

COURS DE JEAN-PIERRE SERRE

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_

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

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

NUMDAM

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

f

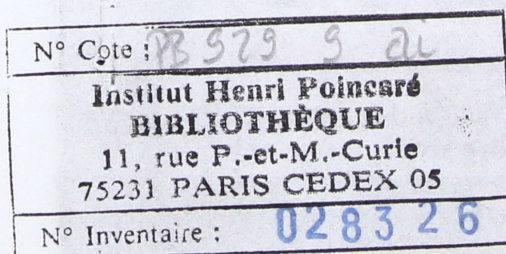
ANNUAIRE
DU
COLLÈGE DE FRANCE
1984-1985

Algèbre et géométrie

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

31 MAI 1999

RÉSUMÉ
DES COURS ET TRAVAUX



85^e année

PARIS

11, place Marcelin-Berthelot (V^e)

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 $\rho_1 : G \rightarrow \mathbf{GL}(V_1)$ et $\rho_2 : G \rightarrow \mathbf{GL}(V_2)$ 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 $\text{Tr } \rho_i$ le caractère de ρ_i . Les fonctions $\text{Tr } \rho_1$ et $\text{Tr } \rho_2$ 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 :

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

Notons M la sous- $\mathbf{Z}_\ell$ -algèbre de $\mathrm{End}(V_1) \times \mathrm{End}(V_2)$ 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 $\theta : M \rightarrow \mathbf{Z}_\ell$ est surjective. Par réduction $(\mathrm{mod} \ell)$ elle définit une forme linéaire non nulle :

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

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 $\tilde{G}$ 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 $\tilde{G}$ et l'application $t : \tilde{G} \rightarrow \mathbf{Z}/\ell \mathbf{Z}$ mesure en quelque sorte la « déviation » entre ρ_2 et ρ_1 . L'intérêt de $(\tilde{G}, t)$ est que c'est un objet « fini » (alors que G lui-même, en pratique, est infini). Cela permet souvent de dresser la liste des $(\tilde{G}, t)$ possibles sans connaître ρ_1 ni ρ_2 (ni α). Supposons par exemple que cette liste soit formée de :

$$(\tilde{G}_1, t_1), \dots, (\tilde{G}_h, t_h).$$

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

(1) Si $\mathrm{Tr} \rho_2(s_j) = \mathrm{Tr} \rho_1(s_j)$ pour $j = 1, \dots, h$, 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 $\{s_1, \dots, s_h\}$).

Sinon, en effet, il existerait un indice j tel que le couple $(\tilde{G}, t)$ associé à (ρ_1, ρ_2) soit isomorphe à $(\tilde{G}_j, t_j)$, 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 $\mathrm{GL}_2(\mathbf{Z}_2)$. Faisons les hypothèses suivantes :

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

(ii) les deux homomorphismes de G dans $\mathrm{GL}_2(\mathbf{Z}/2\mathbf{Z}) = \mathfrak{S}_3$, 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 $t: \tilde{G} \rightarrow \mathbb{Z}/2\mathbb{Z}$ vaut 0 sur les éléments de $\tilde{G}$ d'ordre ≤ 3 , et 1 sur les autres.

1.3. Courbes elliptiques.

Soient E_1 et E_2 deux courbes elliptiques sur $\mathbb{Q}$. 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 $\mathbb{Q}$ 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 $\mathbb{Q}$, 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 $\mathbb{Q}$ -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 $\tilde{K}/\mathbb{Q}$ contenant K et de groupe de Galois $\tilde{G}$. Connaissant S , on peut déterminer explicitement les extensions $\tilde{K}/\mathbb{Q}$ 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 $\tilde{K}_1, \dots, \tilde{K}_h$ désignent les extensions en question, on choisit pour tout $j = 1, \dots, h$ un nombre premier p_j dont la substitution de Frobenius $\tilde{s}_j$ dans $\tilde{K}_j/\mathbb{Q}$ 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 $\mathbb{Q}$, il suffit que les traces des endomorphismes de Frobenius de E_1 et E_2 soient les mêmes pour les nombres premiers $p_1, \dots, p_h$.

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

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 $\mathbf{Q}$ 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 $\mathbf{Q}$;
- $\bar{K}$ est une clôture algébrique de K ;
- G_K est le groupe de Galois $\text{Gal}(\bar{K}/K)$;
- 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 ;
- $\rho_\ell : G_K \rightarrow \text{Aut}(V_\ell)$ est la représentation ℓ -adique correspondante ;
- G_ℓ est l'image de ρ_ℓ ; c'est un sous-groupe compact de $\text{Aut}(V_\ell)$;
- $\mathfrak{g}_\ell$ est l'algèbre de Lie de G_ℓ ; on a $\mathfrak{g}_\ell \subset \text{End}(V_\ell)$;
- 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 $\text{GL}_{V_\ell} \simeq \text{GL}_{2n}$.

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_t^{alg} est égale à $\mathfrak{g}_t$, ou encore que $\mathfrak{g}_t$ est une sous-algèbre algébrique de $\text{End}(V_t)$.

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

On conjecture que G_t^{alg} est « indépendant de ℓ » (pour A et K fixés), et plus précisément que sa composante neutre $(G_t^{\text{alg}})^\circ$ se déduit du « groupe de Mumford-Tate » par extension des scalaires de $\mathbf{Q}$ à $\mathbf{Q}_t$. 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 $G_t^{\text{alg}}/(G_t^{\text{alg}})^\circ$ est indépendant de ℓ . De façon plus précise, le noyau de l'homomorphisme surjectif*

$$G_K \rightarrow G_t \rightarrow G_t^{\text{alg}}/(G_t^{\text{alg}})^\circ$$

est indépendant de ℓ .

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

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

$$(G_t^{\text{alg}})^\circ = C_t \cdot S_t$$

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

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

2.2.6. (FALTINGS). *On a $C_t = G_m$ si $\text{End}(A) = \mathbf{Z}$. On a $S_t = \{1\}$ si et seulement si A est de type CM.*

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

2.2.7. *Les propriétés suivantes sont équivalentes :*

- (a) $S_t = \text{Sp}_{2n}$ pour un ℓ ;
- (b) $S_t = \text{Sp}_{2n}$ pour tout ℓ ;
- (c) $\text{End}(A) = \mathbf{Z}$ et $\text{rang}(G_t^{\text{alg}}) = 1 + n$.

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

(d) *L'image de $G_K \rightarrow \prod_{\ell} (G_m \cdot \mathrm{Sp}_{2n})(\mathbb{Q}_{\ell})$ est ouverte pour la topologie adélique.]*

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

$$G_{\ell}^{\mathrm{alg}} = G_m \cdot \mathrm{Sp}_{2n}$$

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 $\mathbb{Q}_{\ell}$) 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 $\text{Tr}(x^2)$* , 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 $\mathbf{Q}$* , Genève, janvier 1985 ;
- *$\mathbf{C}$ 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 $\text{GL}_n(\mathbf{F}_p)$* , 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 η* , Bordeaux, mai 1985 ;
- *On the quadratic forms of type $\text{Tr}(x^2)$* , Oberwolfach, juin 1985 ;
- *Propriétés galoisiennes des points d'ordre fini des variétés abéliennes*, Besançon, juin 1985.

Groupe de Galois

et

Représentations p -adiques

—

Collège de France 1984

Notes Boutot — Osterlé

Groupe 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

1. Plan du cours
2. La méthode de Faltings — constructions générales
3. $\tilde{G}$. Le cas ℓ -adique : corps quantiques et isogénies
4. Applications aux niveaux 11 et 5077
5. Représentations ℓ -adiques attachées aux variétés abéliennes
Invariance du rang et de G_ℓ/G_ℓ^1 .
6. Invariance (suite). Applications.
7. " ("). Le cas symplectique. Tors de type H.
8. Tors de Frobenius
9. Applications, notamment en bonne dimension.
10. Le tors = 2 fois. Application : si $\text{End} = \mathbb{Z}$ et dim A impaire (ou 2 ou 6)
alors $G_\ell = \text{CSp}$

Plan du cours

1. Courbes elliptiques Résultats

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

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

$$n \geq 1 \quad E_n = E_n(\bar{K}) = \text{Ker} \{ n : E(\bar{K}) \rightarrow E(\bar{K}) \} \\ \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \quad \text{pas canoniquement}$$

$G = \text{Gal}(\bar{K}/K)$ opère sur E_n , $G \rightarrow \text{Aut}(E_n) \cong \text{GL}_2(\mathbb{Z}/n\mathbb{Z})$

$G_n = \text{image de } G \rightarrow \text{GL}_2$.

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

donc $G \rightarrow \text{GL}_2(\mathbb{Z}_\ell)$ image = G_{ℓ^∞}

et $G \rightarrow \text{GL}_2(\hat{\mathbb{Z}}) = \prod_\ell (\text{GL}_2(\mathbb{Z}_\ell))$ image = G_∞

Th. 1. Si E n'a pas de mult. complexe (i.e. $\text{End}_{\bar{K}} E = \mathbb{Z}$),
 G_∞ est ouvert ($\Leftrightarrow$ d'indice fini) dans $\text{GL}_2(\hat{\mathbb{Z}})$.

Cor 1) pour tout ℓ , G_{ℓ^∞} est ouvert dans $\text{GL}_2(\mathbb{Z}_\ell)$.

2) pour presque tout ℓ , $G_{\ell^\infty} = \text{GL}_2(\mathbb{Z}_\ell)$.

3) , $G_\ell = \text{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$

Rem 1) et 3) $\Rightarrow$ 2)

Le théorème se démontre facilement maintenant avec Faltings

(Faltings)

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

$G \rightarrow GL_2(\mathbb{Z}_\ell) \rightarrow GL_2(\mathbb{Q}_\ell)$ est la rep. ℓ -adique on dit qu'elles sont "isomorphes" si elles sont conjuguées. Il est pas isom pour un $\ell \Rightarrow$ 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) de p en lesquels E a mauvaise réduction (= ens de div premiers du discriminant)

Ponons $N = N_E = \prod_{p \in S} p$ (pas tr's différent du conducteur)

[on pourrait aussi prendre N = conducteur]

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

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

(2) Si $l \geq c_2 \log N$ et si GRH vraie, alors itou.

Rem c_2 est explicite, mais tr's gros.

c_1 : le Chebotarev 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 $|k(v)| = N_v$. On a la formule de Hasse

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

repr les adèles de E et E' sont isomorphes

$$\Downarrow a_v = a'_v \quad \text{pour tout } v \notin S$$

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

car les Frobenius sont deux dans le gr. de Galois et les repr. sont semi-simples.

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

4.4. En fait, si $K = \mathbb{Q}$, $N = \prod_{p \in S} p$, il suffit de vérifier

$$\text{que } a_p = a'_p \quad \text{pour } p \notin S \text{ et } p \leq N^{c_3}$$

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

c_3 et c_4 sont absolument grands !! inévitables

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

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

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

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 variétés abéliennes. Mais 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 $\mathbb{Q}(\sqrt{\frac{n}{K}})$
 $l \nmid \text{disc}$ est soit $\left| \begin{array}{l} \text{inerte} \quad \mathbb{F}_l \text{ opère sur } E_l \\ \text{décomposé} \quad \mathbb{F}_l \times \mathbb{F}_l \text{ opère sur } E_l \end{array} \right.$, alors

$E_l \simeq \bigwedge^n$ dont stable par Galois. Donc x a au plus $l-1$ conjugués $= l(1 - \frac{1}{l})$.

Prenons $n = l_1 \dots l_k$, l_i décomposés $l_1, l_2 \in X$ donné.

Alors $C(x) \leq n \prod (1 - \frac{1}{l_i})$

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

$$- \log \prod (1 - \frac{1}{l_i}) = \sum \frac{1}{l_i} + c + O(1)$$

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

$\frac{1}{2}$ des premiers sont décomposés

$$\frac{n}{\prod (1 - \frac{1}{l_i})} \sim c'' \sqrt{\log X} \stackrel{14}{\sim} c''' \sqrt{\log \log n}$$

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

Si ce sera le nome d'un s/g de Cartan non déployé d'ordre 2 (l^2 la courbe modulaire correspondant à ce s/g soit X_0 a-t-elle d'autres pts rationnels sur $\mathbb{Q}$ que les points et les pts à multi. complexe. C'est 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 $A_m, A_e, \dots$
repr. l -adique $G \rightarrow GL_{2g}$ $\begin{matrix} \mathbb{Z}/n\mathbb{Z} \\ \mathbb{F}_l \\ \mathbb{Z}_l \\ \hat{\mathbb{Z}} \end{matrix}$ $g = \dim A$

On s'intéresse à $G_{e^{\infty}}$ = image de $G = \text{Gal}(\bar{K}/K)$ dans $GL_{2g}(\mathbb{Q}_l)$

(Bogomolov)
Th $G_{e^{\infty}}$ est ouvert dans son adhérence Zariski.

Plus précisément soit H_l le plus petit s/g aff de GL_{2g} , défini sur $\mathbb{Q}_l$, dont le groupe de $\mathbb{Q}_l$ points contienne $G_{e^{\infty}}$.

Alors $G_{e^{\infty}}$ est ouvert dans $H_l(\mathbb{Q}_l)$, i.e. a même algèbre de Lie.

Il y a des conjectures sur H_l (cf texte), peut-être fausses.

C'est la plus forte H_l est indépendant de l = "Mumford-Tate".

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

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

$$H_e^\circ = T_e \cdot S_e \quad T_e = \text{composante neutre du centre de } H_e^\circ$$

$$S_e = \text{groupe dérivé de } H_e^\circ$$

$$T_e \cap S_e \text{ est fini.}$$

- * T_e est indépendant de ℓ (provenant de T sur $\mathbb{Q}$)
et contenant le g G_m de homot.
- * $\text{rang } S_e$ est indep. de ℓ .
- * la repr. du groupe de Cartan de H_e° est indep. de ℓ .
- * (Faltings) le commutant de H_e° est $(\text{End}_K A) \otimes \mathbb{Q}_e$.

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

Pour aller plus loin on peut faire l'hypothèse $\text{End}_K A = \mathbb{Z}$,

$$\text{alors } T_e = G_m.$$

Th (modulo simplification) Si $g = 1, 2, 3$, impair. Alors $S_e = \text{Sp}_{2g}$.

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

$$\text{Sp}_8 \subset \text{GL}_8 \quad \text{ou (après des scalaires)} \quad \text{SL}_2 \times \text{SL}_2 \times \text{SL}_2 \subset \text{GL}_8.$$

(3) Propriétés des repr. mod. ℓ .

A un ab. / K dim $A = g$ $G_{\ell} \subset GL_{2g}(\overline{\mathbb{F}_{\ell}})$
 on s'intéresse à G réduction avec ℓ .

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

- (1) H_{ℓ} est réductif (à repr. semi-simple).
- (2) la composante neutre de son centre est un tore indep. de ℓ
 (red mod ℓ du tore qui intervient dans les repr. 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 (indep. 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. de homothéties

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

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

on a $H_{\ell} = O_m Sp_{2g}$ 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 $CSp_{2g} = O_m Sp_{2g}$ similitude symplectique.

On peut regarder de ce l-adept par points dans la
colonisation de deux 99 ; il y a des résultats analogues pour
les semi-simplifiés. Il manque le th de commutativité de l'anneau.

4. Courbes elliptiques.

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

$$\varphi_\ell: G = \text{Gal}(\bar{\kappa}/\kappa) \rightarrow GL_2(\mathbb{Q}_\ell) \quad E \text{ c. ell sans m.c.}$$

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

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

$$G_{\ell^\infty} \text{ ouvert de } GL_2 \Leftrightarrow \mathfrak{g}_\ell = \mathfrak{gl}_2 = \text{lie } GL_2.$$

$$\text{Faltings} \Rightarrow \left| \begin{array}{l} \text{action de } G_{\ell^\infty} \text{ sur } V_\ell \text{ est semi-simple} \\ \text{commutant} = \text{End } E \otimes \mathbb{Q}_\ell = \mathbb{Q}_\ell \text{ (homothéties)} \end{array} \right.$$

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

$\Leftrightarrow$ 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 connaît $G \xrightarrow{\varphi_\ell} GL_2 \xrightarrow{\det} \mathbb{Q}_\ell^*$

$$\det \circ \varphi_\ell = \chi_\ell \text{ caract. cycl. action de } G \text{ sur } H_{\ell^*}$$

$(\hat{A}H_1 = H_2)$. Donc $\mathfrak{sl}_2$ est exclu. ■

Rem Avant Faltings, on fabriquait une ext d'isogénie et on utilisait Scharfer pour les courbes ell. $\rightarrow$ semi-simplicité

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

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

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

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

On pose $\bar{a} \quad PGL_2(\mathbb{F}_\ell) = GL_2(\mathbb{F}_\ell) / \mathbb{F}_\ell^* \supset PG_\ell$.

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

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

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

irred 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.

2^{es} cas : ordre de PG_ℓ premier à ℓ

$\Rightarrow PG_\ell = \begin{array}{|l} \text{cyclique} \\ \text{dihédral} \\ A_4, S_4, A_5 \end{array}$

on élimine ces possibilités.

- PG_ℓ cyclique $\Rightarrow G_\ell$ abélien $\Rightarrow$ pas abs simple !

- Cas diédral : $G_\ell \subset N_\ell$ normalisatrice d'un Cartan C_ℓ
 $\neq C_\ell$

$\alpha \quad C_\ell$ déployé $\begin{bmatrix} * & 0 \\ 0 & * \end{bmatrix}$

$N_\ell = C_\ell \cup \begin{bmatrix} 0 & * \\ * & 0 \end{bmatrix}$

permutant les 2 diagonales

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

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

$(\Rightarrow)$ + l'arg grand, E_ℓ est non ramifié en dehors de $S(E)$
 sus de mandais réduction de E .

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

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

(l'inertie est modelé par $\#G_\ell$ 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 $E_\ell(\text{inertie}) = 1$.

ie non ramifié.

Comme $S(E)$ est fini fini, il existe un nombre fini de E_ℓ
 possible. Il existe une extension finie K_2 de K telle que

$G_{K_2} \subset G$ soit contenu dans le noyau de tous les E_ℓ possible.

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

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

c) fin de la démo. On sait maintenant

- pour chaque ℓ , G_{E_ℓ} est inclus dans $GL_2(\mathbb{Z}_\ell)$

- pour presque tout ℓ , $G_\ell = GL_2(\mathbb{Z}/\ell\mathbb{Z})$ et

- det connu: $\det: G \rightarrow \mathbb{Z}_\ell^*$ image de $\prod \mathbb{Z}_\ell^*$

Ceci entraîne G surjectif dans $G(\mathbb{Z})$ par pure théorie
des groupes (cf. McGill).

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

dici il existe $x \in H$ le s/g fermé de $SL_2(\mathbb{Z}_l)$ tel que

$$x \equiv \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \pmod{l}$$

$$x = 1 + \varepsilon \quad \varepsilon \equiv \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \pmod{l} \quad \varepsilon^2 \equiv 0 \pmod{l}$$

$$\begin{aligned} x^l &\equiv 1 + l\varepsilon + \varepsilon^l \pmod{l^2} & \varepsilon^l &= \varepsilon^2 \cdot \varepsilon^l \cdot \varepsilon^{l-4} \\ &\equiv 1 + l\varepsilon \pmod{l^2} & &\equiv 0 \pmod{l^2} \end{aligned}$$

pour $s \in SL_2(\mathbb{F}_l)$ H contient $x \equiv 1 + ls \pmod{l^2}$

donc remplir les dans mod l^2 , on garde un $l \geq 5$.

Pour pour 2, 3 le lemme est faux

le contre ex pour $l=3$ dans McGill est faux!

Il faut montrer que $\text{Im}(G) \supset 1 \times \dots \times GL_2(\mathbb{Z}_l) \times \dots$ le grand
par th. des groupes c'est un peu embêtant. Soit I_l le s/g fermé
de $\text{Im}(G)$ engendré par les g d'inertie (à conjuguer) en les places
 $v|l$. C'est un s/g invariant de $\text{Im } G$.

Prop. Si l est assez grand, $I_l = 1 \times \dots \times 1 \times GL_2(\mathbb{Z}_l) \times 1 \times \dots \times 1$.

en effet en tout cas $\subset$, distingué, $\det I_l = \overline{\mathbb{Z}_l}^*$

et en red mod l contient les 22 tors d'inertie.

l'image par π est aussi un $\mathbb{Z}/\ell\mathbb{Z}$ et donc $GL_2(\mathbb{Z}/\ell\mathbb{Z})$

On conclut par une variante du lemme pour GL_2 .

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

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

comme les projecteurs de K sont unités, il est facile de voir que K est unité (en utilisant Sylow).

Application de la méthode Faltings :

- ① Majorations effectives pour les courbes elliptiques / $\mathbb{Q}$.
- ② Méthode effective pour reconnaître que 2 courbes elliptiques sont isogènes (ex: 1 seule c. ell. à isogénie p-i de cond 11, la courbe de Mestre de conducteur 5077 et de Weil).

Construction générale.

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

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

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

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

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

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

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

$$t(s) = \frac{1}{\ell^\alpha} (\text{Tr } \rho_1(s) - \text{Tr } \rho_2(s)) \pmod{\ell}$$

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

$$t(1) = 0, \quad t \text{ non ident. } 0$$

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

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

ex: $G \subset GL_n \times GL_n$

$$G = \{(s_1, s_2) \mid s_1 \equiv s_2 \pmod{\ell^3}\} \quad 2 \text{ repr. cond.}$$

$$d = 3 \quad t = \text{Tr} \left(\frac{s_1 - s_2}{\ell^3} \right) \pmod{\ell}.$$

(= sous $\mathbb{Z}_\ell$ -module)

Construction (Faltings) - Soit M la sous- $\mathbb{Z}_\ell$ -algèbre de $\text{End}(C_1) \times \text{End}(C_2)$ engendrée par les $(p_1(s), p_2(s))$, $s \in G$.

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

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

$$(u_1, u_2) \in M \Rightarrow \text{Tr}(u_1) \equiv \text{Tr}(u_2) \pmod{\ell^d}$$

donc $M \rightarrow \mathbb{Z}_\ell \quad (u_1, u_2) \mapsto \frac{1}{\ell^d} (\text{Tr}(u_1) - \text{Tr}(u_2))$

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

$$\text{Card} (M/\ell M)^* < \text{Card} (M/\ell M) \leq \ell^{2n^2} \quad (\text{car } M \leq 2n^2)$$

($n=0$ est impossible car $\text{Tr} p_1 \neq \text{Tr} p_2$). $\blacksquare$

Application aux isogénies de variétés abéliennes

cf. Faltings.

A_1, A_2 var. ab. sur K , corps de n°bs $\dim A_1 = \dim A_2 = g \geq 1$.

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

On veut une critère effectif pour décider si les représ. sont isomorphes. Soit ℓ premier fixé.

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

A_1 et A_2 ont bonne réduction et contenant les places divisant l . Alors les repr. l -adp. p_i attachées à A_i sont non ramifiées en $v \notin S$ et $T_{p_i}(\varphi) = T_{\text{Frob}_v}(\tilde{A}_i) = a_v(i)$ où $\tilde{A}_i = \text{red mod } v$ de A_i . $\text{Frob}_v \in \text{Gal}(\bar{K}/K)$.

Les Frobenius sont deux, donc

$$\text{repr. isom.} \Leftrightarrow a_v(1) = a_v(2) \text{ pour tout } v \notin S.$$

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

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

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

démo. Supposons que p_1 et p_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

p_1 et p_2 non isom. et semi. simple $\Rightarrow p_1$ et p_2 n'ont pas même

$$\text{donc } t: G \rightarrow \tilde{G} \rightarrow \mathbb{Z}/\ell\mathbb{Z} \text{ avec } \text{Card } \tilde{G} < \ell^{2g^2}.$$

$\text{Gal}(\bar{K}/K) \rightarrow \tilde{G}$, le noyau est ouvert i.e. $\tilde{G} = \text{Gal}(E/K)$ E corps de nbs. E/K non ramifié en dehors de S

Soit T la partie de $\tilde{G}$ formée de $s \in \tilde{G}$ avec $t(s) \neq 0$,

$T \neq \emptyset$ et invariant par conjugaison. Choisissons

$v \notin S$ avec $\text{Frob}_v(\tilde{G}) \in T$ et Nv minimum pour ces propriétés

(par Cebotarev il y a une infinité de tels v).

$$t(\text{Frob}_v) \neq 0 \Rightarrow T_1 f_1 \neq T_2 f_2 \pmod{l^{\alpha+1}}$$

Cebotarev effectif dit $N_v \leq x(\text{degé}, S, [K:\mathbb{Q}])$
 d_K

ref: cf. Serre I HES 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.

$$= N_S^{c_2} \text{ sans hypothèse}$$

c_1 et c_2 csts absolues calculables, c_1 calculée.

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

Soit $E/\mathbb{Q}$ une courbe elliptique.

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

$$\begin{array}{c} E \\ | \\ \mathbb{Q} \end{array} \quad n_E = [E:\mathbb{Q}] \leq 255$$

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

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

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

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

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

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

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

Théorème Soit E c. ell. sur $\mathbb{Q}$ et $N_E = \prod p$ de man. red.

Supposons E sans m.c. $\text{End}_{\overline{\mathbb{Q}}}(E) = \mathbb{Z}$.

Alors le gr. 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 est abs.

$\geq C_4(\log N_E)$ sous GRH.

C_i sont des ests absolus calculables.

dem. Soit $G_p = \text{image de } G = \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \text{ dans } GL_2(\mathbb{Z}/p\mathbb{Z})$

donnée par la rep. $G \rightarrow \text{Aut}(E_p)$.

Si $G_p \neq GL_2(\mathbb{Z}/p\mathbb{Z})$, on a l'une des possibilités suivantes:

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

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

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

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

On sait que $\text{der } G_p = (\mathbb{Z}/p\mathbb{Z})^*$. La liste est celle des

groupes d'indice premier à p^{28} . Sinon on regarde le p -Sylow

si unique dans un Borel

si on étend 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 $c \in G$ donne $\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$ non dans $\mathbb{F}_p^\times$.

(4) est impossible si $p \geq 17$, car on montre (Ceb. p. 197)

que le gr. d'inertie relatif à p ne peut pas.

A_4 et A_5 impossibles pour tout p .

$\subset PSL_2$

S_4 impossible si $p \equiv \pm 1 \pmod{8}$

Gal n'est pas dans PSL_2 . Dans les autres cas le gr. d'inertie
contient un élément d'ordre ≥ 6 dans PSL_2 donc $\neq S_4$.

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

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

car le gr. d'inertie en $\ell \subset \text{Cartan}$. (Invent. 72) $\square$

$\bar{E}_\varepsilon$ = torsion de $\bar{E}$ par ε

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

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

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

Donc il existe $p \leq x(N_E)^{29}$ 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 subtil).
Invent. 15(72) p. 317, C₅

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

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

en effet

$$\text{Frob}_{p_0} \in G_p$$

$$\varepsilon(p_0) = -1 \Rightarrow \text{Frob}_{p_0} \in \text{Norm} - \text{Cartan}$$

$$\Rightarrow \text{Tr}(\text{Frob}_{p_0}) \equiv 0 \pmod{p}$$

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

$$\Rightarrow p \leq |a_{p_0}| \leq 2 p_0^{1/2} \quad \square$$

Isogénies de courbes elliptiques.

Si E_1 et E_2 ne sont pas isogènes elles fabriquent un $\tilde{G}$.

On va montrer que sous certains hypp aucun groupe ne contourne
 donc E_1 et E_2 sont isogènes.

Revenons à la construction de $\tilde{G}$ dans le cas
 général $G \xrightarrow{p_1, p_2} GL_n(\mathbb{Z}_\ell) \times GL_n(\mathbb{Z}_\ell)$ avec

$T_{\ell} p_1 \neq T_{\ell} p_2$
 Hyp $\mathbb{A}$ red. mod ℓ de p_1 et p_2 sont isomorphes et

absolument irréductibles (ie irred 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 choix d'un système de base)
 à l'ens. des couples (s_1, s_2) avec $s_1 \equiv s_2 \pmod{\ell^2}$ (ℓ défini
 par $\ell^2 \mid \ell^2$)

$$\text{donc } G \rightarrow \text{Aut } C_1 \times \text{Aut } C_2$$

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

$$G \rightarrow \text{End}(C_1) \simeq M_n(\mathbb{Z}_\ell)$$

l'image engendrée End car abs. mod. de Nakayama

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

En général si $\Phi \subset \Phi_1 \times \Phi_2$ se projette sur chaque facteur

(groupes), les Φ se décomposent de façon unique par

$$\left\{ \begin{array}{l} N_1 \text{ s/g invariant de } \Phi_1 \\ N_2 \text{ " " } \Phi_2 \\ \Phi_1/N_1 \xrightarrow{\varphi} \Phi_2/N_2 \end{array} \right\} \rightarrow \begin{array}{l} \Phi = \text{"graphe" de } \varphi \\ = \{ (s_1, s_2) + s. \\ \varphi(s_1 \bmod N_1) = s_2 \bmod N_2, \end{array}$$

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

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

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

N_1 est un idéal bilatère de M_n .

N_2 " " " M_n

$$M_n/N_1 \xrightarrow{\varphi} M_n/N_2.$$

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

M est un idéal 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 $N_1 = l^{\alpha_1} M_n$

$N_2 = l^{\alpha_2} M_n$ α_1, α_2 entiers > 0

et $M_n(\mathbb{Z}/l^{\alpha_1}\mathbb{Z}) \xrightarrow[\varphi]{} M_n(\mathbb{Z}/l^{\alpha_2}\mathbb{Z})$

d'où $\alpha_1 = \alpha_2 =: \beta$.

Les automorphismes de $M_n(\mathbb{Z}/l^\beta\mathbb{Z})$ sont intérieurs, on se ramène donc à $\varphi = \text{id}$ et $M = (\{s_1, s_2\} \mid s_1 \equiv s_2 \pmod{l^\beta})$

alors $\text{Tr } s_1 \equiv \text{Tr } s_2 \pmod{l^\beta}$

et il existe (s_1, s_2) avec $\not\equiv \pmod{l^{\beta+1}}$. Donc $\beta = \alpha$.

$(0, l^\beta \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix})$. $\square$

Structure de M/lM . $\simeq M_n(\mathbb{F}_l) \oplus \varepsilon M_n(\mathbb{F}_l)$

$\varepsilon^2 = 0$ $\varepsilon \in \text{centre}$

$\simeq \left\{ (s, t) \mid s, t \in M_n(\mathbb{F}_l) \right.$
 $\left. (s, t)(s', t') = (ss', st' + ts') \right\}$.

en effet :

$$M \longrightarrow M_n(\mathbb{F}_l) \oplus \varepsilon M_n(\mathbb{F}_l)$$

$$(s_1, s_2) \longmapsto \left(\begin{array}{c} s_1 \pmod{l} \\ s_2 \pmod{l} \end{array}, \frac{s_2 - s_1}{l^\alpha} \pmod{l} \right)$$

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

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

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

$$\begin{array}{ccc} M_n(\mathbb{F}_\ell) & \xrightarrow{\quad} & (M/EM)^* \xrightarrow{\quad} GL_n(\mathbb{F}_\ell) \xrightarrow{\quad} \\ \text{additif} & & \downarrow \quad \downarrow \\ & & s_1 + \varepsilon s_2 \quad \mapsto \quad s_1 \\ & & s \neq 0 \end{array}$$

On a $\tilde{G} \subset (M/EM)^* = GL_n(\mathbb{F}_\ell) \cdot M_n(\mathbb{F}_\ell)$
 et $\tilde{G}$ engendre le $\mathbb{F}_\ell$ -esp. vectoriel M/EM .
 $\tilde{G} \rightarrow GL_n(\mathbb{F}_\ell)$ = red mod ℓ de ρ_1 et ρ_2 .

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

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

On s'intéresse au cas :

$m=2, \ell=2$ $\det \rho_1 = \det \rho_2$ + hyp standard
 C_2 d'ordre 2.
 Alors $\tilde{G} \subset S_4 \times C_2$

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

Remarque Sans Matur on élimine les g triangulaires

impossible pour $l > (p_0^{1/2} + 1)^8$ si E a bonne red en p_0

(cf. Invent.). On a en tout cas $p_0 \ll \log N_E$.

D'où OK pour $l \gg (\log N_E)^4$. Cet argument marcherait pour un sys de nombres quelconques.

Retour à $\tilde{G}$.

$$G \xrightarrow{p_1, p_2} GL_n(\mathbb{Z}_l)$$

t_1, t_2 red mod l absolument irréductibles et isomorphes

et $t_2 p_1 \neq t_1 p_2$.

$\mathbb{Z}_l$ -algèbre M , engendrée par l'image de G dans $M_n(\mathbb{Z}_l) \times M_n(\mathbb{Z}_l)$

Il existe un entier $\alpha \geq 1$ tel que (quitte à conjuguer p_1)

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

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

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

$$\tilde{G} = \text{image } \{ G \rightarrow (M/lM)^* \}.$$

$$s_1 + \varepsilon u \in M/lM \quad t(s_1 + \varepsilon u) = T_2(u) \in \mathbb{F}_l$$

$$s \in G \rightarrow \tilde{s} \in \tilde{G} \rightarrow t(\tilde{s}) \in \mathbb{Z}/l\mathbb{Z}$$

$$t(\tilde{s}) \equiv \frac{T_2 p_2(s) - T_1 p_1(s)^{34}}{l^\alpha} \pmod{l}$$

Variante.

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

gr. add (abélien)

$$\begin{array}{c} \uparrow A \\ p_2 \mid p_1 \\ G \end{array} \nearrow$$

donc un cocycle

$$p_2(s) = m(s) p_1(s)$$

$s \mapsto m(s)$ 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 $G \rightarrow GL_n(\mathbb{F}_\ell) \cdot M_n(\mathbb{F}_\ell)$ pr. semi-direct

$$s \mapsto m(s) p_1(s)$$

Hypothèse suppl. $\det p_1 = \det p_2$.

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

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

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

donc $s_1, s_2 \quad s_1 \equiv s_2 \pmod{\ell^\alpha}$

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

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

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

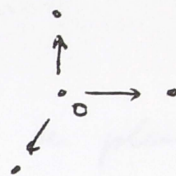
$$\text{Donc } \text{Tr}(u) \equiv 0 \pmod{\ell}.$$

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

repr. abs. irréd mod 2 isomorphe et $\det p_1 = \det p_2$.

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

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 cyclotome.)

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

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

A, B s.e.v. 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 $= 0, 1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$; $M_2^0 \supset A_2$

Dans $M_2(k)$ on peut plonger tout k' avec k'/k de degré 2 ^{sep.}

(choix d'un Cartan non déformé); alors $M_2(k) = k'.\text{lin} \oplus k'.\text{anti.lin.}$

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

$B =$ 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 ³⁶ e.v. de dim 2.

$$S_3 \cdot M_2^0 = S_4 \times C$$

Cyclique d'ordre 2

Cœur de $\mathbb{F}_2$

S_4 gr. sym de 4 lettres

$$S_4 = S_3 \cdot B$$

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 action par permutation de $V_4 - \{0\}$.

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

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

cl de S_4	1	-1	
(1)	0	0	(1)
(12)	0	0	(12)
(123)	0	1	(123)
(1234)	1	1	(12)
(12)(34)	0	0	(1)

$S_4 \rightarrow S_3$

ds S_3 les 3 premiers (1), (12), (123) et 1

$$1 + \varepsilon u \quad u=0 \Rightarrow \text{Tr}(u) = 0.$$

(1, -1) ds $S_4 \times C$ est $1 + \varepsilon \cdot 1$

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

$$\text{Tr}(u+v) = \text{Tr}(u) + \text{Tr}(v)$$

$$t(s, -c) = t(s, c) + \text{Tr}(s)$$

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

donc la deuxième colonne, à partir de la première.

• Dans $S_3 \cdot (\mathbb{F}_2 \oplus B)$, (12)(34) et dans B donc $\text{Trace} = 0$.

* (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 ds S_3 et has de carré = 1.)

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

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

② $S_4 \rightarrow S_4 \times \{1\}$

③ S_4 ("plgt diagonal" = (s, c) t.q. $\text{sgn}(s) = c$)

④ $S_4 \times C$

} ces 2 cas
sont conjugués

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

donc $\text{image}(\tilde{G} \rightarrow S_4)$ 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 poss. 234.

Remarque Dans le cas $S_3 \times C$, on a $t = 1$ si (et seulement si)

(s, c) est tel que s ordre 3 et $c = -1$.

Dans les cas ② et ③, $t = 1 \Leftrightarrow$ la comp. ~~de~~ 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 red en dehors de S (ens. de primes)

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

② Leurs pts de division par 2 engendrent une ext de $\mathbb{Q}$ de degré 8 à g. de Galois S_3 (et la même pour les 2 courbes).

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

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

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

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

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

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

Exemples Courbes de cond $57 = 3 \cdot 19$ cf. Annexes vol 4 p. 88

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

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

$$N_p = 1 + p - a_p \quad \text{on trouve les } a_p \quad \text{p. 117}$$

Il y a 3 a_p impairs d'au leur d'ordre 3 de G_{Gal}

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

d'au signature non triviale. D'au $G_{\text{Gal}} S_3$.

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

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

les a_p sont congrus mod 2. en fait 4

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

$$\begin{array}{c} L \\ | 3 \end{array}$$

$$\mathbb{Q}(\sqrt{-19})$$

$$| 2$$

$$\mathbb{Q}$$

on prend l'ext de deg 3 ramifiée en 2

(2 est inerte de $\mathbb{Q}(\sqrt{-19})$ d'au $\mathbb{F}_4^*$ ordre 3)

car L .

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

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

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

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

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

$$\text{en effet } t = 1 \Leftrightarrow \text{Frob}_p = (\text{elt d'ordre 3}, -1)$$

$$\begin{array}{ccc} \nearrow & & \updownarrow \\ \text{pt de pr d'ordre 2} & & \left(\frac{p}{3}\right) = -1 \\ \text{rat sur } \mathbb{F}_p & & p \equiv 1 \pmod{3} \end{array}$$

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

f_3 = eq de pts d'ordre 2. ⁴⁰ en fait a_p impair suffit

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

S_4 impossible

Si ce n'était pas 4 en dessous, 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 quadratique ne serait pas possible, discriminant impossible.

2^e Exemple

conducteur 37

37_A

37_B

$\Delta = +37$

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

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

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

trivialement : non ramifié en dehors de 2 et de 37

Hyp : m autres au pt d'ordre 2, S_3 .

Soit $p \in S$, $p \geq 5$ gr d'inertie en p ($\text{to } p_1, p_2$) est mod e' , donc cyclique d'ordre premier à p .

Soit $p = p_1$; action de l'inertie dans la repr. ρ .

1^{er} cas : bonne red en p , alors gen de l'inertie $\mapsto 1$ — Trace = 2

2^e cas : red mult. α , alors ⁴¹ gen de l'inertie $\sim \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$ Trace = 2

multiples

2° cas red additive

2.1 j non p-entier forme torquée du cas précédent

$$\text{gén} \mapsto \begin{pmatrix} -1 & * \\ 0 & -1 \end{pmatrix} \quad T_1 = -2.$$

2.2. j p-entier (pet. bonne red.)

gr. d'inertie et d'ordre	val disc $v(\Delta)$ mod 12	T_1
2	6	-2
3	4, 8	-1
4	3, 9	0
5	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 courbes, l'elt 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 courbes ont red. mult. en p .

Exemple Si E_1, E_2 ont red. 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 ont bonne red en 2, supersingulier $a_2' \equiv a_2^2 \equiv 0 \pmod{max}$
 et $a_2^1 = a_2^2$.
 Alors, à cong. près, le gr. de déc. en 2 dans $\tilde{G}$ est égal à S_3
 et le gr. d'inertie est A_3 .

Cor d'extension L'/L est non ramifié en 2.

$$S_4 \left(\begin{array}{c} L' \\ | \\ L \\ | \\ \mathbb{Q} \end{array} \right) S_3$$

La dev. utilise Honda, Cartier, Mering, Fontaine :
 (conjecture dim 1)

th Deux groupes p -divisibles 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 relevés d'un gr.

formel de lit h dans LT $t \mapsto t + \alpha_2 t^2 + \dots$

ici $t \mapsto \alpha_1 t + \alpha_2 t^2 + \dots$

donc c'est compatible.

la classification est faite par des modules de Drinfeld filtrés, un seul type possible.

le th. entraîne : les repr. 2-adiques attachées à p_1 et p_2 sont isom.
 sur le gr. de déc. en 2 (i.e. sur $\mathbb{Q}_2$) et sont abs. ind. mod 2.

Revenons à la def de $\tilde{G}$

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

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

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 $G \bmod 2^\alpha$: en effet il existe un G -isomorphisme $\psi_\alpha: C_1/2^\alpha C_1 \rightarrow C_2/2^\alpha C_2$ compatible avec G , donc avec G_2 . Mais alors $\text{ind} \Rightarrow$ commutatif de G_2 = bon

$$\text{donc } \psi_\alpha = u \cdot \varphi \bmod l^\alpha \quad u \text{ unité } 2\text{-adique}$$

(supersing. 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 $S_3 \subset \tilde{G}$. (u=0).

Serre

(Cours n°4)

29/10/84

Th (Agrawal, Coates, Hirst, Van der Poorten)

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

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

(B. Selmer : pour $p=7, 13, 23, 29, \dots, 281$ (1975) il n'y a pas 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 (^{une} à 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 Selmer). Le corps

Kengendré 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

$$\rho: \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \rightarrow \mathbb{Z}/3\mathbb{Z} \text{ ramifié que en } 11 \text{ et } 2.$$

Mais l'inertie en p agit par un élément unipotent donc d'ordre 2. Ainsi p provient d'un homom.

$\mathbb{Q}_2^\times \rightarrow \mathbb{Z}/3\mathbb{Z}$ par le corps de dév. local. Absurde.

Prop (Description de K). Le corps fixé par A_3 est $\mathbb{Q}(\sqrt{-11})$
 Comme $\binom{2}{11} = -1$, 2 est inerte dans $\mathbb{Q}(\sqrt{-11})$. On a
 $h(-11) = 1$, $0/20 \cong F_4$, $(0/20)^\times \cong \mathbb{Z}/3\mathbb{Z}$ d'où une
 est ramifiée seule 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 elt d'ordre 2) donc
 est $\mathbb{Q}(\sqrt{-11})$ ou $\mathbb{Q}(\sqrt{11})$. Si $\mathbb{Q}(\sqrt{-11})$, la th. du corps
 de dév. permet de conclure. Si $\mathbb{Q}(\sqrt{11})$, la th. du
 corps de dév. permet aussi de conclure.

La réduction de la courbe en 2 est supersingulière
 (Si $a_2 \equiv$ trace Frobenius en 2,
 $a_2 \equiv 0 \pmod{2}$, i.e. $a_2 = 0, 2, -2$)

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 a_2 egal a -1 , E est isogène à E_0 . Si ce n'était pas le cas, soit $\tilde{G}$ la dérivée centrée E et E_0 . Il s'agit d'une extension $\tilde{K}$ de $\mathbb{Q}$

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

Lemme: Si E_1 et E_2 ont bonne red. en dehors de p première, $p \neq 2$, et red. supersingulière en 2 avec $\hat{m}$ a_2 et ne sont pas isogènes, $\tilde{G} = S_4$.

$\tilde{G}^{\text{ab}} = \tilde{G}/(\tilde{G}, \tilde{G})$ 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 (théorème sur les groupes formels), donc a une image nulle dans $\tilde{G}$. $\tilde{G}$ est une extension biquadrique ramifiée seulement en p , ce qui n'existe pas.

On a donc $S_4 \begin{pmatrix} \tilde{K} \\ 1 \\ K \\ S_3 \\ \mathbb{Q} \end{pmatrix}$ d'inertie en 2 est un cycle d'ordre 3 et l'inertie en p est (12) des S_3

l'inertie en p est donc soit d'ordre 2, soit cyclique d'ordre 4 des S_4 . Mais $\tilde{G}$ a trois des éléments conjugués est 2, donc la diff. des traces est 0. Ceci

implique que ~~l'inertie en 2 est une~~ l'inertie en 2 est une transposition.

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

2^{ème} étape: Déterminer le nbre de branches de K .

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

Montrons que si a_2 de E est 0, E est isomorphe à la courbe à C.M. par $\mathbb{Q}(K_{11})$ (gros caractère associé: il associe à un idéal α de $\mathbb{Z}[K_{11}]$ le germe α tel que $\alpha \pmod{11}$ cané)
 $a_2 = 2$ E est cond. 11 * caract. de dépendance en 11

On reprend la construction précédente avec $\tilde{K} \approx S_4$.
 En 11 la ramification est cette fois-ci d'ordre 2 ou 4.
 On a $|d_{K_4}| \leq 2^{1/4} 11^{3/4} < 10$.

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

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 trivial en $s=1$?

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

Conclusion: il existe une courbe elliptique de W_{11} de conducteur 5077 avec $a_2 = -2, a_3 = -3, \dots$

comme pour $p < 420$. ; ce sont les $\hat{m}$ que ceux de la courbe E . Il faut vérifier que ces courbes sont isogènes (ce qui entraînera qu'elles sont isomorphes)

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

Démo: On obtient par les $\hat{m}$ arguments 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 ramifiée sur K .

En 2, on connaît la ramification de S_3 de corps quad est $\mathbb{Q}(\sqrt{5077})$. On a $h=1$ et 2 est inerte, d'où sur K canonique

Fait Il existe trois extensions $\tilde{K}$ ayant les propriétés exposées (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 se décode: si $\tilde{K}$ est l'un des précédents, 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 ext. de degré 4 avec des coeff. assez petits, ce qui permet de le calculer

Digression: Soit k un corps, k_s une clôture séparée
 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 ,
 $\text{Gal}(\tilde{K}/k) = S_6$. Elle est Galoisienne sur K de type $(2, 2)$.
 Soit Γ l'ensemble de ses extensions, auquel on adjoint
 un élément neutre, K lui-même.

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

On a des bijections:

$$\begin{aligned}
 \Gamma &\longleftrightarrow H^1(\text{Gal}(k_s/k), V) = \text{Hom}_{S_3}(\text{Gal}(k_s/K)^{\text{ab}}, V) \\
 &= \text{Ker}(\text{Cor}: H^1(k_s, \mathbb{Z}/2\mathbb{Z}) \rightarrow H^1(k, \mathbb{Z}/2\mathbb{Z}))
 \end{aligned}$$

a) le dernier groupe est $\{ \alpha \in k_s^X \text{ mod } k_s^{X^L} / N \alpha \text{ surré} \}$.

Un 1-cocycle de $(\text{Gal}(k_s/k), V)$ fournit

$$\text{Gal}(k_s/k) \rightarrow S_3 \ltimes V \quad \text{ie une ext. de type } S_6.$$

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

$$\begin{array}{ccccccc}
 H^1(S_3, V) & \rightarrow & H^1(G_k, V) & \rightarrow & H^0(S_3, H^1(G_k, V)) & \rightarrow & H^2(S_3, V) \\
 \text{"} & & \text{"} & & \text{"} & & \text{"} \\
 0 & & & & & & 0
 \end{array}$$

(Les 0 viennent du fait que V est projectif sur S_3 , car c'est la repr. réf. de 2-Sylow).

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

$$\text{Cor: } H^1(G_k, \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \rightarrow H^1(G_k, \mathbb{Z}/2\mathbb{Z})$$

proviennent de $(x, y, z) \mapsto x + y + z$ de $(\mathbb{Z}/2\mathbb{Z})^3$ de $(\mathbb{Z}/2\mathbb{Z})$

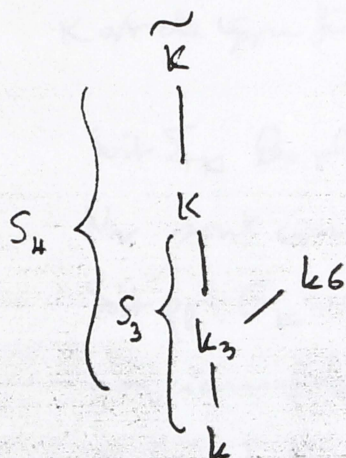
La suite $(4/22) \rightarrow 4/22 \rightarrow 0$ et sa suite

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

La correspondance fournit pour $\tilde{K}$ une extension k_6 de k_3 (elle associe à la racine d'un i^{th} α de k_3).

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

$\text{Gal}(\tilde{K}/k_6) = \text{stabilisateur de } (12) \cap \text{stabilisateur de } (34)$



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

$$k_3 = k(x_1 x_2 + x_3 x_4)$$

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

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

$$\sigma_3 = x_1 x_2 x_3 + x_1 x_2 x_4 + \dots$$

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

Les corps cubiques de $\text{disc} < 100000$ (tot. rel.) ont < 20000 (complexes)

été dét. par Angell, avec aide de données et unités fond.

Mike Matthews 76

Bloemer et Kramer.

Brouer - Kromer

(*) Noter que $(x_1 + x_2)^2 = -(x_1 + x_2)(x_3 + x_4) = x_1 x_2 + x_3 x_4 - \sigma_2$ et $\sigma_2 = \sum_{i < j} x_i x_j$
Donc $(x_1 + x_2)^2 \in k_3$.

Et noter que $\sum x_i = 0 \Rightarrow \sigma_3 = (x_1 + x_2)(x_1 + x_3)(x_1 + x_4)$.

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

5/11/84

Série (Cours n°5)

V-1

Représentations l -adiques attachées aux variétés abéliennes.

Soit K un corps de nombres. (Les résultats sont en fait vrais sur 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 $G_K = \text{Gal}(\bar{K}/K)$.

Soit $\rho_l: G_K \rightarrow \text{Aut}(V_l)$ une représentation continue de G_K , non ramifiée en dehors de $S \cup S_l$ (avec $S \subset \Sigma_K$ fini et $S_l = \{v \text{ places de } K \text{ au dessus de } l\}$). Supposons $\rho_l \text{ rat}/\mathbb{Q}$ relativement à S (ce qui par définition signifie que

$\chi_v \neq 1 \notin S \cup S_l$, $\text{Car}(\rho_l(\text{Frob}_v)) \in \mathbb{Q}[T]$).

Covariante: idem pour presque tout v ; on ne sait pas si c'est équiv.

Exemple: A s.ab./ K , S ens. des places de mauvaise

réduction, $V_l = V_l(A) = H_1(A, \bar{K}, \mathbb{Q}_l)$. Le polynôme caracté-

ristique de $\rho_l(\text{Frob}_v)$ coïncide avec le pol. caractéristique

de l'endomorphisme de Frob. de $\bar{A}_v$ (red. 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 ^{équiv.} compatibles (par rapp. à S) si

$\text{Car}(\rho_{l_1}(\text{Frob}_v)) = \text{Car}(\rho_{l_2}(\text{Frob}_v))$ pour $v \notin S \cup S_{l_1} \cup S_{l_2}$

Covariante: idem pour presque tout v ; on ne sait pas si il y a équiv.

Si on connaît ρ_{l_1} , il y a au plus une ρ_{l_2} compatible avec ρ_{l_1} (conséquence immédiate de l'absolue

Problème 1 Si ρ est une repr. l -adique sat., et $l' \neq l$, existe-t-il une repr. l' -adique compatible avec ρ , sans être ramifiée sur un nombre fini de l' ?

Remarque: H_3 se plonge dans $GL_2(\mathbb{Q}_l)$ pour $l \neq 3$ mais pas dans $GL_2(\mathbb{Q}_3)$: il se plonge dans $(\text{quat-en } 2)$, ce qui montre que dans le pb. 1, on ne peut espérer "pour tout l ". Cependant la phénoménologie à l'échelle est la seule obstruction à "pour tout l " connue de Serre.

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

Problème 3: Soient ρ_{l_1}, ρ_{l_2} deux représentations du type précédent, compatibles et semi-simples. Si ρ_{l_1} est irréductible, en est-il de même de ρ_{l_2} ? (en appliquant ceci aux p-iss tensorielles, ceci entraîne que les invariants de ρ_{l_1} et ρ_{l_2} ont m même dimension). C'est lié à la conj. de Tate caractérisant les classes de cycles

{ algébrique
de Galois absolu

Soit A une variété abélienne, ℓ une ligne première,

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

G_ℓ l'image de ρ_ℓ .

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

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

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

Thm¹ (Boyd-Mazur): - G_ℓ est ouvert dans $\underline{G}_\ell(\mathbb{Q}_\ell)$

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

Th2. $\underline{G}_\ell$ contient G_m (homothéties)

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

Th3. Le quotient $\underline{G}_\ell / \underline{G}_\ell^\circ$ est indépendant de ℓ (et c'est un $G_K \rightarrow \underline{G}_\ell / \underline{G}_\ell^\circ$ est indép. de ℓ)

On sait que $\mathfrak{g}_\ell = \mathfrak{c}_\ell \oplus \mathfrak{s}_\ell$ avec $\mathfrak{c}_\ell$ abélienne et $\mathfrak{s}_\ell$ 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.

Th4 T_ℓ est indépendant de ℓ (i.e. il provient d'un tore sur $\mathbb{Q}$, indépendant de ℓ)

Th5 Le rang de S_ℓ (ou celui de $\underline{G}_\ell^\circ$, cela revient au vu le Th. 4) est indépendant de ℓ . Plus précisément les tors maximaux de $\underline{G}_\ell^\circ$ possèdent

(après extension des scalaires)
dans $C_2/\mathbb{Q}$.

d'ordre/2 plongé

Th. 6 A est de type $CF \Leftrightarrow S_\ell = \{1\}$ i.e. G_ℓ abélienne.

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

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

Soit Z le centre de Λ $Z = \prod Z_\alpha$ avec $\mathbb{Q} \subset Z_\alpha$ corps

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

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

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 $\text{Lie } T_Z(\mathbb{Q}_\ell) = Z_\ell$ plongé
dans $\text{End}(V_\ell)$

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

En effet C_ℓ commute à G_ℓ , donc à G_ℓ
après ext. finie des scalaires, et C_ℓ commute à Λ_ℓ . Or
par Faltings le commutant de G_ℓ est Λ_ℓ , d'où C_ℓ est
de Λ_ℓ , i.e. $C_\ell \subset Z_\ell$

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

$$\det_{Z_\ell} : G_K \rightarrow Z_\ell^\times$$

$\searrow \quad \nearrow$
 G_ℓ

on ne veut pas des alg. de Lie $C_\ell \oplus S_\ell \rightarrow Z_\ell$ annule

54
 S_ℓ et $C_\ell = \sum C_{\ell, \alpha} \in \bigoplus Z_{\alpha, \ell}$

l'image de C est $\sum d_{x,l} z_{x,l}$ avec $d_{x,l} = \dim z_{x,l}$.
Comme C est une $\mathbb{Q}$ -algèbre, il suffit de voir
que l'image de $\det_{\mathbb{Z}} \rho_l : G_K \rightarrow \mathbb{Z}_l^\times$ est algébrique,
indépendante de l , contenant G_m .

(cf. Mc Gill, 1967, Henniart DPP, 1980-81)

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

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

Exercice : Expliquez $\det_{\mathbb{Z}} \rho_l$.

2 méthodes a) donner des Schurman
b) Utiliser Hodge-Tate

(modulo th. 1)

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

Lemme : Si $v \nmid 5$ ou p et $\pi_v = \text{image de } \text{Frob}_v \text{ dans } \text{Aut}(V_v)$.

Le plus petit sous-groupe algébrique de GL_2 contenant
 π_v contient G_m . En effet si π est une matrice semi-
simple inversible, $\pi = \begin{pmatrix} \lambda_1 & \\ & \lambda_2 \end{pmatrix}$, l'enveloppe algébrique
des groupe engendré par π est $\left\{ \begin{pmatrix} t_1 & 0 \\ 0 & t_2 \end{pmatrix} / \prod t_i^{m_i} = 1 \text{ si } \prod \lambda_i^{m_i} = 1 \right\}$.

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

Théorème $G_{\mathbb{Q}}^0 = T_{\mathbb{Q}} \Leftrightarrow A$ de type (M/K) ($\Leftrightarrow \text{rg}(\text{End } A \otimes \mathbb{Q}) = g$
où $g = \dim A$)

avec $g = \text{dimension maximum des sous-alg. commutatives (réelles)}$

(A de type CM $\Leftrightarrow$ A s'inscrit à un produit de v-places simples d'anneau d'ent. $\mathbb{Q}$ en corps $\mathbb{Z}$ de degré $2 \dim A$ sur $\mathbb{Q}$.)

L'implication $\Rightarrow$ résulte de Faltings (en effet le sous-espace de $\mathbb{Z}$ des $\text{End } V_\ell \otimes \mathbb{Q}_\ell$ est de rang $\leq g$) et celui de G_ℓ est à priori plus grand si $G_\ell^0 = T_\ell$)

Exercice (Question de Bruce Jordan) : Soit A une var. abél. $v \notin S$; $\tilde{A}_v$ supersingulière si une puissance de Frobenius est une homothétie, i.e. si $\tilde{A}_v$ est produit de c. ell. supersingulières.

Théorème : Si A n'est pas de type CM (sur $\overline{\mathbb{K}}$), $\exists v \notin S$ tel que $\tilde{A}_v$ est supersingulière et densité 0. En fait $\text{Card} \{v / v \text{ a cette propriété et } N_v \leq u\} = O\left(\frac{u}{(\log u)^{1+\delta}}\right)$ avec $\delta > 0$.

Dém. : soit ℓ choisi. Considérons l'image He de G_ℓ dans $\text{PGL}(V_\ell)$. Dire que $\tilde{A}_v$ est supersingulière signifie que l'image Π_v^H de Frob_v dans He 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~~ ^{forment} un sous-ensemble analytique de H d'intérieur vide.

Soit v avec Frob_v dans cet ensemble ont donc densité 0.

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

Soit x un pt intérieur de H_m . Notons $Ad(x)$ l'autom
de $\mathfrak{h}$ de x de $\mathfrak{h} = \text{Lie } H$.

$$\text{Ker}(Ad(x) - 1) = \text{Lie}(\text{Cent. algébrique de } x)$$

C_x est discret (sinon il existe $c_n \in C_x$, $c_n \rightarrow 1$,

$$\text{d'où } (c_n x)^m = 1 \text{ d'où } c_n^m = 1, \text{ absurde})$$

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

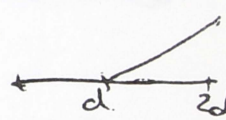
Thm 9 (Borel - Mostow) - Toute alg. de Lie (en car. 0) qui a
un autom sans pts fixes est résoluble.

Ceci achève le thm 8.

En sens inverse, on conjecture que G est avec rés.

ordinaire (i.e. où $\sigma_1, \dots, \sigma_d$ d. premiers

pts sym.-élémt. unités) et de densité > 0



~~Il est évident que si G est résoluble, alors G est sans pts fixes.~~ Ceci suit sent^t le
lemme 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

Série. (Cours n°6)

Borel-Mostow: Soit $\mathfrak{g}$ une alg. de Lie de dimension finie (sur $\mathbb{C}$)

Si $\sigma \in \text{Aut}(\mathfrak{g})$, $\sigma x \neq x$ pour $x \neq 0$, $\mathfrak{g}$ est résoluble

Steinberg: Endomorphisms of Lie algebras : étude des

endom. de $\mathfrak{g}$ Lie alg.

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

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

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

Soit $\underline{B}$ la variété des Borel, σ opère sur $\underline{B}$. Soit $\lambda(\sigma)$ le nombre de Lefschetz de σ opérant sur $\underline{B}$
 $(= \sum (-1)^i \text{Tr } \sigma | H^i(\underline{B}) |)$. 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:

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

Or il est multiple de σ par un autom. intérieur, on peut supposer que σ conserve une couple (B, T)

On a $\underline{B} = \bigcup_w BwB/B = \bigcup_{w \in W} s_w$ de where $H(\underline{B})$ est en degré pair et a pour base les cycles s_w .

$\text{Tr}(\sigma) =$ nbre des s_w fixés par σ . D'où le résultat

σ présente un beral B . Soit U le radical nilpotent de B . On a $\sigma(U) = U$. Soit $T = B/U$, σ définit un auto-morphisme σ_T de T , σ_T présente le système de racines, la base associée à B , la base engendrée, donc a une l'et un pt fixe $\neq 0$.

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

Remarques : 1) Si G a un auto σ d'ordre premier avec pts fixes $\neq 0$, G est nilpotente (en toute cas, d'après Jacobson)

2) Si σ d'ordre 4 : il y a une alg. de Lie $\mathfrak{g}$ non nilpotente avec un auto σ sans pt fixe d'ordre 4.

Soit $\mathfrak{g}_a(1)$ sur lequel agit G_m par $t \cdot x$. On prend le produit semi-direct $G_m \rtimes (\mathfrak{g}_a(1) \rtimes \mathfrak{g}_a(-1))$

(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.

$x \mapsto -x$, $e \mapsto f$, $f \mapsto -e$ (c'est un auto d'ordre 4)

Question : Si G fini a un auto σ sans pts fixes $\neq 1$, G est-il résoluble? (σ sans pts fixes $\Leftrightarrow \sigma$ est "à" injectif)

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. C , N un entier ≥ 1 et

$d: GL_N \rightarrow \text{Aff}_N^*$ rep. affine de dim N , puis de l'application $a_N = 0$.

$$x \mapsto a_1(x) = \sum \text{val. propres}$$

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

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

Deux pts ont $\tilde{m}$ images $\Leftrightarrow$ ils ont $\tilde{m}$ rel. caract.

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

Th Soit G un sous-gr. alg de GL_N . Alors

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

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

Plus précisément, si T est une torse maximale de G , $d(T) = d(G)$. Si G est réductif sur $\bar{K}$ connexe, on a encore $\dim d(G) = \text{rg } G$.

3) Si M_1 et M_2 sont deux groupes de type ~~connexes~~ multiplicatifs, on a $d(M_1) = d(M_2) \Leftrightarrow M_1$ et M_2 sont géom. conjugués dans GL_N .

4) Si $N \subset G$, N invariant dans G et $g \in G$, alors $d(gN)$ est fermé dans Aff_N^* .

Soit T_N la torse standard de GL_N

$$d \left(\begin{pmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_N \end{pmatrix} \right) = (\sigma_1(\lambda), \sigma_2(\lambda), \dots, \sigma_N(\lambda))$$

c'est un morphisme fini de T_N sur Aff_N^* surjectif.

Plus précisément $T_N/G_N \simeq \text{Aff}_N^*$.

Remarquons que si M est de type multiplicatif, $d(M)$ est fermé de dimension égale à celle de M . En effet, quitte à étendre les scalaires, on peut se supposer $M \subset T_N$, d'où $d(M)$ fermé de dimension.

Si M_1, M_2 sont connexes et de types multiplicatifs dans T_N avec $d(M_1) = d(M_2)$, M_1 et M_2 sont conjugués par G_N (car $T_N \rightarrow \text{Aff}_N^*$ est un revêtement galoisien, cf AC IV, conj des idéaux primaires au-dessus d'un idéal).

Tout sous- $\mathfrak{g}$. alg. ^{M} de T_N est défini sur $\mathbb{Q}$, donc aussi $d(M)$.

Soit G réductif connexe et T tore maximal de G . Tout $\mathfrak{e}^+$ semi-simple de G est conjugué géom à un $\mathfrak{e}^+$ de T . On en déduit $d(G) = d(T)$.

On a $d(G) = d(G/U)$ donc on s'étend aux cas où G non réductif. D'où 2) et 1).

Si $x \in G$ et $\sigma \in \text{Aut}(k/\mathbb{Q})$, on montre que $d(x)^\sigma \in d(G)$. Le plus petit sous- $\mathfrak{g}$. alg. ^{M} contenant x est de type multiplicatif. On a $d(M)$ défini sur $\mathbb{Q}$ et $M \subset G$ et donc $d(x)^\sigma \in d(M) \subset d(G)$.

Il reste à prouver 4) et 1) si G non connexe, et de faire 4) ^{avec N connexe}, appliquée avec $N = G^0$ au cas 1) et 4). On le fera plus tard.

Soyent ρ_1, ρ_2 deux repr. l.-ad. réductibles
compatibles, semi-simples, de même dimension N

Soyent G_{ρ_1}, G_{ρ_2} leurs images et $\underline{G}_{\rho_1}, \underline{G}_{\rho_2}$ leurs enveloppes
algébriques (qui sont réductives)

Thm. - $\text{rang } G_{\rho_1} = \text{rang } G_{\rho_2}$

Quitte à étendre le corps de base, on peut supposer
les groupes connexes. Alors $d(G_{\rho_1})$ et $d(G_{\rho_2})$ sont des
fonct. définies sur $\mathbb{Q}$, de Aff_N^* . En fait on a
 $d(G_{\rho_1}) = d(G_{\rho_2})$: ces suites sont l'adhérence
de l'ensemble des pol. de Frobenius, pour $v \notin \text{us. fin}$
des places. Ceci prouve le théorème.

Plus précisément, si T_1 et T_2 sont des tors maximaux
de G_{ρ_1} et G_{ρ_2} sont conjugués dans toute extension
contenant $\mathbb{Q}_{\rho_1}$ et $\mathbb{Q}_{\rho_2}$

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

Notation:

Soit G un gr. alg. linéaire, f une fonction sur G

(morphisme de G dans le double affixe). Soit

$d_G(f=0)$ = la densité des pts de G où $f=0$ au-dessus

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

Considérons les représentations ρ_1, ρ_2 et soit f une polynôme en les $a_i(x) (= \text{Tr } \Lambda^i(\rho(x)))$ à coeff dans $\mathbb{Q}$.

Théorème $d_{G_{\mathbb{Q}_\ell}}(f=0) = d_{G_{\mathbb{Q}_\ell}}(f=0)$
 ($d_{G_{\mathbb{Q}_\ell}}(f=0)$ = densité des places v de K telles que $f(a_i(\text{Frob}_v))=0$)

Il suffit pour ce le fixer de démontrer l'égalité entre parenthèses. On a $G_{\mathbb{Q}} \subset G_{\mathbb{Q}_\ell}(\mathbb{Q})$. Soit

$$G_{\mathbb{Q}}^\circ = G_{\mathbb{Q}} \cap G_{\mathbb{Q}_\ell}^\circ$$

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

$$\text{Soit } G_{\mathbb{Q}} = \bigcup_{i=1}^l \gamma_i G_{\mathbb{Q}}^\circ$$

Soit $f=0$ sur $\gamma_1 G_{\mathbb{Q}}^\circ, \dots, \gamma_l G_{\mathbb{Q}}^\circ$ et $f \neq 0$ sur

$\gamma_{l+1} G_{\mathbb{Q}}^\circ, \dots, \gamma_{l+k} G_{\mathbb{Q}}^\circ$. On a $d_{G_{\mathbb{Q}_\ell}}(f=0) = \frac{l}{l+k}$.

Pour que $f(a_i(\text{Frob}_v))=0$, il faut et il suffit que Frob_v tombe dans $\gamma_i G_{\mathbb{Q}}^\circ$ ($1 \leq i \leq l$) ou dans une sous-variété aut. d'int. vide de $\gamma_i G_{\mathbb{Q}}^\circ$ ($l+1 \leq i \leq l+k$).

D'où le résultat par le lemme de Chebotarev.

Soit $d(f=0)$: densité des v avec $f(\text{Frob}_v) = 0$.

Précision sur le nbre des v avec $f(\text{Frob}_v) = 0$ et $N_v \leq X$:

$$\text{C'est } d(f=0) \frac{X}{\log X} + O\left(\frac{X}{(\log X)^{1+\epsilon}}\right)$$

Thm 1. Pour que G_ℓ soit connexe, il faut et il suffit que, pour tout polynôme $f \in \mathbb{Z}[a_1, \dots, a_n]$, on ait $d(f=0) = 0$ ou 1.

Corollaire : le noyau de $\text{Gal}(K/K) \rightarrow G_\ell/G_\ell^\circ$ est indépendant de ℓ .

(En effet c'est le plus petit corps K sur lequel l'image de G_ℓ est connexe).

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

(ceci entraîne le th 1)

1^{ère} lem : Soit G groupe linéaire, G° le sous-groupe neutre $g \in G/G^\circ$, $g \neq 1$.

Soit $\sigma : G/G^\circ \rightarrow GL(V)$ ^{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 gr. linéaire, et $G \rightarrow GL(E)$ repr. fidèle, toute repr. de G est sous-quotient d'une $T_{n,1} = E^{\oplus n} \otimes E^{\ast \oplus 1}$

On prend $E = \mathbb{P}^1$ espace de $\mathbb{P}^1$

$$\sigma : G \rightarrow G/G^\circ \rightarrow GL(V)$$

Si $x \in G$, les $a_i(T_{n,s}(x))$ ont des pol. en $a_1(x), \dots, a_n(x)$
 & $a_n'(x)$ à coeff. entiers

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

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

avec q assez grand

Ceci est une polynôme. Posons

$$f = \prod_{\substack{\text{racines} \\ \text{primaires} \\ \text{m-és de 1}}} P_{1,\mu}$$

f s'annule sur gG°

On a $f_{1,\mu}(1) \neq 0$

pour tout μ , d'où

$$f(1) \neq 0.$$

Autre démonstration (en admettant 4)

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

$\mathcal{L}(1)$ n'est pas dans $\mathcal{L}(gG^\circ)$ car sinon gG° contiendrait un $\mathbb{G}_m^+$ 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 $P(a_1, \dots, a_n, a_n')$ qui est zéro sur gG° et $\neq 0$ en 1. Comme les F_{ab} ont des pol.

car à coeff. des $\mathbb{Q}$ et sont définies dans G , gG° est défini sur $\mathbb{Q}$ et P peut être pris à coeff. rationnels.

Provenons que si $N \triangleleft G$, N connexe, $g \in G$, $\mathcal{L}(gN)$ est fermé de dimension $\leq \text{rg}_{\text{red}} N$.

Quelques cas particuliers du th. 4

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

$\dim \mathfrak{d}(gN) = \dim N$ car $\mathfrak{d}: T_{\text{stabil}} \rightarrow \mathfrak{A}$ est fini

- 2) N est un tore et g semi-simple.

g induit un autom. de N d'ordre fini

$$\mathbb{Q} \otimes \hat{N} = \underbrace{\text{partie fixe}}_{\text{sous } g} \oplus \underbrace{\text{parties non fixes}}_{\text{Ker}(1-\sigma)} = \text{Im} \left(\frac{1+\sigma}{2} \right)$$

$$N = N_+ \cdot N_-$$

$$\begin{cases} N_+ \text{ tore fixe par } \sigma \\ N_- \text{ conjugué par } \sigma(t)t^{-1} \end{cases}$$

$$\text{On a } \mathfrak{d}(gN) = \mathfrak{d}(gN_+)$$

$$\text{Soit en fait } n \in N \quad n = t_+ (\sigma(t)t^{-1}) \text{ avec}$$

$$\sigma(t) = g^{-1}tg \quad gn = gt_+g^{-1}tg t^{-1} = tt_+gt^{-1}$$

$$\text{conjugué de } t_+gt^{-1} = gt_+$$

Dans ce cas $\mathfrak{d}(gN)$ est fermé de dimension égale à $\dim N_+$ (centralisateur de g)

Donc $\dim \mathfrak{d}(gN) \leq \dim N$ avec égalité $\Leftrightarrow$ conjugué à N .

19/11/84

Série (Cours n° 7)

Rappel 1 k alg.⁺ des.

$$\ell: GL_N \rightarrow \text{App}_N^* = \{a_1, \dots, a_N \mid a_N \neq 0\}$$

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

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

La dem. avait été commencée.

Cas 1, 2 : g semi-simple et H tore.
 Cas 2' : g q.c.g. et H tore (on fera après)
 Cas 3 : g semi-simple et H réductif : On utilise le

Thm de Borel-Motzkin : tout autom. semi-simple d'un
 (comme autom. de l'alg. de Lie)
 gr. réductif conserve un tore maximal.

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 $\ell(gH) = \ell(gN)$. Comme N est réunion
 disjointe de $n_\alpha T$ en nombre fini. On conclura grâce à 2'

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

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

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

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

Comme $u \in H$, $u^{-1}g'u^{-1} \in gH$ car H distingué dans G .

Comme g et $u^{-1}g'u^{-1}$ normalisent T , le aussi.

On a donc $u^{-1}g'u^{-1} \in gN$.

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

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

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

Dém.: Soit $g = g_{ss}g_u$. L'autom $h \mapsto g_u h g_u^{-1}$ est dans la sous-structure $\text{Aut}(H)$, donc est intérieur et est un autom. 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 commutatif à H .

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

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

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

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

Comme α commute à c et que αc est unipotent et α semi-simplifiable, c est unipotent et c commute à g_{ss} .

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

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

4) Cas général.

On remplace l'élément arbitraire par son semi-simplifiable par rapport à l'action de G . Alors G devient réductif (et H aussi car H est distingué dans G)

On a $d_Y(gH) = d_{Y^{ss}}(gH)$ et on retombe dans le cas précédent.

La d_{ss} donne une critère pour que $\dim d(gH) = \dim H$: Il faut et il suffit que l'automorphisme σ_g du tore maximal conjugué de H soit l'identité (au moins si H est réductif). A vérifier.

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

Dém: Si $w \in W$, $w' \in W^*$, le coeff. $m_{w, w'} : s \mapsto \langle sw, w' \rangle$ est un élément de l'alg. affine de G .

Si la repr. de 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 $\hat{\otimes} V \otimes V^*$). Un coeff de W est donc un coeff ^{comb. lin.} d'un certain $T_{\lambda, \mu}$. Or

on a

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

On a à remplacer E par E^n . On peut supposer que les coeff. sont égaux. Soit $m_{w, w'} = m_{\varepsilon, \varepsilon'}$ ($\varepsilon \in E$, $\varepsilon' \in E'$). Dans $W \oplus E$, $x = (w, -\varepsilon)$ et $x' = (w', +\varepsilon')$ vérifient $\langle x, x' \rangle = 0$. Les transformées de x sont contenues dans $x'^{\perp}$. Soit F le plus petit sous app. de $W \oplus E$ contenant x , stable par G .

On a $F \cap W \oplus \{0\} = \{0\}$ car $F \perp x'$

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

$F \rightarrow E$ est injectif et W est un quotient de F car $F \cap W = \{0\}$.

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

Enonc premier

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

$$G = \text{Gal}(K/K) \xrightarrow{\rho_{\ell}} GL(V_{\ell}(A)) \simeq GL_2(\mathbb{Q}_{\ell})$$

G_{ℓ} image de G , G_{ℓ} env. alg. de G_{ℓ}

G_{ℓ} est réductif. On a n_{ℓ} qz pour rang (et son tore maximal) sont indépendants de ℓ .

Si on choisit une ^{représentation} χ 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 $\pi_v = Frob_v$.

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

G_{ℓ} est donc contenu dans le groupe des similitudes symplectiques CSp_{2n}

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

On a $\text{rg}(G_{\ell}) \leq 1+n$.

Th. Si $\text{End}_{\overline{K}} A = \mathbb{Q}$

$$\text{rg } \underline{G} = 1+n \iff \underline{G} = \text{CSpr}_{2n, \ell}$$

Corollaire Si $\underline{G} = \text{CSpr}_{2n, \ell}$ pour un ℓ , $\underline{G} \simeq \text{CSpr}_{2n, \ell}$ pour tout ℓ .

(En effet $\underline{G} \simeq \text{CSpr}_{2n, \ell} \Rightarrow \text{End}_{\overline{K}} A = \mathbb{Q}$).

Démonstration

$$g_{\ell} = C_{\ell} \oplus D_{\ell} \quad \text{sp} \subset \text{spr}_{2n}$$

C_{ℓ} = homothétie et la repr. naturelle de sp est absolument irréductible, d'après Faltings.

On a sp abs. ind. et de rang n dans $\text{spr}_{2n, \ell}$.

Lemme (Brel de Sieberthal) : soit α alg. de degré simple de rang n , $\alpha \subset \alpha'$ semi-simple de rang n .
Comment déterminer celle qui sont max $\neq \alpha$.

Recette α_i base des racines de α

$$\tilde{\alpha} = \sum m_i \alpha_i \text{ plus q. de racine}$$

Soit i tel que m_i soit première et R_i le sous-système de R formé des racines avec $\alpha_i \equiv 0$ mod m_i .

Alors R_i est un syst. de racines de rang n , max et i conjugués ils sont tous ainsi.

spr_{2n} :

$$\tilde{\alpha} = 2\alpha_1 + 2\alpha_2 + \dots + 2\alpha_{p-1} + \alpha_p$$

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

$\text{spr}_{2i} \oplus \text{spr}_{2n-2i} \hookrightarrow \text{spr}_{2n}$. Toutes les sous alg. de

spr_{2n} max. de rang max sont de cette forme, mais elles ne sont pas irréductibles, donc ne conviennent pas.

Remarque : pour les gros descripteurs, c'est la m¹ chose
mais pas pour les g¹ exceptionnels.

Géométriquement sur les diagrammes de
Dynkin, on prend le diagramme complété et
on supprime le sommet d'indice 1.

Compléments

$l \neq p$

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

- Simplicité des V_ℓ } en car $\neq 2$ (Zachar)
 - $\text{Comm} = \text{endom} \otimes \mathbb{Q}_\ell$ } en car 2 (Moret non publié, (Robert Bailey, thèse))

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

$\underline{\mathcal{G}}_\ell$ est un g¹e réductif.

On peut décomposer $\underline{\mathcal{G}}_\ell = \mathcal{T}_\ell \ltimes \mathcal{S}_\ell$.

$\mathcal{T}_\ell$ est défini sur $\mathbb{Q}$, indépendant de ℓ , contenu dans
le tore des centres des endomorphismes de A .

$$\text{Lie } \mathcal{G}_\ell = \mathcal{T}_\ell \oplus \mathcal{S}_\ell.$$

$$\mathcal{G}_\ell = \text{Lie } \mathcal{G}_\ell = \mathcal{Z}_\ell \oplus \mathcal{S}_\ell \quad \text{avec } \dim \mathcal{Z}_\ell = 1.$$

(comme $\mathcal{G}_\ell$ est réductif elle contient la dérivée de
son enveloppe algébrique, $\mathcal{S}_\ell$)

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

Exemple: Soit $E/\mathbb{F}_q$ ordinaire, considérée par
 ses valeurs propres comme sur $\mathbb{F}_q(\lambda)$. Elle a
 un $Q(V, d)$ qui fournit une tore T de dim 2.
 Le Frobenius sur $\mathbb{F}_q$ donne $\pi \in T(\mathbb{Q})$ et Z est la
 ses. op. analytique sur π .

Le rang de $G_{\mathbb{Q}}$ est indep^t de l , ainsi que celui
 de $g_{\mathbb{Q}}$. Le rang $G_{\mathbb{Q}}/G_{\mathbb{Q}^c}$ est indep^t de l .

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

Théorème: Le groupe $G_{\mathbb{Q}}$ contient une tore "de type H "

(géométriquement)

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

Ex: cas des courbes elliptiques:

• ses mult. compl: $G_{\mathbb{Q}} = GL_2 \supset \begin{pmatrix} * & 0 \\ 0 & * \end{pmatrix}$

• avec " " : $G_{\mathbb{Q}}$ est une tore (de type H après
 est des racines)

Soit v une place de K divisant l et $\bar{v}$ une place de $\bar{K}$

prolongant v . On a $G \supset D_v \supset I_v$ (D_v gr. de dév de $\bar{v}$,
 I_v "d'inertie de v)

La restriction de la représentation l -adique à I_v
 géométriquement
 contient une tore $H_{1/2} (\approx \begin{pmatrix} \lambda & & 0 \\ & \ddots & \\ 0 & 1 & \ddots & 1 \end{pmatrix})$: c'est la
 théorie des modules de Hodge-Tate.

Or les homothéties sont contenues dans $G_{\mathbb{Q}}$. D'où le
 résultat.

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

$$\underline{G}_\ell = \text{Sp}_4.$$

En effet $\mathcal{G}_\ell = \text{homothéties} \oplus \mathcal{D}_\ell$ avec $\mathcal{D}_\ell \subset \text{Sp}_4$ abs² irréductible.

Si $\text{rg } \mathcal{D}_\ell = 2$ $\mathcal{D}_\ell = \text{Sp}_4$ (déjà vu)

Si $\text{rg } \mathcal{D}_\ell = 1$ $\mathcal{D}_\ell \simeq \text{sl}_2$ (géométriquement) et la repr. de dim 4 de sl_2 est Sym^3 (repr. irréductible).

On a donc $\underline{G}_\ell \simeq \text{GL}_2$ dans sa repr. Sym^3 . La torse 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. Contre-diction.

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

$\text{SO}_3 \oplus \text{GL}_2$ 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 montrons plus tard que ce groupe est impossible).

Problème. Soit X le ^{5^{es} groupe} alg. de $\underline{G}_\ell^\circ$ engendré par les conjugués (géom.) des tores de $\underline{G}_\ell^\circ$ de type H. Est-il vrai que $X = \underline{G}_\ell^\circ$?

Remarque : la représentation galoisienne dans $\underline{G}_\ell^\circ / X$ est, quitte à étendre le scalaires, non ramifiée au-dessus de $\mathbb{C}$.

26/11/84

XVII (Lours n°8)

VII - 1

Tore 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 note 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'une tore par un groupe fini cyclique.

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

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

$\chi = \chi(\Theta_s) \in \text{Hom}_{\bar{k}}(\Theta_s, G_m)$ et la représentation $\rho: \Theta_s \rightarrow GL_N$

est déterminée par son caractère $\chi(\rho) = \sum_{x \in X} n_x x$

avec les n_x positifs, presque tous positifs, et

puisque par définition sur k , $\chi(\rho)$ est $\text{Gal}(\bar{k}/k)$ -

invariant.

En fait: $\chi(\Theta_s)$ s'identifie au sous-groupe de $\bar{k}^\times$ engendré par les valeurs propres λ_i de s à λ val. propre correspond

$\chi_\lambda \in \chi(\Theta_s)$ tel que $\chi_\lambda(s) = \lambda$. On a

$$\chi(\rho) = \sum_{\lambda} \chi_\lambda n_\lambda$$

Si T_S est le tore maximal de E_S , on a

$$\begin{aligned} X(T_S) &= X(E_S) / X(E_S)_{\text{tors.}} \\ &= (\text{car. alg. par ex. val. p-prim.}) / (\text{racines de l'unité qu'il contient}) \end{aligned}$$

Soit A une variété abélienne de dim n / $\mathbb{F}_q$.
 À l'endom. de Frobenius π de A on associe comme
 ce-dessus Θ_π et T_π . Comme ces groupes alg. ne
 dépendent que des polynômes caractéristiques de π ,
 ils peuvent être définis sur $\mathbb{Q}$.

Autre solution: $\mathbb{Q}[\pi] \subset \mathbb{Q} \otimes \text{End } A$. La gauche mult.
 de $\mathbb{Q}[\pi]$ est représentée par un tore $T_{\mathbb{Q}[\pi]}$ et E_π 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 , $V_0 \otimes \mathbb{Q}_l \cong V_l$ comme $\mathbb{Q}_l[\pi]$ -module
 (et q variable)

Théorème 1 Pour n donné, il n'existe qu'un nombre
 fini de (T_π, E_π) dans GL_N , à conjugaison géomé-
 trique près.

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

Démonstration

1^{er} pas: il existe une borne ne dépendant que de
 n à $(\Theta_\pi = T_\pi)$: en effet le dual de ce groupe est
 l'ensemble des racines de 1 contenu dans le corps
 sup. par $\mathbb{Q}_0$ λ : le corps est de degré borné ($\leq n$!).

Ce qui implique que l'ordre $(G_n = T_n)$ est borné.

On suppose $n \geq 1$. Alors G_n est contenue dans T_n (remarque de Deligne vue dans un cas précédent). Il correspond par dualité à un homomorphisme $X(G_n) \rightarrow \mathbb{Z}$ qui à chaque λ associe 1: cet homomorphisme est $\lambda \mapsto 2 \frac{\log |\lambda|}{\log q}$.

On a d'autre part un homomorphisme canonique $G_n \rightarrow G_{n-1}$ qui à π associe q . Le composé $G_n \rightarrow G_{n-1} \rightarrow G_n$ est l'élévation au carré.

On a $G_n \subset$ tore maximal de Sp_{2n}
 Ce tore est $\{ \text{diag}(x_1, \dots, x_n, y_1, \dots, y_n) / x_1 y_1 = x_2 y_2 = \dots = x_n y_n = 1 \}$

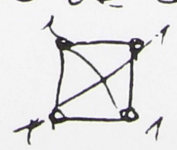
L'homomorphisme $G_n \rightarrow G_{n-1}$ est induit par $(x_1, \dots, x_n, y_1, \dots, y_n) \mapsto x_1, y_1$.

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

- 1) $x_1 = x_2 = y_2 = y_1$ (c'est le cas si $A = E \times E$ avec E hyper-singulière)
- 2) $x_1 = x_2, y_2 = y_1$ (c'est le cas si $A = E \times E$ avec E ordinaire)
- 3) $x_2 = y_2$ (toujours 2) (c'est le cas si $A = E \times E'$ avec E hyper-singulière et E' ordinaire)

- 4) tore maximal: pas de relations autres que

$$x_1 y_1 = x_2 y_2$$



On va utiliser les renseignements p -adiques
sur π (et le fait que les valeurs propres sont des unités
 l -adiques pour $l \neq p$).

Soit $X \in \overline{\mathbb{Q}}^*$ le n -qm. eng. par les valeurs propres
de π et π^{-1} place ult. de $\overline{\mathbb{Q}}$ prolongeant la
valuation p -adique de $\mathbb{Q}$. Les λ_i sont conjugués
par 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 $X \rightarrow \mathbb{Z}$. Or $\lambda \mapsto \frac{v_p(\lambda)}{v(q)}$ est
un homomorphisme continu de X dans $\mathbb{Q}$. Il existe
 $\delta \geq 1$ entier tel que $\varphi_\delta(X) \subset \frac{1}{\delta} \mathbb{Z}$, d'où $\delta \varphi_\delta(X) \subset \mathbb{Z}$.
Alors $\delta \varphi_\delta$ correspond à un groupe à un paramètre
de T , dont l'image ne dépend pas de δ .
(La remarque de Deligne réinterprète le groupe
à un paramètre des caractères de façon ana-
logue à partir de la valeur absolue archimédienne).

Si $\frac{v(\lambda_i)}{v(q)} = \varepsilon_i$, le groupe à un paramètre est
 $\{ \text{diag}(\lambda^{\delta \varepsilon_1}, \dots, \lambda^{\delta \varepsilon_n}) \} = \{ \text{diag}(\lambda^{\varepsilon_1}, \dots, \lambda^{\varepsilon_n}) \}$.

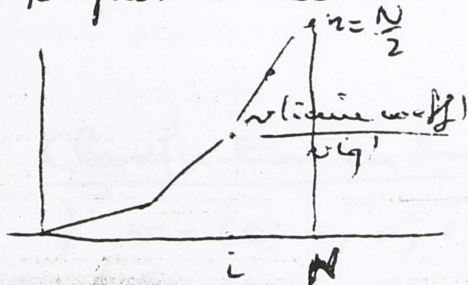
Lemme: pour n fixé, les ε_i ne prennent qu'un
nombre fini de valeurs: on a $0 \leq \varepsilon_i \leq 1$ et
le dénominateur des ε_i est $\leq N = 2n$.

Lemme 2: Les sous-groupes à un paramètre associés aux différents places v dépendent de T_{π} .

Ces lemmes impliquent le th. 1.

Dém du Lemme 2: L'intersection du noyau de 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 $v | p$. D'autre part toutes les valeurs absolues ℓ -adiques de λ sont les mêmes. La formule du produit entraîne alors que $|\lambda| = 1$ pour toute valeur absolue de $\bar{\mathbb{Q}}$, donc que λ est une racine de l'unité.

Les ε_i sont les pentes du polygone de Newton du polynôme caractéristique de Frobenius inversé $\prod_{i=1}^N (1 - \lambda_i X)$.

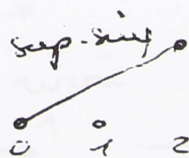


On a $\varepsilon_i \geq 0$ car λ_i est un.

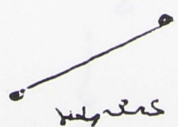
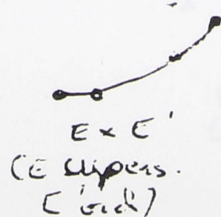
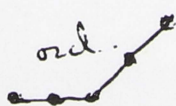
$\varepsilon_i \leq 1$ car $v(\lambda_i) + v(\bar{\lambda}_i) = 1$.

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 due au fait que $v(\lambda_i) + v(\bar{\lambda}_i) = 1$)

la th  orie est vraie pour les repr  sentations
l-adiques $\mathrm{H}^i(V \otimes \overline{\mathbb{F}_q}, \mathbb{Q}_\ell)$ avec V projective
lisse sur $\mathbb{F}_q$ (mais $\varepsilon_i \leq 1$ est remplac   par $\varepsilon_i \leq f$)

Le groupe p-divisible attach      la vari  t  
d  finition se d  compose en morceaux irr  ductibles
index  s par (r,s) premiers entre eux avec pour
pente $\frac{r}{r+s}$ et multiplicit   $r+s$.

Corollaire : Si d est le d  nominateur d'un $\varepsilon = \frac{v(p_i)}{v(q)}$
le nombre de p_i qui donnent ε est divisible par d .

Ex: $n=3$

0	0	0	1	1	1
0	0	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	1
0	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	1
$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$
$\frac{1}{3}$	$\frac{1}{3}$	$\frac{1}{3}$	$\frac{2}{3}$	$\frac{2}{3}$	$\frac{2}{3}$

seules imp
seules paires

Classification en dim 3, $\varphi_v: X \rightarrow \mathbb{Q}$ unique.

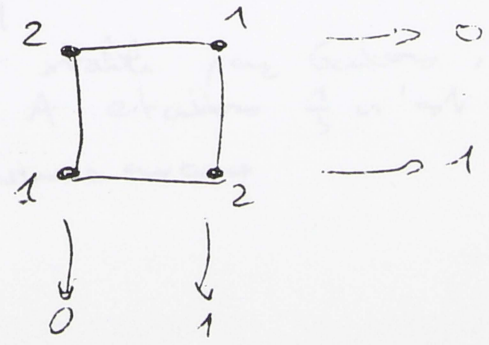
1) $v = (0, 0, 0, 1, 1, 1)$

Si l'espace affine est aff. par les ~~points~~ ~~points~~ ~~points~~

de dim 1 on doit avoir



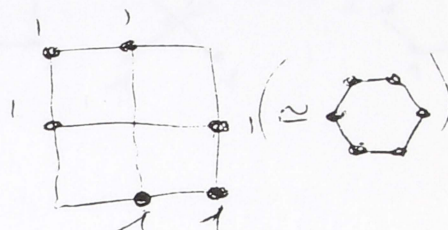
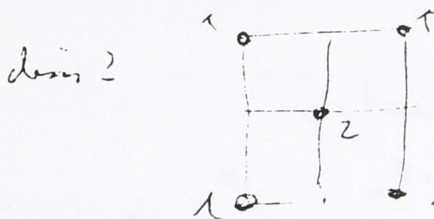
de dim 2 on doit avoir



dim 3

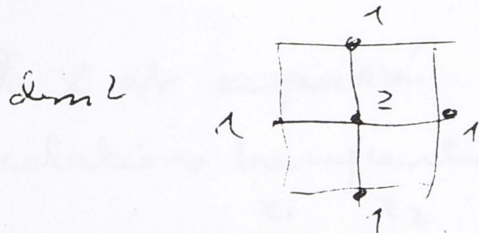


2) $v = (0, 0, \frac{1}{2}, \frac{1}{2}, 1, 1)$



dim 3 comme avant.

3) $v = (0, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}, 1)$

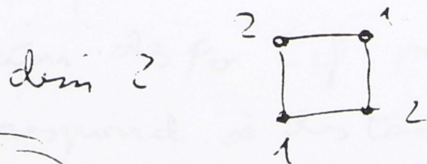


dim 3 comme avant

4) $v = (\frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2})$

6

5) $\frac{1}{3}, \frac{1}{3}, \frac{1}{3}, \frac{2}{3}, \frac{2}{3}, \frac{2}{3}$



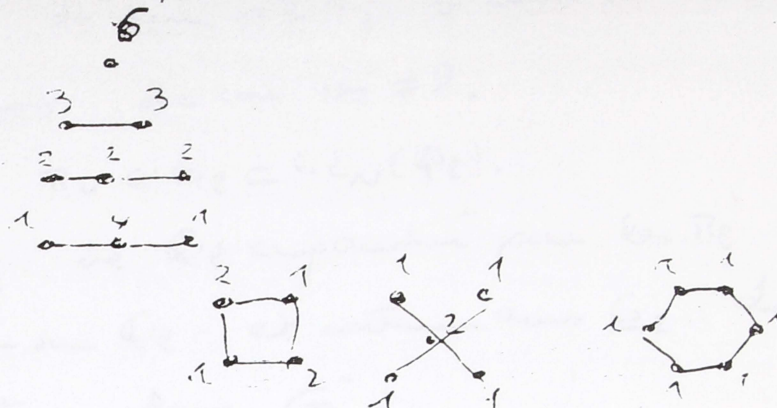
Ceci est impossible car



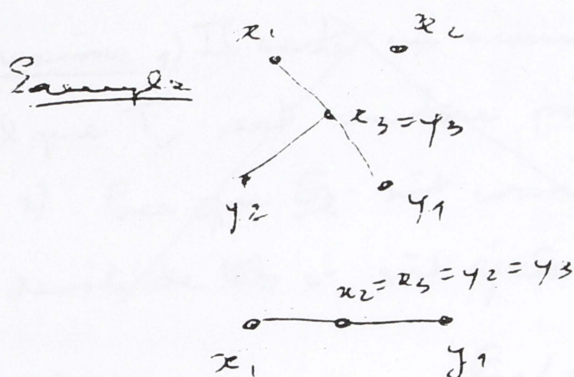
ne peut être par Galois, ce qui décompose
A et alors $\frac{1}{3}$ n'est plus possible.

dim 3 comme avant

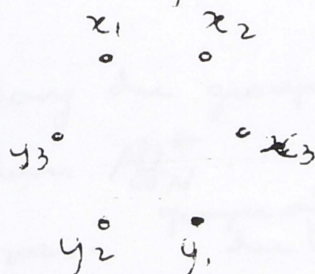
Conclusion: 8 possibilités pour la tore et sa représentation



octaèdre



Le X est engendré par les sommets soumis aux relations barycentriques:



$$x_3/y_3 = (x_2/x_1)^2 \text{ est l'éq. du tore.}$$

Remarque: le degré n'entraîne pas la détermination des p_i (cf. par exemple l'octaèdre qui correspond à des tors de possibilité)

Soit A une ab/K de dim $n \geq 1$, v une place de K à bonne réduction, de con. $v \neq 0$.

π_v le Frobenius, $\pi_v \in G_v \subset GL_N(\mathbb{F}_v)$.

Le sous- q -alg. de G_v engendré par les π_v est G_{π_v} , défini sur $\mathbb{F}_v$ et contenu dans G_v . La tore T_{π_v} est contenu dans G_v .

Théorème 1) Il existe un ensemble de places v de densité > 0 tel que T_v soit une tore maximal de G_v .

2) Pour que G_v soit connexe, il faut et il suffit que la densité de tels v soit égale à 1.

En fait: Si $c = \frac{1}{c}$ (de G_v/G_v^0). La densité des v tels

que $G_v = T_v$ et que T_v soit une tore maximal de G_v est $\frac{1}{c}$.

Soit n le rang du groupe G_v . Notons d l'application de G_v dans Aff_n^* .

Soit $\Lambda = \sum$ sous-^{groupes alg.} du tore standard qui sont géom. conjugués à un Θ de Frobenius de dimension $< n$. Ces tores sont en nombre fini. Si $\Theta \in \Lambda$, $d(\Theta) \subset \text{Aff}_n^*$ est de dimension $< n$.

Considérons M la sous variété de G_v^0 , définie sur $\mathbb{F}_v$ réunion

de ~~des éléments non réguliers (réguliers~~ ^{ou} ~~signifiant que le centralisateur est une tore maximal)~~

et des Θ dont l'image par d appartient à l'un des $d(\Theta)$.

Corrections et compléments

a) Si ρ_1, ρ_2 sont deux représentations de G dans une ^{sur les alg. alg. lin} n -alg. lin. sur $\mathbb{C}$, on symétrise ρ_1 et ρ_2 et ρ_1, ρ_2 sont conjuguées dans $G_{\mathbb{C}}$, elles G sont dans $O_n(\mathbb{C})$ (resp. Sp_n)

(si n impair, on a avec SO_n
 n pair, pour SO_n)

J Tits, exposé Bblu, 1955)

b) Dans le dernier cours, inutile de parler d'éléments réguliers

c) Le th. énoncé G (on passe à $G_{\mathbb{C}}$ (peut-être) $G_{\mathbb{C}}$ correct:

Énoncé correct : $\{v / T_v = O_v \text{ et } T_v, \text{ la torse}$
 maximal de $G_v^0\}$ est de densité $\frac{1}{c}$ où $c = [G_{\mathbb{C}} : G_{\mathbb{C}}^0]$

En particulier $G_{\mathbb{C}}$ connexe $\Leftrightarrow$ cet ensemble est de densité 1.

Application

Il existe une infinité de v (densité > 0) tels que G_v^0 soit déployé

Dém. Choisissons v tel que T_v soit de dimension $\neq 0$ au rang de G_v^0 . Alors T_v/O_v est une torse maximal de G_v^0 . Or le torse maximal est définissable sur $\mathbb{Q}$ et un tel torse est déployé sur une v de place de densité > 0 (celles décomposées dans la représentation galoisienne sur les caractères).

Rappel sur les courbes elliptiques :

1) Pas de CM : $\underline{G}_\ell = \underline{G}_\ell^\circ = GL_2/\mathbb{Q}_\ell$

$$T_{\Pi_v} \subset \mathbb{Q}_{\Pi_v}^\times$$

a) v ordinaire : $T_{\Pi_v} = \mathbb{Q}_{\Pi_v}^\times =$ torse maximal "groupe multiplicatif des corps quad. imaginaires $\mathbb{Q}(\text{Frob}_v)$ ".

(*) Il y a une infinité de $\mathbb{Q}(\text{Frob}_v)$ et Lang-Trotter conjecturent que tout corps quadratique imaginaire intervient pour une infinité de v .

b) v supersingulière : $T_{\Pi_v} = G_m$. On ignore s'il y a une infinité de v supersingulières, et ce pour toute courbe. On conjecture qu'il y en a une infinité.

2) type CM, défini sur K . Alors $\underline{G}_\ell = \underline{G}_\ell^\circ$ est le gr. mult. du corps de mult. complexe

3) type CM, non défini sur K . Alors $[G_\ell : G_\ell^\circ] = 2$ et G_ℓ° est comme dans le cas 2).

Dans un groupe réductif M sur $\mathbb{Q}_\ell$ il n'y a qu'un nombre fini de torse maximaux modulo conjugaison par $M(\mathbb{Q}_\ell)$.

Prop: Soient $\ell_1, \dots, \ell_k$ nbres premiers distincts, $T_{\ell_1}, \dots, T_{\ell_k}$ des torse maximaux de $\underline{G}_{\ell_1}^\circ, \dots, \underline{G}_{\ell_k}^\circ$. Alors il y a une infinité de v (dans > 0) telles que $\mathbb{Q}_v/\ell_i$ soit un tore conjugué de T_i .

(exemple : cas de GL_2 le comportement en ℓ de $\mathbb{Q}(\text{Frob}_v)$ peut être interprété pour un nombre fini de ℓ , d'où (*))

Dem Soit T une tore de E . Soit $x \in T(\mathbb{Q}_\ell)$.
 La réunion des conjugués de x par $G_\ell(\mathbb{Q}_\ell)$ est
 tout un voisinage (analytique) de x .

Prenez x assez proche de 1 pour que x
 appartienne à $T(\mathbb{Q}_\ell) \cap G_\ell$ et choisissons $\bar{v}$
 régulier. Choisissons un $\bar{v}$ qui donne une tore
 maximal et tel que $\pi_{\bar{v}}$ tombe dans ce voisinage.

Exercice 1) Soit $G \subset GL_n(\mathbb{Z}_\ell)$ tel que

$\{x \equiv 1 \pmod{\ell} \mid x \in G\}$ pour tout $x \in G$, l'anneau
 $\{x \equiv 1 \pmod{\ell^2} \mid x \in G\}$

algébrique de G dans GL_n est non vide.

2) Si A est une variété algébrique dont les points
 ont une dimension (pour un $n \geq 3$) pour tout K , alors
 les G_K ont une image non triviale.

Classification des tores de Frobenius

Soit A une

variété algébrique de G_ℓ . L'anneau de endomorphismes

de A est un $\mathbb{Q}_\ell$ -espace vectoriel de dimension n .

Chaque élément de A agit sur l'espace de symétrie

(dans $\frac{1}{2}X$), on note ω cette symétrie. On

a $\omega^2 = 1$ et ω est l'unique élément de A qui agit comme -1 sur l'espace de symétrie.

Il existe une infinité de v tel que la tore
 donne une isomorphisme avec la tore T_v .

On en déduit :

- 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 $\varphi: X \rightarrow \mathbb{Q}$ (associée à une place de $\bar{\mathbb{Q}}$ au dessus de la caract. résiduelle) avec :

- (b1) Les valeurs de φ sur les poids Σ sont dans $[0, 1]$
- (b2) Les conjugués de φ par Σ engendrent le dual de X , autrement dit $\bigcap_{\sigma \in \Sigma} \ker(\varphi^\sigma) = \{0\}$
- (b3) Si C est une orbite de Σ dans l'ensemble des poids et si $\frac{a}{b} \in \mathbb{Q}$, avec $\text{pgcd}(a, b) = 1$, le nombre des poids $w \in C$ avec $\varphi(w) = \frac{a}{b}$ est divisible par b .

Les propriétés (b1), (b2), (b3) sont valables sur les corps de nombres et de p -ad. La suivante n'est valable que pour les corps de nombres :

- (b4) Dans toute orbite C de Σ il existe au moins un w tel que $\varphi(w) = 0$.

Dém de (b4) : On peut supposer que la place v utilisée est de degré 1 (ie N est un nombre premier), et N 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 sous-ensemble de valeurs propres, stable par $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. Alors

$$v\left(\sum_{\lambda \in C} \lambda_i\right) > 0 \quad \text{et} \quad \sum_{\lambda \in C} \lambda_i > 0 \text{ un certain}$$

Mais $|\sum_{i \in C} \lambda_i| \leq 2n\sqrt{p}$ et $p > 4n^2$, on a donc $\sum_{i \in C} \lambda_i = 0$. 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 cas possibles, lorsque $\text{End}_{\mathbb{K}} A = \mathbb{C}$ et $\dim A \leq 10$

$\mathcal{G}_\ell^\circ = G_n S$ avec S abst irréductible.

On veut la classification (sur $\mathbb{C}$) des S irréductibles dans Sp_{2n} .

On est amené à regarder les reps. 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 reps. orthogonales ^{en dim} et symplectiques en $\dim \leq 20$ des groupes simples.

La formule de H. Weyl donne le degré d'une rep. en termes du poids dominant

$$\omega = a_1 \omega_1 + \dots + a_n \omega_n \quad \begin{array}{l} (a_i \geq 0 \\ \omega_i \text{ poids fond.} \\ \text{le rang du groupe}) \end{array}$$

$\dim V_\omega$ est une fonction de $\mathbb{N}$ linéaire en ω

$\Sigma x: A_1, SL_2, a_1 \omega_1, \text{rep} = \text{Sym}^{a_1}(V_2)$

$\dim = a_1 + 1.$

$A_2, SL_3, a_1 \omega_1 + a_2 \omega_2$

$\dim = (1+a_1)(1+a_2)(1 + \frac{a_1+a_2}{2})$

(on écrit $\prod_{\lambda: \text{racine} \geq 0} (1 + \frac{\sum \lambda_i a_i}{\sum \lambda_i})$
 $n = \sum \lambda_i a_i$ du syst. dual

$G_2 \quad \omega_1 \quad \omega_2 \quad \dim = (1+a_1)(1+a_2)(1 + \frac{a_1+a_2}{2})$
 $\downarrow \quad \downarrow$
 $\gamma \quad \frac{1}{14}$
 $(1 + \frac{a_1+2a_2}{3})(1 + \frac{a_1+3a_2}{4})(1 + \frac{2a_1+3a_2}{5})$

N

A de dim 1 2	A_1	SL_2	standard		oui
A de dim 2 4	A_4	$\text{Sym}^3(\text{standard})$	impossible		non
	C_2	Sp^4			oui
3 6	$A_1 \times A_1$	Standard $\otimes$ $\text{Sym}^2(\text{St.})$	$\begin{smallmatrix} 2 \\ 3 \end{smallmatrix} \times \begin{smallmatrix} 1 \\ 1 \end{smallmatrix}$		non
	A_1	Sym^5	non		
	C_3	Sp_6	<u>oui</u>		

Preuve du "non" pour $A_1 \times A_2$

$\begin{matrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{matrix}$

(2,5) n'est pas une orbite sous Σ

ϕ n'est donc ni horizontal, ni vertical

$\phi(2) \neq \phi(5)$. Par ex. $\phi(2)=0$. Pas alors

$\phi(1)=\phi(3)=0$, ϕ horizontal . Absurde .

Conclusion. En dim 1, 2, 3, $\text{End}_{\bar{k}} A = \mathbb{Q} \Rightarrow G_{\mathbb{Q}}^0 = G_m \times \mu_{24}$

$$\dim A = 4$$

A_1 non

C_4 oui

$$A_1 \times A_1 \times A_1$$

$$(\text{std})^{\otimes 3}$$



possible pour un corps de nombres

(géométriquement)

Mumford, Math Ann (≈ 1968), "Remarque sur un article de Shimura": il existe une famille de v. ab. dont le nombre générique a un gr. de Mumford Tate du type $A_1 \times A_1 \times A_1$. Par un thm de Deligne, Gal. est contenu dans ce groupe (cycles de Hodge absolus).
 Vu la liste, cette condition est satisfaite.

Si $l_1, \dots, l_g$ sont donnés, il existe une infinité de spécialisations de A sur lesquels les $G_{\mathbb{Q}_l}$ 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. invariants	Description
[2]	A_1	ω_1	-	SL_2 dans sa rep. standard
[3]	A_1	$2\omega_1$	+	" " " Sym^2 (standard)
	$\begin{cases} A_2 \\ A_2 \end{cases}$	ω_1 ω_2	o o	rep. standard de SL_3 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)
	$\begin{cases} A_3 \\ A_3 \end{cases}$	ω_2 ω_3	o o	SL_4 dans sa rep. standard duale de la précédente
[5]	A_1	$4\omega_1$	+	Sym^4 (standard)
	B_2	ω_1	+	repr. standard de SO_5
	$\begin{cases} A_4 \\ A_4 \end{cases}$	ω_1 ω_4	o o	repr. standard de SL_5 duale de la précédente
[6]	A_1	$5\omega_1$	-	Sym^5 (standard)
	$\begin{cases} A_2 \\ A_2 \end{cases}$	$2\omega_1$ $2\omega_2$	o o	Sym^2 (standard) (de SL_3) duale de la précédente
	$A_3 (= D_3)$	ω_2	+	Λ^2 (standard de SL_4) $\cong$ standard de SO_6
	C_3	ω_1	-	standard de Sp_6
	$\begin{cases} A_5 \\ A_5 \end{cases}$	ω_1 ω_5	o o	standard de SL_6 duale de la précédente

... /

Formes bilin. invariants :

91

o

(pas de forme $\neq 0$)

+

(formes sym. inv. $\neq 0$)

-

(formes alternées inv. $\neq 0$)

Représentations irréductibles de bas degré des groupes simples (suite)

Dimension	Type	Poids dominant	Formes bilin. inv.	Description
<u>7</u>	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	o	repr. standard de SL_7
	A_6	ω_6	o	duale de la précédente
<u>8</u>	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 $\tilde{SO}_7$
	C_4	ω_1	—	repr. standard de Sp_8
	D_4	ω_1	+	repr. standard de SO_8
	D_4	ω_3	+	repr. semi-spinorielle de $\tilde{SO}_8$
	D_4	ω_4	+	deuxième repr. semi-spinorielle
	A_7	ω_1	o	repr. standard de SL_8
	A_7	ω_7	o	duale de la précédente
<u>9</u>	A_1	$8\omega_1$	+	Sym^8 (standard)
	B_4	ω_1	+	repr. standard de SO_9
	A_8	ω_1	o	repr. standard de SL_9
	A_8	ω_8	o	duale de la précédente
<u>10</u>	A_1	$9\omega_1$	—	Sym^9 (standard)
	A_2	$3\omega_1$	o	Sym^3 (standard de SL_3)
	A_2	$3\omega_2$	o	duale de la précédente
	B_2	$2\omega_2$	+	repr. adjointe
	A_3	$2\omega_1$	o	Sym^2 (standard)
	A_3	$2\omega_3$	o	duale de la précédente
	A_4	ω_2	o	Λ^2 (standard)
	A_4	ω_3	o	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	o	repr. standard de SL_{10}
	A_9	ω_9	o	duale de la précédente

Représentations irréductibles symplectiques de degrés ≤ 20 des groupes semi-simples

1) Pour chaque dimension $2d$, A_1 dans sa rep. Sym^{2d-1} (standard).

Impossible pour une var. algébrique dès que $d \geq 2$. Prio: $\circ \circ \circ \dots \rightarrow \circ$

2) Pour chaque dimension $2d$, $C_d = \text{Sp}_{2d}$ dans sa rep. standard

Possible (au moins sur les corps de nombres). Prio *

3) Autres cas:

Dimension	Alg. de Lie	Description	Prio	Possibilité pour une v.a.
<u>6</u>	$A_1 \times A_1$	$\text{St}_2 \otimes \text{Sym}_3^2(\text{St})$		non
<u>8</u>	$A_1 \times A_1 \times A_1$	$\text{St}_2 \otimes \text{St}_2 \otimes \text{St}_2$ $2 \times 2 \times 2$		<u>oui</u> (corps de nombres)
<u>10</u>	$A_1 \times A_1$	$\text{St}_2 \otimes \text{Sym}_5^4 \text{St}$		non
	$A_1 \times B_2$	$\text{St}_2 \otimes \text{St}_5$		non
<u>12</u>	$A_1 \times D_3$	$\text{St}_2 \otimes \text{St}_6$		non (corps de nombres)
	$A_1 \times A_1$	$\text{Sym}_3^2(\text{St}) \otimes \text{Sym}_4^3(\text{St})$ 3×4		non
	$A_1 \times C_2$	$\text{Sym}_3^2(\text{St}) \otimes \text{St}_4$ 3×4		non
<u>14</u>	$A_1 \times A_1$	$\text{St}_2 \otimes \text{Sym}_7^6 \text{St}$		non
	$A_1 \times G_2$	$\text{St}_2 \otimes \text{rep. } \omega_1$ 2×7		non
	$A_1 \times B_3$	$\text{St}_2 \otimes \text{St}_7$		non
	C_3	rep. de poids ω_3 ($R^3 - A$)		non (corps de nombres)
<u>16</u>	C_2	rep. de poids $\omega_1 + \omega_2$		non
	$A_1 \times A_2$	$\text{St}_2 \otimes \text{Adjointe}_8$		non
	$A_1 \times B_3$	$\text{St}_2 \otimes \text{Spinorielle}_8$	Sommets d'un cube = 4 dim.	? (prob: non)
	$A_1 \times C_4$	$\text{St}_2 \otimes \text{Standard}_8$		non (corps de nombres)
	$A_1 \times A_1 \times A_1$	$\text{St}_2 \otimes \text{St}_2 \otimes \text{Sym}_4^3 \text{St}$ $2 \times 2 \times 4$		non
	$A_1 \times A_1 \times C_2$	$\text{St}_2 \otimes \text{St}_2 \otimes \text{Stand}_4$ $2 \times 2 \times 4$	Sommets d'un cube = 4 dim.	? (prob: non)

Rep. Symplectiques (Suite)

Dimension	Type	Description	Pois	Possibilité pour une v.a.
18	$A_1 \times A_1$	$St_2 \otimes Sym_3^8(St)$		non
	$A_1 \times B_4$	$St_2 \otimes St_9$		non
	$A_1 \times A_1 \times A_1$	$St_2 \otimes Sym_3^2(St) \otimes Sym_3^2(St)$		non
20	A_5	$\omega_3 : Sym^3(St)$		oui)
	C_2	fois 3 ω_1		non
	$A_1 \times A_1$	$Sym_4^3(St) \otimes Sym_5^4(St)$		non
	$A_1 \times B_2$	$St_2 \otimes Adjointe$		non
	$A_1 \times B_2$	$Sym_4^3(St) \times St_5$		non
	$A_2 \times D_5$	$St_2 \otimes St_{10}$		non (corps de nombres)
	$A_1 \times C_2$	$Sym_5^4(St) \otimes St_4$		non
	$B_2 \times C_2$	$St_5 \otimes St_4$		non
				..

Serre (l'ours n°10)

On suppose que K est un corps de nombres
(géométriquement)

G contient une tore "de type H ", i.e. il existe une
décomposition $V_2 = V_1 \oplus V_2$ avec $H \cong G_m \times G_m$ agissant par λ
sur V_1 et μ sur V_2

Envisageons $G_2 = G_m S$ avec S semi-simple. La représen-
tation V_2 de S est alors irréductible symplectique, et
 S contient (géométriquement) une tore du type $\begin{pmatrix} \lambda & & 0 \\ & \lambda^{-1} & \\ 0 & & \lambda^{-1} \end{pmatrix}$

On veut donc les repr. irréd. d'un groupe
semi-simple cont. une tore de dim 1 ayant 2 poids
et 2 seulement dans la représentation.

Si $V = V_1 \oplus \dots \oplus V_\ell$ avec V_i repr. irréd. de G_i presque
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 95 $\begin{pmatrix} \lambda & & 0 \\ & \lambda^{-1} & \\ & & \lambda^{-1} \end{pmatrix}$ avec $i+j=\ell+1$
et $ia=jb$

$\Lambda^l E$ ($2 \leq l \leq h-2$) avec le rep. à un paramètre $\begin{pmatrix} \lambda & & & 0 \\ & \lambda^{-1} & & \\ & & \ddots & \\ 0 & & & \lambda^{-1} \end{pmatrix}$

2. Type (Be) SO_{2l+1}

Représ. spinorielle de Be , de dim 2^l
à l'intérieur de SO_{2l+1} Le gr. à un param est $\begin{pmatrix} \lambda & & & 0 \\ & \lambda^{-1} & & \\ & & \ddots & \\ 0 & & & \lambda^{-1} \end{pmatrix}$; dans la repr. spinorielle, il n'a que deux p. La repr. ainsi obtenue est symplectique si et seulement si $l \equiv 1, 2 \pmod{4}$.

3. Type Ce Sp_{2l}

représentation standard de dim $2l$ avec $\begin{pmatrix} \lambda & & & 0 \\ & \lambda^{-1} & & \\ & & \ddots & \\ 0 & & & \lambda^{-1} \end{pmatrix}$

4. Type De $\widetilde{SO}_{2l}$

a) Représ. standard de dim $2l$ avec $\begin{pmatrix} \lambda & & & 0 \\ & \lambda^{-1} & & \\ & & \ddots & \\ 0 & & & \lambda^{-1} \end{pmatrix}$
associé à une dé. tot isotrope
(repr. non symplectique)

b) Représentations semi-spinorielles de dim 2^{l-1}
Celle repr. est symplectique $\Leftrightarrow l \equiv 2 \pmod{4}$.

5. Groupes exceptionnels: rien

Démonstration

Soit $(\alpha_1, \dots, \alpha_l)$ une base du 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.} du syst. dual.

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 $\langle \omega_i, \alpha_j^\vee \rangle = \langle \tilde{\omega}_i, \alpha_j \rangle = \delta_{ij}$

Les repr. irréductibles sont classés par leur

plus haut poids $\omega = \sum k_i \omega_i$ ($k_i \in \mathbb{Z}$, $k_i \geq 0$.)

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 Le sous-groupe à un paramètre est, "à homothétie près" défini par un $\omega_j^\vee$ minuscule ($n_j = 1$) (en considérant $\omega_j^\vee$ comme appartenant à $\mathbb{Q} \otimes_{\mathbb{Z}} \text{Hom}(G_m, G)$).

Assertion 3: Bien que le couple $(\omega_i, \omega_j^\vee)$ soit acceptable, il faut et il suffit que

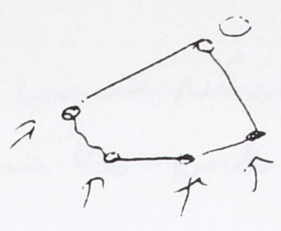
$$(\omega_i, \omega_j^\vee) + (\omega_{i'}, \omega_j^\vee) = 1$$

où $i \rightarrow i'$ est l'involution d'ordre 2 de la base choisie (l'involution standard est celle qui "correspond" à l'automorphisme -1 du syst. de racines).

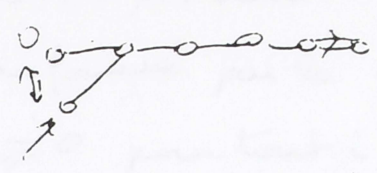
Cette involution est d'ordre 1 si $-1 \in W$ (ex. de U_{sp})
2 si $-1 \notin W$

On trouve les poids minuscules en regardant le diagramme affine. Réciproquement du syst. de racines dual et en regardant quels sommets sont transformés de 0 par un automorphisme du diagramme complet).

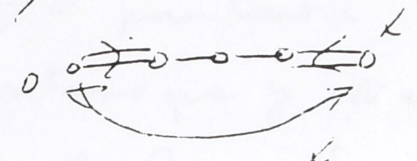
type A



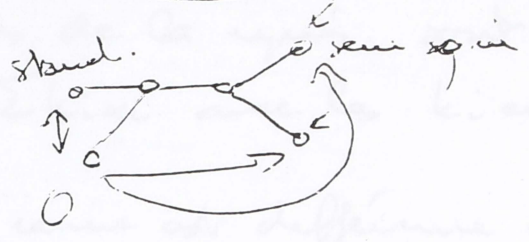
type B



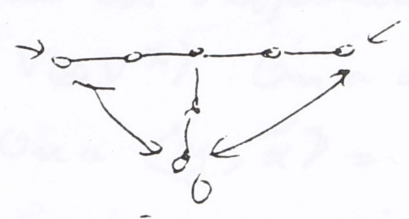
type C



type D



type E₆



Une représentation minuscule (Lie VII, § 7, c-3)
est caractérisée par chacune des cond. 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).

Démonstration l'assertion 1 : vecteur à deux poids est un él^{tr} y de $\mathbb{Q} \otimes Y(T)$ tel que $\{(\omega, y) / \omega$ poids de la repr^s $\}$ ait exactement deux éléments.

Si on avait une chaîne de longueur 3 dans les poids, elle serait orthogonale à y , soit 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 repr. ρ prennent sur y des valeurs λ, μ , avec $\lambda - \mu = 1$ et imaginons y par sa transformée par le groupe de Weyl de sorte que $\langle y, \alpha_i \rangle \geq 0$ pour tout i .

Montrons que y est un poids minuscule. Les poids de la repr. ρ sont de la forme $w - \sum k_i \alpha_i$ avec les k_i entiers ≥ 0 .

Toute racine est différence de deux poids (car $\mathfrak{g} \subset V \otimes V^*$). On a donc $\langle y, \alpha \rangle = \frac{1}{0}$ pour $\alpha \geq 0$. On a $\langle y, \tilde{\alpha} \rangle = 1$ ou 0 , d'où, si $\tilde{\alpha} = \sum m_i \alpha_i$, y poids minuscule associé à un i tel que $m_i = 1$. Ceci prouve l'assertion.

Le plus bas poids de la repr. de poids dominant w est $-w'$ avec ρ l'involution canonique.

Donc y est compatible avec w si et seulement si

$\langle y, w \rangle - \langle y, -w' \rangle = 1$. Ceci prouve l'ord. 3.

Théorème - Si $\dim A$ impair et $\text{End}_k A = \mathbb{C}$,
 $\mathcal{O}_\ell = \mathbb{C} \otimes \mathcal{P}_n / \mathcal{Q}_\ell$.

(Des arguments importants de la démon. ont été extraits d'un article de Ribet, Ann. of Math., 1983, qui cherchait à déterminer le groupe de Heckecke-Tate.)

(Ribet) des gr. seuls
Lemme : - Si une représentation symplectique est
 irréductible et de dimension $\neq 0 \pmod 4$, c'est la
 représentation standard d'un groupe symplectique.

A_l ($l \geq 2$): $\Lambda^i(\text{St}_{l+1})$ sympl $\Leftrightarrow i = \frac{l+1}{2}$ et l impair
 (si $i \neq \frac{l+1}{2}$, $(\Lambda^i)^* \simeq \Lambda^{l+1-i}$ n'est pas isom à Λ^i .
 si $i = \frac{l+1}{2}$, $\Lambda^i \otimes \Lambda^i \rightarrow \Lambda^{l+1}$ fournit une forme
 symplect. invariante).

$$\dim = \frac{\binom{l+1}{\frac{l+1}{2}}}{\binom{l+1}{2}}$$

Lemme : si N impair > 1 , $\binom{2N}{N} \equiv 0 \pmod 4$.

type B: dim 2^l

type C: Standard acceptée.

type D: standard (non sympl.)

semi-spl. 2^{l-1}

Soit $V_\ell(A) = V_\ell$. Géométriquement $V_\ell \simeq \bigotimes W_i$ avec
 les S agissant sur V_i suivant ρ_i (Lie $S \simeq \bigoplus \rho_i$)

Il existe, si $l = 2n$ avec n impair, un
 facteur et une seul de dim. paire et il y a un
 nombre impair de facteurs symplectiques. Il y a
 donc une seul facteur symplectique

On peut supposer que W_1 est symplectique et
 W_i orthogonal de dim. paire pour $i \geq 2$)

On doit avoir un tore de type M . Il ne peut 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.

^{Sur un corps de nombres}
Lemme. Si $\text{End}_K A = \mathbb{Z}$, il n'est pas possible que $V_{\mathbb{Q}}$ soit de la forme $W_1 \oplus W_2$ avec W_1 représentation minimale et 0 poids de W_2 (ce qui est le cas lorsque W_2 est orthogonal de dim impaire).

On utilise l'hypothèse "minimale".
 sous la forme "Le minimum de deux poids n'est pas un poids." d'où.

des poids est $\{(\lambda + \mu) / \lambda \text{ poids de } W_1, \mu \text{ poids de } W_2\}$

Sont $\Omega_1 = \{\text{poids de } W_1\}$

$\Omega_2 = \{ \text{ " " } W_2 \}$

Les poids du tore simple sont les éléments de $\Omega_1 \times \Omega_2$.

Ω_1 se plonge dans $\Omega_1 \times \Omega_2$ par $\lambda \rightarrow (\lambda, 0)$.

Lemme: tout automorphisme affine de $\Omega_1 \times \Omega_2$ laisse stable $(\Omega_1, \times 0)$.

En effet $\omega_1 + \omega_2 \in \Omega_1 \times \{0\}$

$$\Leftrightarrow \text{Ad}_{\rho_\omega}(\Omega_1 \times \Omega_2) \cap (\Omega_1 \times \Omega_2) = \{\Omega_2\}$$

si ρ_ω est la symétrie par rapport à 0.

Soit un tore de Frobenius associé à une place v telle que $Nv = p^2$ soit premier.
 d'ensemble des centres $\mathcal{N}_1 \times \mathcal{N}_2 = \mathcal{N}$ stable par $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. d'un des points de cet ensemble a donc valuation nulle. Donc φ_v s'annule sur $\alpha \times \mathcal{N}_2$, absurde.

Géométriquement, la représentation est la représentation standard de Sp_{2n} .

Comme $\mathbb{G}_m \subset \text{Sp}_{2n}/\mathbb{Q}_\ell$, c'est une représentation naturellement réelle.

Liste de problèmes

1) Galois = Mumford Tate?

($\Leftrightarrow$ ^{donc de} chronologie ℓ -adique invariants par Galois, à torsion de Tate p.s., provient des cycles de Hodge absolue, rapp. des cycles algébriques si l'on voit la conj. de Hodge).

2) Plus faible

don (invariants de Galois) dans des rep's. ℓ -adiques et ℓ' -adiques compatibles sont les in.

Si $G \subset G_\ell$ red. connexe et si l'on connaît la dim des invariants de G dans toutes les reps ℓ -ad. réelles, connaît-on G ?

- 3) Problèmes numériques : Donner des exemples de courbes dont les jacobiniens ont $\text{Gal} \cong \text{CS}_p$.
- 4) Montrer qu'il y a une infinité de places avec réduction ordinaire (et m. dans 1) si les groupes sont connexes).
- 5) Etc - a que G_L^0 est suspendue géométriquement par ses sous-tors de type H? (C'est une conséquence de 1)).
- 6) Montrer qu'aucun facteur géométrique de G_L^0 est de type exceptionnel
 (on peut aussi envisager de le faire avec les tors 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. $\text{Sym}^{2d-1}(St)$, where St = standard representation of degree 2. Weights: $\circ - \circ - \dots - \circ - \circ$.

This is impossible for an abelian variety as soon as $d \geq 2$.

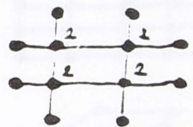
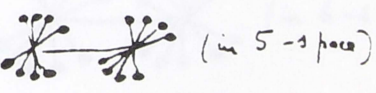
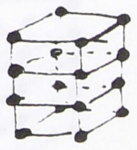
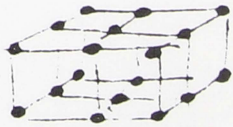
2) For each dimension $2d$, $C_d = Sp_{2d}$ in its standard representation. Weights (for $d=2$): $\circ \begin{smallmatrix} \nearrow \\ \searrow \end{smallmatrix} \circ$. This is possible for an ab. variety, over a number field.

3) Other cases:

Dimension	Group	Representation	Weights	Occurs for an abelian var. over a number field
<u>6</u>	$A_1 \times A_1$	$St_2 \otimes \text{Sym}_3^2 St_2$		no
<u>8</u>	$A_1 \times A_1 \times A_1$	$St_2 \otimes St_2 \otimes St_2$		yes (Mumford)
<u>10</u>	$A_1 \times A_1$	$St_2 \otimes \text{Sym}_5^4 St_2$		no
	$A_1 \times B_2$	$St_2 \otimes St_5$		no (in 3-spac)
<u>12</u>	$A_1 \times D_3$	$St_2 \otimes St_6$		no (in 4-spac)
	$A_1 \times A_1$	$\text{Sym}_3^2(St) \otimes \text{Sym}_4^2(St)$		no
	$A_1 \times C_2$	$\text{Sym}_3^2(St) \otimes St_4$		no
<u>14</u>	$A_1 \times A_1$	$St_2 \otimes \text{Sym}_7^6 St_2$		no

... / ...

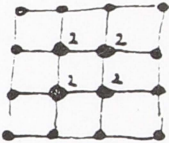
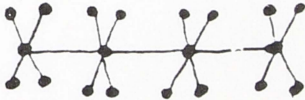
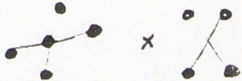
(St = standard representation)

Dimension	Group	Representation	Weight	Occurs for an abelian val. over a number field
[14] ctd...	$A_1 \times G_2$	$St \otimes Rep(w_1)$ 2 7		no
	$A_1 \times B_3$	$St \otimes St$ 2 7	 (in 4-space)	no
	C_3	$Rep(w_3) = \wedge^3 St - St$	 vertices of a cube + centers of faces	no
[15]	C_2	$Rep(w_1 + w_2)$		no
	$A_1 \times A_2$	$St \otimes Adj$ 2 8		no
	$A_1 \times B_3$	$St \otimes Spinor$ 2 8	vertices of a 4-dim. cube	? (probably no)
	$A_1 \times C_4$	$St \otimes St$ 2 8	 (in 5-space)	no
	$A_1 \times A_1 \times A_1$	$St \otimes St \otimes Sym^3 St$ 2 2 4		no
	$A_1 \times A_1 \times C_2$	$St \otimes St \otimes St$ 2 2 4	vertices of a 4-dim. cube	? (probably no)
[18]	$A_1 \times A_1$	$St \otimes Sym^8 St$ 2 9		no
	$A_1 \times B_4$	$St \otimes St$ 2 9	 (in 5-space)	no
	$A_1 \times A_1 \times A_1$	$St \otimes Sym^2(St) \otimes Sym^2(St)$ 2 3 3		no

... / ...

$Rep(w_1)$ = irred. representation with highest weight w_1 (Zorn's lemma notation)

Adj = adjoint representation

Dimension	Group	Representation	Weights	Occurs for an abelian variety on a number field
<u>20</u>	A_5	$\text{Rep}(\omega_3) = \Lambda^3(\text{St})$		yes
	C_2	$\text{Rep}(3\omega_1)$		no
	$A_1 \times A_1$	$\text{Sym}_4^3(\text{St}) \otimes \text{Sym}_5^4(\text{St})$		no
	$A_1 \times B_2$	$\text{St}_2 \otimes \text{Adj}_{10}$		no
	$A_1 \times B_2$	$\text{Sym}_4^3(\text{St}) \otimes \text{St}_5$	 (in 3-space)	no
	$A_1 \times D_5$	$\text{St}_2 \otimes \text{St}_{10}$	 (in 6-space)	no
	$A_1 \times C_2$	$\text{Sym}_5^4(\text{St}) \otimes \text{St}_4$		no
	$B_2 \times C_2$	$\text{St}_5 \otimes \text{St}_4$		no