

# L'analogie pour $GL(1)$ du théorème de Wiles

(d'après Tunnell et Wiles)

L'idée de ce texte est de motiver et d'éclairer les méthodes de Wiles de façon élémentaire en les appliquant au cas de  $GL(1)$ . Bien que cela réduise dramatiquement les détails techniques et les connaissances requises pour suivre le raisonnement, cette étude n'est pas triviale : nous verrons qu'elle aboutit à une preuve élégante du théorème classique de Kronecker-Weber, à savoir :

**Théorème 1** (*Kronecker-Weber, 1886*). *Toute extension abélienne  $K/\mathbf{Q}$  de degré fini de  $\mathbf{Q}$  est contenue dans une extension cyclotomique  $\mathbf{Q}(\mu_m)$  (où  $\mu_m$  est une racine primitive  $m$ -ème de l'unité.)*

Ce théorème est considéré ici comme analogue au résultat suivant démontré par Wiles :

**Théorème 2** *Soit  $E/\mathbf{Q}$  une courbe elliptique définie sur  $\mathbf{Q}$  telle que  $E$  est semi-stable. Alors  $E$  est modulaire, c'est à dire qu'il existe un entier  $N > 0$  et une forme modulaire  $f$  de poids 2 pour  $\Gamma_0(N)$  telle que*

$$L(E, s) = L(f, s)$$

*le membre de gauche étant la fonction  $L$  de Hasse-Weil de  $E$  et celui de droite la fonction  $L$  de Hecke de  $f$ .*

L'analogie qui n'est pas parfaitement apparente provient du fait que nous déduirons aisément le théorème 1 d'un autre résultat (théorème 3 plus loin) qui permet d'identifier les caractères du groupe de Galois de  $\overline{\mathbf{Q}}$  sur  $\mathbf{Q}$  à valeurs dans une extension finie de  $\mathbf{Q}_\ell$  comme provenant d'une façon bien précise de caractères associés naturellement aux corps cyclotomiques, alors que Wiles établit le théorème 2 comme corollaire d'un résultat disant que certaines classes au moins de représentations  $\ell$ -adiques de degré 2 de  $\text{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$  sont isomorphes aux représentations que l'on sait construire à partir des formes modulaires.

## 1 Caractères de Hecke algébriques de $\mathbf{Q}$

Nous commençons par définir et étudier les objets qui dans ce cas sont les analogues des formes modulaires ; ce sont donc des objets à l'apparence transcendante qui s'avèrent être dotés de propriétés arithmétiques importantes, en particulier on verra dans la section suivante comment leur associer des représentations de degré 1, c'est à dire des caractères, de  $\text{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ .

**Définition 1** Soit  $m \geq 1$ ,  $k \geq 1$  des entiers ; un caractère de Hecke de  $\mathbf{Q}$  de niveau  $m$  et de poids  $k$  (ou caractère de Hecke, pour abréger), est un homomorphisme

$$\chi : \mathbf{Q}^\times(m) \rightarrow \mathbf{C}^\times$$

(où  $\mathbf{Q}^\times(m)$  désigne le groupes des idéaux fractionnaires de  $\mathbf{Q}$  premiers avec  $m$ ) tel que si  $\alpha \in \mathbf{Z}$  vérifie  $\alpha \equiv 1$  (modulo  $m$ ), on a

$$\chi((\alpha)) = |\alpha|^k$$

N.B. (1) Le groupe d'idéaux fractionnaires considérés est en fait le groupe des rationnels correspondants modulo les unités de  $\mathbf{Z}$ , c'est à dire au signe près. De toute façon nous allons immédiatement abandonner cette définition un peu compliquée après avoir exhibé deux exemples qui seront les seuls envisagés par la suite (d'autant plus légitimement qu'en réalité ces exemples donnent tout les caractères de Hecke algébriques de  $\mathbf{Q}$ ).

(2) Une définition vraiment naturelle ferait intervenir les caractères des idèles de  $\mathbf{Q}$ , mais introduire la notion correspondante ne semble pas en valoir la peine, surtout au vu de la remarque précédente.

(3) Les caractères de Hecke forment un groupe par multiplication, et le poids est additif.

**Exemple 1.** Soit  $n \geq 1$  un entier, et considérons un caractère  $\chi$  de  $(\mathbf{Z}/n\mathbf{Z})^\times$  :

$$\chi : (\mathbf{Z}/n\mathbf{Z})^\times \rightarrow \mathbf{C}^\times$$

Alors ce caractère induit naturellement un caractère de Hecke, également noté  $\chi$ , de niveau  $n$  et de poids 0, définit par multiplicativité et par réduction modulo  $n$  pour les entiers, puisque par définition si  $\alpha \equiv 1$  (modulo  $n$ ), on a  $\chi(\alpha) = 1$ .

On appelle aussi ces caractères des caractères de Dirichlet modulo  $n$ .

**Exemple 2.** Considérons l'application  $N$  suivante :

$$N : \begin{cases} \mathbf{Q}^\times & \rightarrow \mathbf{C}^\times \\ x & \mapsto |x| \end{cases}$$

(la valeur absolue). Alors il est immédiat que  $N$  est un caractère de Hecke algébrique de niveau 1 et de poids 1. Par conséquent, pour tout  $k \in \mathbf{Z}$ ,  $N^k$  est un caractère de Hecke de niveau 1 et de poids  $k$ .

Les caractères de Hecke considérés dorénavant seront toujours de la forme

$$\chi = \chi_{Dir} N^k$$

où  $\chi_{Dir}$  est un caractère de Dirichlet modulo  $m$  et  $N$  est la valeur absolue. Notons au passage que  $\chi$  est alors de niveau  $m$  et de poids  $k$ . Ces caractères particuliers forment un sous-groupe du groupe des caractères de Hecke algébriques (qui est en fait le groupe entier, mais nous n'en aurons pas besoin.)

On voit que la définition des caractères de Hecke n'impose apparemment pas de condition d'algébricité sur les valeurs de  $\chi$  : c'est en ce sens qu'ils semblent transcendants. La proposition suivante est immédiate dans ce cas, mais le résultat correspondant pour les formes modulaires (il existe une base de l'espace des formes modulaires dont les coefficients de Fourier engendrent un corps de nombre) est plus profond.

**Proposition 1** *Soit  $\chi$  un caractère de Hecke algébrique, et notons  $L_\chi$  le corps engendré sur  $\mathbf{Q}$  par les valeurs de  $\chi$ , ie*

$$L_\chi = \mathbf{Q}(\chi(x) \mid x \in \mathbf{Q}^\times(m))$$

*Alors  $L/K$  est une extension de degré fini de  $\mathbf{Q}$ .*

**Preuve.** Le poids  $k$  étant entier, on voit que par définition les valeurs  $\chi(\alpha)$ , pour  $\alpha \equiv 1$  (modulo  $m$ ), engendrent un corps de nombre (même, sont rationnelles ici). Or il est immédiat que  $\mathbf{Q}^\times(m)/\{\alpha \mid \alpha \equiv 1 \pmod{m}\}$  est fini, et les caractères d'un groupe fini prennent valeurs parmi les racines de l'unité d'ordre au plus l'ordre du groupe.

◇

## 2 Représentations $\lambda$ -adiques associées aux caractères de Hecke

Nous allons voir ici comment associer aux caractères de Hecke algébriques des représentations dites  $\lambda$ -adiques

$$\rho_\chi : \text{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \rightarrow GL(1, \mathcal{O}_{L,\lambda})$$

où  $L$  est un corps de nombre et  $\lambda$  un idéal premier de  $\mathcal{O}_L$ , l'anneau des entiers de  $L$ .

Mais avant cela, définissons plus précisément ces objets et quelques notions associées, la principale étant celle de ramification d'une représentation en un nombre premier  $p$ .

### 2.1 Représentations $\lambda$ -adiques et ramification

**Définition 2** *Soit  $L/\mathbf{Q}_\ell$  une extension finie de  $\mathbf{Q}_\ell$ ,  $\mathcal{O}_L$  l'anneau des entiers de  $L$  et  $\lambda \subset \mathcal{O}_L$  l'idéal premier de  $\mathcal{O}_L$ . Une représentation  $\lambda$ -adique de degré 1 de  $\text{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$  est un homomorphisme continu*

$$\rho : \text{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \rightarrow GL(1, \mathcal{O}_L)$$

Étant donnée une telle représentation  $\rho$ , et un entier  $n \geq 0$ , on notera  $\overline{\rho}_n$  l'homomorphisme

$$\overline{\rho}_n : \text{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \rightarrow GL(1, \mathcal{O}_L/\lambda^n)$$

obtenu par composition de  $\rho$  avec la flèche canonique

$$\mathcal{O}_L \rightarrow \mathcal{O}_L/\lambda^n$$

En particulier, on notera généralement  $\bar{\rho} = \overline{\rho_0}$ , et on l'appellera la réduction modulo  $\lambda$  de  $\rho$ .

Pour étudier une telle représentation, on considère sa restriction à divers sous-groupes “mieux connus” de  $\text{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ , en particulier au sous-groupe de décomposition en un nombre premier  $p$ ,  $D_p$ , qui est naturellement isomorphe à  $\text{Gal}(\overline{\mathbf{Q}_p}/\mathbf{Q}_p)$ , et au sous-groupe d'inertie en  $p$ ,  $I_p$ , inclus dans ce dernier et correspondant par la correspondance de la théorie de Galois à l'extension non-ramifiée maximale de  $\mathbf{Q}_p$ . Cela amène à la définition suivante.

**Définition 3** *Soit  $\rho$  une représentation  $\lambda$ -adique de degré 1 (en fait, la définition s'applique au cas plus général d'une représentation de degré  $d$  quelconque), une représentation  $\bar{\rho}_n$  comme ci-dessus, et soit  $p$  un nombre premier.*

*On dit que  $\rho$  est non-ramifiée en  $p$  si le groupe d'inertie en  $p$ ,  $I_p \subset D_p \subset \text{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ , agit trivialement ie si  $\rho(i) = 1$  pour tout  $i \in I_p$ .*

Il est facile de donner une définition plus élémentaire ne s'appuyant que sur la notion d'extension de  $\mathbf{Q}$  non-ramifiée en  $p$ .

En effet, considérons le noyau de  $\rho$  : par la correspondance de Galois, il correspond à une extension  $K/\mathbf{Q}$  telle que

$$\overline{\mathbf{Q}}^{\text{Ker } \rho} = K$$

$K/\mathbf{Q}$  est une extension finie dans le cas de  $\bar{\rho}_n$ , sinon elle peut être infinie, comme on en verra plus loin un exemple. Mais de toute façon, soit  $K' \subset K$  une sous-extension finie. On a alors la

**Proposition 2**  *$\rho$  est non-ramifiée en  $p$  si et seulement si pour tout  $K'$  ainsi obtenu, l'extension  $K'/\mathbf{Q}$  est non-ramifiée en  $p$ .*

**Preuve.** Par définition même,  $\rho$  est non-ramifiée en  $p$  si et seulement si  $I_p$  agit trivialement, si et seulement si  $I_p \subset \text{Ker}(\rho)$ , si et seulement si  $\overline{\mathbf{Q}}^{\text{Ker } \rho} \subset \overline{\mathbf{Q}}^{I_p}$ , ce qui donne le résultat.

◇

L'avantage de cette formulation est que l'on a un critère maniable pour déterminer si un nombre premier  $p$  est ramifié dans une extension  $K/\mathbf{Q}$  de degré fini :  $p$  est ramifié si et seulement si  $p$  divise le discriminant de  $K$  sur  $\mathbf{Q}$ . Plus généralement, si l'on sait déterminer le corps fixe du noyau de  $\rho$ , et qu'on connaît les nombres premiers ramifiés dans celui-ci, cela donnera le résultat correspondant pour  $\rho$ .

Comme on le verra, cette information sur la ramification joue un rôle essentiel dans la dernière partie de la démonstration du théorème de Kronecker-Weber, cf. la fin de la section 3.

**Exemple.** On va illustrer cela avec le cas très important du caractère cyclotomique. Soit  $\ell$  un nombre premier,  $n \geq 0$  un entier et considérons le groupe des racines  $\ell^n$ -èmes de l'unité,  $\mu_{\ell^n} \subset \mathbf{C}^\times$ . Le groupe de Galois  $\text{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$  agit sur  $\mu_{\ell^n}$ , et cette action est compatible avec les homomorphismes canoniques  $\mu_{\ell^m} \rightarrow \mu_{\ell^n}$  existant pour  $n \mid m$  (définis par  $\mu \mapsto \mu^{m/n}$ ). Mais l'on a des isomorphismes

$$\mu_{\ell^n} \simeq (\mathbf{Z}/\ell^n \mathbf{Z})$$

de sorte qu'en prenant la limite projective on obtient une action de  $\text{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$  sur  $\mathbf{Z}_\ell$ , c'est à dire une flèche

$$\chi_\ell : \text{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \rightarrow GL(1, \mathbf{Z}_\ell)$$

appelée le  $\ell$ -ème caractère cyclotomique.

La propriété caractéristique de  $\chi_\ell$  est par construction

$$\sigma(\mu) = \mu^{\chi_\ell(\sigma)}$$

pour tout  $\sigma \in \text{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ , et  $\mu$  racine  $\ell^m$ -ème de l'unité.

Étudions la ramification de cette représentation  $\ell$ -adique. La formule précédente donne  $\sigma \in \text{Ker}(\chi_\ell)$  si et seulement si  $\sigma(\mu) = \mu$  pour  $\mu$  racine  $\ell^m$ -ème de l'unité, c'est à dire exactement

$$\text{Ker}(\chi_\ell) = \text{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}(\mu_{\ell^\infty}))$$

En particulier, la théorie des corps cyclotomiques montre alors que  $\chi_\ell$  n'est ramifiée qu'en  $\ell$ .

## 2.2 Représentations $\lambda$ -adiques associées aux caractères de Hecke

Revenons au problème d'associer des représentations  $\lambda$ -adique à un caractère de Hecke algébrique  $\chi$  de  $\mathbf{Q}$ . Nous verrons que pour tout nombre premier  $\ell$ , il existe une telle représentation à valeurs dans  $GL(1, \mathcal{O}_{L, \lambda})$ ,  $L$  étant une extension finie de  $\mathbf{Q}$  et  $\lambda \subset \mathcal{O}_L$  un idéal premier divisant  $\ell$ .

Comme dit précédemment, on ne considère ici que les caractères  $\chi$  de la forme  $\chi = \chi_{Dir} N^k$ ,  $\chi_{Dir}$  étant un caractère de Dirichlet modulo  $m$  et  $N$  le caractère "valeur absolue". Pour construire les représentations  $\rho_{\chi, \lambda}$  associées, nous utiliserons la formule naturelle  $\rho_\chi = \rho_{\chi_{Dir}} \rho_N^k$ , ce qui nous amène à distinguer les deux cas

- $\chi = \chi_{Dir}$  est un caractère de Dirichlet
- $\chi = N$  est le caractère valeur absolue

**Cas (1)** On a donc donné un caractère de Dirichlet

$$\chi : (\mathbf{Z}/m\mathbf{Z})^\times \rightarrow \mathbf{C}^\times$$

Mais  $\chi$  est en fait à valeurs dans le groupe des unités de l'anneau des entiers d'une extension finie  $L$  de  $\mathbf{Q}$  ( $L$  est un corps cyclotomique). Et d'autre part comme le groupe de Galois de  $\mathbf{Q}(\mu_m)$  sur  $\mathbf{Q}$  est isomorphe à  $(\mathbf{Z}/m\mathbf{Z})^\times$ , la théorie de Galois fournit une application

$$\pi_m : \text{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \rightarrow (\mathbf{Z}/m\mathbf{Z})^\times$$

Tout cela ensemble se place dans un diagramme

$$\text{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \xrightarrow{\pi_m} (\mathbf{Z}/m\mathbf{Z})^\times \xrightarrow{\chi} \mathcal{O}_L \xrightarrow{i_\lambda} \mathcal{O}_{L,\lambda}$$

pour tout idéal premier  $\lambda \subset \mathcal{O}_L$  au dessus de  $\ell$ . Par définition, on pose

$$\rho_{\chi,\lambda} = i_\lambda \circ \chi \circ \pi_m$$

. **Cas (2)** Pour tout  $\ell$ , on a construit en (2.1) le caractère cyclotomique  $\chi_\ell$  qui est une application

$$\chi_\ell : \text{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \rightarrow GL(1, \mathbf{Z}_\ell)$$

On pose alors par définition  $\rho_{N,\ell} = \chi_\ell$ .

Pour un caractère de Hecke  $\chi$  donné, la famille des représentations  $\rho_{\chi,\lambda}$  associées vérifie une propriété fondamentale de compatibilité, qui justifie en fait l'usage du terme "associées" pour ces représentations.

**Proposition 3** Soit  $\rho : \text{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \rightarrow GL(1, \mathcal{O}_{L,\lambda})$  une représentation  $\lambda$ -adique associée à  $\chi$ . Alors pour presque tout nombre premier  $p$  (ie pour tous sauf un nombre fini d'entre eux), si  $\text{Fr}_p$  est un élément de Frobenius en  $p$  ( $\text{Fr}_p \in D_p$ ), on a

$$\rho(\text{Fr}_p) = \chi(p)$$

**Preuve** Vérifions cela dans les deux cas ci-dessus, ce qui suffit.

**Cas (1)** La théorie des corps cyclotomiques montre que dans l'isomorphisme  $\text{Gal}(\mathbf{Q}(\mu_m)/\mathbf{Q}) \simeq (\mathbf{Z}/m\mathbf{Z})^\times$ , l'élément de Frobenius  $\text{Fr}_p$ , pour  $p \nmid m$ , est la classe de l'entier  $p$  ; la formule donnant  $\rho_\chi$  donne par conséquent  $\rho(\text{Fr}_p) = \chi(p)$  pour un tel nombre premier  $p$ .

**Cas (2)** Là encore, la théorie des corps cyclotomiques montre que pour  $p \neq \ell$ , on a  $\text{Fr}_p = q$  (considéré comme élément de  $\mathbf{Z}_\ell^\times$ ), de sorte que  $\rho(\text{Fr}_p) = p = N(p)$  pour  $p \neq \ell$ .

◇

On voit que ces représentations  $\rho$  sont étroitement liées aux corps cyclotomiques. Cela est encore mis en évidence lorsque l'on étudie la ramification de  $\rho_{\chi,\lambda}$ .

**Proposition 4** Soit  $\chi$  un caractère de Hecke algébrique,  $\rho_\chi$  la représentation  $\lambda$ -adique associée. Alors le corps  $\overline{\mathbf{Q}}^{\text{Ker}(\rho_\chi)}$  fixé par le noyau de  $\rho_\chi$  est une extension cyclotomique (éventuellement infinie) de  $\mathbf{Q}$ .

### 3 Le théorème de comparaison

On a donc construit des représentations  $\lambda$ -adiques de degré 1 de  $\text{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$  à partir de caractères de Hecke ; il est naturel de se demander si, réciproquement, toute représentation  $\lambda$ -adique  $\rho$  est de ce type. Il est trivialement nécessaire de demander que  $\rho$  ne soit ramifiée qu'en un nombre fini de nombres premiers, puisque c'est le cas des représentations  $\rho_\chi$ . Et le fait est que cette condition suffit.

**Théorème 3** *Soit  $\rho : \text{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \rightarrow GL(1, \mathcal{O}_{L,\lambda})$  une représentation de degré 1 de  $\text{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$  ramifiée en un nombre fini de nombres premiers. Alors il existe un caractère de Hecke algébrique  $\chi$  tel que*

$$\rho = \rho_\chi$$

Convenons d'appeler “modulaire” une représentation

$$\rho : \text{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \rightarrow GL(1, \mathcal{O}_{L,\lambda})$$

pour laquelle la conclusion du théorème est valide, ie  $\rho = \rho_\chi$ .

Ainsi que le fait Wiles, on démontre le théorème en prouvant d'abord un autre résultat dont le sens est que si l'on dispose *a priori* d'une représentation modulaire  $\rho_0$ , alors toute représentation  $\rho$  dont la réduction modulo  $\lambda$  vérifie

$$\overline{\rho} = \overline{\rho_0}$$

est également modulaire, ce qu'on énonce aussi sous la forme : toute déformation d'une représentation modulaire (de degré 1) est également modulaire. C'est exactement l'énoncé du théorème principal de Wiles, degré 2 remplaçant degré 1...

Plus précisément même, nous allons établir un résultat un peu plus fin dont le théorème est un corollaire immédiat :

**Théorème 4** *Soit  $n \geq 1$  un entier et  $\rho : \text{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \rightarrow GL(1, \mathcal{O}_{L,\lambda}/\lambda^n)$  une représentation de degré 1 de  $\text{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$  ramifiée en un nombre fini de nombres premiers. Alors il existe un caractère de Hecke algébrique  $\chi$  tel que*

$$\rho = \rho_\chi \bmod \lambda^n$$

Pour passer de ce théorème au théorème de comparaison, il suffit de passer à la limite projective.

Dans la suite de cette section, remettant la démonstration à plus tard, nous allons d'abord voir comment cela implique le théorème de Kronecker-Weber.

Soit donc  $K/\mathbf{Q}$  une extension abélienne finie de groupe de Galois  $G$ . En écrivant la décomposition de  $G$  comme produit direct de groupes cycliques d'ordre une puissance d'un nombre premier et en observant que le composé

de deux corps cyclotomiques est contenu dans un corps cyclotomique (plus exactement on a  $\mathbf{Q}(\mu_m).\mathbf{Q}(\mu_n) = \mathbf{Q}(\mu_{mn})$  si  $(m, n) = 1$ , mais cela n'est même pas nécessaire), on se ramène au cas où  $G \simeq (\mathbf{Z}/\ell^n\mathbf{Z})$  est cyclique d'ordre une puissance d'un nombre premier.

On a donc une extension  $K/\mathbf{Q}$  de groupe de Galois  $G$  et on procède à l'adjonction des racines  $\ell$ -èmes de l'unité, ce qui nous donne le diagramme suivant :

$$\begin{array}{ccc} K & \longrightarrow & K(\mu_\ell) \\ \uparrow & & \uparrow \\ \mathbf{Q} & \longrightarrow & \mathbf{Q}(\mu_\ell) \end{array}$$

Remarquons qu'il suffit de montrer maintenant que  $K(\mu_\ell)$  est contenu dans un corps cyclotomique, puisque  $K \subset K(\mu_\ell)$ .

Or  $\text{Gal}(\mathbf{Q}(\mu_\ell)/\mathbf{Q}) \simeq (\mathbf{Z}/\ell\mathbf{Z})^\times$ , qui est d'ordre premier à  $\ell$ , et il est facile d'en déduire que le groupe de Galois de  $K(\mu_\ell)/\mathbf{Q}$  est isomorphe à  $(\mathbf{Z}/\ell^{n+1}\mathbf{Z})^\times$  (on a recours ici à la suite exacte

$$1 \rightarrow (1 + \ell^n\mathbf{Z})/\ell^{n+1}\mathbf{Z} \rightarrow (\mathbf{Z}/\ell^{n+1}\mathbf{Z})^\times \rightarrow (\mathbf{Z}/\ell\mathbf{Z})^\times \rightarrow 1$$

qui est classique.)

Cela étant, par théorie de Galois, l'extension  $K(\mu_\ell)/\mathbf{Q}$  nous fournit donc gratis une flèche

$$\rho_n : \text{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \rightarrow (\mathbf{Z}/\ell^{n+1}\mathbf{Z})^\times$$

qui n'est évidemment ramifiée qu'en un nombre fini de nombres premiers puisque le corps fixé par le noyau est  $K(\mu_\ell)$  lui-même.

De plus, par construction même, on a  $\overline{\rho_n} = \overline{\rho_{\chi_\ell}}$ , la représentation associée au caractère cyclotomique, et l'on est en position d'appliquer le théorème 4 à  $\rho_n$ .

On a donc un caractère de Hecke algébrique  $\chi$  tel que

$$\rho_n = \rho_\chi \bmod \lambda^n$$

Mais alors on a  $K(\mu_\ell) = \overline{\mathbf{Q}}^{\text{Ker}\rho_n} \subset \overline{\mathbf{Q}}^{\text{Ker}\rho_\chi}$  et, d'après l'étude de la section 2, ce dernier corps est inclus dans une extension cyclotomique (proposition 4).

Celle-ci est éventuellement de degré infini, mais on peut alors écrire une famille de générateurs de  $K(\mu_\ell)$  comme combinaison linéaire d'un nombre fini de racines de l'unité, et  $K(\mu_\ell)$  est inclus dans l'extension cyclotomique finie engendrée par celles-ci.

◇

## 4 Déformations de représentations $\lambda$ -adiques de degré 1

Nous commençons donc la preuve du théorème 4, suivant toujours les méthodes de Wiles, qui est basée sur l'étude des déformations de représentations galoisiennes.



Un foncteur est requis pour cela. Considérons donc,  $k$  étant un corps fini donné de caractéristique  $p$  et  $A$  un anneau local noethérien de corps résiduel  $k$ , la catégorie  $\mathcal{A}_A$  des  $A$ -algèbres locales artiniennes de corps résiduel  $k$ , les morphismes étant les morphismes induisant l'identité sur  $k$ , ie les flèches  $B \rightarrow C$  telles que le carré

$$\begin{array}{ccc} B & \rightarrow & C \\ \downarrow & & \downarrow \\ k & = & k \end{array}$$

commute.