

Tunnell, Fall '95

(II)

Situation

On est intéressé par les représentations $\rho: G_{\mathbb{Q}} \rightarrow \mathcal{O}^*$ et on suppose que lorsque ρ est réduite modulo m_0 , $\bar{\rho}$ ainsi obtenue est associée à un caractère de Dirichlet

$$x: G_{\mathbb{Q}} \rightarrow \mathcal{O}^*$$
$$\text{ie } \bar{\rho} = \bar{x}: G_{\mathbb{Q}} \rightarrow (\mathcal{O}/m_0)^*$$
$$\text{et } \text{Gal}(\mathbb{Q}(\mu_N)/\mathbb{Q}) \cong (\mathbb{Z}/(N))^*$$

But: sous certaines hypothèses sur ρ , montrer qu'il existe un caractère de Dirichlet x' tel que $x = x'$.

Remarque: on dit qu'un caractère de Dirichlet est de conducteur N si $x: (\mathbb{Z}/N\mathbb{Z})^* \rightarrow \mathcal{O}^*$ n'est pas un caractère de $(\mathbb{Z}/N'\mathbb{Z})^*$ pour un $N' | N$ et $N' \neq N$.

Soit $\bar{x}: (\mathbb{Z}/(N))^* \rightarrow \mathcal{O}^*$ la réduction de x et $N(\bar{x})$ le conducteur de \bar{x} .

Soit q premier tel que $\begin{cases} q \neq \text{choc}(\mathcal{O}/m_0) \\ q \nmid N(\bar{x}) \end{cases}$; q pourrait appartenir au 3^e conducteur de $x' \neq x$ tel que $\bar{x}' = \bar{x}$.

Fait: dans cette situation q divise $N(x')$ au plus à la puissance 1.

Dém: $x'x^{-1}$ vérifie $x'x^{-1} \pmod{m_0} = 1$.

Si $N' | x$ on a $(\mathbb{Z}/N\mathbb{Z})^* \rightarrow (\mathbb{Z}/N')^*$

"
 $\pi: (\mathbb{Z}/p^a\mathbb{Z})^*$

On a

$$(\mathbb{Z}/(N(x)))^\times \xrightarrow{x} 0^\times$$

et

$$(\mathbb{Z}/(q^j))^\times \prod_{p \neq q} (\mathbb{Z}/(p))^\times = (\mathbb{Z}/(N(x)))^\times \xrightarrow{\bar{x}} (\mathcal{O}/m_0)^\times$$

$$\downarrow$$

$$(\mathbb{Z}/(N(\bar{x})))^\times$$

et donc $x|(\mathbb{Z}/(q^j))^\times$ vérifie $x|(\mathbb{Z}/(q^j))^\times = 1 \pmod{m_0}$
 ce qui implique que $x|(\mathbb{Z}/(q^j))^\times$ est d'ordre une puissance de la caractéristique de \mathcal{O}/m_0 , ie $(q-1)q^{j-1}$ est une puissance de p . Il en découle que $j=1$ (sinon x devrait être trivial sur un q -groupe et le conducteur serait plus petit).

D)

Cela motive la classe de déformations suivantes que l'on va étudier.

On se donne $\bar{x}: (\mathbb{Z}/(N(\bar{x})))^\times \rightarrow (\mathcal{O}/m_0)^\times$, où \bar{x} est la réduction d'un caractère de Dirichlet x .

La donnée de déformation associée \mathfrak{D} est :

$$\mathfrak{D} = \left(\sum, p^j \right)$$

ensemble fini de
nombres premiers
tel que $p \in \Sigma$

une puissance de p

On dit qu'une déformation $\rho: G_\mathbb{Q} \rightarrow A^\times$ de \bar{x}

$$\bar{x} \mapsto \frac{1}{\bar{x}} \cdot \frac{x}{x - \rho(\bar{x})} = A_{\rho(\bar{x})}^\times$$

est de type \mathfrak{D} si

- (i) ρ est non-ramifiée en dehors de l'ensemble fini Σ
- (ii) $\rho|_{G_p}$ se factorise à travers $\text{Gal}(\mathbb{Q}_p(\mu_{p^j})/\mathbb{Q}_p)$

groupes de
décomposition
en $P = \text{Gal}(\mathbb{Q}_p/\mathbb{Q}_p)$

N.B. (ii) contrôle le niveau de $\rho|_{G_p}$, ie celui du x qui on cherche.

N.B. Un caractère de Dirichlet x' de conducteur $N(x')$ qui vérifie $x' \equiv \bar{x} \pmod{m_0}$ est de type \mathfrak{D} si et seulement si

$$N(x') \mid p^j N(\bar{x}) \prod_{q \in \Sigma \setminus \{p\}, q \nmid N(\bar{x})} q^1$$

partie première à p
du conducteur de \bar{x}

Dém: Supposons $\bar{x} \equiv x' \pmod{m_0}$; on a vu que si $q \nmid N(\bar{x})$, q apparaît dans $N(x')$ au plus à la puissance 1; de plus, x' de type \mathfrak{D} implique que q n'apparaît pas si $q \notin \Sigma$.

En \mathfrak{D} , si x' est de type \mathfrak{D} , par la condition (i) on a

$$x': \text{Gal}(\mathbb{Q}(\mu_{N(x')})/\mathbb{Q}) \longrightarrow 0^\times$$

\cup

$$(\mathbb{Z}/(p^k))^\times \times \dots$$

se factorise, après restriction à G_p , par $\text{Gal}(\mathbb{Q}_p(\mu_{p^j})/\mathbb{Q}_p)$ ie $k \leq j$.

Pour $q \nmid N(\bar{x})$, on vérifie par un petit calcul que x' ne peut pas être plus ramifié que \bar{x} ...

La preuve ... \Rightarrow

Quand $\sigma \leftarrow$, c'est à peu près évident.

□

N.B. "Type 2" ne mentionne pas un conducteur explicite, mais on a montré comment le limiter...

Pourquoi y-a-t-il une algèbre universelle pour les déformations de type 2? On regarde la construction et ça marche...

Proposition - Il existe une \mathcal{O} -algèbre locale complète noethérienne

R_D et une déformation $\rho_D: G_D \rightarrow R_D^\times$ telle que pour toute déformation $\rho: G_D \rightarrow A^\times$ de type 2 de \bar{x} , il existe $R_D \xrightarrow{\rho} A$ tel que le diagramme

$$\begin{array}{ccc} & R_D^\times & \\ \rho_D \swarrow & \downarrow \psi^\times & \\ G_D & \longrightarrow & A^\times \\ & \searrow & \\ & \bar{x} & \\ & \downarrow & \\ & R^\times & \end{array}$$

commute.

Notons T_D l'algèbre de déformation de Dirichlet de type 2 : par la remarque ci-dessus, c'est simplement l'algèbre $T_{N,m}$ vue la dernière fois.

Il existe alors une surjection de \mathcal{O} -algèbres

$$R_D \xrightarrow{\varphi} T_D \xrightarrow{\pi} \mathcal{O}$$

Objectif: montrer que φ est un isomorphisme, en veillant

$$\ell(O/\eta_{T_D})$$

que l'on peut appliquer le théorème de Wilmes-Lanstra: on doit montrer que $\ell(O/\eta_D) \geq \ell(I_{R_D}/I_{R_D}^2)$, et que les deux sont finis.

On a déjà calculé O/η_D précédemment.

Définition - Étant donné deux données de déformation $\mathcal{D} = (\Sigma, \rho)$ et $\mathcal{D}' = (\Sigma', \rho')$, on dit que $\mathcal{D}' \geq \mathcal{D}$ si et seulement si $\Sigma' \supset \Sigma$ et $\rho' = \rho$.

Proposition - (Etape de récurrence)

Supposons que la donnée \mathcal{D} vérifie

$$\ell(I_{R_D}/I_{R_D}^2) \leq \ell(O/\eta_D)$$

Alors pour toute donnée de déformation $\mathcal{D}' \geq \mathcal{D}$, on a aussi

$$\ell(I_{R_{\mathcal{D}'}}/I_{R_{\mathcal{D}'}}^2) \leq \ell(O/\eta_{\mathcal{D}'})$$

Dém. D'abord, de \mathcal{D} on a tiré le "conducteur maximal"

$$N = \prod_{q \in \Sigma - \{\rho\}} N_q(\bar{x}) \cdot p^\delta$$

et on sait que dans ce cas on a

$$\eta_D = |(\mathbb{Z}/(N))^\times| \cdot \mathcal{O}$$

de sorte que voici comment ça change à droite sera fait

Et par récurrence on peut supposer $\Sigma' = \Sigma \cup \{q\}$.

Il vient donc

$$\eta_{\mathcal{D}'} = |(\mathbb{Z}/(N))^\times| \cdot \mathcal{O}$$

on s'attend à ce que \mathcal{D}' soit deux fois ramifiée au niveau q et à Σ

$$\text{et } \eta_D = |(\mathbb{Z}/(Nq))^*| \circ \\ = (q-1) \eta_D \\ (= p^{v_p(q-1)} \eta_D)$$

car $q \nmid N$.

Reste la partie difficile...

$$\text{On veut comprendre } \Phi_D = I_{R_D}/I_{R_D}^2$$

$$\text{Considérons } R_D/I_{R_D}^2 \rightarrow R_D/I_{R_D} \rightarrow 0$$

||
0

d'où la suite exacte

$$(*) \quad 0 \rightarrow \Phi_D \rightarrow R_D/I_{R_D}^2 \rightarrow 0 \rightarrow 0$$

Lemme. Pour tout entier $k \geq 1$,

$$\text{Hom}_0(\Phi_D, \mathcal{O}_{m_0}^k) \cong \text{Hom}_D(G_\Sigma, \mathcal{O}_{m_0}^k)$$

où G_Σ est le groupe de Galois de l'extension abélienne maximale non-ramifiée en dehors de Σ et " Hom_0 " signifie l'ensemble des morphismes de groupe "de type 0" (ce qui sera expliqué plus loin).

Lemme suivant

Dém. (Lemme). Notons $p_D: G_Q \rightarrow R_D^\times$ la déformation universelle et $p_{D,2}: G_Q \rightarrow (R_D/I_{R_D}^2)^\times$ la réduction modulo $I_{R_D}^2$.

Considérons également $p_0: G_Q \rightarrow (R_D/I_{R_D}^2)^\times$

obtenue via $G_Q \rightarrow 0^\times \rightarrow (R_D/I_{R_D}^2)^\times$.
On regarde alors $p_{D,2} \circ p_0^{-1}$: cela donne en fait $p_{D,2} \circ p_0^{-1}: G_Q \rightarrow \Phi_D$ par définition.

Si donc on a $f: \Phi_D \rightarrow \mathcal{O}_{m_0}^k$, on déduit $\tilde{f}: G_Q \rightarrow \mathcal{O}_{m_0}^k$ et cela donne

$$\text{Hom}(\Phi_D, \mathcal{O}_{m_0}^k) \rightarrow \text{Hom}(G_Q, \mathcal{O}_{m_0}^k)$$

ou plutôt

$$\text{Hom}(\Phi_D, \mathcal{O}_{m_0}^k) \rightarrow \text{Hom}(G_\Sigma, \mathcal{O}_{m_0}^k)$$

et de "type 2" au sens évident.

$$\text{Hom}(\Phi_D, \mathcal{O}_{m_0}^k) \rightarrow \text{Hom}_D(G_\Sigma, \mathcal{O}_{m_0}^k)$$

On verra la prochaine fois que c'est effectivement un isomorphisme

o

Le lemme nous amène à étudier le "groupe de Selmer"

$$\text{Hom}_D(G_\Sigma, \mathcal{O}_{m_0}^k)$$

La proposition découlera de la composition entre

$$\text{Hom}_D(G_\Sigma, \mathcal{O}_{m_0}^k)$$

$$\text{et } \text{Hom}_D(G_\Sigma, \mathcal{O}_{m_0}^k)$$

On a déjà une flèche

$$0 \rightarrow \text{Hom}_D(G_\Sigma, \mathcal{O}_{m_0}^k) \rightarrow \text{Hom}_D(G_\Sigma, \mathcal{O}_{m_0}^k)$$

et on a de plus

$$\text{Hom}_D(G_\Sigma, \mathcal{O}_{m_0}^k) \rightarrow \bigoplus_q \text{Hom}(G_q, \mathcal{O}_{m_0}^k)$$

$$\bigoplus_q \text{Hom}(I_q, \mathcal{O}_{m_0}^k)$$

$$\begin{array}{ccc}
 0 \rightarrow \text{Hom}_{\mathcal{D}}(G_{\Sigma}, \mathcal{O}/m_0^k) & \rightarrow \text{Hom}_{\mathcal{D}}(G_{\Sigma}, \mathcal{O}/m_0) \\
 \downarrow & & \downarrow \\
 \oplus \text{Hom}(G_q, -) & \longrightarrow & \oplus \text{Hom}(G_q, -) \\
 \downarrow & & \downarrow \\
 \oplus \text{Hom}(I_q, -) & \longrightarrow & \oplus \text{Hom}(I_q, -) \\
 q \in \Sigma & & q \in \Sigma \\
 \Rightarrow & & \\
 0 \rightarrow \text{Hom}_{\mathcal{D}}(G_{\Sigma}, \mathcal{O}/m_0^k) & \rightarrow \text{Hom}_{\mathcal{D}}(G_{\Sigma}, \mathcal{O}/m_0^k) & \xrightarrow{\text{Res}} \text{Hom}(I_q, \mathcal{O}/m_0) \\
 & & \text{(extensions locales)}
 \end{array}$$

$\Sigma' = \Sigma \cup \{q'\}$

8/11/95

Rappel sur \mathcal{O} , anneau de valuation discrète de corps résiduel de caractéristique p .

$\mathcal{D} = (\Sigma, \rho^{\pm})$ donnée de déformation, Σ ensemble fini de nombres premiers.

- x : $G_{\mathcal{D}} \rightarrow \mathcal{O}^*$ caractère de Dirichlet
- $N(x) / p^{\pm} N(\bar{x})$
- \bar{x} : sa réduction

$R_{\mathcal{D}}$: l'algèbre de déformation de \bar{x} de type \mathcal{D}

$T_{\mathcal{D}}$: de \bar{x} pour caractères de Dirichlet de type \mathcal{D}

On a des flèches

$$R_{\mathcal{D}} \rightarrow T_{\mathcal{D}} \rightarrow 0$$

auxquelles on veut appliquer le théorème de Wieferichstra.

On note $\mathfrak{F}_{\mathcal{D}} = \mathfrak{F}_{R_{\mathcal{D}}}$.

Proposition: On a un isomorphisme naturel $\ell + \mathfrak{F}_{\mathcal{D}} = \ell$

$$\text{Hom}_{\mathcal{D}}(\mathfrak{F}_{\mathcal{D}}, \mathcal{O}/m_0^k) \xrightarrow{\sim} \text{Hom}_{\mathcal{D}}(G_{\mathcal{D}}, \mathcal{O}/m_0)$$

Avant de (re) prouver la proposition, rappelons qu'on veut contrôler $\ell(\mathfrak{F}_{\mathcal{D}})$; la proposition est le lemme ad-hoc dans cette situation:

Lemme: Soit \mathcal{O} un anneau de valuation discrète, M un \mathcal{O} -module de type fini. On peut écrire

$$M = \mathcal{O} \oplus \mathcal{O}/m_0 \oplus \dots \oplus \mathcal{O}/m_0^k \quad (*)$$

Alors on a

$$\text{Hom}(\mathcal{O}/m_0^k, M) \cong M/m_0^k M$$

Dém.: On vérifie pour si M cyclique

$$\begin{aligned}
 1^{\text{er}} \text{ cas: } M &= 0, \quad \text{Hom}_{\mathcal{O}}(0, \mathcal{O}/m_0^k) \cong \mathcal{O}/m_0^k, \text{ ce qu'on veut} \\
 2^{\text{e}} \text{ cas: } M &= \mathcal{O}/(a_1), \quad \text{Hom}_{\mathcal{O}}(\mathcal{O}/m_0^k, \mathcal{O}/m_0) \cong m_0^{k-\ell(a_1)} / m_0^k \\
 a_1 &= \mathcal{O}/m_0^k \\
 &= M/m_0^k M
 \end{aligned}$$

D'autre côté, on a

En particulier $\lim_{k \rightarrow \infty} \ell(\text{Hom}(\mathcal{O}/m_0^k, M)) = \ell(M)$ (car si M est de torsion, on a $M/m_0^k M = M$ pour k assez grand).

D'un autre côté, on a

$$\ell(\text{Hom}(\mathcal{O}/m_0^k, M)) = \ell(M/m_0^k M) = \text{nombre de facteurs cycliques de } M \text{ (cf. (*))}$$

Cela est intéressant pour notre situation car on peut écrire

$R = 0 + I_{\mathcal{D}}^{\text{loc}}$, et par le lemme de Nakayama, si $I_{\mathcal{D}}/I_{\mathcal{D}}^2 \subsetneq \mathcal{D}$ est engendré par ≤ 2 éléments, alors R est engendré comme \mathcal{O} -algèbre locale, par ≤ 2 éléments.

Démonstration de la proposition

1^e cas : $k = 1$

(On cherche $\text{Hom}_{\mathcal{O}}(\mathcal{D}, \mathcal{O}/m_0)$)

Par définition, on a $\text{Hom}_{\mathcal{O}}(\mathcal{D}, \mathcal{O}/m_0) = \text{Def}_{\mathcal{D}}(\bar{x}, \mathcal{A})$

$$\text{Def}_{\mathcal{D}}(\bar{x}, \mathcal{A}) = \text{Hom}(R_{\mathcal{D}}, \mathcal{A})$$

Soit $A = k[\varepsilon]/(\varepsilon^2)$ l'anneau des nombres duaux, dans cette formule.

On a d'abord

$$\text{Hom}_{\mathcal{O}\text{-alg}}(R_{\mathcal{D}}, k[\varepsilon]/(\varepsilon^2)) = \text{Hom}_{\mathcal{O}}(\mathcal{D}, k)$$

car si $\varphi \in \text{Hom}(R_{\mathcal{D}}, k[\varepsilon]/(\varepsilon^2))$, φ est déterminée (\mathcal{D} locale) par

par $\varphi(I_{\mathcal{D}})$, qui est $\mathcal{O}[\varepsilon]/(\varepsilon^2) \cong \mathcal{O}[\varepsilon] / (\varepsilon^2)$, pour

$$\varphi : \mathcal{D} = I_{\mathcal{D}}/I_{\mathcal{D}}^2 \xrightarrow{\sim} k$$

D'un autre côté, calculons $\text{Def}_{\mathcal{D}}(\bar{x}, k[\varepsilon]/\varepsilon)$:

soit (M) une déformation de \bar{x} dans \mathcal{A} , ρ est

$$\begin{array}{ccc} \rho : G_{\mathcal{D}} & \longrightarrow & (k[\varepsilon]/(\varepsilon^2))^{\times} \\ \bar{x} & \mapsto & k^{\times} \end{array}$$

et doit être de la forme $g \mapsto \bar{x}(g)(1+x_{\rho}(g)\varepsilon)$;

comme ρ est un morphisme, $\rho(gh) = \rho(g)\rho(h)$, ce qui implique que $x_{\rho} : g \mapsto x_{\rho}(g)$ vérifie

$$\bar{x}(g^2)(1+x_{\rho}(gh)\varepsilon) = \bar{x}(g)\bar{x}(h)(1+x_{\rho}(g)\varepsilon)(1+x_{\rho}(h)\varepsilon)$$

d'où $x_{\rho}(gh) = x_{\rho}(g) + x_{\rho}(h)$ (ce qui x_{ρ} est un morphisme de groupes $G_{\mathcal{D}} \rightarrow k$).

Comme ρ est de type \mathcal{D} , on trouve que $x_{\rho}|I_{\mathcal{D}}$ pour $\mathfrak{f} \in \Sigma$ doit être trivial, et de même $x_{\rho}|D_{\mathcal{D}}$ se factorise via $\text{Gal}(\mathcal{O}_{\rho}/\mathcal{O}_{\mathcal{D}})/\mathcal{O}_{\mathcal{D}}$. Alors $\rho \mapsto x_{\rho}$ est un isomorphisme.

Cela donne, exactement inversement, $x_{\rho} \mapsto \rho$ via

$$\text{Hom}(G_{\mathcal{D}}, k) \xrightarrow{\sim} \text{Hom}(\mathcal{D}, k)$$

et on vérifie que c'est aussi un isomorphisme de \mathcal{O} -module.

2^e cas : k quelconque

On introduit l'anneau $\mathcal{A}_k = \mathcal{O}[\varepsilon]/(m_0^k \varepsilon, \varepsilon^2) = \{a + a\varepsilon | a \in \mathcal{O}/m_0\}$

et on écrit encore l'isomorphisme

$$\text{Def}_{\mathcal{D}}(\bar{x}, \mathcal{A}_k) = \text{Hom}(R_{\mathcal{D}}, \mathcal{A}_k)$$

On commence par $\alpha \in \text{Hom}_{\mathcal{O}}(G_{\mathcal{D}}, \mathcal{O}/m_0)$,

$$= \ker(\text{Hom}(G_{\mathcal{D}}, \mathcal{O}/m_0)) \xrightarrow{\cong} \text{Hom}(G_{\mathcal{D}}, \mathcal{O}/m_0)$$

où \mathcal{E} sous-groupe de $G_{\mathcal{D}}$.

(i) si $\mathfrak{f} \notin \Sigma$,

Définition : $\text{Hom}_{\mathcal{O}}(G_{\mathcal{D}}, \mathcal{O}/m_0) = \{ \alpha : G_{\mathcal{D}} \rightarrow \mathcal{O}/m_0 \mid \alpha|I_{\mathcal{D}} = 0 \}$

groupes de Selmer

pour $\mathfrak{f} \notin \Sigma$, et $\alpha|D_{\mathcal{D}}$ se

factorise par $\text{Gal}(\mathcal{O}_{\rho}/\mathcal{O}_{\mathcal{D}})$

Etant donné α , on définit une déformation $\bar{x} \circ \mathcal{A}_k$ par

$$\begin{array}{ccc} \rho_{\alpha} : G_{\mathcal{D}} & \longrightarrow & \mathcal{A}_k^{\times} \\ g & \mapsto & x(g)(1+\alpha(g)\varepsilon) \end{array}$$

qui est effectivement une déformation de type \mathcal{D} , car χ l'est lui-même de type \mathcal{D} .

Par l'isomorphisme canonique, ça correspond donc à une flèche de \mathcal{O} -algèbres

$$\varphi_d : R_{\mathcal{D}} \rightarrow A_d$$

De nouveau φ_d est déterminée par $\varphi_d|_{I_{\mathcal{D}}}$ qui soit en fait

$$\varphi_d : I_{\mathcal{D}} \rightarrow \mathcal{E}(0/m_0)$$

i.e. (car φ_d est une flèche d'algèbres)

$$\varphi_d : \mathbb{F}_{\mathcal{D}} \rightarrow 0/m_0$$

La flèche $\varphi \mapsto \varphi_d$ donne l'isomorphisme recherché.

L'inverse peut être écrit explicitement : soit $\psi \in \text{Hom}_{\mathcal{O}}(\mathbb{F}_{\mathcal{D}}, 0/m_0)$;

on a la "déformation universelle" $G_{\mathcal{D}} \xrightarrow{\varphi_d} R_{\mathcal{D}}^*$, on compose et on obtient

$$G_{\mathcal{D}} \xrightarrow{p_2} (R_{\mathcal{D}}/I_{\mathcal{D}})^*$$

D'autre part, on a

$$\mathbb{F}_{\mathcal{D}} \longrightarrow 0^* \longrightarrow (R_{\mathcal{D}}/I_{\mathcal{D}})^*$$

Considérons alors $p_2 \circ p_1^{-1} : G_{\mathcal{D}} \longrightarrow (R_{\mathcal{D}}/I_{\mathcal{D}})^*$, mais

$$p_1^{-1} \equiv 1 \pmod{I_{\mathcal{D}}}$$

$$0 \rightarrow \mathbb{F}_{\mathcal{D}} \longrightarrow R_{\mathcal{D}}/I_{\mathcal{D}} \longrightarrow 0 \rightarrow 0$$

$$\Rightarrow 0 \rightarrow (1+I_{\mathcal{D}})/I_{\mathcal{D}} \longrightarrow (R_{\mathcal{D}}/I_{\mathcal{D}})^* \longrightarrow 0 \rightarrow 1$$

$$\text{ce qui donne } \alpha = p_2 \circ p_1^{-1} : G_{\mathcal{D}} \longrightarrow \mathbb{F}_{\mathcal{D}}$$

et, par composition avec φ_d , il vient une flèche

qui est celle de $\mathbb{F}_{\mathcal{D}} \xrightarrow{\varphi_d} 0/m_0$ et celle de $\mathcal{E}(0/m_0) \xrightarrow{\psi} 0/m_0$

et $\varphi_d \circ \psi \in \text{Hom}_{\mathcal{O}}(G_{\mathcal{D}}, 0/m_0)$.

On vérifie sans difficulté que $\varphi_d \circ \psi$ donne ce qu'on veut.

□ Retour à l'étape de récurrence.

Proposition Supposons que pour tout \mathcal{D} on ait

$$\text{et } e(\mathbb{F}_{\mathcal{D}}) = e(0/m_0)$$

Alors si $\mathcal{D}' \geq \mathcal{D}$ (i.e. $\mathcal{D}' = (\Sigma', \rho')$ et $\Sigma' \supset \Sigma$), on a encore

$$e(\mathbb{F}_{\mathcal{D}'}) = e(0/m_0)$$

Démonstration On suppose $\Sigma' = \Sigma \cup \{q\}$.

On a déjà vu que $\eta_{\mathcal{D}} = |(Z/N)| \cdot 0$,

$$\eta_{\mathcal{D}'} = |(Z/(qN))|^* \cdot 0$$

$$\text{donc } e(0/m_0) - e(0/\eta_{\mathcal{D}}) = e(0/(q-1)0) = \exp(q-1)$$

Il faut donc montrer que

$$e(\mathbb{F}_{\mathcal{D}'}) - e(\mathbb{F}_{\mathcal{D}}) \leq e(0/(q-1)0)$$

Pour cela on va appliquer la proposition (et le lemme précédent).

On choisit $\varphi \in \text{Hom}_{\mathcal{O}}(G_{\mathcal{D}'}, R_{\mathcal{D}'})$ tel que $\varphi|_{I_{\mathcal{D}'}} = \varphi|_{I_{\mathcal{D}}}$

et $\varphi \circ \psi \in \text{Hom}_{\mathcal{O}}(G_{\mathcal{D}'}, 0/m_0)$.

(cf. Darmon, "Sene's Conjecture", CMS Conf. Proc. 17]

Exposé des cas où la conjecture de Serre est connue.

Rappel

(forte)

Conjecture Soit \mathbb{F} un corps fini de caractéristique p et $\rho: G_{\mathbb{Q}} \rightarrow GL(2, \overline{\mathbb{F}})$ une représentation galoisienne (continue) telle que : (i) ρ est irréductible

$$(ii) \det(\rho(z \otimes \bar{z})) = -1 \quad (\rho \text{ impaire})$$

Alors il existe une forme modulaire $f = \sum a_n q^n$ de poids k , niveau N , caractère χ (cf. plus loin) telle que les coefficients a_n vérifient au $\mathbb{F}[\mathcal{O}_K]$, entiers d'un corps de nombre K , et il existe $p \in \text{Spec}(\mathcal{O}_K)$ avec $p \mid \rho$ et pour tout $l \nmid N$, on a

$$a_l \equiv \text{Tr } \rho(Frob_p) \pmod{p}$$

N.B. N et k ont été discutés précédemment.
On n'a pas parlé de χ , mais il y a aussi une recette pour se

$$|\text{Tr } \rho(Frob_p)| = p^k$$

Variante :

Conjecture faible - Mêmes hypothèses, mais dans la conclusion on ne prétend pas connaître N , k , et χ .

Il y a deux résultats généraux importants connus:

Théorème ("conjecture faible \Rightarrow conjecture forte")

Soit p impair, $p \neq 3$. Alors si la conjecture faible est vérifiée pour p , la conjecture forte l'est également.

N.B. Pour $p=2$, on n'a pas ce résultat.

Ribet
Mazur
Diamond

Pour $p=3$, on va faire un peu plus. Le pb. est que la conjecture faible pour Serre est faux pour $p=3$. Mais tant que $p \nmid \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(\sqrt{-3}))$ n'est pas abélienne, alors la conjecture faible implique la conjecture forte.

Théorème Soit E/\mathbb{Q} une courbe elliptique et $\rho_{E,p}$ la représentation de $G_{\mathbb{Q}}$ sur les points d'ordre p de E .

$$\rho: G_{\mathbb{Q}} \rightarrow GL(2, \mathbb{F}_p) \cong \text{Aut}(E[p])$$

et supposons que $\rho_{E,p}$ est absolument irréductible. Alors la conjecture de Serre est vraie pour $\rho_{E,p}$ aussi.

(i) E est de la forme $y^2 = (x-A)(x-B)(x-C)$ (i.e E a 4 points rationnels d'ordre 2)

(ii) E soit bonne, soit multiplicatives en 3 et en 5.

Wilensky
(Diamond)

N.B. Sur la condition d'irréductibilité.

En $\mathbb{F}_p^2 \rightarrow GL(2, \mathbb{F}_p)$ est irréductible. (évidemment) mais n'est pas absolument irréductible car

$$\mathbb{F}_p^2 \rightarrow GL(2, \mathbb{F}_p)$$

est semi-simple (il est la somme directe de deux copies).

Mais : une représentation irréductible n'est pas nécessairement irréductible.

lemme Soit $\rho: G_K \rightarrow GL(2, \mathbb{F})$ une représentation de degré 2 où K un corps fini, \mathbb{F} corps fini de caractéristique $p \neq 2$. Alors si ρ est impaire et irréductible, ρ est absolument irréductible.

Dém. ρ impaire $\Rightarrow \rho$ (conjugaison) a deux valeurs propres ± 1 et $\pm i$, et si ρ est irréductible sur une extension \mathbb{F}'/\mathbb{F}

il existe des vecteurs propres v_1 et v_2 pour σ , $\text{sp}(\sigma) \neq G$.

Puisque σ (conjugaison) a des vecteurs propres rationnels multiples, v_1 et v_2 doivent être des multiples de ceux-ci et ρ est réductible sur F !

□

(Remarquons que toutes les représentations ne viennent pas de courbes elliptiques.)

cf. le poids par exemple, je pense (?)

Autres cas connus

Ce sont pour la plupart des cas où $\text{Im } \rho \subset \text{GL}(2, F)$ est "petit" en un certain sens.

Exemple : supposons qu'il existe un sous-groupe fini $H \subset \text{GL}(2, \mathbb{C})$ tel que $\text{Im } \rho \cong H$

Ex. Les sous-groupes finis non-abéliens de $\text{GL}(2, \mathbb{C})$ sont :

• groupes diédraux, i.e. $D_n = \mathbb{Z}_{(n)} \times \mathbb{Z}/(2)$

des $\text{PGL}(2, \mathbb{C})$: $A_4, A_5, \text{SL}(2, \mathbb{Z}/3)$ (matrice $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$)

$$\begin{pmatrix} \zeta_5 & 0 \\ 0 & \zeta_5^{-1} \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Cela amène à la conjecture d'Artin-Tangleson.

Conjecture : soit $\sigma: G_{\mathbb{Q}} \rightarrow \text{GL}(2, \mathbb{C})$ une représentation d'image finie de $G_{\mathbb{Q}}$ telle que σ soit irréductible.

Alors il existe une forme modulaire f de poids k telle que $L(\sigma, s) = L(f, s)$ i.e. pour presque tout s

$$\text{Tr}(\sigma(F_s)) = \alpha f(s)$$

Un cas connu de cette conjecture est le suivant : si

general

$\text{Im } \sigma$ est décomposable (dans $\text{GL}(2, \mathbb{C})$), la conjecture est vraie (sauf dans $\{\text{Spf}(A_5)\}$).

Ex. Dans le cas où $\text{Im } \sigma$ est diédral : $\text{Im } \sigma = H = D_n \subset \text{GL}(2, \mathbb{C})$

Le diagramme indique $G_{\mathbb{Q}} \xrightarrow{\sigma} D_n$

: $G_{\mathbb{Q}} \cong (\mathbb{Z}/2)^2$ (i.e. $\mathbb{Z}/2 \times \mathbb{Z}/2$)

$G_{\mathbb{Q}} \xrightarrow{\sigma} D_n$ (i.e. $D_n \cong (\mathbb{Z}/2)^2 \rtimes \mathbb{Z}/2$)

$\mathbb{Q} \xrightarrow{\sigma} D_n$ (i.e. $D_n \cong (\mathbb{Z}/2)^2 \rtimes \mathbb{Z}/2$)

La forme modulaire f associée est une fonction thêta

$$f(q) = \sum_{a \in \mathcal{O}_K^N} x(a) q^{Na}$$

où $x(a)$ est un caractère du groupe d'idéaux a , $\pi(a) = \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}$

$$x(F_s) = \begin{pmatrix} s_n & 0 \\ 0 & s_{n-1} \end{pmatrix}$$

Les autres cas sont essentiellement sporadiques ...

(Serie 1...): $(A_4, \text{SL}(2, \mathbb{Z}/3)) + \dots$

(5.1) : cas $p=2$ qui nécessite \mathbb{F}_2

$$\rho: G_{\mathbb{Q}} \rightarrow \text{GL}(2, \mathbb{F}_2) \cong G_3 \cong D_3$$

donc on peut utiliser le résultat de Hecke, mais cela donne \mathbb{F}_2 de poids 1, et il faut encore étudier son niveau et son caractère et on doit peut ajuster le poids ...

Il y a des exemples où ça marche mal. Le cas générale, pour la conjecture forte, n'est pas clair...

(5.2) : $|F|=4$, $\text{SL}(2, \mathbb{F}_4) \cong A_5$

$$(5.4): |F| = 9, \quad \mathrm{SL}(2, F_9) \cong \tilde{A}_6$$

$$(5.5): |F| = 49, \quad |\mathrm{PSL}(2, F_7)| = 168$$

Idee: $G \hookrightarrow \mathrm{GL}(2, \mathbb{F})$

$G = \mathrm{Imp}$

(1) On construit des exemples d'extensions K/\mathbb{Q} avec $\mathrm{Gal}(K/\mathbb{Q}) \cong G$: on écrit le polynôme correspondant.

(2) On calcule $\mathrm{Tr}(\rho(F_\ell)) \in \mathbb{F}$

(3) On détermine N_p, k_p, ϵ_p , comme indiqué, puis on calcule l'espace des formes paraboliques de ce type

(4) On regarde si les coeff. de Fourier de ces formes sont congrus avec les $\mathrm{Tr}(\rho(F_\ell))$...

[il faut un théorème de Faltings pour finir la vérification à un nb. fini de nombres premiers] $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix} \right) = (\pm i)^q$

13-11-95

X - caractère de Dirichlet

$$G_\mathbb{Q} \rightarrow \mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q}) \cong \mathbb{Z}_p^\times,$$

$\mathcal{O}_{m_0} = h$ de caractéristique p (I.R.)

$$\bar{x}: G_\mathbb{Q} \rightarrow h^\times$$

On considère les déformations de \bar{x} de type $\mathfrak{D} = (\Sigma, \rho)$

(non-ramifiée en dehors de Σ , se factorise par $\mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q})$)

On a introduit $R_{\mathfrak{D}}$ et $T_{\mathfrak{D}}$ et la surjection

$$R_{\mathfrak{D}} \xrightarrow{\varphi} T_{\mathfrak{D}} \xrightarrow{\chi} \mathcal{O}$$

On en était à vérifier l'étape de récurrence:

Prop. Supposons que $\mathfrak{D}' \geq \mathfrak{D}$. Alors

$$\ell(I_{\mathfrak{D}}/I_{\mathfrak{D}'}) \leq \ell(O_{\mathfrak{D}'})$$

on a également

$$\ell(I_{\mathfrak{D}}/I_{\mathfrak{D}'}) \leq \ell(O_{\mathfrak{D}})$$

Dém.: Rappelons que l'on a montré

$$\mathrm{Hom}_0(\mathbb{F}, \mathcal{O}/m_0^k) \cong \mathrm{Hom}_0(G_\mathbb{Q}, \mathcal{O}/m_0^k)$$

où Hom_0 signifie : non-ramifiée (i.e trivial sur $I_\mathfrak{D}$) pour $\ell \notin \Sigma$, et se factorise par $\mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q})$.

On peut encore supposer $\Sigma' = \Sigma \cup \{q'\}$, $q' \notin \Sigma$.

Alors la flèche de restriction

$$\mathrm{Hom}_0(\mathbb{F}, \mathcal{O}/m_0^k) \xrightarrow{\mathrm{Res}} \mathrm{Hom}(I_{q'}, \mathcal{O}/m_0^k)$$

au sous-niveau $\mathrm{Hom}_0(G_\mathbb{Q}, \mathcal{O}/m_0^k)$ est

$$0 \rightarrow \mathrm{Hom}_0(G_\mathbb{Q}, \mathcal{O}/m_0^k) \rightarrow \mathrm{Hom}_0(G_\mathbb{Q}, \mathcal{O}/m_0^k) \xrightarrow{\mathrm{Res}} \mathrm{Hom}(I_{q'}, \mathcal{O}/m_0^k)$$

et on essaie de calculer $\ell(\mathrm{Hom}_0(\mathbb{F}, \mathcal{O}/m_0^k))$ via

$$\ell(\mathrm{Hom}_0(\mathbb{F}, \mathcal{O}/m_0^k)) \leq \ell(\mathrm{Hom}_0(G_\mathbb{Q}, \mathcal{O}/m_0^k))$$

puis on ajoute $\ell(\mathrm{Hom}(I_{q'}, \mathcal{O}/m_0^k))$

$$\ell(\mathrm{Hom}(I_{q'}, \mathcal{O}/m_0^k))$$

et plus précisément on doit montrer :

$$\ell(\mathrm{Hom}(I_{q'}, \mathcal{O}/m_0^k)) \leq \ell(O_{\mathfrak{D}'}) - \ell(O_{\mathfrak{D}})$$

En faisant $k \rightarrow \infty$, cela donne la proposition.

Le terme de droite est, on l'a vu, égal à

$$\ell(O/(q'-1)\mathcal{O})$$

Proposition. Soit $q \neq p$ un nombre premier. Alors

$$G_q = \mathrm{Gal}(\mathbb{Q}_q/\mathbb{Q}_p)$$

(i) On a une filtration

$$G_{q_1} \supset I_{q_1} \supset I_1$$

modérément ramifiée

$$\frac{G_{q_1}}{I_1}$$

$$\begin{matrix} \overline{I}_{q_1} \\ \overline{I}_1 \\ \overline{I}_{q_1} \\ \overline{I}_{q_1} \end{matrix}$$

non-ramifiée

$$G_{q_1}/I_1 \cong \text{Gal}(\overline{F}_{q_1}/F_{q_1})$$

$$I_{q_1}/I_1 \cong \varprojlim (\overline{F}_{q_1})^{\times}$$

I_1 est le pro- p -Sylow sous-groupe de I_{q_1} .

(ii) On a le générateur $F_{q_1} \in \text{Gal}(\overline{F}_{q_1}/F_{q_1}) = G_{q_1}/I_1$, et

$$(*) (F_{q_1})^\sigma = \sigma^{q_1} \quad \text{quand } \sigma \in I_{q_1}/I_1.$$

Maintenant, parce que \mathbb{Z}/m_p^k est d'ordre une puissance de p , toute flèche $d: I_{q_1} \rightarrow \mathbb{Z}/m_p^k$ se factorise via I_{q_1}/I_1 , et même, si d vient par restriction de G_{q_1}

(iii) montre que d vient de $(\overline{F}_{q_1})^{\times}$ (à un niveau le plus bas). : $(*) \Rightarrow d(\sigma) = \sigma^{q_1} \Rightarrow d(\sigma)^{q_1-1} = 0$

Fait : $\text{Im}(\text{Res}: \text{Hom}(G_\alpha, \mathbb{Z}/m_p^k) \rightarrow \text{Hom}(I_{q_1}, \mathbb{Z}/m_p^k))$

$$= \text{Hom}(I_{q_1}/I_1, \mathbb{Z}/m_p^k) \quad \text{(via } q_1 \times \mathbb{Z}/m_p^k)$$

$$= \text{Hom}(\varprojlim (\overline{F}_{q_1})^{\times}, \mathbb{Z}/m_p^k) \quad \text{(car } \mathbb{Z}/m_p^k \text{ commutatif)}$$

$$= \text{Hom}(\overline{F}_{q_1}^{\times}, \mathbb{Z}/m_p^k) \quad \text{(via (ii))}$$

dont la longueur est $\ell(\mathcal{O}_{(q_1-1)p})$ si k est assez grand.

D

Première partie du séminaire de Terry

$$M = (\Sigma, \rho)$$

le départ de la récurrence

L'idée de Wilf est la suivante : pour étudier R_D et T_D , avec \mathfrak{D} "minimal", on introduit des nombres premiers auxiliaires. Plus précisément, $\mathfrak{D} = (\Sigma, p^d)$, et on a vu (au tout début) qu'il existe un caractère de Dirichlet congruent à χ au niveau minimal (analogie de Ribet).

Répondons alors : Σ par $\Sigma \cup \{q_1, \dots, q_m\}$, et étudions la taille des invariants pour \mathfrak{D}' , en construisant des déformations pour ce \mathfrak{D}' , assez pour pouvoir contrôler Σ avec cette information. L'outil est la cohomologie des groupes et la cohomologie galoisienne.

Cohomologie des groupes

Soit G un groupe fini, M un \mathbb{Z} -groupe commutatif sur lequel G agit, c'est un G -module. (sans autre chose)

Définition : le 1er groupe de cohomologie de G à coefficient dans M est défini comme l'ensemble (l'ensemble)

$$H^1(G, M) = C^1(G, M)/Z^1(G, M)$$

où $C^1(G, M) = \{f: G \rightarrow M \mid f(g'h) = (fg)f(h) + f(g)\}$

(ou) $Z^1(G, M) = \{f: G \rightarrow M \mid \forall g, h \in G, f(g'h) = g.f(h) + f(g)\}$

Exemples : $\{f: G \rightarrow M \mid f(g) = 0\} = Z^1(G, M)$

N.B. Si la G -action sur M est triviale,

$$H^1(G, M) = \text{Hom}(G, M)$$

homomorphismes de groupes

Définition: Avec les mêmes notations, on pose

$$H^0(G, M) = M^G$$

$$H^1(G, M) = C^*(G, M)/Z^*(G, M)$$

où $Z^*(G, M) = \{f: G \times G \rightarrow M \mid f(hg_1, g_2) = f(h, g_1)g_2\}$

$Z^*(G, M) = \{f: G \times G \rightarrow M \mid \text{ "Définition"}\}$

Propriétés: Supposons qu'on ait une suite exacte de groupes

abéliens munis d'une action de G

$$0 \rightarrow M_1 \rightarrow M_2 \rightarrow M_3 \rightarrow 0$$

alors il y a une suite exacte longue des groupes abéliens

$$\begin{aligned} 0 &\rightarrow H^0(G, M_1) \rightarrow H^0(G, M_2) \rightarrow H^0(G, M_3) \rightarrow H^1(G, M_1) \\ &\rightarrow H^1(G, M_2) \rightarrow H^1(G, M_3) \rightarrow H^2(G, M_1) \rightarrow \dots \end{aligned}$$

Cohomologie des groupes

(de Galois en particulier)

Soit G un groupe topologique, M un groupe abélien muni de la topologie discrète et d'une action continue de G , i.e. $G \times M \rightarrow M$ continue.

[Cela équivaut à demander que $\text{Stab}_G(m) \subset G$ est un sous-groupe ouvert pour tout m]

Ex: (1) G fini avec la topologie discrète

(2) G profini, en particulier $G = \text{Gal}(\bar{\mathbb{K}}/\mathbb{K})$

(3) $M = \mathbb{R}$, $G = \text{Gal}(\bar{\mathbb{K}}/\mathbb{K})$: G agit effectivement continûment sur M

$$M = \mathbb{R}^\times, G = \text{Gal}(\bar{\mathbb{K}}/\mathbb{K}).$$

Chaines continues

$$C^*(G, M) = \{f: G^n \rightarrow M \mid f \text{ continue}\}$$

Differentielle

$$d: C^*(G, M) \rightarrow C^{n+1}(G, M)$$

$$\{ \quad \} \mapsto df: (x_1, \dots, x_n) \mapsto x_n f(x_1, \dots, x_n)$$

$$df(g_1, \dots, g_n) = \sum_{i=1}^n (-1)^i f(g_1, \dots, g_{i-1}, g_{i+1}, \dots, g_n) + (-1)^{n+1} f(g_1, \dots, g_n)$$

Fait: $d \circ d: C^*(G, M) \rightarrow C^{n+2}(G, M)$ est nulle.

$$\text{Ex: } n=0: C^0(G, M) \rightarrow C^1(G, M)$$

$$M \stackrel{\cong}{\longrightarrow} \{m\} \stackrel{\cong}{\longrightarrow} (\text{dm}: g \mapsto g, m \mapsto m)$$

$$n=1: C^1(G, M) \rightarrow C^2(G, M)$$

$$f \mapsto (df: (g_1, g_2) \mapsto g_1 f(g_2) - f(g_1 g_2) + f(g_1))$$

$$n=2: C^2(G, M) \rightarrow C^3(G, M)$$

$$df(g_1, g_2, g_3) = g_1 f(g_2, g_3) - f(g_1 g_2, g_3) + f(g_1, g_2 g_3)$$

$$(f \circ g) \circ h = f \circ (g \circ h) \text{ donc } f(g_2, g_3) = f(g_2, g_1 g_2)$$

Soit $Z^n(G, M) = \text{Ker}(d: C^n(G, M) \rightarrow C^{n+1}(G, M))$ (cocycles)

$B^n(G, M) = \text{Im}(d: C^{n-1}(G, M) \rightarrow C^n(G, M))$ (cobords)

lemme: $B^n(G, M) \subset Z^n(G, M)$

Définition: On pose $H^n(G, M) := Z^n(G, M)/B^n(G, M)$

$$\text{Ex: } n=0: H^0(G, M) = Z^0(G, M) = \text{Ker}(d: C^0 \rightarrow C^1)$$

$$M \stackrel{\cong}{\longrightarrow} \{m\} \stackrel{\cong}{\longrightarrow} \{m\} = \{m \mid \sqrt[n]{qm} = m\} = M^G$$

$$n=1: H^1(G, M) = Z^1/G = \{f: G \rightarrow M \mid f(gh) = gf(h) + f(g)\}$$

$$\begin{cases} f: G \rightarrow M / \mathbb{Z}_n \\ f(g) = gm \end{cases}$$

$$n=2 : H^2(G, M) = \frac{\{f: G \times G \rightarrow M \mid f(g_1 g_2, g_3) = g_1 f(g_2, g_3) + f(g_1, g_2 g_3)\}}{\{f: G \times G \rightarrow M \mid \exists \tilde{f}: G \rightarrow M, f(g_1 g_2) = g_1 f(g_1) + f(g_2)\}}$$

Exemples classiques

$H^2(G, M)$, où G et M sont finis, classe les classes d'équivalences d'extensions :

$$0 \rightarrow M \xrightarrow{\alpha} E \xrightarrow{\beta} G \rightarrow 1$$

On choisit en effet une section ensemble : $G \rightarrow E$.

Pour tout $x \in E$, on a $x = x \circ \beta(x)^{-1} \in M$, donc $E \cong M \times G$ comme ensemble partiellement.

Considérons $\{ (g_1, g_2) \mapsto s(g_1, g_2), s(g_1)^{-1}, s(g_2)^{-1} \}$

On a l'associativité $(g_1 g_2) g_3 = g_1 (g_2 g_3)$

$$\begin{aligned} f(g_1 g_2, g_3) &= s(g_1 g_2, g_3) - s(g_1, g_2)^{-1} - s(g_3)^{-1} \\ &= f(g_1, g_2) + s(g_1, g_3) - s(g_1)^{-1} - s(g_2)^{-1} \\ f(g_1, g_2 g_3) &= s(g_1, g_2 g_3) - s(g_1)^{-1} - s(g_2 g_3)^{-1} \\ &\quad (M, \oplus) \end{aligned}$$

H^1 : soit G fini cyclique engendré par γ , d'ordre n , et regardons $H^1(G, M)$

$$f(g_1, g_2) = g_1 f(g_2) + f(g_1)$$

$\Rightarrow f$ est déterminée par $f(\gamma) \in M$

$$\begin{aligned} \text{De plus } 0 &= f(\gamma^n) = \gamma f(\gamma^{n-1}) + f(\gamma) \\ &= \gamma f(\gamma) + f(\gamma) + \dots + f(\gamma) \\ &= N(f(\gamma)) \end{aligned}$$

(où $N = \sum g$ dans $Z(G)$)

$$Z^1(G, M) = \text{Ker}(N: M \rightarrow M)$$

$$B^1(G, M) = \{m' \mid \exists m, m' = jm - m\}$$

Hilbert a étudié ces cas dans les années 20

$$(B^1(G, M))^G \cong Z^1(G, M)$$

En théorie des déformations :

soit G un groupe, O un anneau local, $k = O/\mathfrak{m}_O$, on s'intéresse aux représentations $\rho_0: G \rightarrow GL(n, k)$ et plus exactement aux déformations $\rho: G \rightarrow GL(n, A)$, A locale de corps résiduel telles que $\bar{\rho} = \rho_0$.

Soit $A = k[[\epsilon]]$ l'anneau des nombres duals, et ρ une déformation de ρ_0 dans $GL(n, A)$.

$$\begin{aligned} \text{On peut écrire } \rho(g) &= \rho_0(g) \cdot (1 + \epsilon c(g)), \text{ avec} \\ c(g) &\in M(n, k), \text{ et comme } \rho(g_1 g_2) = \rho(g_1) \rho(g_2), \text{ il vient} \\ &\rho(g_1 g_2) = \rho_0(g_1) \rho_0(g_2) (1 + \epsilon c(g_1 g_2)) = \rho_0(g_1) (1 + \epsilon c(g_1)) \\ &\quad \rho_0(g_2) (1 + \epsilon c(g_2)) \end{aligned}$$

$$\begin{aligned} &= \rho_0(g_1) \rho_0(g_2) g_0(g_2)^{-1} (1 + \epsilon c(g_1)) \rho_0(g_2) \\ &\quad (1 + \epsilon c(g_2)) \\ &\quad \vdots \\ &= \rho_0(g_1) \rho_0(g_2) \dots \rho_0(g_n)^{-1} (1 + \epsilon c(g_1)) \rho_0(g_2) \dots (1 + \epsilon c(g_n)) \end{aligned}$$

$$\begin{aligned} \text{Faisons } c(g_1 g_2) &= \rho_0(g_2)^{-1} c(g_1) \rho_0(g_2) + c(g_2) \\ &= \text{Ad}(g_2) c(g_1) + c(g_2) \end{aligned}$$

ce qui établit un 1-cocycle $c \in Z^1(G, M(n, k))$ où G agit sur $M(n, k)$ via la représentation adjointe de ρ_0 par conjugaison.

Fonctorialité

Soit A et B des G -modules et qu'on a une application

$$\alpha: A \rightarrow B \text{ de } G\text{-modules.}$$

Alors α induit pour tout n une application fonctorielle

$$H^n(G, A) \xrightarrow{\alpha} H^n(G, B)$$

($f \mapsto \alpha \circ f$) est évident.

Si on a une suite exacte de G -modules alors

$$0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0$$

alors on a une suite exacte longue induite :

$$0 \rightarrow H^0(G, A) \rightarrow H^0(G, B) \rightarrow H^0(G, C) \xrightarrow{\delta} H^1(G, A) \rightarrow \dots \rightarrow H^n(G, A) \rightarrow H^n(G, B)$$

$$\rightarrow H^n(G, C) \xrightarrow{\delta} H^{n+1}(G, A) \rightarrow \dots$$

(où les flèches de connexion δ sont les flèches du sequence, classiques).

$$[H^0(G, C) \rightarrow H^0(G, A) \text{ via } c \in G^C, c + b \in G^C, g \mapsto gb - b \in Z(G, A) \dots]$$

17/11/95 Séminaire

Variantes de l'équation de Fermat

[cf. Darmont "Equations: $x^n + y^n = z^2$ and $x^n + y^n = z^3$ ", IMRN 1993, #10 (in Duke Journal)]

Ribet "On the equation $a^p + 2^2 b^p + c^p = 0$ ", preprint]

On s'intéresse à des équations diophantiennes de la forme $A + B + C = 0$.

Approche générale: associer une courbe elliptique à la

solution hypothétique, montrer qu'elle est modulaire avec bonnes (paramètres) (R, N, E) , et vérifier que c'est possible ou pas. On retrouve soit une contradiction, soit des solutions continues, si l'on peut démontrer que la solution n'existe pas.

Irréductibilité de $P_{E,p}$, E courbe elliptique

Dire que $P_{E,p}$ est irréductible, veut dire que E contient un sous-groupe rationnel d'ordre p (rationnel globalement, pas point par point...), i.e. E a une origine rationnelle de degré p . De telles courbes sont associées à un point rationnel sur $X_0(p)$ (non-cuspidaux).

Proposition: Si p est premier, $p > 13$, le nombre total de points rationnels non-cuspidaux de $X_0(p)$ est donné par

17	19	37	43	67	163	$p > 163$
2	1	2	1	1	1	0

Darmont remarque, en calculant explicitement, que pour ces courbes elliptiques associées, l'invariant $j(E)$ est dans $\mathbb{Z}\left[\frac{1}{2}\right]$, i.e.

Lemme: Si $p > 13$, $P_{E,p}$ est irréductible, alors $j(E) \in \mathbb{Z}\left(\frac{1}{2}\right)$.

[N.B.: On a vu (cf. exposé de José):

Lemme: Si E est semi-stable et $p > 5$, $P_{E,p}$ est irréductible (si de plus il y a un pt d'ordre 2 rationnel).

Proposition (Kamienny). Soit K un corps quadratique imaginaire, p premier scindé dans K , q non-scindé dans K . Si il

existe n premier tel que n divise le numérateur $\frac{(pq)(q-1)}{2^4}$,
 n ne divise pas $q(q-1)$, n ne divise pas $p\chi(K)$, alors toute
courbe elliptique E/K qui a un sous-groupe d'ordre pq
défini sur K a réduction potentiellement bonne en toute
place ne divisant pas 6.

Corollaire 1 - Supposons $p \equiv 1 \pmod{4}$ et soit $E/\mathbb{Q}(\sqrt{-1})$ admettant
un sous-groupe $\mathbb{Q}(\sqrt{-1})$ -rationnel d'ordre $2p$; alors

$$j(E) \in \mathbb{Z}[\sqrt{-1}] \left[\frac{1}{6} \right]$$

Corollaire 2 - Supposons $p \equiv 3 \pmod{4}$ et p, n est pas un nombre
de Mersenne. Si $E/\mathbb{Q}(\sqrt{-3})$ est une courbe elliptique
admettant un sous-groupe $\mathbb{Q}(\sqrt{-3})$ -rationnel d'ordre $3p$.
Alors

$$j(E) \in \mathbb{Z}[\sqrt{-3}] \left[\frac{1}{6} \right]$$

On considère pour p premier, $p > 13$, l'équation

$$x^3 + y^3 = z^2$$

Supposons que (a, b, c) est une solution avec a, b, c premiers
deux à deux.

Si nécessaire on peut échanger a et b , multiplier c par -1 ,
pour mettre la solution sous l'une des deux formes suivantes

$$(1) \quad a \equiv 0 \pmod{2}, \quad c \equiv 1 \pmod{4}$$

$$(2) \quad a \equiv -1 \pmod{4}, \quad c \equiv 0 \pmod{2}$$

$$\text{Cas (1)}: \quad y^2 = x^3 + cx^2 + \frac{a^6}{4}x; \quad \Delta = (a^2b)^6 \quad \text{et} \quad (E) \in \frac{2^6(a^2b)^6}{(a^2b)^6}$$

Cas (2): $y^2 = x^3 + 2cx^2 + a^6x; \quad \Delta = 2^6(a^2b)^6$

Soit $\ell \neq 2$ premier, si la réduction de E à ℓ est mauvaise

Soit $\ell \neq 2$ premier, la réduction de E , quand elle est
mauvaise, est multiplicativité.

En effet, $\ell \mid a^2b$ donc $\ell \nmid c$; mais on voit que réduction
additive $\Rightarrow \ell \mid c$ (racines triple modulo ℓ).

De plus le discriminant est divisible par ℓ (calcul
facile à partir des formules pour les isomorphismes d'un modèle
de Weierstraß).

Rappelons (cf. José) que pour le conducteur d'Artin, ℓ sa
partie plutôt, cela implique que $v_\ell(\Delta) \geq 1$ car
 $\text{Orde}(\Delta) \equiv 0 \pmod{\ell}$.

Si $\ell = 2$:

(1) On fait le changement de variables

$$\begin{cases} Y = 8y + 4x \\ X = 4x \end{cases} \quad \text{et} \quad (1) \iff Y^2 + XY = X^3 + \left(\frac{c-1}{4}\right)X^2 + \frac{a^6}{2^6}X$$

$\Rightarrow Y^2 + XY = X^3 + \left(\frac{c-1}{4}\right)X^2 + \frac{a^6}{2^6}X; \quad \Delta = \frac{(a^2b)^6}{2^{12}}$
et cette courbe a réduction additive modulo 2.

Donc $v_2(\Delta) \not\equiv 0 \pmod{\ell}$: il y a 2 apparaît à la puissance 1 dans
le conducteur d'Artin.

(2) On a réduction additive en 2.

On a cependant:

$$\text{Fait: } v_\ell(l \cdot (\rho_{E,p})) \leq \begin{cases} 5, & \ell=2 \\ 3, & \ell=3 \\ 2, & \ell \geq 3 \end{cases}$$

(cf. un exposé ultérieur de José)

dans le cas (v)

Donc on a $\rho = (2, \rho_{E,p}) \mid 2^5$

Utilisant le théorème de Wiles (-Diamond), E étant semi-stable en 5 et en 3, E est modulaire dans les deux cas.

Dans les deux cas, on voit également que le poids est 2.

N.B. Ici on a pas besoin de vérifier que $\rho_{E,p}$ est irréductible, pour avoir la forme modulaire, de poids 2.

Mais pour descendre le niveau à la valeur prédictive, il faut appliquer le Th. de Ribet, ce qui requiert l'irréductibilité.

Théorème - L'équation $x^p + y^p = z^2$ n'a pas de solutions entières primitives à part $(1, 0, \pm 1)$, $(0, 1, \pm 1)$, $(\pm 1, \mp 1, 0)$ quand $p \geq 1 \pmod{4}$, $p \neq 13$.

Dém. Soit D' abord, $j(E) \in \mathbb{Z}[\frac{1}{2}]$:

si $j(E) \notin \mathbb{Z}[\frac{1}{2}]$, on doit avoir $a^2 b^2 = 2^n$
 $\Rightarrow a = 2^m$, $b = \pm 1$

soit $2^{pm} = c^2 \pm 1$, mais

que l'on résoud trivialement

$$2^{pm} = c^2 + 1, \text{ impossible mod. 4}$$

$$2^{pm} = (c-1)(c+1), \text{ impossible}$$

(Gla si $ab \neq 0$, i.e. E est une courbe elliptique, on traite les autres cas à part).

D'après le Lemme du début, $\rho_{E,p}$ est irréductible,

ce qui donne une forme de poids 2 et niveau $2\sqrt{2}$ qui n'existe pas.

(cas (2)) : E peut être de niveau 32, mais

donc il y a une seule forme f correspondante, qui se trouve être associée à

$y^2 = x^3 - x$ (qui fait multiplication complexe par $\mathbb{Z}(i)$).

Notons $\rho_0, \rho = \rho_{E,p}$, $\rho = \rho_{E,p}$

Fait : ces deux représentations sont conjuguées.

(par Cebotarev par exemple, elles ont le même caractère : chaque classe d'isogénie de $\text{Gal}(\mathbb{Q}/\mathbb{Q})$ contient une infinité de Frobenius, etc.)

On est en caractéristique p -réduite et il faut encore dire quelque chose :

si on a une représentation semi-simple en caractéristique p , le caractère détermine p modulo $\ell!$ ajout de ℓp fois

mais la représentation ci-dessus dans $\text{GL}(2)$ qui est un peu petit pour accomoder p fois p [cf. Curtis-Reiner].

Maintenant, le fait est qu'on en soit un rayon au sujet de ρ_0 (et donc de ρ):

$$y^2 = x^3 - x \quad E(0) = \mathbb{C}/\mathbb{Z}(i)$$

Isogenie : $[i] : (x, y) \mapsto (-x, y)$

* 3 des composantes irréductibles de ρ

(\cdot) est dans $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ dans $\mathcal{O}_{\mathbb{Z}(i)}$ et engendre l'anneau des isogénies.

Remarquons que la représentation de $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}(i))$ coïncide avec cette représentation de $\text{End}(E)$. Un calcul simple montre que cela force cette représentation à être contenue dans $\langle \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \rangle$.

Donc

$$\rho_p(\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}(i))) \subset \rho_p(\text{isogénies}) = (\mathbb{Z}(i)/\rho\mathbb{Z}(i))^*$$

car $p \equiv 1 \pmod{4}$.

Cela nous dit qu'on a deux sous-groupes d'ordre p rationnels sur $\mathbb{Q}(i)$.

De plus, $(0,0)$ est un point rationnel d'ordre 2 non-trivial, donc on a un sous-groupe d'ordre 2p rationnel sur $\mathbb{Q}(i)$.

Par le corollaire ⁽¹⁾ à la proposition de Kamienny, les seuls nombres premiers divisant le dénominateur de $J(E)$ sont 2 et 3.

Comme a, b sont impairs, on a $ab \equiv 3 \pmod{4}$

$$3^{p^n} \equiv (-1)^n + 1$$

qui n'a aussi que des solutions triviales.

N.B. Pour l'équation $x^p + y^p = z^3$, sans hypothèse p irrégulier, le lemme précédent montre qu'il n'y a rien.

Réultat similaire, et on appliquera le corollaire (2) (la courbe $y^2 = x^3 + 16$ apparaîtra...).

[Une des courbes, cependant, a réduction additive en 3 donc n'est pas modulaire pour l'instant ...]

20/11/95

Fin de la preuve du théorème de Kronecker-Weber

Il faut modifier un peu la situation...

Rappelons qu'on a défini une représentation

$$\rho: G_{\mathbb{Q}} \rightarrow A^*$$

$(A, \mathcal{O}$ -algèbre locale de corps résiduel tel que $\text{char}(\mathcal{O}) = p$) comme étant de type $\mathfrak{D} = (\Sigma, \rho^j)$ si et seulement si

(i) ρ est non-ramifiée en dehors de Σ , i.e. $\rho|I_q = 1$, si $q \notin \Sigma$

(ii) $\rho|D_p$ se factorise via $\text{Gal}(\mathbb{Q}_p(\mu_{p^j})/\mathbb{Q}_p)$

En fait, la condition ad-hoc est :

(ii') $\rho|D_p$ se factorise via $\text{Gal}(\mathbb{Q}_p(\mu_N)/\mathbb{Q}_p)$ pour un N tel que $p^j \parallel N$

(ii'') $\rho|D_p$ se factorise via le groupe de Galois de $\mathbb{Q}(\mu_p)$ ou L/\mathbb{Q}_p est non-ramifiée.

On va utiliser maintenant (ii').

On fait aussi (ii') $\Leftrightarrow \rho|I_p \cap \text{Gal}(\mathbb{Q}_p(\mu_{p^j})/\mathbb{Q}) = 1$.

Proposition (Etape de récurrence) : $\text{soit } j \in \mathbb{N}$

On dit que $\mathfrak{D}' = (\Sigma', \rho'^j) \Rightarrow \mathfrak{D} = (\Sigma, \rho^j) \Leftrightarrow j \geq j'$ et $\Sigma' \supset \Sigma$.

Supposons que

$$e(\bar{\rho}_0) \leq e(0/\eta_0)$$

Alors

$$e(\bar{\rho}_0) \leq e(0/\eta_0)$$

Dém.

Il suffit de traiter les deux cas suivants:

$$\text{Cas (i)}: \quad \mathcal{D} = (\sum_{i \in \mathbb{Z}} v_i q^i), \quad \bar{\rho}^j = (\sum_i, \rho^j)$$

$$\text{Cas (ii)}: \quad \mathcal{D} = (\sum_i, \rho^{j+1}), \quad \bar{\rho} = (\sum_i, \rho^j)$$

On a déjà fait le cas (i).

Rappelons brièvement que: si ℓ est premier avec p ,

$$\text{Hom}_{\mathbb{Z}}(G_Q, \mathbb{Q}/m_0^\ell) = \text{Hom}_{\mathbb{Z}}(G_Q, \mathbb{G}/m_0^\ell)$$

$$\begin{cases} \text{si } I_p = 0, & j \notin \Sigma \\ \text{si } I_p \cap \text{Gal}(\mathbb{Q}_p(\mu_{p^j})/\mathbb{Q}_p) = 0 & \end{cases}$$

$$\text{et on a: } \text{Hom}_{\mathbb{Z}}(G_Q, \mathbb{Q}/m_0^\ell) \xrightarrow{\text{Res}} \text{Hom}_{\mathbb{Z}}(I_{q^j}, \mathbb{Q}/m_0^\ell)$$

$$\text{Or } e(\text{Hom}(I_{q^j}, \mathbb{Q}/m_0^\ell)) \leq e(0/(q^{j-1})\mathbb{O})$$

(car I_{q^j} contient un \mathbb{Z}_{q^j} -Sylow sous-groupe et I_{q^j}/\mathbb{O}_{q^j} est $\varprojlim_{q^n} \mathbb{F}^\times$; or \mathbb{Q}/m_0^ℓ est un \mathbb{Z}_p -groupe donc)

2: $I_{q^j} \rightarrow \mathbb{Q}/m_0^\ell$ se factorise via I_{q^j}/\mathbb{O}_{q^j} , dont tout les quotients sont cycliques, et sur lequel l'action de \mathbb{F} conjointement par Frobenius est l'élevation à la puissance q^j -ème, i.e. l'image par ℓ du générateur est d'ordre $[q^j - 1]$.

$$\text{etc... } \therefore (e(0/(q^{j-1})\mathbb{O})) = (e(0/\eta_0) + e(0/\eta_0))$$

Dans le cas (ii), même idée: on a bien

$$\text{Hom}_{\mathbb{Z}}(G_Q, \mathbb{Q}/m_0^\ell) \rightarrow \text{Hom}_{\mathbb{Z}}(G_Q, \mathbb{G}/m_0^\ell) \xrightarrow{\text{Res}} \text{Hom}(I_p \cap G_{p^j}/I_p \cap G_{p^{j+1}}, \mathbb{G}/m_0^\ell)$$

(où $G_{p^j} = \text{Gal}(\mathbb{Q}_p(\mu_{p^j})/\mathbb{Q}_p))$

On remarque que

$$\text{Hom}(I_p \cap G_{p^j}/I_p \cap G_{p^{j+1}}, \mathbb{G}/m_0^\ell) \rightarrow \text{Gal}(\mathbb{Q}_p(\mu_{p^{j+1}})/\mathbb{Q}_p(\mu_{p^j}))$$

Si $j=0$: le dernier groupe est $\cong (\mathbb{Z}/p)^\times$

Si $j \geq 1$: le dernier groupe est $\cong \mathbb{Z}/(p)$

On calcule:

$$e(\text{Hom}_{\mathbb{Z}}(G_Q, \mathbb{Q}/m_0^\ell)) \leq e(\text{Hom}_{\mathbb{Z}}(G_Q, \mathbb{G}/m_0^\ell)) + \begin{cases} 0 & \text{si } j=0 \\ e(0/p\mathbb{O}), & \text{si } j \geq 1 \end{cases}$$

$$\leq e(0/\eta_0) + \begin{cases} 0 & \\ e(0/p\mathbb{O}) & \end{cases} = e(0/\eta_0)$$

$$\text{car } 0/\eta_0 = \mathbb{G}/((\mathbb{Z}/p\mathbb{Z})\mathbb{O})$$

On commence la récurrence facilement: type D

Théorème. Soit $\rho: G_Q \rightarrow A$ une déformation du caractère de Dirichlet trivial, i.e. $\rho(g) \equiv 1 \pmod{m_1}$.

Alors ρ est de la forme ρ_χ pour un caractère de Dirichlet

Dém. Soit $\mathcal{D}_0 = (\emptyset, \rho^0)$, la donnée de déformation minimale.

On doit calculer $\ell(\emptyset_{\mathcal{D}_0})$ et $\ell(0/\emptyset_{\mathcal{D}_0})$ et comparer.

Si ils sont égaux, l'étape de récurrence donne le théorème.

Or, clairement

$$\ell(0/\emptyset_{\mathcal{D}_0}) = \ell(0/(Z_{\mathbb{Z}}) \times 0) = 0$$

et pour le grand

$$\ell(\emptyset_{\mathcal{D}_0}) = \text{Hom}_{\mathcal{D}_0}(G_{\mathbb{Q}}, \mathcal{O}_{\mathbb{Q}, \emptyset}^\times)$$

Mais une telle $d: G_{\mathbb{Q}} \rightarrow \mathcal{O}_{\mathbb{Q}, \emptyset}^\times$ serait non-ramifiée partout, i.e. son noyau aurait une extension abélienne non-ramifiée partout ; comme ceci n'est pas possible par le théorème de Minkowski,

$\text{Ker } d = G_{\mathbb{Q}}$ et $\ell(\emptyset_{\mathcal{D}_0}) = 0$.

N.B. On ne s'en tire pas si facilement dans le cas de Wiles.

Théorème (Kronecker-Weber)

Toute extension abélienne finie de $\mathbb{Q} = \mathbb{Q}(\zeta_N)$ contenue dans une extension cyclotomique $\mathbb{Q}(\mu_N)$ pour un N .

Dém. Il suffit de traiter le cas d'une extension de groupe de Galois $G \cong \mathbb{Z}/(p^k)$, p premier (en étendant G comme produit de plusieurs groupes et en composant les corps obtenus).

Soit donc K/\mathbb{Q} une extension galoisienne telle que

$$\text{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/(p^k)$$

Soit \mathcal{O} l'anneau des entiers de $\mathbb{Q}(\mu_{p^k})$, et considérons

$$\text{la flèche } G_{\mathbb{Q}} \xrightarrow{\rho} \mathcal{O}^\times \hookrightarrow$$

$$\text{racine primitive } p \text{ i.e. } \mathcal{O}^\times \xrightarrow{\text{primitive de } p} \mathbb{Z}/(p^k)^\times \text{ de degré } p^k$$

On calculera si $p \bmod m_0 = 1$ car $\text{char}(\mathbb{Q}/m_0) = p$.

La question est maintenant : est-ce que ρ est de type

\mathcal{D} ? Dès pour une certaine donnée de déformation \mathcal{D} ?

Dirabord, si ρ est non-ramifiée en dehors de l'ensemble fini des places où K est ramifié.

Pour traiter ρ , il faut le lemme suivant : le lemme (version locale du th. de Kronecker-Weber).

Soit E/\mathbb{Q}_p une p -extension abélienne finie.

Alors E est contenue dans une extension obtenue en ajoutant à \mathbb{Q} les racines p^j ièmes de l'unité à une extension non-ramifiée de \mathbb{Q} ($\Rightarrow E$ est inclus dans une extension cyclotomique, via la construction des extensions non-ramifiées) (ce lemme implique que ρ est de type \mathcal{D} (avec $\Sigma = \{ \text{places ramifiées de } K \}$, j. donné par le lemme)).

Il suffit alors de montrer \mathcal{D} satisfait aux critères.

Par la théorie des déformations, on a alors $\rho = \rho_x$ pour un caractère de Dirichlet associé à une extension cyclotomique,

$$K = \overline{\mathbb{Q}} \cap \mathbb{Q}(\zeta_{p^k}) \text{ est cyclotomique}$$

Reste à prouver le lemme local.

On utilise la complexité minimalement dans le lemme local.

Dém. Soit E/\mathbb{Q}_p une telle p -extension abélienne de \mathbb{Q}_p .

Notons L la composition de toutes les extensions cycliques d'ordre divisant p^m de \mathbb{Q}_p .

On va montrer: En est obtenue, en saignant les racines p^m -èmes de l'unité, une extension non ramifiée de \mathbb{Q}_p .

En effet, soit: L_m l'unique extension d'ordre p^m dans $\mathbb{Q}_p(\mu_{p^m})$ (si p est impair; $p=2$ voir plus loin).

Alors $L_m K_m$ est l'extension non ramifiée de \mathbb{Q}_p d'ordre p^m .

Alors $L_m K_m \subseteq E$. En effet, montrons que:

soit $\sigma \in \text{Gal}(E/\mathbb{Q}_p)$, alors $\sigma(L_m) = L_m$.

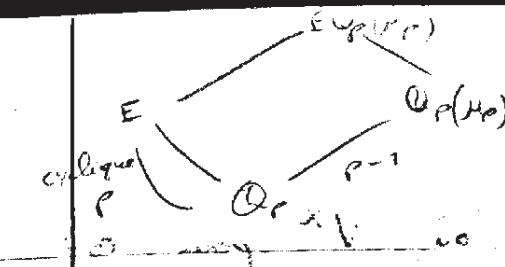
Or on sait précisément que L_m est alors (topologiquement) engendré par le même nombre de générateurs que G/ρ_G .

Ici $G/\rho_G = \text{Gal}(E/\mathbb{Q})$. Si il n'y a que deux générateurs, comme on a déjà L_m et K_m , cela sera OK...

On veut donc classifier les extensions de \mathbb{Q}_p abéliennes d'exposant p . Les extensions cycliques de degré p de $\mathbb{Q}_p(\mu_p)$ sont toutes construites par $\mathbb{Q}_p(\mu_p, \alpha^{1/p})$ pour un $\alpha \in \mathbb{Q}_p(\mu_p)$, i.e. sont classifiées par les sous-groupes de K^*/K^{*m} ($K = \mathbb{Q}_p(\mu_p)$).

$$B \subset K^*/K^{*m} \rightarrow \mathbb{Q}_p(\{\alpha^{1/p} | \alpha \in B\}).$$

Si on veut les extensions cycliques d'ordre p de \mathbb{Q}_p



27/11/95

On étudie les extensions abéliennes de \mathbb{Q}_p qui sont de plus cycliques d'ordre p .

On connaît déjà deux telles extensions de \mathbb{Q}_p :

- (i) l'unique extension non ramifiée de degré p .
- (ii) une extension ramifiée de degré p sur $\mathbb{Q}_p(\mu_2)$.

Rappel: (théorie de Kummer)

(a) Soit K un corps contenant une racine primitive m -ème de l'unité. Alors toute extension cyclique de degré m de K est de la forme $K(\sqrt[m]{\alpha})$ pour $\alpha \in K$.

[Dém] Par th 90 de Hilbert implique que $\alpha \in K$ est cyclique et si $z \in L$ vérifie $N_{L/K}(z) = 1$, il existe $w \in L$ et $\sigma \in \text{Gal}(L/K)$ tel que $z = \frac{w^\sigma}{w}$, on applique cela à $z = \omega_m$: $Nz = 1 \Rightarrow Nz = \frac{\omega_m}{\omega_m}$ lors où $\omega_m = \text{racine } m$ de 1 $\Rightarrow \omega_m^m = \omega_m$.

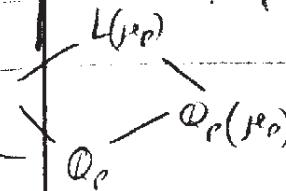
(b) Supposons $K(\sqrt[p]{\alpha_1}) = K(\sqrt[p]{\alpha_2})$, alors $\alpha_1 = \alpha_2^{t_1} \tau_1^{p^n}$ pour un $\alpha_i \in K$ (i.e. α_1 et α_2 engendrent le même sous-groupe de $K^*/(K^*)^m$)

$$\text{Dém } \sigma(\sqrt[p]{\alpha_1}) = \sqrt[p]{\alpha_1} \Rightarrow \sigma(\sqrt[p]{\alpha_2}) = \sqrt[p]{\alpha_2}.$$

génération de $\text{Gal}(L/K)$ et on a $\alpha_1 = \alpha_2^{t_1} \tau_1^{p^n}$ donc $\sqrt[p]{\alpha_1} = \sqrt[p]{\alpha_2}^{t_1}$

$$\text{i.e. } \alpha_1 = \frac{\sqrt[p]{\alpha_2}}{\sqrt[p]{\alpha_2}^{t_1}} \in K \Rightarrow \dots$$

lemme: les extensions cycliques de degré p de $\mathbb{Q}_p(\mu_p)$ qui sont abéliennes sur \mathbb{Q}_p sont de la forme $L(\mu_p)$ (L/\mathbb{Q}_p cyclique de degré p), correspondent aux sous-groupes d'ordre p



de $\left[\mathbb{Q}_p(\mu_p)^x / (\mathbb{Q}_p(\mu_p))^x \right]^{\times}$, où V^x pour tout $\sigma \in \text{Gal}(\mathbb{Q}_p(\mu_p)/\mathbb{Q}_p)$ -module V , $V^x = \{v \mid \sigma(v) = x(\sigma) \cdot v\}$, et $x \in \text{Gal}(\mathbb{Q}_p(\mu_p)/\mathbb{Q}_p) \xrightarrow{\sim} (\mathbb{Z}/(p))^\times$ est le caractère cyclotomique.

Dém. Soit $E/\mathbb{Q}_p(\mu_p)$ cyclique d'ordre p . On a donc q racines de $\mathbb{Q}_p(\mu_p)(\sqrt[p]{\alpha})$ dans E et on veut que E/\mathbb{Q}_p soit abélienne.

Supposons que ce soit le cas.

Soit d'abord $\sigma \in \text{Gal}(\mathbb{Q}_p(\mu_p)/\mathbb{Q}_p)$, il existe $\tilde{\sigma} \in \text{Gal}(E/\mathbb{Q}_p)$ tel que $\tilde{\sigma}(\mathbb{Q}_p(\mu_p)) = \sigma$.

On a $\tilde{\sigma}(\sqrt[p]{\alpha}) \in E$ et $\tilde{\sigma}\alpha = \alpha^t \tilde{\sigma}$ (par (b) ci-dessous) pour un $t \in \mathbb{Z}$.

Notons τ l'élément de $\sqrt{a} \mapsto \sqrt[p]{a}$ de

$\text{Gal}(E/\mathbb{Q}_p(\mu_p))$.

Par définition, $\tilde{\sigma} : S \hookrightarrow S^{x(\sigma)}$

Écrivons maintenant $\tilde{\sigma}\tau = \tau \tilde{\sigma}$ en $\sqrt[p]{a}$: on conclut que $t = x(\sigma)$.

Lemme 2. Soit $n = 1 - 5$, $\mathcal{O} = \mathbb{Z}_p[5]$.

L'ensemble des puissances p -èmes dans $1 + \pi \mathcal{O}$ est

$1 + \pi^{p+1} \mathcal{O}$ si $p \neq 2$ l'application naturelle

$$\frac{1 + \pi \mathcal{O}}{1 + \pi^{p+1} \mathcal{O}} \hookrightarrow \frac{\mathbb{Q}_p(\mu_p)^x}{(\mathbb{Q}_p(\mu_p))^x}.$$

induit un isomorphisme des π -espaces propres correspondants.

$$\text{Dém. } \rho = (1-5)^{p-1} \cdot \frac{(1-5)(1-5^2)\dots(1-5^{p-1})}{(1-5)^{p-1}}$$

$$= (1-5)^{p-1} u_0, \text{ où } u_0 \text{ est une unité.}$$

$$u_0 = (1+5)(1+5+5^2)\dots(1+5+\dots+5^{p-2}) V \exists \rho \text{ si } \\ u_0 = 2 \cdot 3 \dots (p-1) = (p-1)! \pmod{\pi}$$

$$\rho \equiv -1 \pmod{\pi} \text{ et on peut prendre } \tilde{\rho} = \rho + \pi^{p+1}$$

Maintenant, si $x \in 1 + \pi \mathcal{O}$, $x^p \in 1 + \pi a + \pi^2 b$, on a

$$x^p = (1 + \pi a + \pi^2 b)^p = 1 + p\pi a + \pi^p a^p \pmod{\pi^{p+1}}$$

$$= (1 + \pi u_0 a + \pi u_0 \pi^2 a^p) \pmod{\pi^{p+1}}$$

$$= 1 + \pi^p (au_0 + a^p) = 1 \pmod{\pi^{p+1}}$$

or $au_0 + a^p \equiv -a + a^p \pmod{\pi}$, on peut choisir a entier donc $\pi^p \nmid au_0 + a^p$ et $\pi \nmid au_0 + a^p$.

Donc $\rho \equiv (1 + \pi \mathcal{O})^p \pmod{1 + \pi^{p+1} \mathcal{O}}$.

Réiproquement, soit $\epsilon \equiv 1 \pmod{\pi^{p+1}}$; on veut résoudre $x^p \equiv \epsilon$

avec $\epsilon \equiv 1 \pmod{\pi}$. On réhabilite un cas particulier du lemme de Hensel : supposons donné $\epsilon_i \in 1 + \pi^i \mathcal{O}$ avec $i \leq p+1$.

Alors $\epsilon_i^p \equiv \epsilon_i \pmod{\pi^i}$ et $\epsilon_i^p \equiv \epsilon_{i+1} \pmod{\pi^{i+1}}$.

Alors $\epsilon_i \rightarrow \epsilon$ une limite et $\epsilon_i^p = \epsilon_{i+1}$ construit donc ϵ .

On commence par $\epsilon_{p+1} = 1$, alors $\epsilon_i^p = \epsilon_{i+1}$.

Calculons $\frac{\epsilon_i^p - \epsilon_{i+1}}{\pi^p} = 1 + a_i \pi^i \pmod{\pi^{i+1}}$ (*)

et à définition, $\epsilon_{i+1} = \epsilon_i (1 + a_i \pi^{i+1})$

et ça marche : $\epsilon_{i+1}^p = \epsilon_i^p (1 + a_i \pi^{i+1})^p = \epsilon_i^p (1 + a_i \pi^{-p+1})$

$(\epsilon_i^p)^p = \epsilon_i^p (1 + a_i \pi^{-p+1})^p = \epsilon_i^p (1 + a_i \pi^{-p+1})$

$= \epsilon_i^p (1 + a_i \pi^i) \pmod{\pi^{i+1}}$

$= \epsilon$ par (*).

Cela nous donne donc la flèche désirée :

$$\frac{1+\pi^0}{1+\pi^{p+1}0} \hookrightarrow \mathbb{Q}_p(\mu_p)^\times / (\mathbb{Q}_p(\mu_p)^\times)^p$$

Si $\bar{x} \in V^X$ ($x \in \mathbb{Q}_p(\mu_p)^\times$), écrivons $x = (\bar{x}, \eta)$ où

$$x = \pi^h (\eta^{-1})$$

avec $\eta \in \mathcal{O}^\times$, et écrivons la condition pour $\bar{x} \in V^X$:

$$\sigma(x) = \sigma(\bar{x})^h \cdot \sigma(\eta) = 1 \quad (\text{condition})$$

$$\Rightarrow \bar{x}^{\pi(\sigma)} \beta^p = \pi^{\pi(\sigma)h} \eta^{\pi(\sigma)} \beta^p$$

$$\Rightarrow \bar{x}^{\pi(\sigma)} h = h \pmod{p}$$

Si p est impair, $\pi^{\pi(\sigma)} \neq 1$ donc $h=0 \pmod{p}$, i.e. on peut écrire $\bar{x} = \bar{x}'$ avec $\bar{x}' \in \mathcal{O}$.

De même on voit facilement que $\mathcal{O}/1+\pi^0$ n'intervient pas dans l'espace propre.

Corollaire: Si $p \neq 2$, l'extension abélienne maximale de \mathbb{Q}_p d'exposant p est de degré p^2 , donc elle est obtenue en joignant des racines de l'unité de degré p^2 à l'extension non-ramifiée de degré $p+1$.

Dém. On veut montrer que

$$\left| \left(\frac{1+\pi^0}{1+\pi^{p+1}0} \right)^X \right| = p^2$$

Soit \bar{x} dans cet espace propre (remarquons que $5=1-\pi$ vérifie $\sigma 5 = 5^{\pi(\sigma)}$ i.e. 5 est tordus); en multipliant par une puissance de 5 on peut supposer $u \equiv 1 \pmod{p^2}$.

Écrivons plus généralement $u \equiv 1 + a\pi^i \pmod{p^{i+1}}$; on a

$$a \in \mathbb{Z}$$

$$\frac{\sigma(\pi)}{1-\pi} = \frac{1-\pi^{\pi(\sigma)}}{1-\pi} = 1 + \pi^i + \dots + \pi^{\pi(\sigma)-1}$$

alors $\sigma(u) = 1 + a\pi^i \pi^{\pi(\sigma)} + \dots + \pi^{\pi(\sigma)-1}$

$$= (1+a\pi^i)^{\pi(\sigma)} \pi^{\pi(\sigma)-1}$$

Fait : on trouve alors

$$a\pi^i \pi^{\pi(\sigma)} = a\pi^{\sigma(\sigma)} \pmod{p^{i+1}}$$

i.e. soit $a\pi = 0 \pmod{p^i}$

soit $a \equiv 0 \pmod{p^i}$

Donc on peut écrire

$$(1+\pi^0/1+\pi^{p+1}0)^X = < 5, 1+\pi^p >$$

d'où

$$\left(\frac{1+\pi^0}{1+\pi^{p+1}0} \right)^X = < 5, 1+\pi^p >^2$$

Rappelons que l'on cherche $(\mathbb{Q}_p(m)/\mathbb{Q}_p)$, l'extension abélienne maximale de \mathbb{Q}_p d'exposant m , qui contient l'extension non-ramifiée de degré m et l'extension cyclotomique inclus dans $\mathbb{Q}_p(\mu_{p^m})$.

$$\text{On a } \text{Gal}(\mathbb{Q}_p(m)/\mathbb{Q}_p) = \mathbb{Z}/(p^m) \times \text{Gal}(\mathbb{Q}_p(m))$$

et le nombre de facteurs $\mathbb{Z}/(p^m)$ est le même que dans

$$\text{Gal}(\mathbb{Q}_p(1)/\mathbb{Q}_p) = \mathbb{Z}/(p) \times \mathbb{Z}/(p)$$

qui est, on l'a vu précédemment, $p-1$.

$$\text{Gal}(\mathbb{Q}_p(1)/\mathbb{Q}_p) = \mathbb{Z}/(p) \times \mathbb{Z}/(p)$$

$$\text{d'où } \text{Gal}(\mathbb{Q}_p(m)/\mathbb{Q}_p) = \mathbb{Z}/(p^m) \times \mathbb{Z}/(p^m)$$

ce qui montre la validité du lemme (auquel il faut ajouter)

Cela finit la démonstration pour p impair.

Le cas $p=2$: $(\mathbb{Z}/(2^m))^\times$ est un groupe cyclique de $\deg(\mathbb{Q}_2(\mu_{2^m})/\mathbb{Q}_2) = 2^{m-1}$.
on a alors $\text{Gal}(\mathbb{Q}_2(\mu_{2^m})/\mathbb{Q}_2) \cong (\mathbb{Z}/(2^m))^\times$, qui n'est plus cyclique: c'est isomorphe à

$$\mathbb{Z}/(2) \times \mathbb{Z}/(2^m)$$

cela donne 3 facteurs cycliques.

On doit donc vérifier que $\mathbb{Q}_2(2 \pm 10)$ tienne.

$$\text{Gal}(\mathbb{Q}_2(2)/\mathbb{Q}_2) \cong \mathbb{Z}/(2) \times \mathbb{Z}/(2^m) \times \mathbb{Z}/(2^m)$$

Pour $m=1$: on cherche les extensions quadratiques de \mathbb{Q}_2 .
Cette fois, par Kummer, c'est classifié par $\mathbb{Q}_2^\times / (\mathbb{Q}_2^\times)^2$ qui est directement

$$2^{\infty} \langle -1, 5 \rangle$$

\Rightarrow 3 facteurs, trois extensions

$$\mathbb{Q}_2(2), \mathbb{Q}_2(\sqrt{-1}), \mathbb{Q}_2(\sqrt{5})$$

(non ramifiée)

Retour au cas $p=2$:

Th. (version locale de th. de Kronecker-Weber)

Soit L/\mathbb{Q}_p une extension cyclique de degré p^m . Alors L est contenue dans une extension obtenue en adjoignant des racines de l'unité à une extension non-ramifiée.

Dém. Pour m donné, on notait $\mathbb{Q}_p(m)$ l'extension abélienne maximale d'exposant p^m de \mathbb{Q}_p .

On cherche $\text{Gal}(\mathbb{Q}_p(m)/\mathbb{Q}_p)$, abélien d'exposant p^m .

Quand $p=2$, on a vu que $\deg(\mathbb{Q}_p(1)/\mathbb{Q}_p) = p^2$, ce qui implique qu'en général $\text{Gal}(\mathbb{Q}_p(m)/\mathbb{Q}_p)$ ait deux générateurs. Comme on connaît déjà deux extensions disjointes dans $\mathbb{Q}_p(m)$ de groupe de Galois $\mathbb{Z}/(p^m)$, cela termine ce cas.

Pour $p=2$:

$$\begin{array}{ccc} \mathbb{Q}_2(m) & & \\ \text{non-ramifiée} & \nearrow & \searrow \\ \mathbb{Q}_2 & & \mathbb{Q}_2(\mu_{2^m}) \end{array}$$

$$\text{cyclique} \quad \mathbb{Z}/(2^m) \cong \mathbb{Z}/(2) \times \mathbb{Z}/(2^m)$$

On veut montrer que $\text{Gal}(\mathbb{Q}_2(m)/\mathbb{Q}_2)$ a trois générateurs,

$$\text{Gal}(\mathbb{Q}_2(m)/\mathbb{Q}_2) \cong \mathbb{Z}/(2) \times \mathbb{Z}/(2^m) \times \mathbb{Z}/(2^m)$$

On peut encore utiliser le cas $m=1$ pour déterminer le nombre de générateurs.

(cas $m=1$): $\mathbb{Q}_2(1)$ est composé des extensions quadratiques de \mathbb{Q}_2 . Par théorie de Kummer, c'est déterminé par

$$\mathbb{Q}_2^\times / (\mathbb{Q}_2^\times)^2 = \langle -2, -1, 5 \rangle$$

$$\Rightarrow \text{Gal}(\mathbb{Q}_2(1)/\mathbb{Q}_2) \cong (\mathbb{Z}/(2) \times \mathbb{Z}/(2) \times \mathbb{Z}/(2))$$

Cas général: on sait que $\text{Gal}(\mathbb{Q}_2(m)/\mathbb{Q}_2)$ a trois facteurs cycliques, comme on connaît deux quotients d'ordre 2^m , ce doit être de la forme $\mathbb{Z}/(2) \times \mathbb{Z}/(2^m) \times \mathbb{Z}/(2^m)$.

$$\text{Gal}(\mathbb{Q}_2(m)/\mathbb{Q}_2) \cong \mathbb{Z}/(2^m) \times \mathbb{Z}/(2^m) \times \mathbb{Z}/(2^m)$$

et il faut montrer que $j \leq 1$.

Il suffit de compléter à calculer $\text{Gal}(\mathbb{Q}_2(2)/\mathbb{Q}_2)$.

$$\text{On a } \text{Gal}(\mathbb{Q}_2(2)/\mathbb{Q}_2) = \langle \sqrt[4]{a}, \sqrt[4]{x+y\sqrt{a}} \rangle \text{ d'après}$$

La discussion précédente et il faut noter que $\sigma^j = 1$.

$$\text{Si } j \neq 1, \text{ alors } \text{Gal}(\mathbb{Q}_2(2)/\mathbb{Q}_2) = \langle \sqrt[4]{a}, \sqrt[4]{x}, \sqrt[4]{y\sqrt{a}} \rangle$$

Alors toute extension quadratique de \mathbb{Q}_2 (en particulier,

$\mathbb{C}(\mathbb{Q}_2(2))$) serait incluse dans une extension cyclique de degré

$$4.$$

lemme. Soit F un corps de caractéristique $\neq 2$, et supposons que $F(\sqrt{a})$ soit contenu dans une extension cyclique de degré

$$4. \text{ Alors } a = u^2 + v^2 \text{ avec } (u, v) \in F \times F.$$

On applique cela à $\mathbb{Q}_2(\sqrt{-1})$: cela dit que $\mathbb{Q}_2(\sqrt{-1})$

n'est pas contenue dans une extension cyclique de degré 4,

car $-1 = u^2 + v^2$ est impossible modulo 4.

Cela termine instantanément l'histoire !

Preuve du lemme

Supposons $F(\sqrt{a}) \subset K$, K/F cyclique de degré 4.

On doit avoir

$$K = F(\sqrt{a}, \sqrt{x+y\sqrt{a}})$$

par théorie de Kummer.

Fait: $G = \text{Gal}(K/F)$ est engendré par:

$$\sigma: \begin{cases} \sqrt{a} \mapsto -\sqrt{a} \\ \sqrt{x+y\sqrt{a}} \mapsto \sqrt{x+y\sqrt{a}} (r+s\sqrt{a}) \end{cases}$$

(N.B. $F(\sqrt{x+y\sqrt{a}}) = K$ par normalité)

$$\Rightarrow \sqrt{x+y\sqrt{a}} = (x+y\sqrt{a})(r+s\sqrt{a})^2 \text{ (par théorie)}$$

de Kummer (encore) $[\sigma, \sigma] = \sigma^2 \in \langle \sigma^2 \rangle = \langle \sigma^2 \rangle H$

On calcule σ^2 qui doit être non-trivial:

$$\sigma(\sqrt{a}) = \pm \sqrt{a} \text{ car } \sigma^2 \in \langle \sigma^2 \rangle$$

$$\Rightarrow \sigma^2(\sqrt{x+y\sqrt{a}}) = -\sqrt{x+y\sqrt{a}} \text{ nécessairement}$$

Mais aussi $\sigma^2(\sqrt{x+y\sqrt{a}}) = \sqrt{x+y\sqrt{a}} \cdot (r+s\sqrt{a})(1-s\sqrt{a})$

$$\Rightarrow r^2 - as^2 = -1$$

$$r^2 + 1 = as^2$$

$$\left(\frac{r}{s}\right)^2 + \left(\frac{1}{s}\right)^2 = a$$

si $s \neq 0$, ce qui est équivalant (par la M. 1.2)

$$\square \quad (\tau, \delta) \text{ tel que } = \langle \tau, \delta \rangle H$$

Cela conduit l'épisode $GL(1)$ de cette étrange histoire...

Le chapitre suivant: Cohomologie, le retour

$M(\tau, \delta)$ On va donner le formalisme des groupes de cohomologie. Les preuves viendront plus tard.

Soit donc G un groupe profini, M un G -module (continu).

$$C^0(G, M) = \{f: G \times \text{Lie}(G) \rightarrow M \mid f \text{ continue}\}$$

On a

$$\text{morphisme: } C^0(G, M) \rightarrow C^{0+1}(G, M)$$

$$\text{évalué: } (g_1, \dots, g_n) \mapsto (df: (g_1, \dots, g_n) \mapsto g_1 f(g_2, \dots, g_n))$$

$$= \sum_{i=1}^n (-1)^i f(g_1, \dots, g_i g_{i+1}, \dots, g_n) + (-1)^{n+1} f(g_1, \dots, g_n)$$

$$H^0(G, M) = \text{Ker}(d: C^0(G, M) \rightarrow C^1(G, M))$$

(Im(d: C^0 \rightarrow C^1))

ce sont des groupes abéliens.

$$\text{N.B. } H^0(G, M) = M^G, \text{ les invariant de } M$$

$$H^1(G, M) = \left\{ f: G \rightarrow M \mid \begin{array}{l} f(gh) = g f(h) + f(g) \\ f \text{ continue} \end{array} \right\}$$

$\{f: G \rightarrow M \mid \exists b \in M$
 $f(g) = g \cdot b - b\}$

Si M est un G -module triviale, alors on a:

$$H^1(G, M) = \text{Hom}_{\text{cont}}(G, M)$$

Calculs de cohomologie

(1) Si G est fini et cyclique, engendré par σ , on a

$$H^0(G, M) = \text{Ker } N / (\sigma-1)M$$

$$N: M \rightarrow M$$

qui à $m \mapsto (\sum \sigma^i m)$

(2) La suite exacte longue de cohomologie : si on a une suite exacte de G -modules:

$$0 \rightarrow M_1 \rightarrow M_2 \rightarrow M_3 \rightarrow 0$$

on a une suite exacte longue induite:

$$\begin{aligned} 0 &\rightarrow H^0(G, M_1) \rightarrow H^0(G, M_2) \xrightarrow{\delta} H^0(G, M_3) \rightarrow H^1(G, M_1) \rightarrow H^1(G, M_2) \rightarrow \dots \\ &\quad \rightarrow H^{n-1}(G, M_3) \xrightarrow{\delta} H^n(G, M_1) \rightarrow H^n(G, M_2) \rightarrow \dots \end{aligned}$$

Exemples - (i) $G = 1$ (premier si $q=0$)

alors $H^q(G, M) = \begin{cases} \text{entier } n & \text{si } q=1 \\ 0 & \text{si } q \geq 1 \end{cases}$

(ii) (Hilbert) Soit L/K une extension galoisienne, $G = \text{Gal}(L/K)$, et l'étudions $H^q(G, L^\times)$.

alors dans le cas où $q=0$, L^\times est K^\times et $q \geq 1$

$$H^q(G, L^\times) = \begin{cases} \text{entier } n & \text{si } q=0 \\ 0 & \text{si } q \geq 1 \end{cases}$$

Proposition - $(H, 30)$

$$H^1(G, L^\times) = 0$$

Démonstration: Soit $f: G \rightarrow L^\times$ un 1-cocycle, c'est à dire

$$f(gh) = g f(h) f(g)$$

Posons $b = \sum_{h \in G} f(h) h \cdot c$ pour tout $c \in L^\times$ choisi arbitrairement.

Si $b \neq 0$, on calcule que f est solution de

$$\begin{aligned} (g \cdot b) \cdot f(g) &= \sum g f(h) \cdot (gh) \cdot c \\ (g \cdot b) \cdot f(g) &= \sum g f(h) f(g)^{-1} \cdot (gh) \cdot c \\ &= f(g)^{-1} b \end{aligned}$$

$$\text{i.e. } f(g) = \frac{b}{g b^{-1}} \quad (\text{si } g \cdot b \neq 0, \text{ toujours})$$

Maintenant, il existe c tel que $b \neq 0$ par le théorème d'indépendance linéaire des automorphismes. Cela donne donc

$$\Rightarrow H^1(G, L^\times) = 0$$

(iii) (Théorie de Kummer)

Soit L/K une extension galoisienne et considérons la flèche $L^\times \xrightarrow{n} L^\times$; cela donne la suite exacte

$$1 \rightarrow \mu_n(L) \rightarrow L^\times \xrightarrow{n} L^\times \xrightarrow{\text{Res}} H^1(G, \mu_n(L)) \rightarrow 1$$

On montre que le Th. de Hilbert reste valide pour une extension infinie.

Pour exemple pour $L = K^{(p)}$, cela donne

$$1 \rightarrow \mu_n(L) \rightarrow L^\times \xrightarrow{n} L^\times \xrightarrow{\text{Res}} H^1(G, \mu_n(L)) \rightarrow 1$$

d'où la suite exacte longue

$$1 \rightarrow \mu_n(K) \rightarrow K^\times \xrightarrow{n} K^\times \xrightarrow{\text{Res}} H^1(G, \mu_n(L)) \rightarrow H^1(G, L^\times) \rightarrow \dots$$

$$\Rightarrow H^1(G, \mu_n(L)) \cong K^\times / (K^\times)^n$$

Si K contient les racines n -èmes de l'unité, on trouve $H^1(G, \mu_n(L)) \cong \text{Hom}_{\mathbb{Z}/(n)}(G, \mu_n(L))$. L'action triviale $\rho = \text{Hom}(G, \mathbb{Z}/(n))$ ie on a

$$\text{Hom}(G, \mathbb{Z}/(n)) \cong K^\times / (K^\times)^n$$

Cela redonne la théorie de Kummer!

Calculs de cohomologie, 2

(3) Restriction: soit $H \leq G$ un sous-groupe.

On a une flèche triviale $\text{Res}: C^*(G, M) \rightarrow C^*(H, M)$

qui induit pour tout $q \geq 1$ une flèche naturelle

$$H^q(G, M) \xrightarrow{\text{Res}} H^q(H, M)$$

avec (4) Co-restriction: soit $H \triangleleft G$ d'indice fini n .

Alors il existe une flèche naturelle

$$H^q(H, M) \xrightarrow{\text{Core}} H^q(G, M)$$

Dans le cas où $q=0$: tout avec transcription est (3).

$$\begin{aligned} M^G &\xrightarrow{\text{Res}} M^H \\ \text{traversant} \quad \{ M^H \xrightarrow{\text{Core}} M^G \} &= \text{traversant} \\ (m) &\mapsto \sum_{g \in G/H} g m \end{aligned}$$

Observation: soit $H \triangleleft G$ d'indice fini; on a la composition

$$H^q(G, M) \xrightarrow{\text{Res}} H^q(H, M) \xrightarrow{\text{Core}} H^q(G, M)$$

qui est Coreo o Res = multiplication par n .

Séminaire
Tunnell

1/12

Conducteurs de variétés et de représentations

On appelle conducteur d'une variété V sur \mathbb{F}_p le nombre

On sait associer ces jolis nombres à des représentations ℓ -adiques...

Déf.: Soit G un groupe profini. Un homomorphisme continu

vers $GL(n, \mathbb{Q}_\ell)$ est appelé une représentation ℓ -adique.

N.B.: (i) Soit ρ une représentation ℓ -adique. Alors il existe $T \in \mathbb{Q}_\ell^n$ un réseau invariant par ρ ($T \subseteq \mathbb{Z}_\ell^n$). Le après changement de base, on peut supposer $\rho: G \rightarrow GL(n, \mathbb{Z}_\ell)$...

Dém. Soit $T \in C(\mathbb{Q}_\ell)$ n'importe quel réseau (ex: \mathbb{Z}_ℓ).
Par continuité, si $L \subset C(\mathbb{Q}_\ell)$, étant ouvert, l'ensemble des $g \in G$ tels que $p(g)L \subset L$ est également ouvert.

G est profini donc $H \subset G$ est un sous-groupe d'indice fini, et $\sum_{g \in G/H} gLg^{-1} = L$ est un réseau stable pour l'action de G (idem $C(\mathbb{Q}_\ell)$).

D

(ii) Par conséquent pour toute représentation ℓ -adique,

$$p: G \rightarrow GL(n, \mathbb{Q}_\ell)$$

il existe $L \subset C(\mathbb{Q}_\ell)$ réseau tel que p induit

$$\bar{p}: G \rightarrow \text{Aut}(L) \cong GL(n, \mathbb{Z}_\ell)$$

que l'on peut réduire modulo ℓ , obtient

$$p: G \rightarrow GL(n, \mathbb{Z}/\ell\mathbb{Z}) \cong GL(n, \mathbb{Z}_\ell^\ell)$$

ie le genre de représentations considérées par Serre (il

peut dépendre de L , mais on montre que sa semi-simplification n'en dépend pas).

Conducteur (à l'ordre ℓ au moins)

Soit K un corps, extension finie de \mathbb{Q}_p , E/K une extension galoisienne finie (ℓ -stable), non triviale.

Pour toute représentation $\rho: \text{Gal}(E/K) \rightarrow \text{Aut}(V)$, on a attaché un nombre $a(V)$ via la formule

$$a(V) = \sum_{i=0}^{\ell-1} \frac{1}{[G_i : G_0]} \dim(V/G_i)$$

$a(V)$ est un entier, appelé ℓ -exposant du conducteur d'Artin en p .

pb: comment généraliser cette notion à une extension ℓ -finie?

Si p , ou même p/I_ℓ , (se factorise par un quotient plus) utilise la même formule.

En général, si ρ dépendant, une représentation ℓ -adique de G_K dans $GL(n, \mathbb{Q}_\ell)$ n'est pas triviale sur un sous-groupe d'indice fini des sous-groupes d'inertie. D'où la définition

(conducteur à l'ordre ℓ)

On a une filtration $\rho(I_\ell) \subset \rho(I_{\ell^2}) \subset \dots \subset \rho(K)$

et I_ℓ est un sous-groupe de ρ -groupe d'inertie

stratégique (cf. p. 100)

Ex. $n=20$, considérons $(p)G_K$ flag des éléments $\ell^n/q\mathbb{Z}$, $\ell|q$, $p \nmid \ell$
et les éléments d'ordre ℓ^n dans $\overline{\mathbb{K}}/\mathbb{Z}$.

soit $\xi \in \mathbb{K}^\times$ tel que $\xi^{\ell^n} = 1$, racine primitive
 $\zeta = \sqrt[\ell^n]{q}$

engendrent ce sous-groupe de $\overline{\mathbb{K}}/\mathbb{Z}$ ie il est $\cong \mathbb{Z}_{(\ell^n)} \times \mathbb{Z}_{(\ell^n)}$

A la limite (cela) donne une représentation ℓ -adique

sur $G_K \rightarrow GL(2, \mathbb{Z}_\ell)$

(où on écrit $V = \varprojlim (\overline{\mathbb{K}}/\mathbb{Z})[\ell^n]$ et $\text{Aut } V \cong GL(2, \mathbb{Z}_\ell)$).

On a une base naturelle de V fournie par les ξ et ζ ,

ce qui donne $\rho = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in GL(2, \mathbb{Z}_\ell)$

$$\rho(q) = \begin{pmatrix} \pi(q) & \star(q) \\ 0 & 1 \end{pmatrix} \in GL(2, \mathbb{Z}_\ell)$$

Si $q \in I_\ell$, comment $\ell \nmid p$, $\pi \in K^\times$, on a

$$\rho(q) = \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$$

Mais si α n'est jamais nul sur \mathbb{F}_q , il existe fini, car $|q|_p < 1$, donc en prenant $\sqrt[p]{q}$ pour α tendant vers ∞ , on a de plus en plus de ramifications, donc $\sqrt[p]{q}$ ne peut pas être une extension finie de \mathbb{F}_q .

Comment fait-on alors ?

Théorème 1. (Grothendieck)

Soit $G_K = \text{Gal}(\bar{K}/K)$, où K/\mathbb{Q}_p est une extension finie, et ρ une représentation ℓ -adique de G_K . Alors il existe un sous-groupe d'indice fini $I' \subset I$ de I tel que pour $g \in I'$, $\rho(g)$ est unipotente, i.e. toutes les valeurs propres de $\rho(g)$ sont égales à 1.

On utilise cela pour définir le conducteur.

Rappel : structure de G_K : on a la filtration naturelle

avec : (1) $G_K/I = \text{Gal}(K^{\text{ur}}/K) = \text{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q)$, topologiquement engendré par un élément noté $F_{\mathbb{F}_q}$.

$$\text{Dès } \mathbb{F}_p \text{ (2) } I/p = \text{Gal}(K^{\text{ur}}/K^{\text{ur}}) \cong \varprojlim (\mathbb{F}_{q^n})^*$$

$$\cong \prod_{\ell \neq p} \mathbb{Z}_\ell$$

P est un pro- p -groupe.

$$\text{De plus pour } h \in I/p, \quad F_{\mathbb{F}_q} h F_{\mathbb{F}_q}^{-1} = h^q \quad (*)$$

Et en fait on va seulement utiliser cette structure de G .

Choisirons un $\ell \neq p$ et une application $t_\ell : I/p \rightarrow \mathbb{Z}_\ell$: vu (2), t_ℓ est unique modulo \mathbb{Z}_ℓ^\times . $t_\ell(g)$

On peut alors énoncer :

Théorème 1' Sous les hypothèses du Th. 1, il existe $I' \subset I$ d'indice fini, tel que pour l'ig. $E(I')$ on ait

$$t_\ell(g) = \exp(t_\ell(g)N) \quad \text{où } N \in M_n(\mathbb{Q}_\ell)$$

où $N \in M_n(\mathbb{Q}_\ell)$ est une matrice nilpotente.

N.B. N nilpotente $\Rightarrow \exp(N)$ est même pas une série...

$$\rho(g) = I + N_g \quad \text{avec } N_g \text{ nilpotente, donc Th. 1' } \Rightarrow \text{ Th. 1.}$$

Ex. Dans le cas de l'exemple précédent on a

$$\text{et on a } t_\ell(I) = \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \in GL(2, \mathbb{Z}_\ell) \text{ fini.}$$

donc on a $t_\ell(I) = \langle \tau \rangle \mathbb{Z}_\ell$ avec $\tau(1), \tau(2), \tau(3)$ on doit avoir $\tau = ct_\ell$, ce qui donne le Th. 1' avec $N = \begin{pmatrix} 0 & c \\ 0 & 0 \end{pmatrix}$.

Comment exploite-t-on ce théorème ?

On a $G_K \xrightarrow{\rho} \text{Aut}(V)$, V : \mathbb{Q}_p -v. de dimension finie.

On considère la semi-simplification ρ'' de ρ , agissant

$$\text{sur } V'' = \bigoplus V_i / \text{v. irréductible } \text{une repr } \ell\text{-adique}$$

Corollaire : si V est semi-simple*, alors il existe $I' \subset I$ d'indice fini agissant trivialement sur V .

Dém. Il suffit de considérer le cas où V est irréductible.

La th. 1' fournit $I' \subset I$ d'indice fini et $N : V \rightarrow V$ l'op-

* comme représentation de $W_K = \langle I, F_r \rangle$

Or, $\ker N \cap V$ est stable par W_K .

Si $w \in W_K$, on calcule $\rho(wgw^{-1})$ et on obtient

$$\rho(w)N\rho(w^{-1}) = q^{n_w}N$$

(avec $n_w = 0$ si $w \in I$, $n_w = 1$ si $w = Fr$, et est additif).

En effet, $\rho(wgw^{-1}) = \exp(t_{\ell}(g)\rho(w)N\rho(w)^{-1})$ d'un côté, et de l'autre on utilise la formule (*).

Cette formule donne le résultat, et par semi-simplicité elle donne $N = 0$ et donc $\rho|I^{\perp} = Id$.

On peut maintenant donner la définition.

Définition: soit $\rho: G_K \rightarrow GL(n, \mathbb{Q}_{\ell})$ une représentation ℓ -adique. L'exposant $a(\rho) = a(V)$ du conducteur d'Artin de ρ est

$$a(V) = a(V^{ss}) + \dim(V^{ss})^I - \dim V^I$$

où $a(V^{ss})$ est donné par la formule nouvelle (ce qui est bien défini d'après le corollaire).

N.B. (i) Dans notre exemple, $\rho = \sigma \otimes \chi$ et $\rho|I = \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$

Que vaut $a(\rho)$?

On a $\rho^{ss} = 1 \oplus 1$ i.e. $a(\rho^{ss}) = 0$.

Mais $\dim(\rho^{ss})^I = 2$ et $\dim \rho^I = 1$, donc

$a(\rho) = 1$ dans ce cas.

(ii) On peut démontrer la formule de la page suivante:

$$a(V) = \sum_{i=0}^{\infty} \frac{\dim V^{ss}/V^{ss}G_i}{[G_0 : G_i]} + \dim(V^{ss})^I - \dim V^I$$

$$= \dim V^{ss} - (\dim V^{ss})^I + \sum_{i \geq 1} \frac{\dim(V^{ss}/V^{ss}G_i)}{[G_0 : G_i]}$$

$$= \dim V/V^I + sw(V)$$

conducteur de Swan

(iii) Considérons $\rho' = \rho \otimes \chi$: si χ est ramifié

$$a(\rho') = 2a(\chi) + 0 = 0 = a(\chi)$$

Première partie du théorème 1':

On va regarder $(K')^{\perp}$ pour K'/K extension finie: il suffit de montrer que $\rho|_{(K')^{\perp}}$ est pro- ℓ .

et on peut déjà choisir K' de sorte que (on suppose que K vérifie)

$$(*) \quad \rho(I) = Id \pmod{\ell^2}$$

(considérons $GL(n, \mathbb{Z}_{\ell}) \supset [1 + \ell^2 M_n(\mathbb{Z}_{\ell})]$)

soit $S_{\ell} \subset \mathbb{Z}_{\ell}^{\times} \subset \mathbb{Z}^{\times} \otimes \mathbb{Z}_{\ell}$

donc $\rho(I)$ est un pro- ℓ -groupe, le se factorise via

$\rho(I/\ell)$, et dans (2) ci-dessous, on voit que sa se factorise

même via $\rho((I/\ell)/\prod \mathbb{Z}_{\ell})$, sur laquelle on a $t_{\ell}(I)$.

Il suffit alors d'appliquer le lemme de Schur.

On écrit

$$\rho(\sigma) = \exp(t_{\ell}(\sigma)N)$$

avec le log qui converge à cause de (*).

la formule de conjugaison par Fr_q fournit le fait que N est conjuguée à qN : cela implique que les valeurs propres de N sont toutes nulles, i.e. N est nilpotente.

Réduction semi-stable des courbes elliptiques et des variétés abéliennes

Une courbe elliptique sur F un corps est une courbe cubique non-singulière de la forme

$$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6$$

(Si $\text{char } F \neq 2, 3$, on peut se ramener à ce type)

(i.e. $y^2 = x^3 + ax + b$ avec $a, b \in F$ et C non-singulière $\Leftrightarrow 4a^3 + 27b^2 \neq 0$).

L'ensemble des pts de C a une structure de groupe abélien:

$$P + Q + R = O \Leftrightarrow P, Q, R \text{ alignés}$$

Une variété abélienne est une variété projective connexe qui est aussi un groupe algébrique.

Courbes elliptiques \hookrightarrow variétés abéliennes de dim. 1

Pour avoir "explicitement" une variété abélienne:

on part de C , courbe algébrique de genre g , et on considère

la jacobienne $J(C)$ de dimension g .

Si A est une variété abélienne sur C , on a

$$\text{la structure naturelle } A(\mathbb{C}) = \mathbb{C}^d / \Lambda \text{ réseau de } \mathbb{C}^d$$

où Λ est l'ensemble des pts de torsion de $A(\mathbb{C})$

$$\text{et le rang fini de } \Lambda = \frac{1}{n} N/\Lambda \cong (\mathbb{Z}/(n))^{\text{rd}}$$

Th. (Mordell - Weil). Soit A une variété abélienne sur un corps de nombres F . Alors $A(F)$ est un groupe abélien de type fini:

$$A(F) = A(F)_{\text{tors}} \oplus \mathbb{Z}^r$$

groupe fini rang de A

On a un algorithme pour calculer $A(F)_{\text{tors}}$:

Th. (Nagell - Lutz). Soit $E : y^2 = x^3 + ax + b$ une courbe elliptique sur \mathbb{Q} , $a, b \in \mathbb{Z}$.

$$\text{Alors } (x, y) \in E(\mathbb{Q})_{\text{tors}} \Rightarrow x, y \in \mathbb{Z}$$

$y^2 \mid (4a^3 + 27b^2)$

On peut même classifier les groupes $E(\mathbb{Q})_{\text{tors}}$ possibles:

Théorème (Mazur). On a l'un des cas suivants:

$$(i) E(\mathbb{Q})_{\text{tors}} \cong \mathbb{Z}/(n), \quad n = 1, \dots, 10, 12$$

$$(ii) E(\mathbb{Q})_{\text{tors}} = \mathbb{Z}/(2) \times \mathbb{Z}/(2n), \quad n = 1, \dots, 4$$

Conjecture: soit A/K une variété abélienne de dimension d sur un corps de variables K de degré $\leq m$. Il existe une constante

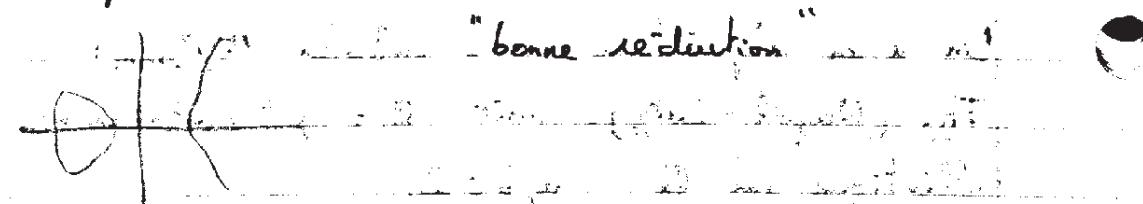
$$C(d, m) \text{ t.q. } |A(F)_{\text{tors}}| \leq C(d, m)$$

N.B. pour $d=1$: th de Mordell
pour $d \geq 2$, ??

Soit E/K une courbe elliptique sur un corps de nombres K .
On peut se ramener à une équation à coefficients dans \mathcal{O}_K ; soit \tilde{E} la réduction de cette courbe modulo $p \in \text{Spec } \mathcal{O}_K$.

Def. E a réduction semi-stable en $p \Leftrightarrow E$ est F -isomorphe à une courbe elliptique \tilde{E} telle que, soit \tilde{E} est non-singulière, soit \tilde{E} a un pt singulier qui est un pt double avec deux tangentes distinctes.

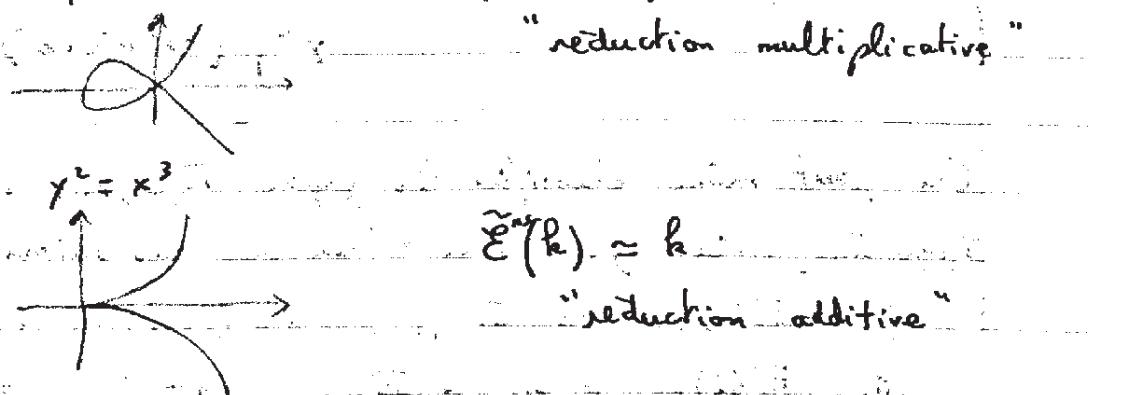
Ex. $y^2 = x^3 - x$



$$y^2 = x^3 + x^2$$

$$\tilde{E}^{\text{ns}}(k) = k^\times$$

"réduction multiplicative"



$$\tilde{E}(k) \simeq k$$

"réduction additive"

Pour une variété abélienne A sur F : pour chaque $p \in \text{Spec } \mathcal{O}_F$
 A a un "bon" modèle sur \mathcal{O}_F , t. j. est formée à
partir de deux types: \tilde{A} et \tilde{A}' telle que
variété abélienne

semi-géométrique (c'est à dire que les fibres sont des groupes additifs simples) ou \tilde{A}' est semi-stable.
Et on dit que A a réduction semi-stable si \tilde{A} n'a pas de partie de type 1 (groupes additifs simples).
De façon générale, A a réduction semi-stable si elle a réduction semi-stable en tout $p \in \text{Spec } \mathcal{O}_F$.

Thm. (Grothendieck): Pour toute variété abélienne A sur F
il existe F'/F extension finie telle que $A \otimes_F F'$ a réduction semi-stable (c'est à dire que \tilde{A} n'a pas de partie de type 1).

On va utiliser le résultat suivant:

Thm. (Wiles - Diamond): Soit E/\mathbb{Q} une courbe elliptique semi-stable en 3 et 5. Alors E est modulaire.

Théorème (Raynaud): Soit A/F une variété abélienne sur un corps de nombres, et $n \geq 3$.

Si $A_n(F) \subset A_n(F)$, alors A est semi-stable en tout $p \nmid n$.

Par Mazur, cela ne peut pas servir à montrer qu'une courbe elliptique E/\mathbb{Q} est semi-stable.
Mais on va généraliser... on va utiliser la théorie des représentations.

On a une dualité $e: A \times A \rightarrow \mu_n$ (en fait, $A \times A^{\vee}$ mais on prend une polarisation) - $(\otimes - \otimes)$ -

Soit $S \subset A_n$ un sous-groupe isotrope maximal.

(ex. tout sous-groupe cyclique d'ordre n sur une courbe elliptique)

Théorème (Zahrin-Silverberg). Soit A/F une variété abélienne, $n \geq 5$ tel que $A_n(F) \supset S$ un sous-groupe isotrope maximal. Alors A est semi-stable en tout $p \nmid n$.

Application: (i) Restrictions sur $A(F)_{\text{tors}}$ si A n'est pas semi-stable en un certain p .

(ii) Construction de familles infinies de courbes elliptiques modulaires:

Corollaire (connu précédemment). E/\mathbb{Q} courbe elliptique, $n \geq 5$.
Iq $E(\mathbb{Q})$ contient un point d'ordre n . Alors E est semi-stable en tout $p \nmid n$.

Corollaire + Wiles/Taylor-Wiles/Diamond + Mazur \Rightarrow soit E/\mathbb{Q} une courbe elliptique telle que $E(\mathbb{Q})_{\text{tors}}$ est l'un des groupes suivants

$$\begin{cases} \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}, n=8, \dots, 10, 12 \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/(2n)\mathbb{Z}, n=1, 2, 3, 4 \end{cases}$$

Alors E est modulaire.

Très explicitement :

$$y^2 + (1-d(d-1))xy - d^2(d-1)y = x^3 - d^2(d-1)x^2$$

($d \in \mathbb{Q} \setminus \{0, 1\}$) est une famille infinie de courbes elliptiques modulaires (car $(0, 0)$ est un point rationnel d'ordre 7).

Théorème (S-Z). Soit A/F une variété abélienne,

$n=2, 3, 4$; tq $S \subset A(F) \supset$ un sous-groupe isotrope maximal de A_n , $p \nmid n$.

Alors pour toute extension galoisienne de F de degré $4, 3, 2$ respectivement totalement ramifiée en p , A a réduction semi-stable en l'idéal premier divisant p .

La preuve du Th. dépend du résultat classique suivant:

Th. (Siegel-Minkowski). Soit α une matrice entière, telle que $\alpha^T = \alpha$ et $\alpha \equiv I \pmod{n}$. Alors si $n \geq 3$, $\alpha = I$.

Généralisation: remplacez " $\alpha \equiv I \pmod{n}$ " par " $(\alpha - I)^k = 0 \pmod{n}$ " (avec $k=2$, cela sert pour la généralisation du Th. de Raynaud).

On utilise aussi le critère de semi-stabilité suivant:

A à réduction semi-stable en $p \Leftrightarrow \forall \sigma \in I_p, (\sigma - 1)^2 = 0$ agissant sur $T_p(A)$.

4/12/95

Outils cohomologiques, 3

(1) La suite exacte longue de cohomologie.

(2) G -profini s'écrit $G = \varprojlim_{U \in G \text{ ouvert}} G/U$

Pour tout G -module A , A^U est un G/U -module et

$$H^q(G, A) = \varprojlim H^q(G/U, A^U)$$

(3) Thm 90 de Hilbert. $H^q(\text{Gal}(L/K), L^\times) = 1$ pour toute extension galoisienne L/K .

Dém. Extension finie puis utiliser (2) \square

(4) La restriction : soit $H \subset G$ un sous-groupe fermé.

Il existe une flèche naturelle

$$\text{Res} : H^q(G, A) \longrightarrow H^q(H, A)$$

[induite par la restriction $f : C^q(G, A) \longrightarrow C^q(H, A)$]

$$f : C^q(G, A) \longrightarrow C^q(H, A)$$

$$f \longmapsto f|_{(H \times \dots \times H)}$$

(5) La co-restriction : soit $H \subset G$ un sous-groupe fermé d'indice fini. Il existe une flèche naturelle

$$\text{Cores} : H^q(H, A) \longrightarrow H^q(G, A)$$

qui, pour $g=0$, est

$$\begin{cases} A^H \longrightarrow A^G \\ a \longmapsto \sum_{g \in G/H} g.a \end{cases}$$

Propriété. Dans cette situation, la composition

$$H^q(G, A) \xrightarrow{\text{Res}} H^q(H, A) \xrightarrow{\text{Cores}} H^q(G, A)$$

est la flèche de multiplication par $[G:H]$.

(6) La suite exacte d'inflation-restriction

Il existe une suite exacte

$$0 \longrightarrow H^q(G/H, A^H) \xrightarrow{\text{Inf}} H^q(G, A) \xrightarrow{\text{Res}} H^q(H, A)$$

pour $H \trianglelefteq G$ normal et fermé.

Si, la ~~flèche~~ flèche d'inflation

$$H \trianglelefteq G \xrightarrow{\text{Inf}} G/H \xrightarrow{\text{Res}} A$$

$$H^q(G/H, A^H) \xrightarrow{\text{Inf}} H^q(G, A)$$

est induite par $f \longmapsto f \circ \text{Res}$.

Dém. (On doit montrer) que $\text{Ker Res} = \text{Im Inf}$, essentiellement.

D'abord : Inf est injective.

Soit f tel que $\text{Inf}(f) = 0$

$$\Leftrightarrow \exists a \in A, \quad \text{Inf}(f)(g) = g.a - a$$

$$f(g) = ga - a$$

Appliquant cela à gh , on déduit que $ha = a$ pour $a \in A$ ie $a \in A^H$ et $f = 0$ dans $H^q(G/H, A^H)$ et Inf est injective.

Ensuite : $\text{Im } (\text{Inf}) = \text{Ker } (\text{Res})$:

(i) $\text{Res} \circ \text{Inf} = 0$. trivialement

(ii) Soit $f \in H^q(G, A)$ telle que $\text{Res } f = 0 \in H^q(H, A)$ ie $\exists a \in A, \forall h \in H, f(h) = ha - a$

La classe de f est la classe de $f - \delta(h)$, donc cela montre qu'on peut supposer $f(h) = 0$ pour $h \in H$.

Pour $g \in G, h \in H$, il vient

$$\begin{aligned} f(gh) &= g f(h) + f(g) \\ &= f(g) \end{aligned}$$

ie f vient d'une application $G/H \rightarrow A$

$$\text{Puis } f(g) = f(hg) = hf(g) + f(h)$$

$$\text{ie } f(g) = hf(g)$$

ie f est en fait $G/H \rightarrow A^H$ ie $f \in \text{Im } (\text{Inf})$.

On peut même préciser cette suite exacte : on a en fait

$$0 \rightarrow H^q(G/H, A^H) \xrightarrow{\text{Ind}} H^q(G, A) \xrightarrow{\text{Res}} H^q(H, A)^{G/H}$$

où G/H agit sur $H^q(H, A)$ via

$$\bar{g} \cdot f(h_1, \dots, h_q) = g \cdot f(g^{-1}h_1g, \dots, g^{-1}h_qg)$$

et on peut prolonger en

$$0 \rightarrow H^1(G/H, A^H) \rightarrow H^1(G, A) \xrightarrow{G/H} H^2(G/H, A^H) \rightarrow H^2(G, A)$$

qui est exacte.

(7) Le lemme de Shapiro :

Lemme. Soit $H \triangleleft G$ un sous-groupe fermé, A un H -module. $\text{Ind}_H^G A$ le G -module induit, (ie

$\text{Ind}_H^G A = \{ \alpha : G \rightarrow A \mid \alpha \text{ continue}, \text{ et } \alpha(hg) = h\alpha(g), \forall h \in H \}$

muni de l'action

$$(ga)(g_1) = \alpha(g_1g)$$

On a un isomorphisme naturel

$$H^q(G, \text{Ind}_H^G A) \cong H^q(H, A)$$

induit par la flèche

$$\begin{cases} \text{Ind}_H^G A & \longrightarrow A \\ \alpha & \longmapsto \alpha(1) \end{cases}$$

$$\text{Ex. } q=0 : H^0(G, \text{Ind}_H^G A) = (\text{Ind}_H^G A)^G = A^H$$

est évident

Applications

(1) Si M est un G -module d'exposant m , alors

$H^q(G, M)$ est d'exposant m .

Dém. Trivial. \square

(2) Si G est un groupe fini, $H^q(G, M)$ est annulé par $|G|$.

[Mais n'est pas nécessairement fini]

Dém. $H^q(G, M) \xrightarrow{\text{Res}} H^q(H, M) \xrightarrow{\text{GRes}} H^q(G, M)$ est multiplication par $|G|$. \square

(2') $H^q(G, M)$ est annulé par $\text{pgcd}(|G|, |M|)$, si G et M sont finis.

Dém. (1) & (2) ... \square

(3) Si G est profini, $H^q(G, M)$ est un groupe abélien de torsion.

Dém. $H^q(G, M) = \varprojlim_{\text{ouvert } H \triangleleft G} H^q(G/H, M^H)$ et (2) \square

(4) Si G est profini, et M est sans torsion avec G -action triviale, alors $H^q(G, M) = 0$.

Dém. $H^q(G, M) = \varprojlim H^q(G/H, M^H) = \varprojlim \text{Hom}(G/H, M) = 0$

(5) Soit M un groupe abélien uniquement divisible. (ie. pour tout $n \in \mathbb{Z}$, $M \xrightarrow{n} M$ est un isomorphisme) Alors $H^q(G, M) = 0$

pour $q \geq 1$.

Dém. On a $0 \rightarrow M \xrightarrow{n} M \rightarrow 0$ qui induit

$$0 \rightarrow H^q(G, M) \xrightarrow{n} H^q(G, M) \rightarrow 0$$

(\square ex $M = \mathbb{Q}$)

(bout de la suite exacte longue)

Par (3), on a $H^q(G, M) = 0$. \square

(6) Considérons la suite exacte

$$0 \rightarrow \mathbb{Z} \rightarrow \mathbb{Q} \rightarrow \mathbb{Q}/\mathbb{Z} \rightarrow 0$$

et faisons agir G trivialement sur ces 3 groupes. Il vient

$$H^r(G, \mathbb{Q}/\mathbb{Z}) \xrightarrow{\delta} H^{r+1}(G, \mathbb{Z})$$

est un isomorphisme pour $r \geq 1$.

Dém. Suite exacte longue, plus (5). \square

Décalage de la dimension

Soit A un G -module continu.

Prop. Il y a une flèche naturelle de G -modules

$$A \rightarrow \text{Ind}_1^G(\text{Res}_1^G A)$$

qui est injective et induite par $a \mapsto [g \mapsto g.a]$

Corollaire. Soit A' le conoyau de cette flèche, c'est à dire

$$0 \rightarrow A \rightarrow \text{Ind}_1^G(\text{Res}_1^G A) \rightarrow A' \rightarrow 0$$

Par le lemme de Shapiro, il vient

$$\boxed{H^{q+1}(G, A) \cong H^q(G, A')}$$

via la flèche de connection.

Dém. (prop.) C'est essentiellement une tautologie. \square

Ex. (calcul d'un H^2 non trivial...) Soit $G = \text{Gal}(\mathbb{C}/\mathbb{R})$

agissant sur \mathbb{C}^\times . On cherche $H^2(G, \mathbb{C}^\times)$.

On calcule $\text{Ind}_1^G(\text{Res}_1^G \mathbb{C}^\times) \cong \mathbb{C}^\times \times \mathbb{C}^\times$ muni de l'action

$$\sigma \cdot (z_1, z_2) = (z_2, z_1)$$

et la flèche de la composition est celle

$$z \mapsto (z, \bar{z})$$

c'est à dire qui donne la suite exacte

$$1 \rightarrow \mathbb{C}^\times \rightarrow \mathbb{C}^\times \times \mathbb{C}^\times \rightarrow \mathbb{C}^\times \rightarrow 1$$

$$(z_1, z_2) \mapsto \frac{z_2}{z_1}$$

Et le second \mathbb{C}^\times est muni de l'action du σ

$$\sigma \cdot w = \frac{1}{w}$$

$$(1, w) \mapsto (w, 1) = (1, \bar{w}) \text{ ds } \mathbb{C}^\times \times \mathbb{C}^\times / (\mathbb{C}^\times)$$

On a alors le diagramme commutatif suivant

$$H^2(G, \mathbb{C}^\times) = H^1(G, (\mathbb{C}^\times)_{\text{tordu}})$$

$$= \text{Ker}(N) / (\sigma-1)(\mathbb{C}^\times)_{\text{tordu}}$$

Le noyau N est

$$N: (\mathbb{C}^\times)_{\text{tordu}} \rightarrow ((\mathbb{C}^\times)_{\text{tordu}})^*$$

$$w \mapsto w \cdot \frac{1}{w} = \frac{w}{w}$$

i.e. $\text{Ker } N = \mathbb{R}^\times$

$$\text{Enfin } (\sigma-1)(w) = \frac{1}{w} = \frac{-1}{\bar{w}w} = \frac{1}{|w|^2} \text{ i.e. } (\sigma-1)(w) = \mathbb{R}^\times$$

et finalement

$$H^2(G, \mathbb{C}^\times) \cong \mathbb{Z}/(2)$$

Interprétation cohomologique de la version locale du Thm.

de Kronecker-Weber

Plus généralement, étudions les extensions abéliennes

de degré p d'un corps K , par des méthodes cohomologiques.

Soit $G_K = \text{Gal}(\bar{K}/K)$; par théorie de Galois, on cherche donc $\text{Hom}(G_K, \mathbb{Z}/(p)) = H^1(G_K, \mathbb{Z}/(p))$, G_K agissant trivialement sur $\mathbb{Z}/(p)$.

Considérons $G_{K(\mu_p)} \triangleleft G_K$; par restriction^{on une flèche}

$$H^1(G_K, \mathbb{Z}/(p)) \xrightarrow{\text{Res}} H^1(G_{K(\mu_p)}, \mathbb{Z}/(p))^{\text{G}_K/G_{K(\mu_p)}}$$

On calcule donc d'abord $H^1(G_{K(\mu_p)}, \mathbb{Z}/(p)) = H^1(G_{K(\mu_p)}, \mu_p)$ car $G_{K(\mu_p)}$ fixe μ_p i.e. $\mathbb{Z}/(p) \cong \mu_p$ comme $G_{K(\mu_p)}$ -modules.

Par la suite exacte de Kummer, il vient

$$H^1(G_{K(\mu_p)}, \mu_p) \cong \mathbb{K}(\mu_p)^*/(\mathbb{K}(\mu_p)^*)^p$$

via l'application

$$\mathbb{K}(\mu_p)/(\mathbb{K}(\mu_p)^*)^p \xrightarrow{\alpha} \mathfrak{d} \xrightarrow{\text{Res}} \begin{cases} \mathfrak{d}\alpha \in H^1(G_{K(\mu_p)}, \mu_p) \\ \sigma \mapsto \frac{\sigma\sqrt[p]{\alpha}}{\sqrt[p]{\alpha}} \end{cases}$$

Soit alors $g \in G_K$; g agit sur $H^1(G_{K(\mu_p)}, \mathbb{Z}/(p))$ via

$$f_g(\sigma) = g(f_\sigma(g^{-1}\sigma g))$$

$$= f_\sigma(g^{-1}\sigma g) \quad (\text{car } \mathbb{Z}/(p) \text{ est } G_K\text{-module trivial})$$

$$= \frac{(g^{-1}\sigma g)(\sqrt[p]{\alpha})}{\sqrt[p]{\alpha}}$$

$$= g^{-1} \left(\frac{\sigma g(\sqrt[p]{\alpha})}{g(\sqrt[p]{\alpha})} \right) = g^{-1} \frac{\sigma(\sqrt[p]{\alpha})}{\sqrt[p]{\alpha}}$$

soit $\sigma \in \mathfrak{d}$, $f_g(\sigma) = g(f_\sigma(g^{-1}\sigma g))$ et donc $\text{ang}^*(\sigma) = \sigma^p$.

Donc \mathfrak{d} est stable par $G_K/G_{K(\mu_p)}$ si et seulement si d vérifie les deux conditions suivantes :

\mathfrak{d} est stable par $G_K/G_{K(\mu_p)}$ si et seulement si

$$\Leftrightarrow \sigma^p = g^{-1}(d) \quad ; \text{ autrement dit}$$

$$\Leftrightarrow \sigma^p \in \mathfrak{d} \quad \text{et} \quad \sigma^p \in \left[\mathbb{K}(\mu_p)/(\mathbb{K}(\mu_p)^*)^p \right]^X$$

sur lequel G_K agit via $G_K \rightarrow (\mathbb{Z}/(p))^*$

donné par l'action sur μ_p

Pour retrouver les résultats précédents, il faut montrer que

Res est un homomorphisme.

Proposition : $\text{Hom}(G_K, \mathbb{Z}/(p)) \xrightarrow{\text{Res}} H^1(G_{K(\mu_p)}, \mathbb{Z}/(p))^{\text{G}_K/G_{K(\mu_p)}}$

Dém : la suite d'inflation-restriction est i.e.

$$0 \rightarrow H^0(\mathbb{Z}/(p)) \xrightarrow{\text{Res}} H^1(G_K, \mathbb{Z}/(p)) \xrightarrow{\text{Res}} H^1(G_{K(\mu_p)}, \mathbb{Z}/(p))^{\text{G}_K/G_{K(\mu_p)}}$$

(puis d'invariant de la restriction, \Rightarrow $H^2(G_K/G_{K(\mu_p)}, \mathbb{Z}/(p)) = 0$)

Mais $G_K/G_{K(\mu_p)}$ est d'ordre $p-1$ premier à p donc

$$H^1(G_K/G_{K(\mu_p)}, \mathbb{Z}/(p)) = 0$$

et de même

$$H^2(G_K/G_{K(\mu_p)}, \mathbb{Z}/(p)) = 0$$

Outils cohomologiques, 3 : le cup-produit

Soient A, B, C trois G -modules et supposée donnée

$$0 \rightarrow A \times B \rightarrow C \otimes_{A \otimes B} \mathbb{Z}/(p)$$

forme bilinéaire θ invariante, si θ vérifie

$$\theta(ga, gb) = g\theta(a, b)$$

(Ex. Soit A un G -module tel que $\alpha A = 0$)

Déf. Le dual de A est $A^* = \text{Hom}(A, \mu_n(\mathbb{Q}))$ muni de l'action :

$$(g\varphi)(a) = g\cdot\varphi(g^{-1}a)$$

L'accouplement dualité entre A et A^* est

$$\langle , \rangle : \begin{cases} A \times A^* \longrightarrow \mu_n(\mathbb{Q}) \\ (a, \varphi) \mapsto \varphi(a) \end{cases}$$

et c'est une forme bilinéaire G -invariante.

$$\langle ga, g\varphi \rangle = (g\varphi)(ga) = g\cdot\varphi(g^{-1}ga)$$

$$= g\cdot\varphi(a) \quad (\text{d'après } \varphi(g^{-1}ga) = g\cdot\varphi(a))$$

Le "coup-produit" est la (les) forme(s) bilinéaire(s) pour $r=0$

$$H^r(G, A) \times H^s(G, B) \longrightarrow H^{r+s}(G, C)$$

$$(\delta, g) \mapsto f_{ug} \quad (\text{ou } f_{ug})$$

qui est

$$(f_{ug})(g_1, \dots, g_r, g_{r+1}, \dots, g_{r+s}) = \theta(f(g_1, \dots, g_r), g_{r+1}, \dots, g_{r+s})$$

Ex. $r=s=0$: $A^G \times B^G \longrightarrow C^G$

$$(a, b) \mapsto \theta(a; b)$$

$$[g\theta(a, b) = \theta(ga, gb) = \theta(a, b)]$$

Cohomologie galoisienne, et ce qu'elle signifie arithmétiquement

Soit K un corps, $G_K = \text{Gal}(K/\mathbb{Q}_p)$ le sous-groupe des éléments

Notation : On note $H^r(G_K, A) := H^r(K, A)$.

Si L/K est une extension, $H^r(L/K, A) \in H^r(\text{Gal}(L/K), A)$.

Théorème (dualité locale) (Tate)

Soit K/\mathbb{Q}_p une extension de degré fini, M un groupe abélien fini muni d'une action de G_K .

(1) $H^r(G_K, M)$ est fini à ptz. $r \geq 0$.

(2) $H^r(G_K, \mu_n) \hookrightarrow \mathbb{Q}/\mathbb{Z}$ de façon compatible avec les injections canoniques $\mu_n \hookrightarrow \mu_{nm}$.

(3) Il existe une dualité parfaite ; pour $i=0, 1, 2$,

$$H^i(G_K, M) \times H^{2-i}(G_K, M^\vee) \longrightarrow H^2(G_K, \mu_n) \hookrightarrow \mathbb{Q}/\mathbb{Z}$$

induite par (2) et le "coup-produit".

(4) Si $p \neq \infty$, $H^i(K, M) = 0$ pour $i \geq 3$, et

$$|H^i(K, M)| = |H^0(K, M)| |H^2(K, M)| \cdot |M \otimes \mathbb{Z}_p|$$

(5) Si $p \neq \infty$, M est d'ordre premier à p , les groupes

$H^i(G_{K/I}, M^\vee)$ (et $H^i(G_{K/I}, (M^\vee)^\vee)$), après inflation de

$H^i(K, M)$ (resp. $H^i(K, M^\vee)$), sont orthogonaux via la dualité

de (3) et sont l'orthogonal l'un de l'autre
même exactement.

Ex.

(1) $H^0(K, M) = M^{G_K}$ est clairement fini si M est fini

Prop. $H^r(K, M)$ est fini.

Dém. Si $M = \mu_n$, on a $H^1(K, \mu_n) = K^*/(K^*)^n$ via la théorie de Kummer, et puisque K est une extension finie de \mathbb{Q}_p , c'est un groupe fini.

Si $p \neq \infty$, ce n'est clair.

Si $p \neq \infty$, on a $K^* = U \times \mathbb{Z}$ avec U/U^n est fini car $U \subset K^*$ est un \mathbb{Z} -groupe compact ouvert et $U^n \subset U$ est ouvert dans U , donc $[U : U^n] < +\infty$.

Dans le cas général, on étudie l'application de saut $G_L \subset G_K$ agit trivialement sur (M, μ_n) à savoir

$$1 \rightarrow H^1(G_K/G_L, M^{G_L}) \rightarrow H^1(G_K, M) \xrightarrow{\text{can}} H^1(G_L, M)$$

fini car les deux arguments sont finis et le sont les deux arguments.

On peut apposer μ_n pour $M \cong \mathbb{Z}/(n)$, et alors

$$H^1(G_K, M) \cong \bigoplus H^1(G_L, \mathbb{Z}/(n))$$

qui est fini par la première étape, et cela conclut.

(2) Un fait fondamental: soit K/\mathbb{Q}_p une extension finie.

$$\text{Alors } H^1(G_K, \mathbb{Z}^*) \cong \mathbb{Q}/\mathbb{Z}$$

(graphe de Brauer)

La suite exacte

$$1 \rightarrow \mu_n \rightarrow \bar{K} \rightarrow \bar{K} \rightarrow 1$$

donne en particulier

$$1 \rightarrow H^1(G_K, \mu_n) \cong \mathbb{Q}/\mathbb{Z} \rightarrow \mathbb{Q}/\mathbb{Z}$$

ce qui donne (2) du théorème.

Le troisième résultat avec condition supplémentaire est

(3) Soit K/\mathbb{Q}_p une extension de degré fini, et $K \supset \mathbb{Q}_p$.

Considérons les représentations de $\mathbb{Z}/(n)$ avec action triviale, $\mu_n = \mathbb{Z}/(n)$ (car $K \supset \mathbb{Q}_p$), et leurs duals :

$(\mathbb{Z}/(n))^* = \text{Hom}(\mathbb{Z}/(n), \mathbb{Z}/(n))$ $\cong \mathbb{Z}/(n)$ comme G_K -module

[et c'est vrai en général, i.e même si $n \notin K$].

La dualité est de la forme $\mu_n \otimes \mathbb{Z}/(n) \rightarrow \mathbb{Z}/(n)$.

$$H^1(K, \mathbb{Z}/(n)) \xrightarrow{\text{can}} H^1(K, \mu_n) \rightarrow H^1(K, \mu_n) \hookrightarrow \mathbb{Q}/\mathbb{Z}$$

de sorte que $K^*/(K^*)^n \cong \mathbb{Z}/(n)$ et $\mathbb{Z}/(n) \cong \mu_n$

et c'est en fait la forme bilinéaire suivante

$$(a, b) \mapsto \left((F\bar{1})^{v(a)v(b)} \frac{a^{v(b)}}{b^{v(a)}} \right)^{\frac{q-1}{n}}$$

(où v est la valuation sur K) et $\bar{1}$ désigne la réduction modulo m_K .

On peut écrire $\mathbb{Z}/(n) \otimes \mathbb{Z}/(n) \rightarrow \mathbb{Z}/(n)$.

On considère l'image de l'inflation, i.e.

$$H^1(G_{K/I}, \mathbb{Z}/(n)) \xrightarrow{\text{inf}} H^1(G_K, \mathbb{Z}/(n)).$$

Fait. L'image est $U_K/\bar{U}_I \hookrightarrow K^*/(K^*)^n$.

On voit alors directement que l'orthogonal de l'image de l'inflation est l'image de $H^1(G_{K/I}, \mathbb{Z}/(n))$ i.e elle-même est orthogonale à U_K/\bar{U}_I .

On obtient ainsi la 3ème partie (vi).

On voit alors directement que l'orthogonal de l'image de l'inflation est l'image de $H^1(G_{K/I}, \mathbb{Z}/(n))$ i.e elle-même est orthogonale à U_K/\bar{U}_I .