

REPRÉSENTATIONS GALOISIENNES PAIRES

par M.-F. VIGNÉRAS

En honneur de Robert Rankin à l'occasion de son soixante-dixième anniversaire.

On présente des exemples de représentations de $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ de dimension 2, de déterminant pair, qui sont de type diédral (I) ou de conducteur premier et de type quelconque (II), en imitant la construction de Tate (Serre [11]) de représentations de déterminant impair.

On remarquera qu'une des applications est la construction explicite de formes modulaires non holomorphes, correspondant à la valeur propre $\lambda = 1/4$ du Laplacien. En effet, si l'image de la représentation dans $\text{PGL}(2, \mathbb{C})$ n'est pas isomorphe au groupe alterné A_5 , la fonction L d'Artin de la représentation est une fonction entière et sa transformée de Mellin (en un sens convenable) est une forme modulaire de poids 1, si le déterminant est impair, et une forme modulaire non holomorphe avec $\lambda = 1/4$, si le déterminant est pair.

Un théorème de Deligne–Serre affirme que l'on obtient ainsi une bijection entre un ensemble de formes modulaires de poids 1, et un ensemble de représentations galoisiennes de déterminant pair, satisfaisant la conjecture d'Artin. Un résultat analogue pour les formes modulaires non holomorphes, avec $\lambda = 1/4$, semble encore hors d'atteinte.

1. Représentations diédrales paires. On les obtient ainsi (Serre [11], §7, p. 237): on part d'un corps quadratique K/\mathbb{Q} , correspondant à un caractère ω du groupe de Galois $G_{\mathbb{Q}}$ de $\bar{\mathbb{Q}}/\mathbb{Q}$, et d'une représentation χ de dimension 1 de G_K . Si σ engendre $\text{Gal}(K/\mathbb{Q})$ soit

$$\chi_{\sigma}(\gamma) = \chi(\sigma\gamma\sigma^{-1}), \quad \gamma \in G_K.$$

Soient f le conducteur de χ et d le discriminant de K . Soit $\rho = \text{Ind}_{K/\mathbb{Q}}(\chi)$ et $\tilde{\rho}$ la représentation projective associée. Alors:

- 1) ρ est diédrale (ou irréductible) si et seulement si $\chi \neq \chi_{\sigma}$
- 2) le conducteur N de ρ est $|d| \cdot N_{K/\mathbb{Q}}(f)$
- 3) ρ est paire, ρ est dite paire si son déterminant est pair, si et seulement si K est réel, et χ prend la même valeur $\varepsilon = \pm 1$ sur les deux Frobenius à l'infini. Si $c \in G_{\mathbb{Q}}$ est la conjugaison complexe, on a $\rho(c) = \varepsilon \text{id}$.
- 4) $\det(\rho) = \omega\chi_{\mathbb{Q}}$, où en termes d'idèles, $\chi_{\mathbb{Q}}$ est la restriction de χ aux classes d'idèles de \mathbb{Q} .
- 5) Si ρ est diédrale, $\tilde{\rho}(G_{\mathbb{Q}}) = D_n$, où n est l'ordre de $\chi^{-1}\chi_{\sigma}$, et D_n est le groupe diédral d'ordre $2n$.

1.1. *Représentations diédrales paires de conducteur premier p , $p < 2000$.* On déduit de ci-dessus:

- 1) $p \equiv 1 \pmod{4}$
- 2) le nombre de classes h de $K = \mathbb{Q}(\sqrt{p})$ est impair, différent de 1

Glasgow Math. J. **27** (1985) 223–237.

3) $\varepsilon = 1$ (par la théorie du genre)

4) $\det(\rho)$ comme caractère de Dirichlet est le symbole de Legendre $n \rightarrow \left(\frac{n}{p}\right)$

5) χ est un caractère non ramifié de K , $\chi^2 \neq 1$ (la norme d'un idéal de K étant principale, $\chi\chi^\sigma = 1$)

6) il y a $(h-1)/2$ représentations diédrales irréductibles paires non équivalentes de conducteur p .

On les obtient en utilisant les tables numériques de Borevich–Chafarevich ([2]):

Il y a 143 nombres premiers p , $p \equiv 1 \pmod{4}$, $p < 2000$.

Le nombre de classes h est égal à 3 pour les 8 nombres

229, 257, 733, 761, 1229, 1373, 1489, 1901.

Le nombre de classes h est égal à 5 pour les 3 nombres

401, 1093, 1429.

Le nombre de classes h est égal à 7 pour les 3 nombres

577, 1009, 1601.

On a $h = 9$ pour $p = 1129$, et $h = 11$ pour $p = 1297$.

Pour les 127 premiers restants, on a $h = 1$.

Donc, le nombre n de représentations diédrales non isomorphes de conducteur premier $p < 2000$ est égal à:

n	p
1	229, 257, 733, 761, 1229, 1373, 1489, 1901
2	401, 1093, 1429
3	577, 1009, 1601
4	1129
5	1297

Il est égal à 0 pour les autres valeurs de p , $p < 2000$.

A conjugaison près, $GL(2, \mathbb{C})$ contient un seul sous-groupe H_n isomorphe au groupe diédral D_n : si ξ est une racine primitive d'ordre n de l'unité,

$$H_n = \left\{ \begin{pmatrix} \xi^a & \\ & \xi^{-a} \end{pmatrix}, \begin{pmatrix} & \xi^a \\ \xi^{-a} & \end{pmatrix}, 0 \leq a < n \right\}, \text{ si } n \neq 2.$$

$$H_2 = \left\{ \begin{pmatrix} \mp 1 & \\ & \mp 1 \end{pmatrix} \right\}.$$

Si n est impair, $\tilde{H}_n \simeq H_n \simeq D_n$, et si n est pair, $\tilde{H}_n \simeq H_n/\{\mp 1\} \simeq D_{n/2}$. A conjugaison près, il y a $\varphi(n)$ plongements de $D_n = \langle x, y \rangle$, $x^n = 1$, $y^2 = 1$, $xy = yx^{-1}$ dans $GL(2, \mathbb{C})$ si n est impair.

Les 32 représentations diédrales paires de conducteur $p < 2000$ premier s'obtiennent

aussi de la façon suivante: soit E l'extension abélienne maximale non ramifiée de K ; elle est galoisienne sur \mathbb{Q} , de groupe de Galois $G_{E/\mathbb{Q}}$ isomorphe à D_h . Si $h \neq 1$, les représentations ρ de conducteur p s'obtiennent en composant la surjection canonique de $G_{\mathbb{Q}}$ sur $G_{E/\mathbb{Q}}$ avec les $(h - 1)/2$ plongements de D_h dans $GL(2, \mathbb{C})$. Quand $h = 3$, E est la clôture galoisienne d'un corps cubique non abélien totalement réel. Les tables numériques de Delone–Faddeev ([6]) donnent l'équation correspondante pour $p \leq 1229$. Les équations pour $p = 1373, 1489, 1901$ m'ont été communiquées par J. Martinet.

conducteur	équation
229	$x^3 - 4x - 1$
257	$x^3 - x^2 - 4x + 3$
733	$x^3 - x^2 - 7x + 8$
761	$x^3 - x^2 - 6x - 1$
1229	$x^3 - x^2 - 7x - 3$
1373	$x^3 - 8x + 5$
1489	$x^3 - 8x^2 + 9x - 1$
1901	$x^3 + x^2 - 9x + 4$

1.2. Représentations diédrales paires de conducteur $N \leq 200$. La représentation ρ détermine le couple (d, f) où $f = N_{K/\mathbb{Q}}(\mathfrak{f})$. On voit comme en 1:

1) Il y a $(h - h_2)/2$ représentations diédrales paires non isomorphes avec $N = d, f = 1, \xi = 1$, où h_2 est le nombre de classes d'idéaux de K annulées par 2.

2) Il y a $(h^+ - h_2^+)/2 - (h - h_2)/2$ représentations diédrales paires non isomorphes avec $N = d, f = 1, \varepsilon = -1$, où h^+ est le nombre de classes d'idéaux au sens restreint de K et h_2^+ le nombre de ces classes qui sont annulées par 2.

Il y a 60 discriminants $d \leq 200$ de corps quadratiques réels. Les tables ([2]) montrent que

$$\begin{aligned}
 h &= \begin{cases} 1 & \text{pour } 46 \text{ discriminants} \\ 2 & \text{pour } 13 \text{ discriminants} \\ 4 & \text{pour } d = 145 \end{cases} \\
 h^+ &= \begin{cases} 1 & \text{pour } 22 \text{ discriminants} \\ 2 & \text{pour } 29 \text{ discriminants} \\ 4 & \text{pour } d = 60, 105, 120, 136, 140, 145, 156, 165, 168. \end{cases}
 \end{aligned}$$

La théorie du genre ([2]) montre $h_2^+ = 2^{t-1}$ où t est le nombre de diviseurs premiers distincts de d . On en déduit que pour les nombres

$$136, 145$$

le groupe des classes au sens restreint est isomorphe à $\mathbb{Z}/4\mathbb{Z}$.

Le corps de classes associé est une extension galoisienne non abélienne E_d/\mathbb{Q} de degré 8 (car $\chi \neq \chi^\sigma$). Elle contient un corps biquadratique totalement réel L_d (correspondant à la factorisation de d en produit de deux discriminants $L_{136} = \mathbb{Q}(\sqrt{2}, \sqrt{17}), L_{145} = \mathbb{Q}(\sqrt{5}, \sqrt{29})$).

Il y a deux groupes non abéliens d'ordre 8:

- le groupe diédral D_4 ayant 3 sous-groupes distingués d'ordre 4, 5 sous-groupes d'ordre 2 (dont 2 distingués), 1 sous-groupe d'ordre 1,
- le groupe quaternionien $H_8 = \langle i, j \rangle$, $i^4 = 1$, $ij = ji^3$, $i^2 = j^2$, ayant 3 sous-groupes distingués d'ordre 4, 1 sous-groupe distingué d'ordre 2, sous-groupe d'ordre 1. Il se plonge par un isomorphisme unique à conjugaison près dans $GL(2, \mathbb{C})$ via les matrices de Pauli:

$$i \rightarrow I = \begin{pmatrix} i & \\ & -i \end{pmatrix}, \quad j \rightarrow J = \begin{pmatrix} & -1 \\ 1 & \end{pmatrix}.$$

Son image dans $PGL(2, \mathbb{C})$ est le groupe diédral D_2 .

On en déduit que $\text{Gal}(E_d/\mathbb{Q})$ est isomorphe à H_8 . Nous avons obtenu:

Il existe deux représentations diédrales paires non isomorphes avec $N = d \leq 200$, $f = 1$. Pour l'une $N = 136$, $\varepsilon = -1$, pour l'autre $N = 145$, $\varepsilon = 1$. On les obtient en composant la surjection canonique de $G_{\mathbb{Q}}$ sur $\text{Gal}(E_d/\mathbb{Q})$ avec le plongement de H_8 dans $GL(2, \mathbb{C})$.

Si $f \neq 1$, on se propose de montrer:

Il existe une unique représentation diédrale paire, à isomorphisme près, avec $N \leq 200$, $f \neq 1$. Si E/\mathbb{Q} est l'extension galoisienne de groupe de Galois S_3 engendrée par les racines du polynôme $x^3 - x^2 - 3x + 1$, la représentation s'obtient en composant la surjection canonique de $G_{\mathbb{Q}}$ sur $\text{Gal}(E/\mathbb{Q})$ avec le plongement unique à conjugaison près de S_3 dans $GL(2, \mathbb{C})$.

Preuve. On fait les observations suivantes

- 1) χ n'est pas d'ordre 2, si ρ est diédrale,
- 2) χ vu comme caractère d'idéaux, χ est trivial sur le groupe des idéaux principaux engendrés par un élément de $K_{\mathfrak{f}}^+ = \{a \in K^+, a \equiv 1 \pmod{\mathfrak{f}}, N_{K/\mathbb{Q}}(a) > 0\}$.
- 3) l'ordre $h_{\mathfrak{f}}^+$ du groupe des classes $C_{\mathfrak{f}}^+$ associé est donné par la formule:

$$H_{\mathfrak{f}}^+ = h_{\mathfrak{f}}^2 / [U_{\mathfrak{f}} : U_{\mathfrak{f}}^+], \quad h_{\mathfrak{f}} = h\varphi(\mathfrak{f}) / [U : U_{\mathfrak{f}}]$$

où U est le groupe des unités de K , $U_{\mathfrak{f}}^+$ le sous-groupe des unités de K appartenant à $K_{\mathfrak{f}}^+$, et $U_{\mathfrak{f}}$ celles congrues à 1 modulo \mathfrak{f} . On rappelle que

$$\varphi(\mathfrak{f}) = \prod N_{K/\mathbb{Q}}(P)^{m(P)-1} (N_{K/\mathbb{Q}}(P) - 1) \quad \text{si} \quad \mathfrak{f} = \prod P^{m(P)}$$

4) soit X un caractère de $C_{\mathfrak{f}}^+$, identifié au groupe de Galois du corps de classes $K_{\mathfrak{f}}^+/K$ associé; si $h_{\mathfrak{f}}^+ = h_{\mathfrak{f}}^+$, alors X prend la valeur +1 sur les deux Frobenius à l'infini; si $h_{\mathfrak{f}}^+ = h_{\mathfrak{f}}^+$ avec $\mathfrak{f}' \mid \mathfrak{f}$, alors le conducteur de X divise \mathfrak{f}' .

5) si $\mathfrak{f} = \mathfrak{f}^{\sigma}$, $K_{\mathfrak{f}}^+/\mathbb{Q}$ est galoisien, et il existe X tel que $x \neq X^{\sigma}$, si et seulement si $K_{\mathfrak{f}}^+/\mathbb{Q}$ n'est pas abélien.

6) si $f = f^{\sigma}$, et si $F \geq 1$ engendre $\mathfrak{f} \cap \mathbb{Z}$, alors $K_{\mathfrak{f}}^+ \supset \mathbb{Q}(\sqrt[F]{1})$ (si $A = (a) \ a \in K_{\mathfrak{f}}^+$, alors $N_{K/\mathbb{Q}}(A) = aa^{\sigma}$, $a, a^{\sigma} \in 1 + \mathfrak{f}$, et $aa^{\sigma} \in (1 + \mathfrak{f}) \cap \mathbb{Z} = 1 + F$).

On dresse alors la liste des 84 valeurs de (d, f) , avec $N = df \leq 200$. On [calcule $h_{\mathfrak{f}}$ et $h_{\mathfrak{f}}^+$ pour les idéaux \mathfrak{f} de norme f .

d	f	$h_{\mathbf{f}}$	$h_{\mathbf{f}}^+$	d	f	$h_{\mathbf{f}}$	$h_{\mathbf{f}}^+$
5	5	1	2	28	2 . 3	1	2
	5 ²	1	2		5*	1	2
	2 ²	1	1	29	2	1	2
	2 ⁴	1	2		2 ²	1	2
	3 ²	1	2		7	3	6
	2 ² 3 ²	1	2		3*	1	2
	2 ² 5	1	2	33	2 ²	1	1
	11*	1	1		5	2	2
	19*	1	1	37	2*	1	2
	29*	2	2		2 ²	1	2
31*	1	1	*		1	2	
8	2	1	1		3	1	2
	2 ²	1	2		2 . 3*	1	2
	2 ³	1	2	30	2 ²	3	3
	2 ⁴	1	2		3*	2	2
	3 ²	1	2	41	2	2	2
	5 ²	2	4		2 ²	2	4
	2 . 3 ²	1	2		5	2	4
	7*	1	1		3*	1	1
	17*	1	2		44	2	1
	23*	1	1	2 ²		1	2
12	2	1	2	57	3	1	2
	2 ²	1	2		2*	1	2
	2 ³	1	2	60	2	2	4
	2 ⁴	2	4		3	2	4
	3	1	2	61	3*	1	1
	3 ²	1	2		65	2*	2
	2 . 3	1	2	73		2*	1
	2 ² . 3	1	2		76	2	1
	11*	1	2	88		2	1
	13*	1	2		89	2*	1
13	2 ²	1	1	92		2	1
	3*	1	1		97	2*	1
	3 ² *	1	1				
		1	2				
17	2*	1	1				
	2 ²	1	1				
	*	2	2				
	3 ²	1	2				
21	2 ²	1	2				
	3	1	2				
	3 ²	1	2				
	7	3	6				
	5*	1	2				
24	2	1	2				
	2 ²	2	4				
	2 ³	2	4				
	3	1	2				

Dans le tableau ci-dessus, * signifie que $f \neq f^\sigma$. Utilisant 1) on ne retient que les 11 valeurs de (d, f) où $h_f > 2$. On calcule K_f^+ dans chaque cas.

d	f	h_f	h_f^+	K_f^+
8	5^2	2	4	$\mathbb{Q}(\sqrt{2}, \sqrt[3]{1})$
12	2^4	2	4	$\mathbb{Q}(\sqrt{3}, \sqrt{-1})$
21	7	3	6	$\mathbb{Q}(\sqrt{21}, \sqrt[3]{1})$
24	2^2	2	4	$\mathbb{Q}(\sqrt{6}, \sqrt{-1}, \sqrt{-2})$
	2^3	2	4	$\mathbb{Q}(\sqrt{6}, \sqrt{-1}, \sqrt{-2})$
28	7	3	6	$\mathbb{Q}(\sqrt{-1}, \sqrt[3]{1})$
37	2^2	3	3	corps engendré par les racines du polynôme $x^3 - x^2 - 3x + 1$, de groupe de Galois sur \mathbb{Q} égal à D_3
40	2^2	2	4	$\mathbb{Q}(\sqrt{10}, \sqrt{2}, \sqrt{-1})$
	5	2	4	$\mathbb{Q}(\sqrt{10}, \sqrt[3]{1})$
60	2	2	4	$K^+ = \mathbb{Q}(\sqrt{15}, \sqrt{5}, \sqrt{-3})$
	3	2	4	$K^+ = \mathbb{Q}(\sqrt{15}, \sqrt{5}, \sqrt{-3})$

Tous les corps K_f^+ sont abéliens sauf celui correspondant à $N = 148$.

1.3. *Représentations diédrales paires associées à un corps cubique non abélien totalement réel.* Un corps cubique non abélien totalement réel L/\mathbb{Q} produit une représentation diédrale ρ avec les propriétés suivantes:

1) si E est la clôture galoisienne de L , alors $\text{Gal}(E/\mathbb{Q})$ est isomorphe à D_3 et ρ est le composé de la surjection naturelle de $G_{\mathbb{Q}}$ sur $\text{Gal}(E/\mathbb{Q})$ et du plongement, unique à conjugaison près, de D_3 dans $\text{GL}(2, \mathbb{C})$.

2) soit D le discriminant de L/\mathbb{Q} , et $K = \mathbb{Q}(\sqrt{D})$ de discriminant d . Alors $E = KL$, et $\rho = \text{Ind}_{G_K}^{G_{\mathbb{Q}}}(\chi)$, où χ est le composé de la surjection canonique de G_K sur $\text{Gal}(E/K)$ et d'un caractère non trivial de $\text{Gal}(E/K)$.

3) $\varepsilon = 1$.

4) $N = df$, où l'idéal $(f)_K$ engendré par f dans K est égal au discriminant $\Delta_{E/K}$ de E/K .

5) Soit $N = \prod p^{n(p)}$ et $D = \prod p^{m(p)}$; on a

$m(p) = n(p)$ si $p \neq 2$ ou 3,

$m(3) = n(3)$ si et seulement si $m(3) \leq 3$ (par [6] p. 217, $m(3) \leq 5$),

$m(2) = n(2)$ si et seulement si 2 n'est pas totalement ramifié dans L quand on a simultanément $m(2) = 2$ et $2 \mid d$ (par [6], $m(2) = 2$ ou 3).

6) En général N est donné par la formule:

$$N = d \prod p^{m(p)} \prod q^{m(q)-1}$$

où p parcourt les premiers totalement ramifiés dans L , non ramifiés dans K et q ceux totalement ramifiés dans L et dans K .

Preuve. Vérifions la formule, le reste se déduit de ce qui précède. On a les relations

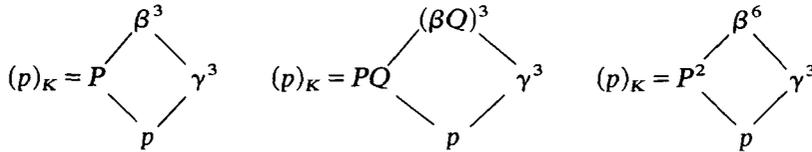
de transitivité entre différentes et discriminants:

$$\mathcal{D}_{E/Q} = \mathcal{D}_{E/K} \mathcal{D}_{K/Q} = \mathcal{D}_{E/L} \mathcal{D}_{L/Q}, \quad \Delta_{E/Q} = (\Delta_{E/K})^2 d^3.$$

Si p premier ne se ramifie pas dans L , il ne divise pas $\Delta_{E/K}$.

Si $(p)_L = \gamma^2 Q$, est la décomposition en idéaux premiers de l'idéal engendré par p dans L , alors p ne divise pas $\Delta_{E/K}$.

Supposons donc $(p)_L = \gamma^3$. Alors:



Si $p \neq 3$, la ramification de E/K en $\beta | p$ est modérée et l'exposant de β dans $\mathcal{D}_{E/K}$ est égal à 2.

Si $p = 3$, et si $m(3) \geq 3$, l'exposant de $\beta | 3$ dans $\mathcal{D}_{E/K}$ est égal à $m(p)$ si $p \nmid d$, et $2(m(p) - 1)$ si $p | d$. Prenant la norme sur K , on obtient la formule.

Pour les 28 corps cubiques non abéliens totalement réels donnés par les tables ([6]), on a $N = D$.

Discriminant	Equation	d	f	N
148 = 2 ² . 37	$x^3 - x^2 - 3x + 1$	37	2 ²	148
229	$x^3 - 4x - 1$	229	1	229
257	$x^3 - x^2 - 4x + 3$	257	1	257
316 = 2 ² . 79	$x^3 - x^2 - 4x + 2$	2 ² . 79	1	316
321 = 3 . 107	$x^3 - x^2 - 4x + 1$	3 . 107	1	321
404 = 2 ² . 101	$x^3 - x^2 - 5x - 1$	101	2 ²	404
469 = 7 . 67	$x^3 - x^2 - 5x + 4$	7 . 67	1	469
473 = 11 . 43	$x^3 - 5x - 1$	11 . 43	1	473
564 = 2 ² . 3 . 47	$x^3 - x^2 - 5x + 3$	3 . 47	2 ²	564
568 = 2 ³ . 71	$x^3 - x^2 - 6x - 2$	2 ³ . 71	1	568
621 = 3 ³ . 23	$x^3 - 6x - 3$	3 . 23	3 ²	621
697 = 17 . 41	$x^3 - 7x - 5$	17 . 41	1	697
733	$x^3 - x^2 - 7x + 8$	733	1	733
756 = 2 ² . 3 ³ . 7	$x^3 - 6x - 2$	3 . 7	2 ² . 3 ²	756
761	$x^3 - x^2 - 6x - 1$	761	1	761
785 = 5 . 157	$x^3 - x^2 - 6x + 5$	5 . 157	1	785
788 = 2 ² . 197	$x^3 - x^2 - 7x - 3$	197	2 ²	488
837 = 3 ³ . 31	$x^3 - 6x - 1$	3 . 31	3 ²	837
892 = 2 ² . 223	$x^3 - x^2 - 8x + 10$	2 ² . 223	1	892
940 = 2 ² . 5 . 47	$x^3 - 7x - 4$	2 ² . 5 . 47	1	940
985 = 5 . 197	$x^3 - x^2 - 6x + 1$	5 . 197	1	985
993 = 3 . 331	$x^3 - x^2 - 6x + 3$	3 . 331	1	993
1016 = 2 ³ . 127	$x^3 - x^2 - 6x + 2$	2 ³ . 127	1	1016
1076 = 2 ² . 269	$x^3 - 8x - 6$	269	2 ²	1076
1101 = 3 . 367	$x^3 - x^2 - 9x + 12$	3 . 367	1	1101
1129	$x^3 - 7x - 3$	1129	1	1129
1229	$x^3 - x^2 - 7x + 6$	1229	1	1229
1257 = 3 . 419	$x^3 - x^2 - 8x + 9$	3 . 419	1	1257

2. Représentations de conducteur premier paires. Soit $\rho: G_{\mathbb{Q}} \rightarrow GL(V)$ une représentation de $G_{\mathbb{Q}}$ dans un espace vectoriel complexe V de dimension 2, de conducteur un nombre premier p . Alors $\det \rho$ est une représentation de $G_{\mathbb{Q}}$ de dimension 1, non triviale, de conducteur premier p . En effet, la formule du conducteur (Martinet [10], p. 22)

$$\sum_{i \geq 0} g_i / g_0 \operatorname{codim} V^{G_i} = 1$$

où g_i est l'ordre du i -ème groupe de ramification G_i de $\operatorname{Gal}(\operatorname{Ker} \rho / \mathbb{Q})$ en un idéal $P \mid p$, donne $G_i = \{1\}$ pour $i \geq 1$, et $\operatorname{codim} V^{G_0} = 1$. Si $I_p \subset G_{\mathbb{Q}}$ est le groupe d'inertie en une place de $\bar{\mathbb{Q}}$ sur p , on a:

$$\rho|_{I_p} = 1 \oplus \psi, \quad \det \rho|_{I_p} = \psi$$

où ψ est une représentation de dimension 1, non triviale de I_p . Si q est un premier, $q \neq p$, alors ρ (restreint à I_q est trivial. On a $p \neq 2$.

Si ρ est réductible, alors $\rho = 1 \oplus \chi$ où χ est une représentation de dimension 1 de $G_{\mathbb{Q}}$, de conducteur p . Le nombre de représentations réductibles de dimension 2, de conducteur premier $p \neq 2$ est égal à $p-1$. Il y en a $(p-1)/2$ avec $\det \rho$ pair.

Il existe $(h-1)/2$ représentations irréductibles non isomorphes ρ de dimension 2 de $G_{\mathbb{Q}}$, de conducteur premier $p \neq 2$, telles que $\tilde{\rho}(G_{\mathbb{Q}})$ soit un groupe diédral;

1) si $p \equiv 1 \pmod{4}$, $\det \rho$ est pair, h est le nombre de classes de $\mathbb{Q}(\sqrt{p})$ (I)

2) si $p \equiv 3 \pmod{4}$, $\det \rho$ est impair, h est le nombre de classes de $\mathbb{Q}(\sqrt{-p})$ ([11]) Le

caractère $\det \rho$ est le symbole de Legendre $n \rightarrow \left(\frac{n}{p}\right)$.

On suppose désormais ρ irréductible, non diédrale, alors $\det \rho(G_{\mathbb{Q}})$ est un sous-groupe fini de $\operatorname{PGL}(2, \mathbb{C})$ isomorphe à A_4 , S_4 , ou A_5 . On suppose aussi que $\det \rho$ est pair. Serre a traité le cas où $\det \rho$ est impair. Ses méthodes s'étendent bien. Les isomorphismes canoniques:

$$\det \rho(G_{\mathbb{Q}}) = \det \rho(I_p) = \rho(I_p) = \tilde{\rho}(I_p)$$

montre que $\det \rho(G_{\mathbb{Q}})$ est un sous-groupe cyclique de A_4 , S_4 ou A_5 , non trivial, donc d'ordre 2, 3, 4 ou 5. Comme $\det \rho$ est pair, on peut le voir comme un caractère de $(\mathbb{Z}/p\mathbb{Z})^{\times}$ trivial sur l'image de -1 .

1) si $\det \rho$ est d'ordre 2, alors $\det \rho$ est le symbole de Legendre $n \rightarrow \left(\frac{n}{p}\right)$, $p \equiv 1 \pmod{4}$,

et ρ est de type S_4 ou A_5

2) si $\det \rho$ est d'ordre 3, alors $p \equiv 1 \pmod{3}$, et ρ est de type A_4 ou A_5

3) si $\det \rho$ est d'ordre 4, alors $p \equiv 1 \pmod{8}$, et ρ est de type S_4

4) si $\det \rho$ est d'ordre 5, alors $p \equiv 1 \pmod{5}$, et ρ est de type A_5

En effet, comme A_4 et A_5 n'ont pas d'éléments d'ordre 4, comme A_4 et S_4 n'ont pas d'éléments d'ordre 5, on a 3) et 4). Si $\det \rho$ était d'ordre 3, et ρ de type S_4 , l'application composée:

$$I_p \rightarrow S_4 \rightarrow S_4/A_4$$

serait triviale, et le noyau de la composition de $G_{\mathbb{Q}} \rightarrow S_4 \rightarrow S_4/A_4$ correspondrait à un corps quadratique partout non ramifié, ce qui est impossible. On démontre de même ([11]) que $\det \rho$ d'ordre 2, et ρ de type A_4 est impossible (utiliser la surjection $A_4 \rightarrow \mathbb{Z}/3\mathbb{Z}$). On déduit aussi:

5) si $p \equiv 23, 47$ ou $59 \pmod{60}$, il n'existe pas de représentations irréductible non diédrales de dimension 2 de $G_{\mathbb{Q}}$ de conducteur p .

Inversement, soit p un nombre premier, et E/\mathbb{Q} une extension galoisienne. On considère les cas suivants:

$$\text{Gal}(E/\mathbb{Q}) = A_4 \text{ et } p \equiv 1 \pmod{3} \tag{1}$$

$$\text{Gal}(E/\mathbb{Q}) = S_4 \text{ et } p \equiv 5 \pmod{8} \tag{2_a}$$

$$\text{Gal}(E/\mathbb{Q}) = S_4 \text{ et } p \equiv 1 \pmod{8} \tag{2_b}$$

$$\text{Gal}(E/\mathbb{Q}) = A_5 \text{ et } a(p \equiv 1 \pmod{5}), \quad b(p \equiv 1 \pmod{3}), \quad c(p \equiv 1 \pmod{4}) \tag{3_{a,b,c}}$$

où $a, b, c \in \{0, 1\}$ et $0(A) = \text{non } A, 1(A) = A$.

Soit $\bar{\rho}_E$ le composé de la surjection canonique de $G_{\mathbb{Q}}$ dans $\text{Gal}(E/\mathbb{Q})$ et d'un plongement de $\text{Gal}(E/\mathbb{Q})$ dans $\text{PGL}(2, \mathbb{C})$.

THÉOREME. $\bar{\rho}_E$ admet un relèvement $\rho_E : G_{\mathbb{Q}} \rightarrow \text{GL}(2, \mathbb{C})$ de conducteur p , avec $\det \rho_E$ pair si et seulement si:

(1) E est la clôture galoisienne d'un corps quartique totalement réel E_4 de discriminant p^2 .

(2_a) E est la clôture galoisienne d'un corps quartique totalement réel E_4 de discriminant p .

(2_b) E est la clôture galoisienne d'un corps quartique totalement réel E_4 de discriminant p ou p^3 .

(3_{a,b,c}) E est la clôture galoisienne d'un corps quintique totalement réel E_5 de discriminant $a(p^4)$ ou $b(p^2)$ et la décomposition en idéaux premiers de l'idéal engendré par p dans E_5 est du type P^3Q ou P^3QR ou $c(p^2)$ et la décomposition de l'idéal engendré par p dans E_5 n'est pas du type précédent).

Preuve. La condition E totalement réel est équivalente à $\det \rho$ pair, pour un (= pour tout) relèvement ρ de $\bar{\rho}_E$. Les conditions sur le discriminant et sur la ramification de p sont nécessaires d'après les conditions 1) à 4) vues précédemment. En effet, si G_0 est groupe d'inertie de p dans $\text{Gal}(E/\mathbb{Q})$, elles sont équivalentes à:

(1) G_0 est cyclique d'ordre 3 (comme $p \equiv 1 \pmod{3}$, E/\mathbb{Q} est modérément ramifié en p , et G_0 est un groupe cyclique d'ordre 2, 3 ou 6. Comme $G_0 \subset A_4$, 6 est impossible; il n'est pas d'ordre 2, sinon l'extension cubique cyclique L/\mathbb{Q} contenue dans E serait partout non ramifiée, ce qui est impossible).

(2_a) G_0 est cyclique d'ordre 2 ($p \equiv 5 \pmod{8}$ montre que E/\mathbb{Q} est modérément ramifiée, et G_0 est un groupe cyclique d'ordre 2 ou 6. Comme $G_0 \subset S_4$, 6 n'est pas possible).

(2_b) G_0 est cyclique d'ordre 2 ou 4 (si le discriminant est p^3 , G_0 est un groupe cyclique d'ordre $4d$, $d \mid 6$. Etant contenu dans S_4 , il est d'ordre 4).

(3_{a,b,c}) G_0 est cyclique d'ordre $a(5)$ ou $b(3)$ ou $c(2)$ (si le discriminant est p^4 , et $p \equiv 1 \pmod{5}$, G_0 est un groupe cyclique d'ordre $5d$, $d \mid 12$. Comme $G_0 \subset A_5$, G_0 est

d'ordre 5; si le discriminant est p^2 , et $p \equiv 1 \pmod{4}$ ou $\pmod{3}$, alors G_0 est un groupe cyclique d'ordre $2d$, $d \mid 6$ ou $3d$, $d \mid 4$. Comme $G_0 \subset A_5$, G_0 est d'ordre 2 ou 3. Les deux cas sont possibles; pour les distinguer, il suffit de connaître la décomposition de l'idéal premier engendré par p dans E_5 .

D'après ([11], p. 248–250) ces conditions sont suffisantes. Si $\text{Card}(G_0) \geq 3$, comme $\text{Card}(G_0)$ divise $p-1$, on applique le lemme ([11], p. 248); si $\text{Card}(G_0) = 2$, on raisonne comme dans ([11], p. 249–250).

Quand les conditions du théorème sont satisfaites, dans chaque cas, $\tilde{\rho}_E$ admet deux relèvements irréductibles non isomorphes, de conducteur p , de déterminant pair, si ρ est l'un d'eux, l'autre est $\tilde{\rho} = \rho \oplus \det(\rho)^{-1}$.

Le nombre de classes de conjugaison de plongements de A_4 , resp. S_4 , A_5 dans $\text{PGL}(2, \mathbb{C})$ est 1, resp. 1, 2. Il existe donc:

2x représentations irréductibles de dimension 2 de $G_{\mathbb{Q}}$ de type A_4

2y représentations irréductibles de dimension 2 de $G_{\mathbb{Q}}$ de type S_4

4z représentations irréductibles de dimension 2 de $G_{\mathbb{Q}}$ de type A_5

non isomorphes, de conducteur p , de déterminant pair, où x , (resp. y , z), est le nombre de corps quartiques, (resp. quartiques, quintiques) satisfaisant les hypothèses du théorème, cas (1), (resp. cas 2_a ou 2_b selon p , cas $3_{a,b,c}$ (a, b, c) étant déterminé par p).

EXEMPLES NUMÉRIQUES. On note ρ une représentation de dimension 2 de $G_{\mathbb{Q}}$ de déterminant pair, de conducteur un nombre premier p .

Les tables de corps quintiques de Buhler ([1]) semblent indiquer que:

Pour $p < 10000$, il n'existe aucun ρ de type A_5 . (3)

Les tables de corps quartiques totalement réels E_4/\mathbb{Q} , ne contenant pas de sous-corps quadratique (condition nécessaire et suffisante pour que la clôture galoisienne E/\mathbb{Q} de E_4 ait un groupe de Galois isomorphe à A_4 (si le discriminant de E_4/\mathbb{Q} est un carré) ou S_4 (sinon)) de Godwin ([8] p. 484) montrent que

(1) *pour $p < 106$, il n'existe aucun ρ de type A_4 ,*

(2) *pour $p < 11348$, il existe 10 ρ non isomorphes de type S_4 avec $\det \rho$ égal au symbole de Legendre. Les 5 valeurs de p sont:*

2777, 7537, 8069, 10273, 10889, 11197.

Si $p \equiv 1 \pmod{8}$, et E_4/\mathbb{Q} de discriminant p^3 , alors $\mathbb{Q}(\sqrt{p}) \subset E$ a un nombre de classes divisible par 3. Pour $p < 2000$, il y a trois valeurs possibles ([2])

$p = 257, 761, 1489.$

Je ne sais pas si elles fournissent des exemples.

(2_b) *pour $p \equiv 1 \pmod{8}$, $p < 2000$, $p \neq 257, 761, 1489$, il n'existe pas de ρ de type S_4 .*

Application: *représentations paires de conducteur premier p , de déterminant égal au symbole de Legendre $n \rightarrow \left(\frac{n}{p}\right)$, $p \equiv 1 \pmod{4}$.*

Il y en a :

- 1) 1 réductible,
- 2) $(h - 1)/2$ diédrales où h est le nombre de classes de $\mathbb{Q}(\sqrt{p})$,
- 3) $2x$ de type S_4 où x est le nombre de corps quartiques totalement réels ne contenant pas de sous-corps quadratiques, et de discriminant p ,
- 4) $4s$ de type A_5 , où s est le nombre de corps quintiques E_5/\mathbb{Q}
 - (a) de discriminant p^2
 - (b) tels que $E_5 \mathbb{Q}(\sqrt{p})/\mathbb{Q}$ ne soit pas galoisien (par exemple, si $5 \nmid h$)
 - (c) tels que l'indice de ramification d'un idéal premier $P \mid p$ de E_5 soit inférieur ou égal à 2.

Le groupe de Galois de la clôture galoisienne E/\mathbb{Q} de E_5 est un sous-groupe de A_5 , différent de $\mathbb{Z}/5\mathbb{Z}$, par (a) et de D_5 par (b), donc égal à A_5 . Par (c), le groupe d'inertie de $\text{Gal}(E/\mathbb{Q})$ en p est d'ordre 2.

Si ρ est réductible, ou diédrale, la conjugaison complexe opère trivialement; je ne sais pas si elle opère trivialement dans les autres cas.

3. Fonctions L

3.1. *Représentations galoisiennes de dimension 2.* Soit ρ une représentation irréductible, linéaire, complexe, de dimension 2 de $G_{\mathbb{Q}}$, de déterminant pair, telle que $\rho(c) = (-1)^a \text{id.}$, où $c \in G_{\mathbb{Q}}$ est une conjugaison complexe, et $a = 0$ ou 1.

Soit $N(\rho)$ le conducteur d'Artin et $L(s, \rho)$ la fonction d'Artin de la représentation ρ (on réfère à [10] p. 7 à 18 pour leurs définitions). On pose

$$\Lambda(s, \rho) = N(\rho)^{s/2} \pi^{-(s+a)} \Gamma\left(\frac{s+a}{2}\right)^2 L(s, \rho).$$

Alors, on sait que Λ s'étend en une fonction méromorphe de s sur tout le plan complexe et vérifie l'équation fonctionnelle:

$$\Lambda(1-s, \rho) = W(\rho) \Lambda(s, \bar{\rho})$$

où $\bar{\rho}$ est la contragrédiente de ρ , et $W(\rho)$ une constante de module 1. La conjecture d'Artin dit que Λ est une fonction holomorphe de S . Il est utile d'introduire la condition (A):

(A) Il existe un entier M tel que pour toute représentation linéaire continue χ de dimension 1 de $G_{\mathbb{Q}}$, de conducteur premier à M , la fonction $\Lambda(s, \rho \otimes \chi)$ est holomorphe en s .

La représentation vérifie la condition (A) si l'image de ρ dans $\text{PGL}(2, \mathbb{Q})$ n'est pas isomorphe à A_5 (c'est bien connu si ρ est de type diédral, c'est un célèbre résultat de Langlands si ρ est de type A_4 , le résultat pour ρ de type S_4 se déduit de celui pour A_4 comme l'a démontré Tunnell ([12]).

3.2. *Représentations automorphes de $GL(2)$.* Soit $A_{\mathbb{Q}}$ l'anneau des adèles de \mathbb{Q} ; soit π une représentation automorphe cuspidale de $GL(2, A_{\mathbb{Q}})$, autrement dit un composant irréductible de l'action naturelle de $GL(2, A_{\mathbb{Q}})$ dans l'ensemble des fonctions sur

$GL(2, \mathbb{Q}) \backslash GL(2, A_{\mathbb{Q}})$ satisfaisant des conditions raisonnables (pour les définitions, on réfère à [3]). On écrit π comme un produit tensoriel restreint

$$\pi = \otimes \pi_v$$

de représentations irréductibles admissibles unitaires π_v de $GL(2, \mathbb{Q}_v)$, où v parcourt les places de \mathbb{Q} , et \mathbb{Q}_v est le complété de \mathbb{Q} en v . On suppose que pour la place archimédienne $v = \infty$, la représentation π_∞ est la représentation, dite de la série principale, définie par l'une des propriétés équivalentes suivantes ([5]):

1) π_∞ est la représentation obtenue par le foncteur d'induction unitaire à partir de la représentation continue, de dimension 1, du groupe triangulaire supérieur:

$$(\text{sign}^a \otimes \text{sign}^a) \begin{pmatrix} x & y \\ 0 & z \end{pmatrix} = (\text{sign } x)^a (\text{sign } z)^a$$

2) π_∞ est l'unique représentation irréductible admissible de $GL(2, \mathbb{R})$ telle que

– la restriction de π_∞ au centre de $GL(2, \mathbb{R})$ est triviale,

– il existe dans l'espace de π_∞ un vecteur v invariant par $SO(2, \mathbb{R})$ et tel que

$$\pi_\infty \begin{pmatrix} 1 & \\ & -1 \end{pmatrix} v = (-1)^a v$$

– soit C l'opérateur de Casimir standard dans l'algèbre enveloppante de $GL(2, \mathbb{R})$ alors $\pi_\infty(C) = -1/4$.

La fonction $L(s, \pi_\infty)$ associée à π_∞ est égale à:

$$L(s, \pi_\infty) = \pi^{-(s+a)} ((s+a)/2)^2.$$

On définit le conducteur $N(\pi)$, la fonction $L(s, \pi)$ et le facteur $\varepsilon(s, \pi)$ de la représentation π ; on a

$$\varepsilon(s, \pi) = N(\pi)^{-(s+1/2)} W(\pi),$$

où $W(\pi)$ est une constante de module 1. Jacquet et Langlands ont montré que la fonction L se prolonge en une fonction holomorphe de s sur le plan complexes et vérifie une équation fonctionnelle:

$$L(s, \pi) = \varepsilon(s, \pi) L(1-s, \tilde{\pi}),$$

où $\tilde{\pi}$ est la représentation contragrédiente de π . Si $\omega(\pi)$ est le caractère central associé à π , alors $\tilde{\pi} = \pi \otimes \omega(\pi)^{-1}$. On pose

$$\Lambda(s, \pi) = N(\pi)^{s/2} L(s, \pi).$$

Alors la fonction Λ est une fonction holomorphe de s et vérifie l'équation fonctionnelle:

$$\Lambda(1-s, \pi) = W(\pi) \Lambda(s, \tilde{\pi}).$$

3.3. Le théorème fondamental. Par la théorie du corps de classes, une représentation linéaire continue de dimension 1 de $G_{\mathbb{Q}}$ s'identifie avec un caractère de A^{\times} trivial sur \mathbb{Q}^{\times} , donc aussi en composant avec le déterminant à une représentation de dimension 1 de $GL(2, A_{\mathbb{Q}})$.

THÉORÈME. Soit ρ une représentation comme en 1) vérifiant la condition (A), alors il existe π comme en 2) tel que pour tout χ vérifiant (A):

$$\Lambda(s, \rho \otimes \chi) = \Lambda(s, \pi \otimes \chi).$$

Ce résultat n'est qu'un cas particulier du célèbre théorème de Hecke–Weil–Jacquet–Langlands, pour lequel on réfère à la version améliorée obtenue par W. Li ([9]).

Si π et ρ se correspondent comme ci-dessus, alors on a de plus:

$$N(\pi) = N(\rho), \quad W(\pi) = W(\rho), \quad \omega(\pi) = \det(\rho).$$

Il est connu que les classes d'isomorphie de π et de ρ sont déterminées par les fonctions $\Lambda(s, \rho\chi)$ et $\Lambda(s, \pi\chi)$ pour tout χ vérifiant (A). On ne sait pas si l'application $\rho \rightarrow \pi$, définie sur l'ensemble des représentations galoisiennes de dimension 2, de déterminant pair, vérifiant (A), à valeurs dans l'ensemble des représentations automorphes paraboliques π de $GL(2, A_{\mathbb{Q}})$ telles que $\pi_{\infty}(C) = -1/4$ est une surjection.

Calcul de la constante d'Artin $W(\rho)$, si ρ est de conducteur p , et vérifie (A). Si ρ est de conducteur p , on a vu que $\det \rho$ est aussi de conducteur p . Si ρ vérifie (A), soit π l'image de ρ par l'application ci-dessus. Pour tout nombre premier q , ρ_q est de la série principale, obtenue par le foncteur d'induction unitaire d'une représentation continue de dimension 1, du groupe triangulaire supérieur:

$$(\mu_1 \otimes \mu_2) \begin{pmatrix} x & y \\ & z \end{pmatrix} = \mu_1(x)\mu_2(z)$$

où μ_1, μ_2 sont deux caractères de \mathbb{Q}_q^{\times} ; le couple non ordonné (μ_1, μ_2) est déterminé par la représentation π_q . Si $q \neq p$, les deux caractères sont non ramifiés, tandis que si $q = p$, on peut supposer μ_1 non ramifié, et

$$\mu_1\mu_2 = (\omega(\pi))_p.$$

Il est connu que $W(\pi)$ est le produit de constantes locales

$$W(\pi) = \prod W(\pi_v)$$

et que:

$$W(\pi_{\infty}) = (-1)^a \quad ([7] \text{ p. 114})$$

$$W(\pi_p) = W(\mu_1)W(\mu_2),$$

où $W(\mu)$ est une constante de module 1, égale à 1 si μ est non ramifié, et

$$W(\mu)W(\mu^{-1}) = \mu(-1).$$

On en déduit:

$$(-1)^a W(\pi) = W(\omega(\pi)^{-1}) = W(\omega(\pi))^{-1}.$$

Comme $W(\pi) = W(\rho)$ et $\omega(\pi) = \det \rho$, on a:

LEMME. Si ρ est de conducteur p , vérifie (A), et si $\rho(c) = (-1)^a \text{id}$, alors

$$W(\rho) = W(\det \rho)(-1)^a.$$

En particulier, si $\det \rho$ est le symbole de Legendre, alors $W(\det \rho) = 1$, (voir [10]) et

$$W(\rho) = (-1)^a.$$

REMARQUE. La théorie du nouveau vecteur ([5]) fait le lien entre les représentations automorphes de $GL(2, A_{\mathbb{Q}})$ et les formes modulaires classiques (holomorphes ou non). Elle permet de développer une théorie des formes primitives, pour les formes modulaires non holomorphes, introduites par Maass, analogue à celle connue pour les formes classiques; dans ce langage, la forme primitive de Maass associée à ρ vérifiant les conditions du théorème, avec

$$L(s, \rho) = \sum_{n \geq 1} a(n)n^{-s} \quad \text{et} \quad \rho(c) = (-1)^a$$

s'écrit:

$$f(x, y) = \sqrt{y} \sum_{\substack{n \in \mathbb{Z} \\ n \neq 0}} a(|n|)(\text{sign } n)^a K_0(2\pi |n| y) e^{2imnx}$$

où K_0 est la fonction de Bessel définie par:

$$K_0(x) = \int_0^{\infty} (t^2 + 1)^{-1/2} \cos(xt) dt, \quad \text{si } x > 0.$$

La fonction f est propre pour le Laplacien hyperbolique

$$\Delta = -y^2(d^2/dx^2 + d^2/dy^2)$$

de valeur propre $\lambda = 1/4$.

Je remercie C. Bonfont et K. Ribet pour de nombreuses conversations intéressantes.

BIBLIOGRAPHIE

1. J. P. Buhler, Icosahedral Representations *Springer-Verlag Lecture Notes* **654** (1978).
2. Z. Borevich et I. Chafarevich, *Théorie des nombres* (Gauthiers-Villars, 1967).
3. A. Borel et H. Jacquet, Automorphic forms and automorphic representations (dans Automorphic Forms, Representations, and L-functions, *AMS Proc. of Symp. in Pure Math.* vol. XXXIII, part 1, p. 189–202 (1979)).
4. W. Casselman, GL_n dans *Algebraic Number Fields*, A. Fröhlich (Academic Press 1977).
5. W. Casselman, On some results of Atkin-Lehner, *Math. Ann.* **201** (1973), 301–314.
6. B. N. Delone et D. K. Faddev, *The theory of irrationalities of the third degree* Transl. of Math. Mon. vol. 10, AMS (1964).
7. S. Gelbart, *Automorphic forms on adeles groups* (Ann. of Math. Studies, n° 23, Princeton University Press 1975).
8. H. J. Godwin, Real quartic fields with small discriminant, *J. London Math. Soc.* **31** (1956), 478–485.
9. W. Li, On converse theorems for GL_2 and GL_1 *Amer. J. of Math.* **103** (1981), 851–885.
10. J. Martinet, Character Theory and Artin L-functions dans *Algebraic Number Fields*, A. Fröhlich (Academic Press 1977).

11. J-P. Serre, Modular forms of weight one and Galois representations dans *Algebraic Number Fields*, A. Fröhlich (Academic Press 1977).

12. J. Tunnell, Artin's conjecture for representations of octahedral type *Bull. Amer. Math. Soc.* **5** (1981), 173–175.

ÉCOLE NORMALE SUPÉRIEURE
92120 MONTROUGE
FRANCE