(1) H_ℓ est réductif (à repn semi-simple).

(2) la composante neutre de son centre est un tore indép de ℓ (réd mod ℓ du tore qui intervient dans les repn ℓ-adiques).

(3) le rang de H_ℓ est égal au rang du gr. ℓ-adique correspondant

(4) $G_\ell \cap H_\ell(\overline{\mathbb{F}_\ell})$ est d'indice borné (indép. de ℓ) dans G_ℓ et dans $H_\ell(\overline{\mathbb{F}_\ell})$.

Cor G_ℓ contient un s/g d'indice borné du gr. des homothéties

Je ne suis pas arrivé à démontrer "tout le gr. des homothéties" dans le cas général.

Th Dans les hyp $\mathrm{End}\, A = \mathbb{Z}$ et $g = 1, 2, 3$, impair.

on a $H_\ell = G_m Sp_{2g}$ et de plus l'image de Galois dans $\prod_\ell GL_2(\mathbb{Z}_\ell)$ est ouverte dans $\prod_\ell CSp_{2g}(\mathbb{Z}_\ell)$

où $CSp_{2g} = G_m Sp_{2g}$ similitude symplectique.

—

On peut regarder ds cqp l-adiques purs dans la cohomologie de deux gg ; il y a ds résultats analogues pr les semi-simplifiés. Il manque le th de commutation de Falting

4. Courbes elliptiques.

deux der th. 1. a) On regarde d'abord la rep ℓ-adique

$\varphi_\ell : G = \mathrm{Gal}(\bar{K}/K) \longrightarrow GL_2(\mathbb{Q}_\ell)$ E c. ell sans m. c.

On veut montrer $\mathrm{Im}(\varphi_\ell) = G_{\ell^\infty}$ est ouverte.

C'est un gr de Lie ℓ-adique $\mathfrak{g}_\ell = \mathrm{Lie}\, G_{\ell^\infty}$

G_{ℓ^∞} ouvert de $GL_2 \iff \mathfrak{g}_\ell = \mathfrak{gl}_2 = \mathrm{Lie}\, GL_2$.

Faltings $\Rightarrow$ | action de G_{ℓ^∞} sur V_ℓ est semi-simple

| commutant $= \mathrm{End}_E \otimes \mathbb{Q}_\ell = \mathbb{Q}_\ell$ (homothéties)

$\iff$ action de G_{ℓ^∞} sur V_ℓ est absolument simple

$\iff$ action de $\mathfrak{g}_\ell$ est absol. simple.

Les seuls s.alg de Lie ayant cette propriété sont $\mathfrak{gl}_2$ et $\mathfrak{sl}_2$.

Mais on connait $G \xrightarrow{\varphi_\ell} GL_2 \xrightarrow{\det} \mathbb{Q}_\ell^*$

$\det \circ \varphi_\ell = \chi_\ell$ caract cyclo. action de G sur μ_{ℓ^∞}

$\left(\overset{2}{\wedge} H_1 = H_2 \right)$. Donc $\mathfrak{sl}_2$ est exclu. ∎

Rem Avant Faltings, on fabriquait une isog d'isogénie et on utilisait Safarevic pour les courbes ell. → semi-simplicité

Pour exclure l'action abélienne $\mathfrak{g}_\ell$ = Cartan de GL_2, on utilise la théorie de rep abéliennes ℓ-adiques ; qui fabrique une famille abélienne pour tous ℓ, dont idem pour tout ℓ. On en déduit qu'il y a de la mult. complexe, un ℓ déployé donne contradiction.

b) Montrer que $G_\ell = GL_2(\mathbb{F}_\ell)$ pour ℓ assez grand.

Faltings $\Rightarrow$ G_ℓ est absolument irréductible pour $\ell \geq \ell_0$.

et on sait $\det G_\ell = \mathbb{F}_\ell^*$ pour $\ell \geq \ell_0$.

On passe à $PGL_2(\mathbb{F}_\ell) = GL_2(\mathbb{F}_\ell)/\mathbb{F}_\ell^* \supset PG_\ell$.

1er cas : ordre de PG_ℓ divisible par ℓ, donc aussi celui de G_ℓ.

irréd. + ordre de G_ℓ divisible par ℓ $\Rightarrow$ $G_\ell \supset SL_2(\mathbb{F}_\ell)$

un élément d'ordre ℓ pour les obtenus $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$

irréd droite non stable par Gal donc $G_\ell \supset \begin{pmatrix} -1 & 0 \\ -1 & 1 \end{pmatrix}$.

enfin $GL_\ell = GL_2(\mathbb{F}_\ell)$ grâce au det.

2e cas : ordre de PG_ℓ premier à ℓ

$\Rightarrow$ $PG_\ell =$ | cyclique
| dièdral
| A_4, S_4, A_5

on élimine ces possibilités,

- PG_ℓ cyclique $\Rightarrow$ G_ℓ abélien $\Rightarrow$ pas abs simple !

- Cas dièdral : $G_\ell \subset N_\ell$ normalisateur d'un Cartan C_ℓ
$\not\subset C_\ell$

a C_ℓ déployé $\begin{bmatrix} * & 0 \\ 0 & * \end{bmatrix}$ $\quad N_\ell = C_\ell \cup \begin{bmatrix} 0 & * \\ * & 0 \end{bmatrix}$

permute les 2 droites

$\varepsilon_\ell : G_\ell \to N_\ell/C_\ell = \{\pm 1\}$ car quad.

Prop Si ℓ est assez grand, ε_ℓ est non ramifié aux places divisant ℓ.

($\Leftarrow$ si ℓ assez grand, ε_ℓ est non ramifié en dehors de $S(E)$ ens de mauvaise réduction de E.

On utilise la th de Raynaud des groupes de type $(\ell,\dots,\ell)$: action de l'inertie en une place $v|\ell$ sur E_ℓ a pour image soit "demi-Cartan" $\begin{pmatrix} A & 0 \\ 0 & 1 \end{pmatrix}$ $A \in \mathbb{F}_\ell^*$.

soit un Cartan non déployé $\mathbb{F}_{\ell^2}^* \subset GL_2$.

(l'inertie est modérée car $\#G_\ell$ est d'ordre premier $\neq \ell$).

On a rigidité. inertie $\subset G_\ell \subset N_\ell$ norm. de Cartan

la seule possibilité est inertie $\subset C_\ell$, donc $\varepsilon_\ell(\text{inertie}) = 1$.

ie non ramifié.

Comme $S(E)$ est fini fini, il existe un nombre fini de ε_ℓ possible. Il existe une extension finie K_2 de $\mathbb{Q}$ telle que $G_{K_2} \subset G$ soit contenu dans le noyau de tous les ε_ℓ possibles.

On passe à K_2, cela ramène le cas dièdral au cas cyclique

- A_4, S_4, A_5 pour $\ell \geq 7$ les gp d'inertie ne contient pas (cyclique d'ordre ≥ 5).

c) <u>fin de la démo</u>. On sait maintenant

- pour chaque ℓ, G_{ℓ^∞} est ouvert dans $GL_2(\mathbb{Z}_\ell)$
- pour presque tout ℓ, $G_\ell = GL_2(\mathbb{Z}/\ell\mathbb{Z})$ et
- det connu : $\det : G \twoheadrightarrow \hat{\mathbb{Z}}^*$ ouvert de $\prod \mathbb{Z}_\ell^*$

Ceci entraîne G_α ouvert dans $G(\hat{\mathbb{Z}})$ par pure théorie des groupes (cf. Mc Gill).

Lemme. Si $\ell \geq 5$, tout s/g fermé de $SL_2(\mathbb{Z}_\ell)$ dont l'image par réduction mod ℓ est $SL_2(\mathbb{Z}/\ell\mathbb{Z})$ est $SL_2(\mathbb{Z}_\ell)$.

Dem. il existe $x \in H$ le s/g fermé de $SL_2(\mathbb{Z}_\ell)$ tel que

$$x \equiv \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \mod \ell$$

$$x = 1+\varepsilon \qquad \varepsilon \equiv \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \mod \ell \qquad \varepsilon^2 \equiv 0 \mod \ell$$

$$x^\ell \equiv 1 + \ell\varepsilon + \varepsilon^\ell \mod \ell^2 \qquad \varepsilon^\ell = \varepsilon^2 \varepsilon^{\ell-4} \equiv 0 \mod \ell^2$$

$$\equiv 1 + \ell\varepsilon \mod \ell^2$$

pour $s \in SL_2(\mathbb{F}_\ell)$ H contient $x \equiv 1 + \ell s \pmod{\ell^2}$ donc remplit les sous mod ℓ^2. On conclut par le lemme.

Rem pour 2, 3 le lemme est faux

le contre ex pour $\ell = 3$ dans Mc Gill est faux !

Il faut montrer que $\mathrm{Im}(G) \supset 1 \times 1 \cdots \times GL_2(\mathbb{Z}_\ell) \times \cdots$ (ℓ grand par th. des groupes c'est un peu embêtant. Soit I_ℓ le s/g fermé de $\mathrm{Im}(G)$ engendré par les gr d'inertie (à conj près) en les places v/ℓ. C'est un s/g distingué de $\mathrm{Im}\, G$.

Prop. Si ℓ est assez grand, $I_\ell = 1 \times \cdots \times 1 \times GL_2(\mathbb{Z}_\ell) \times 1 \times \cdots \times 1$.

en effet en tout cas $\subset$, distingué, $\det I_\ell = \overline{\mathbb{Z}_\ell^*}$

et en vu mod ℓ contient les tous d'inertie.

l'image par ρ_ℓ mod ℓ est dans $GL_2(\mathbb{Z}/\ell\mathbb{Z})$

On conclut par une variante du lemme pour GL_2.

Alors $\operatorname{Im} G \supset \prod_{\ell \geq \ell_0} GL_2(\mathbb{Z}_\ell)$

donc $\operatorname{Im} G = K \times \prod_{\ell \geq \ell_0} GL_2(\mathbb{Z}_\ell)$ $\qquad K \subset \prod_{\ell \leq \ell_0} (\mathbb{Z}_\ell)$

comme les projections de K sont ouverts, il est facile de voir que K est ouvert (en utilisant Sylow).

J.P. SERRE - 15.10.84 - (Cours n°2)

Application de la méthode Faltings à :

① Majorations effectives pour la courbes elliptiques / $\mathbb{Q}$.

② Méthode effective pour reconnaître que 2 courbes elliptiques sont isogènes (ex: 1 seule c. ell. à isogénie pri de cond 11, la courbe de Mestre de conducteur 5077 est de Weil).

Construction générale.

G un groupe, $\rho_1 : G \to GL_n(\mathbb{Z}_\ell) = Aut(C_1)$ ℓ premier fixé (par ex. 2

$$\rho_2 : G \to GL_n(\mathbb{Z}_\ell) = Aut(C_2)$$

C_i $\mathbb{Z}_\ell$-module libre de rang n.

Hypothèse : $Tr\,\rho_1 \neq Tr\,\rho_2$ (i.e. il existe $s \in G$, $Tr\,\rho_1(s) \neq Tr\,\rho_2(s)$

Soit $\alpha \geq 0$ le plus grand entier tel que

$$Tr\,\rho_1(s) \equiv Tr\,\rho_2(s) \pmod{\ell^\alpha} \quad \text{pour tout } s \in G.$$

En pratique on ne connaît pas α. On définit la "déviation" entre ρ_1 et ρ_2 :

$$t(s) = \frac{1}{\ell^\alpha}\left(Tr\,\rho_1(s) - Tr\,\rho_2(s)\right) \mod \ell$$

$$t : G \to \mathbb{Z}/\ell\mathbb{Z} \quad \text{(application)}.$$

$t(1) = 0$, t non identiquement 0

Prop. Il existe un quotient de G, soit $\tilde{G}$ d'ordre $< \ell^{2r}$ à travers lequel se factorise t.

$$G \to \tilde{G} \xrightarrow{t} \mathbb{Z}/\ell\mathbb{Z}.$$

ex : $G \subset GL_n \times GL_n$

$G = \{(s_1, s_2) \;/\; s_1 \equiv s_2 \bmod \ell^3\}$ 2 repr coïnc.

$\alpha = 3 \qquad t = Tr\left(\frac{s_1 - s_2}{\ell^3}\right) \bmod \ell$.

Construction (Faltings) - Soit M la sous-$\mathbb{Z}_\ell$-algèbre (= sous $\mathbb{Z}_\ell$-module) de $End(C_1) \times End(C_2)$ engendrée par les $(\rho_1(s), \rho_2(s))$, $s \in G$.

$$G \longrightarrow M^* \longrightarrow (M/\ell M)^* \dashrightarrow \mathbb{Z}/\ell\mathbb{Z}$$

on a $\quad t : M/\ell M \longrightarrow \mathbb{Z}/\ell\mathbb{Z}$

$(u_1, u_2) \in M \Rightarrow Tr(u_1) \equiv Tr(u_2) \bmod \ell^\alpha$

donc $\quad M \to \mathbb{Z}_\ell \qquad (u_1, u_2) \longmapsto \frac{1}{\ell^\alpha}\left(Tr(u_1) - Tr(u_2)\right)$

On pose $\tilde{G}$ = image de G dans $(M/\ell M)^*$.

$$Card\,(M/\ell M)^* < Card\,(M/\ell M) \leq \ell^{2n^2} \qquad (\text{rg } M \leq 2n^2)$$

($n = 0$ est impossible car $Tr\rho_1 \neq Tr\rho_2$). ∎

Application aux isogénies de variétés abéliennes

cf. Faltings.

A_1, A_2 var. ab. sur K, corps de nbres $\quad \dim A_1 = \dim A_2 = g \geq 1$.

On sait que : si les rep. ℓ-adiques de $G = Gal(\bar{K}/K)$ attachées à A_1 et A_2 sont isomorphes / $\mathbb{Q}_\ell$, alors A_1 est isogène à A_2.

On veut un critère effectif pour décider si les repr. sont isomorphes. Soit ℓ premier fixé.

Soit S un ensemble fini de places de K en dehors duquel

A_1 et A_2 ont bonne réduction et contiennent les places divisant ℓ. Alors les rep. ℓ-adiques ρ_i attachées à A_i sont non ramifiées en $v \notin S$ et $\mathrm{Tr}\, \rho_i(\mathrm{Frob}_v) = \mathrm{Tr}\, \mathrm{Frob}_v(\tilde{A}_i) = a_v(i)$ où $\tilde{A}_i$ = red mod v de A_i. $\mathrm{Frob}_v \in \mathrm{Gal}(\bar{K}/K)$.

Les Frobenius sont denses, donc

$$\text{rep. isom.} \iff a_v(1) = a_v(2) \quad \text{pour tout } v \notin S.$$

<u>Théorème</u> (Faltings) Il existe un nombre réel x, calculable effectivement à partir de K, g, S, tel que

$$a_v(1) = a_v(2) \quad \text{pour tout } v \notin S, \ Nv \leq x$$

$$\Rightarrow \quad A_1 \text{ et } A_2 \text{ sont } K\text{-isogènes.}$$

<u>Idée</u>. Supposons que ρ_1 et ρ_2 ne sont pas isomorphes. On va construire un "petit" v avec $a_v(1) \neq a_v(2)$.

$n = 2g$, on applique la construction précédente

ρ_1 et ρ_2 non isom et semi-simples $\Rightarrow \rho_1$ et ρ_2 n'ont pas même plan

donc $t : G \to \tilde{G} \to \mathbb{Z}/\ell\mathbb{Z}$ avec $\mathrm{Card}\, \tilde{G} < \ell^{8g^2}$.

$\mathrm{Gal}(\bar{K}/K) \twoheadrightarrow \tilde{G}$, le noyau est ouvert i.e. $\tilde{G} = \mathrm{Gal}(E/K)$

E corps de nbres. E/K non ramifié en dehors de S

Soit T la partie de $\tilde{G}$ formée des $s \in \tilde{G}$ avec $t(s) \neq 0$, $T \neq \emptyset$ et invariant par conjugaison. Choisissons $v \notin S$ avec $\mathrm{Frob}_v(\bar{G}) \in T$ et Nv minimum pour ces propriétés (par Čebotarev il y a une infinité de tels v).

$t(\mathrm{Frob}_v) \neq 0 \Rightarrow T_2 \rho_1 \not\equiv T_2 \rho_2 \pmod{l^{\alpha+1}}$

Cebotarev effectif dit $Nv \leq x(\text{deg\'e}, S, [K:\mathbb{Q}])$ d_K.

ref : cf. Serre IHES n° 54
Lagarias - Odlyzko.

Exemple $K = \mathbb{Q}$, $g = 1$, courbes elliptiques.

S = ensemble fini de nbs premiers contenant l et plus à mauvaise réduction.

$N_S = \prod_{p \in S} p$.

On peut prendre $x(S) = c_1 (\log N_S)^2$ sous GRH.

$= N_S^{c_2}$ sans hypothèse.

c_1 et c_2 cstes absolues calculables, c_1 calculée.

Rem Cebotarev effectif sans GRH n'a été fait que sur $\mathbb{Q}$ par Rosser et Schoenfeld (th. des nbs premiers, dVP).

dem. $l = 2$ $\quad |\tilde{G}| < 2^8 = 256$

E / $\mathbb{Q}$ $\quad n_E = [E:\mathbb{Q}] \leq 255$

$d_E = |\mathrm{disc}_E| \leq n_E^{n_E} \prod_{p \in S} p^{n_E - 1}$ (cf. Cebot)

$\log d_E \leq n_E (\log n_E + \log N_S)$

$\leq \alpha + \beta \log N_S$ $\quad \alpha, \beta$ effectifs.

Par Ceb effectif (sans GRH), [cf. th. 6 IHES] on trouve.

$$x \leq 280 \cdot n_E^2 \left(\log n_E + \log N_S\right)^2 .$$

$$\leq 280 \cdot 255^2 \left(\log 255 + \log N_S\right)^2 \ll \left(\log N_S\right)^2 .$$

Sans GRH on remplace $(\log d_E)^2$ par $d_E^{C_2}$. ∎

Théorème Soit E c. ell. sur $\mathbb{Q}$ et $N_E = \prod_p$ de mauv. red.
Supposons E sans m.c. $\mathrm{End}_{\overline{\mathbb{Q}}}(E) = \mathbb{Z}$.
Alors le gp de Galois des points de p-division de E est égal à $GL_2(\mathbb{Z}/p\mathbb{Z})$ pour $p \geq N_E^{C_3}$ C_3 cste abs
$\geq C_4 (\log N_E)$ sous GRH.

C_i sont des cstes absolues calculables.

Déb. Soit G_p = image de $G = Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ dans $GL_2(\mathbb{Z}/p\mathbb{Z})$ donnée par la repn $G \to Aut(E_p)$.
Si $G_p \neq GL_2(\mathbb{Z}/p\mathbb{Z})$, on a l'une des possibilités suivantes.

(1) $G_p \subset$ Borel $\begin{pmatrix} * & * \\ 0 & * \end{pmatrix}$ $p \geq 5$

(2) $G_p \subset$ n/s de Cartan non depl. $\simeq \mathbb{F}_{p^2}^*$.

(3) $G_p \subset$ normal de n/s de Cartan, mais pas de le Cartan

(4) G_p a pour image de PGL_2 l'un des gpes A_4, S_4, A_5.

On sait que $\det G_p = (\mathbb{Z}/p\mathbb{Z})^*$. La liste est celle des groupes d'ordre premier à p! Sinon on regarde le p-Sylow

si unique dans un Borel

sinon extension SL_2.

(1) est impossible si $p \geq 19$ et $p \neq 37$ (th de Mazur).

(2) est impossible si $p \geq 3$, car Gal contient la conj. complexe $c \in G$ c donne $\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$ non dans $\mathbb{F}_{p^2}^{\times}$.

(4) est impossible si $p \geq 17$, car on montre (Čeb. p. 197) que le gr d'inertie relatif à p ne tente pas.

A_4 et A_5 impossibles pour tout p.

S_4 impossible si $p \equiv \pm 1 \ (8)$ $\quad \subset PSL_2$

Gal n'est pas dans PSL_2. Dans les autres cas le gr d'inertie contient un élément d'ordre ≥ 6 dans PGL_2 donc $\not\subset S_4$.

(3) $G \xrightarrow{\varepsilon} G_p \longrightarrow \{\pm 1\}$ = Norm/Cartan.

Lemme Ce caractère est non ramifié en dehors de $S_E = \{p$ de mauvaise réduction$\}$.

car le gr d'inertie en ℓ $\subset$ Cartan. (Invent. 72) □

E_ε = tordue de E par ε

de rep ℓ-adique E_ε = rep de $E \otimes \varepsilon$

$$a_p(E_\varepsilon) = \varepsilon(p)\, a_p(E) \qquad p \text{ de bonne red}$$

E et E_ε ne sont pas isogènes/$\mathbb{Q}$, car pas de m.c.

Donc il existe $p \leq x(N_E)$ tel que $a_p(E_\varepsilon) \neq a_p(E)$

donc $\varepsilon(p) = -1$ et $a_p(E) \neq 0$. Soit p_0 ce p.

On ne peut pas avoir $p_0 = p$ (argument oublié). Invent. 15(72) p. 317, C.S.

Si $p \neq p_0$ et $p > 2 p_0^{1/2}$ pour tout ε $\Rightarrow$ (3) est impossible.

(p_0 dépend de ε, nbre fini de ε possible.).

en effet $\mathrm{Frob}_{p_0} \in G_p$ $\quad \varepsilon(p_0) = -1 \Rightarrow \mathrm{Frob}_{p_0} \in$ Norm – Cartan

$\Rightarrow T_2(\mathrm{Frob}_{p_0}) \equiv 0 \pmod{p}$

$\Rightarrow p \mid a_{p_0}(E)$

$\Rightarrow p \leq |a_{p_0}| \leq 2 p_0^{1/2}$. ∎

Isogénies de courbes elliptiques.

Si E_1 et E_2 ne sont pas isogènes elles fabriquent un $\bar{G}$. On va montrer que sous certaines hypothèses aucun groupe ne convient donc E_1 et E_2 sont isogènes.

Revenons à la construction de $\bar{G}$ dans le cas général $G \xrightarrow[\rho_1, \rho_2]{} GL_n(\mathbb{Z}_\ell) \times GL_n(\mathbb{Z}_\ell)$ avec

Hyp $T_r \rho_1 \neq T_r \rho_2$

Hyp Les réd. mod ℓ de ρ_1 et ρ_2 sont isomorphes et absolument irréductibles (ie irréd et commutant = scalaires)

Th Sous ces hypothèses, la $\mathbb{Z}_\ell$-algèbre M de $M_n \times M_n$ engendrée par G est égale (après éventuel chgt de base) à l'ens des couples (s_1, s_2) avec $s_1 \equiv s_2 \pmod{\ell^\alpha}$ (α défini

dem $G \to \mathrm{Aut}\, C_1 \times \mathrm{Aut}\, C_2$

C_i $\mathbb{Z}_\ell$-libre de rang n.

$$G \to \mathrm{End}(C_1) \simeq M_n(\mathbb{Z}_\ell)$$

l'image engendre End car abs ired $\Rightarrow$ bic mod ℓ + Nakayama

donc $M \subset M_n \times M_n$ se projette sur chaque facteur.

En general si $\Phi \subset \Phi_1 \times \Phi_2$ se projette sur chaque facteur (groups), les Φ se décrivent de façon unique par

$$\begin{cases} N_1 \trianglelefteq \text{ invariant de } \Phi_1 \\ N_2 \quad " \quad \Phi_2 \\ \Phi_1/N_1 \xrightarrow{\varphi} \Phi_2/N_2 \end{cases} \longrightarrow \begin{array}{l} \Phi = \text{"graphe" de } \varphi \\ = \{(s_1, s_2) \quad + \cdot s. \\ \varphi(s_1 \bmod N_1) = s_2 \ (\bmod N_2, \end{array}$$

$N_1 = \Phi \cap (\Phi_1 \times \{1\})$. (lemme de Goursat)

Ici on pose $N_1 = M \cap (M_n \times \{0\})$

$N_2 = M \cap (\{0\} \times M_n)$

N_1 est un idéal bilatère de M_n.

N_2 " " M_n

$M_n/N_1 \overset{\varphi}{\simeq} M_n/N_2$.

Tout idéal bilatère de $M_n(\mathbb{Z}_\ell)$ est $M_n(\mathfrak{a})$ où $\mathfrak{a}$ est un idéal de $\mathbb{Z}_\ell$. $\mathfrak{a} = 0$ est exclu car p_1 et p_2 non isom.

M est un écran de $M_n \times M_n$ i.e. l'algèbre sur $\mathbb{Q}_\ell$ engendrée par G est $M_n(\mathbb{Q}_\ell) \times M_n(\mathbb{Q}_\ell)$. —

donc $N_1 = \ell^{\alpha_1} M_n$

$N_2 = \ell^{\alpha_2} M_n$ $\quad \alpha_1, \alpha_2$ entiers > 0

et $M_n(\mathbb{Z}/\ell^{\alpha_1}\mathbb{Z}) \xrightarrow{\sim}_{\varphi} M_n(\mathbb{Z}/\ell^{\alpha_2}\mathbb{Z})$

d'où $\alpha_1 = \alpha_2 =: \beta$.

Les automorphismes de $M_n(\mathbb{Z}/\ell^\beta\mathbb{Z})$ sont intérieurs on se ramène donc à $\varphi = id$ et $M = \left(\{s_1, s_2\} \; s_1 \equiv s_2 \bmod \ell^\beta\right)$

alors $\mathrm{Tr}\, s_1 \equiv \mathrm{Tr}\, s_2 \bmod \ell^\beta$

et il existe (s_1, s_2) avec $\neq \bmod \ell^{\beta+1}$. Donc $\beta = \alpha$.

$\left(0, \ell^\beta \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\right)$. ∎

<u>Structure de $M/\ell M$</u>. $\simeq M_n(\mathbb{F}_\ell) \oplus \varepsilon M_n(\mathbb{F}_\ell)$

$\varepsilon^2 = 0$ $\quad \varepsilon$ central

$\simeq \left\{ (s,t) \quad s,t \in M_n(\mathbb{F}_\ell) \right.$

$\left. (s,t)(s',t') = (ss', st' + ts') \right\}$.

en effet : $M \longrightarrow M_n(\mathbb{F}_\ell) \oplus \varepsilon M_n(\mathbb{F}_\ell)$

$(s_1, s_2) \longmapsto \left(\begin{matrix} s_1 \bmod \ell \\ " \\ s_2 \bmod \ell \end{matrix}, \dfrac{s_2 - s_1}{\ell^\alpha} \bmod \ell \right)$

$(0, \ell^\alpha) \longmapsto \varepsilon$

$(M/\ell M)^* \simeq$ produit semi-direct de $GL_n(\mathbb{F}_\ell)$ par $M_n(\mathbb{F}_\ell)$ (action adjointe).

$s_1 + \varepsilon s_2$ inversible $\Leftrightarrow$ s_1 inversible

$\to M_n(\mathbb{F}_\ell) \to (M/\ell M)^* \longrightarrow GL_n(\mathbb{F}_\ell) \to 1$

additif $\qquad s_1 + \varepsilon s_2 \longmapsto s_1$

$s + t\varepsilon \hookleftarrow$

On a $\tilde{G} \subset (M/\ell M)^* = GL_n(\mathbb{F}_\ell) \cdot M_n(\mathbb{F}_\ell)$

et $\tilde{G}$ engendre le $\mathbb{F}_\ell$ - esp. vectoriel $M/\ell M$.

$\tilde{G} \to GL_n(\mathbb{F}_\ell)$ = red mod ℓ de ρ_1 et ρ_2.

$t : M/\ell M \longrightarrow \mathbb{F}_\ell$

$t(s_1 + \varepsilon s_2) = \mathrm{Tr}(s_2)$

On s'intéressera aux cas :

$n = 2$, $\ell = 2$ $\quad \det \rho_1 = \det \rho_2$ + hyp standards

C_2 d'ordre 2.

Alors $\tilde{G} \subset S_4 \times C_2$

mieux = S_4, S_4 diagonal, $S_3 \times C_2$, $S_4 \times C_2$.

J.P. SERRE. 22.10.84

(Cours n°3)

Remarque Sans Matin on élimine les g. triangulaires impossible pour $\ell > (p_0^{1/2}+1)^g$ si E a bonne réd en p_0 (cf. Invent.). On a en tout cas $p_0 \ll \log N_E$.
D'où OK pour $\ell \gg (\log N_E)^4$. Cet argument marcherait pour un corps de nombres quelconque.

Retour à $\tilde{G}$.

$$G \xrightarrow[\rho_1,\rho_2]{} GL_n(\mathbb{Z}_\ell)$$

t_2 réd mod ℓ absolument irréd et isomorphe
et $t_2\rho_1 \neq t_2\rho_2$.

$\mathbb{Z}_\ell$-algèbre M, engendrée par l'image de G dans $M_n(\mathbb{Z}_\ell)\times M_n(\mathbb{Z}_\ell)$
Il existe un entier $\alpha \geq 1$ tel que (quitte à conjuguer ρ_1)

$M = \{(s_1,s_2),\ s_1 \equiv s_2 \pmod{\ell^\alpha}\}$. $\quad (s_1,s_2) \mapsto \left(s_1, \frac{s_2-s_1}{\ell^\alpha}\right)$

$M/\ell M = M_n(\mathbb{F}_\ell) \oplus \varepsilon M_n(\mathbb{F}_\ell)$ $\quad \varepsilon$ central, $\varepsilon^2 = 0$.

$(M/\ell M)^*$ = produit semi-direct de $GL_n(\mathbb{F}_\ell)$ par $M_n(\mathbb{F}_\ell)$
avec action adjointe.

$\tilde{G}$ = image $\{G \to (M/\ell M)^*\}$.

$s_1 + \varepsilon u \in M/\ell M \qquad t(s_1+\varepsilon u) = Tr_2(u) \in \mathbb{F}_\ell$

$s \in G \to \tilde{s} \in \tilde{G} \to t(\tilde{s}) \in \mathbb{Z}/\ell\mathbb{Z}$

$$t(\tilde{s}) \equiv \frac{Tr\,\rho_2(s) - Tr\,\rho_1(s)}{\ell^\alpha} \pmod{\ell}$$

Variante.

$$0 \to M_n(\mathbb{F}_\ell) \to GL_n(\mathbb{Z}/\ell^{\alpha+1}\mathbb{Z}) \longrightarrow GL_n(\mathbb{Z}/\ell^{\alpha}\mathbb{Z}) \to 0$$

gr. add (abélien)

$$\rho_2 \uparrow \quad \uparrow \rho_1 \qquad \nearrow$$

$$G$$

dont un cocycle

$$\rho_2(s) = m(s)\rho_1(s)$$

$s \mapsto m(s)$ est un 1-cocycle de G à val. dans $M_n(\mathbb{F}_\ell)$

G opère à travers $GL_n(\mathbb{F}_\ell)$, le cocycle permet de définir un hom $G \longrightarrow GL_n(\mathbb{F}_\ell) \cdot M_n(\mathbb{F}_\ell)$ pr. semi direct

$$s \longmapsto m(s)\rho_1(s)$$

Hypothèse suppl. $\det \rho_1 = \det \rho_2$.

Alors $\tilde{G}$ est contenu dans le produit semi-direct $GL_n(\mathbb{F}_\ell) \cdot M_n^0(\mathbb{F}_\ell)$

où $M_n^0(\mathbb{F}_\ell) = \{u / u \in M_n(\mathbb{F}_\ell), Tr(u) = 0\} = sl_n(\mathbb{F}_\ell)$

$1 + \varepsilon u = s(1 + \varepsilon s^{-1}u)$ est dedans $\Leftrightarrow$ $Tr(s^{-1}u) = 0$.

Donc s_1, s_2 $\quad s_1 \equiv s_2 \mod \ell^\alpha$

$$s_2 = s_1(1 + \ell^\alpha u)$$

$$\det(s_2) = \det(s_1) \Rightarrow \det(1 + \ell^\alpha u) = 1$$

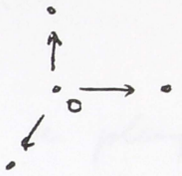
$$\equiv 1 + \ell^\alpha Tr(u) \mod \ell^{\alpha+1}.$$

D'où $Tr(u) \equiv 0 \pmod{\ell}$.

Cas $n=2$ et $\ell=2$.

rep. abs. irréd mod 2 isomorphe et $\det \rho_1 = \det \rho_2$.

$GL_2(\mathbb{F}_2) = S_3$



par red mod 2 G s'envoie sur S_3

pour les courbes ell. $\Leftrightarrow$ le corps des pts de division par 2 est de degré 6

(ie poly irréd de deg 3 non cyclique.)

$M_2(\mathbb{F}_2)$ comme module sur $GL_2(\mathbb{F}_2) = S_3$.

On a canon. $M_2(\mathbb{F}_2) = A \oplus B$

A, B s.ev. de dim. 2 stable par S_3

$A \supset A_1$ de dim 1 (sans suppl.) module non s.i.

$$M_2^0 = A_1 \oplus B$$

A_1 = matrices scalaires $= 0, 1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$; $M_2^0 \supset A_1$

Dans $M_2(k)$ on peut plonger tout k' avec k'/k de degré 2 sep. (choix d'un Cartan non déployé) ; alors $M_2(k) = k'\text{-lin} \oplus k'\text{-antilin}$.

Si $k = \mathbb{F}_2$, dans $M_2(\mathbb{F}_2)$ il y a un unique sous-corps à 4 éléments $\{0, 1$ et les 2 éléments d'ordre 3 (rotations)$\} = A$ par déf

B = endom de $M_2(\mathbb{F}_2)$ antilinéaire pour cette structure.

$$= \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

$M_2^0 = \mathbb{F}_2 \oplus B$ module semi-simple

S_3 agit trivialement sur $\mathbb{F}_2$

action naturelle sur B e.v. de dim 2.

$S_3 . M_2^\circ = S_4 \times C$ — C cyclique d'ordre 2

S_4 groupe des permutations de 4 lettres

C sous-groupe de $\mathbb{F}_2$

$S_4 = S_3 . B$

On regarde dans S_4 le groupe V_4 type $(2,2)$. On plonge S_3 dans S_4 en choisissant l'un des pts fixes par permutation de $V_4 - \{0\}$.

$t : M/2M \longrightarrow \mathbb{Z}/2\mathbb{Z}$

Valeurs de t sur $S_4 \times C$; c'est une fonction centrale, on donne ses valeurs sur la classe de conjugaison

ℓ de S_4 \ ℓ de C	1	-1
(1)	0	0
(12)	0	0
(123)	0	1
(1234)	1	1
(12)(34)	0	0

$S_4 \longrightarrow S_3$

(1)

(12)

(123)

(12)

(1)

Les $S_3 \times 1$ les 3 premiers (1), (12), (123) et 1

$1 + \varepsilon u \quad u = 0 \Rightarrow T_2(u) = 0$.

$(1,-1)$ de $S_4 \times C$ est $1 + \varepsilon . 1$

$(s, c)(1,-1) = (s, -c)$

$T_2(u+v) = T_2(u) + T_2(v)$

$t(s,-c) = t(s,c) + T_2(s)$

$(s + \varepsilon u)(1 + \varepsilon 1) = s + \varepsilon(u + s)$

dans la deuxième colonne, à partir de la première.

- Dans $S_3 . (\mathbb{F}_2 \oplus B)$, (12)(34) est dans B donc Trace $= 0$.

× (1234) se représente par $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} + \varepsilon \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$ (car d'ordre 2 de S_3 et trace de carré $= 1$.)

Il y a quatre possibilités à conj. près pour $\tilde{G} \subset S_4 \times C$.

① $S_3 \times C$ 4 plgts conjugués entre eux

② S_4 $(\to S_4 \times \{1\})$

③ S_4 ("plgt diagonal" $= (s, c)$ t.q. $\varepsilon(s) = c$) } ces 2 cas sont conjugués

④ $S_4 \times C$

Il n'y en a pas d'autres car $\tilde{G} \to S_4 \to S_3$ est surjectif

donc image $(\tilde{G} \to S_4)$ est soit S_3 ① ou S_4 ②③④.

On ne peut pas avoir $\tilde{G} = S_3$ car $|\tilde{G}| \geq 8$, $\tilde{G}$ engendre M (ou encore t serait 0 dessus). Restent $\tilde{G} = S_4$ les pos. 234.

Remarque Dans le cas $S_3 \times C$, on a $t = 1$ si (et seult. si) (s, c) est tel que s ordre 3 et $c = -1$.

Dans les cas ② et ③, $t = 1 \Leftrightarrow$ la comp. dans S_4 est d'ordre 4

Dans le cas ④ "réunion" des cas précédents.

Applications aux courbes elliptiques

E_1, E_2 c. ell / $\mathbb{Q}$, bonne réd en dehors de S (ens de premiers)

Hyp. ① E_1 et E_2 ne sont pas isogènes sur $\mathbb{Q}$.

② Leurs pts de division par 2 engendrent une extn de $\mathbb{Q}$ de degré finie à gr. de Galois S_3 (et la même pour les 2 courbes).

Alors rep. 2-adiques associés conjugués $(\tilde{G}, \alpha)$.

a_p^1, a_p^2 $(p \neq 2, p \notin S)$ trace de Frob en p

$$\frac{a_p^2 - a_p^1}{2\alpha} \equiv t(\mathrm{Frob}_p \in \tilde{G}) \mod 2$$

Corollaire. Si $t(\mathrm{Frob}_p) = 1$, alors $a_p^1 \neq a_p^2$.

Ex Si $\tilde{G} = S_4$, il existe

$$\begin{array}{c} F \\ | \\ S_4 \\ | \\ \mathbb{Q} \end{array} \quad (E_1, E_2) \quad \text{t.q. si } \mathrm{Frob}_p = (1234), \text{ alors } a_p^1 \neq a_p^2.$$

1er Exemple Courbe de cond $57 = 3 \cdot 19$ cf. Antwerp vol 4 p. 88

57_E $y^2 + y = x^3 - x^2 - 2x + 2$ $\quad \Delta = -3^2 \cdot 19$

57_F $y^2 + y = x^3 + x^2 + 20x - 32$ $\quad \Delta = -3^{10} \cdot 19$

$N_p = 1 + p - a_p$ on trouve les a_p p. 117

Il y a des a_p impairs donc élément d'ordre 3 du gr. de Gal

S_3 opérant sur pts de div par 2 , disc n'est pas un carré

donc signature non triviale. Donc gr. S_3.

(l'ext quadratique est $\mathbb{Q}(\sqrt{\Delta}) = \mathbb{Q}(\sqrt{-19})$

L / S_3 / $\mathbb{Q}$.

les a_p sont congrus mod 2. en fait 4

On $\mathbb{Q}(\sqrt{-19})$ = 1

L / 3 / $\mathbb{Q}(\sqrt{-19})$ / 2 / $\mathbb{Q}$

on prend l'ext de deg 3 ramifiée en 2

(2 est inerte dans $\mathbb{Q}(\sqrt{-15})$ donc $\mathbb{F}_4^*$ ordre 3)

cher L.

On calcule $t = \dfrac{a_p^1 - a_p^2}{4}$.

On est dans le cas $S_3 \times C$:

L / S_3 / $\mathbb{Q}$; L' / C

extensions disjointes $L' = \mathbb{Q}(\sqrt{-3})$

caractère de Legendre $\left(\frac{p}{3}\right)$

en effet $t = 1 \iff Frob_p$ = (elt d'ordre 3, -1)

$\updownarrow$

pt de pr d'ordre 2 rat sur $\mathbb{F}_p$ $\left(\frac{p}{3}\right) = -1$ $p \equiv 1 \ (-3)$

$t = 1 \iff$ $\begin{cases} p \equiv -1 \ (3) \\ f_3(x) \equiv 0 \mod p \text{ n'a pas de solution} \end{cases}$ $p \neq 2, 3, 19$

f_3 = eq des pts d'ordre 2. en fait a_p impair suffit

Pour démontrer que c'est vraiment ce cas, il suffit d'éliminer les autres possibilités.

S_4 impossible

Si ce n'était pas 4 en dehors, ce serait 2 ; mais alors le tableau est stupide pas de corps (quad.) possible.

Pour éliminer $S_4 \times C$, on montre que le corps quartique ne serait pas possible, discriminant impossible.

2e Exemple conducteur 37 37_A 37_B $\Delta = +37$

$a_p^A \equiv a_p^B \pmod 2$ pas mod 4

$\tilde{G} = S_4 \leftrightarrow$ corps quartique de discriminant $2^4 \cdot 37$ (tables)

Ramification dans le groupe $\tilde{G}$.

trivialement : non ramifié en dehors de 2 et de S

Hyp : $\hat{m}$ actue sur les pts d'ordre 2, S_3.

Soit $p \in S$, $p \geq 5$ gr. d'inertie en p (ρ_1, ρ_2) est modérée, donc cyclique d'ordre premier à p.

Soit $\rho = \rho_1$; actions de l'inertie dans la repr. ρ.

0ème cas bonne réd en p, alors gen de l'inertie $\mapsto 1$ — Trace = 2

1er cas : réd mult. α, alors gen de l'inertie $\sim \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$ Trace = 2
unipotente

2° cas réd additive

2.1 f non p-entière forme tordue du cas précédent

$$\text{gén} \mapsto \begin{pmatrix} -1 & * \\ 0 & -1 \end{pmatrix} \qquad \mathrm{Tr} = -2.$$

2.2. f p-entier (pot. bonne réd.)

gr. d'inertie est d'ordre	val disc $v(\Delta)$ mod 12	Tr.
2	6	-2
3	4, 8	-1
4	3, 9	0
6	2, 10	1

la trace est celle de la racine de l'unité correspondante.

Remarque ① Si l'inertie a même trace pour les deux coniks, l'élt de $\tilde{G}$ correspondant à un générateur de l'inertie en p est tel que $t=0$. (C'est le cas en particulier si les deux coniks ont réd. mult. en p.

Exemple. Si E_1, E_2 ont réd. mult en p et si le corps $\mathbb{Q}(\sqrt{\Delta})$ est ramifié en p, alors le gr. d'inertie en p a une image dans S_4 qui est (12).
(car (1234) est exclu car $t = 1$).

Ramification en 2.

Prop Hyp. E_1, E_2 sont bonne red en 2, supersinguliers $a_2^1 \equiv a_2^2 \equiv 0 \pmod{\text{mx}}$ et $a_2^1 = a_2^2$.

Alors, à conj. près, le gr. de déc. en 2 dans $\tilde{G}$ est égal à S_3 et le gr. d'inertie est A_3.

Cor L'extension L'/L est non ramifiée en 2.

$$\begin{array}{c} L' \\ | \\ L \\ | \ S_3 \\ \mathbb{Q} \end{array} \quad S_4$$

La démonstration Honda, Carlitz, Messing, Fontaine :

Th Deux groupes p-divisibles (connexe dim 1) de hauteur 2 sur $\mathbb{Z}_p$ qui ont même réduction mod p sont isomorphes (même si $p=2$).

Attention Lubin-Tate $h-1$ paramètres pour les relèvements d'un gr. formel de hauteur h dans LT $\quad t \mapsto t + a_2 t^2 + \cdots$

ici $\quad t \mapsto a_1 t + a_2 t^2 + \cdots$

donc c'est compatible.

La classification est faite par des modules de Dieudonné filtrés, un seul type possible.

Le th. entraîne : les repr. 2-adiques attachés à ρ_1 et ρ_2 sont isom. sur le gr. de déc. en 2 (i.e. sur $\mathbb{Q}_2$) et sont absolument irréd. mod 2.

Revenons à la def de $\widetilde{G}$

$C_1/\ell^\alpha C_1 \simeq C_2/\ell^\alpha C_2$

Soit $\varphi : C_1 \xrightarrow{\sim} C_2$ un isom. $\mathbb{Z}_\ell$-linéaire compatible avec l'action de G mod ℓ^α ; alors $M = \{(s_1, s_2) \mid s_i \in \mathrm{End}(C_i)$
$\varphi s_1 \equiv s_2 \varphi \mod \ell^\alpha\}$

Ici soit $G_2 \subset G$ un gr. de décomp. en 2.
Je choisis φ compatible avec l'action de G_2. Alors φ est compatible avec l'action de G mod 2^α : en effet il existe un G-isomorphisme $\psi_\alpha : C_1/2^\alpha C_1 \to C_2/2^\alpha C_2$ compatible avec G, donc avec G_2. Mais alors $\mathrm{ind} = \text{commutant de } G_2 = \text{bound}$
donc $\psi_\alpha = u.\varphi \mod \ell^\alpha$ u unité 2-adique
(supposons en 2 $\Rightarrow$ gr. de déc. en 2 sur les pts de div par 2 $= S_3$
les éléments de G_2 donnent des images dans $S_3 \subset \widetilde{G}$. $(u \to \infty)$.

Serre

(Cours n°4) 29/10/84

Th (Agrawal, Coats, Hunt, Van der Poorten)

A isogénie près, il n'y a qu'une seule courbe elliptique de conducteur 11, à savoir

$$y^2 - y = x^3 - x^2 \quad (\Delta = -11) \qquad + \text{2 isogènes.}$$

(B. Setzer : pour $p = 7, 13, 23, 29, \ldots, 281$ (1975) il n'y a pas de de courbes elliptiques de cond. p).

Si $p = u^2 + 64$, on a une courbe elliptique avec un pt d'ordre 2 rationnel, de cond. p, à savoir

$$y^2 = x^3 + ux^2 - 16x$$

Cette courbe est la seule de cond. p avec un pt d'ordre 2 (à une 2-isogénie près) et on ne sait pas si elle est modulaire. D'ailleurs le fait qu'il y ait un pt rationnel d'ordre 2 sur une courbe de cond. p implique $p = 17$ ou $p = u^2 + 64$.

Le conducteur 11 :

Soit E une courbe elliptique de conducteur 11.

Il n'y pas de point d'ordre 2 (thm de Setzer). Le corps K engendré sur $\mathbb{Q}$ par les pts d'ordre 2 est donc soit A_3, soit S_3

En fait c'est S_3 (Sinon on aurait un homomorphisme $\rho : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathbb{Z}/3\mathbb{Z}$ ramifié que en 11 et 2.

Mais l'inertie en p agit par un élément unipotent donc d'ordre 2. Ainsi p ramifierait dans $\mathbb{Q}_2^\times \to \mathbb{Z}/3\mathbb{Z}$ par la corps de classes local. Absurde.

Prop (Description de K). Le corps fixé par A_3 est $\mathbb{Q}(\sqrt{-11})$

Comme $\left(\frac{2}{11}\right) = -1$, 2 est inerte dans $\mathbb{Q}(\sqrt{-11})$. On a $\mathbb{Q}(-11) = 1$, $\mathcal{O}/2\mathcal{O} \simeq \mathbb{F}_4$ $(\mathcal{O}/2\mathcal{O})^\times \simeq \mathbb{Z}/3\mathbb{Z}$ d'où mon est ramifiée seulement en 2, de degré 3, de $\mathbb{Q}(\sqrt{-11})$: c'est K.

Démonstration: Le corps fixé par A_3 est ramifié en 11 (car l'inertie en 11 agit par un élt d'ordre 2) donc est $\mathbb{Q}(\sqrt{\pm 11})$ ou $\mathbb{Q}(\sqrt{11})$. Si $\mathbb{Q}(\sqrt{-11})$, la th. des corps de classes permet de conclure. Si $\mathbb{Q}(\sqrt{11})$, la th. du corps de classes permet encore de conclure.

La réduction de la courbe en 2 est supersingulière

(Si a_2 = trace Frobenius en 2.

$a_2 \equiv 0 \bmod 2$, ie $a_2 = 0, 2, -2$)

Le groupe d'inertie en 2 est A_3 et le groupe de décomposition S_3.

Pour la courbe connue E_0 : $y^2 + y = x^3 - x^2$

il y a 5 pts mod 2, d'où $a_2 = -2$.

Montrons que si E a un 2 égal à -1, $\tilde{G}$ est isogène à E_0. Si ce n'était pas le cas, soit $\tilde{G}$ la déviation entre E et E_0. Il correspond à une extension $\tilde{K}$ de $\mathbb{Q}$

$\tilde{G}$ peut a priori être $S_4 \times C$, S_4, S_4^{disp}, $S_3 \times C$ (en fait S_4 et S_4^{disp} sont conjugués dans $(M/2M)^*$ remarqué depuis le dernier cours par Serre)

Lemme : Si E_1 et E_2 ont bonne réd. en dehors de p premier, $p \neq 2$, et réd. multiplicative en 2 avec $\hat{m}$ ar et ne sont pas isogènes, $\tilde{G} = S_4$.

$\tilde{G}^{ab} = \tilde{G}/(\tilde{G}, \tilde{G})$ est un groupe de type 2,2 si $\tilde{G} = S_4 \times C$ ou $\tilde{G} = S_3 \times C$. Le groupe d'inertie en 2 est cyclique d'ordre 3 (dans les groupes formels), donc a une image nulle dans $\tilde{G}$. $\tilde{G}$ est une extension bicyclique ramifiée seulement en p, ce qui n'existe pas.

On a donc
$$S_4 \left(\begin{array}{l} \tilde{K} \\ | \\ K \\ | S_3 \\ \mathbb{Q} \end{array} \right.$$
l'inertie en 2 est un cycle d'ordre 3 et l'inertie en p est $= (12)$ dans S_3

l'inertie en p est donc soit d'ordre 2, soit cyclique d'ordre 4 dans S_4. Mais dans tous les éléments conjugués est 2, donc la diff. des traces est 0. Ceci implique que l'inertie en 2 est une transposition.

Une tel corps n'existe pas : 1ère démo : $\tilde{K}$ est de degré 24. On a $|d|^{\frac{1}{n}} = \prod_p p^{1-\frac{1}{4}} = 2^{\frac{2}{3}} 11^{\frac{1}{2}} < 10$ et Odlyzko dit $|d|^{1/n} > 10/6$

2ème étape : Déterminer le nbre de sommets de K.

3ème étape : Soit K_4 l'un des corps de degré 4 associés à $\widetilde{K}$. On a $|d_{K_4}| = 2^2 \cdot 11 = 44$. Il n'y a pas de corps de ce discriminant

Montrons que si le a_2 de E est $\neq 0$, E est isom à la courbe à C.M. par $\mathbb{Q}(\sqrt{-11})$ (grâce au caractère associé : il associe à un idéal $\mathfrak{a}$ de $\mathbb{Z}[\sqrt{-11}]$ le générateur α tel que $\alpha \equiv$ mod 11 carré)

$a_2 = 2$ $\in$ cond. 11 $*$ caract. de Legendre en 11

On reprend la construction précédente avec $\widetilde{K} \simeq S_4$. En 11 la ramification est cette fois à d'ordre 2 ou 4

On a $|d_K| \leq 2^{7/4} 2^{2/3} 11^{3/4} < 10^3$.

(en effet : $\left(2^{2/3} 11^{3/4}\right)^3 = 4 \cdot 121 \cdot 11^{1/4} \leq 8 \cdot 121 = 968 \leq 10^3$)

Courbe de conducteur 5077

$$y^2 + y = x^3 - 7x + 6$$

et de rang 3 sur $\mathbb{Q}$.

Question : - Cette courbe est-elle de Weil

- $L_E(s)$ a-t-elle un zéro triple en $s=1$?

T_2 a dans $S_2(\Gamma_0(5077))$ $a_2 = -2$ comme val. propre simple et pas d'autres valeurs propres rationnelles.

Conclusion : il existe une courbe elliptique de Weil de conducteur 5077 avec $a_2 = -2$, $a_3 = -3$, ...
connus pour $p < 420$; ce sont les mêmes que ceux de la courbe E. Il faut vérifier que ces courbes sont isogènes (ce qui entraînera qu'elles sont isomorphes)

Thm : Deux courbes elliptiques / $\mathbb{Q}$, de conducteur 5077 ayant le même a_2 ($= 0, 2, -2$) et les mêmes a_p pour $p = 5$ et $p = 11$, sont isogènes.

Démo : On obtient par les méthodes exposées une extension $\tilde{K}/\mathbb{Q}$, à groupe de Galois S_4, contenant l'extension $K/\mathbb{Q}$ à groupe S_3 "évidente", $\tilde{K}$ non ramifié sur K.
En 2, on connaît la ramification des S_3
Le corps quad est $\mathbb{Q}(\sqrt{5077})$. On a $h = 1$ et 2 est inerte, d'où un K convenable

Fait Il existe trois extensions $\tilde{K}$ ayant les propriétés imposées (ie contenant K, non ramifiées sur K, à g. S_4). De plus, dans chacune d'elles, l'un des nbres premiers 5 et 11 est d'ordre 4).

Le résultat pour 5077 en découle : si $\tilde{K}$ est l'une des précédentes, 5 (ou 11) est tot^t inerte $\Rightarrow$ cycle d'ordre 4, d'où $t = 1$, d'où $a_p \neq a'_p$.

On cherche K_4 de discriminant $2^2 5077$
1) On a pour un tel corps une extension de degré 4 avec des coeff. assez petits, ce qui permet de les calculer

Digression: Soit k un corps, k_s une clôture séparable K/k une extension de groupe S_3. On s'intéresse aux extensions $\tilde{K} \subset k_s$ $\tilde{K}/K$, $\tilde{K}$ Galoisienne sur k, $\mathrm{Gal}(\tilde{K}/k) \simeq S_4$. Elle est galoisienne sur K de type $(2,2)$. Soit Γ l'ensemble de ses extensions, auquel on adjoint une élément neutre, K lui-même.

Il y a sur Γ une structure de groupe abélien naturelle. Soit V le groupe $(2,2)$ avec action de S_3 (si on le veut comme on prend $V = \{0\} \cup \{$ ext. cubiques de k dans $K\}$).

On a des bijections:

$$\Gamma \longleftrightarrow H^1(\mathrm{Gal}(k_s/k), V) = \mathrm{Hom}_{S_3}(\mathrm{Gal}(k_s/K)^{ab}, V)$$
$$= \mathrm{Ker}\left(\mathrm{Cor} : H^1(k_3, \mathbb{Z}/2\mathbb{Z}) \to H^1(k, \mathbb{Z}/2\mathbb{Z})\right)$$

a) Le dernier groupe est $\{a \in k_3^\times \bmod k_3^{\times 2} / \mathrm{Nr}\ \text{carrés}\}$.
Un 1-cocycle de $\mathrm{Gal}(k_s/k, V)$ fournit $\mathrm{Gal}(k_s/k) \to S_3 \ltimes V$ i.e. une ext. de type S_4.

b) La dernière flèche vient de la suite spectrale de Hochschild-Serre

$$H^1(S_3, V) \to H^1(G_k, V) \to H^0(S_3, H^1(G_K, V)) \to H^2(S_3, V)$$
$$\| \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \| \qquad\qquad (*)$$
$$0 \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad 0$$

(Les 0 viennent du fait que V est non-trivial sur S_3, car c'est la repré. rég. des 2-Sylow).

On a $H^1(G_{k_3}, \mathbb{Z}/2\mathbb{Z}) = H^1(G_k, \mathrm{Ind}_{G_{k_3}}^{G_k} \mathbb{Z}/2\mathbb{Z})$
$$= H^1(G_k, \underbrace{\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}}_{\text{permut}})$$

Cor: $H^1(G_k, \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \to H^1(G_k, \mathbb{Z}/2\mathbb{Z})$
provient de $(x,y,z) \mapsto x+y+z$ de $(\mathbb{Z}/2\mathbb{Z})^3$ dans $\mathbb{Z}/2\mathbb{Z}$

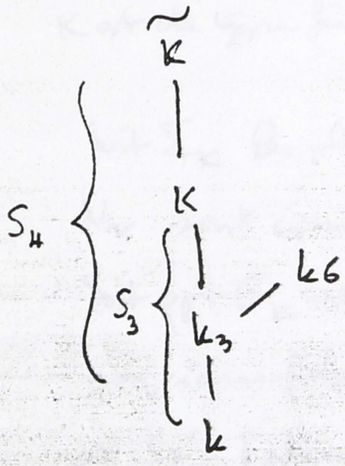
La suite $\to (\mathbb{Z}/2\mathbb{Z})^2 \to \mathbb{Z}/2\mathbb{Z} \to 0$ est exacte

$(1,1,1) \leftarrow 1$

La correspondance fournit pour $\tilde{K}$ une extension k_6 de k_3 (celle associée à la racine d'un élt α de k_3).

On a $\mathrm{Gal}(\tilde{K}/k_3)$ = stabilisateur de la partition $(12)(34)$
$\simeq D_4$

$\mathrm{Gal}(\tilde{K}/k_6)$ = stabilisateur de (12) = stabilisateur de 3 et 4



$\tilde{K} = k(x_1, x_2, x_3, x_4)$

$k_3 = k(x_1x_2 + x_3x_4)$

$k_6 = k_3(x_1+x_2) = k_3\sqrt{(x_1+x_2)^2}$ (*)

$N_{k_3/k}(x_1+x_2)^2 = \sigma_3^2$

$\sigma_3 = x_1x_2x_3 + x_1x_2x_4 + \cdots$

Cas de 5077: k_3 est le corps des racines de $x^3 - 28x - 50 = 0$
avec $\mathrm{disc} = 4 \cdot 5077$.

Les corps cubiques de disc < 100000 (hôt red) ont
< 20000 (complexe)
été dét. par Angell, avec nbre de classes et unités fond.

Duke Math J 76 ~~Bloomer et Cramer~~ Brumer – Kramer.

(*) Noter que $(x_1+x_2)^2 = -(x_1+x_2)(x_3+x_4) = x_1x_2 + x_3x_4 - \sigma_2$ où $\sigma_2 = \sum_{i<j} x_ix_j$
donc $(x_1+x_2)^2 \in k_3$.

Et noter que $\sum x_i = 0 \Rightarrow \sigma_3 = (x_1+x_2)(x_1+x_3)(x_1+x_4)$.
d'où $N_{k_3/k}(x_1+x_2)^2 = \sigma_3^2$

5/11/84 Serre (Cours n°5)

Représentations ℓ-adiques attachées aux variétés abéliennes.

Soit K un corps de nombres (les résultats sont en fait vrais si K est un corps de type fini sur $\mathbb{Q}$; certains s'étendent au cas où K est de type fini sur $\mathbb{F}_p$).

Soit Σ_K les places ultramétriques de K. Si $v \in \Sigma_K$, K_v, p_v, N_v sont comme d'habitude. On pose $G_K = \mathrm{Gal}(\bar{K}/K)$

Soit $\rho_\ell : G_K \to \mathrm{Aut}(V_\ell)$ une représentation continue de G_K, non ramifiée en dehors de $S \cup S_\ell$ (avec $S \subset \Sigma_K$ fini et S_ℓ = {places de K au dessus de ℓ}. Supposons ρ_ℓ rat/$\mathbb{Q}$ relativement à S (ce qui par définition signifie que si $v \notin S \cup S_\ell$, $P_{car}(\rho_\ell(\mathrm{Frob}_v)) \in \mathbb{Q}[T]$.

(variante : idem pour presque tout v ; on ne sait pas si c'est équivalent)

Exemple : A v.ab / K, S ens. des places de mauvaise réduction, $V_\ell = V_\ell(A) = H_1(A_{/\bar{K}}, \mathbb{Q}_\ell)$. Le polynome caractéristique de $\rho_\ell(\mathrm{Frob}_v)$ coïncide avec le pol. caractéristique de l'endom de Frob. de $\bar{A}_v$ (réd. de A mod v).

Si ℓ_1, ℓ_2 sont deux nombres premiers, ρ_{ℓ_1} et ρ_{ℓ_2} rat. (par rapport à S), sont dits compatibles (par rapp. à S) si $P_{car}(\rho_{\ell_1}(\mathrm{Frob}_v)) = P_{car}(\rho_{\ell_2}(\mathrm{Frob}_v))$ pour $v \notin S \cup S_{\ell_1} \cup S_{\ell_2}$

(variante : idem pour presque tout v ; on ne sait pas si il y a équivalence.)

Si on connaît ρ_{ℓ_1}, il y a au plus une ρ_{ℓ_2} semi-simple compatible avec ρ_{ℓ_1} (conséquence immédiate de Čebotarev)

Problème 1 : Si ρ est une repés. ℓ-adique rat., et $\ell' \neq \ell$, existe-t-il une repés. ℓ'-adique compatible avec ρ, sauf peut-être pour un nbre fini de ℓ' ?

Remarque : H_3 se plonge dans $GL_2(\mathbb{Q}_\ell)$ pour $\ell \neq 2$ mais pas dans $GL_2(\mathbb{Q}_2)$: il se plonge dans (quat. ou 2)*, ceci montre que dans le pb. 1, on ne peut espérer "pour tout ℓ'". Cependant le phénomène n'est pas la seule obstruction à "pour tout ℓ'" comme le dit Serre.

Problème 2 : Une repés. ℓ-adique a un analogue sur $\mathbb{R}$: c'est une forme modulaire ou une repés. d'un groupe algébrique (cf a) Größencharakter
b) Conj de Weil)
. Quel est-il ?

Problème 3 : Soient $\rho_{\ell_1}, \rho_{\ell_2}$ deux représentations du type précédent, compatibles et semi-simples. Si ρ_{ℓ_1} vérifie la repés. mixte, en est-il de même de ρ_{ℓ_2} ?
(en appliquant ceci aux puissances tensorielles, ceci entraîne que les invariants de ρ_{ℓ_1} et ρ_{ℓ_2} ont même dimension) C'est lié à la conj. de Tate concernant les classes de cycles {algébriques / de Hodge absolu

Soit A une variété abélienne, ℓ un nbre premier,

$\rho_\ell : G_K \to GL_{2d}(\mathbb{Q}_\ell) = Aut(V_\ell)$

G_ℓ l'image de ρ_ℓ

Thm de Faltings : la représentation V_ℓ est semi-simple. Son commutant est $\mathbb{Q}_\ell \otimes End_K(A)$

Soit $\underline{G}_\ell$ l'adhérence de Zariski de G_ℓ dans $GL_{2d}/\mathbb{Q}_\ell$

On a $G_\ell \subset \underline{G}_\ell(\mathbb{Q}_\ell)$

Thm (Bogomolov). - G_ℓ est ouvert dans $\underline{G}_\ell(\mathbb{Q}_\ell)$

Ceci équivaut à dire que $\mathfrak{g}_\ell = Lie(G_\ell)$ est égal à $Lie(\underline{G}_\ell)$, ou encore que $\mathfrak{g}_\ell$ est une alg. de Lie algébrique (au sens de Chevalley)

Th 2. $\underline{G}_\ell$ contient G_m (homothéties)

$\underline{G}_\ell$ est un groupe réductif. Soit $\underline{G}_\ell^\circ$ la composante neutre.

Th 3. Le quotient $\underline{G}_\ell / \underline{G}_\ell^\circ$ est indépendant de ℓ (et ce noyau $G_K \to \underline{G}_\ell / \underline{G}_\ell^\circ$ est indép de ℓ)

On sait que $\mathfrak{g}_\ell = c_\ell \oplus s_\ell$ avec c_ℓ abélienne et s_ℓ semi-simple, d'où $\underline{G}_\ell^\circ = T_\ell S_\ell$ avec T_ℓ tore central S_ℓ semi-simple connexe, $T_\ell \cap S_\ell$ fini.

Th 4 T_ℓ est indépendant de ℓ (i.e il provient d'un tore sur $\mathbb{Q}$, indépendant de ℓ)

Th 5 Le rang de S_ℓ (ou celui de $\underline{G}_\ell^\circ$, cela revient au même via le Th 4) est indépendant de ℓ. Plus précisément les tores maximaux de $\underline{G}_\ell^\circ$ provenant

(après extension des scalaires) d'un tore/$\mathbb{Q}$ plongé dans $GL_{2d}/\mathbb{Q}$.

Th. 6 A est de type (A4) $\Leftrightarrow$ $S_\ell = \{1\}$ i.e. G_ℓ abélien ∀ ℓ.

Démonstrations Sauf pour le th. 3, on peut supposer que $\mathrm{End}_K(A) = \mathrm{End}_{\bar{K}}(A)$. Posons alors

$\Lambda = \mathbb{Q} \otimes \mathrm{End}_K(A)$

Soit Z le centre de Λ $\quad Z = \prod Z_\alpha$ avec les Z_α corps

$\Lambda = \prod \Lambda_\alpha$ avec Λ_α central simple sur Z_α.

$Z_\ell = Z \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$ opère sur V_ℓ d'où $Z_\ell^\times \hookrightarrow \mathrm{End}\, V_\ell$.

Si M est une alg. commutative semi-simple sur $\mathbb{Q}$,

$M^* = T_M(\mathbb{Q})$

On a $Z_\ell^\times = T_Z(\mathbb{Q}_\ell)$. On a lie $T_Z(\mathbb{Q}_\ell) = Z_\ell$ plongé dans $\mathrm{End}(V_\ell)$

Lemme : Le tore T_ℓ est contenu dans T_Z, ce qui revient au même C_ℓ est contenu dans $Z_\ell = \mathrm{Lie}_{\mathbb{Q}_\ell} T_Z$

En effet C_ℓ commute à G_ℓ, donc à G_ℓ après extension des scalaires, et C_ℓ commute à $\Lambda_\ell \cdot \mathcal{O}_\ell$ par Faltings le commutant de G_ℓ est Λ_ℓ, d'où $C_\ell \subset$ centre de Λ_ℓ, i.e. $C_\ell \subset Z_\ell$

$W_\ell = \det_{Z_\ell} V_\ell$ est un Z_ℓ-module projectif

$\det_Z \rho_\ell : G_K \to Z_\ell^\times$ (factorise par G_ℓ)

au niveau des alg. de Lie $C_\ell \oplus S_\ell \to Z_\ell$ annule S_ℓ et $\ldots$ $\quad C_\ell = \sum C_{\ell,\alpha} \subset \bigoplus Z_{\alpha,\ell}$

l'image de $c(\rho)$ est $\sum d_{\chi,\ell}\,\xi_{\chi,\ell}$ avec $d_{\chi,\ell} = \dim_{\mathbb{Z}_\ell} V_\chi$.
Comme ces $\mathbb{Z}$ sont une $\mathbb{Z}$-base, il suffit de voir que l'image de $\det_{\mathbb{Z}}(\rho): G_K \to \mathbf{Z}_\ell^\times$ est algébrique, indépendante de ℓ, contient G_m.
(cf. Mc Gill, 1967, Hamiart DPP, 1980-81)

Principe : Frob_v a dans $\mathbf{Z}_\ell^\times$ une image dans $\mathbb{Z}^\times$ indépendante de ℓ.

On a ensuite 2 méthodes : soit par transcendance (Waldschmidt - Hamiart), soit en utilisant la décomposition de Hodge-Tate.

Exercice : Expliciter $\det_{\mathbb{Z}}(\rho)$.

2 méthodes a) Analyse dans Schemmel
b) Utiliser Hodge-Tate (module Thm. 1)

Nous avons démontré le th. 4. Prouvons le th. 2. En fait

Lemme : Si $v \notin S \cup S_\ell$ et π_v = image de Frob_v dans $\mathrm{Aut}(V_\ell)$, le plus petit sous-groupe algébrique de GL_{2l} contenant π_v contient G_m. En effet si π est une matrice semi-simple inversible, $\pi = \begin{pmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_N \end{pmatrix}$, l'enveloppe algébrique du groupe engendré par π est $\left\{ \begin{pmatrix} t_1 & & 0 \\ & \ddots & \\ 0 & & t_N \end{pmatrix} \Big/ \prod t_i^{m_i} = 1 \text{ si } \prod \lambda_i^{m_i} = 1 \right\}$.

Pour montrer que les homothéties sont dans l'enveloppe il faut prouver que $\prod \lambda_i^{m_i} = 1 \Rightarrow \sum m_i = 0$. Ceci résulte du fait que les λ sont tous de valeur absolue $q^{w/2}$.

Théorème 7 $G_\ell^0 = T_\ell \iff A$ de type CM/K ($\iff \eta_g(\mathrm{End}_{\bar{K}}(A)\otimes\mathbb{Q}) = 2g$ où $g = \dim A$)

avec η_g = dimension maximum des sous-alg. commutatives étales

(A de type CM $\Leftrightarrow$ A isogène à un produit de v.ab simples d'anneau d'end. $\otimes\mathbb{Q}$ un corps Z. de degré $2\dim A$ sur $\mathbb{Q}$.

L'implication $\Rightarrow$ résulte de Faltings (en effet le commutant de $\mathbb{Z}_\ell$ dans $\mathrm{End}\, V_\ell \otimes \mathbb{Q}_\ell$ est de rang $2g$) et celui de G_ℓ est à priori plus grand si $G_\ell^0 = T_\ell$)

Exercice (Austin de Bruce Jordan) : Soit A une var. abél. $v \notin S$; $\bar{A}_v$ supersinguliere si une puissance de Frobenius est une homothétie, i.e. si $\bar{A}_v$ est produit de c. abél. supersinguliers.

Prop : Si A n'est pas de type CM (sur $\bar{K}$), les $v \notin S$ tels que $\bar{A}_v$ soit supersinguliere sont de densité 0. En fait $\mathrm{Card}\{v / v \text{ cette propriété et } Nv \leq x\} = O\left(\frac{x}{(\log x)^{1+\delta}}\right)$ avec $\delta > 0$.

Dém : Soit ℓ choisi. Considérons l'image H_ℓ de G_ℓ dans $PGL(V_\ell)$. Dire que $\bar{A}_v$ est supersinguliere signifie que l'image $\Pi_v^{H_\ell}$ de Frob v dans H_ℓ est d'ordre fini

Lemme : Soit H une groupe de Lie ℓ-adique compact dont l'alg. de Lie n'est pas résoluble. Les éléments d'ordre fini de H forment un sous-ensemble analytique de H d'intérieur vide.

Les v avec Frob$_v$ dans cet ensemble sont de densité 0.

Il existe H^0 ouvert dans H sans él^t d'ordre fini $\neq 1$. Si $x \in H$ d'ordre fini $x^{[H:H^0]} = 1$. Donc $n = [H:H^0]$ $\{x / x^n = 1\}$ est une sous-variété analytique de H.

Soit x un pt intérieur de H_m. Notons $Ad(x)$ l'automorphisme $y \mapsto xyx^{-1}$ de $\mathfrak{h} = \mathrm{Lie}\, H$.

$\mathrm{Ker}(Ad(x) - 1) = \mathrm{Lie}$ (Centralisateur de x)

C_x est discret (sinon il existe $c_n \in C_x$, $c_n \to 1$, C_x^0

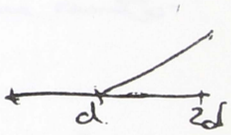
d'où $(c_n x)^m = 1$ d'où $c_n^m = 1$, absurde)

Ainsi $\mathrm{Ker}(Ad(x) - 1) = 0$.

Thm 9 (Borel-Mostow). Toute alg. de Lie (en car. 0) qui a un automorphisme sans pt fixes est résoluble.

Ceci achève le thm 8.

En sens inverse, on conjecture que tout arc réd. ordinaire (i.e. où $\sigma_1, \ldots, \sigma_d$ d premières pts symétriques entiers) est de densité > 0



~~[illegible]~~ On sait seulement le faire pour σ_1 et σ_2 (car la boule de σ_1 et σ_2 est $O(p)$ et divisibilité par $p \Leftrightarrow$ un nbre fini d'équations)

12/11/84 Serre. (Cours n°6)

Borel Mostow : Soit $\mathfrak{g}$ une alg. de Lie de dim finie (ou cas $\mathbb{C}$)
Si $\sigma \in \mathrm{Aut}(\mathfrak{g})$, $\sigma x \neq x$ pour $x \neq 0$, $\mathfrak{g}$ est résoluble
Steinberg : Endom of lin. alg groups : étude des end de gr. lin. alg

1er pas : $\mathfrak{g}$ peut être supposée semi-simple (si $\mathfrak{r}$ est le radical de $\mathfrak{g}$, $\mathfrak{g}/\mathfrak{r}$ est semi-simple et si σ n'a pas de val. propre 1 sur $\mathfrak{g}$ il n'en a pas plus sur $\mathfrak{g}/\mathfrak{r}$)

Soit G le groupe adjoint ; σ se relève en un automorphisme de G.

Lemme : Tout autom. d'un groupe semi-simple conserve un Borel (sur $\overline{K}$)

Soit $\underline{B}$ la variété des Borel, σ opère sur $\underline{B}$. Soit $\Lambda(\sigma)$ le nbre de Lefschetz de σ opérant sur $\underline{B}$ $(= \sum (-1)^i \mathrm{Tr}\, \sigma \mid H^i(\underline{B}))$. On va vérifier que $\Lambda(\sigma) \geq 1$.

Soit T le tore canonique, W son groupe de Weyl ; σ opère sur W. Soit W^σ le sous-groupe fixé par σ. On a :

$$\Lambda(\sigma) = |W^\sigma|$$

Quitte à multiplier σ par un automorphisme intérieur, on peut supposer que σ conserve un couple (B, T)
On a $\underline{B} = \bigcup_w B w B/B = \bigcup_{w \in W} S_w$. La cohom. $H(\underline{B})$ est en degré pair et a pour base les cycles S_w.
$\mathrm{Tr}(\sigma) =$ nbre des S_w fixés par σ. D'où le résultat

σ préserve un Borel B. Soit U le radical unipotent de B. On a $\sigma U = U$. Soit $T = B/U$, σ définit un automorphisme σ_T de T, σ_T préserve le système de racines, le sous-groupe associé à B, le sous-groupe engendré, disons a dans $\mathrm{Lie}\, T$ un plus fixe $\neq 0$.

Résultat : si un automorphisme σ est semi-simple, σ conserve un tore.

Remarques : 1) Si σ a un automorphisme σ d'ordre premier sans points fixes $\neq 0$, σ est nilpotente (en tout cas, d'après Jacobson)

2) Si σ d'ordre 4 : il y a une alg. de Lie sur $\mathbb{C}$ non nilpotente avec un automorphisme sans point fixe d'ordre 4. Soit $G_a(1)$ sur lequel agit G_m par t est. On prend le produit semi-direct $G_m \ltimes (G_a^{(1)} \times G_a(-1))$

(base de l'alg. de Lie x, e, f avec $[x,e] = e$, $[x,f] = -f$, $[e,f] = 0$.

C'est non nilpotent car le centre est 0.

$x \mapsto -x$, $e \to f$, $f \to -e$ est un automorphisme d'ordre 4)

Question : Si G fini a un automorphisme σ sans points fixes $\neq 1$, G est-il résoluble ? (σ sans pts fixes $\Leftrightarrow$ $x \mapsto x \sigma(x)^{-1}$ surjective)

Thompson a prouvé que si σ est d'ordre premier, G est nilpotent.

Si σ d'ordre pq (p, q premiers non nécessairement distincts), alors G est résoluble.

Soit K un corps de car. 0, N un entier ≥ 1 et

$d : GL_N \longrightarrow \mathbb{A}ff_N^*$ cp affine de dim N, muni de l'hyperplan $a_N = 0$.

$x \longmapsto a_1(x) = \Sigma$ val. propres

$a_i(x) = \mathrm{Tr}\, \Lambda^i(x)$

$a_N(x) = \det(x)$

Deux pts x, x' ont $\hat{m}$ images $\Leftrightarrow$ ils ont $\hat{m}$ pol. caract.

$\Leftrightarrow$ leurs comps. semi-simples sont conjugués (sur K ou $\bar{K}$, c'est équivalent)

Th Soit G un sous gp. alg de GL_N. Alors

1) $d(G)$ est Zariski fermé dans $\mathbb{A}ff_N^*$ et défini sur $\mathbb{Q}$.

2) Si G est réductif ~~connexe~~, $\dim d(G) = \mathrm{rg}(G)$.

Plus précisément, si T est un tore maximal de G, $d(T) = d(G)$. Si G est réductif non connexe, on a encore $\dim d(G) = \mathrm{rg}\, G$.

3) Si M_1 et M_2 sont deux groupes ~~connexes~~ de type multiplicatifs, on a $d M_1 = d M_2 \Leftrightarrow M_1$ et M_2 sont $G(\bar{K})$-conjugués dans GL_N.

4) Si $N \subset G$, N invariant dans G et $g \subset G$, alors $d(gN)$ est fermé dans $\mathbb{A}ff_N^*$.

Soit T_N le tore standard de GL_N

$$d\begin{pmatrix} t_1 & & \\ & \ddots & \\ & & t_N \end{pmatrix} = (\sigma_1(t), \sigma_2(t), \dots, \sigma_N(t))$$

c'est un morphisme fini de T_N sur $\mathbb{A}ff_N^*$ surjectif.

Plus précisément $T_N / G_N \simeq \mathbb{A}ff_N^*$.

Rappelons que si M est de type multiplicatif, $\mathcal{A}M$ est fermé de dimension égale à celle de M. En effet quitte à étendre les scalaires, on peut supposer $M \subset T_N$, d'où $\mathcal{A}(M)$ fermé de $\mathbb{Z}^n$ dimension.

Si M_1, M_2 sont connexes et de types multiplicatifs dans T_N avec $\mathcal{A}M_1 = \mathcal{A}M_2$, M_1 et M_2 sont conjugués par G_N (car $T_N \to \mathrm{Aff}_N^*$ est un revêt galoisien, cf AC V, exj des idéaux premiers au dessus d'un idéal).

Tout sous gr. alg.^{M} de T_N est défini sur $\mathbb{Z}$, donc aussi $\mathcal{A}(M)$.

Soit G réductif connexe et T tore maximal de G. Tout él^t semi-simple de G est conjugué géom à un él^t de T. On en déduit $\mathcal{A}(G) = \mathcal{A}(T)$

On a $\mathcal{A}(G) = \mathcal{A}(G/U)$ donc on s'étend au cas où G non réductif. D'où 2) et 1).

Si $x \in G$ et $\sigma \in \mathrm{Aut}(k/\mathbb{Q})$ / montrons que $\mathcal{A}(x)^\sigma \in \mathcal{A}(G)$. Le plus petit sous-gr. alg.^{M} contenant x est de type multiplicatif. On a $\mathcal{A}(M)$ défini sur $\mathbb{Q}$ et $M \subset G$ et donc $\mathcal{A}(x)^\sigma \in \mathcal{A}(M) \subset \mathcal{A}(G)$.

Il reste à prouver 4) et 1) si G non connexe, et de fait 4) avec N connexe, appliqué avec $N = G^\circ$ entraîne 1) et 4). On le fera plus tard.

Soient $\rho_{\ell_1}, \rho_{\ell_2}$ deux repés. ℓ-adiques rationnelles compatibles, semi-simples, de même dimension N. Soient G_{ℓ_1}, G_{ℓ_2} leurs images et $\underline{G}_{\ell_1}, \underline{G}_{\ell_2}$ leurs enveloppes algébriques (qui sont réductives).

Thm. - $\operatorname{rang} \underline{G}_{\ell_1} = \operatorname{rang} \underline{G}_{\ell_2}$

Quitte à étendre le corps de base, on peut supposer les groupes connexes. Alors $\mathcal{A}(G_{\ell_1})$ et $\mathcal{A}(G_{\ell_2})$ sont des fermés, définis sur $\mathbb{Q}$, de Aff_N^*. En fait on a $\mathcal{A}(G_{\ell_1}) = \mathcal{A}(G_{\ell_2})$: des variétés sont l'adhérence de Zariski des pol. de Frobenius, pour $v \notin$ ens. fini de places. Cela prouve le théorème.

Plus précisément, si T_1 et T_2 sont des tores maximaux de $\underline{G}_{\ell_1}$ et $\underline{G}_{\ell_2}$ sont conjugués dans toute extension contenant $\mathbb{Q}_{\ell_1}$ et $\mathbb{Q}_{\ell_2}$

(Plus concrètement, se donner un tore, c'est se donner $\hat{T}$ un $\mathbb{Z}$-module libre de type fini, et se donner une repés de T, c'est se donner $\mathrm{ch}(\rho) = \sum_{\lambda \in \Lambda} n_\rho e^\lambda$ combinaison linéaire formelle, avec les $n_\rho \geq 0$, à support fini. de th. de Weyl dit simplement que les réseaux de T_1 et T_2 avec leurs poids n_ρ sont isomorphes).

Notation :
Soit G un gp alg linéaire, f une fonction sur G (morphisme de G dans la droite affine). Soit

$d_G(f=0)$ = la densité des pts de G où f s'annule

$$= \frac{\text{nbre de comp. connexes où } f=0}{\text{nbre tot de comp. connexes}}$$

Considérons les représentations $\rho_{\ell_1}, \rho_{\ell_2}$ compatibles et soit f une polynôme en les $a_i(x)$ $(= \mathrm{Tr}\,\wedge^i(\rho(x)))$ à coeff dans $\mathbb{Q}$.

Thm $d_{\underline{G}_{\ell_1}}(f=0) = d_{\underline{G}_{\ell_2}}(f=0)$

($d_{\underline{G}_\ell}^{(f=0)}$ = densité des places v de K telles que $f(a_i(\mathrm{Frob}_v))=0$)

Il suffit pour un ℓ fixé de démontrer l'égalité entre parenthèses. On a $G_\ell \subset \underline{G}_\ell(\mathbb{Q}_\ell)$. Soit

$G_\ell^\circ = G_\ell \cap \underline{G}_\ell^\circ$

$\underline{G}_\ell / \underline{G}_\ell^\circ$ est un groupe alg. fini. Tous les pts rationnels sont définis sur $\mathbb{Q}_\ell$ car G_ℓ est Zariski dense dans $\underline{G}_\ell$, et $G_\ell/G_\ell^\circ \simeq \underline{G}_\ell/\underline{G}_\ell^\circ$.

Soit $G_\ell = \bigcup_{\text{disj}} \gamma_\alpha G_\ell^\circ$

Soit $f=0$ sur $\gamma_1 G_\ell^\circ, \dots \gamma_h G_\ell^\circ$ et $f\neq 0$ sur $\gamma_{h+1} G_\ell^\circ, \dots \gamma_{h+k} G_\ell^\circ$. On a $d_{\underline{G}_\ell}(f=0) = \frac{h}{h+k}$.

Pour que $f(a_i(\mathrm{Frob}_v))=0$, il faut et il suffit que Frob_v tombe dans $\gamma_i G_\ell^\circ$ $(1 \le i \le h)$ ou dans une sous-var. alg. $\neq G_\ell^\circ$ de $\gamma_i G_\ell^\circ$ $(h+1 \le i \le h+k)$. D'où le résultat par Čebotarev.

Soit $d(f=0)$ = densité des v avec $f(Frob_v)=0$.

Précision sur le nbre des v avec $f(Frob_v)=0$ et $N_v \leq X$:
il est $d(f=0)\frac{X}{\log X} + O\left(\frac{X}{(\log X)^{1+\alpha}}\right)$

Thm 1. Pour que $\underline{G}_\ell$ soit connexe, il faut et il suffit que, pour tout polynôme $f \in \mathbb{Z}[a_1, \ldots, a_N]$, on ait $d(f=0) = 0$ ou 1.

Corollaire : le noyau de $Gal(\overline{K}/K) \longrightarrow \underline{G}_\ell / \underline{G}_\ell^\circ$ est est indépendant de ℓ.
(En effet c'est le plus petit corps K tel que l'image de G_ℓ est connexe).

Th 2. - Si $g \in G$, $g \notin G^\circ$, $(G = \underline{G}_\ell)$ il existe $f \in \mathbb{Z}[a_1, \ldots a_N]$ avec $f(gG^\circ) = 0$, $f(1) \neq 0$.

(ceci entraîne le th 1)

1ère démo : Soit G groupe linéaire, G° la comp. neutre $g \in G/G^\circ$, $g \neq 1$.
Soit $\sigma : G/G^\circ \to GL(V)$ irréductible avec $\sigma(g) \neq 1$
Soit $\lambda \neq 1$ une valeur propre de $\sigma(g)$, $\lambda \neq 1$, et $n \geq 2$ son ordre.

Remarque : Si G gp. linéaire, et $G \to GL(E)$ repré. fidèle, toute repré. de G est sous-quotient d'une $T_{r,s} = E^{\otimes r} \otimes E^{*\otimes s}$

On prend $E =$ espace de pp
$\sigma : G \to G/G^\circ \to GL(V)$

Si $x \in G$, les $a_i(T_{r,s}x)$ sont des pol. en $a_1(x), \dots, a_N(x)$ et $a_N(x) \neq 0$ car x inversible

Soit $N_{r,s} = \dim T_{r,s} = N^{r+s}$

Soit $f_{1,\lambda}(x) = \left[\lambda^{N_{r,s}} - a_1(T_{r,s}x)\lambda^{N_{r,s}-1} + \dots \pm a_{N_{r,s}}(T_{r,s}x)\right]$

avec q assez grand

Ceci est un polynôme. Posons

$$f = \prod_{\substack{\text{racines} \\ \text{puissances} \\ \text{entières de 1}}} f_{1,\mu}$$

f s'annule sur gG°

On a $f_{1,\mu}(1) \neq 0$ pour tout μ, d'où $f_1(1) \neq 0$.

Autre démonstration (en admettant 4)

Regardons $\mathrm{cl}(gG^\circ)$. Il est fermé d'après 4).

$\mathrm{cl}(1)$ n'est pas dans $\mathrm{cl}(gG^\circ)$ car sinon gG° contiendrait un élt unipotent, dont l'enveloppe algébrique, égale à 1 ou G_a est connexe). On aurait donc $gG^\circ \supset$ sous groupe connexe de G, absurde.

Il existe $P(a_1, \dots, a_N, a_N^{-1})$ qui est $= 0$ sur gG° et $\neq 0$ en 1. Comme les Frob sont bien pol. car $\cdot$ à coeff dans $\mathbb{Q}$ et sont dense dans G, gG° est défini sur $\mathbb{Q}$ et P peut être pris à coeff. rationnels.

Prouvons que si $N \triangleleft G$, N connexe, $g \in G$, $\mathrm{cl}(gN)$ est fermé de dimension $\leq \mathrm{rg}_{\mathrm{red}} N$.

Quelques cas particuliers du th. 4

1) N est un tore, g est semi-simple, commute à N.
Le sous groupe M engendré par N et g est alors de type multiplicatif. Alors $\mathcal{A}(M)$ est fermé

dim $\mathcal{A}(gN)$ = dim N car $\mathcal{A}: T_{stand} \to \mathbb{A}^{ff}$ est fini

2) N est un tore et g est semi-simple.
g induit un automorphisme de N d'ordre fini
$\mathbb{Q} \otimes \hat{N}$ = partie fixe sous g $\oplus$ partie nulle sous g
$\mathrm{Ker}(1-\sigma)$ $\quad = \mathrm{Im}^{g}(1-\sigma^{-1})$

$N = N_+ N_-$

$\begin{cases} N_+ \text{ tore fixé par } \sigma \\ N_- \text{ engendré par les } \sigma(t)t^{-1} \end{cases}$

On a $\mathcal{A}(gN) = \mathcal{A}(gN_+)$
Soit en effet $n \in N$ $\quad n = t_+(\sigma(t)t^{-1})$ avec
$\sigma(t) = g^{-1}tg$ $\quad gn = gt_+g^{-1}tgt^{-1} = tt_+^g t^{-1}$
conjugué de $t_+^g g = gt_+$
Dans ce cas $\mathcal{A}(gN)$ est fermé de dimension égale à dim N_+ (subalgebra de g)
Donc dim $\mathcal{A}(gN) \leq$ dim N avec égalité $\Leftrightarrow$ g commute à N.

19/11/84

Serre (Cours n°7)

Rappel : k alg^t clos

$d : GL_N \to \mathbb{A}^{N*} = \{a_1, \dots, a_N \mid a_N \neq 0\}$

$(M \longmapsto \text{coeff de } P_{car}(M))$

Th. Soit G alg dans GL_N, H sous-gr. alg. distingué dans G. Soit $g \in G$. Alors $d(gH)$ est fermé, de dimension $\leq$ rang réductif (H)

La dém. avait été commencée.

Cas 1, 2 : g semi-simple et H tore.
(Cas 2' : g qcq et H tore (on fera après))
Cas 3 : g semi-simple et H réductif : On utilise le Thm de Borel-Mostow : tout automorphisme semi-simple d'un gr. réductif conserve un tore maximal. (comme automorphisme de l'alg de Lie)

Il existe donc T tore maximal de H avec $gTg^{-1} = T$

Soit $N = N_H(T)$ le normalisateur de T dans H.

On va prouver que $d(gH) = d(gN)$. Comme N est réunion disjointe de $n_\alpha T$ en nbre fini. On conclura grâce à 2'

a) Soit $g' \in gH$ semi-simple. D'après Borel Mostow, il existe un tore maximal T' de H, stable par $\mathrm{Int}(g')$, et T' est de la forme $u^{-1}Tu$ avec $u \in H$. L'égalité

$g'T'g'^{-1} = T'$

$u\, g'u^{-1}\, uTu^{-1}\, ug'^{-1}u^{-1} = T$

$u\, g'u^{-1}$ normalise T.

Comme $u \in H$, $ug'u^{-1} \in gH$ car H distingué dans G.
$= gh$ avec $h \in H$
Comme g et $ug'u^{-1}$ normalisent T, h aussi.
On a donc $ug'u^{-1} \in gN$.

b) Soit $g' \in gH$ quelconque. Par $G \xrightarrow{\pi} G/H$ l'image de g'_{ss} est $\pi(g')_{ss}$ et celle de $g = g_{ss}$ est $\pi(g) = \pi(g)_{ss}$. Comme $\pi(g) = \pi(g')$, on a $g'_{ss} \in gH$

De a) et b) résulte

$$d(g') = d(g'_{ss}) \in d(gN).$$

Prouvons 2') : Si H est réductif, $d(gH) = d(g_{ss} H)$

Dém : Soit $g = g_{ss} g_u$. L'auton $h \to g_u h g_u^{-1}$ est dans la comp. neutre de $\mathrm{Aut}(H)$, donc est intérieur et est un auton intérieur par un élément unipotent α de H. On a donc $\alpha h \alpha^{-1} = g_u h g_u^{-1}$, d'où $g_u = \alpha c$ avec c commutant à H.

On a $\beta = g_{ss} \alpha g_{ss}^{-1}$ qui vérifie

$$\beta^{-1} h \beta^{-1} = (g_{ss} g_u g_{ss}^{-1}) h (g_{ss} g_u g_{ss}^{-1})^{-1} = g_u h g_u^{-1} = \alpha h \alpha^{-1}$$

α et β sont unipotents et diffèrent par un élément central (donc semi-simple) par suite $\alpha = \beta$ et α commute à g_{ss}.

Si $gh \in gH$ $\quad g h = g_{ss} \alpha c h = g_{ss} \alpha h c$

Comme α commute à c et que αc est unipotent et α aussi, c est unipotent et c commute à g_{ss}

Donc $d(gh) = d(g_{ss} \alpha h c) = d(g_{ss} \alpha h)$

Comme $h \mapsto \alpha h$ est bijective, on a l'égalité désirée

4) Cas général.

On remplace l'ext ambiant par son sous-groupe simplifié par rapport à l'action de G. Alors G devient réductif (et H aussi car H est distingué dans G)

On a $d_V(gH) = d_{V^{ss}}(gH)$ et on retombe dans les cas précédents.

La déf donne un critère pour que $\dim d(gH) = \dim gH$: Il faut et il suffit que l'automorphisme σ_g du tore maximal canonique de H soit l'identité (ou moins si H est réductif. A vérifier.

Rappel 2 Soit G un groupe linéaire algébrique, $G \hookrightarrow GL(V)$ une repés. fidèle. Alors toute repés. irréductible $G \to GL(W)$ intervient dans un $T_{r,s}(V) = \hat{\otimes}^r V \hat{\otimes}^s V^*$.

Déf : Si $w \in W$, $w' \in W^*$, le coeff. $m_{w,w'} : g \mapsto \langle gw, w' \rangle$ est un élément de l'alg. affine de G.
Si la repés. dans V est fidèle, l'alg. affine de G est engendrée par les monômes en les a_{ij} et $(\det)^m$ $m \in \mathbb{Z}$ (et ceux ci sont des coeff. de $\hat{\otimes}^r V \hat{\otimes}^s V^*$). Un coeff de W est donc une comb. lin. de coeff d'un certain $T_{r,s}$. On a

Lemme : Soient W, E deux repés. de G, avec W irréductible. Si un coeff. de W est comb. lin. de coeff de E, W intervient dans E.

Quitte à remplacer E par $E^n \oplus \dots$ on peut supposer que les coeff. sont égaux. Soit $m_{ww'} = m_{\varepsilon\varepsilon'}$ ($\varepsilon \in E$, $\varepsilon' \in E'$). Dans $W \oplus E$, $x = (w, -\varepsilon)$ et $x' = (w', +\varepsilon')$ vérifient $\langle gx, x' \rangle = 0$. Les transformés de x sont contenus dans $x'^\perp$. Soit F le plus petit sous esp. de $W \oplus E$ contenant x, stable par G.

On a $F \cap W \oplus \{o'\} = \{o\}$ car $F \perp x'$

la proj de F sur W est tout (car IN irréductible et la projection contient x).

$F \to E$ est injectif et W est un quotient de F

cqfd.

A v. ab sur K corps de nbres, de dim n.

ℓ nbre premier

$V_\ell(A) \simeq \mathbb{Q}_\ell^{2n}$

$G = Gal(\bar{K}/K) \xrightarrow{\rho_\ell} GL(V_\ell(A)) \simeq GL_{2n}(\mathbb{Q}_\ell)$

G_ℓ image de G, $\underline{G}_\ell$ env. alg de G_ℓ

$\underline{G}_\ell$ est réductif. On a vu que son rang (et son tore maximal) sont indépendants de ℓ.

Si on choisit une polarisation de A, définie sur K, cela donne une forme bil. alternée non dégénérée sur V_ℓ et on a, pour $\sigma \in G$, $\langle \sigma x, \sigma y \rangle = \chi_\ell(\sigma) \langle x, y \rangle$ où χ_ℓ est le caractère cyclotomique.

En particulier si v a bonne réduction, et $\pi_v = Frob_v$.

$$\langle \pi_v x, \pi_v y \rangle = N_v \langle x, y \rangle$$

$\underline{G}_\ell$ est donc contenu dans le groupe des similitudes symplectiques CSp_{2n}

On a un hom. $CSp_{2n} \to \mathbb{G}_m$, le multiplicateur de la similitude (sur $\bar{\mathbb{Q}}_\ell$, $CSp_{2n} = Sp_{2n} \mathbb{G}_m$ et le mult. induit $x \mapsto x^2$ sur $\mathbb{G}_m$).

On a $rg(\underline{G}_\ell) \leq 1+n$.

Th. Si $\mathrm{End}_{\bar{K}} A = \mathbb{Z}$

$\dim G_\ell = 1+n \iff G_\ell = CSp_{2n,\ell}$

Corollaire Si $G_\ell = CSp_{2n,\ell}$ pour un ℓ, $G_\ell = CSp_{2n,\ell}$ pour tout ℓ.

(En effet $G_\ell \simeq CSp_{2n,\ell} \Rightarrow \mathrm{End}_{\bar{K}} A = \mathbb{Z}$)

Déf des Thm

$g_\ell = c_\ell \oplus s_\ell \qquad s_\ell \subset Sp_{2n}$

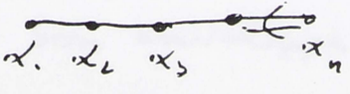
c_ℓ = homothéties et la repré. naturelle de s_ℓ est absolument irréductible, d'après Faltings. On a s_ℓ abs. irréd. et de rang n dans $Sp_{2n,\ell}$.

Lemme (Borel de Siebenthal) : soit $\mathfrak{a}$ une alg. de Lie simple de rang n, $s \subset \mathfrak{a}$ semi-simple de rang n. Comment détermine-t-elle qui sont max $\neq \mathfrak{a}$.

Recette α_i base des racines de $\mathfrak{a}$

$\tilde{\alpha} = \sum m_i \alpha_i$ plus grande racine

Soit i tel que m_i soit premier et R_i le sous-sys. de R formé des racines avec $\alpha_i \equiv 0 \bmod m_i$ (coeff de α_i). Alors R_i est un syst. de racines de même rang, max et à conj près ils sont tous ainsi.

Sp_{2n} : 

$\tilde{\alpha} = 2\alpha_1 + 2\alpha_2 + \dots + 2\alpha_{\ell-1} + \alpha_\ell$.

Pour chaque $i \leq n-1$, $V_{2n} = V_{2i} \oplus V_{2n-i}$ orthogonale

$Sp_{2i} \oplus Sp_{2n-2i} \hookrightarrow Sp_{2n}$. Toutes les sous alg. de Sp_{2n} max. de rang max sont de cette forme, mais elles ne sont pas irréductible, donc ne conviennent pas

CONTD

Remarque : pour les gpes classiques, c'est la même chose mais pas pour les gpes exceptionnels.

Géométriquement sur les diagrammes de Dynkin, on prend le diagramme complété et on supprime le sommet d'indice i.

Compléments

$l \neq p$.

Que se passe-t-il lorsque K est un corps de fonctions sur un corps fini.

- Semi-simplicité des V_ℓ } en car $\neq 2$ (Zarhin)
- Commutant = endom $\otimes \mathbb{Q}_\ell$ } en car 2 (Moi non publié) (Nori Bailly, thèse)

On a $G_\ell \subset \underline{G}_\ell$ env. alg.

$\underline{G}_\ell$ est un gpe réductif.

On peut décomposer $\underline{G}^\circ_\ell = T_\ell S_\ell$.

T_ℓ est défini sur $\mathbb{Q}$, indépendant de ℓ, contenu dans le tore des centre des endomorphismes de A.

$\mathrm{Lie}\, \underline{G}_\ell = t_\ell \oplus s_\ell$.

$\mathfrak{g}_\ell = \mathrm{Lie}\, G_\ell = z_\ell \oplus s_\ell$ avec $\dim z_\ell = 1$.

(comme $\mathfrak{g}_\ell$ est réductive elle contient la dérivée de son enveloppe algébrique, s_ℓ)

Pour prouver que $\dim z_\ell = 1$, il suffit de montrer que $\mathbb{Z}_\ell \times \mathbb{Z}_\ell$ n'est pas quotient d'un $\mathrm{Gal}(\bar{K}/K)$ (utiliser la th. des corps de classes).

Exemple : Soit $E/\mathbb{F}_q$ ordinaire, considérée par cet. des scalaires comme courbe sur $\mathbb{F}_q(\sqrt{\ })$. Elle a mc. par $\mathbb{Q}(V_\ell)$ qui fournit un tore T de dim 2. Le Frobenius sur $\mathbb{F}_q$ donne $\pi \in T(\mathbb{Q})$ et z est la seule vp analytique req par π.

Le rang de $\underline{G}_\ell$ est indép de ℓ, ainsi que celui de g_ℓ. De plus $\underline{G}_\ell / \underline{G}_\ell^0$ est indép de ℓ.

Définition : Soit $n \geq 1$. Dans GL_{2n} un tore "de type H" est un tore géométriquement conjugué à $\begin{pmatrix} \lambda & & 0 \\ & \ddots & \\ & & \lambda \\ & & & \mu \\ 0 & & & & \ddots \\ & & & & & \mu \end{pmatrix}$

Théorème : Le groupe G_ℓ contient un tore "de type H" (géométriquement)

(ceci n'est pas vrai sur les corps de nbs)

Ex : cas des courbes elliptiques :

- sans mult. compl : $G_\ell = GL_2 \supset \begin{pmatrix} * & * \\ 0 & * \end{pmatrix}$
- avec " " : G_ℓ est un tore (de type H après ext. des scalaires)

Soit v une place de K divisant ℓ et $\bar{v}$ une place de $\overline{K}$ prolongeant v. On a $G \supset D_v \supset I_v$ (D_v gp de déc de $\bar{v}$, I_v " d'inertie de v)

La restriction de la représentation ℓ-adique à I_v contient (géométriquement) un tore $H_{1/\ell}$ $\left(\simeq \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ & & 1 \\ 0 & & & \ddots \end{pmatrix}\right)$: c'est la théorie des modules de Hodge-Tate.

Or les homothéties sont contenues dans G_ℓ. D'où le résultat.

Exemple : Si $\dim A = 2$ et $\mathrm{End}_{\bar{K}} A = \mathbb{C}$

$$\underline{G}_\ell = \mathbb{G}_{\mathrm{m}}.$$

En effet $\mathfrak{g}_\ell$ = homothéties $\oplus$ $\mathfrak{s}_\ell$ avec $\mathfrak{s}_\ell \subset \mathfrak{sp}_4$ absolument irréductible.

Si $\dim \mathfrak{s}_\ell = 2$ $\quad \mathfrak{s}_\ell = \mathfrak{sp}_4$ (déjà vu)

Si $\dim \mathfrak{s}_\ell = 1$ $\quad \mathfrak{s}_\ell \simeq \mathfrak{sl}_2$ (géométriquement) et la repré. de dim 4 de $\mathfrak{sl}_2$ est Sym^3 (repré. évidente).

On aurait donc $\underline{G}_\ell \simeq \mathrm{GL}_2$ dans sa repré. Sym^3. Le tore max de GL_2 dans Sym^3 s'écrit $\begin{pmatrix} \lambda^3 & 0 & 0 & 0 \\ 0 & \lambda^2\mu & 0 & 0 \\ 0 & 0 & \lambda\mu^2 & 0 \\ 0 & 0 & 0 & \mu^3 \end{pmatrix}$ donc a 4 caractères différents et n'est pas de type (H). Contradiction.

(On pourrait tenter de faire la même chose si $\dim A = 3$, mais on aura à exclure le groupe suivant

$\mathrm{SO}_3 \otimes \mathrm{GL}_2$ agissant sur $W \otimes V$ avec W muni d'une forme quad., V d'une f. alt, et $W \otimes V$ de la f. produit tensoriel. Or $1 \otimes \begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix}$ est un tore de type (H).

Nous montrerons plus tard que ce groupe est impossible).

Problème. Soit X le sous-groupe alg. de G_ℓ° engendré par les conjugués (géom.) des tores de G_ℓ° de type H. Est-il vrai que $X = \underline{G}_\ell^\circ$?

Remarque : la représentation galoisienne dans G_ℓ° / X est, quitte à étendre les scalaires, non ramifiée au-dessus de ℓ

26/11/84

Xème (Cours n°8)

Tores de Frobenius

Soit k un corps parfait et s un élément de $GL_N(k)$. On s'intéresse au plus petit sous-groupe algébrique de GL_N contenant s, que l'on notera Θ_s.

On se restreindra au cas où s est semi-simple. Alors Θ_s est un sous-groupe multiplicatif, isomorphe sur $\bar{k}$ au produit d'un tore par un groupe fini cyclique.

Remarque: après extension des scalaires, on peut mettre s sous la forme $\mathrm{diag}(\lambda_1, \dots, \lambda_N)$ et Θ_s est l'ensemble des $\mathrm{diag}(x_1, \dots x_N)$ où Θ_s x_i satisfont les relations monomiales satisfaites par les λ_i.

Autre description: un groupe multiplicatif est connu lorsqu'on connaît son groupe de caractères

$\chi = X(\Theta_s) = \mathrm{Hom}_{\bar{k}}(\Theta_s, \mathbb{G}_m)$ et la représentation $\rho: \Theta_s \to GL_N$ est déterminée par son caractère $\mathrm{tr}(\rho) = \sum_{x \in X} n_x x$ avec les n_x positifs, presque tous positifs, et puisque ρ est définie sur k, $\mathrm{tr}(\rho)$ est $\mathrm{Gal}(\bar{k}/k)$-invariant.

En fait: $X(\Theta_s)$ s'identifie au sous-groupe de $\bar{k}^\times$ engendré par les valeurs propres λ_i de s: à λ valeur propre correspond $\chi_\lambda \in X(\Theta_s)$ tel que $\chi_\lambda(s) = \lambda$. On a

$$\mathrm{tr}(\rho) = \sum_\lambda \chi_\lambda.$$

Si T_S est le tore maximal de G_S, on a

$$X(T_S) = X(G_S) / X(G_S)_{\text{tors}}.$$

= (sous-gr. engt par les val. propres) / (racines de l'unité qu'il contient)

Soit A une variété abélienne de dim n / $\mathbb{F}_q$

À l'endom. de Frobenius π de A on associera comme ci-dessus $\mathcal{G}_\pi$ et T_π. Comme ces groupes alg. ne dépendent que des polynômes caractéristiques de π, il pourrait être défini sur $\mathbb{Z}$.

Autre solution : $\mathbb{Q}[\pi] \subset \mathbb{Q} \otimes \mathrm{End}\, A$. La grande subst. de $\mathbb{Q}[\pi]$ est représenté par un tore $T_{\mathbb{Q}(\pi)}$ et $\mathcal{G}_\pi$ est le plus petit sous-gr.-alg de $T_{\mathbb{Q}(\pi)}$ contenant π.

Remarque : il existe un espace vectoriel V_0 sur $\mathbb{Q}$ de dim $N = 2n$, muni d'une action de $\mathbb{Q}(\pi)$ tel que, pour chaque ℓ, $V_0 \otimes \mathbb{Q}_\ell \simeq V_\ell$ comme $\mathbb{Q}_\ell[\pi]$-module (et q variable)

Théorème 1 Pour n donné, il n'existe qu'un nombre fini de $(T_\pi, \mathcal{G}_\pi)$ dans GL_N, à conjugaison géométrique près.

Ex : $n=1$, $N=2$: on a deux possibilités pour T_π : le tore des homothéties $\begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}$ ou $\begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix} \simeq \mathbb{G}_m \times \mathbb{G}_m$.

Démonstration

1ère pas : il existe une borne ne dépendant que de n à $(\mathcal{G}_\pi : T_\pi)$: en effet le dual de ce groupe est l'ensemble des racines de 1 contenues dans le corps engt par les λ : ce corps est de degré borné ($\leq N!$)

Il reste à montrer que l'ordre $(\Theta_\pi : T_\pi)$ est borné.

On suppose $n \geq 1$. Alors G_m est contenu dans T_π (remarque de Deligne vue dans un cas précédent). Il correspond par dualité à un homomorphisme $X(\Theta_\pi) \to \mathbb{Z}$ qui à chaque λ associe 1 : cet homomorphisme est $\lambda \longmapsto 2\frac{\log(\lambda)}{\log q}$.

On a d'autre part un homomorphisme canonique $\Theta_\pi \longrightarrow G_m$ qui à π associe q : le composé $G_m \to \Theta_\pi \to G_m$ est l'élévation au carré.

On a $\Theta_\pi \underset{\text{géom}}{\subset}$ tore maximal de CSp_{2n}

Ce dernier est $\{ \mathrm{diag}(x_1, \dots, x_n, y_n, \dots, y_1) / x_1 y_1 = x_2 y_2 = \dots = x_n y_n \}$

L'homomorphisme $\Theta_\pi \to G_m$ est induit par $(x_1, \dots, x_n, y_1, \dots, y_n) \mapsto x_1 y_1$.

Soit $n = 2$: on a pour T_π quatre possibilités :

1) $x_1 = x_2 = y_2 = y_1$ (c'est le cas si $A = E \times E$ avec E supersingulière) • 4

2) $x_1 = x_2$, $y_2 = y_1$ (c'est le cas si $A = E \times E$ avec E ordinaire) 2 2

3) $x_2 = y_2$ (tore de dim 2) (c'est le cas si $A = E \times E'$ avec E supersingulière et E' ordinaire) 1 2 1

4) tore maximal : pas de relations autres que $x_1 y_1 = x_2 y_2$ 1 1 1 1

On va utiliser les renseignements p-adiques sur η (et le fait que les valeurs propres sont des unités l-adiques pour $l \neq p$).

Soit $X \subset \overline{\mathbb{Q}}^*$ le sous-gp. engendré par les valeurs propres de π et w une place ultra. de $\overline{\mathbb{Q}}$ prolongeant la valuation p-adique de $\mathbb{Q}$. Les tels w sont conjugués par $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$

X est le groupe des caractères de T. Un groupe à 1-paramètre de T correspond à un homomorphisme $X \to \mathbb{Z}$. Or $\lambda \overset{\varphi_w}{\longmapsto} \frac{w(\lambda)}{w(q)}$ est un homomorphisme non trivial de X dans $\mathbb{Q}$. Il existe $\delta \geq 1$ entier tel que $\varphi_w(X) \subset \frac{1}{\delta}\mathbb{Z}$, d'où $\delta\varphi_w(X) \in \mathbb{Z}$. Alors $\delta\varphi_w$ correspond à un groupe à un paramètre de T, dont l'image ne dépend pas de δ.
(La remarque de Bolzano généralise le groupe à un paramètre des homothéties de façon analogue à partie de la valeur absolue archimédienne).

Si $\frac{w(\lambda_i)}{w(q)} = \varepsilon_i$, le groupe à un paramètre est

$$\{\mathrm{diag}(\lambda^{\delta\varepsilon_1}, \ldots, \lambda^{\delta\varepsilon_N})\} = \{\mathrm{diag}(\lambda^{\varepsilon_1}, \ldots, \lambda^{\varepsilon_N})\}.$$

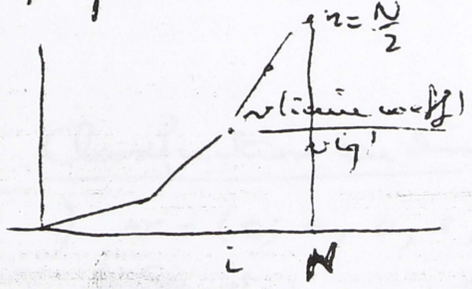
Lemme 1 : pour n fixé, les ε_i ne prennent qu'un nombre fini de valeurs : on a $0 \leq \varepsilon_i \leq 1$ et le dénominateur des ε_i est $\leq N = 2n$.

Lemme 2 : Les sous-groupes à un paramètre associés aux différentes places v dépendent T_π.

Cet lemme implique le th. 1.

Dém du lemme 2 : L'intersection du noyau des φ_v est réduite aux racines de l'unité de X, car si λ appartient à cette intersection, λ est une unité ℓ-adique pour $\ell \neq p$ et $v(\lambda) = 0$ pour $v \nmid p$. D'autre part toutes les valeurs absolues archimédiennes de λ sont les mêmes. La formule du produit entraîne alors que $|\lambda| = 1$ pour toute valeur absolue de $\overline{\mathbb{Q}}$, donc que λ est une racine de l'unité.

Les ε_i sont les pentes du polygone de Newton du polynôme caractéristique de Frobenius inverse $\prod_{i=1}^{N}(1 - \lambda_i X)$

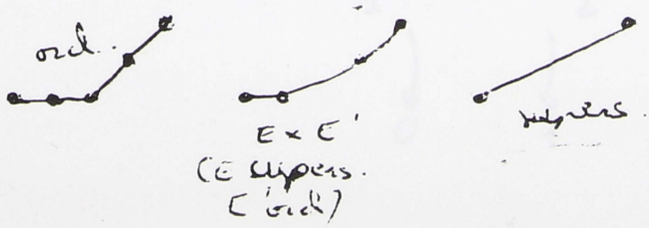


On a $\varepsilon_i \geq 0$ car λ_i entier.
$\varepsilon_i \leq 1$ car $v(\lambda_i) + v(\bar{\lambda}_i) = 1$.

Thm : Les sommets du polygone ont des coordonnées entières (ce qui implique le lemme 1)

Exemple : $n = 1$

$n = 2$



(on a une certaine symétrie dire un fait que $v(\lambda_i) + v(\bar{\lambda}_i) = 1$)

Le théorème est vrai pour les représentations
l-adiques $H^i(V \otimes \overline{\mathbb{F}_q}, \mathbb{Q}_\ell)$ avec V projective
lisse sur $\mathbb{F}_q$ (mais $\varepsilon_i \in 1$ est remplacé par $\varepsilon_i \in \mathbb{Z}$)

Le groupe p-divisible attaché à la variété
abélienne se décompose en morceaux irréductibles
indexés par (r,s) premiers entre eux avec pour
pente $\frac{r}{r+s}$ de multiplicité $r+s$.

Corollaire : Si δ est le dénominateur d'un $\varepsilon = \frac{\nu(\alpha_i)}{\nu(q)}$
le nombre de λ_i qui donnent ε est divisible par δ.

Ex : $n=3$

$0\ 0\ 0\ 1\ 1\ 1$
$0\ 0\ \frac{1}{2}\ \frac{1}{2}\ 1\ 1$
$0\ \frac{1}{2}\ \frac{1}{2}\ \frac{1}{2}\ \frac{1}{2}\ 1$
$\frac{1}{2}\ \frac{1}{2}\ \frac{1}{2}\ \frac{1}{2}\ \frac{1}{2}\ \frac{1}{2}$
$\frac{1}{3}\ \frac{1}{3}\ \frac{1}{3}\ \frac{2}{3}\ \frac{2}{3}\ \frac{2}{3}$

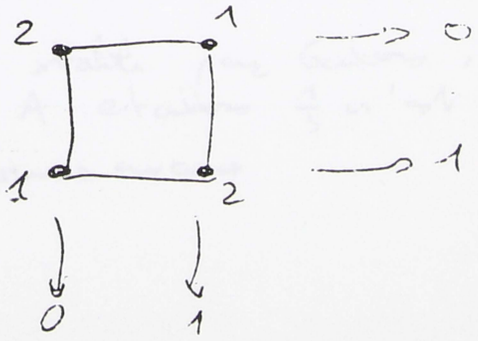
sont les seules possibilités

Classification en dim 3 / $\varphi_r : X \to \mathbb{P}^r$ rompus.

1) $\nu = (0,0,0,1,1,1)$

Si l'espace affine engendré par les noeuds est
de dim 1 on doit avoir

de dim 2 on doit avoir

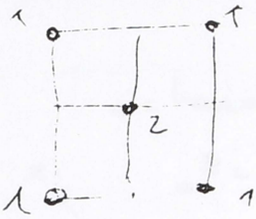


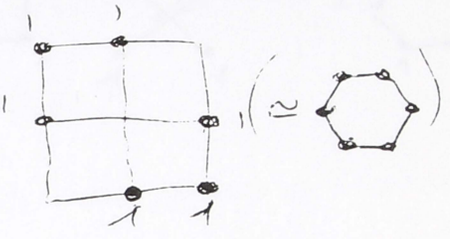
dim 3

2) $v = (0, 0, \frac{1}{2}, \frac{1}{2}, 1, 1)$

dim 1

dim 2



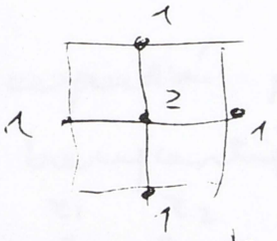


dim 3 comme avant.

3) $v = (0, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}, 1)$

dim 1

dim 2



dim 3 comme avant

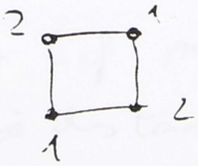
4) $v = (\frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2})$

6

5) $\frac{1}{3}\ \frac{1}{3}\ \frac{1}{3}\ \frac{2}{3}\ \frac{2}{3}\ \frac{2}{3}$

dim 1

dim 2

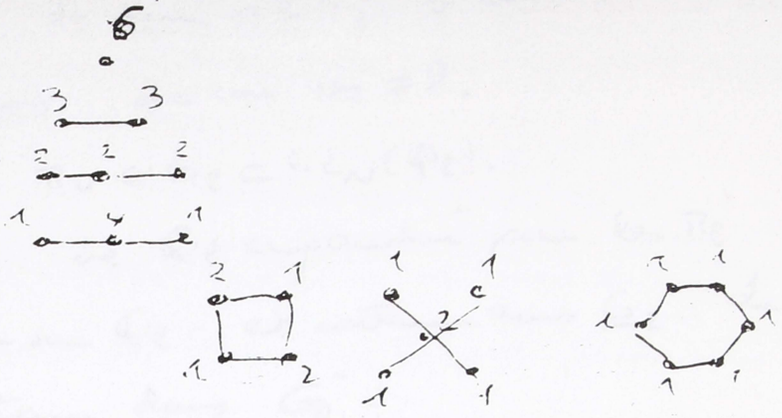


Ceci est impossible car

exact établie par Galois, ce qui décomposition
A étalons $\frac{1}{3}$ n'est plus possible.

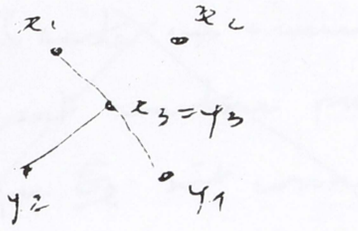
dim 3 comme avant

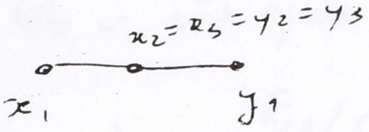
Conclusion : 8 possibilités pour le tore et sa représentation



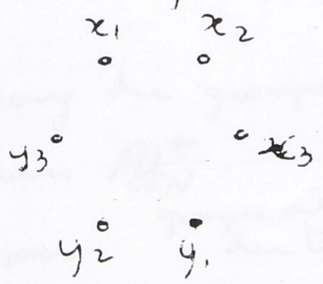
octaèdre

Exemple





Le X est engendré par les sommets soumis aux relations barycentriques :



$x_3 / y_3 = (x_2/x_1)^2$ est l'ép. du tore.

Remarque : le dessin n'entraîne pas la détermination des p_σ (cf. par exemple l'octaèdre qui correspond à des tas de possibilités)

Soit A vcn ab/K de dim $n \geq 1$, v une place de K à bonne réduction, de car. rés. $\neq l$.

π_v de Frobenius, $\pi_v \in G_\ell \subset GL_N(\bar{\mathbb{Q}}_\ell)$.

le sous-gp. alg. de GL_N engendré par les $\pi_v^{\mathbb{Z}}$ est Θ_{π_v}, défini sur $\mathbb{Q}_\ell$ et contenu dans G_ℓ. Le tore T_{π_v} est contenu dans G_ℓ°.

Théorème 1) Il existe un ensemble de places v de densité > 0 tel que T_v soit un tore maximal de G_ℓ.

2) Pour que G_ℓ soit connexe, il faut et il suffit que la densité de tels v soit égale à 1.

En fait : Si $c = (G_\ell : G_\ell^\circ)$. La densité des v tels que $\Theta_v = T_v$ et que T_v soit un tore maximal de G_ℓ est $\frac{1}{c}$.

Soit r le rang du groupe G_ℓ. Notons Φ l'application de G_ℓ dans Aff_N^*.

Soit $\Lambda = \{$ sous-groupes alg. de tore standard qui sont géom. conjugués à un Θ de Frobenius de dimension $< r\}$. Ces tores sont en nombre fini. Si $\Theta \in \Lambda$, $\Phi(\Theta) \subset \mathrm{Aff}_N^*$ est de dimension $< r$.

Considérons M la sous-variété de G_ℓ°, définie sur $\mathbb{Q}_\ell$, réunion ~~des éléments non réguliers (régulier signifiant par le centralisateur est tore maximal)~~ de tous les éléments dont l'image par Φ appartient à l'un des $\Phi(\Theta)$.

3/12/84 Serre (Cours n°3)

Corrections et compléments

a) Si ρ_1, ρ_2 sont deux représentations de G dans un groupe orth. ou symplectique en car. $\neq 2$ et si ρ_1, ρ_2 sont conjuguées dans GL_n, elles le sont dans O_n (resp. Sp_n)

(si n impair, vrai avec SO_n
n pair / faux pour SO_n)

(cf Tits, exposé Bbaki, 1955)

b) Dans le dernier cours, inutile de parler d'éléments réguliers

c) Le th. énoncé la fois passée était (faut-il être) erroné:

Enoncé correct. $\exists v$ / $T_v = \Theta_v$ et $T_{v,\ell}$ tore maximal de G_ℓ° } est de densité $\frac{1}{c}$ où $c = [G_\ell : G_\ell^\circ]$

En particulier G_ℓ connexe $\Leftrightarrow$ cet ensemble est de densité 1.

Application

Il existe une infinité de ℓ (densité >0) tels que G_ℓ° soit déployé

Dém: Choisissons v tel que $T_{n,v}$ soit de dimension égale au rang de G_ℓ°. Alors $T_{n,v}/\Theta_v$ est un tore maximal de G_ℓ°. Or le tore maximal est déployable sur $\mathbb{Q}$ et un tel tore est déployé en une infinité de places de densité >0 (celles décomposées dans la représentation galoisienne [illegible] sur les caractères).

Rappel sur les courbes elliptiques :

1) Pas de CM : $\underline{G}_\ell = \underline{G}_\ell^\circ = GL_2/\mathbb{Q}_\ell$

$T_{\pi_v} \subset \mathbb{G}_{\pi_v}$

a) v ordinaire : $T_{\pi_v} = \mathbb{G}_{\pi_v} =$ tore maximal "groupe multiplicatif des corps quad. imaginaire $\mathbb{Q}(Frob_v)$".

(*) Il y a une infinité de $\mathbb{Q}(Frob_v)$ et Lang-Trotter conjecturent que tout corps quadratique imaginaire intervient pour une infinité de v.

b) v supersinguliers : $T_{\pi_v} = G_m$. On ignore s'il y a une infinité de v supersinguliers, et ceci pour toute courbe. On conjecture qu'il y en a une infinité.

2) type CM, défini sur K. Alors $\underline{G}_\ell = \underline{G}_\ell^\circ$ et le gr. mult. des corps de mult. complexe

3) type CM, non défini sur K. Alors $[\underline{G}_\ell : \underline{G}_\ell^\circ] = 2$ et $\underline{G}_\ell^\circ$ est comme dans le cas 2).

Dans un groupe réductif M sur $\mathbb{Q}_\ell$ il n'y a qu'un nbre fini de tores maximaux modulo conjugaison par $M(\mathbb{Q}_\ell)$.

Prop : Soient $\ell_1, \dots, \ell_k$ nbres premiers distincts, $T_1, \dots, T_k$ des tores maximaux de $\underline{G}_{\ell_1}^\circ, \dots, \underline{G}_{\ell_k}^\circ$. Alors il y a une infinité de v (dans $\neq 0$) telles que $\mathbb{G}_{\pi_v/\ell_i}$ soit un tore conjugué de T_i.

(exemple : cas de GL_2. Le comportement en ℓ de $\mathbb{Q}(Frob_v)$ peut être imposé pour un nbre fini de ℓ, d'où (*))

Dem Soit T un tore de G_ℓ. $x \in T(\mathbb{Q}_\ell)$

La réunion des conjugués de x par $G_\ell(\mathbb{Q}_\ell)$

tient un voisinage (analytique) de x.

Prenons x assez proche de 1 pour que x appartienne à $T(\mathbb{Q}_\ell) \cap G_\ell$ ... choisissons le régulier. Choisissons un $\bar{v}$ (grand de G) qui donne un tore maximal et tel que $\pi_{\bar{v}}$ tombe dans ce voisinage.

Exercice: 1) Si $G \subset GL_n(\mathbb{Z}_\ell)$ tel que $\begin{cases} x \equiv 1 \bmod \ell & \text{si } \ell \neq 2 \\ x \equiv 1 \bmod 4 & \text{si } \ell = 2 \end{cases}$ pour tout $x \in G$, l'enveloppe algébrique de G dans GL_n est connexe.

2) Si A est une variété abélienne dont les pts de division (pour un $n \geq 3$) sont rat$/K$, alors les G_ℓ sont connexes.

Exploitation des lois de Frobenius

Dem A = ...

[illegible] de G_ℓ, X groupe des caractères, ensemble des poids (dans les repr. de V_ℓ)

L'ensemble des poids a un centre de symétrie (dans $\frac{1}{2}X$), on note [illegible] cette symétrie. On a [illegible] = 2 centre de symétrie = [illegible] de la similitude symplectique.

Il existe une infinité de v tel que le tore donné soit isomorphe au tore T_{π_v}.

On en déduit : Σ

a) Une action d'un groupe fini Σ sur X préservant la famille des (e_i) (Σ est l'image du groupe de Galois dans la représentation sur X).

b) Il existe une application additive $\varphi : X \to \mathbb{Q}$ (associée à une place de $\overline{\mathbb{Q}}$ au dessus de la caract. résiduelle) avec :

(b_1) Les valeurs de φ sur les poids sont dans $[0,1]$

(b_2) Les conjugués de φ par Σ engendrent le dual de X, autrement dit $\bigcap_{\sigma \in \Sigma} \ker(\varphi^\sigma) = \{0\}$

(b_3) Si C est une orbite de Σ dans l'ensemble des poids et si $\frac{a}{b} \in \mathbb{Q}$, avec $\mathrm{pgcd}(a,b) = 1$, le nombre des poids $w \in C$ avec $\varphi(w) = \frac{a}{b}$ est divisible par b.

Des propriétés (b_1), (b_2), (b_3) sont valables sur les corps de nbres et de fct. La suivante n'est établie que pour les corps de nbres :

(b_4) Dans toute orbite C de Σ il existe au moins un w tel que $\varphi(w) = 0$.

Dém de (b_4) : On peut supposer que la place v utilisée est de degré 1 (ie N_v est un nbre premier), et N_v aussi grand qu'on veut. Le tore de Frobenius est alors relatif à un nombre premier. Soit C une orbite où φ est toujours >0. C s'identifie à un pour - ensemble de valeurs propres, stable par $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Alors

$v_p\left(\sum_{\lambda_i \in C} \lambda_i\right) > 0$ et $\sum_{\lambda_i \in C} \lambda_i$ est un entier

Mais $\left|\sum_{\lambda_i \in C} \lambda_i\right| \leq 2n\sqrt{p}$ si $p > 4n^2$, on a donc $\sum_{\lambda_i \in C} \lambda_i = 0$. Si le groupe de Galois est assez proche de 1 (ce qu'on peut supposer, quitte à étendre le corps de base), toute somme partielle de valeurs propres est $\neq 0$.

Description des gpes possibles, lorsque $\mathrm{End}_{\bar{K}} A = \mathbb{Z}$ et $\dim A \leq 10$

$G_\ell^\circ = G_m S$ avec S abs^t irréductible.

On veut la classification (sur $\bar{\mathbb{Q}}_\ell$) des S irréductibles dans Sp_{2n}.

voir tables p. IX-8 à IX-11 ←

On est amené à regarder les repés. irréd. symplectiques de $S_1 \times \dots \times S_k$ avec les S_i presque simples. Ceci revient à prendre $V = V_1 \otimes \dots \otimes V_k$ avec les V_i soit orthogonaux, soit symplectiques (car V isomorphe à V^*) et le nbre des symplectiques doit être impair.

On aura donc besoin des repésent. orthogonales en dim $\leq 2c_\Phi$ des gpes simples S_i et symplectiques en dim $\leq 2c_\Phi$ des gpes simples.

La formule de H. Weyl donne le degré d'une repés. en termes du poids dominant

$$\omega = a_1\omega_1 + \dots + a_k\omega_k \qquad (a_i \geq 0$$

(ω_i poids fond.
k rang du groupe)

$\dim V_\omega$ est un produit de fcts linéaires en les a_i

Ex : A_1, SL_2, $a_1\omega_1$, $rep = Sym^{a_1}(V_2)$

$dim = a_1 + 1$.

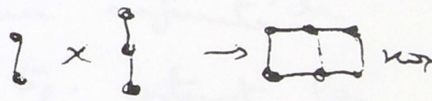
A_2, SL_3, $a_1\omega_1 + a_2\omega_2$

$$dim = (1+a_1)(1+a_2)\left(1+\frac{a_1+a_2}{2}\right)$$

(on écrit $\prod_{\substack{\alpha \text{ racine} > 0 \\ \pi = \sum \lambda_i \alpha_i \text{ du syst. dual}}} \left(1 + \frac{\sum \lambda_i a_i}{\sum \lambda_i}\right)$)

C_2 ω_1 ω_2 $\quad dim = (1+a_1)(1+a_2)\left(1+\frac{a_1+a_2}{2}\right)$

$\left(1+\frac{a_1+2a_2}{3}\right)\left(1+\frac{a_1+3a_2}{4}\right)\left(1+\frac{2a_1+3a_2}{5}\right)$

	N				
A de dim 1	2	A_1	SL_2	standard	 oui
A de dim 2	4	A_4	Sym^3(standard)		 non
			impossible		
		C_2	Sp^4		 oui
3	6	$A_1 \times A_1$	standard $\otimes$ Sym^2(st.)		 non
			2 3		
		A_1	Sym^5		non
		C_3	Sp^6		oui

Preuve du "non" pour $A_1 \times A_2$

(2,5) = une orbite sous Σ

φ n'est donc ni horiz, ni vertical

$\varphi(2) \neq \varphi(5)$. Par ex. $\varphi(2) = 0$. Mais alors

$\varphi(1) = \varphi(3) = 0$, φ horizontal. Absurde.

<u>Conclusion</u>. En dim 1, 2, 3, $\mathrm{End}_{\bar{k}} A = \mathbb{Z} \Rightarrow G_\ell^0 = G_m\, Sp_{2n}$

dim $A = 4$

A_1 non

C_4 oui

$A_1 \times A_1 \times A_1$ $\quad (std)^{\otimes 3}$ 

possible pour un corps de nombres (géométriquement)

Mumford, Math. Ann. ($\simeq 1968$), "Remarque sur un article de Shimura" : il existe une famille de v. ab. dont ([illegible] de t. [illegible]) le membre générique a un gr. de Mumford Tate du type $A_1 \times A_1 \times A_1$. Par un thm de Deligne, Gal. contenu dans ce groupe (Cycles de Hodge absolus). Vu la liste, ceci entraîne égalité.

Si $\ell_1, \dots, \ell_k$ sont donnés, il existe une infinité de spécialisation de A sur lesquels les G_{ℓ_i} restent les mêmes.

Représentations irréductibles de bas degré des groupes simples

Dimension de la représentation	Type de l'alg. de Lie	Poids dominant	Formes bilin. invariantes	Description
2	A_1	ω_1	–	SL_2 dans sa rep. standard
3	A_1	$2\omega_1$	+	" " " Sym^2(standard)
	A_2	ω_1	o	rep. standard de SL_3
	A_2	ω_2	o	duale de la précédente
4	A_1	$3\omega_1$	–	Sym^3 (Standard)
	$C_2 (= B_2)$	ω_1	–	Sp_4 dans sa rep. standard (=spinorielle de B_2)
	A_3	ω_2	o	SL_4 dans sa repr. standard
	A_3	ω_3	o	duale de la précédente
5	A_1	$4\omega_1$	+	Sym^4 (standard)
	B_2	ω_1	+	repr. standard de SO_5
	A_4	ω_1	o	repr. standard de SL_5
	A_4	ω_4	o	duale de la précédente
6	A_1	$5\omega_1$	–	Sym^5 (standard)
	A_2	$2\omega_1$	o	Sym^2 (standard) (de SL_3)
	A_2	$2\omega_2$	o	duale de la précédente
	$A_3 (= D_3)$	ω_2	+	Λ^2(standard de SL_4) $\simeq$ standard de SO_6
	C_3	ω_1	–	standard de Sp_6
	A_5	ω_1	o	standard de SL_6
	A_5	ω_5	o	duale de la précédente

.../

Formes bilin. invariantes :

o	(pas de forme $\neq 0$)
+	(forme sym. inv. $\neq 0$)
–	(forme alternée inv. $\neq 0$)

... 2/... Représentations irréductibles de bas degré des groupes simples (suite)

Dimension	Type	Poids dominant	Formes bilin. inv.	Description
7	A_1	$6\omega_1$	+	Sym^6 (standard)
	G_2	ω_1	+	octonions de trace 0
	B_3	ω_1	+	repr. standard de SO_7
	A_6	ω_1	○	repr. standard de SL_7
	A_6	ω_6	○	duale de la précédente
8	A_1	$7\omega_1$	−	Sym^7 (standard)
	A_2	$\omega_1+\omega_2$	+	repr. adjointe de SL_3
	B_3	ω_3	+	repr. spinorielle de $\widetilde{SO}_7$
	C_4	ω_1	−	repr. standard de Sp_8
conj. $\leftarrow$ Aut D_8 $\rightarrow$	D_4	ω_1	+	repr. standard de SO_8
	D_4	ω_3	+	repr. semi-spinorielle de $\widetilde{SO}_8$
	D_4	ω_4	+	seconde repr. semi-spinorielle
	A_7	ω_1	○	repr. standard de SL_8
	A_7	ω_7	○	duale de la précédente
9	A_1	$8\omega_1$	+	Sym^8 (standard)
	B_4	ω_1	+	repr. standard de SO_9
	A_8	ω_1	○	repr. standard de SL_9
	A_8	ω_8	○	duale de la précédente
10	A_1	$9\omega_1$	−	Sym^9 (standard)
	A_2	$3\omega_1$	○	Sym^3 (standard de SL_3)
	A_2	$3\omega_2$	○	duale de la précédente
	B_2	$2\omega_2$	+	repr. adjointe
	A_3	$2\omega_1$	○	Sym^2 (standard)
	A_3	$2\omega_3$	○	duale de la précédente
	A_4	ω_2	○	Λ^2 (standard)
	A_4	ω_3	○	duale de la précédente
	C_5	ω_1	−	repr. standard de Sp_{10}
	D_5	ω_1	+	repr. standard de SO_{10}
	A_9	ω_1	○	repr. standard de SL_{10}
	A_9	ω_9	○	duale de la précédente

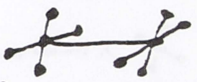
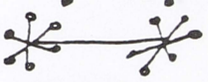
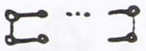
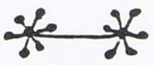
Représentations irréductibles symplectiques de degré ≤ 20 des groupes semi-simples

---

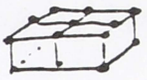
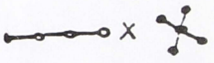
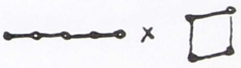
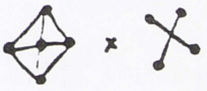
1) Pour chaque dimension $2d$, A_1 dans sa rep. Sym^{2d-1} (standard).
Irréductible pour une var. algébrienne dès que $d \geq 2$. Poids : o—o—o· · ·→o

2) Pour chaque dimension $2d$, $C_d = Sp_{2d}$ dans sa rep. standard
Possible (au moins sur les corps de nombres). Poids *.

3) Autres cas :

Dimension	Alg. de Lie	Description	Poids	Possibilité pour une v.a.
6	$A_1 \times A_1$	$\underset{2}{St} \otimes \underset{3}{\mathrm{Sym}^2}(St)$		non
8	$A_1 \times A_1 \times A_1$	$\underset{2}{St} \otimes \underset{\times 2}{St} \otimes \underset{\times 2}{St}$		oui (corps de nomb
10	$A_1 \times A_1$	$\underset{2}{St} \otimes \underset{5}{\mathrm{Sym}^4} St$		non
	$A_1 \times B_2$	$\underset{2}{St} \otimes \underset{5}{St}$		non
12	$A_1 \times D_3$	$\underset{2}{St} \otimes \underset{6}{St}$		non (corps de nbres)
	$A_1 \times A_1$	$\underset{3}{\mathrm{Sym}^2}(St) \otimes \underset{4}{\mathrm{Sym}^3}(St)$		non
	$A_1 \times C_2$	$\underset{3}{\mathrm{Sym}^2}(St) \otimes \underset{4}{St}$		non
14	$A_1 \times A_1$	$\underset{2}{St} \otimes \underset{7}{\mathrm{Sym}^6} St$		non
	$A_1 \times G_2$	$\underset{2}{St} \otimes \underset{7}{\text{rep. } \omega_1}$		non
	$A_1 \times B_3$	$\underset{2}{St} \otimes St.$		non
	C_3	rep. de poids ω_3 $(\lambda^3 - \lambda)$		non (corps de nombres
16	C_2	rep. de poids $\omega_1 + \omega_2$		non
	$A_1 \times A_2$	$\underset{2}{St} \otimes \underset{8}{\text{Adjointe}}$		non
	$A_1 \times B_3$	$\underset{2}{St} \otimes \underset{8}{\text{Spinorielle}}$	Sommets d'un cube = 4 dim.	? (probt non)
	$A_1 \times C_4$	$St_2 \otimes \underset{8}{\text{Standard}}$		non (corps de nombres)
	$A_1 \times A_1 \times A_1$	$\underset{2}{St} \otimes \underset{2}{St} \otimes \underset{4}{\mathrm{Sym}^3} St$		non
	$A_1 \times A_1 \times C_2$	$\underset{2}{St} \otimes \underset{2}{St} \otimes \underset{4}{St}$ and	Sommets d'un cube = 4 dim	? (probt non)

Rep. Symplectiques (finies)

Dimension	Type	Description	Poids	Possibilité pour une v.o.
18	$A_1 \times A_1$	$St_2 \otimes Sym^8_3(St)$		non
	$A_1 \times B_4$	$St_2 \otimes St_9$		non
	$A_1 \times A_1 \times A_1$	$St_2 \otimes Sym^2_3(St) \otimes Sym^2_3(St$		non
20	A_5	$\omega_3 : Sym^3(St)$		oui)
	C_2	poids $3\omega_1$		non
	$A_1 \times A_1$	$Sym^3_4(St) \otimes Sym^4_5(St)$		non
	$A_1 \times B_2$	$St_2 \otimes Adjointe_{10}$		non
	$A_1 \times B_2$	$Sym^3_4(St) \times St_5$		non
	$A_2 \times D_5$	$St_2 \otimes St_{10}$		non (corps de nombres)
	$A_1 \times C_2$	$Sym^4_5(St) \otimes St_4$		non
	$B_2 \times C_2$	$St_5 \otimes St_4$		non

10/12/84

Serre. (lours n°10)

On suppose que K est un corps de nombres

G_ℓ° contient un tore "de type H" (géométriquement), i.e. il existe une décomposition $V_{2n} = V_1 \underset{n}{\oplus} V_2$ avec $H \underset{n}{\simeq} G_m \times G_m$ agissant par λ sur V_1 et μ sur V_2

Écrivons $G_\ell^\circ = G_m S$ avec S semi-simple. La représentation V_2 de S est alors irréductible symplectique, et S contient (géométriquement) un tore de type $\begin{pmatrix} \lambda & & 0 \\ & \ddots & \\ 0 & & \lambda^{-1} \end{pmatrix}$

On veut classer les repés. irréd. d'un groupe semi-simple connexe ayant un tore de dim 1 ayant 2 poids et 2 seulement dans la représentation.

Si $V = V_1 \otimes \dots \otimes V_k$ avec V_i repés. irréd de G_i groupe simple et G isogène à $\prod G_i$, on a

Lemme : Tout tore de G de dim 1 à 2 poids provient d'un tore à 2 poids d'un des G_i.

Evident.

Il s'agit donc de traiter le cas d'un groupe simple. Une représentation irréductible correspond à un poids dominant

Le résultat

1) Type A_ℓ ($SL_{\ell+1}$ agissant sur E de dim $\ell+1$) groupe à 1 par $\begin{pmatrix} \lambda^a & & 0 \\ & \ddots & \\ 0 & & \lambda^b \\ & & & \ddots \\ & & & & \lambda^{-b} \end{pmatrix}$ avec $i+j = \ell+1$, $ia = jb$

$\Lambda^i E$ $(2 \le i \le l-2)$ avec le vas pr. à ses paramètre $\begin{pmatrix} \lambda & & 0 \\ & \lambda^{-1} & \\ 0 & & \ddots \\ & & & \lambda^{-1} \end{pmatrix}$

2. Type (B_l) SO_{2l+1}

Repré spinorielle de B_l, de dim 2^l

à l'intérieur de SO_{2l+1} Les pr. à ses vaps est $\begin{pmatrix} \lambda & & & 0 \\ & \lambda^{-1} & & \\ & & \ddots & \\ 0 & & & 1 \end{pmatrix}$; dans la repré spinorielle, il n'a que deux poids. La repré ainsi obtenue est symplectique si et seulement si $l \equiv 1, 2 \bmod 4$.

3. Type C_l Sp_{2l}

Représentation standard de dim $2l$ avec $\begin{pmatrix} \lambda & & & 0 \\ & \lambda & & \\ & & \lambda^{-1} & \\ 0 & & & \ddots \\ & & & & \lambda^{-1} \end{pmatrix}$

4. Type D_l $\widetilde{SO}_{2l}$

a) Repré. standard de dim $2l$ avec $\begin{pmatrix} \lambda & & & 0 \\ & \ddots & & \\ & & \lambda^{-1} & \\ 0 & & & \ddots \\ & & & & \lambda^{-1} \end{pmatrix}$ associé à une déc. tot isotrope

(repré. non symplectique)

b) Représentations semi-spinorielles de dim 2^{l-1}

Cette repré. est symplectique $\Leftrightarrow l \equiv 2 \bmod 4$.

5. Groupes exceptionnels : rien

Démonstration

Soit $(\alpha_1, \dots, \alpha_l)$ une base des syst. de racines,

$(\check{\alpha}_1, \dots, \check{\alpha}_l)$ la base duale

$(\omega_1, \dots, \omega_l)$ les poids fondamentaux

$(\check{\omega}_1, \dots, \check{\omega}_l)$ les poids (fond.) des syst. duals.

Soit $\tilde{\alpha} = \sum m_j \alpha_j$ la plus grande racine

$\tilde{\alpha}^\vee = \sum n_i \alpha_i^\vee$ " " " " du syst. dual.

On a $\langle \omega_i, \alpha_j^\vee \rangle = (\omega_i, \alpha_j) = \delta_{ij}$

Les repr. irréductibles sont classés par leur plus haut poids $\omega = \sum k_i \omega_i$ $\left(\begin{matrix} k_i \in \mathbb{Z} \\ k_i \geq 0 \end{matrix}\right)$

Assertion 1 Si V_ω a un tore à 2 poids, ω est un poids minuscule, i.e. est l'un des ω_i avec $n_i = 1$.

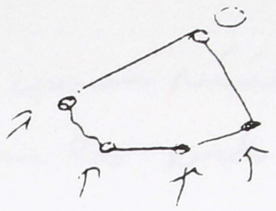
Assertion 2 . de sous-groupe à un paramètre est, "à homothétie près" défini par un $\omega_j^\vee$ minuscule ($m_j = 1$) (en considérant $\omega_j^\vee$ comme appartenant à $\mathbb{Q} \otimes_{\mathbb{Z}} \mathrm{Hom}(\mathbb{G}_m, G)$).

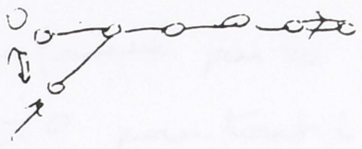
Assertion 3 : Pour que le couple $(\omega_i, \omega_j^\vee)$ soit acceptable, il faut et il suffit que

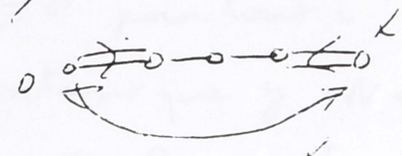
$$(\omega_i, \omega_j^\vee) + (\omega_{i'}, \omega_j^\vee) = 1$$

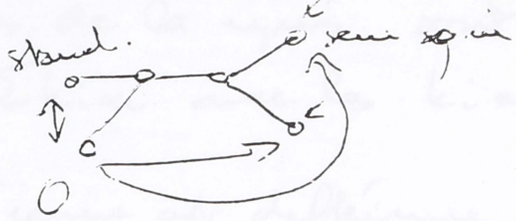
où $i \mapsto i'$ est l'involution standard de la base choisie (l'involution standard est celle qui "correspond à l'automorphisme -1 du syst. de racines").
Cette involution est d'ordre 1 si $-1 \in W$ (gr. de Weyl)
2 si $-1 \notin W$

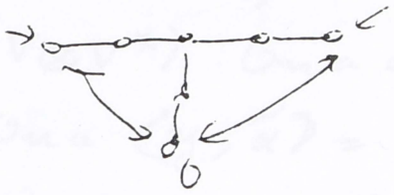
(on trouve les poids minuscules en regardant le complété affine $\check{R}_{\mathrm{aff}}$ du syst. de racines dual et en regardant quels sommets sont transformés de 0 par un automorphisme du diagr. complété)

type A 

type B 

type C 

type D 

type E_6 

Une représentation minuscule (Lie VIII, §7, n°3) est caractérisée par chacune des conditions suivantes :

- Le groupe de Weyl agit transitivement sur les poids.
- Pour toute racine α, si ω est le poids dominant, on a $(\omega, \alpha^\vee) = 0, 1$ ou -1 (en effet tous les $\omega - n\alpha$ avec $0 \leq n \leq (\omega, \alpha^\vee)$, si $(\omega, \alpha^\vee) \geq 0$ sont des poids de la représentation).

Démontrons l'assertion 1 revient à dire qu'il existe un élément y de $\mathfrak{h}_{\mathbb{Q}} \otimes Y(T)$ tel que $\{\langle \omega, y \rangle / \omega$ poids de la représ.$\}$ ait exactement deux éléments.

Si on avait une chaîne de longueur 3 dans les poids, elle serait orthogonale à y, ainsi que ses transformés par W, d'où absurdité. Donc toute chaîne est de longueur 2.

soit y comme précédemment, et normalisons y de sorte que les poids de la repré. permutent sous y des valeurs λ, μ, avec $\lambda - \mu = 1$ et supposons y pour en transformé par le groupe de Weyl de sorte que $(y, x_i) \geq 0$ pour tout i.

Montrons que y est un poids minuscule des poids de la repré. sont de la forme $\omega = -\sum k_i x_i$ avec les k_i entiers ≥ 0.

Toute racine est différence de deux poids (car $\mathfrak{g} \subset V \otimes V^*$). On a donc $\langle y, x \rangle = \begin{matrix} 1 \\ 0 \end{matrix}$ pour $x \geq 0$. On a $\langle y, \tilde{x} \rangle = 1$ ou 0, d'où, si $\tilde{x} = \sum m_i x_i$, y poids minuscule associé à un i tel que $m_i = 1$. Ceci prouve l'assertion?

Le plus bas poids de la repré. de poids dominant ω est $-\omega'$ avec $'$ involution canonique. Donc y est compatible avec ω si et seulement si $\langle y, \omega \rangle - \langle y, -\omega' \rangle = 1$. Ceci prouve l'ass. 3.

Théorème - Si $\dim A$ impaire et $\mathrm{End}_k A = \mathbb{Z}$, $\mathcal{G}_\ell = C \mathrm{Sp}_{2n}/\mathbb{Q}_\ell$.

(Des arguments importants de la dém. sont extraits d'un article de Ribet, Am. J of Math, 1983, qui concerne à déterminer le groupe de Mumford-Tate)

(Ribet) de dimension

Lemme. - Si une représentation symplectique est irréductible et de dimension $\neq 0$ modulo 4, c'est une représentation standard d'un groupe symplectique.

A_ℓ $(\ell \geq 2)$: Λ^i (St$_{\ell+1}$) sympl $\Leftrightarrow$ $i = \frac{\ell+1}{2}$ et ℓ impair

(si $i \neq \frac{\ell+1}{2}$, $(\Lambda^i)^* \simeq \Lambda^{\ell+1-i}$ n'est pas isom à Λ^i.

si $i = \frac{\ell+1}{2}$, $\Lambda^i \otimes \Lambda^i \hookrightarrow \Lambda^{\ell+1}$ fournit une forme sympl. invariante).

$$\dim = \binom{(\ell+1)}{\left(\frac{\ell+1}{2}\right)}$$

Lemme : si N impair > 1, $\binom{2N}{N} \equiv 0 \bmod 4$.

type B : dim 2^ℓ

type C : Standard acceptée.

type D : standard (non sympl.)

semi-spin $2^{\ell-1}$

Soit $V_\ell(A) = V_\ell$. Géométriquement $V_\ell \simeq \bigotimes W_i$ avec Lie S agissant sur V_i suivant S_i (Lie $S \simeq \bigoplus S_i$)

Il existe, si $\ell = 2n$ avec n impair, un facteur et un seul de dim. paire et il y a un nbre impair de facteurs symplectiques. Il y a donc un seul facteur symplectique

On peut supposer que W_1 est symplectique et W_i orthogonal de dim impaire pour $i \geq 2$)

On doit avoir un tore de type M. Il provient nécessairement du facteur symplectique. Par suite

W_1 correspond à la représentation standard.

Nous allons voir qu'il n'y a pas d'autres facteurs.

Lemme. Sur un corps de nbres k si $\mathrm{End}_k A = \mathbb{Z}$, il n'est pas possible que V_ℓ soit de la forme $W_1 \otimes W_2$ avec W_1 représentation minimale et 0 poids de W_2 (et $\dim W_2 \geq 2$) (ce qui est le cas lorsque W_2 est orthogonal de dim impaire).

On utilisera l'hypothèse "minimale": sous la forme "le milieu de deux poids n'est pas un poids" l'ens. des poids est $\{(\lambda+\mu) / \lambda$ poids de W_1, μ poids de $W_2\}$

Soit $\Omega_1 = \{$poids de $W_1\}$

$\Omega_2 = \{$ " " $W_2\}$

Les poids du sous-module sont les éléments de $\Omega_1 \times \Omega_2$.

Ω_1 se plonge dans $\Omega_1 \times \Omega_2$ par $\lambda \to (\lambda, 0)$.

Lemme : tout automorphisme affine de $\Omega_1 \times \Omega_2$ laisse stable $(\Omega_1 \times 0)$.

En effet $\omega_1 + \omega_2 \in \Omega_1 \times \{0\}$

$\Leftrightarrow \mathrm{Card}(\rho_\omega(\Omega_1 \times \Omega_2) \cap (\Omega_1 \times \Omega_2)) = |\Omega_2|$

si ρ_ω est la symétrie par rapport à 0.

Soit un tore de Frobenius associé à une place v telle que $N_v = p$ soit premier.
L'ensemble des racines $\Omega_1 \times \Omega_2 \to \mathbb{R}$ est stable par $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. L'un des points $(a, 0)$ de cet ensemble a donc valuation nulle. Donc φ_v s'annule sur $a \times \Omega_2$, absurde.

Géométriquement, la représentation est la représ. standard de Sp_{2n}.
Comme $G_\ell \subset GSp_{2n}/\mathbb{Q}_\ell$, c'est en fait relativement facile.

Liste de problèmes

1) Galois = Mumford Tate ?
($\Leftarrow$ dans la cohomologie ℓ-adique invariantes par Galois, à torsion de Tate près, proviennent des cycles de Hodge absolus, resp. des cycles algébriques si l'on sait la conj. de Hodge).

2) Plus faible

dem (invariants de Galois) dans des représ. ℓ-adiques et ℓ'-adiques compatibles sont les mêmes.

** Si $G \subset G_{\mathbb{Q}}$ réd. connexe et si l'on connaît la dim des invariants de G dans toutes les puissances tensorielles, connaît-on G ?

3) Problèmes numériques : Donner des exemples de courbes dont les jacobiennes ont $G_{\ell} \simeq CS_p$

4) Montrer qu'il y a une infinité de places avec réduction ordinaire (et même dens. 1 si les groupes sont connexes)

5) Est-ce que G_{ℓ}° est engendré géométriquement par des sous-tores de type H ? (Ce serait une conséquence de 1)).

6) Montrer qu'aucun facteur géométrique de G_{ℓ}° est de type exceptionnel

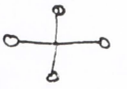
(**) (on pourrait envisager de le faire avec les tores de Frobenius)

7) Interprétation de la dualité de Langlands

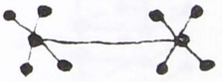
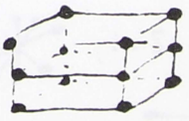
8) Conjecture à énoncer dans le cas des corps de fonctions.

Table of irreducible symplectic representations of degree ≤ 20 of semi-simple groups (over an alg. closed field of ch. 0)

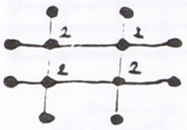
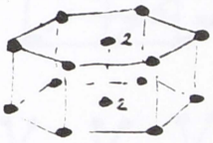
1) For each dimension $2d$, $A_1 = SL_2$ in its repr. $\mathrm{Symm}^{2d-1}(St)$, where St = Standard representation of degree 2. Weights:  .
This is impossible for an abelian variety as soon as $d \geq 2$.

2) For each dimension $2d$, $C_d = Sp_{2d}$ in its standard representation. Weights (for $d=2$):  . This is possible for an ab. variety, over a number field.

3) Other cases:

Dimension	Group	Representation	Weights	Occurs for an abelian var. over a number field
6	$A_1 \times A_1$	$St_2 \otimes \mathrm{Sym}^2 St_3$		no
8	$A_1 \times A_1 \times A_1$	$St_2 \otimes St_2 \otimes St_2$		yes (Mumford)
10	$A_1 \times A_1$	$St_2 \otimes \mathrm{Sym}^4 St_5$		no
	$A_1 \times B_2$	$St_2 \otimes St_5$	 (in 3-space)	no
12	$A_1 \times D_3$	$St_2 \otimes St_6$	 (in 4-space)	no
	$A_1 \times A_1$	$\mathrm{Sym}^2(St)_3 \otimes \mathrm{Sym}^2(St)_4$		no
	$A_1 \times C_2$	$\mathrm{Sym}^2(St)_3 \otimes St_4$		no
14	$A_1 \times A_1$	$St_2 \otimes \mathrm{Sym}^6 St_7$		no

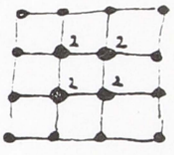
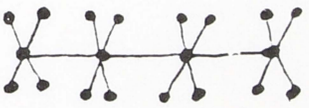
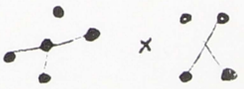
(St = Standard representation)

Dimension	Group	Representation	Weights	Occurs for an abelian var. over a number field
14 ctd...	$A_1 \times G_2$	$St_2 \otimes Rep(\omega_1)_7$		no
	$A_1 \times B_3$	$St_2 \otimes St_7$	 (in 4-space)	no
	C_3	$Rep(\omega_3) = \overset{3}{\wedge} St - St$		no
			vertices of a cube + centers of faces	
16	C_2	$Rep(\omega_1 + \omega_2)$		no
	$A_1 \times A_2$	$St_2 \otimes Adjt_8$		no
	$A_1 \times B_3$	$St_2 \otimes Spinor_8$	vertices of a 4-dim. cube	? (probably no)
	$A_1 \times C_4$	$St_2 \otimes St_8$	 (in 5-space)	no
	$A_1 \times A_1 \times A_1$	$St_2 \otimes St_2 \otimes Sym^3 St_4$		no
	$A_1 \times A_2 \times C_2$	$St_2 \otimes St_2 \otimes St_4$	vertices of a 4-dim cube	? (probably no)
18	$A_1 \times A_1$	$St_2 \otimes Sym^8 St_9$		no
	$A_1 \times B_4$	$St_2 \otimes St_9$	 (in 5-space)	no
	$A_1 \times A_1 \times A_3$	$St_2 \otimes Sym^2(St)_3 \otimes Sym^2(St)_3$		no

.../...

$Rep(\omega_i)$ = irred. representation with highest weight ω_i (Bourbaki notation)

$Adjt$ = adjoint representation

Dimension	Group	Representation	Weights	Occurs ? for an abelian variety over a number field
20	A_5	$Rep(\omega_3) = \Lambda^3(St)$		yes
	C_2	$Rep(3\omega_1)$		no
	$A_1 \times A_1$	$Sym^3(St) \otimes Sym^4(St)$ (4, 5)		no
	$A_1 \times B_2$	$St \otimes Adjt$ (2, 10)		no
	$A_1 \times B_2$	$Sym^3(St) \otimes St$ (4, 5)	 (in 3-space)	no
	$A_1 \times D_5$	$St \otimes St$ (2, 10)	 (in 6-space)	no
	$A_1 \times C_2$	$Sym^4(St) \otimes St$ (5, 4)		no
	$B_2 \times C_2$	$St \otimes St$ (5, 4)		no