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

Séminaire : vendredi 2h50 → 4h10 (425) (Dist ...)

29-9 : 2h50, Hill 425) Tunnell, "Conjecture de Serre"

6-10 : T. Girardi, "Artin Conductor"

H. Weyl Lectures IAS

K. Ribet, oct. 16-17-18-20

Wed 9:50 - 11:10, Hill 525

Tunnell, Fall '95

(I)

d 112, Louis St.

l 249 - 8119

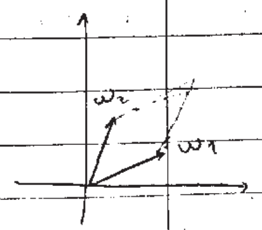
or 545 - 4807

Théorie de Weierstraß des fonctions elliptiques

Soit $\Lambda \subset \mathbb{C}$ un réseau, $\Lambda = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$, $\omega_1, \omega_2 \in \mathbb{C}$ linéairement indépendants sur $\mathbb{R}$.

Déf. Une fonction méromorphe $f : \mathbb{C} \to \mathbb{C}$ est dite elliptique $(/ \Lambda)$ $\iff$ $\forall \lambda \in \Lambda, f(z+\lambda) = f(z)$

Remarques faciles : (i) Si f est entière et elliptique, f est constante (Dém f bornée sur le parallélogramme compact donc sur $\mathbb{C}$ et th de Liouville...)



(ii) On choisit un parallélogramme P tel que f n'a pas de pôles sur le bord.

$$\sum_{\substack{z \text{ pôle} \\ \text{de } P}} \operatorname{Res}_z f \quad \left(= \frac{1}{2i\pi} \int_P f(z)\,dz = 0 \right)$$

(iii) $\#\{\text{zéros de } f \text{ ds } P\} = \#\{\text{pôles de } f \text{ ds } P\}$ $\left(\int_P \frac{f'}{f}(z)\,dz = 0 \right)$

(iv) $\sum_{\substack{a_i \text{ zéro ou pôle} \\ \text{de mult. } m_i}} m_i a_i \in \Lambda$ $\left(\int_P z f'/f(z)\,dz = 0 \right)$

Soit maintenant $\Lambda = \Lambda_\tau = \mathbb{Z} \oplus \mathbb{Z}\tau$, $\tau \in \mathcal{H}$

Le plus simple que l'on peut espérer est une fction elliptique avec un pôle double...

Soit $$\wp_\Lambda(z) = \frac{1}{z^2} + \sum_{\substack{\lambda \in \Lambda \\ \lambda \neq 0}}' \left[\frac{1}{(z-\lambda)^2} - \frac{1}{\lambda^2} \right]$$

C'est une fonction elliptique et elle a un pôle double en 0 (et en tout $\lambda \in \Lambda$) ; on écrit $\wp_{\Lambda_\tau}(z) =: \wp(z,\tau)$

On peut développer en série de Laurent en 0 :

$$\wp(z,\tau) = \frac{1}{z^2} + 3G_4(\tau)z^2 + 5G_6(\tau)z^4 + \dots$$

où $G_k(\tau) = \sum_{(m,n)\neq(0,0)} (m+n\tau)^{-k}$

Dém. $$\wp(z,\tau) - \frac{1}{z^2} = \overbrace{\sum' \left(\frac{1}{(z-\lambda)^2} - \frac{1}{\lambda^2} \right)}^{\text{CV abs}^{nt} \text{ unif}^{nt} \text{ sur compacts}}$$

On désire :

$$n!\, a_n(\tau) = (-1)^n \sum_{\lambda \in \Lambda}' \frac{(n+1)!}{\lambda^{2k}} = (-1)^n (n+1)!\, G_k(\tau)$$

$\left(G_{2k+1}(z) = 0 \text{ trivialement} \right)$

$\square$

$1/z^2$ $\qquad\qquad$ $-2/z^3+\cdots$

$\shortparallel$ $\qquad\qquad\qquad\qquad$ $\shortparallel$

<u>Observation</u> : considérons $\wp(z,\tau)$ et $\wp'(z,\tau)$

$\wp'(z,\tau)^2$ a un pôle d'ordre 6 ; on peut soustraire un multiple de $\wp^3$ et l'éliminer :

$\wp'(z,\tau)^2 - 4\wp(z,\tau)^3$ a des pôles d'ordre plus petit ... on continue et

$$\wp'(z,\tau)^2 - 4\wp(z,\tau)^3 = -60\,G_4(\tau)\,\wp(z,\tau) - 140\,G_6(\tau)$$

car la différence n'a pas de pôle donc est constante !

C'est à dire qu'on a une flèche

$$\begin{cases} \mathbb{C}/\Lambda \longrightarrow E(\mathbb{C}) \\ z\notin\Lambda \longmapsto (\wp(z,\tau), \wp'(z,\tau)) \\ \lambda \longmapsto \infty \end{cases} \quad , \quad E : y^2 = 4x^3 - 60\,G_4(\tau)x - 140\,G_6(\tau)$$

<u>Proposition</u>. Cette application est une bijection

<u>Dém.</u> Surjectivité : soit $(x_0, y_0) \in E(\mathbb{C}) \setminus \{\infty\}$; il existe z_0 tel que $\wp(z_0) = x_0$ puisque $z \mapsto \wp(z) - x_0$ est elliptique et a un pôle double donc par (ii) doit avoir un zéro !

Alors $\wp'(z_0,\tau) = \pm y_0$ car E est quadratique en y !

En changeant z_0 en $-z_0$, on trouve ce qu'on veut.

Injectivité : exercice

□

Comment cette application traite-t-elle la structure de groupe ?

Si $u_1, u_2 \in \mathbb{C}/\Lambda$ et $u_1+u_2+u_3 = 0$, alors les points $(\wp(u_1), \wp'(u_1))$, $(\wp(u_2), \wp'(u_2))$, $(\wp(u_3), \wp'(u_3))$ sont alignés sur $E(\mathbb{C})$.

<u>Dém.</u> Soit $y = ax+b$ la droite passant par les deux premiers points ; $\wp'(z) - (a\wp(z)+b)$ est une fonction elliptique qui a un pôle triple à l'origine donc elle a 3 zéros. Mais on connait déjà u_1, u_2 ; $\overset{\text{soit } w_3 \text{ l'autre}}{\text{par (iv)}}$ ci-dessus on a $u_1+u_2+w_3 \in \Lambda$

ie $\overline{w_3} = u_3 \in \mathbb{C}/\Lambda$

□

Autre pb : est-ce que toute courbe elliptique est réalisée de cette façon ?

Réponse : oui, mais plus tard.

On veut adapter aux $\overset{\text{corps}}{\vee}$ p-adiques.

(Tate, "A review of non-archimedean elliptic functions", Elliptic Curves, Modular Forms and Fermat's Last Theorem, Proceedings, Hong-Kong 1994 ; écrit en 1959)

<u>Question</u> : soit K un corps, complet % à une valeur absolue $|\cdot|$ $\left(|x| \geq 0,\ |xy| = |x||y|,\ |x+y| \leq |x|+|y| \right)$

[<u>Ex.</u> $\mathbb{C}, \mathbb{R}, \mathbb{Q}_p$]

Peut-on faire quelque chose de similaire ?

Le cas de $\mathbb{R}$ montre que ce n'est pas facile à adapter directement.

<u>Objectif</u> : donner une application

$$\overline{K}^\times / q^{\mathbb{Z}} \longrightarrow E(\overline{K})$$

où E est une certaine courbe elliptique.

<u>N.B.</u> Partant de $\mathbb{C}/\Lambda_\tau$, si on applique l'exponentielle, on trouve $\mathbb{C}^\times / (e^{2\pi i\tau})^{\mathbb{Z}}$, ce qui explique la forme recherchée ci-dessus.

Si on considère $\wp(z,\tau) = \dfrac{1}{z^2} + \sum\limits_{\lambda\in\Lambda_\tau}{}' \left(\dfrac{1}{(z-\lambda)^2} - \dfrac{1}{\lambda^2} \right)$,

on a en particulier

$\overset{\text{automatique ds le pt de vue multiplicatif}}{\text{par}}$ $\wp(z) = \wp(z+1)$, $\wp(z) = \wp(z+\tau)$

On voudrait une fonction $x(u)$ sur $\overline{K}^\times$ avec les propriétés suivantes :

(1) $x(qu) = x(u)$ pour un certain q, et $x(u) = x(u^{-1})$

On <u>considère alors</u> :

on prend $u \in K^\times$, $q \in K$ tel que $|q| \leq 1$ et on pose

$$\text{(I)} \quad \boxed{x(u) = \sum_{m\in\mathbb{Z}} \frac{uq^m}{(1-uq^m)^2} - 2\sum_{n\geq 1} \frac{q^n}{(1-q^n)^2}}$$

<u>Fait</u> : cette série converge.

$\dfrac{u}{(1-u)^2} = \dfrac{u^{-1}}{(1-u^{-1})^2}$ permet d'écrire

$$\text{(II)} \quad x(u) = \frac{u}{(1-u)^2} + \sum_{m\geq 1} \left(\frac{uq^m}{(1-uq^m)^2} - \frac{2q^m}{(1-q^m)^2} + \frac{u^{-1}q^m}{(1-u^{-1}q^m)^2} \right)$$

Si $|q| < 1$ est fixée : la série converge $\overset{\text{unif}^{\text{nt}} \text{ sur } u \text{ ds un compact}}{\text{absolument}}$ en u par comparaison avec la série géométrique $\sum\limits_{n\geq 1} q^n$.

On essaye de vérifier (1) : $x(u) = x(u^{-1})$ est évident sur (2) et de même $x(qu) = x(u)$ est facile.

$) = \frac{1}{(1-x)^2}$
$= \sum n x^{n-1}$

<u>N.B.</u> C'est à peu de choses près la série de Fourier de la fction) de Weierstraß.

On revient à $K = \mathbb{C}$ pour voir.

[Remarquons d'abord que si $|u| < |q| < |u^{-1}|$, alors on peut écrire en développant en série de Taylor ($|uq| < 1$, $|u^{-1}q| < 1$) :

$$(\mathrm{III}) \quad \boxed{x(u) = \frac{u}{(1-u)^2} + \sum_{m\geq 1}\sum_{n=1}^{\infty}\left(u^n q^{mn} n + u^{-n} q^{mn} n - 2n q^{mn}\right)}$$

(et cela converge unif$^{\text{nt}}$ pour $|r_1| < |u| < |r_2|$, $|u - q^n| \geq \varepsilon \quad \forall n$)]

On définit donc, pour $\tau \in \mathcal{H}$, $q = e^{2i\pi\tau}$:

$$f(z) = x(e^{2i\pi z})$$

Alors f est une fonction méromorphe dont les pôles se trouvent dans $\mathbb{Z} + \mathbb{Z}\tau$, et on a

$$\begin{cases} f(z+1) = f(z) & (\text{définition}) \\ f(z+\tau) = x(e^{2i\pi z} e^{2i\pi\tau}) = x(q e^{2i\pi z}) = x(e^{2i\pi z}) = f(z) \end{cases}$$

ie f est elliptique % Λ_τ !

On va la comparer à la fonction de Weierstraß. Pour cela, il faut étudier les pôles, pour cela on calcule ~~[illegible]~~ le développement de Laurent à l'origine :

on modifie (III) :

$$(\mathrm{IV}) \quad \boxed{x(u) = \frac{1}{u^{-1} + u - 2} + \sum_{n\geq 1}\frac{n q^n}{(1-q^n)}\left(u^n + u^{-n} - 2\right)}$$

$$u = e^{2i\pi_n z} = 1 + 2i\pi_n z + \frac{1}{2}(2i\pi_n z)^2 + \frac{1}{6}(2i\pi_n z)^3 + \frac{1}{24}(2i\pi_n z)^4$$
$$u^{-1} = e^{-2i\pi_n z} = 1 - 2i\pi_n z + \frac{1}{2}(2i\pi_n z)^2 + \frac{1}{6}(2i\pi z)^3 + \frac{1}{24}(2i\pi_n z)^4 +$$
$$u^n + u^{-n} = 2 + (2i\pi n z)^2 + \frac{1}{12}(2i\pi n z)^4 + \dots$$

$\Rightarrow$

$$f(z) = \frac{1}{(2i\pi z)^2 + \dots} + \text{série entière en } z \,!$$

$\Rightarrow$ f n'a qu'un pôle double en $z = 0$, et même $f - \frac{\wp(\tau)}{(2i\pi)^2}$ est une constante. Laquelle ? (exercice)

<u>Proposition</u> On a $f(z) = \wp(z,\tau)(2i\pi)^{-2} - \frac{1}{12}$ (1)

En fait, en calculant plus loin, on trouve

$$f(z) = \wp(z,\tau)(2i\pi)^{-2} - \frac{1}{12}$$

$$\frac{1}{2i\pi})^2\frac{1}{z^2} - \frac{1}{12} + \left(\frac{1}{240} + \sum_{n\geq 1}\frac{n^3 q^n}{1-q^n}\right)(2i\pi z)^2 + \left(\frac{-1}{6048} + \frac{1}{12}\sum_{n\geq 1}\frac{n^5 q^n}{1-q^n}\right)(2i\pi z)^4 + \dots$$

Cela donne des informations sur les G_k !

$$\left(\frac{1}{240} + \sum_{n\geq 1}\frac{n^3 q^n}{1-q^n}\right)(2i\pi)^2 = \frac{3G_4(\tau)}{(2i\pi)^2} \qquad (2)$$

$$\left(\frac{-1}{6048} + \frac{1}{12}\sum_{n\geq 1}\frac{n^5 q^n}{1-q^n}\right)(2i\pi)^4 = \frac{5G_6(\tau)}{(2i\pi)^2} \qquad (3)$$

On peut alors revenir au cas général. On sait que

$$\wp'(z,\tau)^3 = 4\wp(z,\tau)^3 - 60\,G_4(\tau)\,\wp(z,\tau) - 140\,G_6(\tau)$$

et on peut réécrire le membre de droite et celui de gauche en terme de séries entières/de Laurent en q, u.

$u = e^{2i\pi z}$
$du = 2i\pi e^{2i\pi z}\,dz$
$= 2i\pi u\,dz$
$dz = \frac{1}{2i\pi}\frac{du}{u}$

Soit $\frac{\wp(z,\tau)}{(2i\pi)^2} = x(u) + \frac{1}{12}$

$$\frac{d}{dz}\frac{\wp(z,\tau)}{(2i\pi)^2} = \frac{\wp'(z,\tau)}{(2i\pi)^3} = \sum_{m=-\infty}^{+\infty}\left(\frac{q^m u}{(1-q^m u)^2} + \frac{2(uq^m)^2}{(1-uq^m)^3}\right)$$
$$= x(u) + 2\,y(u) \qquad (4)$$

avec $y(u) = \sum_{m\in\mathbb{Z}}\left(\frac{(q^m u)^2}{(1-q^m u)^3} + \frac{q^m}{(1-q^m)^2}\right)$

On sait que $\wp(z,\tau)$ vérifie l'équation de Weierstraß :

$$\wp'(z,\tau)^2 = 4\wp(z,\tau)^3 - 60\,G_4(\tau)\,\wp(z,\tau) - 140\,G_6(\tau)$$

On divise alors par $(2i\pi)^6$ et grâce à (1), (2), (3) et (4) il vient

$$(x(u) + 2y(u))^2 = 4\left(x(u) + \frac{1}{12}\right)^3 - 60\frac{G_4(\tau)}{(2i\pi)^4}\left(x(u) + \frac{1}{12}\right) - \frac{140G_6(\tau)}{(2i\pi)^6}$$

puis enfin après calculs :

$$y(u)^2 - x(u)y(u) = x(u)^3 - 5\underbrace{\left(\sum_{n\geq 1}\frac{n^3 q^n}{1-q^n}\right)}_{\sum_{n\geq 1}\sigma_3(n)q^n} x(u) - \sum_{n\geq 1}\left(\frac{5\sigma_3(n) + 7\sigma_5(n)}{12}\right. \times q^n$$

<u>Proposition 1.</u> Pour tout corps K complet et tout $q \in K^*$, $|q| < 1$ soit (E_q) la courbe d'équation (affine)

$$E_q : \; y^2 - xy = x^3 - 5\left(\sum_{n\geq 1}\sigma_3(n)q^n\right)x - \sum_{n\geq 1}\left(\frac{5\sigma_3(n) + 7\sigma_5(n)}{12}\right)q^n$$

Alors (E_q) est une courbe elliptique sur K, ie elle est non-singulière.

<u>Dém.</u> On calcule le discriminant, du moins le début de la série de Taylor : $\Delta(E_q) = q + \underbrace{\sim\sim}_{\leq |q|^2} \neq 0$ □

Proposition 2 – Il existe une application $\varphi : K^\times \longrightarrow E_q(K)$
$$u \longmapsto (x(u), y(u))$$

Dém. Si u est une puissance entière de q, on envoie u sur le point à l'infini, donc cette flèche est bien définie.
Il est clair ensuite que $x(u), y(u) \in K$. Mais pourquoi satisfont-ils l'équation ?
Considérons comme série formelle (sur n'importe quel corps)

$$f(u,q) = y(u)^2 - x(u)\,y(u) - x(u)^3 + \left(\sum 5\sigma_3(n) q^n\right) x(u) + \left(\sum_{n\geq 1} \frac{5\sigma_3(n) + 7\sigma_5(n)}{12}\, q^n\right)$$

On a $f(q,u) \in K\{q,u\}$ [séries de Laurent] ; même si on développe en série entière en puissances de q, on trouve que
$$f(q,u) \in K(u)[[q]] \text{ , \underline{même} } f \in \mathbb{Z}(u)[[q]]$$
Soit alors u, q des complexes non nuls, avec
$$|q| < |u| < |q^{-1}|$$
On a vu que $f(q,u) = 0$ alors ; cela implique que les coefficients $a_n(u)$ de f sont les ~~[illegible]~~ nuls (en tant que nbres complexes) ; faisant ensuite varier u, il découle de cela que $a_n \equiv 0$ identiquement, ie que $f = 0$, ce que l'on recherchait, vu que x, y sont bien définies (convergentes).

$\square$

N.B. C'est un exemple du principe de Lefschetz en géométrie algébrique en caractéristique nulle.

Proposition 3 – $\varphi : K^\times \longrightarrow E_q(K)$ est un morphisme de groupes, et $\operatorname{Ker} \varphi = q^{\mathbb{Z}}$

Dém. Le raisonnement est tout à fait similaire : le fait que φ est un morphisme de groupe équivaut à $\varphi(xy^{-1}) = \varphi(x) - \varphi(y)$; on écrit cela en termes d'identité entre séries entières et on vérifie sur $\mathbb{C}$. Comme précédemment, le résultat en découle.
Enfin, $\operatorname{Ker}\varphi$ est trivialement égal à $q^{\mathbb{Z}}$ par la définition même de φ.

$\square$

Proposition $4_{\mathbb{C}}$ – $\varphi : K^\times \longrightarrow E_q(K)$ est surjective si $K = \mathbb{C}$.

Dém. On réécrit en termes de fonctions de Weierstraß, et on applique le fait que cette dernière $\wp(\tau) : \mathbb{C} \longrightarrow \mathbb{C}$ est elle-même surjective.

$\square$

N.B. On a donc établi que, pour $K = \mathbb{C}$,
$$\varphi : \mathbb{C}^\times/q^{\mathbb{Z}} \longrightarrow E_q(\mathbb{C}) \simeq \mathbb{C}/\Lambda$$
est un isomorphisme.

On veut étendre la proposition 4 à tout corps complet K. On commence par un lemme galoisien.

Lemme – Soit $q \in K^\times$ tel que $|q| < 1$ et L/K une extension finie séparable. Soit $u \in L$ tel que $\varphi(u) \in E_q(K)$, alors $u \in K$.

Dém. Quitte à agrandir L, on peut prendre la clôture normale de L et supposer que L/K est une extension galoisienne.
Dans les cas que l'on considère, on sait que le groupe de Galois $\mathrm{Gal}(L/K)$ agit par automorphismes continus sur L :

$$\begin{tikzcd} L \arrow[d, dash, "G"] \\ K \end{tikzcd}$$

$K = \mathbb{R}$, $L = \mathbb{C}$: $x \longmapsto \bar{x}$

$K = \mathbb{Q}_p$ ou extension finie : clair

On en déduit aussitôt, puisque les séries donnant x et y sont à coefficients rationnels :
$$\varphi(u^\sigma) = (x(u^\sigma), y(u^\sigma)) = (x(u)^\sigma, y(u)^\sigma) = \varphi(u)^\sigma = \varphi(u)$$
car $\varphi(u) \in E_q(K)$ par hypothèse.
D'après la proposition précédente, il vient $u^\sigma/u \in \operatorname{Ker}\varphi$ ie il existe $j_\sigma \in \mathbb{Z}$ tel que $u^\sigma/u = q^{j_\sigma}$; mais $\left|\frac{u^\sigma}{u}\right| = 1$ et $|q| < 1$, donc $j_\sigma = 0$ et $u^\sigma = u$, d'où finalement $u \in K$.

$\square$

Cela permet déjà de traiter le cas $K = \mathbb{R}$ de la proposition 4_K :

Proposition 4_K – $\varphi : K^\times/q^{\mathbb{Z}} \longrightarrow E_q(K)$ est surjective

__Proposition__ $4_{\mathbb{R}}$. Pour $K=\mathbb{R}$, $\varphi : \mathbb{R}^{*}/q^{\mathbb{Z}} \longrightarrow E_q(\mathbb{R})$ est surjective.

__Dém.__ Par théorie de Weierstraß, $\varphi_{\mathbb{C}} : \mathbb{C}^{*}/q^{\mathbb{Z}} \longrightarrow E_q(\mathbb{C})$ est surjective; or $\mathbb{C}/\mathbb{R}$ est une extension finie séparable, appliquant le lemme, si $(x,y) \in E_q(\mathbb{R})$ a un antécédent $\varphi_{\mathbb{C}}^{-1}(x,y)$ dans $\mathbb{C}$, il appartient en fait à $\mathbb{R}$

□

Reste à traiter le cas non-archimédien

__N.B.__ Avant de s'embarquer dans ce cas, notons le résultat suivant qui est facile :

__Proposition.__ L'application $\varphi_{\bar{K}} : \bar{K}/q^{\mathbb{Z}} \longrightarrow E_q(\bar{K})$ est surjective quand elle est restreinte aux points d'ordre fini si char $K = 0$.

__Dém.__ On sait que $E_q(K)[m]$ est un groupe fini d'ordre $\leq m^2$

D'un autre côté, on identifie facilement le groupe des éléments d'ordre m de $\bar{K}/q^{\mathbb{Z}}$:

(i) Si $\xi^m = 1$ et ξ est une racine primitive de l'unité, $<\xi> \hookrightarrow \bar{K}/q^{\mathbb{Z}}$ injecte un sous-groupe d'ordre m (cyclique) dans $(\bar{K}/q^{\mathbb{Z}})[m]$

(ii) Si u_0 vérifie $u_0^m = q$, alors $<u_0> \hookrightarrow \bar{K}/q^{\mathbb{Z}}$ donne un autre sous-groupe d'ordre m (cyclique) de $(\bar{K}/q^{\mathbb{Z}})[m]$

On voit aussitôt que l'intersection de ces deux sous-groupes est triviale, donc leur produit est d'ordre m^2, $\simeq \mathbb{Z}/(m) \times \mathbb{Z}/(m)$

Par conséquent la flèche φ induit une injection

$$1 \longrightarrow \mathbb{Z}/(m) \times \mathbb{Z}/(m) \xrightarrow{\varphi} E_q(\bar{K})[m]$$

et comme l'ordre de $E_q(\bar{K})[m]$ est $\leq m^2$, ce doit être une surjection (et même un isomorphisme).

□

La preuve de la proposition 4_K annoncée va maintenant être donnée; elle requiert l'étude de certaines propriétés des séries entières sur un corps complet non-archimédien...

27/9/95

K corps complet avec $|\cdot|$ ($K \simeq \mathbb{C}, \mathbb{R}$, non-archimédien)

$q \in K^{*}$, $|q| < 1$

On a exhibé la courbe elliptique :

(E_q) : $y^2 - xy = x^3 + a_4(q)\,x + a_6(q)$

où $a_4(q) = -5 \sum_{n\geq 1} \sigma_3(n)\, q^n$

$a_6(q) = \frac{-1}{12}\left(5\sum_{n\geq 1} \sigma_3(n) q^n + 7 \sum_{n\geq 1} \sigma_5(n)\, q^n\right)$

$\Delta_{E_q} = q + \sum_{n\geq 1} a_n q^n$, $a_n \in \mathbb{Z}$

$c_4(q) = 1 + 240 \sum_{n\geq 1} \sigma_3(n)\, q^n$

$c_6(q) = -1 + 504 \sum_{n\geq 1} \sigma_5(n)\, q^n$

$j(q) = \frac{c_4^3}{\Delta} = \frac{1}{q} + \ldots$

$$\begin{cases} x(u) = \sum_{m\in\mathbb{Z}} \frac{q^m u}{(1-q^m u)^2} - 2 \sum_{m\in\mathbb{Z}} \frac{q^m}{(1-q^m)^2} \\ y(u) = \ldots \end{cases}$$

permettent de définir une flèche

$$\varphi \begin{cases} K^{*} \longrightarrow E_q(K) \\ u \longmapsto (x(u), y(u)) , \ u \neq q^m \\ q^m \longmapsto \infty = O \end{cases}$$

On a vu que φ est un morphisme de groupe dont le noyau est $q^{\mathbb{Z}}$

On veut ici atteindre :

__Théorème__ L'application $\varphi : K^{*}/q^{\mathbb{Z}} \longrightarrow E_q(K)$ est un isomorphisme.

__Dém.__ (i) Si $K \simeq \mathbb{C}$, c'est la théorie de Weierstraß.

(ii) Si $K = \mathbb{R}$, c'est le lemme précédent et le cas (i)

(iii) Supposons K non-archimédien : il faut des faits de base sur les séries entières sur K non-archimédien.

(...

On considère $f(z) = z + a_1 z^2 + \ldots + a_{n-1} z^n + \ldots$

__Fait__ : si pour tout n, on a $|a_n| \leq r^n$, alors $f(z)$ converge pour $|z| < \frac{1}{r}$

__Dém.__ $|a_{i-1} z^i| = |a_{i-1}||z^i| < \frac{r^{i-1}}{r^i} < \frac{1}{r}$ ... □

__1° observation__ : f donne une application $\{z \in K \mid |z| < \frac{1}{r}\} \to \{z \in K \mid |z| < \frac{1}{r}\}$

__Lemme.__ f est une bijection sur $\{z \in K \mid |z| < \frac{1}{r}\}$ (!)

__Dém__ On écrit l'inverse...

Calculons l'inverse formelle de f, $g(z) = z + b_1 z^2 + b_2 z^3 + \dots$ tel que $g(f(z)) = z$ (en tant que série formelle):

$$f(z) + b_1 (f(z))^2 + b_2 (f(z))^3 + \dots = z$$
$$" z + a_1 z^2 + b_1 z^2 + \dots$$

d'où on a des formules par récurrence pour les b_i! ($b_1 = -a_1 \dots$)

Note: on trouve que b_k est une combinaison linéaire à coefficients entiers de b_i, $i < k$, et de a_i, $i \leq k \dots$

Par récurrence, cela entraîne immédiatement

$$\forall i, \quad |b_i| < r^i$$

On a donc
$$\begin{tikzcd} B_{r^{-1}} \arrow[r, "f"] & B_{r^{-1}} \arrow[l, bend left, "g"] \end{tikzcd}$$

et cela donne aussitôt le lemme □

Corollaire. Soit $h(z) = \frac{1}{z} + c_1 + c_2 z + \dots + c_n z^{n-1} + \dots$ avec $|c_i| < r^i$. Alors h induit une bijection

$$h : \{z \in K \mid 0 < |z| < \tfrac{1}{r}\} \longrightarrow \{z \in K \mid r < |z| \}$$

Dém. Regardons $\frac{1}{h}$: c'est une série formelle qui vérifie les conditions du lemme:

[$\frac{1}{h(z)} = z + a_2 z^2 + \dots$
et a_i est une combinaison linéaire à coeff. entiers des c_k, $k \leq i$, et des a_j, $j < i \dots$]

□

$\dots$)

On veut maintenant:

Lemme. Étant donné $x \in K^*$, il existe $u \in L$, L extension séparable finie de K, telle que $x(u) = x$

Cela donne alors le théorème: on a $(x_0, y_0) \in E_q(K)$; le lemme donne $u \in L/K$ tel que $x(u) = x_0$. On peut ajuster u de sorte que $(x(u), y(u)) = (x_0, y_0)$: x_0, y_0 vérifient une équation de degré 2 en y_0 (étant donné x_0), et si nécessaire on remplace u par u^{-1}.

On a donc $u \in L$ tel que $\varphi(u) \in E_q(K)$; le lemme précédent donne alors $u \in K$ et c'est terminé! □

Preuve du lemme.

On réécrit la formule pour x:

$$x(u) = \frac{u}{(1-u^2)} + \sum_{n \geq 1} \frac{n q^n}{1-q^n} (u^n + u^{-n} - 2) \qquad \text{(formule (IV))}$$
$$= \frac{1}{u^{-1} + u - 2} + \sum_{n \geq 1} \frac{n q^n}{1-q^n} (u^n + u^{-n} - 2)$$

On pose $w = u + u^{-1} - 2$; on découvre que

$$u^n + u^{-n} - 2 = (w+2)(u^{n-1} + u^{1-n} - 2) - (u^{n-2} + u^{2-n} - 2) + 2w$$

par récurrence on peut donc exprimer $u^n + u^{-n} - 2$ comme polynôme de degré n en w, polynôme entier à coeff dominant 1, et tel que son terme constant est nul.

On peut donc écrire

$$x(u) = \frac{1}{w} + a_1 w + a_2 w^2 + \dots = \tilde{x}(w)$$

On veut appliquer le corollaire ci-dessus. Il faut évaluer $|a_n| \dots$

Fait : $|a_n| \leq |q|^n$ (exercice)

Pour le corollaire, on a $|c_n| = |a_{n-1}| \leq |q|^{n-1} < (\sqrt{|q|})^n$, ie on voit que $\tilde{x}(w)$ donne une bijection sur $|x_0| > |q|^{1/2}$, et par une extension quadratique on trouve $u \in L/K$ tel que

$$x(u) = x_0.$$

Pour trouver les x_0 tels que $|x_0| \leq |q|^{1/2}$, on fait le changement de variable $\tilde{w} = u + q/u$

□

Applications des courbes de Tate

Regardons d'abord quelles courbes sont de la forme E_q.

Fait : les courbes (E_q) on $j(q) = \frac{1}{q} + \dots$

(i) Sur $\mathbb{C}$, $j(q)$ prend toutes les valeurs complexes, ie toute courbe elliptique $E/\mathbb{C}$ est de la forme E_q pour un q tel que $|q| < 1$.

(ii) Sur $\mathbb{R}$, étant donnée $E/_{\mathbb{R}}$ on a $j(E) \in \mathbb{R}$, $j(E) = j(q)$, $q \in \mathbb{C}$ et la formule pour j donne $q \in \mathbb{R}$, et c'est pareil.

(iii) Sur K non-archimédien : on a trivialement $|j(E_q)| > 1$, donc on ne peut pas espérer avoir toutes les courbes comme une E_q.

Lemme Soit $j \in K^\times$ tel que $|j| < 1$, alors il existe q tel que $j(q) = j$.

Dém Le corollaire au lemme sur les séries entières s'applique pour $r = 1$...

□

Si on a E/K avec $|j(E)| > 1$, on a donc un q tel que $j(E_q) = j(E)$ ie $E_{q/L} \simeq E_{/L}$ après une extension finie L/K.

Soient A, B, C des entiers, $ABC \neq 0$, avec $A+B+C=0$, premiers entre eux. Considérons encore

$$(E_{A,B,C}) \qquad y^2 = x(x-A)(x+B)$$

On a

$$\Delta = 2^4 (ABC)^2$$

$$j = \frac{2^8 (C^2 - AB)^3}{(ABC)^2}$$

Si p est un nombre premier impair tel que $p \mid ABC$ (ie $p \mid A$ ou B ou C), alors trivialement

$$|j|_p = \left| \frac{2^8 (C^2-AB)^3}{(ABC)^2} \right|_p \leq \left| \frac{1}{p^2} \right|_p^2 > 1$$

ie il existe une courbe de Tate avec $j(E_q) = j$

$$\begin{tikzcd} L(E_{A,B,C}[n]) \arrow[d, dash, "G"'] \\ \mathbb{Q} \end{tikzcd}$$

Soit maintenant les points d'ordre n sur $E_{A,B,C}$, et $L(E[n])$ l'extension qu'ils engendrent. Cette extension est galoisienne (facile). Prenons $\ell \in \mathbb{Q}$ un nombre premier ; on est intéressé par la ramification de ℓ, sa décomposition...
Écrivons $(\ell) = \ell_1^{e_1} \dots \ell_r^{e_r}$; supposons ℓ_1 ne ramifie pas

$$\begin{tikzcd} \mathcal{O}_L \arrow[d, dash] & \ell_1 & \mathcal{O}_L/(\ell) \arrow[d, dash, "<\sigma>"] \\ \mathbb{Z} & \ell & \mathbb{Z}/(\ell) \end{tikzcd}$$

On a $G_{\ell_1} \twoheadrightarrow <\sigma_\ell>$ (Th. nbres algébriques)

Il y a donc le noyau I_{ℓ_1} et une classe $I_{\ell_1} Fr_{\ell_1}$ telle que $I_{\ell_1} Fr_{\ell_1} \longmapsto \sigma_\ell$
et on appelle Fr_{ℓ_1} le Frobenius en ℓ_1.

Ce Fr_{ℓ_1} est bien défini % à ℓ modulo conjugaison.
On est intéressé par l'action de ce Frobenius sur les points d'ordre n...

25/9/95

Étant donné un corps complet K et $q \in K^\times$ tel que $|q| < 1$, on a construit une courbe elliptique E_q/K, telle que :

$$E_q(K) \simeq K^\times / q^{\mathbb{Z}}$$

Réciproquement, étant donnée une courbe elliptique E/K, quand existe-t-il q tel que $E_q \simeq_K E$?

On a vu la dernière fois que :

(i) pour $K = \mathbb{C}$, toute courbe elliptique $E/\mathbb{C}$ est de la forme E_q

(ii) pour $K = \mathbb{R}$, il y a une condition :
rappelons que l'invariant c_4 de E_q est donné par

$$c_4(E_q) = 1 + 240 \sum_{n \geq 1} \sigma_3(n) q^n$$

$$\left[y^2 = x^3 - \frac{c_4}{48} x - \frac{1}{864} c_6 \right]$$

$$\text{et} \quad c_6(E_q) = -1 + 504 \sum \sigma_5(n) q^n$$

et on a

$$c_4/c_6 = 1 + q + \dots$$

et (pour tout K) on vérifie facilement que $-c_4/c_6 \in K^2$ (c'est un carré), et cette condition est <u>invariante</u> par isomorphisme.

Prop. Si $-c_4/c_6 > 0$, alors il existe $q \in \mathbb{R}^\times$, $|q| < 1$, tel que

$$E \simeq_{\mathbb{R}} E_q$$

(iii) pour K non-archimédien : la même condition $-c_4/c_6 \in K^2$ s'applique : $E \simeq_K E_q$ pour un certain $q \iff \begin{cases} -\frac{c_4}{c_6}(E) \in K^{\times 2} \\ |j(E)| > 1 \end{cases}$

(mais dans ce cas, on voit que $c_4(E_q) \neq 0$)

(La 2ᵉ condition dit que $E_{\bar K} \simeq_{\bar K} E_{q,\bar K}$)

Dém. exercice ($j = \frac{c_4^3}{c_4^3 - c_6^2}$) ◇

Donc pour toute courbe E/K avec $|j(E)| > 1$, $E \simeq_L E_q$ après une extension <u>quadratique</u> L/K, précisément

$$L \simeq K\left(\sqrt{\frac{-c_4}{c_6}}\right)$$

Fait : cette extension, pour $K = \mathbb{Q}_p$ (ou une extension finie), cette extension est (soit triviale soit) non-ramifiée, ie on a

$$\left|\frac{-c_4}{c_6}\right|_K = 1 \qquad (?)$$

Dém. La formule $-\frac{c_4}{c_6} = 1 + q + \ldots$ le démontre aussitôt □

Soit $(A, B, C) \in \mathbb{Z}^3$ tels que $A + B + C = 0$, A, B, C premiers entre eux

$$E_{A,B,C} : \quad y^2 = x(x-A)(x+B)$$
$$\Delta = 16\,(ABC)^2$$

Soit p un nombre premier, et considérons le corps des points de p-division ie $\mathbb{Q}(E_{A,B,C}[p]) / \mathbb{Q} = K/\mathbb{Q}$

Proposition. Soit $\ell \neq p$ un nombre premier tel que $\ell \mid ABC$, ℓ impair.
Supposons que $\mathrm{ord}_\ell(ABC) \equiv 0 \ (p)$ [Fermat !]
Alors (i) Si $\ell \neq p$, ℓ n'est pas ramifié dans cette extension.
(ii) Si $\ell = p$, ℓ est "peu ramifié", au sens expliqué plus bas.

Dém. (Idée : établir une relation entre $E_{A,B,C} / \mathbb{Q}_\ell$ et une courbe de Tate, puis exploiter cela...)

$$E_{A,B,C} : \quad y^2 = x(x-A)(x+B) \qquad \Delta = 2^4 (ABC)^2$$
$$j = \frac{2^8 (C^2 - AB)^3}{(ABC)^2}$$

Fait : $\ell \nmid C^2 - AB$ pour ℓ impair
On en déduit $|j|_\ell > 1$.

[**Rappel** :

$$\begin{tikzcd} \mathbb{Q}(E_{A,B,C}[p]) \arrow[d, dash] & \ell_1 \ldots & \overset{\text{(complétion \% } \ell_1)}{\Longrightarrow} & \overset{e}{\ell_1} & \mathbb{Q}_\ell(E_{A,B,C}[p]) \arrow[d, dash] \\ \mathbb{Q} & \ell & & \ell & \mathbb{Q}_\ell \end{tikzcd}$$

La ramification est une question locale]

Donc après, au pire, une extension quadratique, $E_{A,B,C} \simeq E_q$ une courbe de Tate.

Supposons d'abord $E \underset{\mathbb{Q}_\ell}{\simeq} E_q$.
On en déduit

$$E(\overline{\mathbb{Q}_\ell}) \simeq \overline{\mathbb{Q}_\ell}^\times / q^{\mathbb{Z}}$$

et cela nous donne aussitôt $\mathbb{Q}_\ell(E_{A,B,C/\mathbb{Q}_\ell}[p])$:

$$\begin{tikzcd} \mathbb{Q}_\ell(\mu_p, q^{1/p}) = \mathbb{Q}_\ell(E_{A,B,C}[p]) \arrow[d, dash] \\ \mathbb{Q}_\ell(\mu_p) \arrow[d, dash] \\ \mathbb{Q}_\ell \end{tikzcd}$$

} là, seul p ramifie, donc si $\ell \neq p$, ce n'est pas ramifié

La condition $\mathrm{ord}_\ell(ABC) \equiv 0 \ (p)$ donne $q = u \cdot \ell^{p \cdots}$
ie la 2ᵉ étape est de la forme : p-ème racine d'une unité, et on connait bien le type de ramification de telles extensions.

Déf. ℓ est "peu ramifié" $\iff$ ℓ est ramifié comme l'extension de $\mathbb{Q}_p$ par une racine p-ème d'une unité.

(?) Sinon, supposons $32 \mid A$, $B \equiv 1 \ (4)$: alors $\ell \nmid c_4, c_6$ (vérifier), et l'extension quadratique est clairement non-ramifiée

[on écrit $y^2 = x(x-A)(x+B)$
de la forme

$$y^2 + \underset{\substack{\downarrow \\ a_1 = 1}}{xy} = x^3 + \underbrace{\left(\frac{B-A-1}{4}\right)}_{a_2} x^2 + \underbrace{\frac{-AB}{16}}_{a_4} X$$

et les formules classiques donnent :

$$\ell \mid a_3, a_4, a_6, \Delta$$

puis $\ell \nmid c_4, c_6$ (utiliser $(A, B, C) = 1$!)]

(...)
□

Comment exploite-t-on cette proposition pour le théorème de Wiles ?
On a besoin de deux théorèmes difficiles :
soit $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow GL(2, \mathbb{Z}_p)$ une représentation continue de Galois $G_{\mathbb{Q}}$

On dit que ρ est <u>modulaire</u> s'il existe une forme modulaire de poids 2 sur $\Gamma_0(N)$ donnée par un développement de Fourier

$$f(z) = \sum a_n q^n$$

et si pour tout ℓ tel que $\ell \nmid N$, $a_\ell = \mathrm{Tr}(\rho(Fr_\ell))$ (dans une extension de $\mathbb{Q}_p$)

cf plus loin pour l'énoncé correct

~~**Théorème** (Ribet, 1986). Soit $\rho : G_{\mathbb{Q}} \longrightarrow GL(2, \mathbb{Z}_p)$ est modulaire, de niveau N. Supposons que $\ell \mid N$ vérifie~~

~~(i) pour $\ell \neq p$ premier, $\bar\rho = \rho \bmod p : G_{\mathbb{Q}} \longrightarrow GL(2, \mathbb{F}_p)$ est non-ramifiée à ℓ~~

~~Alors il existe une forme modulaire g de poids 2 et de niveau N/ℓ, telle que $g(z) = \sum b_n q^n$ et $b_\ell = tr(\rho(Fr_\ell))$, $\forall \ell$~~

~~(ii) pour $\ell = p$, ρ est "peu ramifié" dans $\bar\rho$: alors le même énoncé est valide, ρ est modulaire de niveau N/ℓ~~

$\mathbb{Q}(\ker\bar\rho)$ non-ramifié

ou groupe tie agit ialement

On a ensuite le gros

Théorème (Wiles, 1993-95). Les courbes $E_{A,B,C}$ et les représentations associées sur les groupes de p-division sont modulaires.

Ces deux résultats, avec les calculs sur la ramification du § précédent, donnent finalement le théorème de Fermat !

Car on part d'un niveau $N \mid \Delta = 2^4 (ABC)^{2p}$, et les résultats de Ribet et Wiles donnent une forme modulaire associée de niveau 2 ! Laquelle, on le sait, n'existe pas...

N.B. Wiles utilise le théorème de Ribet...

Echauffement : le cas de $GL(1)$

On considère des représentations continues $\rho : G_{\mathbb{Q}} \to GL(1, \mathbb{Z}_p) \simeq \mathbb{Z}_p^\times$ qui devraient être plus faciles à comprendre.

$$\begin{tikzcd} \mathbb{Z}_p^\times \arrow[d] \\ (\mathbb{Z}/(p^n))^\times \end{tikzcd}$$

On prend un n, on a $\rho_n : G_{\mathbb{Q}} \longrightarrow (\mathbb{Z}/(p^n))^\times$ et l'extension associée au noyau

$$\begin{tikzcd} K_n \arrow[d, dash, "G \subset (\mathbb{Z}/(p^n))^\times \text{ abélien}"] \\ \mathbb{Q} \end{tikzcd}$$

N.B. les corps cyclotomiques "ressemblent à ça" :

$$\begin{tikzcd} \mathbb{Q} \arrow[r, dash] \arrow[rr, dash, bend right, "(\mathbb{Z}/(p^n))^\times"'] & \mathbb{Q}(\mu_p) \arrow[r, dash] & \mathbb{Q}(\mu_{p^n}) \end{tikzcd}$$

Peut-être, sous certaines conditions, ces corps K_n peuvent être compris par le biais des corps cyclotomiques, en particulier identifiés.

Il faut au moins limiter la ramification ($\mathbb{Q}(\mu_p)$ n'est ramifié qu'en p) des extensions considérées.

Théorème (Kronecker-Weber)

Si $L/\mathbb{Q}$ est une extension abélienne finie de $\mathbb{Q}$, alors il existe $n \in \mathbb{N}$ tel que $L \subset \mathbb{Q}(\mu_n)$.

But : on va essayer de prouver cela par les techniques de Wiles pour s'exercer.

Ensuite on généralisera puissamment.

Cela devrait donner des motivations et une meilleure compréhension des choses.

27/9/95

Rappel : étant donnée une représentation continue $\rho : G_{\mathbb{Q}} \to GL(2, \mathbb{Z}_p)$ (que l'on cherche à classifier), on dit que ρ est modulaire de niveau N (et de poids 2) s'il existe une forme modulaire f de niveau N, poids 2 (ie ~~une~~ une différentielle holomorphe sur $\Gamma_0(N) \backslash \mathcal{H}^+$) telle que f admette le développement de Fourier

$$f = \sum a_n q^n$$

avec pour tout ℓ premier, $(\ell, N) = 1$

$$a_\ell = tr(\rho(Fr_\ell))$$

Th. (Wiles) Si $E/\mathbb{Q}$ est une courbe elliptique $y^2 = x(x-A)(x+B)$ alors $\rho_E : G_{\mathbb{Q}} \longrightarrow GL(2, \mathbb{Z}_p)$ est modulaire.

Th. (Ribet) Supposons que $\rho : G_{\mathbb{Q}} \longrightarrow GL(2, \mathbb{Z}_p)$ est modulaire de niveau N et considérons $\bar\rho : G_{\mathbb{Q}} \longrightarrow GL(2, \mathbb{Z}_p) \longrightarrow GL(2, \mathbb{F}_p)$ sa réduction modulo p.

(i) Si $\ell \mid N$ et $\ell \neq p$, et si $\bar\rho$ est non-ramifiée en ℓ, alors il existe une forme modulaire g de niveau N/ℓ, de poids 2, telle que $g = \sum b_n q^n$ et pour presque tout nombre premier q,

$$b_q \equiv tr(\rho(Fr_q)) \quad (\text{mod } \mathfrak{p}, \text{ idéal au-dessus de } p)$$

(**N.B** g peut avoir des coefficients dans une extension de $\mathbb{Q}$, même si $a_n \in \mathbb{Q}$)
(ii) Si $p \mid N$ et $\bar{\rho}$ est "peu ramifiée" (au sens de la dernière fois), la même condition est valide.

Wiles + Ribet $\Rightarrow$ Fermat : on construit $E_{A,B,C}$, elle est modulaire, les courbes de Tate montrent que les conditions (i) ou (ii) sont toujours valide, on trouve g de niveau N/ℓ, g vérifie encore les conditions.

Le cas de $GL(1)$

Il y a un analogue des formes modulaires pour $GL(1)$.

Déf. Un caractère de Hecke algébrique sur un corps de nombres $K/\mathbb{Q}$ est donné de la façon suivante :

on choisit $\mathfrak{m}$ un idéal de $\mathcal{O}_K$

on pose $G(\mathfrak{m})$ = groupe des idéaux fractionnaires premiers avec $\mathfrak{m}$

et soit $\chi : G(\mathfrak{m}) \longrightarrow \mathbb{C}^\times$ un morphisme de groupes tel que :

si $\alpha \in \mathcal{O}_K$ et $\alpha \equiv 1 \ (\mathfrak{m})$, alors $\chi((\alpha)) = \boxed{\pm} \prod_{i : K \hookrightarrow \mathbb{C}} \alpha^{r_i} \bar{\alpha}^{s_i}$

$[\mathbb{R} \otimes K = \oplus]$ pour que ça soit bien défini

où $r, s \in \mathbb{Z}$.

plus
portants
dans le
n de
$\mathbb{Q}$

Ex. (i) Si $r_i = s_i = 0$: $\chi : \underbrace{G(\mathfrak{m}) / (\alpha \mid \alpha \equiv 1 \ (\mathfrak{m}))}_{\text{fini par finitude du groupe de classes}} \longrightarrow \mathbb{C}^\times$ induit un tel caractère

(ii) Le caractère "norme" : $N : G(\mathfrak{m}) \longrightarrow \mathbb{C}^\times$, $\mathfrak{a} \longmapsto N\mathfrak{a}$ est un caractère de Hecke algébrique

(iii) $K = \mathbb{Q}(i)$: $\chi((\alpha + i\beta)) = (\alpha + i\beta)^4$ est un caractère de Hecke algébrique

Déf. $\mathfrak{m}$ est appelé le <u>niveau</u> de χ, et les (r_i, s_i) sont appelés le "poids".

[On considère maintenant le cas $K = \mathbb{Q}$.

(i) les caractères de Dirichlet

$\chi : (\mathbb{Z}/(n))^\times \longrightarrow \mathbb{C}^\times$ (poids 0, niveau n)

(ii) la norme (niveau 1)

$\chi : (n) \longmapsto |n|$]

Proposition. Les valeurs d'un caractère de Hecke algébrique engendrent une extension finie de $\mathbb{Q}$.

Dém.
$$\begin{tikzcd} G(\mathfrak{m}) \arrow[r, "\chi"] & \mathbb{C}^\times \\ \{\alpha \mid \alpha \equiv 1 \ (\mathfrak{m})\} \arrow[u, phantom, "\cup", "\text{indice fini}"'] \arrow[r] & (\text{composé de } K \text{ et de ses conjugués}) \arrow[u] \end{tikzcd}$$

donc les valeurs de χ sont dans une extension finie

☐

On note L le corps des valeurs de χ.

Rappel : la théorie cyclotomique

$$\begin{tikzcd} \mathbb{Q}(\mu_n) \arrow[d, dash, "(\mathbb{Z}/(n))^\times"] \\ \mathbb{Q} \end{tikzcd}$$

On regarde une tour :

(ℓ premier)
$$\underbrace{\underbrace{\underbrace{\mathbb{Q} — \mathbb{Q}(\mu_\ell)}_{(\mathbb{Z}/(\ell))^\times} — \mathbb{Q}(\mu_{\ell^2})}_{(\mathbb{Z}/(\ell^2))^\times} — \cdots}_{\mathbb{Z}_\ell^\times = \varprojlim (\mathbb{Z}/(\ell^n))^\times}$$

Dans $\mathbb{Q}(\mu_n)/\mathbb{Q}$, Fr_ℓ, $\ell \nmid N$, est :
$$Fr_\ell = \ell \in (\mathbb{Z}/(n))^\times$$

Et dans le cas infini, pour $q \neq \ell$ premier, on a :
$$Fr_q(x) = x^q \in \mathbb{Z}_\ell^\times$$

Par théorie de Galois, on a une flèche

$$G_{\mathbb{Q}} \longrightarrow (\mathbb{Z}/(n))^{\times}$$

et aussi

$$G_{\mathbb{Q}} \longrightarrow \mathbb{Z}_{\ell}^{\times}$$

et donc des caractères de $(\mathbb{Z}/(n))^{\times}$ donnent des caractères de $G_{\mathbb{Q}}$

- $K = \mathbb{Q}$, χ un caractère de Hecke algébrique de la forme

$$\chi = \chi_{Dir} \cdot (N)^{r}$$

χ_{Dir} ↙ caractère de Dirichlet de niveau N

χ a valeurs dans L

fait ce sont
les ra de
ke alg de $\mathbb{Q}$)

<u>Pb.</u> associer à χ une représentation λ-adique de $G_{\mathbb{Q}}$ de dimension 1,

$$G_{\mathbb{Q}} \longrightarrow GL_1(O_{L,\lambda})$$

où λ est un idéal premier de O_L.

D'abord pour $\chi = \chi_{Dir}$, caractère de Dirichlet :

$$\begin{tikzcd} G_{\mathbb{Q}} \arrow[r, "\text{cyclotomique}"] \arrow[rrrr, bend right, "\rho_{\chi,\lambda}"'] & (\mathbb{Z}/n\mathbb{Z})^{\times} \arrow[r, "\chi"] \arrow[rd, "\chi"'] & L^{\times} \arrow[r] & L_{\lambda}^{\times} \\ & & O_L^{\times} \arrow[u, hook] & \end{tikzcd}$$

Comme les valeurs de χ sont dans $O_L^{\times}$, les valeurs de ρ_{χ} sont dans $O_{L,\lambda}$:

$$\rho_{\chi,\lambda} : G_{\mathbb{Q}} \longrightarrow GL(1, O_{L,\lambda})$$

Cela existe <u>pour tout λ</u> idéal premier de O_L.

Quelle est la relation entre ρ_{χ} et le χ original ? ρ_{χ} a la propriété que, pour presque tout q premier, on a

$$\boxed{\rho_{\chi}(Fr_q) = \chi(q)}$$

<u>N.B.</u> Les différentes $\rho_{\chi,\lambda}$ pour λ variant, sont "compatibles" d'après cette formule.

Pour $\chi = N = |\cdot|$ (la norme, de niveau 1) :
on considère $G_{\mathbb{Q}} \xrightarrow{\chi_{\ell}} \mathbb{Z}_{\ell}^{\times}$ (le caractère cyclotomique)
et on construit $\rho_N : G_{\mathbb{Q}} \longrightarrow GL(1, \mathbb{Z}_{\ell})$ par

$$\begin{tikzcd} G_{\mathbb{Q}} \arrow[r, "\rho_N"] \arrow[rd, "\chi_{\ell}"'] & \mathbb{Z}_{\ell}^{\times} \arrow[d, equal] \\ & \mathbb{Z}_{\ell}^{\times} \end{tikzcd}$$

et calculons pour $q \neq \ell$:

$$\boxed{\begin{aligned} \rho_N(Fr_q) &= q \in \mathbb{Z}_{\ell}^{\times} \quad (!) \\ &= N(q) \end{aligned}}$$

<u>N.B.</u> Ces deux cas sont différents en cela que χ_{Dir} est d'ordre fini, et N d'ordre infini.

Pour le cas général $\chi = \chi_{Dir} N^{a}$, on pose

$$\rho_{\chi} : G_{\mathbb{Q}} \longrightarrow GL(1, O_{L,\lambda})$$

par $\rho_{\chi} = \rho_{\chi_{Dir}} \cdot (\rho_N)^{a}$ …

- Etudions la ramification de ces caractères :

$$\rho : G_{\mathbb{Q}} \longrightarrow GL(1, O_{L,\lambda})$$

Alors $\operatorname{Ker}\rho \subset G_{\mathbb{Q}}$ est un sous-groupe fermé ; soit $\overline{\mathbb{Q}}^{\operatorname{Ker}\rho}$ le corps fixe : on étudie la ramification de $\overline{\mathbb{Q}}^{\operatorname{Ker}\rho}$.

$$\begin{tikzcd} \overline{\mathbb{Q}} \arrow[d, dash] \\ \overline{\mathbb{Q}}^{\operatorname{Ker}\rho} \arrow[d, dash, "\}\,\ell"] \\ \mathbb{Q} \end{tikzcd}$$

(1) Si $\chi = \chi_{Dir}$ de niveau m alors ρ_{χ} est ramifiée <u>au plus</u> en les $p \mid m$, par construction
(2) Pour ρ_N : ρ_N est ramifié <u>au plus</u> en ℓ, et de fait elle l'est

Pour $\chi = \chi_{Dir} |\cdot|^{a}$: au plus, $\rho_{\chi,\lambda}$ ramifie en $p \mid \ell m$, où bien sûr $\lambda \mid \ell$.

- <u>Question</u> : obtient-on toutes les $\rho : G_{\mathbb{Q}} \longrightarrow GL(1, O_{L,\lambda})$ de cette façon ? On impose évidemment la condition ci-dessous :
soit $\rho : G_{\mathbb{Q}} \longrightarrow GL(1, O_{L,\lambda})$ tel que ρ n'est ramifiée qu'en un nombre fini de places ; est-ce que $\rho = \rho_{\chi}$ pour un caractère

de Hecke algébrique χ ? Quel est alors le niveau et le poids de χ ?

Historiquement, on répond à cela en remarquant que ρ factorise par $G_{\mathbb{Q}}^{ab}$ et on connait ce groupe par la théorie du corps de classe.
On ne va pas procéder ainsi...

- L'analogue du théorème de Ribet

Soit $\rho : G_{\mathbb{Q}} \longrightarrow GL(1, \mathcal{O}_{L,\lambda})$ et supposons que $\rho = \rho_\chi$ pour χ caractère de Hecke algébrique de niveau m.

Considérons $\bar\rho : G_{\mathbb{Q}} \longrightarrow GL(1, \mathcal{O}_{L,\lambda}/_{\mathfrak{m}_\lambda})$.

ramifie dans ρ, mais as dans la éduction)

Si $\bar\rho$ est non-ramifiée ~~à~~ en un $q \nmid m$, existe-t-il un caractère χ' de niveau m/q tel que :

$$\bar\rho = \overline{\rho_{\chi'}} \quad ?$$

(ie est-ce que $\rho(Fr_q) \equiv \rho_{\chi'}(Fr_q) \pmod\lambda$?)

Ex. : deux caractères de Hecke algébriques

$\chi_1 = \chi_{Norm} = |\cdot|$ — $\rho_N : G_{\mathbb{Q}} \to GL(1, \mathbb{Z}_\ell^\times)$

$\chi_p : (\mathbb{Z}/_{(p)})^\times \longrightarrow \mathbb{C}^\times$

$\xi_{prim} \longmapsto e^{2i\pi/p}$ — $\rho_{\chi_p} : G_{\mathbb{Q}} \to GL(1, \mathbb{Z}[e^{2i\pi/p}]_\lambda)$

caractère cyclotomique aussi !

Prenons $\ell = p$: dans $\mathbb{Q}(e^{2i\pi/p})$, p est totalement ramifié, $p = (\mathfrak{p})^{p-1}$ et on a $\mathbb{Z}[e^{2i\pi/p}]_{\lambda = \mathfrak{p}} \simeq \mathbb{Z}_\ell$, d'où

$$\begin{tikzcd} \rho_N : G_{\mathbb{Q}} \arrow[r] & GL(1, \mathbb{Z}_p^*) \\ \rho_{\chi_p} : G_{\mathbb{Q}} \arrow[r] \arrow[dr] & GL(1, \mathbb{Z}_p^*) \arrow[d, bend left, "\text{réduction}"] \\ & (\mathbb{Z}/_{(p)})^\times \arrow[u] \end{tikzcd}$$

(car $x^{p-1}-1$ a p racines ds $\mathbb{Z}_p^\times$: $a, a^p, a^{p^2}, \ldots \in \mathbb{Z}_p$ et $a^{p^n} \to \alpha$, on a $\alpha^p = \alpha$)

N.B.

$$\begin{tikzcd} \mathbb{Z}_p^\times \arrow[r] & \mathbb{F}_p^\times \arrow[dl, "\text{(représentant de Teichmüller)}"] \\ \text{racines (p-1)-ème de l'unité} \arrow[u, phantom, "\cup"] & \end{tikzcd}$$

La réduction est scindée.

Fait : ρ_N et ρ_{χ_p} sont congruentes modulo p !

Dém. $\bar\rho_N$ et $\overline{\rho_{\chi_p}}$ sont la même application canonique

$$\mathbb{Z}_p^\times \longrightarrow \underbrace{(\mathbb{Z}/_{(p)})^\times}_{\text{racines (p-1)-èmes de l'unité}}$$

$\square$

Séminaire 1 (29-9 ; Tunnell)

Les conjectures de Serre

Référence : Serre, Duke Math. J. 54 (1) 1987, p°179-230
Ribet, dernier Bulletin of the Am. Math. Soc.
Darmon, "Serre's conjecture", to appear

- Objets d'études :

(I) Représentations galoisiennes de $G_{\mathbb{Q}} = Gal(\bar{\mathbb{Q}}/\mathbb{Q})$: on considère plus précisément $\rho : G_{\mathbb{Q}} \longrightarrow GL(2, \mathbb{F})$, où $\mathbb{F}$ est un corps fini de caractéristique p

[Variantes : (i) on peut penser à $\rho : G_{\mathbb{Q}} \longrightarrow GL(2, \overline{\mathbb{F}_p})$ d'image finie

(ii) $\operatorname{Ker}\rho \subset G_{\mathbb{Q}}$ est d'indice fini donc $G_K = \operatorname{Ker}\rho$ a comme corps fixe K, et ~~la~~ $K/\mathbb{Q}$ est une extension finie, et on a

$$\rho : Gal(K/\mathbb{Q}) \longrightarrow GL(2, \mathbb{F}) \quad]$$

$$\begin{tikzcd} \mathfrak{l}_1, \ldots, \mathfrak{l}_r & K \arrow[d, dash] \\ \ell & \mathbb{Q} \end{tikzcd}$$

ℓ premier dans $\mathbb{Z}$

$\mathfrak{l}_i \mid \ell$
$\cap$
$\operatorname{Spec} \mathcal{O}_K$

Supposons que ℓ ne se ramifie pas ; il existe alors un élément $\sigma \in Gal(K/\mathbb{Q})$ tel que :

(i) $\sigma \mathfrak{l}_i = \mathfrak{l}_i$

(ii) σ induit $\sigma : \mathcal{O}_K/\mathfrak{l}_1 \longrightarrow \mathcal{O}_K/\mathfrak{l}_1$ qui est le générateur canonique de $Gal(\mathcal{O}_K/\mathfrak{l}_1 / \mathbb{Z}/(\ell))$: $x \longmapsto x^\ell$

σ est défini à conjugaison près

(II) <u>Formes modulaires</u>: soit k un entier positif, N aussi, ε_0 un caractère de Dirichlet modulo N. On s'intéresse aux formes modulaires de type (k, N, ε_0) ie

$$f : \mathbb{H} \longrightarrow \mathbb{C}$$

telle que : - f est holomorphe

- $f\left(\frac{az+b}{cz+d}\right) = \varepsilon_0(d)\,(cz+d)^k f(z) \qquad \forall \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$
- le développement de Fourier de f est

$$f(z) = \sum_{n \geq 0} a_n q^n \quad , \quad q = e^{2i\pi z}$$

$\Rightarrow$ pour $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$, donne $1 = \varepsilon_0(-1)(-1)^k$

- <u>Exemples</u>:

(II) Formes modulaires : les séries d'Eisenstein

$$C^{te} \times \sum_{(m,n) \neq 0} \frac{1}{(mz+n)^{2k}} = F_{2k}(z)$$

<u>Fait</u>: F_{2k} est une forme modulaire de type $(2k, 1, \chi_0)$.
La C^{te} est choisie de sorte que

$$F_{2k}(z) = \frac{4k(-1)^k}{B_k} + \sum_{n \geq 1} \sigma_{2k-1}(n) q^n$$

Ici, on a donc $a_\ell(F_{2k}) = 1 + \ell^{2k-1}$ pour ℓ premier

(I) Une représentation galoisienne :

$$\begin{tikzcd} G_{\mathbb{Q}} \arrow[r, "\rho"] \arrow[d] & GL(2, \mathbb{F}_p) \arrow[d, equal] \\ (\mathbb{Z}/(p))^\times \simeq Gal(\mathbb{Q}(\mu_p)/\mathbb{Q}) \arrow[r, "1 \oplus \chi_p"] & GL(2, \mathbb{F}_p) \end{tikzcd}$$

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

(σ entier premier à p)

<u>NB</u> : soit $\ell \neq p$, ie ℓ ne ramifie pas dans $\mathbb{Q}(\mu_p)$, le Frobenius en ℓ est $\ell \in (\mathbb{Z}/(p))^\times$ et donc

$$\rho(Fr_\ell) = \begin{pmatrix} 1 & 0 \\ 0 & \ell \end{pmatrix}$$

Similairement, on a $\rho^k = 1 \oplus \chi_p^{2k-1} : \sigma \longmapsto \begin{pmatrix} 1 & 0 \\ 0 & \ell^{2k-1} \end{pmatrix}$
et on a pour tout $\ell \neq p$,

$$Tr(Fr_\ell) = 1 + \ell^{2k-1} \in \mathbb{F}_p$$

ie $\qquad Tr(\rho^k(Fr_\ell)) \equiv a_\ell(F_{2k}) \quad (p) \qquad !!$

<u>Idée de Serre</u>: ce genre de relation est-il général ?

<u>Conjecture de Serre</u> (forme "naïve")

Soit $\rho : G_{\mathbb{Q}} \longrightarrow GL(2, \mathbb{F})$ comme en (I), et supposons que :

- ρ est irréductible (ie pas comme dans l'exemple ...)
- $\rho(c_x)$, l'image de la conjugaison complexe, vérifie

$$\det(\rho(c_x)) = -1$$

(c'est le cas pour l'exemple des séries d'Eisenstein)

Alors : il existe une forme modulaire f d'un certain type (k, N, ε_0) telle que $f = \sum_{n \geq 1} a_n q^n$ et (a_n) engendre un corps de nombre $L/\mathbb{Q}$, et telle que pour presque tout ℓ premier, on a

$$Tr(\rho(Fr_\ell)) = a_\ell \quad \text{dans } \mathbb{F}'$$

pour un idéal premier $\mathfrak{p}$ de O_L tel que $\mathfrak{p} / p$ et tel que $\mathbb{F}'$ est un corps fini contenant $\mathbb{F}$ et $O_L/\mathfrak{p}$

[Ou : $Tr(\rho(Fr_\ell)) = a_\ell$ dans $\mathbb{F} = \overline{(O_L/\mathfrak{p})}$]

<u>N.B.</u> Autre motivation : on sait aller dans l'autre sens, d'une forme modulaire à une représentation.

<u>Pb.</u> : on ne peut pas tester cette conjecture car (k, N, ε_0) ne sont pas spécifiés !

- <u>Raffinements de la conjecture</u>

Il s'agit de prédire les paramètres de la forme modulaire ...
Etant donnée $\rho : G_{\mathbb{Q}} \longrightarrow GL(2, \mathbb{F})$, on veut donc définir un triplet (k, N, ε_0).

<u>Etape 1</u>. N dépend seulement de la restriction ρ / D_ℓ, où ℓ est premier, $\ell \neq p$, et D_ℓ est le groupe de décomposition

$$\begin{tikzcd} \ell_1 & K \arrow[d, dash] \\ \ell & \mathbb{Q} \end{tikzcd}$$

(i) Si ℓ n'est pas ramifiée dans $K/\mathbb{Q}$ ou $\ell = p$, alors $\ell \nmid N$.
(ii) Ensuite la formule pour N sera donnée dans le prochain exposé (ie les exposants des ℓ ramifiés dans N).

<u>Etape 2</u> k ne dépend que de la restriction ρ / D_p (p caractéristique de $\mathbb{F}$ toujours)

(N.B. dans l'exemple : $K = \mathbb{Q}(\mu_p)$, $N \mid p^\infty$, même $N = 1$ d'après (i) ci-dessus ; D_p = Gal complet)

On détermine d'abord $k \bmod (p-1)$ (cf. Eisenstein)
puis exactement

Etape 3 - Pour ε_0, partant de $\rho : G_{\mathbb{Q}} \longrightarrow GL(2, \mathbb{F})$, on a
$$\det\rho : G_{\mathbb{Q}} \longrightarrow \mathbb{F}^\times$$

racker
Weber

Fait (corollaire de la théorie du corps de classe) : si $E/\mathbb{Q}$ est une extension abélienne finie de $\mathbb{Q}$, alors $\mathrm{Gal}(E/\mathbb{Q})$ est un quotient de $(\mathbb{Z}/(m))^\times$ pour un certain m

Alors on a
$$\begin{tikzcd} & G_{\mathbb{Q}} \arrow[r, "\det\rho"] \arrow[d] & \mathbb{F}^\times \\ (\mathbb{Z}/(m))^\times \arrow[r] & G_{E/\mathbb{Q}} \arrow[ur] \arrow[r] & 1 \end{tikzcd}$$

ordre p^k

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

$\mathbb{Z}/(p^k))^\times, k \geq 2$

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

et on peut considérer $\det\rho$ comme une flèche
$$\begin{tikzcd} \det\rho : (\mathbb{Z}/(m))^\times \arrow[r] \arrow[d] & \mathbb{F}^\times \\ (\mathbb{Z}/(pm'))^\times \arrow[ur] & \end{tikzcd}$$
ordre $p^r - 1$ pour un r
ie premier à p

Donc cela se factorise: $(\mathbb{Z}/(pm'))^\times$ [où $(m', p) = 1$]
$$\| $$
$$(\mathbb{Z}/(p))^\times \times (\mathbb{Z}/(m'))^\times$$

On note alors φ et ε les deux restrictions
$$\varphi = (\det\rho) \mid (\mathbb{Z}/(p))^\times$$
$$\varepsilon = (\det\rho) \mid (\mathbb{Z}/(m'))^\times$$

Mais les éléments de $\mathbb{F}^\times$ d'ordre $p-1$ sont les racines $(p-1)$-èmes de l'unité, ie un groupe d'ordre $p-1 \simeq (\mathbb{Z}/(p))^\times$.

Soit χ_p la flèche
$$\begin{tikzcd} G_{\mathbb{Q}} \arrow[r, "\chi_p"] \arrow[dr] & (\mathbb{Z}/(p))^\times \arrow[r, phantom, "\simeq"] & \mathbb{F}^\times \\ & \mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q}) \arrow[u, "\wr"] & \end{tikzcd}$$

Alors toutes les flèches φ comme ci-dessus doivent s'écrire
$$\varphi = \chi_p^h$$
où h est un entier, <u>bien déterminé modulo $p-1$</u>.

<u>Récap</u> partant de ρ, on va produire N, k (mod $p-1$) et ε_0 : on a bien commencé...

<u>Groupes de Galois d'extensions de $\mathbb{Q}_\ell$</u>

$$\begin{tikzcd} \overline{\mathbb{Q}_\ell} \arrow[d, dash, "G_{\mathbb{Q}_\ell}"] \\ \mathbb{Q}_\ell \end{tikzcd}$$
se découpe assez bien pour commencer :
$$\begin{tikzcd} \overline{\mathbb{Q}_\ell} \arrow[d, dash, "J"] \\ K_t \arrow[d, dash] \\ \mathbb{Q}_\ell^{nr} = \mathbb{Q}_\ell(x \mid x^d = 1,\ (d, \ell) = 1) \arrow[d, dash, "\text{pas de ramification}"'] \\ \mathbb{Q}_\ell \end{tikzcd}$$
I

<u>$\mathrm{Gal}(\mathbb{Q}_\ell^{nr}/\mathbb{Q}) \simeq \mathrm{Gal}(\overline{\mathbb{F}_\ell}/\mathbb{F}_\ell)$</u>

[où K_t - extension modérément ramifiée - est
$\mathbb{Q}_\ell^{nr}(x \mid x^d \in \mathbb{Q}_\ell^{nr},\ (d, \ell) = 1,$]

<u>Fait</u> : J est le ℓ-groupe maximal inclus dans I.

<u>2-10-95</u>

On revient aux caractères de Hecke algébriques (sur $\mathbb{Q}$):
(i) caractères de Dirichlet $(\mathbb{Z}/(N))^\times \longrightarrow \mathbb{C}^\times$
(ii) N, le caractère "norme"
$$N((n)) = |n|$$
et les produits $\chi = \chi_{Dir} N^k$, $k \in \mathbb{Z}$ (niveau N, poids k).

On associe à χ une représentation $\rho_\chi : G_{\mathbb{Q}} \longrightarrow GL(1, O_{L,\lambda})$ où L est le corps engendré par les valeurs de χ ($\Leftrightarrow$ par les valeurs de χ_{Dir}), et λ est n'importe quel idéal premier de O_L.

Soit ℓ tel que $\lambda \mid \ell$ [ℓ premier].

L'idée était :

$$\begin{tikzcd} G_{\mathbb{Q}} \arrow[d] & & G_{\mathbb{Q}} \arrow[d] & \\ \mathrm{Gal}(\mathbb{Q}(\mu_N)/\mathbb{Q}) \simeq (\mathbb{Z}/(N))^\times & & \mathrm{Gal}(\mathbb{Q}(\mu_{\ell^\infty})/\mathbb{Q}) \simeq \mathbb{Z}_\ell^\times & \varprojlim (\mathbb{Z}/(\ell^k))^\times \arrow[l] \end{tikzcd}$$

et on fait les produits correspondant à la décomposition de χ :

$$\chi_{Dir} : G_{\mathbb{Q}} \xrightarrow{\rho_\chi} \mathcal{O}_L^\times \hookrightarrow \mathcal{O}_{L,\lambda}^\times$$
$$N : G_{\mathbb{Q}} \longrightarrow \mathbb{Z}_\ell^\times \hookrightarrow \mathcal{O}_{L,\lambda}$$
$$\Rightarrow \boxed{\rho_\chi : G_{\mathbb{Q}} \longrightarrow \mathcal{O}_{L,\lambda}^\times}$$

On note $\bar{\rho}_\chi : G_{\mathbb{Q}} \longrightarrow \mathcal{O}_{L,\lambda}^\times \longrightarrow (\mathcal{O}_{L,\lambda}/\lambda)^\times$ la réduction modulo λ de ρ_χ.

N.B. Cette représentation ρ_χ est non-ramifiée en dehors de N et de ℓ.

Question (analogue de Ribet). Supposons que $\bar{\rho}_\chi$ est non-ramifiée en un nombre premier q, et que $q \mid N$.
Existe-t-il alors un caractère de Hecke algébrique χ' de niveau N/q tel que $\bar{\rho}_{\chi'} = \bar{\rho}_\chi$?

Théorème. Si χ est un caractère de Hecke algébrique de niveau N et poids k et $\bar{\rho}_\chi$ est non-ramifiée en $q \mid N$, alors il existe χ' de niveau N/q (et de poids k') tel que $\bar{\rho}_{\chi'} = \bar{\rho}_\chi$.

Dém. On utilise la construction explicite :
(i) Si $q \neq \ell$: N n'a pas de ramification en q i.e. ρ_N n'est pas ramifiée à q, donc en fait l'hypothèse implique χ_{Dir} modulo λ est non-ramifiée :

$$\begin{tikzcd} \mathbb{Q}(\mu_N) \arrow[d, dash, "(\mathbb{Z}/(N))^\times"'] \\ \mathbb{Q} \end{tikzcd}$$
$$(\mathbb{Z}/(N))^\times = (\mathbb{Z}/q^\nu)^\times \times (\mathbb{Z}/(N'))^\times$$

et donc $\underset{\eta}{\chi_{Dir} \mid (\mathbb{Z}/q^\nu)^\times} \equiv 1$ modulo λ (*)

On considère $\chi' = \chi\eta^{-1}$: c'est un caractère de Hecke algébrique, et (*) dit qu'en réduisant on a :

$$\bar{\rho}_\chi = \bar{\rho}_{\chi'}$$

Mais χ' est de niveau N/q^ν ...
Remarquons que χ' est de poids k'.
(ii) Si $q = \ell$:
[Exemple : $\chi = N\chi_\ell^{-1}$, où $\chi_\ell : (\mathbb{Z}/(\ell))^\times \longrightarrow \mathbb{C}^\times$, $\xi \longmapsto e^{2i\pi/\ell}$

caractère cyclotomique ; racine ℓ-ième primitive de 1 ; (naturelle)

on a $(\mathbb{Z}/(\ell))^\times \hookrightarrow \mathbb{Z}_\ell^\times$ (Teichmüller)

On remarque que $\bar{\rho}_\chi$ est non-ramifiée en ℓ (le niveau de χ est ℓ), et ensuite on observe que $\chi' \equiv 1$ (niveau 1, poids 0) vérifie :

$$\bar{\rho}_{\chi'} = 1 = \bar{\rho}_\chi$$

Mais le poids a changé !]

Dans le cas général, $\rho_\chi : G_{\mathbb{Q}} \to \mathcal{O}_{L,\lambda}^\times$ vérifie
$\bar{\rho}_\chi : G_{\mathbb{Q}} \to (\mathcal{O}_{L,\lambda}/\lambda)^\times$ non-ramifiée en ℓ.

Or par construction $\rho_\chi = \rho_{\chi_{Dir}} \rho_N^k$, et

$$\rho_\chi : G_{\mathbb{Q}} \longrightarrow \mathrm{Gal}(\mathbb{Q}(\mu_N, \mu_{\ell^\infty})/\mathbb{Q}) \longrightarrow \mathcal{O}_{L,\lambda}^\times$$

On réduit modulo λ :

$$\bar{\rho}_\chi : G_{\mathbb{Q}} \longrightarrow \underbrace{\mathbb{F}^\times}_{\text{d'ordre premier à } \ell}, \text{ où } \mathrm{char}\, \mathbb{F} = \ell$$

$$\begin{tikzcd} \mathbb{Q}(\mu_N, \mu_{\ell^\infty}) \arrow[d, dash] \\ \mathbb{Q}(\mu_N) \arrow[d, dash] \\ \mathbb{Q} \end{tikzcd}$$
$\mathbb{Z}_\ell^\times$, $(\mathbb{Z}/(N))^\times$

En réduisant, la ℓ-partie doit s'annuler car c'est un ℓ-groupe.
Donc $\bar{\rho}_\chi$ non-ramifiée $\Rightarrow \chi_{Dir} \mid (\mathbb{Z}/\ell^{v_\ell(n)})^\times \equiv \chi_\ell^{-k}$ (λ)

On construit maintenant $\chi' = \underbrace{\chi_{Dir} \left(\chi_{Dir} \mid (\mathbb{Z}/(\ell^{v_\ell(n)}))^\times\right)^{-1}}_{\text{non-ramifié en } \ell} N^j$
de niveau $N' \mid N/\ell$, $N' = N/\ell^{v_\ell(n)}$, de poids j.

On va ajuster maintenant j ... Calculons

$$\bar{\rho}_{\chi'} = \underbrace{\bar{\rho}_{\chi_{Dir}} \bar{\rho}_{\chi_\ell}^{-k}}_{\bar{\rho}_\chi} \bar{\rho}_{\chi_\ell}^{j} \quad (\Rightarrow j = 0 \dots)$$

Donc en fait χ' est juste un caractère de Dirichlet, de niveau N/ℓ^ν, de poids 0 □

N.B. En ajoutant au cas $\ell = p$ la condition " χ de poids 0", le niveau ne change pas non plus...

Rappel:

Th. (Wiles) Etant donnée $\rho : G_{\mathbb{Q}} \longrightarrow GL(2, \mathbb{Z}_\ell)$ vérifiant certaines conditions techniques, il existe une forme modulaire f de poids 2 telle que pour presque tout ℓ

$$a_\ell = Tr(\rho(Fr_\ell))$$

Théorème. (Analogue pour $GL(1)$)

Etant donnée $\rho : G_{\mathbb{Q}} \longrightarrow \mathbb{Z}_\ell^*$ (ou $O_{L,\lambda}^*$, $L/\mathbb{Q}$ finie), il existe un caractère de Hecke algébrique χ tel que

$$\rho = \rho_\chi$$

(ie $\rho(Fr_\ell) = \chi(\ell)$ pour presque tout ℓ)

L'idée principale de Wiles est d'user d'un autre théorème:

Th. (Wiles) Soit $\rho_0 : G_{\mathbb{Q}} \longrightarrow GL(2, \mathbb{Z}_\ell)$ une représentation ℓ-adique (avec conditions techniques). Supposons qu'il existe une forme modulaire f, avec $a_\ell = Tr(\rho_0(Fr_\ell))$.

Alors si $\rho : G_{\mathbb{Q}} \longrightarrow GL(2, \mathbb{Z}_\ell)$ vérifie $\overline{\rho} \simeq \overline{\rho_0}$ (modulo ℓ), ρ est également associée à une forme modulaire ρ (modulo hypothèses techniques).

N.B. Cela incite à étudier les formes modulaires congruentes à une certaine forme, et les représentations congruentes à une représentation

On veut prouver ici (cas $GL(1)$) l'analogue:

(**) Th. Etant donnée $\rho_0 : G_{\mathbb{Q}} \longrightarrow \mathbb{Z}_\ell^*$ telle que $\rho_0 = \rho_\chi$ pour un caractère de Hecke algébrique χ (avec hyp. supplémentaires).

Alors toute $\rho : G_{\mathbb{Q}} \longrightarrow \mathbb{Z}_\ell^*$ telle que $\overline{\rho} = \overline{\rho_0}$ vérifie: il existe χ', caractère de Hecke algébrique, tel que

$$\rho_{\chi'} = \rho.$$

Admettons que cela soit fait, et déduisons-en le théorème de Kronecker-Weber:

Th. Toute extension abélienne de degré fini de $\mathbb{Q}$ est contenue dans une extension cyclotomique.

Dém. Soit $E/\mathbb{Q}$ abélienne finie ; on a

$$G = Gal(E/\mathbb{Q})$$

est un produit de groupes cycliques d'ordre une puissance de p, donc on a

$$\begin{tikzcd}
 & E \arrow[dd, dash] \\
F \arrow[ur, dash] \arrow[dr, dash, "\text{cyclique d'ordre une puissance de } p"'] & \\
 & \mathbb{Q}
\end{tikzcd}$$

et on peut donc par théorie de Galois supposer que G est cyclique d'ordre ℓ^n.

$$\begin{tikzcd}
 & E(\mu_\ell) \\
E \arrow[ur, dash] \arrow[dd, dash] & \\
 & \mathbb{Q}(\mu_\ell) \arrow[uu, dash, "\mathbb{Z}/(\ell^n)"'] \\
\mathbb{Q} \arrow[ur, dash, "(\mathbb{Z}/(\ell))^*"] &
\end{tikzcd} \quad \left(\mathbb{Z}/(\ell^{n+1})\right)^*$$

On peut considérer $E(\mu_\ell)$ et on a une flèche

$$\begin{tikzcd}
G_{\mathbb{Q}} \arrow[r] \arrow[rr, bend right, "\rho"'] & Gal(E/\mathbb{Q}) \arrow[r] & \left(\mathbb{Z}/(\ell^{n+1})\right)^*
\end{tikzcd}$$

Si on peut relier cette flèche à un $\chi = \chi_{0,r} N^k$, G aura des relations avec des groupes de Galois cyclotomiques.

Trivialement (pour $E(\mu_\ell)$) la réduction modulo ℓ est ce qu'on veut, puisque c'est la flèche $G_{\mathbb{Q}} \longrightarrow (\mathbb{Z}/(\ell))^*$ associée à $\mathbb{Q}(\mu_\ell)/\mathbb{Q}$, ie au caractère cyclotomique ◇

Preuve de (**):

On a $\rho_0 : G_{\mathbb{Q}} \longrightarrow O_{L,\lambda}^*$ telle que $\rho_0 = \rho_{\chi_0}$

Considérons $\rho : G_{\mathbb{Q}} \longrightarrow O_{L,\lambda}^*$ telle que $\overline{\rho} = \overline{\rho_0}$ $(= \overline{\rho_{\chi_0}})$, et essayons de classifier toutes ces $\overline{\rho}$. Cela amène à la notion de déformation:

Soit A une $O_{L,\lambda}$-algèbre (ex. $O_{L,\lambda}/\lambda^n$), locale (m idéal maximale), telle que $A/m \simeq O_{L,\lambda}/\lambda$ $(= k)$.

On veut classifier les représentations $\rho : G_{\mathbb{Q}} \longrightarrow A^\times$ telles que $\bar{\rho} = \bar{\rho_0}$ donnée.

$$\begin{tikzcd}
G_{\mathbb{Q}} \arrow[r] \arrow[dr, "\bar{\rho_0}"'] & A^\times \arrow[d] \\
& (A/m)^\times
\end{tikzcd}$$

N.B. Si ρ_1 et ρ_2 sont deux telles représentations, alors on voit que $\rho_1\rho_2^{-1} : G_{\mathbb{Q}} \longrightarrow A^\times$ vérifient $\overline{\rho_1\rho_2^{-1}} = 1$, ie

$$\rho_1\rho_2^{-1}(g) \equiv 1 \quad (\text{modulo } m)$$

Programme : soit le foncteur de la catégorie des algèbres A locales artiniennes, de corps résiduel $O_{L,\lambda}/\lambda$ dans celle des ensembles

$$\Phi : A \longmapsto \{\rho : G_{\mathbb{Q}} \longrightarrow A^\times \mid \bar{\rho} = \bar{\rho_0}\}/_{\text{isom.}}$$

Alors ce foncteur est représentable.

10/95) On est dans la situation suivante : on s'intéresse aux flèches

$$G_{\mathbb{Q}} \xrightarrow{\rho} O^\times$$

où O est l'anneau des entiers d'une extension finie de $\mathbb{Q}_\ell$.
Considérons plus généralement des O-algèbres locales A, d'idéal maximal m_A, telles que $A/m_A \simeq O/m_O = k$, et A noethérienne
(ex. $O = \mathbb{Z}_\ell$, $A = \mathbb{Z}_\ell/(\ell^n)$)

But : Classifier tout les homomorphismes $\rho : G_{\mathbb{Q}} \longrightarrow A^\times$, tels que la "réduction" à k est isomorphe à ρ_0, ρ_0 étant donnée.

$$\begin{tikzcd}
G_{\mathbb{Q}} \arrow[r] \arrow[dr, "\rho_0"'] & A^\times \arrow[d] \\
& k^\times
\end{tikzcd}$$

On veut se ramener à un problème d'algèbre commutative...

Proposition. Il existe une O-algèbre commutative locale (noethérienne) (de corps résiduel k) R et une flèche $\rho_u : G_{\mathbb{Q}} \longrightarrow R^\times$ telle que pour toute représentation $\rho : G_{\mathbb{Q}} \longrightarrow A^\times$ il existe une flèche d'algèbres $R \xrightarrow{\varphi} A$ pour laquelle le diagramme suivant commute

$$\begin{tikzcd}
& R^\times \arrow[d, "\varphi"] \\
G_{\mathbb{Q}} \arrow[ur, "\rho_u"] \arrow[r] \arrow[dr] & A^\times \arrow[d] \\
& k^\times
\end{tikzcd}$$

Algèbres de groupes

Soit G un groupe, O une algèbre ; la O-algèbre du groupe G est l'algèbre notée $O[G]$ des combinaisons linéaires formelles $\sum_{g\in G} \alpha_g g$ avec

$$\left(\sum \alpha_g g\right)\cdot\left(\sum \beta_{g'} g'\right) = \sum \alpha_{gg'}(gg')$$

(N.B. Attention, si G n'est pas abélien, cela n'est pas une algèbre commutative)

La propriété universelle de $O[G]$ est : pour tout homomorphisme de groupe $G \longrightarrow H$, il existe une flèche d'algèbres

$$O[G] \longrightarrow O[H]$$

associée.

Si G est un groupe fini, $O[G]$ est clairement noethérienne (si O l'est). Mais ici on est intéressé par $G_{\mathbb{Q}}$ qui est passablement gros...

$$\begin{tikzcd}
L_\Sigma \arrow[d, dash] \\
\mathbb{Q}
\end{tikzcd}$$

Supposons qu'on se donne un ensemble Σ fini de nombres premiers et qu'on considère les extensions $L/\mathbb{Q}$ non-ramifiée en dehors de Σ, en particulier L_Σ l'extension maximale non-ramifiée en dehors de Σ (existe, car si L_1, L_2 vérifient cette propriété, L_1L_2 la vérifie aussi...)
Soit G_Σ le groupe de Galois de cette extension ; ce groupe est beaucoup moins gros que G.

Proposition. G_Σ est un groupe pro-fini topologiquement de type fini.

/10/95) Séminaire 2 (Tunnell)

$G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, $\mathbb{F}$ corps fini de caractéristique p

$$\mathbb{F}_p \longrightarrow \mathbb{F} \longrightarrow \overline{\mathbb{F}_p}$$

On se donne

$$\rho : G_{\mathbb{Q}} \longrightarrow GL(2, \mathbb{F})$$

La <u>conjecture fondamentale</u> est : il existe une forme modulaire f associée à ρ, au sens où on a $f = \sum a_n q^n$, avec $a_n \in L$ un corps de nombre, et un idéal premier $\mathfrak{p} \subset O_L$ divisant p, tel que pour presque tout nombre premier ℓ,

$$\mathrm{tr}(\rho(\mathrm{Fr}_\ell)) \equiv a_\ell \quad (\text{modulo } \mathfrak{p})$$

Le cas intéressant est celui où ρ est irréductible.

Le raffinement de cette conjecture est de prédire le poids, le niveau et le caractère de f.

Le niveau n'est divisible que par des nombres premiers inclus dans $\{p\} \cup \{\ell \mid \rho \text{ est ramifiée en } \ell\}$.

Ici on s'intéresse au poids.

<u>Structure des extensions de $\mathbb{Q}_p$</u>

$$\begin{array}{lll}
\overline{\mathbb{Q}_p} & & \\
| & \Big]\, P & \\
\mathbb{Q}_p^{nr}(z^{1/d} \mid (d,p)=1) = \mathbb{Q}_p^t & & \Big]\, I \\
| & & \\
\mathbb{Q}_p(\zeta \mid \zeta^d=1, (d,p)=1) = \mathbb{Q}_p^{nr} & & \\
| & & \\
\mathbb{Q}_p & &
\end{array}$$

extension maximale modérément ramifiée de $\mathbb{Q}_p$

$_\ell|\mathbb{Q}_p)$

On a $G_{\mathbb{Q}_p} \supset I \supset P$

<u>Faits</u> : P est un pro-p-groupe, même le pro-p-ss-groupe maximale de $G_{\mathbb{Q}_p}$

- $G_{\mathbb{Q}}/I \simeq \mathrm{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p)$
- $I_t := I/P$ est déterminé (cf. plus loin)

$$I_t \simeq \varprojlim_{(d,p)=1} \mu_d$$

On peut considérer $\mathbb{Z}_p \subset \mathbb{Q}_p$; si on fait l'extension (finie) $\mathbb{Q}(\zeta^d = 1)$, $(d,p)=1$, on a

$$\begin{array}{ccccc}
\mathfrak{p} & \subset \mathbb{Z}_p[\zeta] & \subset & \mathbb{Q}_p(\mu_d) \\
| & & & | \\
(p) & \subset \mathbb{Z}_p & \subset & \mathbb{Q}_p
\end{array}$$

On a $\mathrm{Gal}(\mathbb{Q}_p(\zeta)/\mathbb{Q}_p) \longrightarrow \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$

avec $d \mid p^n - 1$

$$\begin{array}{ll}
\mathbb{Q}_p(z^{1/d}) & \\
| & \Big)\, \mu_d \\
\mathbb{Q}_p(\xi) & \\
| & \\
\mathbb{Q}_p &
\end{array}$$

$\xi^d = 1$

$\sigma \in \mathrm{Gal}(\mathbb{Q}_p(z^{1/d})/\mathbb{Q}_p(\xi))$

$$\Rightarrow \frac{\sigma(z^{1/d})}{z^{1/d}} \in \mu_d$$

En mettant tout cela ensemble par limite projective :

$$I_t = I/P = \varprojlim_{(d,p)=1} \mu_d$$

et tout les quotients n'ont pas de p-partie.

On a aussi $I_t \simeq \varprojlim \mathbb{F}_{p^n}^\times$ car tout d, $(d,p)=1$, vérifie $d \mid p^n - 1$ pour un certain n ($n = \mathrm{ord}_{\mathbb{Z}/(d)}(p)$ convient)

On va étudier ρ en la restreignant à I, P, ...

Soit φ un caractère $I_t \xrightarrow{\varphi} \overline{\mathbb{F}}^\times$, $\mathbb{F}$ corps fini

(i) Comme $I_t = \varprojlim \mathbb{F}_{p^n}^\times$, φ se factorise en $I_t \to \mathbb{F}_{p^n}^\times \to \overline{\mathbb{F}}^\times$

et on dit que φ est de <u>niveau n</u> si elle ne se factorise pas par un n plus petit.

<u>Ex</u> Niveau 1 : $I_t \xrightarrow{\varphi} \mathbb{F}_p^\times$

(Les caractères de niveau d/N forment un groupe)

∘ "Propriétés galoisiennes des points d'ordre fini des courbes elliptiques"

<u>Caractères fondamentaux de niveau n :</u>

si $\mathbb{F}_{p^n}^\times = \mathbb{F}^\times$, on a déjà des automorphismes de corps

$$\mathbb{F}_{p^n} \xrightarrow{\sigma} \mathbb{F}_{p^n}$$

qui induisent des caractères

$$I_t \xrightarrow{\varphi} \mathbb{F}_{p^n}^\times \xrightarrow{\sigma} \mathbb{F}_{p^n}^\times \longrightarrow \overline{\mathbb{F}}^\times$$

appelés fondamentaux : il y en a n, et en les élevant à une puissance entière, on en obtient d'autres.

<u>Fait</u> : tout caractère de niveau n est le produit de puissances de caractères fondamentaux (cf. Serre, Invent. Math. 15, 1972)

<u>Dém.</u> (i) <u>$n=1$</u> :

$$I_t \longrightarrow \mathbb{F}_p^\times \longrightarrow \overline{\mathbb{F}}^\times$$

Il n'y a qu'un caractère de niveau 1 fondamental, noté χ ; $\mathbb{F}_p^\times$ est cyclique donc tout autre caractère est χ^k, $0 \leq k \leq p-2$.

(ii) <u>$n=2$</u> :

$$\begin{tikzcd}
I_t \arrow[r] & \mathbb{F}_{p^2}^\times \arrow[r] \arrow[d] \arrow[dr] & \overline{\mathbb{F}}^\times \arrow[d, phantom, "\cup"] \\
& \text{ordre } (p^2-1) & \mathbb{F}_{p^2}^\times
\end{tikzcd}$$

On a deux flèches naturelles

$$\mathbb{F}_{p^2} \xrightarrow{Id} \mathbb{F}_{p^2} \qquad \varphi_1 \quad (\text{fondamental})$$

$$\mathbb{F}_{p^2} \xrightarrow{x \mapsto x^p} \mathbb{F}_{p^2} \qquad \varphi_2 = \varphi_1^p \quad (\text{fondamental})$$

Si φ est un autre : le nbre de ceux-ci est

$$p(p-1) = p^2 - p = \varphi(p^2)$$

car φ doit envoyer le générateur de $\mathbb{F}_{p^2}^\times$ sur une racine (p^2-1)-ème de 1 qui n'est pas une racine $(p-1)$-ème de l'unité (pour que le niveau soit vraiment 2)

Mais en considérant $\varphi_1^a \varphi_2^b$, on parvient à trouver $\varphi(p^2)$ caractères de niveau n.

On n'aura pas besoin d'autres cas donc on s'arrête là...

◇

$$G_{\mathbb{Q}_p} \supset I \supset P$$

<u>Lemme</u> Soit V un $\mathbb{F}$-e-v de dimension finie et supposons qu'on a une application $G_{\mathbb{Q}_p} \xrightarrow{\rho_p} GL(n, V) \simeq Aut(V)$

Soit V^{ss} la semi-simplifiée de ρ_p.

Alors P agit trivialement sur V^{ss}.

<u>Dém.</u> On peut supposer ρ_p semi-simple, ie $V = V^{ss}$, puis on peut supposer (V, ρ_p) irréductible.

Notons

$$V^P = \{ v \in V \mid gv = v, \ \forall g \in P \}$$

<u>Fait</u> : $V^P \neq 0$

En effet,

$$\begin{tikzcd}
G_{\mathbb{Q}} \arrow[r] \arrow[d, phantom, "\cup"] & GL(n, \mathbb{F}) \\
P \arrow[r] & \overline{P} \arrow[u] \arrow[d] \\
& \text{quotient fini}
\end{tikzcd}$$

P agit via un quotient $\overline{P}$ fini qui est un p-groupe

On a donc un p-groupe fini agissant sur $V \setminus \{0\}$ d'ordre premier à p ; or, notoirement, un p-groupe agissant sur un ensemble S avec $p \nmid |S|$ possède un point fixe.

$$\Big(|S| = \sum_{\mathcal{O} \text{ orbite}} |\mathcal{O}| = \sum \underbrace{|P/P_x|}_{\text{divisible par } p, \text{ ou égal à } 1}$$

comme $p \nmid |S|$, il doit y avoir des 1...)

Ensuite, on sait que $P \lhd I \lhd G_{\mathbb{Q}_p}$, et même $P \lhd G_{\mathbb{Q}_p}$ (car P est le p-groupe maximal dans I, ce qui est une condition invariante).

Or V est irréductible, $V^P \neq 0$, et par normalité V^P est une sous-représentation, donc $V^P = V$ et P agit trivialement

□

Maintenant, étant donnée $\rho : G_{\mathbb{Q}} \longrightarrow GL(2, \mathbb{F})$, on considère

$$\rho_p = \rho|_{D_p} : Gal(\overline{\mathbb{Q}}_p/\mathbb{Q}_p) \longrightarrow GL(2, \mathbb{F})$$

$$\begin{matrix} \triangledown \\ I \\ \triangledown \\ P \end{matrix}$$

<u>N.B.</u> $\left\{ \mathbb{Z}/(p) \hookrightarrow GL(2, \mathbb{F}_p) \right.$, $a \longmapsto \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$ action de $\mathbb{F}_p$ sur $\mathbb{F}_p^2$

avec $\begin{pmatrix} * \\ 0 \end{pmatrix} \subset \mathbb{F}_p^2$ qui est une sous-représentation, mais ce n'est pas une représentation semi-simple)

Dans la semi-simplification de ρ, $I/_P$ agit sur V^{ss} par le lemme; or $I/_P$ est abélien et finalement on doit avoir

$$I/_p \text{ agit via } \varphi_1 \oplus \varphi_2$$

(somme directe de deux caractères) ; on utilise que "l'ordre" de $I/_p$ est premier à celui de $\mathbb{F}^2$

Faisons agir $G_{\mathbb{Q}_p}$ sur I, P par conjugaison:

produit
mi-direct

$$\begin{tikzcd} \mathbb{Q}_p(z^{1/d}) \arrow[d, dash, "\mu_d"] \\ \mathbb{Q}_p(\mu_d) \arrow[d, dash] \\ \mathbb{Q}_p \end{tikzcd}$$

calculons : soit $F_r \in \mathrm{Gal}(\mathbb{Q}_p(\mu_d)/\mathbb{Q}_p)$

$\sigma \in \mathrm{Gal}(\mathbb{Q}_p(z^{1/d})/\mathbb{Q}_p(\mu_d))$

$\sigma(z^{1/d})/z^{1/d} \in \mu_d$

$(*) \qquad \sigma(z^{1/d}) = u\, z^{1/d}$

Supposons $F_r(u) = u^p$; on applique à $(*)$:

$$F_r(\sigma(z^{1/d})) = u^p F_r(z^{1/d})$$

Fait : $F_r \circ \sigma \circ F_r^{-1} = \sigma^p$

(...)

Soit G un groupe, $G \xrightarrow{\rho} \mathrm{Aut}\, V$ une représentation, $I \triangleleft G$ un sous-groupe normal.

Alors posons, pour $g \in G$, $\rho^g(h) = \rho(ghg^{-1})$, qui est une représentation équivalente à ρ, agissant sur I.

Comme ici $I/_p$ agit par $\varphi_1 \oplus \varphi_2$, la conjugaison par g ne peut "qu'arranger la diagonale" ie permuter φ_1 et φ_2 ; en particulier

$$\varphi_1 \oplus \varphi_2 \simeq \varphi_1^p \oplus \varphi_2^p$$

De $\rho : G_{\mathbb{Q}} \longrightarrow Gl(2, \mathbb{F})$ on a produit une paire de caractères de I_t, $\varphi_1, \varphi_2 : I_t \longrightarrow \mathbb{F}^\times$, tels que

$$\{\varphi_1, \varphi_2\} = \{\varphi_1^p, \varphi_2^p\}$$

1^er^ cas $\quad \varphi_1 = \varphi_1^p$ et $\varphi_2 = \varphi_2^p$

2^e^ cas $\quad \varphi_1^p = \varphi_2$ et $\varphi_2^p = \varphi_1$

Dans le 1^s^ cas, les valeurs de φ sont des racines (p-1)-èmes de l'unité, donc φ_1, φ_2 se factorisent par $\mathbb{F}_p^\times$, ie φ_1 et φ_2 sont de niveau 1.

Dans le 2^e^ cas, on a $\varphi_1^{p^2} = 1$, ie les valeurs de φ_1 sont des racines (p^2-1)-èmes de 1, donc le niveau de φ_1, et φ_2, doit être 2.

Enfin, la recette donnant le poids k:

1^s^ cas : φ_1 et φ_2 de niveau 2

$G_{\mathbb{Q}_p} \to \mathrm{Aut}\, V$

Fait : dans ce cas, la représentation V originale était irréductible.
(Sinon, on aurait $W \subset V$ de dimension 1 stable par $G_{\mathbb{Q}_p}$, soit w une base. On peut alors calculer $\rho|W$: W est un "caractère" de $G_{\mathbb{Q}_p}$, donc on a

$$\begin{tikzcd} G_{\mathbb{Q}_p} \arrow[r, "W"] & \mathbb{F}^\times \\ I \arrow[u, phantom, "\cup"] & \end{tikzcd}$$

par restriction, φ_1 et φ_2 doivent être de niveau 1)

On écrit alors φ_1 et φ_2 comme produits de puissances des caractères fondamentaux ψ et ψ' de niveau 2 :

$$\varphi_1 = \psi^a \psi'^b \qquad (\varphi_2 = \varphi_1^p = \dots)$$
$$= \psi^{a+pb}$$

On peut supposer $0 \leq a \lesssim b \leq p-1$ car ψ est d'ordre p^2-1 et alors a et b sont bien déterminés.

Définition - Dans ce cas on pose $\boxed{k = 1 + pa + b}$

(N.B. si $b = a$, $\psi^{(p+1)k}$ est d'ordre $p-1$ donc de niveau 1)

9/10/95

$\mathcal{O}$ anneau des entiers d'une extension finie de $\mathbb{Q}_\ell$ ($\Rightarrow \mathcal{O}$ est noethérienne, locale, $\mathcal{O}/_{m_{\mathcal{O}}} \simeq k$, extension finie de $\mathbb{F}_\ell$.)

Soit $\mathcal{C}$ la catégorie des $\mathcal{O}$-algèbres locales A telles que A est complète, et $A/_{m_A} \simeq k$.

Ex. $\forall k \geqslant 1$, $\mathcal{O}/_{m_{\mathcal{O}}^k} \in \mathcal{C}$

On se donne G, un groupe abélien profini (ex: $Gal(L/\mathbb{Q})$, L extension abélienne de $\mathbb{Q}$)

Donnée de base : on dispose d'un homomorphisme

$$\bar{\rho}_0 : G \longrightarrow k^\times$$

But : classifier les morphismes $G \xrightarrow{\rho} A^\times$, $A \in \mathcal{C}$ tq

$$\bar{\rho} = \bar{\rho}_0.$$

On définit donc l'ensemble $Def(\bar{\rho}_0, A)$ des déformations de $\bar{\rho}_0$ dans une algèbre A

$$Def(\bar{\rho}_0, A) = \{ \rho : G \longrightarrow A^\times \mid \rho \equiv \bar{\rho}_0 \bmod m_A \}$$

ie

$$\begin{tikzcd} G \arrow[r, "\rho"] \arrow[dr, "\bar{\rho}_0"'] & A^\times \arrow[d] \\ & k^\times \end{tikzcd} \quad \text{commute}$$

Théorème. (1) Il existe un anneau $R \in \mathcal{C}$ et une déformation de $\bar{\rho}_0$ dans R, $\rho^{un} : G \longrightarrow R^\times$, telle que pour tout $A \in \mathcal{C}$, on a un isomorphisme canonique

$$Def(\bar{\rho}_0, A) \simeq Hom_{\mathcal{C}}(R, A)$$

$$A^\times \xleftarrow{\varphi} R^\times \xleftarrow{\rho^{un}} G : \varphi \circ \rho^{un} \longleftarrow \varphi$$

(2) Le couple (R, ρ^{un}) est unique à isomorphisme près.

aucoup plus facile que d' (2)!

Preuve On va user de l'algèbre de groupe $\mathcal{O}[G]$, qui est commutative puisque G l'est ; on a $\tilde{\rho}^u : G \longrightarrow \mathcal{O}[G]^\times$.

Par définition, $\mathcal{O}[G]$ vérifie la propriété universelle requise : toute flèche $G \xrightarrow{\varphi} A^\times$ s'étend en une application

$$\mathcal{O}[G] \xrightarrow{\tilde{\varphi}} A$$

vérifiant $\tilde{\varphi} \circ \tilde{\rho}^u = \varphi$.

Mais on n'y est pas tout à fait car on veut un <u>anneau local</u>...

Il faut user de biais...

On commence par $\mathcal{O}[G]$; et $G \longrightarrow \mathcal{O}[G]^\times$, par laquelle toute $\psi : G \to A^\times$ se factorise.

Utilisons la condition de <u>déformation</u> jusqu'ici délaissée...

On a une flèche

$$\begin{tikzcd} G \arrow[r] \arrow[dr] & \mathcal{O}[G]^\times \arrow[d] \\ & k^\times \end{tikzcd}$$

donnée par $\begin{cases} \mathcal{O}[G] \longrightarrow k \\ (\sum \alpha_g g) \longmapsto \sum \bar{\alpha}_g \bar{\rho}_0(g) \end{cases}$ ($\bar{\rho}_0$ étant donnée)

Soit $m \subset \mathcal{O}[G]$ le noyau de cette flèche ; c'est un idéal maximal puisque le quotient est un corps.

On prend alors

$$\boxed{R = \varprojlim \mathcal{O}[G]/_{m^n}}$$

(la complétion de R en m).

R est une $\mathcal{O}$-algèbre, complète, locale par définition.

<u>Cas simple</u> : si G est <u>fini</u>, $\mathcal{O}[G]$ est une algèbre noethérienne (évidemment), et R l'est encore (complétion d'un anneau noethérien).

On a une flèche $\rho^{un} : G \longrightarrow R^\times$ naturelle.

Supposons donnée une déformation de $\bar{\rho}_0$, $\rho : G \to A^\times$; on a la flèche $\mathcal{O}[G] \xrightarrow{\varphi} A$ correspondante, et comme c'est une déformation, il est facile de voir qu'on obtient un morphisme

$$R \xrightarrow{\varphi} A$$

(car l'hypothèse "déformation" implique φ continue de $\mathcal{O}[G]$ muni de la topologie m-adique de A muni de la topologie m_A-adique $\Rightarrow \varphi$ se prolonge au complété R de $\mathcal{O}[G]$ / la topologie m-adique...)

~~[illegible]~~

Il est immédiat que cela donne l'identification

$$Def(\bar{\rho}_0, A) = Hom(R, A)$$

recherchée.

Dans le cas général, il n'est pas toujours vrai que R est noethérienne.

Mais dans notre cas, cela marchera.

(1) N.B. Supposons que G est profini, abélien, et est topologiquement de type fini, ie il existe un nb fini d'éléments $(g_1, \dots, g_N)$ engendrant un sous-groupe dense de G.
On va alors construire l'anneau R d'une autre façon.

Construction "explicite" de l'anneau des déformations (Faltings)

Considérons l'anneau des séries formelles $\hat{R} = \mathcal{O}[[T_1, \dots, T_N]]$: c'est un anneau local $(m_{\tilde{R}} = (m_G, T_1, \dots, T_N))$, complet.
On part de

$$\overline{\rho_0} : G \longrightarrow k^\times$$

On choisit $(a_1, \dots, a_N) \in G^N$ tels que $\overline{a_i} = \overline{\rho_0}(g_i)$.

On considère les idéaux $J \subset \tilde{R}$ avec la propriété :
il existe un morphisme $G \longrightarrow \left(\mathcal{O}[[T_1, \dots, T_N]]/_J\right)^\times$
de la forme $g_i \longmapsto a_i + T_i$

Ex. $J = m_{\tilde{R}}$: le quotient est $k^\times$, pour lequel on a l'application $G \to k^\times$ du départ.

Posons $I = \bigcap_J J$, l'intersection de ces idéaux.

Fait : l'anneau R vérifie

$$R \simeq \tilde{R}/_I$$

(En particulier, on voit que R est noethérien)

Preuve. On doit vérifier la propriété universelle. Soit $R' = \tilde{R}/_I$.
Il nous faut d'abord

$$G \xrightarrow{\rho^{un}} R'^\times$$

qu'on construit par $g_i \longmapsto \overline{(a_i + T_i)} \pmod{I}$
Clairement, cela donnera $\overline{\rho^{un}} = \overline{\rho_0}$.
Vérifions que c'est un morphisme de groupes : c'est une tautologie vu la construction de I comme intersection des idéaux J qui sont

(Partout où on a $G \longrightarrow A^\times$ avec G, A topologisés, on demande que les morphismes soient continus)

conçus pour que l'analogue de cette flèche soit un homomorphisme !
(N.B. Elle se passe au niveau du sous-groupe engendré par les g_i, mais les objets sont complets, et ρ^{un} est continue)

Soit maintenant une déformation de $\overline{\rho_0}$ dans une algèbre $A \in \mathcal{C}$:

$$\rho : G \longrightarrow A^\times$$

On veut $\varphi : R' \longrightarrow A$ avec $\rho = \varphi \circ \rho^{uni}$
On définit φ naturellement par

$$T_i \longmapsto \rho(g_i) - a_i$$

) pour arriver dans l'idéal maximal

ce qui donne $\tilde{R} \xrightarrow{\tilde{\varphi}} A$ au moins.
Soit ensuite $J = \operatorname{Ker} \tilde{\varphi} \subset \tilde{R}$; on a alors évidemment

$$\tilde{R}/_J \longrightarrow A$$

Mais on peut construire alors un homomorphisme

$$\begin{cases} G \longrightarrow \left(\tilde{R}/_J\right)^\times \\ g_i \longmapsto a_i + T_i \text{ "} = \rho(g_i) \text{"} \end{cases}$$

et cela donne le résultat !
:

□

Maintenant on va vérifier que les groupes qui nous intéressent vérifient la condition (1) ci-devant.
Soit $L/_{\mathbb{Q}}$ une extension (abélienne) (peut-être infinie) et telle que $L/_{\mathbb{Q}}$ est non-ramifiée en dehors d'un ensemble fini Σ de nombres premiers.
Proposition. $\operatorname{Gal}(L/\mathbb{Q})$ est topologiquement de type fini.
Dém. L'énoncé fondamental est le suivant :
Th. (Hermite - Minkowski) Il n'y a qu'un nombre fini de corps de nombres $E/\mathbb{Q}$ de degré borné et non-ramifiés en-dehors de Σ.
(ex. facile : les corps quadratiques)
[dans le cas abélien, c'est facile (sketch) : on adjoint les racines k-èmes de 1, puis on applique la théorie de Kummer et on utilise la finitude du nb de classes et du groupe des unités ... Δ]

$$\begin{tikzcd}
 & E(\mu_k \mid k \leq d) \arrow[d, dash] \\
E \arrow[ur, dash] \arrow[d, dash] & \mathbb{Q}(\mu_k \mid k \leq d) \\
\mathbb{Q} \arrow[ur, dash] &
\end{tikzcd}$$

Appliquons cela ici.
On a $L/\mathbb{Q}$ abélienne non-ramifiée en dehors de Σ. On considère les quotients finis de $G = Gal(L/\mathbb{Q})$ ie

$$\begin{tikzcd}L \arrow[d, dash] \arrow[dr, dash] & \\ & E \arrow[dl, dash, "\text{finie}"] \\ \mathbb{Q} & \end{tikzcd}$$

$Gal(E/K)$ est un groupe abélien fini, écrivons-le sous la forme

$$Gal(E/K) \simeq \mathbb{Z}/_{(m_1)} \times \dots \times \mathbb{Z}/_{(m_n)}$$

??
$m_i = p_i^{k_i}$ est une puissance d'un nbre premier.
0? On a pour tout i,

$$\begin{tikzcd}E \arrow[d, dash] \\ F \arrow[d, dash] \\ \mathbb{Q}\end{tikzcd} \; \Big) \; \mathbb{Z}/_{(p_1)} \times \dots \times \mathbb{Z}/_{(p_n)}$$

Détour : d'après le th. de Hermite-Minkowski, il n'y a qu'un nombre fini d'extensions abéliennes $E/\mathbb{Q}$ non-ramifiées en dehors de Σ et d'exposant ℓ.

⋮ (à revoir la prochaine fois)

◇

Exemple. (Iwasawa)
Prenons $L = \mathbb{Q}(\mu_{p^\infty})$: L est non-ramifié en dehors de p, et on a $Gal(L/\mathbb{Q}) = \varprojlim (\mathbb{Z}/_{(p^n)})^\times = \mathbb{Z}_p^\times$

Quels sont des générateurs topologiques ?
On a $1+p\mathbb{Z}_p \subset \mathbb{Z}_p^\times$ et plus généralement

$$\underbrace{1 \longrightarrow 1+p\mathbb{Z}/_{p^n\mathbb{Z}}}_{\text{généré par } 1+p.1} \longrightarrow (\mathbb{Z}/_{(p^n)})^\times \longrightarrow (\mathbb{Z}/_{(p)})^\times \longrightarrow 1$$

Donc $1+p\mathbb{Z}_p$ est engendré par $1+p = \gamma$ et les racines $(p-1)$-èmes de 1, $\varepsilon_1, \dots, \varepsilon_{p-1}$

Fait : dans ce cas, l'anneau des déformations est $R = \mathbb{Z}_p[[T]]$

Plan ensuite : on a

$$\begin{tikzcd}G \arrow[d] & Gal(K/\mathbb{Q})^{ab} \\ G' & Gal(K^{cycl}/\mathbb{Q})\end{tikzcd}$$

On écrit l'anneau des déformations de G et G', ce qui donne

$$R \twoheadrightarrow R'$$

G' est à peu près connu, donc R' aussi. On va étudier R aussi bien que possible pour trouver une condition sous laquelle $R \twoheadrightarrow R'$ est, en fait, un isomorphisme.

11/10/95)

On revient au pb. de finitude des générateurs topologiques...

Proposition. Soit G un groupe profini abélien qui est un pro-ℓ-groupe.
Supposons que $g_1, \dots, g_n \in G$ engendrent $G/_{\ell G}$.
Alors $(g_1, \dots, g_n)$ engendrent topologiquement G lui-même.

N.B. $G = \varprojlim G/_U$, les ss-grpes d'indice fini forment une base de générateurs, donc pour vérifier que $S \subset G$ est dense il suffit de vérifier que $S \longrightarrow G/_U$ est surjective pour tout $U < G$ d'indice fini.

Dém. On considère un tel $U < G$ d'indice fini, même $U < \ell G$ d'indice fini (car $\ell G < G$ est d'indice fini) ; il suffit alors de montrer que $G/_U$ est engendré par les images des g_i.

$$\begin{tikzcd}G/_U \arrow[r] \arrow[d, phantom, "\wr"] & G/_{\ell G} \arrow[r] & 1 \\ \mathbb{Z}/_{(\ell^{n_1})} \times \dots \times \mathbb{Z}/_{(\ell^k)} \arrow[r] & \underbrace{\mathbb{Z}/_{(\ell)} \times \dots \times \mathbb{Z}/_{(\ell)}}_{k \text{ facteurs}} & \end{tikzcd}$$

Comme les g_i engendrent $G/_{\ell G}$, il est clair que k est borné en fonction de n ($k \leq n$, car $|G/_{\ell G}| \leq \ell^n$)

On voit alors que les g_i engendrent $G/_U$

☐

Proposition Soit $\overline{\rho_0} : G_{\mathbb{Q}} \longrightarrow k^\times$ non-ramifiée en dehors de Σ, ensemble fini de nombres premiers.
Il existe un quotient abélien G de $G_{\mathbb{Q}}$, topologiquement de type fini, tel que toute déformation $\rho : G_{\mathbb{Q}} \longrightarrow A^\times$ de $\overline{\rho_0}$ dans une $\mathcal{O}$-algèbre locale A non-ramifiée en dehors de Σ se factorise par G :

$$\begin{tikzcd} G_{\mathbb{Q}} \arrow[r, "\pi_G"] \arrow[rr, bend right, "\rho"'] & G \arrow[r] & A^\times \end{tikzcd}$$

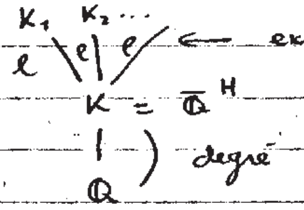
Dém. Remarquons que ρ se factorise par $G_{\mathbb{Q}}^{ab}$ et puis par le groupe de Galois de l'extension abélienne maximale non-ramifiée en dehors de Σ, G_{Σ}^{ab}.
On a donc

$$\begin{tikzcd} \rho : G_{\Sigma}^{ab} \arrow[r] \arrow[dr, "\overline{\rho_0}"'] & A^\times \arrow[d] \\ & k^\times \end{tikzcd}$$

Posons $H = \operatorname{Ker} \overline{\rho_0} < G_{\Sigma}^{ab}$: l'image de H par ρ est incluse dans $1 + m_A$, et H est d'indice fini dans G_{Σ}^{ab}.
On a une filtration évidente

$$1 + m_A \supset 1 + m_A^2 \supset \dots \supset 1 + m_A^n \supset \dots$$

dont les quotients successifs sont des ℓ-groupes. Donc $\rho|H$ se factorise par un pro-ℓ-groupe abélien.
Il suffit de montrer que celui-ci est topologiquement de type fini; pour cela on applique la proposition à H : il faut trouver des générateurs de $H/_{\ell H}$.
On a



← extensions abéliennes non-ramifiées en dehors de Σ

) degré fini, $G \simeq k^\times$ $(\deg K_j \leq \ell |k^\times|)$

Les extensions en question sont de degré borné, non-ramifiées en dehors de Σ ; par Hermite-Minkowski, il n'y a qu'un nombre fini de telles extensions K_j, donc finalement $\rho|H$ se factorise par un ℓ-groupe abélien H', vérifiant : $H'/_{\ell H'}$ est fini.
fini de corps K_j abélien de degré ℓ sur K

K CFC$(\mathbb{Q}_{\Sigma}^{ab})^{\ell H}$,
(F/K) est
lien d'exposant
donc un
duit de $\mathbb{Z}/(\ell)$
différents
eux $\simeq \mathbb{Z}/(\ell)$
ssibles pour
les F ne
vent, par
n, provenir
d'un
que
autre

D'après la proposition précédente, $\rho|H$ se factorise par un pro-ℓ-groupe topologiquement de type fini.
Mais $H < G_{\Sigma}^{ab}$ est d'indice fini, donc G_{Σ}^{ab} est encore topologiquement de type fini.
□

Rappel : supposons que $\rho : G_{\mathbb{Q}} \longrightarrow \mathcal{O}^\times$ est une représentation galoisienne.
De χ, caractère de Hecke algébrique, on peut construire $\rho_\chi : G_{\mathbb{Q}} \rightarrow \mathcal{O}^\times$.
Supposons que (i) $\bar{\rho} = \overline{\rho_\chi}$ (modulo $m_{\mathcal{O}}$)
(ii) ρ est non-ramifiée en dehors d'un ensemble fini Σ de nombres premiers
Espoir : ρ est de la forme $\rho_{\chi'}$ pour un certain χ'.

Notons $\overline{\rho_0} = \overline{\rho_\chi}$ On peut considérer deux [anneaux] problèmes de déformation :
(i) R_Σ, l'anneau des déformations de $\overline{\rho_0}$ (non-ramifiées en dehors de Σ)
Par la proposition précédente et la construction de Faltings, R_Σ est noethérien, isomorphe à un quotient d'un anneau de séries formelles...
(ii) $\mathbb{T}_\Sigma$, l'anneau des déformations des caractères de Hecke algébriques non-ramifiés en dehors de Σ

Clairement cela donne une surjection (surjection car $\Phi_{\text{nat}} \subset \Phi$)

$$R_\Sigma \twoheadrightarrow \mathbb{T}_\Sigma$$

Un peu d'algèbre : théorèmes d'isomorphismes de Wiles-Lenstra

Soit $\mathcal{O}$ un anneau de valuation discrète complet
A une $\mathcal{O}$-algèbre complète locale noethérienne
$\pi : A \rightarrow \mathcal{O}$ une application de $\mathcal{O}$-algèbres.

Ex : $\mathcal{O} \simeq \mathbb{Z}_\ell$, ou $\mathcal{O}_L$, anneau des entiers de $L/\mathbb{Q}_\ell$ finie
A = anneau de déformations $\mathcal{O}[[T_1, \dots, T_N]]/_I$

$\pi : A \to \mathcal{O}$ est donnée par une déformation donnée (supposée "bien connue", cyclotomique dirons)

Les invariants

Définition On pose $I_A = \mathrm{Ker}\, \pi$

"espace cotangent" $\leftarrow$ $\Phi_A = I_A / I_A^2$, c'est un $\mathcal{O}$-module

"idéal de congruence" $\leftarrow$ $\eta_A = \pi(\mathrm{Ann}_A(I_A))$, c'est un idéal dans $\mathcal{O}$

Théorème (Wiles-Lenstra)

Soit A une $\mathcal{O}$-algèbre libre $\underbrace{\ }_{\text{en tant que } \mathcal{O}\text{-module et}}$ de $\overset{\text{rang}}{\text{type}}$ finie, $\pi : A \to \mathcal{O}$ une flèche de $\mathcal{O}$-algèbres et B une $\mathcal{O}$-algèbre complète locale et noethérienne.

Supposons qu'on ait $\varphi : B \to A$ surjective.

Soit $I_B = \mathrm{Ker}(B \xrightarrow{\varphi} A \xrightarrow{\pi} \mathcal{O})$.

Si la longueur de $\mathcal{O}/\eta_A$ comme $\mathcal{O}$-module est finie, et est supérieure à

$$\ell(I_B/I_B^2)$$

alors φ est un isomorphisme.

Exemples (i) $A = \mathcal{O}[[X]]/(f)$ $\underbrace{\ }_{f \text{ tq } f(0)=0}$, $\pi : A \to \mathcal{O}$, $g \longmapsto g(0)$ ("terme constant")

On a alors :

$$I_A = \mathrm{Ker}\, \pi = (X) = X\mathcal{O}[[X]]/(f)$$

On écrit

$$\begin{aligned} f &= a_1 X + a_2 X^2 + \dots \\ &= a_k X^k + \dots \qquad , a_k \neq 0 \\ &= X^k (a_k + a_{k+1} X + \dots) \end{aligned}$$

On a $I_A^2 = X^2 \mathcal{O}[[X]]/(f)$

$$\mathrm{Ann}(I_A) = \{ g \in \mathcal{O}[[X]] \mid Xg \in (f) \}$$

Fait : $I_A/I_A^2 \simeq \mathcal{O}/(a_1)$ et $\eta_A \simeq (a_1)$ (??)

cf. plus loin le calcul correct

~~Si $a_1 = 0$: $I_A = X\mathcal{O}[[X]]/(a_2X^2+\dots)$~~

~~$\cup$~~

~~$I_A^2 = X^2\mathcal{O}[[X]]/(a_2X^2+\dots)$ $\Big\} \Rightarrow I_A/I_A^2 \simeq \mathcal{O}$~~

~~$\eta_A = \pi(\mathrm{Ann}_A(I_A)) = 0$ car si $\pi(g) \neq 0$, Xg a un terme en X~~

~~(En général $\eta_A \subset (a_1)$)~~

~~Si $a_1 \in \mathcal{O}^\times$: on a $(f) = (X)$ et $A = \mathcal{O}[[X]]/(f) \simeq \mathcal{O}[[X]]/(X)$~~

~~$\Rightarrow I_A = 0 = \Phi_A$~~

~~$\eta_A = \mathcal{O}$ $(= (a_1))$!~~

(ii) $A = \mathcal{O}[[X_1, \dots, X_n]]$ $\pi : A \to \mathcal{O}$, $f \longmapsto f(0)$ "terme constant"

$I_A = (X_1, \dots, X_n)$

$\mathrm{Ann}\, I_A = 0$ (car A est intègre) $\Rightarrow \eta_A = (0)$

$I_A^2 = (X_i X_j \mid 1 \leq i, j \leq n)$

$$\begin{cases} I_A/I_A^2 \simeq \mathcal{O}^n \\ f \longmapsto \left(\left(\frac{\partial f}{\partial x_i}\right)(0)\right) \end{cases}$$

Même remarque

~~(iii) $A = \mathbb{Z}_\ell[[X, Y]]/(Y(Y-\ell), X(X-\ell))$ $\mathcal{O} = \mathbb{Z}_\ell$~~

~~**Fait** : On a $\begin{cases} \Phi_A = \mathbb{Z}/(\ell) \oplus \mathbb{Z}/(\ell) \\ \eta_A = (\ell^2) \end{cases}$~~

~~**Dém.** On peut penser à A comme $\mathbb{Z}_\ell^4$ $(= \{a + bX + cY + dXY\})$~~

~~(repris le 18/10). $\triangledown$~~

(cf. "Corps Locaux")

Séminaire 3 -
T. Gillardi

13/10/95

Le conducteur d'Artin

Notations

K corps complet sous une valuation discrète v_K

A_K anneau des entiers $\{x \in K / v_K(x) \geq 0\}$

$p_K \subset A_K$ l'idéal maximal $\{x \in K / v_K(x) > 0\}$

$U_K = A_K^\times = A_K^\times \setminus p_K$

$\overline{K}$ le corps résiduel A_K / p_K

L/K extension galoisienne finie, $G = \mathrm{Gal}(L/K)$

v_L l'unique extension de v_K à L,

$$v_L = \frac{1}{[L:K]} v_K \circ N_{L/K}$$

$\pi \in L$ uniformisante, ie $v_L(\pi) = 1$, et $p_L = <\pi>$

On suppose que l'extension résiduelle $\overline{L}/\overline{K}$ est séparable.

$$\begin{tikzcd} L \arrow[d, dash, "n"'] & \overline{L} \arrow[d, dash, "f"] \\ K & \overline{K} \end{tikzcd}$$

L'indice de ramification est $e_{L/K} = [\mathbb{Z} : v_L(K^\times)]$

On pose $f_{L/K} = [\overline{L} : \overline{K}]$

On a alors

$$n = [L:K] = f_{L/K}\, e_{L/K}$$ (dans les "bons" cas, tout le temps ici)

Lemme. Si $i \geq 1$ est un entier, les conditions suivantes, pour $g \in G$, sont équivalentes

(i) $v_L(g.a - a) \geq i+1 \quad \forall a \in A_L$

(ii) g agit trivialement sur $A_L / p_{A_L}^{i+1}$

(iii) $v_L(g.x - x) \geq i+1$ où $x \in A_L$ engendre A_L comme A_K-algèbre (on peut choisir x de sorte que $\overline{L} = \overline{K}(\overline{x})$)

Dém. (ii) $\iff g.a - a \in p_L^{i+1} \quad \forall a \in A_L$

$\iff g.a - a = u\pi^{i+1}, \quad u \in A_L^\times$

$\iff v_L(g.a - a) \geq i+1$, (i)

(ii) $\iff$ (iii) est similaire

□

Déf. On pose $G_i = \{ g \in G \mid g$ vérifie (i), (ii) et (iii)$\}$

Propriétés (i) Les G_i sont des sous-groupes normaux de G, formant une famille décroissante

(ii) $G_{-1} = G$

(iii) $G_0 < G$ est le groupe d'inertie de L/K

(iv) $G_i = 1$ si i est assez grand

Dém. (i) $v_L = \frac{1}{[L:K]} v_K \circ N_{L/K}$ donc v_L est G-invariante, ce qui montre que les G_i sont normaux...

(...)

□

On dit que les G_i sont les groupes de ramification de G.

Prop. On a $G/G_0 \simeq \mathrm{Gal}(\overline{L}/\overline{K})$.

Dém On a une flèche naturelle (surjective)

$$\begin{cases} G \longrightarrow \mathrm{Gal}(\overline{L}/\overline{K}) \\ g \longmapsto \overline{g} \end{cases}$$

dont le noyau est clairement G_0...

□

Définition On pose $U_L^{(0)} = U_L$ et pour $i \geq 1$ entier

$$U_L^{(i)} = 1 + p_L^i$$

De sorte que les $U_L^{(i)}$ forment une suite décroissante de sous-groupes

$$U_L^{(0)} \supset U_L^{(1)} \supset \ldots \supset U_L^{(n)} \supset \ldots$$

On peut, pour $i \geq 1$, écrire

et non plus G

$$G_i = \{ g \in G_0 \mid v_L(g.\pi - \pi) \geq i+1 \}$$

Lemme $s \in G_i \iff \frac{s(\pi)}{\pi} \in U_L^{(i)} \qquad (i \geq 0)$

Dém. On a :

$$v_L(s(\pi) - \pi) = v_L\left(\pi \left(\frac{s(\pi)}{\pi} - 1\right)\right)$$

$$= 1 + v_L\left(\frac{s(\pi)}{\pi} - 1\right)$$

et le résultat en découle

□

Proposition Pour $i \geq 1$, le quotient G_i/G_{i+1} est naturellement isomorphe à un sous-groupe de $U_L^{(i)}/U_L^{(i+1)}$.

Dém. On définit une application

$$\theta_i \begin{cases} G_i/G_{i+1} \longrightarrow U_L^{(i)}/U_L^{(i+1)} \\ s \longmapsto \frac{s(\pi)}{\pi} \end{cases}$$

Le lemme montre que cela est bien défini,

$$\left(\frac{st(\pi)}{\pi} = \frac{s(\pi)}{\pi} \frac{t(\pi)}{\pi} \frac{s(u)}{u}, \text{ où } u = \frac{t(\pi)}{\pi} \in U_L, \text{ et } s(u) \equiv u \bmod p_L^{i+1} \right)$$

◇

Corollaire Si $\operatorname{char} \bar{L} = p \neq 0$, alors G_i/G_{i+1}, $i \geq 1$, est abélien et est un produit direct de groupes cycliques d'ordre p, et G_1 est un p-groupe.

Dém.
$$\begin{cases} p_L^i \longrightarrow U_L^{(i)} \\ x \longmapsto 1+x \end{cases} \quad \text{induit} \quad U_L^{(i)}/U_L^{(i+1)} \simeq p_L^i/p_L^{i+1}$$

$$\simeq \bar{L}$$

(comme gpe additif)

donc par le lemme, on a le début de la proposition

Ensuite $|G_1| = \prod_{i \geq 1} |G_i/G_{i+1}|$, donc c'est un p-groupe

□

N.B. $\overbrace{\overbrace{\underbrace{L - K^t}_{G_1} - K^{nr}}^{G_0} - K}^{G}$, cf. semaine dernière.

On considère la tour :

$$\underbrace{L \overset{G_0 \quad e_0, f_0}{—} L^{G_0} \overset{e_K, f_K}{—} K}_{\substack{G \\ e, f}}$$

Fait : $f_0 = 1$ et $e_K = 1$ (ie L^{G_0}/K est non-ramifiée)

Dém.

$$\underbrace{[\bar{L} : \bar{K}]}_{f} = \underbrace{[\bar{L} : \bar{L}^{G_0}]}_{f_0} \underbrace{[\bar{L}^{G_0} : \bar{K}]}_{f_K}$$

et $G/G_0 = \operatorname{Gal}(\bar{L}/\bar{K})$

$e_K f_K = f$

$\Rightarrow$

$$e_K f_K = f_0 f_K$$

$$\Rightarrow e_K = f_0 = 1 \quad \text{car} \overset{\text{en plus}}{\sqrt{}} [\bar{L} : \bar{L}^{G_0}] = 1 \,!$$

□

On définit une fonction sur G par

$$i_G(g) = v_L(g.x - x)$$

de sorte que l'on a trivialement

$$\begin{cases} (i) & i_G(1) = +\infty \\ (ii) & i_G(g) \geq 0 \qquad \text{pour } g \neq 1 \end{cases}$$

Propriétés
- (i) $i_G(g) \geq i+1 \iff g \in G_i$
- (ii) $i_G(hgh^{-1}) = i_G(g)$, $\forall h, g \in G$
  $i_G(g^{-1}) = i_G(g)$, $\forall g \in G$
- (iii) $i_G(gh) \geq \text{Inf}\{i_G(g), i_G(h)\}$
- (iv) Soit $H < G$ un sous-groupe de G. Alors
  $i_H(h) = i_G(h) \quad \forall h \in H$
  et $H_i = H \cap G_i$ pour tout i

Tout cela est plus ou moins évident.

Proposition Soit $H \triangleleft G$ un sous-groupe normal, $K' = L^H$.
Soit $\sigma \in G/H$, alors on a
$$i_{G/H}(\sigma) = \frac{1}{e_{L/K'}} \sum_{\substack{g \in G \\ \bar{g} = \sigma}} i_G(g)$$
(Exercice ; ou cf. Tate)

Si $u \in \mathbb{R}$ est ≥ -1, alors on note G_u le i-ème groupe de ramification de G, où i est l'entier le plus petit plus grand que u.
On a $g \in G_u \iff i_G(g) \geq u+1$.

Déf. On définit la fonction $\varphi_{L/K}$ par
$$\varphi_{L/K}(u) = \int_0^u \frac{1}{[G_0 : G_t]}\, dt$$
(avec la convention que $[G_0 : G_t] = [G_{-1} : G_0]^{-1}$, $t = -1$
$[G_0 : G_t] = 1$ si $0 \geq t > -1$)
($\Rightarrow \varphi_{L/K}(u) = u$, $-1 \leq u \leq 0$)

Si on a $m \leq u \leq m+1$, $m \in \mathbb{N}$, alors (où $n_i = |G_i|$)
$$\boxed{\varphi_{L/K}(u) = \frac{1}{n_0}\left(n_1 + n_2 + \dots + n_m + (u-m)\, u_{m+1}\right)}$$

En particulier, pour m entier, $\varphi_{L/K}(m) = \frac{1}{n_0} \sum_{i=1}^{m} n_i$.

Proposition (i) $\varphi_{L/K}$ est linéaire par morceaux, continue, croissante
(ii) si $m < u < m+1$, m entier, on a
$$\varphi'_{L/K}(u) = \frac{1}{[G_0 : G_{m+1}]}$$

Notons $\psi_{L/K}$ la fonction inverse de $\varphi_{L/K}$.

Prop (i) $\psi_{L/K}$ est linéaire par morceaux, continue et croissante.
(ii) si v est un entier, $u = \psi_{L/K}(v)$ est entier.

Dém. $\varphi_{L/K}(u) = \frac{1}{n_0}\left(n_1 + \dots + n_m + (u-m)\, n_{m+1}\right)$, $m \leq u \leq m+1$ m entier positif
$$n_0 v = n_1 + \dots + n_m + (u-m)\, n_{m+1}$$
On a $n_{m+1} \mid n_0$, $i \leq m$, car $G_{m+1} \subset G_i$, donc u est entier
□

Numérotation supérieure des groupes de ramification

On pose
$$G^v = G_{\psi_{L/K}(v)}$$
(ie
$$G_u = G^{\varphi_{L/K}(u)}$$
) N.B. $G_0 = G^0$, $G_{-1} = G^{-1}$

Théorème (Herbrand) Soit $H \triangleleft G$ un sous-groupe normal et $K' = L^H$. On a alors
$$G_u H/H = (G/H)_{\varphi_{L/K'}(u)}$$

Dém.
Lemme 1 $\varphi_{L/K}(u) = \frac{1}{n_0} \sum_{s \in G} \operatorname{Inf}\{i_G(s), u+1\} - 1$
Preuve La fonction à droite dans cette formule est continue, linéaire par morceaux, nulle en 0, valant -1 en -1.
Si $u \geq 1$ est un entier, la fonction à droite s'écrit
$$\frac{1}{n_0}\left(\sum_{G \setminus G_0}(\_\_) + \sum_{\substack{G_0 \setminus G_1 \\ i_G(s) = 1}}(\_\_) + \sum_{G_m \setminus G_{m+1}}(\_\_) + \sum_{G_{m+1}}\right) - 1$$
$$= \frac{1}{n_0}\left(0 + 1\,(n_0 - n_1) + \dots + (u+1)(n_u - n_{u+1}) + (u+1)\, n_{u+1}\right)$$
$$-1$$
$$= \frac{1}{n_0}\left(n_0 + n_1 + \dots + n_u\right) - 1 = \varphi_{L/K}(u)$$
(On regarde ensuite les dérivées entre des entiers)
□

Lemme 2 Soit $\sigma \in G/H$, et $j(\sigma) := \operatorname{Max}\{i_G(s) \mid s \in G, \bar{s} = \sigma\}$
Alors on a $i_{G/H}(\sigma) = \varphi_{L/K'}(j(\sigma) - 1) + 1$

__Dém.__ Soit $s \in G$ tq $\bar{s} = \sigma$ et $i_G(s) = j(\sigma)$

On notera $m = i_G(s)$.

Si $t \in H$, on distingue :

(i) Si $t \in H_{m-1}$, $i_G(t) \geq m$.
$$\Rightarrow i_G(st) \geq m$$
donc $i_G(st) = m$ par définition de m.

(ii) Si $t \notin H_{m-1}$, donc $i_G(t) < m$ et $i_G(st) = i_G(t)$

Dans tout les cas, $i_G(st) = \mathrm{Inf}\{\overset{m}{i_G}(s), \overset{=}{i_G}(t)\}$.

Or on a

$$i_{G/H}(\sigma) = \frac{1}{e_{L/K'}} \sum_{\substack{s \in G \\ \bar{s} = \sigma}} i_G(s) = \frac{1}{e_{L/K'}} \sum_{t \in H} i_G(st)$$
$$= \frac{1}{e_{L/K'}} \sum_{t \in H} \mathrm{Inf}\{i_G(t), m\}$$
$$= \frac{1}{|H_0|} \sum_{t \in H} \mathrm{Inf}\{i_H(t), m\}$$
$$\overset{(\text{lemme } 1)}{=} \varphi_{L/K'}(m-1) + 1.$$

□

On en déduit la preuve du théorème d'Herbrand:

soit $v = \varphi_{L/K'}(u)$; on a

$$\sigma \in G_u H/H \iff j(\sigma) \geq u+1$$
$$\varphi_{L/K'}(j(\sigma)-1) \geq \varphi_{L/K'}(u)$$
$$i_{G/H}(\sigma) - 1 \geq \varphi_{L/K'}(u) = v$$
$$i_{G/H}(\sigma) \geq v+1$$
$$\iff \sigma \in (G/H)_v$$

□

__Théorème__ (Hasse - Arf) Si G est abélien et G^v est un saut de la filtration alors v est un entier

[illegible]

__Dém__ cf. Serre ◇

18/10/95

$\mathcal{O}$ anneau de valuation discrete complet

(*) A $\mathcal{O}$-algèbre locale noethérienne complete, avec une application de $\mathcal{O}$-algèbres $\pi : A \longrightarrow \mathcal{O}$

On a défini les invariants
$$I_A = \mathrm{Ker}\, \pi$$
$$\Phi_A = \underbrace{I_A/I_A^2}_{\mathcal{O}\text{-module}} \qquad \eta_A = \pi(\mathrm{Ann}_A I_A) \subset \mathcal{O}, \text{ idéal de } \mathcal{O}$$

__Exemples__

(i) $A = \mathcal{O}[[T_1, \dots, T_n]]/(f_1, \dots, f_r)$ $\qquad f_i(0) = 0$

On a une application
$$\pi : A \longrightarrow \mathcal{O}$$
$$\bar{f} \longmapsto f(0)$$

On calcule facilement
$$I_A = (T_1, \dots, T_n)A$$

On a : $\begin{cases} I_A \longrightarrow \mathcal{O}^n/\left(\left\{\left(\frac{\partial f_i}{\partial T_1}(0), \dots, \frac{\partial f_i}{\partial T_n}(0)\right)\right\}\right) \\ f \longmapsto \left(\frac{\partial f}{\partial T_1}(0), \dots, \frac{\partial f}{\partial T_n}(0)\right) \end{cases}$

dont le noyau est I_A^2

Donc
$$I_A/I_A^2 \simeq \mathcal{O}^n/\left\{\left(\frac{\partial f_i}{\partial T_1}(0), \dots, \frac{\partial f_i}{\partial T_n}(0)\right) \mid 1 \leq i \leq r\right\}$$

(ii) $A = \mathcal{O}[[T]]/(f_1)$, $f_1(0) = 0$, $f_1 = a_1 T + \dots \Rightarrow I_A = TA$

$$\mathrm{Ann}_A(I_A) = \mathrm{Ann}_A(T) = \left(\frac{f_1(T)}{T}\right)$$
$$\Rightarrow \eta_A = \pi(\mathrm{Ann}_A(I_A)) = \pi\left(\frac{f_1(T)}{T}\right) = (a_1) \subset \mathcal{O}$$

$(\Phi_A = \mathcal{O}/(a_1))$

(iii) $A = \mathbb{Z}_e[[X, Y]]/(X(X-e), Y(Y-e))$, $\pi : f \mapsto f(0)$

$I_A = (X, Y)A$

On en déduit (par (i))

$$\Phi_A = I_A/I_A^2 = \mathbb{Z}_\ell \oplus \mathbb{Z}_\ell \big/ \{(-\ell, 0), (0, -\ell)\}$$

$$\text{ie} \quad \Phi_A \simeq \mathbb{Z}/(\ell) \oplus \mathbb{Z}/(\ell)$$

On calcule η_A :

on remarque que $(X-\ell)(Y-\ell) \in \mathrm{Ann}_A(I_A)$

donc $(\ell^2) \subset \eta_A$

En fait, on a même $(\ell^2) = \eta_A$

Soit en effet $g = a + bX + cY + dXY \in \mathrm{Ann}_A(I_A)$ $[X^2 = X\ell, \dots]$ et cela fait converger une série par $X^n \ell^{m-1} Y$

On $Xg = aX + b\ell X + cXY + d\ell XY = 0 \in A$

$$\Rightarrow \begin{cases} a + b\ell = 0 \\ c + d\ell = 0 \end{cases}$$

$$Yg = aY + bXY + c\ell Y + d\ell XY = 0$$

$$\Rightarrow \begin{cases} a + c\ell = 0 \\ b + d\ell = 0 \end{cases}$$

$$\Rightarrow a = -\ell c = -\ell(-d\ell) = \ell^2 d \Rightarrow \eta_A \subset (\ell^2) \quad \text{CQFD}$$

On peut remarquer que $|\eta_A| = |\Phi_A|$, dans ce cas.

(iv) $A = \mathbb{Z}_\ell[[X, Y]] / (X(X-\ell), Y(Y-\ell), XY)$

$I_A = (X, Y)A$

$\Phi = \mathbb{Z}/(\ell) \oplus \mathbb{Z}/(\ell)$ comme précédemment

Pour calculer η_A, remarquons cette fois que

$X + Y - \ell \in \mathrm{Ann}_A(I_A)$

et donc $\eta_A \supset (\ell)$

et un calcul immédiat donne $\eta_A = (\ell)$.

$$|\eta_A| < |\Phi_A|$$

[l'invariant η est sensible au nb. de relations dans un tel quotient...]

Définition Soit M un $\mathcal{O}$-module de rang fini. On appelle longueur de M, notée $\ell(M)$, la longueur d'une suite de Jordan-Hölder pour M (ie

$$M \supset M_1 \supset M_2 \supset \dots$$

$$M_i / M_{i+1} \text{ simple})$$

Ex . $\ell(\mathbb{Z}/(\ell) \oplus \mathbb{Z}/(\ell)) = 2$

$$\begin{array}{ll} & \mathbb{Z}/(\ell) \oplus \mathbb{Z}/(\ell) \\ \mathbb{Z}/(\ell) \; (& \quad \cup \\ & \quad \mathbb{Z}/(\ell) \\ \mathbb{Z}/(\ell) \; (& \quad \cup \\ & \quad 0 \end{array}$$

$\ell(\mathbb{Z}/(\ell^2)) = 2$ $\qquad$ $\ell(\mathbb{Z}/(\ell)) = 1$

$$\begin{array}{ll} & \mathbb{Z}/(\ell^2) \\ \mathbb{Z}/(\ell) \; (& \quad \cup \\ & \quad \ell\mathbb{Z}/(\ell^2) \\ \mathbb{Z}/(\ell) \; (& \quad \cup \\ & \quad 0 \end{array}$$

. $\ell(\mathbb{Z}_\ell) = +\infty$: $\mathbb{Z}_\ell \supset \ell\mathbb{Z}_\ell \supset \ell^2\mathbb{Z}_\ell \supset \dots \ell^n\mathbb{Z}_\ell \supset \dots$

Lemme Dans la situation donnée $(*)$, on a

$$\ell(I_A/I_A^2) \geq \ell(\mathcal{O}/\eta_A)$$

Dém. Détour par les idéaux de Fitting : (cf Lenstra, Hong-Kong Conf. 1994)

Déf. Soit M un module de rang fini sur un anneau B. Supposons que $(m_1, \dots, m_r)$ engendrent M, ie on a une surjection

$$B^r \xrightarrow{\varphi} M$$

$$(b_i) \longmapsto \sum b_i m_i$$

On définit l'idéal de Fitting $\mathrm{Fit}_B(M) \subset B$ par

$\mathrm{Fit}_B(M) = \{$ l'idéal engendré par les $r\times r$-mineurs de déterminants de matrices dont les colonn sont les "coordonnées" d'éléments de Ker φ

$$= \left(\begin{vmatrix} v_{11} & \cdots & v_{r1} \\ \vdots & & \vdots \\ v_{1r} & \cdots & v_{r,r} \end{vmatrix} \;\middle|\; (v_{i,j})_{1\leq j\leq r} \in \mathrm{Ker}\,\varphi \right)$$

Fait : l'idéal $\mathrm{Fit}_B(M)$ est indépendant de la présentation choisie

En effet, on remarque qu'il suffit d'abord de se limiter à des $(v_{ij})_{1 \leq j \leq r}$ qui engendrent $\operatorname{Ker} \varphi$.
Ensuite, si on ajoute un générateur $m_{r+1} = \sum_{i=1}^{n} c_i m_i$, on a cette fois

$$\left| \begin{array}{ccc} B^{n+1} & \xrightarrow{\varphi'} & M \\ (b_1, \dots b_{n+1}) & \longmapsto & \sum_{1 \leq i \leq r+1} b_i m_i \end{array} \right.$$

On a trivialement $\operatorname{Ker} \varphi' \supset (\operatorname{Ker} \varphi, 0)$

$$(-c_1, \dots, -c_r, 1) \in \operatorname{Ker} \varphi'$$

et on vérifie que $(\operatorname{Ker} \varphi, 0)$ et $(-c_1, \dots, -c_r, 1)$ engendrent $\operatorname{Ker} \varphi'$.
Pour calculer $\operatorname{Fit}_B(M)$, tout déterminant non nul contient un multiple de $\begin{pmatrix} -c_1 \\ \vdots \\ -c_1 \\ 1 \end{pmatrix}$ et est donc de la forme

$$\begin{vmatrix} -c_1 & v_{11} & \dots & v_{r1} \\ \vdots & \vdots & & \vdots \\ -c_n & v_{n1} & & v_{r,n} \\ 1 & 0 & & 0 \end{vmatrix}$$

En développant par la dernière ligne, on trouve aussitôt le même $\operatorname{Fit}_B M$.

Dans le cas de deux présentations, on prend l'union de deux ensembles de générateurs !

Ex. $\mathbb{Z}$-modules

$$\oplus \dots \oplus \mathbb{Z}n_n \to \mathbb{Z}^n \longrightarrow \prod_{i=1}^{n} \mathbb{Z}/(n_i) \longrightarrow 0 \quad , n_i \in \mathbb{N}, 1 \leq i \leq n$$

engendré par $\begin{pmatrix} n_1 & 0 & & 0 \\ 0 & n_2 & \ddots & \vdots \\ \vdots & \vdots & & 0 \\ 0 & 0 & & n_n \end{pmatrix}$

et $\operatorname{Fit}_{\mathbb{Z}} \left(\prod_{i=1}^{n} \mathbb{Z}/(n_i) \right) = \left(\prod n_i \right) \subset \mathbb{Z}$

ie est l'idéal engendré par l'ordre de $\prod \mathbb{Z}/(n_i)$ (si les $n_i \neq 0$), et est nul sinon (ordre infini).

<u>Propriétés</u>

(Fit_1) $\quad \operatorname{Fit}_B(M) \subset \operatorname{Ann}_B(M)$

(<u>Dém.</u> La comatrice A' de toute matrice $A = \begin{pmatrix} v_{11} & \dots & v_{r1} \\ \vdots & & \vdots \\ v_{n,1} & & v_{r,n} \end{pmatrix}$ vérifie $A'A = (\det A) I_d$, et on a $\operatorname{Ker} \varphi \to B^n \twoheadrightarrow M$ donc la multiplication par $\det A$ est nulle dans M, d'où le résultat)

(Fit_2) Considérons un anneau de valuation discrète $\mathcal{O}$, alors

$$\operatorname{Fit}_{\mathcal{O}} \left(\mathcal{O}/m_{\mathcal{O}}^{n_1} \times \dots \times \mathcal{O}/m_{\mathcal{O}}^{n_k} \right) = m_{\mathcal{O}}^{(\sum n_i)} = m_{\mathcal{O}}^{\ell(\prod \mathcal{O}/m_{\mathcal{O}}^{n_i})}$$

(<u>Dém.</u> même calcul que pour $\mathbb{Z}$, sachant que $m_{\mathcal{O}} = (\omega)$)
et

$$\operatorname{Fit}_{\mathcal{O}}(\mathcal{O}) = 0$$

(Fit_3) Si on a une flèche $A \xrightarrow{\pi} \mathcal{O}$ de noyau $\operatorname{Ker} \pi = I_A$.
Alors pour tout A-module M, on a

$$\operatorname{Fit}_{\mathcal{O}}(M/I_A M) = \pi(\operatorname{Fit}_A(M))$$

(<u>Dém.</u> On écrit

$$\begin{tikzcd} \operatorname{Ker} \varphi \arrow[r] \arrow[d, "\pi_1"] & A^n \arrow[r, "\varphi"] \arrow[d, "\pi^n"] & M \arrow[r] \arrow[d] & 0 \\ \hat{m} \text{ relations} \arrow[r] & (A/I)^n \arrow[r, "\varphi'"] & M/IM \arrow[r] & 0 \end{tikzcd}$$

Snake donne

$$\begin{tikzcd} I_A^n \arrow[r, "\sim"] & I_A M \arrow[dl, bend left] \\ \operatorname{Coker} \pi_1 \arrow[r] & 0 \end{tikzcd}$$

donc π_1 surjective et cela suffit

d'où le résultat)

On revient à la preuve du lemme :

$$I_A \longrightarrow A \overset{\pi}{\twoheadrightarrow} \mathcal{O}$$

Calculons $\operatorname{Fit}_A(I_A)$ $\quad$ (t_q $\pi(\operatorname{Fit}_A(I_A)) = \operatorname{Fit}_{\mathcal{O}}(I_A/I_A^2)$, par (Fit_3))

$$\begin{array}{ccccc} & & \pi(\operatorname{Fit}(I_A)) & & \\ & & \cap & & (\mathrm{Fit}_1) \\ & & \pi(\operatorname{Ann}_A(I_A)) & & \\ & & \shortparallel & & \\ \mathcal{O} & \supset & \mathfrak{J}_A & \supset & \operatorname{Fit}(I_A/I_A^2) \\ & & \shortparallel & & \shortparallel \\ & & m_{\mathcal{O}}^{\ell(\mathcal{O}/\mathfrak{J}_A)} & & m_{\mathcal{O}}^{\ell} \end{array} \quad , \text{ où } \ell = \ell(I_A/I_A^2)$$

d'où le résultat

□

On s'intéresse maintenant à ce qu'on peut dire si cette inégalité est une égalité...

Les anneaux d'intersection complète locaux

Déf. Soit O un anneau de valuation discrète, A une O-algèbre locale. On dit que A est une intersection complète locale s'il existe un isomorphisme

$$A \simeq O[[T_1, \dots, T_n]]/(f_1, \dots, f_n)$$

pour un certain n, et A est un O-module libre de rang fini.
(ie autant de générateurs que de relations).

(**But**: pour ces anneaux, l'inégalité est une égalité)

~~**Lemme 1** Soit R une O-algèbre locale complète noethérienne, A une intersection complète locale, et supposons données des surjections~~

$$\cancel{R \xrightarrow{\varphi} A \xrightarrow{\pi} O}$$

~~Alors si $\ell_R(\mathrm{Ker}\, \pi\circ\varphi / (\mathrm{Ker}\, \pi\circ\varphi)^2) = \ell_O(I_A/I_A^2)$, φ est un isomorphisme~~

…métriquement
…regarde
…espaces
…angents…)

plus loin

Lemme 2. Etant donnée une O-algèbre B finie (libre de rang fini comme O-module) et $\pi : B \to O$, il existe une intersection complète locale A et une flèche surjective φ

$$A \xrightarrow{\varphi} B \xrightarrow{\pi} O$$

telle que

$$I_A/I_A^2 \simeq I_B/I_B^2$$

(cf. ex. (iii) et (iv) avant)

…em)

17/10

O anneau des entiers d'une extension finie de $\mathbb{Q}_p$
T O-module muni d'une action de $G_{\mathbb{Q}}$, non-ramifié en dehors d'un nb. fini de p

$W = (T \otimes \mathbb{Q}_p)/T$ $\qquad W_M = \frac{1}{M} T/T$ $\qquad M \subset O$ idéal

Ex: $\chi : G_{\mathbb{Q}} \to O^\times$ caractère, $T = O(\chi)$ libre de rang 1
$O(1) = O(\chi_p) = O \otimes \varprojlim \mu_{p^n}$
cyclotomique

Ex. E courbe elliptique
$T_p(E) = \varprojlim E[p^n]$
$W_M = E[M]$

Groupe de Selmer: on a les groupes de cohomologie continue
(Bloch-Kato)

$$H^1(\mathbb{Q}, W_M) \qquad H^1(\mathbb{Q}, T)$$
$$\cup$$
$$S(W_M)$$ défini par des conditions locales

$$H^1_{nr}(\mathbb{Q}_\ell, W) = \mathrm{Ker}(H^1(\mathbb{Q}_\ell, W) \to H^1(\mathbb{Q}_\ell^{nr}, W))$$
$$= H^1(\mathbb{Q}_\ell^{nr}/\mathbb{Q}_\ell, W^{I_\ell})$$ classes non-ramifiées

Si $\ell \neq p$, on note $H^1_f(\mathbb{Q}_\ell, W) = H^1_{nr}(\mathbb{Q}_\ell, W)_{div}$, ss-grpe divisible maximal de H^1_{nr}
Le ss-grpe local en p est plus difficile à définir.
Ici on pose d'abord

$$S_{\{p\}}(W_M) = \mathrm{Ker}\left(H^1(\mathbb{Q}, W) \longrightarrow \bigoplus_{\ell \neq p} H^1(\mathbb{Q}_\ell, W)/H^1_f(\mathbb{Q}_\ell, W)\right)$$ $\oplus H^1(\mathbb{Q}_\ell,$

ie restriction de α en ℓ est dans H^1_f et est nulle en p (la condition en p la plus forte possible…)

(**N.B.** $V = T \otimes \mathbb{Q}_p$, $\quad 0 \to T \to V \to W \to 0$
Pour V, $H^1_f(\mathbb{Q}_\ell, V) = H^1_{nr}(\mathbb{Q}_\ell, V)$ (en $\ell \neq p$), ie pas besoin de "div"; le $H^1_f(\mathbb{Q}_\ell, W)$ est l'image de $H^1_f(\mathbb{Q}_\ell, V)$ par la flèche induite en cohomologie, modulo qq. chose de fini.)

Dualité

$$T^* = \mathrm{Hom}_O(T, O(1))$$ On pose ; $O(1) \rightsquigarrow$ caractère cyclotomique

$$W_M^* = \mathrm{Hom}_O(W_{M^*}, O(1)/M O(1))$$

On suppose que p est impair

Systèmes d'Euler (Kolyvagin)

Soit $N \in \mathbb{Z}$ divisible par p et tout les ℓ où T est ramifiée

On pose $R = \{ rp^n \mid r \text{ squarefree}, (r,N)=1, n \in \mathbb{N} \}$

$$P_\ell = \det(1 - Fr_\ell X \mid T) \in \mathcal{O}[X] \quad , \quad \ell \nmid N$$

Définition. Un système d'Euler pour T (et N) est une famille de classes de cohomologie $(c_r)_{r \in R}$,

$$c_r \in H^1(\mathbb{Q}(\mu_r), T)$$

telle que

$$\mathrm{Cores}_{\mathbb{Q}(\mu_{\ell r})/\mathbb{Q}(\mu_r)}(c_{r\ell}) = \begin{cases} P_\ell(\ell^{-1} Fr_\ell^{-1})\, c_r & \ell \neq p \\ c_r & \ell = p \end{cases}$$

N.B. $P_\ell(\ell^{-1} Fr_\ell^{-1}) \in \mathcal{O}[Gal(\mathbb{Q}(\mu_r)/\mathbb{Q})]$ agit sur la cohomologie

Théorème fondamental (sur $\mathbb{Q}$). Supposons que soit donné un système d'Euler $(\mathcal{E})$ et que

(i) $W_\mathfrak{p}$ est un $\mathcal{O}/\mathfrak{p}[G]$-module irréductible, et $T \neq 1$

idéal premier de $\mathcal{O}$

(ii) $H^1(\underbrace{\mathbb{Q}(W_{p^n}, \mu_{p^n})}_{\overline{\mathbb{Q}}^{\ker G_\mathbb{Q} \to Aut(W_{p^n} \cdot \mu_{p^n})}}, W^*_{p^n}) = 0 \quad , \forall n$

(iii) Il existe $\sigma \in Gal(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q})$ tel que $T/_{(\sigma-1)T}$ est libre de rang 1 sur $\mathcal{O}$.

Alors on a

$$|S_{\{p\}}(W_M^*)| \leq |\mathcal{O} : ind(c_1, H^1(\mathbb{Q}, T))|$$

où

$$ind(c_1, H^1(\mathbb{Q},T)) = p^n \quad \text{où } n \text{ est maximal}$$

tel que $c_1 \in p^n H^1(\mathbb{Q}, T)$

On peut restreindre les hypothèses si on admet de moins bonnes bornes: si on demande (i') $T \otimes \mathbb{Q}_p$ est irréductible à la place de (i)

(ii') les H^1 de (ii) sont bornés indépendamment de n, à la place de (ii)

(iii') $rg_\mathcal{O}\, T/_{(\sigma-1)T} = 1$

on obtient une borne plus faible, mais plus faible indépendamment de n.

Exemples:

(i) Soit χ un caractère d'ordre fini de $G_\mathbb{Q}$

$$\chi : G_\mathbb{Q} \longrightarrow Gal(\mathbb{Q}(\mu_n)/\mathbb{Q}) \longrightarrow \mathcal{O}$$

tq n est minimal et χ est pair.

On prend $T = \mathcal{O}(1) \otimes \chi \;(= \mathcal{O}(\chi \chi_p))$

On pose $N = pn$.

On cherche

$$c_r \in H^1(\mathbb{Q}(\mu_r), T) = H^1(\mathbb{Q}(\mu_{[n,r]}), T)^{Gal(\mathbb{Q}(\mu_{[n,r]})/\mathbb{Q}(\mu_r))}$$

$$= \left(\mathbb{Q}(\mu_{[n,r]})^\times \hat{\otimes}\, \mathcal{O}\right)^{\chi^{-1}}$$

On peut prendre

$$c_r = \sum_{\sigma \in Gal(\mathbb{Q}(\mu_{[n,p,r]})/\mathbb{Q}(\mu_{[n,r]}))} (1 - \zeta^\sigma_{[n,p,r]})^{\chi(\sigma)}$$

où ζ_r, $r \in R$, est une famille compatible de racines r-ièmes de 1 ($\zeta_{rd}^d = \zeta_r$)

Pour $\ell \neq p$, $N_{\mathbb{Q}(\mu_{[n,r,\ell]})/\mathbb{Q}(\mu_{[n,r]})}\, c_{r\ell} = c_r^{(1 - \chi_\ell Fr_\ell^{-1})}$, ou du moins on doit le vérifier.

On a $W_M^* = \mathcal{O}/_{M\mathcal{O}} \otimes \chi^{-1}$

$F = \overline{\mathbb{Q}}^{\ker \chi}$

$$H^1(\mathbb{Q}, W_M^*) = H^1(F, W_M^*)^{Gal(F/\mathbb{Q})}$$

(χ d'ordre premier à p)

$$= Hom\left((G_F^{ab})^{\chi^{-1}}, \mathcal{O}/_{M\mathcal{O}}\right)$$

Conditions de Selmer: non-ramifiés en dehors de p

trivial en p

$$\Rightarrow S_{\{p\}}(W_M^*) = Hom\left((A_F/_{\langle \mathfrak{p} \mid \mathfrak{p} \mid p \rangle})^{\chi^{-1}}, \mathcal{O}/_{M\mathcal{O}}\right)$$

(A_F classes d'idéaux de F)

Si $\chi(p) \neq 1$, cela est
$$\mathrm{Hom}\left(A_F^{\chi^{-1}}, \mathcal{O}/m\mathcal{O}\right)$$

Le théorème s'applique et démontre que
$$\left|(A_F \otimes \mathcal{O})^{\chi}\right| \leq \left|(\mathcal{O}_F^{\times} \otimes \mathcal{O})^{\chi} / C_F^{\chi}\right|$$

où $C_F^{\chi} = C_1^{\mathcal{O}}$ (unités cyclotomiques) (??)

N.B. Si $\chi(p)=1$, c_1 est triviale. Cela correspond à un zéro trivial d'une fonction L p-adique.

(ii) E courbe elliptique
$T = T_p(E)$

$$S_{\{p\}}(W_M) = S_{\{p\}}(E_M) \subset S(E_M)$$ le "vrai" grpe de Selmer

Les hypothèses du théorème sont :
(i) $\Leftrightarrow$ E n'a pas de p-isogénie, ce qui est vrai pour presque tout p
(i') est vrai pour tout p
(ii) est vrai si l'image de la représentation de Galois
$$G_{\mathbb{Q}} \to \mathrm{Aut}(E_M) \to GL(2, \mathbb{Z}/(n))$$
est surjective ; c'est vrai par Serre pour presque tout p, si E n'a pas de multiplication complexe, et est vrai pour $p \geq 3$, si E a multiplication complexe
(ii') est vrai pour tout p

La condition intéressante est donc (iii) :
$$G_{\mathbb{Q}} \to \mathrm{Aut}(T) \simeq GL(2, \mathbb{Z}_p)$$
$\mathrm{rg}\ T/(\gamma-1)T = 1 \Leftrightarrow \gamma$ a valeur propre 1
$$\gamma = \begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix}, \quad u \in \mathbb{Z}_p^{\times}$$

Cela existe pour presque tout p par Serre s'il n'y a pas de multiplication complexe (mais faux pour MC)
(iii') est vrai pour tout p.

Kato a construit un système d'Euler dans cette situation, si E est modulaire.

N.B. Les pts de Heegner ne sont pas un système d'Euler avec cette définition...

18/10/95

$\mathcal{O}$ anneau de valuation discrète complet $m_{\mathcal{O}} \subset \mathcal{O}$ idéal maximal

(lemme 1)

Lemme Soit R une $\mathcal{O}$-algèbre locale complète et noethérienne, et B une $\mathcal{O}$-algèbre libre de type fini qui est une intersection complète locale.
Supposons qu'on ait une surjection $R \overset{\varphi}{\twoheadrightarrow} B$, et $\pi : B \twoheadrightarrow \mathcal{O}$ et que φ induise un isomorphisme
$$I_R/I_R^2 \simeq I_B/I_B^2$$
et que de plus I_R/I_R^2 est de longueur fini comme $\mathcal{O}$-module
Alors φ est un isomorphisme.

N.B. Les hypothèses sont nécessaires : par exemple on a
(i) $$R = \mathcal{O}[[T]]/(T^3) \xrightarrow{\varphi} B = \mathcal{O}[[T]]/(T^2) \longrightarrow \mathcal{O}$$

φ n'est pas un isomorphisme et pourtant $I_R/I_R^2 \simeq I_B/I_B^2 \simeq \mathcal{O}$ mais ce dernier n'est pas de longueur finie.
(ii) On a vérifié précédemment que dans l'exemple
$$\mathbb{Z}_\ell[[X,Y]]/(X^2-\ell X, Y^2-\ell Y) \overset{\varphi}{\twoheadrightarrow} \mathbb{Z}_\ell[[X,Y]]/(X^2-\ell X, Y^2-\ell Y, XY) \twoheadrightarrow \mathbb{Z}$$

on a $I/I^2 \simeq \mathbb{Z}/(\ell) \oplus \mathbb{Z}/(\ell)$ dans les deux cas, mais φ n'est pas un isomorphisme.

N.B. (i) Si on a un anneau d'intersection complète locale,
$$B \simeq \mathcal{O}[[T_1, \dots, T_n]]/(f_1, \dots, f_n)$$
et $B \xrightarrow{\pi} \mathcal{O}$, soit $b_i \in B$ l'image de T_i dans B.

π étant une application locale, $\pi(b_i) \in m_{\mathcal{O}}$

On pose $S_i = T_i - \pi(b_i)$; comme $\pi(b_i) \in m_{\mathcal{O}}$, les séries en S_i sont des séries formelles en T_i. De plus, évidemment,

$$\pi(S_i) = 0$$

et $B \simeq \mathcal{O}[[S_1, \dots, S_n]]/(g_1, \dots, g_n)$ avec

$$g_i(S) = f_i\left(S_1 + \pi(b_1), \dots, S_n + \pi(b_n)\right)$$

et l'application π devient l'application $g \longmapsto g(0)$ ie la flèche "évaluation à 0".

On supposera désormais que les anneaux d'intersection locale sont présentés de cette façon.

(ii) On se donne donc

$$B = \mathcal{O}[[T_1, \dots, T_n]]/(f_1, \dots, f_n) \longrightarrow \mathcal{O}$$

On a calculé $I_B/I_B^2 \simeq \mathcal{O}^n/\left\{\left(\frac{\partial f_j}{\partial T_1}, \dots, \frac{\partial f_j}{\partial T_n}\right)\right\}_{1 \le j \le n}$

et on vérifie que $\mathrm{Fit}_{\mathcal{O}}(I_B/I_B^2) = \left(\det\left(\frac{\partial f_i}{\partial T_j}\right)\right) = m_{\mathcal{O}}^{\ell(I_B/I_B^2)}$

(car autant de générateurs que de relations)

<u>Démonstration du lemme</u>

(On suppose que π est ajusté comme ci-dessus)

Soit b_i l'image de T_i dans B ; on a donc $\pi(b_i) = 0$ ie $b_i \in \operatorname{Ker} \pi$.

Si on pose $a_{ij} = \frac{\partial f_i}{\partial T_j}(0)$, et qu'on regarde

$$\sum_{j=1}^{n} a_{ij} b_j$$

alors $\sum_{j=1}^{n} a_{ij} b_j \in I_B^2$, vu la dernière remarque.

Introduisons des $r_j \in R$ tels que $\varphi(r_j) = b_j$; on a $r_j \in I_R$

<u>Fait</u> : les r_j engendrent I_R.

En effet, par hypothèse, φ induit $I_R/I_R^2 \simeq I_B/I_B^2$

(<u>Rappel</u> : le lemme de Nakayama

Soit R un anneau commutatif unitaire, M un R-module, $I \subset R$ un idéal contenu dans tous les idéaux maximaux de R. Si $N \subset M$ est un sous-module tel que M/N est de type fini, et si $M = N + IM$, alors $M = N$.

<u>Dém.</u> Soit $m_1, \dots, m_t$ des générateurs de M/N. Supposons que t est minimal et $t > 0$ (ie $M \neq N$).

Par hypothèse, on a

$$m_t = \sum_{i=1}^{t} a_i m_i \qquad \text{avec } a_i \in I$$

$$\underbrace{(1 - a_t)}_{\in R^\times \text{ par hypothèse sur } I} m_t = \sum_{1 \le i \le t-1} a_i m_i$$

$\Rightarrow$ on peut diminuer t : contradiction □

<u>Application</u> Si (R, m) est un anneau local et M est un R-module de type fini, alors $(m_i)_{1 \le i \le n} \in M^n$ engendre M comme R-module $\Leftrightarrow$ $(\bar{m}_i) \in (M/mM)^n$ engendrent M/mM comme R/m-ev.)

I_R est un R-module de type fini, donc il suffit par Nakayama de vérifier que les $\bar{r}_j$ engendrent $I_R/m_R I_R$.

On a

$$I_R/m_R I_R \twoheadleftarrow I_R/I_R^2 \simeq I_B/I_B^2$$

B est un R-module <u>par</u> φ, et $\varphi : R \to B$ <u>devient</u> R-linéaire, donc $I_R/I_R^2 \simeq I_B/I_B^2$ comme Ⓡ-modules

et les b_j engendrent I_B, donc les $\bar{r}_j$ engendrent I_R/I_R^2, et a fortiori $I_R/m_R I_R$.

On construit alors une flèche

$$\begin{cases} \mathcal{O}[[T_1, \dots, T_n]] \twoheadrightarrow R \\ T_i \longmapsto r_i \end{cases}$$

(qui est bien définie car $r_i \in I_R \subset m_R$ donc les séries convergent)

La flèche est surjective car $R = \mathcal{O} + I_R$, et les r_j engendrent I_R.

On a le diagramme

$$\begin{tikzcd} \mathcal{O}[[T_1, \dots, T_n]] \arrow[r, "\psi"] & R \arrow[r, "\varphi"] & \mathcal{O}[[T_1, \dots, T_n]]/(f_1, \dots, f_n) \arrow[r] & \mathcal{O} \\ T_i \arrow[r, mapsto] & r_i \arrow[r, mapsto] & b_i & \end{tikzcd}$$

$$\begin{tikzcd} R \arrow[r, "\varphi"] & B \arrow[r, "\pi"] & \mathcal{O} \\ & \mathcal{O}[[T_i]] \arrow[ul, "\psi"] \arrow[u, "f"'] & \end{tikzcd}$$

Remarquons que comme $\sum a_{ij} b_j \in I_B^2$, $\sum a_{ij} x_j \in I_R^2$ $\left(I_R/I_R^2 \simeq I_B/I_B^2 \right)$

Fait : on a $a_{ij} = \frac{\partial g_i}{\partial T_j}(0)$ pour des $g_i \in \operatorname{Ker} \psi$.
Cela se voit en écrivant $R = \mathcal{O}[[T_1, \dots, T_n]]/_{\operatorname{Ker}\psi}$ et l'observation
(*) précédente : pour tout i, on a $\sum a_{ij} T_j = \sum_{k,\ell} h_{k,\ell} T_k T_\ell + g_i$, avec
$g_i \in \operatorname{Ker}\psi$, d'où le résultat.
On écrit $g_i = \sum h_{i\ell} f_\ell$ car $\varphi \circ \psi(g_i) = 0 \in \mathcal{O}[[T_i]]/_{(f_i)} = B$
$\Rightarrow$

$$a_{ij} = \frac{\partial g_i}{\partial T_j}(0) = \sum_{\ell=1}^{n} h_{i\ell}(0) \frac{\partial f_\ell}{\partial T_j}(0) \quad (\text{car } f_\ell(0) = 0)$$

$$\Leftrightarrow \quad a_{ij} = \sum h_{i\ell}(0)\, a_{\ell j} \quad (\text{par définition de } a_{ij})$$

$$\text{ie} \quad (a_{ij}) = (h_{i\ell}(0)) \cdot (a_{\ell j})$$

La longueur de I_R/I_R^2 est finie ; cela signifie que $\operatorname{Fit}(I_R/I_R^2) \neq$
ie $\det(a_{ij}) \neq 0$, et donc $(h_{i\ell}(0)) = \mathrm{Id}$!

La matrice des $h_{i\ell}$ est $\begin{pmatrix} 1+\dots & 0+\dots \\ & \vdots \\ 0+\dots & 1+\dots \end{pmatrix}$, et cela montre que $h_{i\ell}$ est inversible :

$$\det(h_{i\ell}) = 1 + \dots \quad \text{est une unité dans } \mathcal{O}[[T_1, \dots, T_n]]$$

Par conséquent, chaque f_ℓ s'écrit comme $\sum h'_{i\ell} f_i$, et en particulier $f_\ell \in \operatorname{Ker}\psi$, donc ψ se factorise via

$$\begin{tikzcd} \mathcal{O}[[T_1, \dots, T_n]] \arrow[r] \arrow[dr] & R \arrow[d, two heads, shift left, "\varphi"] \\ & \mathcal{O}[[T_1, \dots, T_n]]/(f_2, \dots, f_n) \arrow[u, shift left, "\psi"] \end{tikzcd}$$

comme $\varphi \circ \psi = \mathrm{Id}$ (évident) et φ est surjective, on doit avoir φ isomorphisme !
□

Lemme (lemme 2) — Soit B une $\mathcal{O}$-algèbre libre de rang finie et $\pi : B \twoheadrightarrow \mathcal{O}$ une flèche d'$\mathcal{O}$-algèbres locales.
Alors il existe un anneau d'intersection complète locale A et une application surjective $\varphi : A \twoheadrightarrow B$, telle que

$$I_A/I_A^2 \simeq I_B/I_B^2$$

De plus, on a

$$\operatorname{Fit}(I_A/I_A^2) = \eta_A = (\pi \circ \varphi)(\operatorname{Ann}_A(I_A))$$

N.B. (i) Exemple : $A = \mathbb{Z}_\ell[[X, Y]]/(X^2 - \ell X, Y^2 - \ell Y)$

$$\downarrow$$

$$B = \mathbb{Z}_\ell[[X, Y]]/(X^2 - \ell X, Y^2 - \ell Y, XY)$$

$$I_A/I_A^2 \simeq I_B/I_B^2 \simeq \mathbb{Z}/(\ell) \oplus \mathbb{Z}/(\ell)$$

(ii) Si B est déjà d'intersection complète, le lemme 2 dit qu'il existe $A \overset{\varphi}{\twoheadrightarrow} B$ avec $I_A/I_A^2 = I_B/I_B^2$, et le η_A est calculé ; si de plus I_A/I_A^2 est un $\mathcal{O}$-module de longueur fini, on sait que φ est un isomorphisme et

$$\eta_B = \operatorname{Fit}(I_B/I_B^2)$$

Dém.
Soit $b_1, \dots, b_n$ des générateurs de I_B.
Etape 1 – $\boxed{\mathcal{O}[b_1, \dots, b_n] = B}$
En effet, soit $C = \mathcal{O}[b_1, \dots, b_n]$, c'est un anneau local d'idéal maximal $m_C = m_B \cap C$ – c'est un résultat d'algèbre commutative : B est de rang fini sur C –.

$$\begin{tikzcd} B \arrow[d, dash] \\ C \arrow[d, dash] \\ \mathcal{O} \end{tikzcd}$$

B est local B/O est finie, donc C doit être local car Spec B → Spec C est surjective

On a encore $B = \mathcal{O} + I_B \subset \mathcal{O} + \sum B b_j \subset C + m_C B$
et, par Nakayama, $B = C$.

Etape 2 – Il existe $m \in \mathbb{N}$ et une surjection de $\mathcal{O}$-algèbres

$$D = \mathcal{O}[X_1, \dots, X_n]/(f_1, \dots, f_n) \twoheadrightarrow B$$

telle que (i) $x_j \mapsto b_j$
(ii) D est de rang $(m+3)^n$ comme $\mathcal{O}$-module, libre, engendrée par $\prod_{i=1}^{n} x_i^{k_i}$, $0 \leq k_i \leq m+2$.

utilisé pour calculer l'invariant η

(iii) $\mathrm{Hom}_{\mathcal{O}\text{-mod}}(\mathcal{D}, \mathcal{O})$ est un $\boxed{\mathcal{D}}$-module libre de $\mathcal{O}$ rang 1, engendré par

$$\lambda : \mathcal{D} \longrightarrow \mathcal{O}$$
$$\begin{cases} \pi_{x_i}^{m+2} \longmapsto 1 \\ \pi_{x_i}^{m+2} \neq \pi_{x_i}^{k_i} \longmapsto 0 \end{cases}$$

---

aine 4. Gillardi
-10-95

Le conducteur d'Artin, suite

Rappel de représentation des groupes

Soit G un groupe fini d'ordre n ; la représentation régulière de G sur $\mathbb{C}$ est $\rho_r : G \longrightarrow GL(V)$; $V = (e_{g_1}, \dots, e_{g_n})$

$$g \longmapsto (e_{g} \longmapsto e_{gh})$$

Soit r_G le caractère de ρ_r ; on a

$$\begin{cases} r_G(s) = 0 & \text{si } s \neq 1 \\ r_G(1) = n = |G| \end{cases}$$

On peut donc écrire

$$V_0 = \langle e_{g_1} + \dots + e_{g_n} \rangle$$

$$\begin{cases} V = 1_G \oplus \rho_n \\ \qquad\quad \hookrightarrow \text{représentation d'augmentation} \\ r_G = 1 + u_G \end{cases}$$

Définition φ est une fonction de classes $\Leftrightarrow$ $\varphi : G \to \mathbb{C}$ est invariante par conjugaison.

On a alors $\varphi = \sum\limits_{\chi \text{ caractère irréductible}} c_\chi \chi$, $c_\chi \in \mathbb{C}$

et φ est un caractère $\Leftrightarrow$ $\forall \chi$, $c_\chi \in \mathbb{N}$.

Pour φ, ψ des fonctions de classe on pose

$$\langle \varphi, \psi \rangle_G = \frac{1}{|G|} \sum_{s \in G} \varphi(s)\, \psi(s^{-1})$$

Lemme Soit $\rho_i : G \to GL(V_i)$ des représentations de G, χ_i

Alors $\langle \chi_1, \chi_2 \rangle_G = \langle V_1, V_2 \rangle_G$, où $\langle V_1, V_2 \rangle_G = \dim \mathrm{Hom}_G(V_1, V_2$

Dém. Pour χ, χ' irréductibles, on sait que $\langle \chi, \chi' \rangle = \delta_{\chi, \chi'}$. $\square$

Si $\varphi : G \to \mathbb{C}$ est une fonction de classe et $H < G$, alors $\varphi|H = \mathrm{Res}_H^G(\varphi)$ est une fonction de classe sur H, en particulier si χ est le caractère de ρ, alors $\chi|H$ est le caractère de $\rho|H$.

D'un autre côté, si ψ est une fonction de classe sur H, il existe une unique fonction de classe induite $\psi^* = \mathrm{Ind}_H^G \psi$ telle que la réciprocité de Frobenius soit vérifiée

$$\forall \varphi : G \to \mathbb{C}, \quad \langle \varphi, \mathrm{Ind}_H^G \psi \rangle_G = \langle \varphi | H, \psi \rangle_H$$

Théorème de Brauer Si χ est un caractère sur G alors on peut écrire $\chi = \sum n_i \chi_i^*$, avec $n_i \in \mathbb{Z}$, et χ_i des caractères de caractères de degré 1 sur des sous-groupes $H_i < G$.

On a L/K extension finie galoisienne de groupe de Galois G.

$$\begin{tikzcd} L \arrow[d, dash, "G_0"] \\ L^{G_0} \arrow[d, dash] \\ K \end{tikzcd}$$

G G_0 $e(L/L^{G_0})$ $f(L/L^{G_0}) = 1$

$e(L^{G_0}/K) = 1$ $f(L^{G_0}/K)$

On a la fonction $i_G : s \longmapsto v_L(s(x) - x)$, x générateur de A_L comme A_K-algèbre.

Définition On pose pour $s \in G$

$$\begin{cases} a_G(s) = -f\, i_G(s), & s \neq 1 \\ a_G(1) = f \sum\limits_{s \neq 1} i_G(s) \end{cases}$$

a_G est une fonction de classe et on a $\langle a_G, 1_G \rangle = 0$ évidemment.

Théorème 1. a_G est le caractère d'une représentation linéaire de G, appelée la représentation d'Artin.

Soit φ une fonction de classe et $f(\varphi) = <\varphi, a_G>$.
Alors :
Th1 $\Leftrightarrow$ **Th.1'** : pour tout caractère χ de G, on a $f(\chi) \in \mathbb{N}$
C'est ce qu'on va démontrer.

Prop. 1. $a_G = (a_{G_0})^* = \mathrm{Ind}_{G_0}^{G} a_{G_0}$

Dém. (Si $H < G$, χ caractère de H
χ^* —— induit sur G

$$\text{On a } \quad \chi^*(s) = \sum_{t \in G/H} \chi(t^{-1}st) \quad \left(\text{avec } \chi(t^{-1}st) = 0 \text{ si } t^{-1}st \notin H\right) \Big)$$

On a donc
$$(a_{G_0})^*(s) = \sum_{t \in G/G_0} a_{G_0}(t^{-1}st)$$

Soit $s \in G \setminus G_0$: dans ce cas, comme $G_0 \lhd G$, on a $t^{-1}st \notin G_0$ et $(a_{G_0})^*(s) = 0$. D'un autre côté, on a
$$s(x) - x \in A_L \setminus p$$
$$\text{ie } \quad v_L(s(x) - x) = 0 \Rightarrow a_G(s) = 0 \text{ par définition}$$

Soit ensuite $s \in G_0 \setminus \{1\}$:
$$(a_{G_0})^*(s) = \sum_{t \in G/G_0} a_{G_0}(t^{-1}st)$$
$$= -\underbrace{f_{L/L^{G_0}}}_{=1} \sum_{t \in G/G_0} i_{G_0}(t^{-1}st) \quad (\text{par définition})$$

or $i_{G_0}(t^{-1}st) = i_{G_0}(s) = i_G(s)$, donc
$$(a_{G_0})^*(s) = -\sum_{t \in G/G_0} i_G(s) = -\frac{|G|}{|G_0|} i_G(s)$$
$$= -f\, i_G(s) \quad \text{car } |G| = ef$$

ie $(a_{G_0})^*(s) = a_G(s)$.

Pour $s = 1$, on observe que les deux termes de l'égalité à démontrer sont orthogonaux à 1_G et coïncident sur $G \setminus \{1\}$: ils doivent alors être égaux.

~~Si $s = 1$ $(a_{G_0})^*(1) = \sum_{t \in G/G_0} a_{G_0}(1) = a_G(1)$ par calcul immédiat~~

$\square$

Prop. 2. G_i le i-ème groupe de ramification, $|G_i| = n_i$
u_i le caractère d'augmentation sur G_i
u_i^* le caractère induit à G
Alors $a_G = \sum_{i \geq 0} [G_0 : G_i]^{-1} u_i^*$

Dém. On calcule :
$$u_i^*(s) = \sum_{t \in G/G_i} u_i(t^{-1}st)$$

Si $s \notin G_i$, on a $u_i^*(s) = 0$ (comme précédemment)
Si $s \in G_i \setminus \{1\}$:
$$u_i^*(s) = \sum_{t \in G/G_i} u_i(t^{-1}st)$$

$$\text{or } \quad u_i(t^{-1}st) = \begin{cases} n_i - 1, & s = 1 \\ -1, & s \neq -1 \end{cases}, \text{ donc}$$

$$u_i^*(s) = \sum_t (-1) = -\frac{|G|}{|G_i|} = -\frac{n_0 f}{n_i}$$

$$\text{Pour } s = 1, \quad u_i^*(1) = (n_i - 1)\frac{|G|}{|G_i|} = f\frac{n_0(n_i - 1)}{n_i}$$

Cela donne $<1, u_i^*> = 0$ (ou réciprocité de Frobenius).

Soit alors $s \in G_k \setminus G_{k+1}$: le côté droit de la formule à prouver est :
$$\sum_{i=0}^{k} [G_0 : G_i]^{-1} u_i^*$$
$$= -f\left([G_0 : G_0]^{-1}\frac{n_0}{n_0} + [G_0 : G_1]^{-1}\frac{n_0}{n_1} + \dots + [G_0 : G_k]^{-1}\frac{n_0}{n_k}\right.$$
$$= -f(k+1)$$

et $a_G(s) = -f\, i_G(s) = -f(k+1)$ par définition.

Pour $s=1$, les deux côtés sont orthogonaux à 1 donc doivent aussi coïncider.

□

Définition. Soit φ une fonction de classes sur G. On pose

$$\varphi(G_i) = \frac{1}{|G_i|} \sum_{s\in G_i} \varphi(s)$$

Corollaire 1 (de la prop. 2). Si φ est une fonction de classes sur G, alors

$$f(\varphi) = \sum_{i\geq 0} \frac{n_i}{n_0} \left(\varphi(1) - \varphi(G_i)\right)$$

Dém. On a $\quad f(\varphi) = <\varphi, a_G>$

Considérons

$$<\varphi, u_i^{*}>_G = <\varphi|G_i, u_i>_{G_i}$$

$$= \frac{1}{|G_i|} \sum_{s\in G_i} \varphi(s)\, u_i(s^{-1})$$

$$= \frac{1}{n_i} \sum_{s\neq 1} (-\varphi(s)) + \frac{1}{n_i} \varphi(1)\,(n_i - 1)$$

$$= \frac{1}{n_i} \left(-\sum_{s\in G_i} \varphi(s) + n_i \varphi(1)\right)$$

$$= -\varphi(G_i) + \varphi(1)$$

et on applique la proposition 2.

□

Corollaire 2. Si χ est un caractère de G, on a

$$f(\chi) = \sum_{n\geq 0} \frac{n_i}{n_0} \operatorname{Codim} V^{G_i}$$

(où χ est le caractère de $\rho : G \to GL(n, V)$)

Dém.

On remarque que $\quad \chi(1) = \dim V$
$\quad \chi(G_i) = \dim V^{G_i}$

et on applique le corollaire 1.

□

Corollaire 3. Soit χ un caractère de G, alors $f(\chi) \in \mathbb{Q}^+$.

Dém. Trivial à partir du corollaire 2. □

Rappel : le discriminant et la différente d'une extension L/K finie séparable de degré n

Déf. Soit $\beta \in L$ tq $L = K(\beta)$. Alors la différente $\mathcal{D}_{L/K}$ est par définition

$$\mathcal{D}_{L/K} = \prod_{\substack{s\neq 1\\ s\in G}} (\beta - s(\beta))$$

et le discriminant $\delta_{L/K}$ est

$$\delta_{L/K} = \det(\sigma_i B^i)^2 \quad \text{avec} \quad \begin{cases} B^n = 1 \\ B^i = \beta^i, i\neq n \end{cases}$$

où (σ_i) parcourt le groupe de Galois.

On a $\quad \delta_{L/K} = N_{L/K}\, \mathcal{D}_{L/K}$
$\quad \mathcal{D}_{L/K} = \mathcal{D}_{L/K'} \cdot \mathcal{D}_{K'/K}$

$\Rightarrow$ transitivité du discriminant

$$\delta_{L/K} = \delta_{K'/K}^{[L:K']}\, N_{K'/K}(\delta_{L/K'})$$

Lemme. Si $\mathcal{D}_{L/K}$ est la différente, alors

$$v_K(\mathcal{D}_{L/K}) = \sum_{s\neq 1} i_G(s)$$

Dém. Par définition □

Proposition 3. Soit $H < G$ un sous-groupe correspondant à une sous-extension K' de L/K. Alors

$$a_G|H = v_K(\delta_{K'/K})\, r_H + f_{K'/K}\, a_H$$

Dém. Soit $s \in H \setminus \{1\}$:

$$\begin{cases} a_G(s) = -f\, i_G(s) = -f_{L/K}\, i_G(s) \\ a_H(s) = -f_{L/K'}\, i_H(s) = -f_{L/K}\, i_G(s) \\ r_H(s) = 0 \end{cases}$$

Soit $r = 1$:

$$a_G(1) = f_{L/K} \sum_{s \neq 1} i_G(s) = f_{L/K}\, v_L(\mathcal{D}_{L/K})$$

$$a_H(1) = f_{L/K'}\, v_{K'}(\mathcal{D}_{L/K'})$$

On $v_L = \frac{1}{f_{L/K}} v_K \circ N$, donc d'après ce qu'on a vu :

$$\begin{cases} a_G(1) = v_K(\delta_{L/K}) \\ a_H(1) = v_K(\delta_{L/K'}) \\ r_H(1) = |H| = [L:K'] \end{cases}$$

On met tout ensemble et on applique la transitivité du discriminant...

□

<u>Corollaire</u>. Soit φ un caractère de $H < G$, φ^* le caractère induit sur G. Alors

$$f(\varphi^*) = v_K(\delta_{K'/K})\varphi(1) + f_{K'/K}\, f(\varphi)$$

<u>Dém</u>. On a par prop 3

$$a_G|H = v_K(f_{K'/K})\, r_H + f_{K'/K}\, a_H$$

$$\Rightarrow \quad f(\varphi^*) = \langle \varphi^*, a_G \rangle = \langle \varphi, a_G|H \rangle$$

$$= v_K(f_{K'/K}) \langle r_H, \varphi \rangle$$

$$+ f_{K'/K} \langle \varphi, a_H \rangle$$

et on a aussitôt

$$\langle r_H, \varphi \rangle = \varphi(1)$$

ce qui conclut...

□

<u>Proposition 4</u>. Soit χ un caractère de degré 1 sur G, c_χ le plus grand entier tel que $\chi | G_{c_\chi} \neq 1$ (et $c_\chi = -1$ si $\chi = 1_G$).
Alors on a

$$f(\chi) = \varphi_{L/K}(c_\chi) + 1$$

<u>Dém</u>. Pour m entier, on sait que

$$\varphi_{L/K}(m) = 0 \quad si \quad m = -1$$

$$= \frac{1}{n_0} \sum_{i=0}^{m} n_i \quad si \quad m \geq 0$$

Alors si $i \leq c_\chi$, on a $\chi | G_i \neq 1$ et donc $\chi(G_i) = ($
si $i > c_\chi$, $\chi | G_i = 1$ et $\chi(G_i) = 1$.

Dans le 1^e^ cas, $\chi(1) - \chi(G_i) = 1$
le 2^e^ cas, $\chi(1) - \chi(G_i) = 0$

Du corollaire 1 à la prop 2, on déduit

$$f(\chi) = \sum_{i=0}^{c_\chi} \frac{n_i}{n_0} = \varphi_{L/K}(c_\chi) + 1.$$

□

<u>Corollaire</u>. Soit $H = \mathrm{Ker}\,\chi$ (χ de degré 1) et $K' = L^H$; notons c'_χ le plus grand entier tel que

$$(G/H)_{c'_\chi} \neq 1 \qquad (c'_\chi = -1 \text{ si } H = G)$$

Alors on a $f(\chi) = \varphi_{K'/K}(c'_\chi) + 1 \in \mathbb{N}$.

<u>Dém</u>. Par Herbrand, on a pour $v = \varphi_{L/K'}(u)$,

$$(G/H)_v = G_u H / H$$

donc

$$(G/H)_{c_\chi'} \neq 1 \iff \chi | G_u \neq 1 \text{ où } \varphi_{L/K'}(u) =$$

$$\iff u = c_\chi \text{ ci-dessus}$$

$$\text{ie } \varphi_{L/K'}(c_\chi) = c_\chi'$$

On applique $\varphi_{K'/K}$ à l'énoncé de la proposition 4 : par transitivité de φ, il vient

$$f(\chi) - 1 = \varphi_{L/K}(c_\chi) = \varphi_{K'/K}(c'_\chi)$$

Maintenant G/H est abélien et $(G/H)_{c_x'} \neq (G/H)_{c_x'+1}$, donc par Hasse-Arf, on a

$$\varphi_{K'/K}(c_x') \text{ est un entier } \geq -1$$

$\Rightarrow$ $f(\chi) \in \mathbb{N}$.

□

Preuve du théorème.

On veut que $f(\chi) \in \mathbb{N}$; on sait que $f(\chi) \in \mathbb{Q}^+$ (corollaire 3 de la prop 2);

Par le théorème de Brauer, on peut écrire

$$\chi = \sum_{\deg(\chi_i)=1} n_i \chi_i^*$$

Il suffit maintenant de voir que $f(\chi_i^*) \in \mathbb{N}$; mais par le corollaire de la prop. 4, $f(\chi_i) \in \mathbb{N}$, et par corollaire de la prop. 3, on a

$$f(\chi^*) = v_K(\delta_{K'/K})\,\chi(1) + f_{K'/K}\, f(\chi) \in \mathbb{N}$$

et cela conclut la preuve

□

Le conducteur d'Artin

Localement, le conducteur d'Artin est l'idéal $\mathfrak{p}_K^{f(\chi)} \subset A_K$.

Globalement, si L/K est une extension finie de groupe de Galois G et $\rho : G \to GL(V)$ une représentation de G ds un $\mathbb{C}$-ev de dimension finie, on pose

$$\begin{tikzcd} O_L \arrow[r, phantom, "\subset"] & L \arrow[d, dash] \\ \mathfrak{p} \subset O_K \arrow[r, phantom, "\subset"] & K \end{tikzcd}$$

$$f(\rho) = \prod_{\mathfrak{p}} \mathfrak{p}^{f_{\mathfrak{p}}(\chi)}$$

Plus généralement si $\rho : G \to GL(V)$ est une représentation de G dans un k-ev de dim finie où char $k = p \neq 0$.

On pose alors

$$f(\rho) = \prod_{\substack{\mathfrak{p} \\ \mathfrak{p} \nmid p}} \mathfrak{p}^{f_{\mathfrak{p}}(\chi)}$$

Remarquons que si ρ est non-ramifiée en $\mathfrak{p}$, alors $f_{\mathfrak{p}}(\chi) =$

on a $\operatorname{Ker}\rho \supset G_0$, et

$$\begin{tikzcd} L \arrow[d, dash] \\ L^{G_0} \arrow[d, dash] \\ K \end{tikzcd}$$

$$f_{\mathfrak{p}}(\chi) = \sum_{i \geq 0} [G_0 : G_i]^{-1} \operatorname{codim} V^{G_i}$$

(corollaire 2 prop. 2)

et $\operatorname{codim} V^{G_i} = 0$ pour tout i !

Donc ce conducteur est bien défini

Ex.

$$\begin{tikzcd} L \arrow[d, dash, "G"'] \\ \mathbb{Q} \end{tikzcd} \qquad \ell$$

$$\rho : G \to GL(2, \mathbb{F}_p)$$

Alors $N = f(\rho) = \prod_{\ell \neq p} \ell^{f_\ell(\chi)}$

Plus spécifiquement, soit ρ la représentation régulière. On a

$$f_\ell(\chi) = \langle r_G, a_G \rangle$$

$$= \frac{1}{|G|} \sum_{s \in G} r_G(s)\, a_G(s) = a_G(1) = f \sum_{s \neq 1} i_G(s$$

$$= f\, v_L(\mathcal{D}_{L/K})$$

$$= v_K(\delta_{L/K})$$

donc

$$f(r_G) = \prod_{\ell} \ell^{v_K(\delta_{L/K})} = \delta_{L/K}$$

23/10/95

Rappel : O anneau de valuation discrète complet

On a montré :

Lemme. Soit R une O-algèbre locale noethérienne complèt
B une O-algèbre libre de rang finie sur O qui est u
intersection complète.

Si on a : une surjection $R \twoheadrightarrow B$ et une flèche $B \to O$
et si, d'une part,

$$I_R/I_R^2 \simeq I_B/I_B^2$$

et d'aute part

$$\ell_O\left(I_R/I_R^2\right) < +\infty$$

Alors φ est un isomorphisme.

Et on veut prouver ici:

Lemme Soit B une O-algèbre locale libre de rang fini.
Alors étant donnée $\pi : B \to O$, il existe une O-algèbre locale d'intersection complete A telle qu'il existe une surjection $A \twoheadrightarrow B$, avec

$$I_A/I_A^2 = I_B/I_B^2$$

De plus, on peut avoir

$$\mathrm{Fit}_O\left(I_A/I_A^2\right) \simeq \eta_A$$

Dém. (cf. dernière fois)
On commence par des générateurs $(b_1, \dots, b_n)$ de I_B. On a vu:

(I) $O[b_1, \dots, b_n] = B$

(II) Considérons $D = O[X_1, \dots, X_n]$; il existe des f_i tels que l'on ait

$$D/(f_1, \dots, f_n) \xrightarrow{\varphi} B$$

avec : (i) $X_j \longmapsto b_j$
(ii) D est un O-module libre de rang fini $(m+3)^n$ de base

$$\left\{ \left(\prod_{1 \leq j \leq n} X_j^{k_j} \right) \;\middle|\; 0 \leq k_j \leq m+2 \right\}$$

(iii) $\mathrm{Hom}_O(D, O)$ est un O-module libre de rang 1 engendré par

$$\lambda : \begin{cases} \prod X_i^{m+2} \longmapsto 1 \\ \prod X_i^{k_j} \longmapsto 0 \quad \text{si il existe } k_j < m+2 \end{cases}$$

Preuve : considérons

$$\begin{cases} O^n \twoheadrightarrow I_B/I_B^2 \\ (c_1, \dots, c_n) \longmapsto \sum c_i b_i \end{cases}$$

Le noyau est libre de rang au plus n, car O est principal.
Soit

$$\left.\begin{matrix} (a_{11}, \dots, a_{1n}) \\ \vdots \\ (a_{n1}, \dots, a_{nn}) \end{matrix}\right\} \text{ n vecteurs dans } O^n \text{ qui engend… le noyau.}$$

Par définition

$$\sum_{j=1}^{n} a_{ij} b_j \in I_B^2$$

$$\begin{tikzcd} O(f_i) \arrow[r, "\varphi"] & B \\ f_i \arrow[r, mapsto] & b_i \end{tikzcd}$$

(cf. aussi (*) précédemment)

Il existe $g_i \in O[X_1, \dots, X_n]$ i.e. polynôme tel que $\frac{\partial g_i}{\partial X_j} = a_{ij}$
c'est à dire tels que $g_i = \sum a_{ij} X_j + (\text{ordre supérieur})$,
avec $\varphi(g_i) = g_i(b) = 0$ (cf. (I)).
Choisissons m un entier tel que $\deg g_i \leq m+2$

les $\left(\prod b_j^{m_j}\right)$ avec $\sum m_j \leq m$ engendrent B comme O-module.

En particulier, tout m assez grand convient.
On a alors $b_i^{m+1} = h_i(b_1, \dots, b_n)$ avec $d^\circ h_i \leq m$; et posons alors

$$\boxed{f_i = X_i^{m+3} - X_i^2 h_i + g_i}$$

Alors $f_i(b_1, \dots, b_n) = g_i(b_1, \dots, b_n) = 0$
et on peut écrire

$$f_i = X_i^{m+3} + (\text{ordre inférieur})$$
$$f_i = \sum a_{ij} X_j + (\text{ordre supérieur})$$

On a une flèche naturelle

$$\varphi : D = O[X_1, \dots, X_n]/(f_1, \dots, f_n) \longrightarrow B$$

(i) est vérifié pour φ
(ii) : les $\prod X_j^{k_j}$, $0 \leq k_j \leq m+2$, engendrent clairement D

et ils sont O-indépendants dans D en regardant le terme dominant : $\sum \lambda_K X^K = \sum \alpha_i f_i \Rightarrow \alpha_i = 0 \Rightarrow \sum \lambda_K X^K = 0 \Rightarrow \lambda_K =$ $\forall K$.

(iii) : considérons $\mathrm{Hom}_O(D, O)$ comme un~~e~~ D-module ~~[illegible]~~ :
étant donnée $\ell : D \longrightarrow O$, O-linéaire, on pose

$$(d\ell)(x) = \ell(dx)$$

D'abord, $\lambda \in \mathrm{Hom}_O(D, O)$ trivialement.
Et on calcule

$$\left(\left(\prod_{j=1}^{n} X_j^{k_j}\right)\lambda\right)\left(\prod_{d=1}^{n} X_k^{d_k}\right) = \lambda\left(\prod_{j=1}^{n} X_j^{k_j+d_j}\right)$$

$$= 1 \quad \text{si} \quad k_j + d_j = m+2$$

$$= 0 \quad \text{si} \quad k_j + d_j < m+2, \ \forall j$$

$$=$$

(matrice triangulaire)
D (II)

(On construit A à partir de O.

$$O \twoheadrightarrow B \twoheadrightarrow O)$$

(III) On peut écrire $D = \prod_{m \subset O \text{ maximal}} D_m$, D_m anneau local complet

En effet,

$D/m_O^t D$ est un anneau artinien commutatif

donc

$O/m_O^t O$ est un produit d'anneau artinien locaux

et on prend la limite.

On écrit $D = D_m \times O'$ avec $\varphi(m) \subset m_B$.

(IV) $D_m = O[[X_1, \dots, X_n]]/(f_1, \dots, f_n)$, O-algèbre locale complète, et c'est un O-module libre de rang fini (admis), donc c'est une intersection complète.

Par III), on a aussi $\mathrm{Hom}_O(D_m, O) \simeq D_m$ comme D_m-module.

On prend alors $A = D_m$.
Reste à vérifier que A satisfait aux propriétés annoncées.
On a

$$O^n \xrightarrow{\psi} I_B/I_B^2$$

et $(a_{j1}, \dots, a_{jn}) \in \mathrm{Ker}\,\psi$, de plus

$$f_i = \sum a_{ij} X^j + (\text{ordre supérieur})$$

On a alors

$$I_B/I_B^2 \simeq O^n/\langle (a_{ji}) \rangle$$

mais on sait calculer

$$I_A/I_A^2 \simeq O^n/\left\langle \left(\frac{\partial f_i(0)}{\partial X_j}\right)\right\rangle \simeq I_B/I_B^2 \quad !$$

Enfin, on calcule $\mathrm{Fit}_O(I_A/I_A^2)$:

<u>Remarques</u>. (1) Si on a $A \xrightarrow{\pi} O$ une application d'O-algèbres locales et $I_A = \mathrm{Ker}\,\pi$, $\eta_A = \pi(\mathrm{Ann}_A I_A)$
Mais π donne à O une structure de A-algèbre sur laquelle I_A agit trivialement, et

$$\left\{\begin{array}{lcl} \mathrm{Hom}_A(O, A) & \simeq & \mathrm{Ann}_A I_A \\ \ell & \longmapsto & \ell(1) \\ (\pi(a) \mapsto ax) & \longleftarrow & x \end{array}\right.$$

donc

$$\boxed{\eta_A = \pi(\mathrm{Hom}_A(O, A))} \subset \mathrm{Hom}(O, O) \simeq O$$

(2) Supposons que $\mathrm{Hom}_O(A, O) \simeq A$ comme A-module (
telle O-algèbre A est appelée une algèbre de <u>Gorenstein</u>) – et écrivons dorénavant $\hat{A} = \mathrm{Hom}_O(A, O)$.
On a alors

$$0 \xrightarrow{\hat{\pi}} \hat{A} \simeq A \xrightarrow{\pi} O$$

$$\begin{aligned} \mathrm{Ann}_A(I_A) &= \mathrm{Hom}_A(O, A) \\ &\simeq \mathrm{Hom}_A(O, \hat{A}) \\ &\simeq \mathrm{Hom}_A(A, O) \quad \text{par dualité} \\ &\simeq A\hat{\pi}, \end{aligned}$$

donc

$$\eta_A = (\pi(\mathrm{Im}\,\hat{\pi}))$$

Revenons au départ : $\mathcal{O}$, par (iii) est une algèbre de Gorenstein

o-95) (On continue la preuve du Lemme 2.)

Remarque (3) On a $\pi : (\mathrm{Ann}_A I_A) \xrightarrow{\sim} \eta_A$ si $\eta_A \neq 0$ et A est

Dém Soit $x \in \mathrm{Ker}\, \pi | \mathrm{Ann}_A I_A = \mathrm{Ann}_A I_A \cap I_A$.

Prenons $a \in \eta_A$ tel que $a \neq 0$, $a = \pi(b)$ avec $b \in \mathrm{Ann}_A I_A$.

On a

$$ax = (a-b)x \quad (\text{car } b \in \mathrm{Ann}_A I_A,\ x \in I_A)$$
$$= 0 \quad \text{car } x \in \mathrm{Ann}_A I_A \text{ et } a-b \in \mathrm{Ker}\, \pi$$

donc $x = 0$.

□

La propriété de Gorenstein

(4) Soient A, B, C des $\mathcal{O}$-modules libres de ~~[illegible]~~ rang fini.

Posons $\hat{A} = \mathrm{Hom}_{\mathcal{O}}(A, \mathcal{O})$: c'est aussi un $\mathcal{O}$-module libre de rang fini $\mathrm{rg}(A)$.

Propriétés

(i) $A \simeq \hat{\hat{A}}$ canoniquement via la flèche usuelle

$$\begin{cases} a \longmapsto (\lambda \longmapsto \lambda(a)) \\ A \longrightarrow \hat{\hat{A}} \end{cases}$$

(ii) Si $A \to B \to C$ est exacte, comme ce sont des modules libres, on a une suite exacte

$$\hat{C} \to \hat{B} \to \hat{A}$$

(iii) Supposons que A est une $\mathcal{O}$-algèbre locale de Gorenstein (ie $\hat{A} = \mathrm{Hom}_{\mathcal{O}}(A, \mathcal{O})$ est un A-module libre de rang 1),

Alors $\hat{A} \otimes_A A/\mathfrak{m}_A \simeq A/\mathfrak{m}_A$, c'est un corps.

(iv) $\mathrm{Ann}_A(I_A) \simeq \mathrm{Hom}_A(\mathcal{O}, A) \simeq \mathrm{Hom}_A(\hat{A}, \hat{\mathcal{O}}) \simeq \mathrm{Hom}_A(A, \mathcal{O})$
(par Gorenstein) $= A\pi$

(car toute $A \xrightarrow{\lambda} \mathcal{O}$ se factorise par Ker π)

de sorte que η_A est engendré par l'image par π d'un élément de $\mathrm{Ann}_A I_A$:

$$\mathcal{O} \xrightarrow{\hat{\pi}} \hat{A} \simeq A \xrightarrow{\pi} \mathcal{O}$$

$\pi \circ \hat{\pi} : \mathcal{O} \to \mathcal{O}$ est défini par son image

$$\mathrm{Im}\, \pi \circ \hat{\pi} = \eta_A$$

Lemme – Soit $A \xrightarrow{\varphi} B \xrightarrow{\pi} \mathcal{O}$ comme d'habitude, A de Gorenstein

Si $\eta_A = \eta_B \neq 0$, alors φ est un isomorphisme.

Dém. On doit calculer Ker φ ; par hypothèse

$\mathrm{Ann}_B I_B \simeq \eta_B \simeq \eta_A \simeq \mathrm{Ann}_A I_A$, or on a une flèche induite

$$\mathrm{Ann}_A I_A \xrightarrow[\sim]{\varphi} \mathrm{Ann}_B I_B$$

Considérons le $\mathcal{O}$-module $B/\mathrm{Ann}_B I_B \subset \mathrm{End}_{\mathcal{O}}(I_B)$: c'es encore un $\mathcal{O}$-module libre de rang fini, et on a une flèch

$$A/(\mathrm{Ker}\,\varphi + \mathrm{Ann}_A I_A) \longrightarrow \varphi(A)/\varphi(\mathrm{Ann}_A I_A) = B/\mathrm{Ann}_B I_B$$

d'où la suite exacte

$$0 \longrightarrow \mathrm{Ker}\,\varphi + \mathrm{Ann}_A I_A \longrightarrow A \longrightarrow B/\mathrm{Ann}_B I_B \to 0$$

Comme $\mathrm{Ker}\,\varphi \subset I_A$, le calcul de (3) ci-devant donne

$$\mathrm{Ker}\,\varphi + \mathrm{Ann}\, I_A = \mathrm{Ker}\,\varphi \oplus \mathrm{Ann}\, I_A$$

et par dualité il vient

$$0 \to (B/\mathrm{Ann}_B I_B)^\wedge \to \hat{A} \longrightarrow (\mathrm{Ker}\,\varphi)^\wedge \oplus (\mathrm{Ann}\, I_A)^\wedge \to 0$$

puis

$$0 \to (B/\mathrm{Ann}_B I_B)^\wedge \otimes k \longrightarrow \underbrace{\hat{A} \otimes k}_{\text{dimension } 1} \longrightarrow ((\mathrm{Ker}\,\varphi)^\wedge \otimes k) \oplus (\mathrm{Ann}\, I_A)^\wedge \otimes$$

$k = A/\mathfrak{m}_A$

Or $(\mathrm{Ann}\, I_A)^\wedge \otimes k \simeq \eta_A^\wedge \otimes k \neq 0$ donc forcément

$$(\mathrm{Ker}\,\varphi)^\wedge \otimes k = 0$$

et finalement $\mathrm{Ker}\,\varphi = 0$.

□

Rappelons qu'on a montré

Lemme – Soit $A \xrightarrow{\varphi} B \xrightarrow{\pi} \mathcal{O}$ avec B d'intersection complète locale Alors si $I_B/I_B^2 \simeq I_A/I_A^2$, φ est un isomorphisme.

Et on revient encore au lemme 2...

Lemme 2. Soit B une $\mathcal{O}$-algèbre libre de rang finie sur $\mathcal{O}$ et $\pi : B \twoheadrightarrow \mathcal{O}$ une surjection.
Alors il existe A, anneau local d'intersection complète (libre de rang fini sur $\mathcal{O}$ donc) et une surjection $\varphi : A \twoheadrightarrow B$ telle que A est de Gorenstein, et $\mathrm{Fit}_{\mathcal{O}}(I_A/I_A^2) = \eta_A$, avec

$$I_A/I_A^2 \simeq I_B/I_B^2$$

Dém.

$\boxed{\text{Exemple}}$ $\begin{cases} \mathbb{Z}_\ell[[X,Y]]/(X^2-\ell X,\ Y^2-\ell Y,\ XY) \xrightarrow{\pi} \mathbb{Z}_\ell \\ f \longmapsto f(0) \end{cases}$

Soient $b_1, \dots, b_n$ des générateurs de I_B sur B.

$I_B = (\bar{X}, \bar{Y})$, $b_1 = \bar{X}$, $b_2 = \bar{Y}$, $I_B^2 = (\ell\bar{X}, \ell\bar{Y})$

On regarde $\begin{cases} B^n \longrightarrow I_B \\ (c_1, \dots, c_n) \longmapsto \sum c_i b_i \end{cases}$

qui induit une application bien définie

$$\begin{cases} \mathcal{O}^n \twoheadrightarrow I_B/I_B^2 \\ (d_1, \dots, d_n) \longmapsto \sum d_i b_i \end{cases}$$

$\begin{cases} \mathbb{Z}_\ell^2 \twoheadrightarrow I_B/I_B^2 = \mathbb{Z}_\ell/(\ell) \oplus \mathbb{Z}_\ell/(\ell) \\ (d_1, d_2) \longmapsto d_1\bar{X} + d_2\bar{Y} \end{cases}$

On a montré que $B = \mathcal{O}[b_1, \dots, b_n]$.

Soient $((a_{i1}, \dots, a_{in}))_{1\leq i\leq n}$ des générateurs du noyau de cette application

On a $\sum a_{ij} b_j \in I_B^2$, $\forall i, 1 \leq i \leq n$, donc c'est un polynôme en les b_k de degré au moins 2, soit $g_i \in \mathcal{O}[X_1, \dots, X_n]$ tel que $g_i(b_1, \dots, b_n) = 0$ et

$$g_i = \sum a_{ij} X_j + (\text{degré supérieur})$$

$\left.\begin{matrix} (\ell, 0) \\ (0, \ell) \end{matrix}\right\}$ engendrent le noyau

$$\ell\bar{X} = \bar{X}^2$$
$$\ell\bar{Y} = \bar{Y}^2$$

donc $\begin{cases} g_1 = -X^2 + \ell X \\ g_2 = -Y^2 + \ell Y \end{cases}$ convient

On choisit m entier tel que les monômes $\prod X_j^{b_j}$ de degré au plus m engendrent B sur $\mathcal{O}$, et $m+2 \geq \deg g_i$, $\forall i$.

$m = 1$: $\bar{X}$ et $\bar{Y}$ engendrent B et $2 \leq 3$

On a $b_i^{m+1} = h_i(b_1, \dots, b_n)$ avec $\deg h_i \leq m$

$b_1^2 = \bar{X}^2 = \ell\bar{X}$ donc $h_1 = \ell X$
$b_2^2 = \bar{Y}^2 = \ell\bar{Y}$ donc $h_2 = \ell Y$

On pose $f_i = X_i^{m+3} - X_i^2 h_i + g_i$

$$f_i(b_1, \dots, b_n) = b_i^2 (b_i^{m+1} - h_i(b_1, \dots, b_n)) = 0$$

et

$$f_i = X_i^{m+3} + (\text{degré inférieur})$$
$$f_i = \sum a_{ij} X_j + (\text{degré supérieur})$$

Enfin,

$$D = \begin{cases} \mathcal{O}[X_1, \dots, X_n]/(f_1, \dots, f_n) \twoheadrightarrow B \\ X_i \longmapsto b_i \end{cases}$$

$f_1 = X^4 - X^2(\ell X) + (-X^2 + \ell X) = X^4 - \ell X^3 - X^2 + \ell X$
$f_2 = Y^4 - \ell Y^3 - Y^2 + \ell Y$

ie $f_1 = (X^2 - \ell X)(X^2 - 1)$
$f_2 = (Y^2 - \ell Y)(Y^2 - 1)$

donc

$$D = \mathbb{Z}_\ell[X,Y]/\left((X^2-\ell X)(X^2-1),\ (Y^2-\ell Y)(Y^2-1)\right)$$

(En particulier, ce n'est pas un anneau local)

On écrit $O = \prod_m O_m$ comme produit d'anneaux locaux

$$O/\ell O = \mathbb{F}_\ell[X,Y]/(X^2(X^2-1),\ Y^2(Y^2-1))$$

$$= \mathbb{F}_\ell[X,Y]/(X^2,Y^2) \times \mathbb{F}_\ell[X,Y]/(X^2,Y+1) \times \mathbb{F}_\ell[X,Y]/(X^2,Y-1)$$

$$\times \ldots \quad (9 \text{ termes})$$

$$D = \mathbb{Z}_\ell[X,Y]/(X^2,Y^2) \times \mathbb{Z}_\ell[X,Y]/(X^2,Y+1) \times \ldots$$

Mais le seul idéal maximal qui nous concerne est celui où $X_i \mapsto 0$,

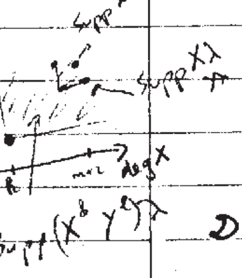
$$D = D_m \times D'$$

On prend alors $A = D_m$, qui a une surjection $A \twoheadrightarrow B$.

$$D_m = \mathbb{Z}_\ell[[X,Y]]/(X^2-\ell X,\ Y^2-\ell Y)$$

On vérifie que D est de Gorenstein en considérant $\lambda \in \hat{O}$ telle que

$$\begin{cases} \prod X_i^{m+2} \longmapsto 1 \\ \prod X_i^{k_i} \longmapsto 0 \quad \text{si } \exists i,\ k_i < m+2 \end{cases}$$



Enfin, on calcule η_A :

D'abord, η_D : comme D est de Gorenstein

$$\mathrm{Ann}_D I_D \simeq \mathrm{Hom}_O(O,O) \simeq \mathrm{Hom}_O(D,O)$$
$$\simeq \mathrm{Hom}_D(D,O)$$
$$\simeq D\pi$$

On sait que $\mathrm{Fit}_D(I_D) \subset \mathrm{Ann}_D I_D$, et on construit un élément de $\mathrm{Fit}(I_D)$ à partir de

$$D^n \twoheadrightarrow I_D \to 0$$

On peut trouver $f_{ij} \in D$ tels que $\sum_{j=1}^{n} f_{ij} X_j = 0$:

$$f_i = X_i^{m+3} - X_i^2 h_i + g_i$$
$$= \underbrace{X_i\,(X_i^{m+2} + \underbrace{\ldots}_{d^0 \leq m+1})}_{f_{ii}} + \underbrace{X_j\,(\underbrace{\ldots}_{d^0 \leq m+1})}_{f_{ij}} + \ldots$$

donc $\det(f_{ij}) \in \mathrm{Ann}_D I_D$

Fait : cet élément engendre $\mathrm{Ann}_D I_D$.
Car si $x \in \mathrm{Ann}_D I_D$ et $\lambda(x) = 1$, x doit engendrer $\mathrm{Ann}_D I_D$.

le déterminant est

$$\begin{vmatrix} X_1^{m+2} & & ? \\ & \ddots & \\ ? & & X_n^{m+2} \end{vmatrix}$$

incomplet

donc il y a au moins le terme $\prod X_i^{m+2}$ dans le déterminant.

Maintenant $\eta_D = \pi(\mathrm{Ann}_D I_D)$ est donné par les termes constants, donc

$$\eta_D = (\det(f_{ij})) = \mathrm{Fit}_O(I_D/I_D^2)$$

☐

Séminaire 5 (Tunnell) 27-10

Rappel de la situation

On a une représentation $\rho : G_{\mathbb{Q}} \to Gl(2,\mathbb{F})$, $\mathbb{F}$ corps fini de caractéristique p.

Conjecture de Serre

(Forme naïve) ρ est modulaire

(Forme raffinée) ρ est modulaire de niveau $N = \prod_{\ell \neq p} \ell^{a(\ell/G_\ell)}$ conducteur d'Artin local

de poids k prédit

de caractère ε, également prédit.

On a dit que : k <u>ne dépend que de</u> $\rho | G_p$

Considérons alors la représentation locale :

$$\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p) = G_p \xrightarrow{\rho_p} GL(2, \mathbb{F}) \simeq \mathrm{Aut}\, V, \quad V\ \mathbb{F}\text{-ev de dim. } 2$$

$$\begin{matrix} \cup \\ I \\ \cup \\ P \end{matrix}$$

Et on a vu que la semi-simplifiée V^{ss} vérifie : P agit trivialement sur V^{ss}, d'où

$$V^{ss}|_I \simeq \varphi \oplus \varphi'$$

pour des caractères $\varphi, \varphi' : I/_P \longrightarrow \overline{\mathbb{F}}_\sigma^\times$

De plus, on a

$$I/_P \simeq \varprojlim \mathbb{F}_{p^n}^\times$$

et φ et φ' sont de niveau 1 ou 2, ie se factorisent par

$$\varphi, \varphi' : I/_P \longrightarrow \overline{\mathbb{F}_{p^n}^\times} \longrightarrow \overline{\mathbb{F}_p^\times}$$

avec $n \leq 2$.

Cela permet de donner la recette pour le poids :

- <u>Cas (I)</u>. φ et φ' sont de niveau 2, (en particulier non triviaux).
- <u>Cas (II)</u>. φ et φ' de niveau 1 et P agit trivialement sur V.
- <u>Cas (III)</u>. φ et φ' ——————, ———— non-trivialement.

<u>1^{e} cas</u>

(<u>Rappel</u> : caractères fondamentaux de degré 2

$$\begin{tikzcd} \mathbb{F}_{p^2} \arrow[r, "\sigma"] & \mathbb{F}_{p^2} \\ \mathbb{F}_{p^2}^\times \arrow[u, phantom, "\cup"] \arrow[r, "\tilde{\sigma}"] & \mathbb{F}_{p^2}^\times \arrow[u, phantom, "\cup"] \end{tikzcd}$$

$\sigma \in \mathrm{Gal}(\mathbb{F}_{p^2}/\mathbb{F}_p)$

ie $\sigma = 1$

ou $\sigma = (x \longmapsto x^p)$

On note φ_1 et φ_2 ces deux caractères fondamentaux)

On écrit $\varphi = \psi^{a+bp}$ $\quad 0 \leq a, b \leq p-2$, ψ un des caractères φ_1, φ_2

$$\varphi' = \varphi^p = \psi^{b+ap}$$

On peut supposer $a \leq b$, et on note que $a \neq b$ car sinon le niveau de φ serait 1...

Finalement on a $0 \leq a < b \leq p-1$ et on pose

$$(1) \qquad \boxed{k = 1 + pa + b}$$

<u>2^{e} cas</u>. On a $I/_P \longrightarrow GL(2, \mathbb{F})$ puisque $\rho|P = \mathrm{Id}$ et $I/_P$ est un groupe abélien d'"ordre" premier à p, donc (comme précédemment pour V^{ss}), V est semi-simple et s'écrit donc avec les caractères précédents

$$\rho | I \simeq \varphi \oplus \varphi' = \psi^a \oplus \psi^b$$

(où $\psi : \mathbb{F}_p^\times \longrightarrow \mathbb{F}_p^\times$ est le caractère fondamental induit par $\mathbb{F}_p \rightarrow$

Cette fois $0 \leq a, b \leq p-2$, et on pose

$$(2) \qquad \boxed{\begin{cases} k = 1 + pa + b & , \ (a,b) \neq (0,0) \\ k = p & , \ (a,b) = (0,0) \end{cases}}$$

après avoir choisi $a \leq b$.

<u>N.B.</u> Le cas $(0,0)$ est différent car la formule donnerait $k = 1$ est "singulier" comme poids pour une forme modulaire.

<u>3^{e} cas</u>. P agit non-trivialement sur l'espace vectoriel V, ie un ensemble fini d'ordre $p^2 - 1$ $(V \setminus \{0\})$ premier à p : par -séquent P fixe $v_0 \in V$ et a fortiori la droite engendrée par

Cela signifie que

$$\rho | P \simeq \begin{pmatrix} 1 & \alpha \\ 0 & \beta \end{pmatrix}$$

Ensuite I agit via $\underbrace{I/_P}_{\text{abélien}}$, donc cela doit donner

$$\rho | I = \begin{pmatrix} \theta_2 & * \\ 0 & \theta_1 \end{pmatrix}$$

On écrit $\theta_2 = \varphi$, $\theta_1 = \varphi'$, $\quad \varphi = \psi^\beta$, $\varphi' = \psi^\alpha$, au

$0 \leq \alpha \leq \underset{!}{\underline{p-2}}$, $1 \leq \beta \leq \underset{!}{\underline{p-1}}$

<u>1^{e} sous-cas</u>. Si $\beta \neq \alpha + 1$, alors on pose

$$(3) \qquad \boxed{k = 1 + p\alpha + \beta}$$

<u>2^{e} sous-cas</u>. Si $\beta = \alpha + 1$:

$$I \left(\begin{tikzcd} \overline{\mathbb{Q}}_p \arrow[dr, dash, "P"] & \\ & \mathbb{Q}_p^t \arrow[dl, dash] \\ \mathbb{Q}_p^{nr} \arrow[d, dash] & \\ \mathbb{Q}_p & \end{tikzcd} \right.$$

on regarde $\mathbb{Q}_p^t / \mathbb{Q}_p^{nr}$: $\mathrm{Gal}(K^t / K^{nr})$

$$\begin{aligned} &\quad \downarrow \\ &\psi^\alpha \oplus \psi^\beta \\ &= \psi^\alpha(\psi \oplus 1) \end{aligned}$$

(car $\beta = \alpha + 1$)

Descendons au niveau fini $K = \overline{\mathbb{Q}_p}^{\operatorname{Ker}\rho}$:

$$\begin{tikzcd} K \arrow[d, dash] \\ K^t \arrow[d, dash] \\ K^{nr} \arrow[d, dash] \\ \mathbb{Q}_p \arrow[uuu, bend left=60, dash, "G"] \end{tikzcd}$$

<u>Affirmation</u> on a $K^t = K^{nr}(\sqrt[p]{1})$, et par théorie de Kummer, $K = K^t(\sqrt[p]{x_1}, \dots, \sqrt[p]{x_n})$

On dit que la situation est <u>peu ramifiée</u> si pour tout i, $p \mid v_p(x_i)$, sinon on dit que c'est <u>très ramifié</u>

Dans le cas peu ramifié, on pose

$$(4) \qquad \boxed{k = 1 + p\alpha + \beta} = 2 + \alpha(p+1)$$

et dans le cas très ramifié, on pose

$$(5) \qquad \boxed{\begin{cases} k = (\alpha+1)(p+1) & p \neq 2 \\ k = 4 & p = 2 \end{cases}}$$

<u>Exemples</u>

Prenons $\rho : G_{\mathbb{Q}} \longrightarrow GL(2, \mathbb{F}_2)$ absolument irréductible

<u>Fait</u> : $GL(2, \mathbb{F}_2) \simeq \mathfrak{S}_3$

$\qquad\qquad \| $

$\quad \operatorname{Aut}(\mathbb{F}_2 \oplus \mathbb{F}_2)$

($\mathbb{F}_2^2$ contient 3 lignes qui doivent permutées)

Pour trouver ρ, il faut trouver un corps $K = \overline{\mathbb{Q}}^{\operatorname{Ker}\rho}$ (de degré ≤ 6)

Quels sont les sous-groupes de $GL(2, \mathbb{F}_2)$:

ordre 3 : $\mathbb{F}_4^\times \triangleleft GL(2, \mathbb{F}_2)$ (action sur $\mathbb{F}_4 \simeq \mathbb{F}_2^2$, irréductible, mais pas absolument irréductible)

Alors

$$\begin{tikzcd} K \arrow[dd, dash] \arrow[dr, dash] & \\ & L \arrow[dl, dash, "\deg \mid 2"] \\ \mathbb{Q} & \end{tikzcd}$$

On voit ainsi que si ρ est absolument irréductible, son image doit être $\mathfrak{S}_3$.

(Si $\operatorname{Im}\rho \neq \mathfrak{S}_3$, on doit avoir $\operatorname{Im}\rho \neq 1$, $\operatorname{Im}\rho$ non abélienne d'ordre 2 et on a vu non $\mathbb{F}_4^\times$ – le 3-Sylow –)

Autrement dit ρ équivaut à se donner un corps K de degré 6 de groupe de Galois $\mathfrak{S}_3$.

$$\begin{tikzcd} \overline{\mathbb{Q}}^{\operatorname{Ker}\rho} = K \arrow[dd, dash, "G"'] \arrow[dr, dash, "3"] & \\ & L \arrow[dl, dash, "2"] \\ \mathbb{Q} & \end{tikzcd}$$

<u>Ex. 1</u> $\quad K = \mathbb{Q}(\mu_3, \sqrt[3]{2}) = \mathbb{Q}(S)$ avec $X^3 - 2 = 0$

$$\begin{tikzcd} q_2^3 \ K \arrow[dd, dash] \arrow[dr, dash] & \\ & p_2 \ \mathbb{Q}(\mu_3) \arrow[dl, dash] \\ 2 \ \mathbb{Q} & \end{tikzcd}$$

Calculons le poids k : on regarde la restriction à D_2 :

$$\begin{tikzcd} K_3 \arrow[d, dash, "{3,\ \text{totalement ramifiée}}"] \\ E \arrow[d, dash, "\text{non-ramifiée de degré 2}"] \\ \mathbb{Q}_2 \arrow[uu, bend left=60, dash, "G_2"] \end{tikzcd}$$

Dans ce cas on a

$$I_2 \simeq \operatorname{Gal}(K_3/I)$$

et donc $P_2 = 1$:

$$G_2 \underset{2}{\supset} I_2 \underset{3}{\supset} P_2 = 1$$

La seule image possible de I_2 doit être $\mathbb{F}_4^\times$, et donc on est dans le cas (I) avec des caractères d'ordre 2

$$I \longrightarrow \mathbb{F}_4^\times \subset GL(2, \mathbb{F}_2)$$

...

On trouve alors $k = 2$.

Quand au niveau, on complète en $\ell \neq 2$, ℓ ramifiant ie $\ell = 3$ on étudie le comportement de $3 \in \mathbb{Q}$:

$$\begin{tikzcd} & K = \mathbb{Q}(\mu_3, \sqrt[3]{2}) \arrow[dl, dash] \arrow[dr, dash] & \\ p_3^2 \ \mathbb{Q}(\mu_3) \arrow[d, dash] & & \mathbb{Q}(\sqrt[3]{2}) \ q_3\, q_3'\, q_3'' \\ 3 \ \mathbb{Q} \arrow[urr, dash, "3"'] & & \end{tikzcd}$$

$$x^3 - 2 \equiv x^3 + 1 \quad (3)$$

$$= (x+1)^3$$

q_3 est soit premier, soit produit de 2 premiers dans K

seul 2 ramifie

Dans K, p_3 ne peut avoir d' exposant plus que 1
donc

. soit p_3 reste premier

1er cas - soit $p_3 = q_a q_b q_c$, $q_a^2 = q_3$.

le 1er cas est impossible via l' autre chemin.

On complète :

$$\begin{tikzcd} K_3 \arrow[d, dash, "\|"] \\ K_r \arrow[d, dash, "2"', "\text{ramifiée}"] \\ \mathbb{Q}_3 \end{tikzcd}$$

et donc G_3 est d' ordre 2. De plus $I_3 = G_3$ car l' extension est ramifiée et $e_3 = 1$ car c'est un 3-groupe.

$$1 = G_1 \subset G = G_0$$

On peut calculer alors le conducteur d' Artin

$$a(\chi) = \sum_{i \geqslant 0} \frac{1}{[G_0 : G_i]} \dim\left(V/_{V}G_i\right)$$

$$= \frac{1}{1} \cdot \dim\left(V/_{V}I_3\right) + \frac{1}{2}\dim\left(V/_V\right)$$

G_3 est d' ordre 2 agissant sur $\mathbb{F}_2^2 \setminus \{0\}$ d' ordre 3 donc fixe un élément, et

$$a(\chi) = 1$$

de sorte que

$$\begin{cases} N = 3^1 = 3 \\ k = 2 \end{cases}$$ hum hum...

10
/95)

Rappel

$\mathcal{O}$ anneau de valuation discrète complet

$R \xrightarrow{\pi} \mathcal{O}$ $\mathcal{O}$-algèbre locale noethérienne (complète)

I_{R}/I_R^2 , $\pi(\mathrm{Ann}_R(I_R)) = \eta_R \subset \mathcal{O}$ les invariants

Lemme 1. Si on a des surjections $R \xrightarrow{\varphi} A \xrightarrow{\pi} \mathcal{O}$ et A est d' intersection complète, et si de plus $I_R/I_R^2 \simeq I_A/I_A^2$ (comme $\mathcal{O}$-modules) et ce sont des modules de longueur finie, alors φ est un isomorphisme.

Lemme 2. Soit $A \xrightarrow{\varphi} B \xrightarrow{\pi} \mathcal{O}$ des surjections, A, B étant des $\mathcal{O}$-algèbres libres de rang fini, et A de Gorenstein.
Alors si $\eta_A = \eta_B \neq 0$, φ est un isomorphisme.

Lemme 3. Si B est une $\mathcal{O}$-algèbre locale libre de rang fini, $\pi : B \twoheadrightarrow \mathcal{O}$ une surjection, alors il existe une surjection $A \xrightarrow{\varphi}$ avec A d' intersection complète et φ induit

$$I_A/I_A^2 \simeq I_B/I_B^2$$

De plus, on peut supposer que A est de Gorenstein et

$$\eta_A = \mathrm{Fit}_{\mathcal{O}}(I_A/I_A^2)$$

Proposition. Soit B une $\mathcal{O}$-algèbre locale libre de rang fin
et $\pi : B \twoheadrightarrow \mathcal{O}$ une surjection (locale).
Supposons que $\eta_B \neq 0$.
Alors B est une intersection complète $\Leftrightarrow$ $\mathrm{Fit}_{\mathcal{O}}(I_B/I_B^2) = \eta_B$.

Dém. On applique le lemme 3 à B : il existe $A \xrightarrow{\varphi} B$ avec A d' intersection complète et $I_A/I_A^2 \simeq I_B/I_B^2$.

Si B est d' intersection complète, le lemme 1 implique qu φ est un isomorphisme, et le lemme 3 dit alors également

$$\eta_B = \eta_A = \mathrm{Fit}(I_A/I_A^2) = \mathrm{Fit}(I_B/I_B^2)$$

Réciproquement, si $\eta_B = \mathrm{Fit}_{\mathcal{O}}(I_B/I_B^2)$ on en déduit

$$\eta_B = \mathrm{Fit}_{\mathcal{O}}(I_A/I_A^2) = \eta_A \ , \quad \eta_B \neq 0$$

et A est de Gorenstein donc le lemme 2 dit que φ est un isomorphisme, et B est d' intersection complète
☐

Théorème d' isomorphisme de Wiles-Lenstra.

Soit R une $\mathcal{O}$-algèbre locale complète noethérienne, B u
$\mathcal{O}$-algèbre finie et libre plate, munie de $B \xrightarrow{\pi} \mathcal{O}$.
Supposons que $\varphi : R \twoheadrightarrow B$ est une surjection de $\mathcal{O}$-algèbre
Alors les conditions suivantes sont équivalentes :

(i) $\ell(I_R/I_R^2) \leq \ell(\mathcal{O}/\eta_B) < +\infty$

(ii) $\ell(I_R/I_R^2) = \ell(\mathcal{O}/\eta_B) < +\infty$

(iii) φ est un isomorphisme, B est d'intersection complète et $\eta_B \neq 0$.

<u>Dém.</u> (iii) $\Rightarrow$ (ii) : d'après la dernière proposition, B étant d'intersection complète et $\eta_B \neq 0$, on a

$$\eta_B = \mathrm{Fit}_{\mathcal{O}}(I_B/I_B^2) = m_{\mathcal{O}}^{\ell(I_R/I_R^2)}$$

Mais $\eta_B \neq 0 \Rightarrow \ell(\mathcal{O}/\eta_B) < +\infty$, et l'égalité dit exactement

$$\ell(\mathcal{O}/\eta_B) = \ell(I_R/I_R^2)$$

(ii) $\Rightarrow$ (i) : trivial

(i) $\Rightarrow$ (iii) : (i) implique $\eta_B \subset \mathrm{Fit}_{\mathcal{O}}(I_R/I_R^2)$ (comme dans la 1e étape)

On a donc

$$R \twoheadrightarrow B \xrightarrow{\pi} \mathcal{O}$$

$$I_R \twoheadrightarrow I_B$$

$$I_R/I_R^2 \twoheadrightarrow I_B/I_B^2$$

et clairement
$$\begin{array}{ccc} \mathrm{Fit}_{\mathcal{O}}(I_R/I_R^2) & \subset & \mathrm{Fit}_{\mathcal{O}}(I_B/I_B^2) \\ \cap & & \cap \\ \eta_R & & \eta_B \end{array}$$
| vu il y a longtemps

D'abord (i) implique donc $\eta_B \neq 0$ grâce à ce diagramme.
Mais (i) implique aussi aussitôt également

$$\eta_B = \mathrm{Fit}_{\mathcal{O}}(I_R/I_R^2)$$

et $\eta_B = \mathrm{Fit}_{\mathcal{O}}(I_B/I_B^2)$ nécessairement ; d'après la proposition, B est donc d'intersection complète.

Comme on a déjà $I_R/I_R^2 \twoheadrightarrow I_B/I_B^2$, $\mathrm{Fit}(I_R/I_R^2) = \mathrm{Fit}(I_B/I_B^2)$ (ie $\ell(I_R/I_R^2) = \ell(I_B/I_B^2)$), suffit pour avoir $I_R/I_R^2 = I_B/I_B^2$, et en appliquant le lemme 1, φ est un isomorphisme.

$\square$

Application

On va considérer le cas suivant :

$\mathbb{T}_N = B = \mathcal{O}[(\mathbb{Z}/(N))^\times]$ "correctement" localisée

R = l'algèbre des déformations, correspondant aux déformations non-ramifiées en dehors de N, plus des conditions locales en $\ell | N$ (sinon, R serait trop gros)

On a alors $\mathrm{Def}\,\mathrm{Alg}_N \twoheadrightarrow \mathbb{T}_N$
et on va appliquer le théorème de Wiles-Lenstra

Invariants η

<u>Ex.</u> (1) $B = \mathcal{O} = \mathcal{O}[T]/T$, $\pi : \mathcal{O} \twoheadrightarrow \mathcal{O}$ $\mathrm{Ker}\,\pi = 0$
et $\mathrm{Ann}(\mathrm{Ker}\,\pi) = 0$, $\eta_{\mathcal{O}} = 0$

(<u>Ou</u> : $\mathcal{O}/\eta_{\mathcal{O}} = \mathrm{Fit}(I_{\mathcal{O}}/I_{\mathcal{O}}^2) = \mathrm{Fit}(0) = 0$)

<u>Ex.</u> (2) $\mathcal{O}[(\mathbb{Z}/(3))^\times] \xrightarrow{\pi} \mathcal{O}$: il y a 2 π possibles
$\qquad \| \qquad\qquad\qquad\qquad\qquad\qquad 1 \mapsto 1, \ -1 \mapsto 1$
$\mathcal{O}.1 \oplus \mathcal{O}.2 \qquad\qquad\qquad$ ou $1 \mapsto 1, \ -1 \mapsto -1$

Remarquons préalablement en général que pour G cyclique d'ordre m engendré par γ, on a

$$\mathcal{O}[G] = \mathcal{O}[T]/(T^m - 1)$$

$$\gamma \longleftrightarrow T$$

donc ici $\mathcal{O}[(\mathbb{Z}/(3))^\times] \simeq \mathcal{O}[T]/(T^2 - 1)$

On localise $\mathcal{O}[G]$ en $\mathrm{Ker}(\mathcal{O}[G] \to \mathcal{O} \to \mathcal{O}/m_{\mathcal{O}})$.

pas surjective si 2 non inversible !

$$\mathcal{O}[T]/_{(T-1)} \times \mathcal{O}[T]/_{(T+1)} \overset{\downarrow}{\longleftrightarrow} \mathcal{O}[T]/_{(T^2-1)} \xrightarrow{\pi} \mathcal{O} \longrightarrow \mathcal{O}/m_{\mathcal{O}}$$

$$(a+b, a-b) \longleftarrow\!\shortmid \ a+bT$$

On trouve ainsi

$$\mathcal{O}[T]/_{(T^2-1)} \simeq \{(r,s) \in \mathcal{O}\times\mathcal{O} \mid r \equiv s \ (\text{mod } 2\mathcal{O})\}$$

<u>1^{er} cas</u> :
$$\begin{cases} \mathcal{O}[T]/_{(T^2-1)} \xrightarrow{\pi} \mathcal{O} \longrightarrow \mathcal{O}/m_{\mathcal{O}} \\ T \longmapsto 1 \\ (a+bT) \longmapsto a+b \longmapsto (a+b) \text{ mod } m_{\mathcal{O}} \end{cases}$$

<u>2^{e} cas</u> :
$$\begin{cases} \mathcal{O}[T]/_{(T^2-1)} \xrightarrow{\pi'} \mathcal{O} \longrightarrow k \\ T \longmapsto -1 \\ (a+bT) \longmapsto a-b \longmapsto (a-b) \text{ mod } m_{\mathcal{O}} \end{cases}$$

Avec l'identification ci-dessous, la composition est :

$$\begin{tikzcd}
\mathcal{O}[T]/_{(T^2-1)} \arrow[r, phantom, "\simeq"] & \{(r,s) \in \mathcal{O}\times\mathcal{O} \mid r \equiv s \ (\text{mod } 2\mathcal{O})\} \\
\frac{r+s}{2} + \frac{r-s}{2}\,T \arrow[d, "\pi\ (\text{resp. } \pi')"'] & (r,s) \arrow[l, mapsto] \arrow[dl] \\
r \ (\text{mod } m_{\mathcal{O}}) \ \ (\text{resp. } s \ (\text{mod } m_{\mathcal{O}})) &
\end{tikzcd}$$

Si 2 est inversible, on voit que $\mathcal{O}[T]/_{(T^2-1)} \simeq \mathcal{O}\times\mathcal{O}$, le noyau est $\mathcal{O}\times m_{\mathcal{O}}$ (resp. $m_{\mathcal{O}}\times\mathcal{O}$) et la localisation est

$$\mathcal{O}[T]/_{(T+1)} \quad \text{ou} \quad \mathcal{O}[T]/_{(T-1)}$$

Si 2 est non-inversible, <u>alors</u> $\mathcal{O}[T]/_{(T^2-1)}$ est <u>déjà</u> local. En effet, on a alors $2 \in m_{\mathcal{O}}$, et

$$\mathcal{O}[T]/_{(T^2-1)} = \{(r,s) \in \mathcal{O}\times\mathcal{O} \mid r \equiv s\,(2\mathcal{O})\}$$
$$\cup$$
$$(2\mathcal{O}, 2\mathcal{O}) \quad \text{idéal (propre) maximal unique}$$

(car $\mathcal{O}/m_{\mathcal{O}}$ est de caractéristique 2)

$(2\mathcal{O}, 2\mathcal{O})$ est le noyau des deux compositions (ce sont les mêmes).

<u>1^{er} cas</u> : $\pi : (r,s) \longmapsto r$

On a
$$\text{Ker}\,\pi = (0, 2\mathcal{O}) = I_B$$
$$\text{Ann}(\text{Ker}\,\pi) = (2\mathcal{O}, 0)$$
$$\eta_B = \pi(\text{Ann}(\text{Ker}\,\pi)) = 2\mathcal{O} = (2)$$

(<u>2^{e} cas</u> : idem.)

On calcule aussi
$$I_B^2 = (0, 4\mathcal{O})$$
$$I_B/I_B^2 = 2\mathcal{O}/4\mathcal{O}$$

($\Rightarrow$ B est une intersection complète)

<u>Ex.</u> G cyclique d'ordre n

$$\mathcal{O}[G] \simeq \mathcal{O}[T]/_{(T^n-1)} \longrightarrow \mathcal{O}$$
$$T \longmapsto \zeta$$

(on suppose que $\mathcal{O}$ contient les racines n-ièmes de l'unité)

(?)

Si on écrit

$$\mathcal{O}[T]/_{(T^n-1)} \hookrightarrow \prod_j \mathcal{O}[T]/_{(T-\zeta^j)}$$
$$a_0 + a_1T + \dots + a_{n-1}T^{n-1} \longmapsto \left(\Sigma a_i \zeta^{ij}\right)_j$$

Si $p \mid \zeta - 1$, on a $\Sigma a_i \zeta^{ij}$ constant modulo p, pour tout j, donc la flèche n'est pas toujours surjective.

Or $T^n - 1 \in \mathcal{O}/m_{\mathcal{O}}[T]$ a des racines distinctes $\Leftrightarrow$ n non nul dans $\mathcal{O}/m_{\mathcal{O}}$.

1/11/95

Soit G un groupe abélien fini, écrit comme produit $G = \prod_{1\leq i\leq k} G_i$, avec G_i groupe cyclique d'ordre une puissance d'un nombre premier $n_i = |G_i|$.
On considère $\mathcal{O}$, l'anneau des entiers dans une extension finie de $\mathbb{Q}_p$, contenant les racines n-èmes de l'unité, $n = |G| = \prod n_i$.

Soit $\chi : G \longrightarrow \mathcal{O}^*$ un morphisme de groupes ; on en déduit une flèche de $\mathcal{O}$-algèbres $\pi : \mathcal{O}[G] \longrightarrow \mathcal{O}$

$$g_i \longmapsto \chi(g_i)$$

<u>But</u>. Analyser l'anneau obtenu en localisant $\mathcal{O}[G]$ à l'idéal maximal $m = \mathrm{Ker}\left(\mathcal{O}[G] \longrightarrow \mathcal{O} \longrightarrow \mathcal{O}/m_{\mathcal{O}}\right)$.
On note donc $A = \mathcal{O}[G]_m$.

<u>Proposition</u> (i) A est une $\mathcal{O}$-algèbre libre de rang finie sur $\mathcal{O}$, locale et complète.

(ii) A est isomorphe à $\mathcal{O}[[T_1, \dots, T_k]] / \left((T_1 + \chi(g_1))^{n_1} - 1, \dots, (T_k + \chi(g_k))^{n_k} - 1\right)$

et la flèche π devient $T_i \longmapsto 0$ via cet isomorphisme.
En particulier A est d'intersection complète

(iii) $I_A / I_A^2 \simeq \mathcal{O}/n_1\mathcal{O} \times \dots \times \mathcal{O}/n_k\mathcal{O}$

(iv) $\eta_A = n\mathcal{O} = |G|\mathcal{O}$

<u>Dém</u>. $\mathcal{O}[G] = \mathcal{O}[u_1, \dots, u_k] / (u_1^{n_1} - 1, \dots, u_k^{n_k} - 1)$

par un calcul facile, donc aussi

$$\mathcal{O}[G] \simeq \mathcal{O}[u_1, \dots, u_k] / \left((u_1 + \chi(g_1))^{n_1} - 1, \dots, (u_k + \chi(g_k))^{n_k} - 1\right)$$

par changement de variables.

Ensuite, pour localiser, il y a plusieurs méthodes.

<u>1e méthode</u> : écrire $\mathcal{O}[G]$ comme produit d'algèbres locales, et ne garder que celle qui correspond à notre idéal maximal.

<u>2e méthode</u> : par théorie des déformations : on va montrer que A et l'algèbre $\tilde{R}$ à droite dans l'isomorphisme de (ii) sont universelles pour le même problème de déformations :
soit $\chi_0 : G \xrightarrow{\chi} \mathcal{O}^* \longrightarrow (\mathcal{O}/m_{\mathcal{O}})^*$
et considérons les déformations de χ_0 :

$$\begin{tikzcd} G \arrow[r] \arrow[dr, "\chi_0"'] & B^* \arrow[d] \\ & (\mathcal{O}/m_{\mathcal{O}})^* \simeq (B/m_B)^* \end{tikzcd}$$

On a vu qu'il existe une algèbre universelle R telle que

$$\mathrm{Def}(\chi_0, B) \simeq \mathrm{Hom}_{\mathcal{O}}(R, B)$$

A est isomorphe à R d'après la définition même de $\mathcal{O}[G]$.
Étudions donc $\tilde{R}$ et montrons $\tilde{R} \simeq R$:
soit $\rho : G \longrightarrow B^*$ une déformation de χ_0 ; on a une flèche évidente $\begin{cases} G \xrightarrow{\rho^u} \tilde{R}^* \\ g_i \longmapsto T_i + \chi(g_i) \end{cases}$

et on construit aussitôt

$$\begin{cases} \tilde{R} \xrightarrow{\psi} B \\ T_i \longmapsto \rho(g_i) - \chi(g_i) \end{cases}$$

qui est bien définie car ρ est une déformation, ie $\rho(g_i) - \chi(g_i) \in m_B$
et qui vérifie $\psi \circ \rho^u = \rho$.

Cela montre alors que A est libre de rang fini sur $\mathcal{O}$, complète et locale, ie (i) et (ii) sont démontrés.

(iii) On sait que pour $R = \mathcal{O}[[T_1, \dots, T_k]] / (f_1, \dots, f_m) \longrightarrow \mathcal{O}$, on peut écrire

$$I_R / I_R^2 \simeq \mathcal{O}^k / \left\{\left(\frac{\partial f_i}{\partial T_1}(0), \dots \frac{\partial f_i}{\partial T_k}(0)\right)\right\}$$

et cela donne ici

$$I_A/I_A^2 \simeq \overbrace{O\times\dots\times O}^{k} \Big/ \{(0,\dots,\overset{\downarrow}{n_i}\underbrace{\chi(g_i)^{n_i-1}}_{\text{unité}},0,\dots0)\}$$

$$\simeq \prod_{i=1}^{k} O/n_iO$$

(iv) A est d'intersection complète donc $\eta_A = \mathrm{Fit}_O(I_A/I_A^2)$, ie ici

$$\eta_A = nO$$

□

- <u>Quelle est la signification de η_A ?</u>

On se place dans la situation précédente : on a $\chi : G \to O^\times$ et on se demande combien de déformations de χ à valeurs dans O existent, ie combien de $\chi' : G \to O^\times$ avec

$$\chi \equiv \chi' \ (m_O) \quad ?$$

Ici $\chi \equiv \chi' \ (m_O) \iff \chi\chi'^{-1} \equiv 1 \ (m_O)$, ie on a des racines de 1 congruentes à 1 modulo m_O (et réciproquement)

<u>Fait</u> Supposons que $p \nmid n_k$, alors on a

$$\chi\chi'^{-1}(g_k) = 1$$

<u>Dém</u> $\chi\chi'^{-1}(g_k)$ est une racine n_k-ème de 1 congruente à 1 modulo m_O, donc si on regarde l'équation $X^{n_k}-1$, c'est une racine égale à 1 dans O/m_O, or $X^{n_k}-1$ est séparable modulo m_O pour $p \nmid n_k$ □

. Toute solution de $X^{p^j}-1=0$ <u>est</u> congruente à 1 modulo m_O ($\mathrm{char}\, O/m_O = p$) : on a $X^{p^j}-1 = (X-1)^{p^j}$

Donc si $n_j = p^j$, le nombre de valeurs possibles pour $\chi'\chi^{-1}(g_j)$ est p^j.

Finalement, le nombre de déformations χ' est égal à $\mathrm{ord}_p G$ (ordre de la p-partie de G)

D'un autre côté, $\eta_A = nO = p^{\mathrm{ord}_p G} O$ et aussi

$$|O/\eta_A| = |O/pO|^{\mathrm{ord}_p(G)} = |O/mO|^{e\,\mathrm{ord}_p G}$$

donc η_A mesure le nbre de χ' congruents à χ... Cela réapparaîtra dans le cas des formes modulaires.

- <u>On considère le cas $G = (\mathbb{Z}/(N))^\times \simeq \mathrm{Gal}(\mathbb{Q}(\mu_N)/\mathbb{Q})$</u>

Une autre façon de voir $O[G]$:

soit V le O-module des fonctions $\underset{(\mathbb{Z}/(N))^\times}{\overset{\shortparallel}{G}} \to O$, qui est libre de rang $|G| = \varphi(N)$

Considérons la sous-algèbre de $\mathrm{End}(V)$ engendrée sur O par les T_m, où $\forall m$, $(m,N)=1$, $T_m \in \mathrm{End}\,V$ est défini par

$$(T_m f)(a) = f(ma)$$

On note $\mathbb{T}_N$ cette algèbre → analogue $Gl(1)$ de l'algèbre de Hecke

<u>Proposition</u> $\mathbb{T}_N \simeq O[(\mathbb{Z}/(N))^\times]$ via l'application

$$O[(\mathbb{Z}/(N))^\times] \ni \sum a_n[n] \xmapsto{\varphi} \sum a_n T_n \in \mathbb{T}_N$$

<u>Dém.</u> D'abord φ est une flèche de O-algèbres :

$$(T_m T_n f)(a) = T_m f(na) = f(mna) = (T_{mn} f)(a)$$

compatible avec $[nm] = [n][m]$.

φ est évidemment surjective.

Pour calculer le noyau, on peut supposer que O contient toutes les racines $\varphi(N)$-èmes de l'unité. On remarque alors que t morphisme de groupe $V \ni \chi : (\mathbb{Z}/(N))^\times \to O^\times$ est une fo propre pour tout les T_m :

$$(T_m \chi)(a) = \chi(am) = \chi(m)\,\chi(a)$$

Maintenant si $\sum a_n T_n = 0$, on en déduit

$$\forall \chi, \quad \sum_{(n,N)=1} a_n \chi(n) = 0$$

ie $a : n \mapsto a_n$ doit être nulle par orthogonalité, et finalement φ est un isomorphisme

$\square$

Retour aux déformations de représentations galoisiennes

Soit $G_{\mathbb{Q}} = \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. On veut explorer la situation suivante: on a une flèche donnée $\bar{\rho}_0 : G_{\mathbb{Q}} \longrightarrow (\mathcal{O}/m_{\mathcal{O}})^*$ et on est intéressé par les déformations $\rho : G_{\mathbb{Q}} \longrightarrow \mathcal{O}^*$. Prenant $H = \bar{\mathbb{Q}}^{\mathrm{Ker}\,\rho}$, $K_0 = \bar{\mathbb{Q}}^{\mathrm{Ker}\,\bar{\rho}_0}$; on a le diagramme

$$\begin{array}{l} K \\ | \\ \left.\begin{array}{c} K_0 \\ | \\ \mathbb{Q} \end{array}\right\} \xrightarrow{\bar{\rho}_0} (\mathcal{O}/m_{\mathcal{O}})^* \end{array}$$

D'un autre côté, d'après le § précédent on a

$$\begin{tikzcd} \mathbb{Q}(\mu_N) \arrow[d, dash] \\ K_0 = \bar{\mathbb{Q}}^{\mathrm{Ker}\,\chi_0} \arrow[d, dash] \\ \mathbb{Q} \end{tikzcd}$$

et on a calculé combien de K/K_0 existent dans $\mathbb{Q}(\mu_N)$.

On va poser des restrictions locales sur les déformations étudiées pour contrôler la situation.

Restrictions sur les déformations

(i) On suppose que la ramification est restreinte en dehors de N, ie même $\rho : G_{\mathbb{Q}} \longrightarrow A^*$ vérifie $\rho|I_\ell = 1$ si $\ell \nmid N$

(ii) On pose des restrictions ~~$\in$~~ en $p = \mathrm{char}(\mathcal{O}/m_{\mathcal{O}})$: c'est la partie difficile

(iii) Pour $\ell \mid N$, on met des restrictions peu contraignantes.

Comment trouve-t-on ces ~~[illegible]~~ restrictions ? On étudie le côté cyclotomique.

N.B: On veut éviter :
qui n'est pas dans une extension finie, mais non-ramifiée en dehors de p.

$$\begin{array}{c} \mathbb{Q}(\mu_{p^\infty}) \\ \vdots \\ \mathbb{Q}(\mu_{p^n}) \\ \vdots \\ | \\ \mathbb{Q} \end{array}$$

Le "truc" qui fera tout marcher sera que pour toute extension abélienne finie de $\mathbb{Q}$, il existe N tel que l'extension vérifie ces conditions pour N.

Séminaire 6
3/11/95
José

Représentations galoisiennes associées aux courbes elliptiques

On s'intéresse aux représentations modulo p liées aux courbes elliptiques.

Soit E une courbe elliptique sur $\mathbb{Q}$, E semi-stable, p nombre premier tel que E a réduction multiplicative en p. On peut alors utiliser la paramétrisation de Tate en p, ie il existe q tel que

$$E/\mathbb{Q}_p \simeq \mathbb{Q}_p^*/q^{\mathbb{Z}} \qquad (|q| < 1)$$

(Théorème (Tate) Soit K un corps p-adique, E/K une courbe elliptique telle que $|j(E)| > 1$, alors il existe $q \in K^*$ avec $|q| < 1$ telle que $E \otimes \bar{k} \simeq E_q \otimes \bar{k}$, E_q étant la courbe de Tate.

(En fait, l'isomorphisme a lieu au pire sur une extension quadratique non-ramifiée en p, et on l'ignore.])

Alors on a $E[p] \simeq \langle \zeta_p, \sqrt[q]{p} \rangle \simeq \mu_p \oplus \mathbb{Z}/(p)$

La situation est la suivante :

$$\begin{tikzcd} \mathbb{Q}_p(\mu_p, \sqrt[p]{q}) \arrow[d, dash, "p"'] \\ \mathbb{Q}_p(\mu_p) \arrow[d, dash, "p-1"'] \\ \mathbb{Q}_p \end{tikzcd}$$

<u>Cas (i)</u> : $v_p(q) \not\equiv 0 \ (p)$, cas "très ramifié"

(ex $q = p$) ~~[illegible]~~

p est ramifié dans les deux étapes

$\mathbb{Q}_p = \mathbb{Q}_p(\mu_p, \sqrt[p]{p})^I \Rightarrow I = G$

On peut décrire $\overset{G}{\overset{\cup}{I}}$ explicitement : soit $\sigma_{i,j} \in \overset{G}{\overset{\parallel}{\mathrm{Gal}}}(\mathbb{Q}_p(\mu_p, \sqrt[p]{q})/\mathbb{Q})$ tel que
$$\begin{cases} \sigma_{i,j}(\zeta) = \zeta^i, & 1 \leq i \leq p-1 \\ \sigma_{ij}(\sqrt[p]{q}) = \zeta^j \sqrt[p]{q}, & 0 \leq j \leq p-1 \end{cases}$$

Le groupe d'inertie sauvage I_p vérifie $(|I/I_p|, p) = 1$
donc $I_p = \mathbb{Z}/(p)$, $I/I_p \simeq (\mathbb{Z}/(p))^\times$
On constate alors directement que :
(1) I_p agit <u>non-trivialement</u> sur les points de p-division (il déplace le générateur $\sqrt[p]{q}$)
(2) $I \longrightarrow \begin{pmatrix} \chi & * \\ 0 & 1 \end{pmatrix}$ (où χ est le caractère cyclotomique)

Donc les deux caractères dans la semi-simplification sont χ et 1, de niveau 1 ; avec les notations de la recette de Serre, on a $\alpha = 0$, $\beta = 1$, ie $\beta = \alpha + 1$, et le poids prédit par Serre est $k = \begin{cases} p+1, & p \text{ impair} \\ 4, & p = 2 \end{cases}$

<u>Cas (ii)</u> : $v_p(q) \equiv 0 \ (p)$, cas "~~[illegible]~~ peu ramifié"

$$\begin{tikzcd} \mathbb{Q}_p(\mu_p, \sqrt[p]{u}) \arrow[d, dash] \\ \mathbb{Q}_p(\mu_p) \arrow[d, dash] \\ \mathbb{Q}_p \end{tikzcd}$$

On écrit $q = p^{ks} u$, $u \in \mathbb{Z}_p^\times$, la situation devient :

p est encore ramifié dans les deux étapes

I_p agit toujours non-trivialement, et I via $\begin{pmatrix} \chi & * \\ 0 & 1 \end{pmatrix}$, et comme précédemment $\alpha = 0$, $\beta = 1$, mais la recette donne cette fois $k = 2$.

<u>Calcul du conducteur de</u> ρ_{E_p}

On le note N.

Soit $\ell \neq p$; supposons que E a réduction multiplicative en ℓ.
On considère la ramification de ℓ

$$\begin{tikzcd} \mathbb{Q}_\ell(\mu_p, \sqrt[p]{q}) \arrow[d, dash] \\ \mathbb{Q}_\ell(\mu_p) \arrow[d, dash] \\ \mathbb{Q}_\ell \end{tikzcd}$$

<u>Cas (i)</u> : $v_\ell(q) \equiv 0 \ (p)$

$q = u\ell^{sp}$ et $\mathbb{Q}_\ell(\mu_p, \sqrt[p]{q}) = \mathbb{Q}_\ell(\mu_p, \sqrt[p]{u})$

et tout est non-ramifié, ie $I = 1$ et $n(\ell, p) = 0$ (exposant de ℓ dans le conducteur)

<u>Cas (ii)</u> : $v_\ell(q) \not\equiv 0 \ (p)$; soit b l'inverse de $v_\ell(q)$ modulo p ; on a alors
$$q^{b/p} = u^{b/p} \ell^{p^s} \ell \text{, pour un certain } s$$
$$\Rightarrow \sqrt[p]{\ell} \in \mathbb{Q}_\ell(\mu_p, \sqrt[p]{q}, \sqrt[p]{u})$$

On a le diagramme

$$\begin{tikzcd}[column sep=small] & & \mathbb{Q}_\ell(\mu_p, \sqrt[p]{q}, \sqrt[p]{u}) = \mathbb{Q}_\ell(\mu_p, \sqrt[p]{u}, \sqrt[p]{\ell}) \\ \mathbb{Q}_\ell(\mu_p, \sqrt[p]{q}) \arrow[urr, dash, "p", "\text{non-ramifié}"'] \arrow[dr, dash, "p"'] & & \\ & \mathbb{Q}_\ell(\mu_p) \arrow[r, dash, "p", "\text{non-ramifié}"'] \arrow[d, dash, "p-1"', "\text{non-ramifié}"] & \mathbb{Q}_\ell(\mu_p, \sqrt[p]{u}) \arrow[uu, dash, "p", "\text{ramifié, } e = p"'] \\ & \mathbb{Q}_\ell & \end{tikzcd}$$

$\Rightarrow$ on en déduit que la ramification intervient dans $\mathbb{Q}_\ell(\mu_p, \sqrt[p]{q}) / \mathbb{Q}_\ell(\mu_p)$, plus précisément, ℓ y est totalement ramifié

On en déduit $I \simeq \mathbb{Z}/(p)$, comme [illegible], I_ℓ est un ℓ-groupe on a $I_\ell = 1$.
On calcule alors d'après la formule
$$n(\ell, p) = \dim T_p(E)/T_p(E)^I + \underset{\rightarrow \text{ partie sauvage}}{0}$$

ie $n(\ell, \rho_{E,p}) = 1$ (sur le diagramme).

On applique cela aux courbes de Frey : soient $A, B, C \in \mathbb{Z}$ premiers entre eux, tels que $A+B+C=0$, et

$$(E) : \quad y^2 = x(x-A)(x+B)$$

On a $\Delta = 2^4(abc)^2$

~~R~~ <u>Réduction modulo $\ell \neq 2$</u> :

On a donc ℓ / ABC, et sur l'équation il est évident que la réduction est multiplicative ; de plus l'équation ci-dessus est minimale en ℓ

<u>Réduction modulo 2</u> :

Supposons $A \equiv -1 \ (4)$, $B \equiv 0 \ (32)$; on fait le changement de variable $x = 4X$, $y = 8Y + 4X$ et l'équation devient

$$(*) \quad Y^2 + XY = X^3 + cX^2 + dX$$

avec $c = \frac{B-1-A}{4}$, $d = -\frac{AB}{16}$

On peut réduire $(*)$ modulo 2, ce qui donne

$$Y^2 + XY = \begin{cases} X^3 & \text{si } A \equiv 7(8) \\ X^3 + X^2 & \text{si } A \equiv 3(8) \end{cases}$$

L'algorithme de Tate fournit que $(*)$ est minimale en 2, et même globalement minimale. De plus dans les deux cas, la réduction est multiplicative.

Le discriminant minimal est $\Delta_{min} = 2^{-8}(ABC)^2$, et E est semi-stable.

On considère donc $\rho_{E,p} : G_{\mathbb{Q}} \longrightarrow GL(2, \mathbb{F}_p)$.

<u>Proposition</u>. Pour $p \geq 5$, $\rho_{E,p}$ est irréductible.

<u>Dém.</u> (idée). Si $\rho_{E,p}$ est réductible, on peut trouver (c'est le 1er cas) $e \in E[p]$ tel que $\sigma(e) = e \ \forall \sigma \in G$, donc e est <u>rationnel</u> d'ordre p.

Mais sur (E) on voit que les points d'ordre 2 sont rationnels aussi, ce qui donne $|E(\mathbb{Q})_{tors}| \geq 4p \geq 20$, et cela est

on a une ligne $\mathcal{L}$ stable sur laquelle $G_{\mathbb{Q}}$ agit par 1 ou χ ; si c'est χ on applique cet argument sur $E/\mathcal{L}$

impossible d'après le théorème de Mazur classifiant les $E(\mathbb{Q})_{tors}$ possibles.

$\square$

(<u>Théorème</u> (Mazur). Soit $E/\mathbb{Q}$ une courbe elliptique, alors $E(\mathbb{Q})_{tors}$ est l'un des 15 groupes suivants :

(i) $\mathbb{Z}/(N)$, pour $1 \leq N \leq 10$ ou $N = 12$

(ii) $\mathbb{Z}/(2) \oplus \mathbb{Z}/(2N)$ pour $1 \leq N \leq 4$

En particulier, $|E(\mathbb{Q})_{tors}| \leq 12$)

On a donc

$$k = \begin{cases} 2 & \text{si } v_\ell(\Delta) \equiv 0 \ (p) \\ p+1 & \text{sinon} \end{cases}$$

$$N = \prod_{\substack{\ell \neq p \\ v_\ell(\Delta) \not\equiv 0 (p)}} \ell \qquad \left(\Leftrightarrow v_\ell(ABC) \not\equiv \begin{cases} 0 & \text{si } \ell \neq 2 \\ 4 & \text{si } \ell = 2 \end{cases} \right)$$

Enfin on applique cela à un hypothétique contre-exemple au théorème de Fermat : supposons $abc \neq 0$ et

$$a^p + b^p + c^p = 0$$

(avec $p \geq 5$), avec $\begin{cases} a \equiv -1 \ (4) \\ b \equiv 0 \ (2) \end{cases}$

Avec $A = a^p$, $B = b^p$, $C = c^p$, on a $v_\ell(ABC) \equiv 0 \ (p)$ pour tout ℓ, et la recette prédit donc

$$\begin{cases} k = 2 \\ N = 2 \end{cases}$$

D'après la conjecture de Serre (forme raffinée), il existe une forme modulaire $f = \sum a_n q^n$ de poids 2 et niveau 2 telle que $a_\ell = \mathrm{Tr}\, \rho(\mathrm{Frob})$ ~~[illegible]~~ presque tout ℓ. Mais cela est impossible car $S_2(\Gamma_0(2)) = 0$.

Ainsi la conjecture de Serre ~~[illegible]~~ implique le théorème de Fermat...