CONGRUENCES DES NOMBRES DE RAMANUJAN ET REPRÉSENTATIONS $\ell-$ADIQUES

par

Henri GUENANCIA & Olivier TAÏBI

Résumé. — Le point de départ de ce mémoire est la fonction de Ramanujan, notée τ, construite implicitement, et dont on aimerait avoir, si ce n'est la valeur en tout point, du moins la valeur en tout point modulo des nombres premiers voire des puissances de nombres premiers. Lorsqu'on se plonge dans les premiers travaux sur ce problème, on découvre que cette fonction vérifie des congruences pour certains nombres premiers ; la question est donc : quels sont tous ces nombres premiers ? Cette question a été résolue dans les années 70, principalement grâce aux travaux de P. Deligne, J.-P. Serre et H. Swinnerton-Dyer. Nous nous proposons donc ici de retracer les grandes lignes de ces recherches, depuis le théorème de Deligne sur l'existence d'un système de représentations ℓ-adiques attachées à Δ jusqu'à la détermination des nombres premiers exceptionnels par Serre et Swinnerton-Dyer conjointement.

Nous tenons à remercier chaleureusement Benjamin SCHRAEN qui a encadré ce mémoire, et nous a donné l'envie d'approfondir ce beau et vaste sujet.

Table des matières

PARTIE I
FORMES MODULAIRES

1. Généralités

1.1. Définition. — Le groupe $\mathrm{PSL}_2(\mathbb{Z})$ agit naturellement (projectivement) sur le demi-plan de Poincaré $\mathcal{H} := \{z \in \mathbb{C} | \Im(z) > 0\}$ par $\begin{pmatrix} a & b \\ c & d \end{pmatrix} . z = \frac{az+b}{cz+d}$, puisque $\mathcal{H} \subset P^1(\mathbb{C})$ est stable sous l'action de $\mathrm{PSL}_2(\mathbb{R})$.

Définition 1.1. — On appelle forme modulaire de poids $2k$ une fonction holomorphe sur $\mathcal{H}$ vérifiant, pour tout $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ et tout $z \in \mathcal{H}$, $f\left(\frac{az+b}{cz+d}\right) = (cz+d)^{2k} f(z)$, et « holomorphe à l'infini ».

Précisons le sens de « holomorphe à l'infini ». Une fonction holomorphe f vérifiant la première condition est 1-périodique : $f(z+1) = f(z)$ pour tout $z \in \mathcal{H}$, ce qui montre que $f(z) = g(q)$ où l'on a posé $q = e^{2i\pi z}$. Ainsi g est définie sur $D \setminus \{0\}$ (avec $D := \{q \in \mathbb{C} \mid |q| < 1\}$). Puisqu'il existe localement des déterminations du logarithme, g est également holomorphe, et admet donc un développement en série de Laurent $g(q) = \sum_{n=-\infty}^{+\infty} a_n q^n$. Le point z « à l'infini »(i.e. $\Im(z) \to +\infty$) correspond à $q = 0$, et on dira donc que f est « holomorphe à l'infini » si g est holomorphe en 0 (ce qui revient à dire que $a_n = 0$ pour $n < 0$). En pratique, il suffit de vérifier que $f(z)$ est bornée lorsque $\Im(z)$ est suffisamment grand.

Définition 1.2. — Avec les mêmes notations, on dit qu'une forme modulaire f est une *forme parabolique* si $a_0 = 0$.

Remarque 1.

Pour montrer que $f\left(\frac{az+b}{cz+d}\right) = (cz+d)^{2k} f(z)$ pour tout $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$, il suffit en fait de le montrer pour $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ et $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, i.e. de montrer les relations $f(z+1) = f(z)$ et $f(-\frac{1}{z}) = z^{2k} f(z)$, car $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ et $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ engendrent $\mathrm{SL}_2(\mathbb{Z})$.

***Exemple 1.3* (Séries d'Eisenstein)**. — Pour $k > 1$ et $\Lambda = \mathbb{Z}^2 \setminus \{(0,0)\}$, soit

$$G_{2k}(z) = \sum_{(m,n) \in \Lambda} \frac{1}{(mz+n)^{2k}}.$$

Cette série converge absolument uniformément sur toutes les parties de la forme $\{z \in \mathcal{H} | \Im(z) \geqslant a \text{ et } |\Re(z)| \leqslant b\}$, donc définit bien une fonction holomorphe sur $\mathcal{H}$. Il est clair que $G_{2k}(z+1) = G_{2k}(z)$ pour tout $z \in \mathcal{H}$. En outre :

$$G_{2k}\left(-\frac{1}{z}\right) = \sum_{(m,n)\in\Lambda} \frac{1}{(-\frac{m}{z}+n)^{2k}} = z^{2k} \times \sum_{(m,n)\in\Lambda} \frac{1}{(-m+zn)^{2k}} = z^{2k} G_{2k}(z).$$

D'autre part, $\lim_{\Im(z)\to+\infty} G_{2k}(z) = 2\zeta(2k)$, donc G_{2k} est « holomorphe à l'infini ». G_{2k} est donc une forme modulaire non parabolique de poids $2k$. On en déduit que $\Delta := (2\pi)^{-12}\left((60G_4)^3 - 27(140G_6)^2\right)$ est une forme modulaire parabolique de poids 12. La théorie des courbes elliptiques montre que Δ ne s'annule pas sauf en l'infini (car Δ est le discriminant d'une courbe elliptique).
D'autre part, on peut montrer par un développement de la cotangente la formule

$$G_{2k}(z) = 2\zeta(2k) + 2\frac{(2\pi i)^{2k}}{(2k-1)!}\sum_{n=1}^{+\infty} \sigma_{2k-1}(n) q^n,$$

où σ est la fonction arithmétique définie dans la section 2.3. Alors, les identités classiques reliant nombres de Bernoulli et fonction zêta montrent que la série d'Eisenstein normalisée de poids $2k$ vérifie :

$$E_{2k}(z) := \frac{G_{2k}(z)}{2\zeta(2k)} = 1 + (-1)^k \frac{4k}{B_{2k}} \sum_{n=1}^{+\infty} \sigma_{2k-1}(n) q^n$$

où $B_{2k} = (-1)^{k+1} b_{2k} \geqslant 0$ avec $\frac{x}{e^x-1} = \sum_{n\geqslant 0} \frac{b_k}{k!} x^k$. Pour $k = 1$, la somme ne converge pas absolument, mais on peut encore définir $G_2(z) = \sum_n \sum'_m \frac{1}{(m+nz)^2}$ où la somme porte sur $(n,m) \neq (0,0)$, qui est une fonction holomorphe sur $\mathcal{H}$. Cependant, lorsque l'on calcule $G_2\left(\frac{-1}{z}\right)$, on voit apparaître la même somme, sauf que l'ordre des sommations est inversé. Le calcul de la différence entre ces deux sommes permet alors d'établir que $G_2\left(\frac{-1}{z}\right) = z^2 G_2(z) - 2i\pi z$, donc G_2 est « presque »une forme modulaire de poids 2. De façon similaire au cas $k > 1$, on peut calculer le développement de G_2 en série :

$$G_2(z) = \frac{\pi^2}{3} - 8\pi^2 \sum_{n\geqslant 1} \sigma_1(n) q^n$$

et on définit la série d'Eisenstein normalisée :

$$E_2(z) := \frac{3}{\pi^2} G_2(z) = 1 - 24 \sum_{n\geqslant 1} \sigma_1(n) q^n$$

1.2. Dimension des espaces de formes modulaires. — La proposition suivante, dont on pourra trouver la démonstration dans [**Ser70**] (VII.3, Cor.1) , est très efficace pour démontrer avec peu de calculs des formules d'apparence complexe.

Proposition 1.4. — *En notant M_{2k} l'espace vectoriel des formes modulaires de poids $2k$,* $\dim M_{2k} = 0$ *si* $k < 0$ *et, pour* $k \geqslant 0$

$$\dim M_{2k} = \begin{cases} \left[\frac{k}{6}\right] & si\ 6|k-1 \\ \left[\frac{k}{6}\right] + 1 & sinon \end{cases} .$$

D'autre part, la multiplication par Δ définit un isomorphisme de M_{2k-6} sur M^0_{2k}, l'ensemble des formes paraboliques de poids $2k$ (ce qui revient à dire que le pôle que Δ possède en l'infini est simple).

Corollaire 1.5. — *M_{2k} admet pour base l'ensemble des monômes $G_4^a G_6^b$ tels que $2a+3b = k$.*

1.3. Réseaux de $\mathbb{C}$. —

Définition 1.6. — On appelle réseau de $\mathbb{C}$ toute partie de la forme $\mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$ où (ω_1, ω_2) est libre (sur $\mathbb{R}$).

Un réseau Γ étant donné, décrivons l'ensemble des bases de Γ. On peut permuter les deux vecteurs de base, donc on peut se limiter aux couples (ω_1, ω_2) tels que $\Im(\frac{\omega_1}{\omega_2}) > 0$, c'est-à-dire $\frac{\omega_1}{\omega_2} \in \mathcal{H}$. Par ailleurs, si (ω_1', ω_2') est une autre base, en écrivant chaque vecteur de chaque base comme combinaison $\mathbb{Z}$-linéaire des vecteurs de l'autre base, on voit que $\begin{pmatrix} \omega_1' \\ \omega_2' \end{pmatrix} = g \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix}$ où $g \in \mathrm{GL}_2(\mathbb{Z})$, et même $\mathrm{SL}_2(\mathbb{Z})$ puisqu'on impose $\frac{\omega_1'}{\omega_2'},\ \frac{\omega_1}{\omega_2} \in \mathcal{H}$. L'ensemble des réseaux de $\mathbb{C}$ s'identifie donc à l'ensemble des orbites de $\left\{(\omega_1, \omega_2) \mid \frac{\omega_1}{\omega_2} \in \mathcal{H}\right\}$ sous l'action de $\mathrm{SL}_2(\mathbb{Z})$. Soit maintenant F une fonction définie sur l'ensemble des réseaux, et telle que pour tout réseau Γ et tout $\lambda \in \mathbb{C}^*$, $F(\lambda\Gamma) = \lambda^{-2k} F(\Gamma)$. En posant $f(z) = F(\mathbb{Z}z \oplus \mathbb{Z}1)$, $F(\mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2) = \omega_2^{-2k} f(\frac{\omega_1}{\omega_2})$. La valeur de $\omega_2^{-2k} f(\frac{\omega_1}{\omega_2})$ ne dépend donc pas de la base du réseau choisie, ce qui revient à dire que $f\left(\frac{az+b}{cz+d}\right) = (cz+d)^{2k} f(z)$. Les formes modulaires peuvent donc également être vues comme des fonctions définies sur l'ensemble des réseaux de $\mathbb{C}$ (noter toutefois que la condition de dérivabilité de f ne s'exprime pas autrement).

Remarque 2.
Les fonctions G_{2k} s'obtiennent à partir de la fonction

$$\Gamma \mapsto \sum_{\gamma \in \Gamma \setminus \{(0,0)\}} \frac{1}{\gamma^{2k}},$$

ce qui les rend plus naturelles.

2. La fonction τ de Ramanujan

2.1. Opérateurs de Hecke. — Pour les résultats non démontrés de ce paragraphe, nous renvoyons à [**Ser70**] (VII.5).

Définition 2.1. — Soit G le groupe abélien libre engendré par l'ensemble des réseaux de $\mathbb{C}$ (i.e. l'ensemble des $\sum n_\Gamma \Gamma$ (la somme porte sur les réseaux Γ) où les n_Γ sont des entiers relatifs presque tous nuls). Pour tout $n \in \mathbb{N} \setminus \{0\}$ et tout $\lambda \in \mathbb{C}^*$ on définit les endomorphismes $T(n)$ et R_λ de G par :

$$\begin{aligned} R_\lambda \Gamma &= \lambda \Gamma \\ T(n)\Gamma &= \sum_{(\Gamma:\Gamma')=n} \Gamma', \end{aligned}$$

la somme portant sur les sous-réseaux Γ' de Γ d'indice n.

Proposition 2.2. — *On a les résultats suivants :*

1. *$T(n)$ et R_λ commutent ;*
2. *$R_\lambda R_\mu = R_{\lambda\mu}$;*
3. *Si n et m sont premiers entre eux, alors $T(mn) = T(n)T(m)$;*
4. *Si $n \geqslant 1$ et p est premier, $T(p^n)T(p) = T(p^{n+1}) + pT(p^{n-1})R_p$.*

Si F est une fonction définie sur l'ensemble des réseaux, F se prolonge à G par $\mathbb{Z}$-linéarité. Si L est un endomorphisme de G, on peut définir $LF = F \circ L$. La condition « $F(\lambda\Gamma) = \lambda^{-2k}F(\Gamma)$ pour tout réseau Γ et tout $\lambda \in \mathbb{C}^*$ »s'écrit donc « $R_\lambda F = \lambda^{-2k}F$ pour tout $\lambda \in \mathbb{C}^*$ ». Puisque $T(n)$ et R_λ commutent, si F vérifie cette condition, $T(n)F$ également. Par conséquent, partant d'une forme modulaire f, on définit une fonction F sur l'ensemble des réseaux par $F(\mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2) = \omega_2^{-2k} f(\frac{\omega_1}{\omega_2})$, à laquelle on associe ensuite une fonction $T(n)F$ sur l'ensemble des réseaux, qui permet elle-même de définir une fonction $T(n)f$ sur $\mathcal{H}$. Par commodité pour les calculs, on définit en fait $T(n)f(z) = n^{2k-1}T(n)F(\mathbb{Z}z \oplus \mathbb{Z})$ Pour montrer que $T(n)f$ est également une forme modulaire, il suffit de vérifier qu'elle est holomorphe sur $\mathcal{H} \cup \{\infty\}$. Cela se déduit simplement du fait que tout sous-réseau de $\Gamma = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$ d'indice n s'écrit $\mathbb{Z}\omega_1' \oplus \mathbb{Z}\omega_2'$ où $\begin{pmatrix}\omega_1' \\ \omega_2'\end{pmatrix} = \begin{pmatrix}a & b \\ 0 & d\end{pmatrix}\begin{pmatrix}\omega_1 \\ \omega_2\end{pmatrix}$ et qu'il n'y a qu'un nombre fini de tels sous-réseaux. Cette même remarque montre que si f est parabolique, $T(n)f$ l'est également.

Théorème 2.3. — *Supposons que f soit une forme modulaire qui est fonction propre de $T(n)$ pour tout n, et notons $\lambda(n)$ la valeur propre correspondante. En notant $f(z) = \sum_{m \geqslant 0} c_m q^m$, on a :*

1. *$c_1 \neq 0$.*
2. *Si $c_1 = 1$, $c(n) = \lambda(n)$ pour tout n.*

Grâce aux relations entre les $T(n)$, on en déduit le corollaire suivant :

Corollaire 2.4. — *Si f est une forme modulaire fonction propre de tous les $T(n)$ et si $c_1 = 1$:*

1. *$c(mn) = c(m)c(n)$ si m et n sont premiers entre eux.*
2. *$c(p^{n+1}) = c(p)c(p^n) - p^{2k-1}c(p^{n-1})$ pour tout p premier et $n \geqslant 1$.*

Remarque 3.
Ceci s'énonce également à l'aide d'une série de Dirichlet de la façon suivante :

$$\sum_{n\geqslant 1} \frac{c(n)}{n^s} = \prod_p \frac{1}{1 - c(p)p^{-s} + p^{2k-1-2s}}.$$

2.2. Les coefficients de la fonction Δ. — Puisque l'espace vectoriel des formes paraboliques de poids 12 est de dimension 1, Δ est fonction propre pour tous les $T(n)$, donc le théorème précédent s'applique. Notons $\tau(n)$ le coefficient de q^n dans le développement en série de Δ. On calcule que $\tau(1) = 1$. Alors on obtient le résultat suivant, conjecturé par Ramanujan et démontré par Mordell :

Proposition 2.5. — *La fonction τ vérifie les propriétés suivantes :*

1. *$\tau(mn) = \tau(m)\tau(n)$ si m et n sont premiers entre eux.*
2. *$\tau(p^{n+1}) = \tau(p)\tau(p^n) - p^{11}\tau(p^{n-1})$ pour tout p premier et $n \geqslant 1$.*

La connaissance des $\tau(p)$, p premier, suffit donc pour connaître la fonction τ.

Le calcul de τ peut par exemple se faire avec le développement en produit suivant :

$$\Delta(z) = q\prod_{n\geqslant 1}(1-q^n)^{24}.$$

Pour prouver cette identité, il suffit de montrer que la fonction $f(z) := q\prod_{n\geqslant 1}(1-q^n)^{24}$ vérifie $f\left(\frac{-1}{z}\right) = z^{12}f(z)$ car l'espace vectoriel des formes paraboliques de poids 12 est de dimension 1 et f et Δ ont même coefficient de degré 1.

$$\begin{aligned}
\frac{\mathrm{d}f}{f} &= \frac{\mathrm{d}q}{q}\left(1 - 24\sum_{n\geqslant 1}\frac{nq^n}{1-q^n}\right) \\
&= \frac{\mathrm{d}q}{q}\left(1 - 24\sum_{n,m\geqslant 1} nq^{nm}\right) \\
&= \frac{\mathrm{d}q}{q}\left(1 - 24\sum_{n\geqslant 1}\sigma_1(n)q^{nm}\right) \\
&= 2i\pi \mathrm{d}z E_2(z)
\end{aligned}$$

Comme de plus $E_2(\frac{-1}{z}) = z^2 E_2(z) - \frac{6i}{\pi} z$, les fonctions f et $z \mapsto z^{-12} f(\frac{-1}{z})$ sont proportionnelles, et l'évaluation en i nous donne que le coefficient de proportionnalité vaut 1.

2.3. Une congruence modulo 691. — L'objectif de ce paragraphe est de montrer comment on peut montrer certaines congruences sur la fonction τ sans passer par l'existence de représentations attachées à Δ. Précisément, ce sont ces congruences qui ont suggéré que l'on peut voir les coefficients des formes modulaires comme trace d'un certain opérateur. Venons-en au résultat principal de cette partie, qui est dû à Ramanujan :

Proposition 2.6. — *Pour tout nombre premier p, on a $\tau(p) \equiv 1 + p^{11} \mod 691$.*

Démonstration. — La démonstration n'utilise que les résultats basiques déjà exposés sur les formes modulaires. On va donc considéré les série d'Eisenstein normalisées de poids 6 et 12 respectivement : si

$$\sigma_q(n) = \sum_{d|n} d^q,$$

alors on a

$$\begin{aligned} E_6(x) &= 1 - 504 \sum_{n=1}^{+\infty} \sigma_5(n) x^n \\ E_{12}(x) &= 1 + \frac{65520}{691} \sum_{n=1}^{+\infty} \sigma_{11}(n) x^n \end{aligned}$$

Alors E_6^2 est une forme modulaire de poids 12, donc est combinaison linéaire de E_{12} et de Δ. Un calcul facile montre que $E_6^2 = E_{12} - a/691\Delta$ avec $a \equiv 65520 \mod 691$. Alors, on multiplie tout par 691, ce qui donne la congruence : $0 \equiv \sum(\sigma_{11}(n) - \tau(n))x^n \mod 691$ car 691 ne divise pas 65520.

□

2.4. Quelques congruences vérifiées par le fonction τ. — Par des calculs un peu similaires à celui développé dans le paragraphe précédent, on peut arriver à établir pour la fonction τ des congruences modulo les nombres premiers $2, 3, 5, 7, 23$ et 691. C'est l'objet du théorème suivant, dû à de nombreux mathématiciens (Ramanujan, Wilton, Swinnerton-Dyer, Lehmer ...) :

Théorème 2.7. — *Pour tous les nombres premiers p différents de $2, 3, 5, 7, 691$ et 23 respectivement, on a :*

$$\begin{aligned}
\tau(p) &\equiv 1 + p^{11} \mod 2^5 \\
\tau(p) &\equiv p^2 + p^9 \mod 3^3 \\
\tau(p) &\equiv p + p^{10} \mod 5^2 \\
\tau(p) &\equiv p + p^4 \mod 7 \\
\tau(p) &\equiv 1 + p^{11} \mod 691
\end{aligned}$$

$$\tau(p) \equiv \begin{cases} 0 \mod 23 \ si \ \left(\frac{p}{23}\right) = -1 \\ 2 \mod 23 \ si \ p = u^2 + 23v^2 \\ -1 \mod 23 \ sinon \end{cases} .$$

Par des méthodes algébriques bien différentes des preuves initiales, nous montrerons au fur et à mesure de l'exposé quelques unes de ces congruences.

PARTIE II
LE THÉORÈME DE DELIGNE

3. Préliminaires au théorème

3.1. Théorie de Galois infinie. — Il n'y a ici pas de grande nouveauté par rapport aux extensions finies. La différence majeure est que, n'étant plus dans le cas discret, pour obtenir une correspondance, il va falloir munir les groupes de Galois de la topologie de Krull, et ne considérer que les sous-groupes fermés. Cette topologie apparaît naturellement quand on considère le résultat suivant : soit L/K une extension galoisienne de groupe G. Pour toute sous-extension galoisienne finie F, on note $H = \mathrm{Gal}(L/F)$ qui est d'indice fini, et soit $\mathscr{F}$ la famille des tels groupes. Alors l'homomorphisme canonique $G \to G/H$ donne par la propriété universelle de la limite projective un homomorphisme

$$G \to \varprojlim_{H \in \mathscr{F}} G/H.$$

Proposition 3.1. — *L'homomorphisme $G \to \varprojlim G/H$ est un isomorphisme.*

Démonstration. — Si σ appartient au noyau, pour tout $x \in L$, il existe une extension galoisienne finie F contenant x, et $\mathrm{Gal}(L/F)$ est d'indice fini, donc $\sigma(x) = x$.

Soit $(\sigma_H)_H \in \varprojlim G/H$ et $x \in L$, alors $x \in F$ pour une certaine extension finie F de L. Pour tout H, G/H est isomorphe à $\mathrm{Gal}(F/K)$ car tout élément de $\mathrm{Gal}(F/K)$ se prolonge à L et H est le noyau de l'opération de restriction à F. Il est donc légitime de poser $\sigma(x) = \sigma_H(x)$ pour tout H tel que $x \in F$, qui ne dépend pas de H par définition de la limite projective. La surjectivité est ainsi établie. □

On munit ainsi G de la topologie limite projective, qui en fait en particulier un groupe topologique compact. On va résumer les principaux résultats dans le théorème suivant, mais auparavant, fixons quelques notations. Soit K un corps de nombres, $\overline{K}$ une clôture algébrique, on note $\mathcal{C}$ l'ensemble des sous-corps de $\overline{K}$ contenant K, et $\mathcal{G}$ l'ensemble des sous-groupes fermés de $\mathrm{Gal}(\overline{K}/K)$.

Théorème 3.2. — *Les applications $L \mapsto \mathrm{Gal}(\overline{K}/L)$ et $H \mapsto \overline{K}^H$ sont des bijections réciproques entre $\mathcal{C}$ et $\mathcal{G}$. De plus, on a :*

(i) *$L \in \mathcal{C}$ est une extension finie de K si et seulement si le groupe $\mathrm{Gal}(\overline{K}/L)$ est ouvert (ie d'indice fini) dans $\mathrm{Gal}(\overline{K}/K)$.*
(ii) *$L \in \mathcal{C}$ est galoisienne si et seulement si $\mathrm{Gal}(\overline{K}/L) \lhd \mathrm{Gal}(\overline{K}/K)$.*

3.2. Extension maximale non ramifiée en dehors de ℓ. — Il est naturel de définir la non-ramification d'une extension maximale par la non-ramification de ses sous-extensions finies. Le but de cette partie est de justifier l'existence, pour tout nombre premier ℓ, d'une

plus grande extension de $\mathbb{Q}$ qui soit non ramifiée en dehors de ℓ. En quelque sorte, c'est la ramification minimale qu'on peut espérer, en vertu d'un résultat de Minkowski figurant dans [**Sam03**] (IV,Thm. 1). Celui-ci montre, par une minoration du discriminant d'un corps de nombre (appelé aussi discriminant absolu), que toute extension finie de $\mathbb{Q}$ est ramifiée en au moins un nombre premier.

Au début, nous avons commencé par remarquer que pour des extensions galoisiennes finies, tout se passait bien :

Proposition 3.3. — *Soient L/K une extension finie de corps de nombres, galoisienne. Si K_1 et K_2 sont deux sous-extensions galoisiennes de L/K non ramifiées en $\mathfrak{p}$ alors K_1K_2 n'est pas ramifiée en $\mathfrak{p}$.*

Démonstration. — Soit donc $\mathfrak{p}$ un idéal premier de $\mathcal{O}_K$ qui ne se ramifie ni dans K_1 ni dans K_2. Soit $\mathfrak{P}$ un idéal premier de $\mathcal{O}_{K_1K_2}$ au-dessus de $\mathfrak{p}$. Alors, on a $\mathfrak{P} \cap \mathcal{O}_K = \mathfrak{p}$, et pour tout $i \in \{1,2\}$ on a que $\mathfrak{P}_i = \mathfrak{P} \cap \mathcal{O}_{K_i}$ est un idéal premier de $\mathcal{O}_{K_i}$ au-dessus de $\mathfrak{p}$. Soit maintenant $\sigma \in I_{\mathfrak{P}}$ (groupe d'inertie de $\mathfrak{P}$).

Alors, pour tout $i \in \{1,2\}$ on a $\sigma_{|K_i} \in D_{\mathfrak{P}_i}$ le groupe de décomposition de $\mathfrak{P}_i$ car $\sigma(\mathfrak{P}_i) = \sigma(\mathfrak{P}) \cap \sigma(\mathcal{O}_{K_i}) = \mathfrak{P} \cap \mathcal{O}_{K_i} = \mathfrak{P}_i$. Soit maintenant $x \in \mathcal{O}_{K_i}$, on a donc $\sigma(x) = x + y$ où $y \in \mathfrak{P} \cap \mathcal{O}_{K_i} = \mathfrak{P}_i$ et ainsi $\sigma_{|K_i} \in I_{\mathfrak{P}_i} = \{\mathrm{id}_{K_i}\}$. Ainsi, comme $\sigma \in \mathrm{Gal}(K_1K_2/K)$, σ est triviale, et donc $\mathfrak{p}$ ne se ramifie pas dans K_1K_2. □

Le même résultat subsiste même sans l'hypothèse que les extensions sont galoisiennes, mais la démonstration est un peu plus technique, et nécessite le lemme suivant :

Lemme 3.4. — *Soient L/K et K'/K deux extensions finies d'un corps valué complet K et $L' = LK'$. Alors, si L/K n'est pas ramifiée, L'/K' ne l'est pas non plus.*

Démonstration. — On sait que la condition de non ramification pour de tels corps s'écrit $[L : K] = [\lambda : \kappa]$ où λ et κ désignent les corps résiduels de L et de K respectivement. D'autre part, l'extension λ/κ est finie, et séparable, donc il existe $\overline{\alpha} \in \lambda$ tel que $\lambda = \kappa(\overline{\alpha})$. Si $\alpha \in \mathcal{O}$ est un relèvement de $\overline{\alpha}$, $f \in \mathfrak{o}[X]$ son polynôme minimal et $\overline{f} = f \bmod \mathfrak{p} \in \kappa[X]$, alors :

$$[\lambda : \kappa] \leqslant \deg \overline{f} = \deg f = [K(\alpha) : K] \leqslant [L : K] = [\lambda : \kappa],$$

d'où l'on déduit $L = K(\alpha)$ et f est le polynôme minimal de α.

On a donc $L' = K'(\alpha)$ et si $g \in \mathfrak{o}'[X]$ est le polynôme minimal de α sur K', et à nouveau $\overline{g} = g \bmod \mathfrak{p}' \in \kappa'[X]$ alors $\overline{g}$ est séparable comme facteur de $\overline{f}$ et irréductible sur κ' car sinon le lemme de Hensel montrerait que g est réductible. On en déduit :

$$[\lambda' : \kappa'] \leqslant [L' : K'] = \deg g = \deg \overline{g} = [\kappa'(\alpha) : \kappa'] \leqslant [\lambda' : \kappa'].$$

□

Théorème 3.5. — *Soient L/K une extension finie de corps de nombres. Si K_1 et K_2 sont deux sous-extensions de L/K non ramifiées en $\mathfrak{p}$ alors K_1K_2 n'est pas ramifiée en $\mathfrak{p}$.*

Démonstration. — L'idée est de se ramener au cas où K, K_1, K_2 et $K_{12} = K_1K_2$ sont des corps munis d'une valuation discrète pour laquelle ils sont complets. On va donc considérer des idéaux premiers $\mathfrak{P}_1, \mathfrak{P}_2$ et $\mathfrak{P}$ de $\mathcal{O}_{K_1}, \mathcal{O}_{K_2}$ et $\mathcal{O}_{K_{12}}$ respectivement, au-dessus de $\mathfrak{p}$. On note F, F_1, F_2 et F_{12} les complétions des corps en question relativement aux valuations induites par chacun des idéaux respectifs. De la définition de ces valuations, on déduit sans grande difficulté que les indices de ramifications $e(F_i/F)$ sont égaux aux indices initiaux $e(K_i/K)$. D'autre part, les F-espaces vectoriels F_1F_2 et F_{12} sont égaux. On peut alors appliquer le lemme précédent en utilisant le fait que $e(F_{12}/F) = e(F_1F_2/F) = e(F_1F_2/F_1)e(F_1/F)$. □

On obtient donc grâce à ce résultat la plus grande extension de $\mathbb{Q}$ qui soit non ramifiée en p, notons là K^p. Alors, l'extension maximale de $\mathbb{Q}$ non ramifiée en dehors de ℓ est :

$$K_\ell = \bigcap_{p \neq \ell} K^p$$

où l'intersection est bien sûr prise sur les p *premiers*.

Remarque 4.
K_ℓ est une extension assez « grosse », et en particulier infinie. En effet, elle contient

$$\mathbb{Q}[\mu_{\ell^\infty}] = \bigcup_{n \geqslant 0} \mathbb{Q}[\mu_{\ell^n}].$$

Le théorème de Deligne combiné à celui de Kronecker-Weber montrera qu'elle est encore beaucoup plus grosse, vu qu'elle n'est pas abélienne.

3.3. Le Frobenius en p. — L'importance de l'extension K_ℓ va apparaître lors de ce paragraphe, car nous allons chercher dans $\mathrm{Gal}(K_\ell/\mathbb{Q})$ des éléments particuliers, appelés Frobenius (en p) généralisant l'automorphisme $\mathrm{Frob}_p : x \mapsto x^p \in \mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$. Pour cela, il faut faire attention à ne pas appliquer exactement les mêmes constructions que pour des extensions galoisiennes *finies*. On considère donc v_p la valuation p-adique classique sur $\mathbb{Q}$, qu'on peut étendre en v valuation sur K_ℓ. Par non ramification, $\mathcal{O}_{K_\ell,p} = v^{-1}(\mathbb{N})$ est muni d'une structure d'anneau de valuation discrète, d'idéal maximal $\mathfrak{P} = v^{-1}(\mathbb{N} - \{0\})$.

On a (cf. [**Ser68b**], III.5, Cor. 1) un isomorphisme $\mathcal{O}_{K_\ell,p}/\mathfrak{P} \simeq \overline{\mathbb{F}}_p$, et si on pose $D = \{\sigma \in \mathrm{Gal}(K_\ell/\mathbb{Q}) \,|\sigma(\mathfrak{P}) = \mathfrak{P}\}$ alors l'application :

$$\begin{array}{rccc} \Psi & : & D & \to & \mathrm{Gal}((\mathcal{O}_{K_\ell,p}/\mathfrak{P})/(\mathbb{Z}/p\mathbb{Z})) \simeq \mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p) \\ & & \sigma & \mapsto & \overline{\sigma} \end{array}$$

est bijective, et on peut définir le Frobenius en p par $F_p = \Psi^{-1}(\mathrm{Frob}_p)$. Cet élément est défini à conjugaison près, et vérifie la propriété : $\forall\, x \in \mathcal{O}_{K_\ell,p}$, $F_p(x) \equiv x^p \bmod \mathfrak{P}$.

4. Le théorème de Deligne

4.1. Le théorème de Čebotarev. — Sa démonstration est relativement longue, et nous voulons seulement donner son énoncé sans démonstration. Combiné avec le théorème de Deligne, il donnera de précieuses informations sur la fonction τ. Mais avant cela, on a besoin d'une définition, qui, bien que naturelle, a besoin d'être formalisée.

Définition 4.1. — Soit $\mathscr{P}$ (resp. $\mathscr{P}_n$) l'ensemble des nombres premiers (resp. nombres premiers inférieurs à n), et $d \in [0,1]$. On dit qu'un sous-ensemble $X \subset \mathscr{P}$ a pour densité (naturelle) d si la suite de terme général $|X \cap \mathscr{P}_n|/|\mathscr{P}_n|$ converge et a pour limite d.

***Théorème 4.2* (Čebotarev)**. — *Soit L une extension galoisienne finie de $\mathbb{Q}$, de groupe de Galois G. Si X est un sous-ensemble de G stable par conjugaison, et P_X l'ensemble des nombres premiers p non ramifiées dans L telles que la classe du Frobenius F_p est contenue dans X. Alors P_X a pour densité naturelle $|X|/|G|$.*

> ***Remarque 5.***
> Notons que ce théorème ressemble au théorème de la progression arithmétique de Dirichlet. Sa démonstration utilise d'ailleurs les mêmes outils analytiques.

Corollaire 4.3. — *Soit L une extension galoisienne infinie de $\mathbb{Q}$ non ramifiée en dehors d'un ensemble fini S. Alors*

(i) *Les éléments de Frobenius des places non ramifiées de L sont denses dans* $\mathrm{Gal}(L/K)$.
(ii) *Soit $X \subset \mathrm{Gal}(L/K)$ stable par conjugaison. Si $\mu(\partial X) = 0$ (μ étant la mesure de Haar normalisée de G), alors l'ensemble des places $p \notin S$ tels que $F_p \subset X$ a pour densité $\mu(X)$.*

Démonstration. — Démontrons d'abord la seconde assertion. Soit $(L_n)_n$ une suite croissante d'extensions galoisiennes de $\mathbb{Q}$ dont la réunion vaut L et soit Y un ensemble mesurable. On note Y_n l'ensemble des restriction à L_n des éléments de Y et $\mu_n(Y) = |Y_n|/|\mathrm{Gal}(L_n/\mathbb{Q})|$. La suite $(\mu_n(Y))_n$ est décroissante car $\mu_n(Y) = \mu(Y^n)$ où Y^n est l'ensemble des prolongements d'éléments de Y_n à L. En effet, la restriction à L_n découpe $\mathrm{Gal}(L/\mathbb{Q})$ en un nombre fini $|\mathrm{Gal}(L_n/\mathbb{Q})|$ de classes ayant toutes même mesure. D'autre part, ces classes sont à la fois ouvertes et fermées dans $\mathrm{Gal}(L/\mathbb{Q})$.

Alors, si Y est fermé, $(Y^n)_n$ est une suite décroissante d'ouverts dont l'intersection est égale à Y car $(\mathrm{Gal}(L/L_n))_n$ est un système fondamental de voisinages de l'identité. Par régularité extérieure de μ, $\mu_n(Y) \to \mu(Y)$.

Soit maintenant X mesurable et stable par conjugaison tel que $\mu(\partial X) = 0$. Soit $d_{sup}(X) = \limsup \frac{|\{p \in \mathscr{P}_n | F_p \subset X\}|}{|\mathscr{P}_n|}$. Alors $\overline{X}$ est stable par conjugaison, et $d_{sup}(X) \leqslant d_{sup}(\overline{X}) \leqslant d_{sup}(\overline{X}_n)$, et ce pour tout n. D'après le théorème de Čebotarev, $d_{sup}(\overline{X}_n) = \mu_n(\overline{X}) \to \mu(\overline{X}) = \mu(X)$. Par passage au complémentaire, $d_{inf}(X) \geqslant \mu(X)$.

La première assertion s'obtient à partir de la seconde appliquée à un voisinage d'une classe donnée de $\mathrm{Gal}(L/K)$.

□

4.2. Le théorème de Deligne. — On considère une forme parabolique de poids k, $f = \sum a_n q^n$ à coefficients entiers, normalisée, et qui soit fonction propre des opérateurs de Hecke T_p pour tout p premier. À cette forme parabolique, nous allons associer le polynôme $H_p(X) = 1 - a_p X + p^{k-1}X^2$ (apparu dans le cas particulier de Δ dans l'expression en produit infini de la série de Dirichlet associée à τ). Le résultat central de tout cet exposé relie ce polynôme à une action linéaire (ou représentation) d'un groupe de Galois sur un espace vectoriel ℓ-adique de dimension 2 :

***Théorème 4.4* (Deligne).** — *Pour tout nombre premier ℓ, il existe une représentation continue $\rho_\ell : \mathrm{Gal}(K_\ell/\mathbb{Q}) \to \mathrm{Aut}(V_\ell)$, où V_ℓ est un $\mathbb{Q}_\ell$-espace vectoriel de dimension 2, et satisfaisant à la condition suivante :*

$$\forall\, p \neq \ell,\ p \text{ premier, on a :} \quad \mathrm{Tr}(\rho_\ell(F_p)) = a_p \quad \text{et} \quad \det(\rho_\ell(F_p)) = p^{k-1}.$$

Remarquons tout de suite qu'imposer des valeurs à la trace et au déterminant de l'image du Frobenius est licite car ces deux opérateurs sont invariants par similitude, et on sait que le Frobenius est défini à conjugaison près. D'autre part, on peut reformuler la condition précédente par la condition, pour tout nombre premier $p \neq \ell$, que le polynôme $\det(1 - \rho_\ell(F_p)X)$ soit égal à $H_p(X)$.

D'autre part, même si le théorème semble très général, l'hypothèse d'intégralité de la forme modulaire est très forte, et en fait, on ne connaît que six exemples de telles formes modulaires, correspondant aux six valeurs de k pour lesquelles la dimension de l'espace des formes paraboliques de poids k est 1, *ie* $k \in \{12, 16, 18, 20, 22, 26\}$. En effet, une telle forme parabolique est alors automatiquement fonction propre des opérateurs de Hecke. Le cas qui nous intéresse est celui où $k = 12$, correspondant à la fonction Δ.

Donnons maintenant quelques conséquences faciles de ce théorème, avant d'aborder la partie suivante réservée aux applications plus profondes.

Le groupe $\mathrm{Gal}(K_\ell/\mathbb{Q})$ agit naturellement sur les racines ℓ^n-ièmes de l'unité, et on obtient ainsi une représentation ℓ-adique de degré 1 $\chi_\ell : \mathrm{Gal}(K_\ell/\mathbb{Q}) \to \mathbb{Z}_\ell^\times = \varprojlim \mu_{\ell^n}$, appelée aussi caractère ℓ-adique cyclotomique. Sachant que $\chi_\ell(F_p) = p$, et que les F_p sont denses dans $\mathrm{Gal}(K_\ell/\mathbb{Q})$, on obtient la formule : $\det(\rho_\ell) = \chi_\ell^{k-1}$.
D'autre part, le théorème de Kronecker-Weber donnant l'isomorphisme $\mathrm{Gal}(K_\ell/\mathbb{Q})^{\mathrm{ab}} \simeq \mathbb{Z}_\ell^\times$ implique que $\chi_\ell \mod \ell$ engendre $\mathrm{Hom}(\mathrm{Gal}(K_\ell/\mathbb{Q}), \mathbb{F}_\ell^\times)$.

On peut se demander pourquoi on choisit de regarder des représentations ℓ-adiques plutôt que des représentations complexes pour lesquelles on possède de nombreux outils, $G = \mathrm{Gal}(K_\ell/\mathbb{Q})$ étant compact. Intuitivement, c'est parce que $\mathbb{Q}_\ell$ a une topologie proche de celle de G. De manière plus concrète, l'existence d'un voisinage de l'identité dans $\mathrm{GL}_n(\mathbb{C})$ ne contenant pas de sous-groupes non triviaux montre que toute représentation complexe de dimension finie de G se factorise par un $\mathrm{Gal}(K/\mathbb{Q})$ où K est un corps de nombres. En particulier, l'image de la représentation est finie, au contraire de χ_ℓ, pourtant de degré 1.

Ainsi, la donnée d'une représentation ℓ-adique fournit beaucoup d'information, et afin de l'utiliser au maximum, une des choses à faire est de regarder ses réductions modulo ℓ^n. C'est le lemme suivant qui nous autorise à le faire, même si en réalité, c'est un faux problème dans notre cas car la théorème de Deligne construit une représentation qui est directement à valeurs dans $\mathrm{GL}_2(\mathbb{Z}_\ell)$:

Lemme 4.5. — *Pour tout sous-groupe compact G de $\mathrm{Aut}(V_\ell)$, il existe un $\mathbb{Z}_\ell$-réseau de V_ℓ stable par G.*

Démonstration. — Soit Γ un réseau quelconque de V_ℓ. Le stabilisateur H de Γ pour l'action de G est un sous-groupe ouvert de G (g stabilise Γ si et seulement si les coefficients de la matrice de g dans une $\mathbb{Z}_\ell$-base de Γ ont une valuation ℓ-adique > -1). Par conséquent, G/H, muni de la topologie quotient, est discret, et puisque G est quasi-compact, G/H également. Il en résulte que G/H est fini. Soit donc $\{\Gamma_1, \dots \Gamma_n\}$ l'orbite de Γ sous l'action de G. En posant $R = \sum_{1 \leqslant i \leqslant n} \Gamma_i$, R est un réseau de V_ℓ (c'est un sous-$\mathbb{Z}_\ell$-module de type fini de V_ℓ contenant une paire de vecteurs libre) stable par G. □

Ainsi, on notera $\rho_{l,n} : \mathrm{Gal}(K_\ell/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$ (ou $\tilde{\rho_\ell}$ lorsque $n = 1$), et les égalités vérifiées par les $\rho_\ell(F_p)$ se transposent de manière évidente en congruences modulo l^n.

Exemple 4.6. — Regardons ce que l'on obtient si on prend $\ell = 23$ et $n = 1$. On note E le corps de décomposition sur $\mathbb{Q}$ du polynôme $x^3 - x - 1$. C'est une extension galoisienne de $\mathbb{Q}$ qui ne se ramifie qu'en 23 (en effet, $(1, x, x^2)$ est une base de E, donc le discriminant de l'extension vaut $-4.(-1)^3 - 27.(-1)^2 = -23$), et dont le groupe de Galois est $\mathfrak{S}_3$ tout entier. Si r désigne la représentation standard de $\mathfrak{S}_3$, on sait qu'elle est irréductible de degré 2, et son caractère $\chi_r(\sigma)$ vaut $0, 2$ ou -1 selon que σ est d'ordre $2, 1$ ou 3. Par maximalité de K_{23}, r peut être vue comme représentation de $\mathrm{Gal}(K_{23}/\mathbb{Q})$. On peut alors montrer que la fonction τ vérifie des propriétés de congruence modulo 23 qui garantissent que ρ_{23} et r ont même polynôme caractéristique modulo 23. Par irréductibilité de r modulo 23, on en déduit : $\rho_{23,1} \equiv r \bmod 23$.

4.3. Représentations galoisiennes attachées à des courbes elliptiques. — Bien que la démonstration de ce théorème de Deligne soit hors de notre portée, celle-ci est « similaire » à la construction d'une représentation galoisienne attachée à une courbe elliptique, qu'il est donc intéressant de citer.

Soit E une courbe elliptique sur $\mathbb{Q}$, c'est-à-dire une variété projective régulière définie par une équation de la forme $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$, où quitte à faire un changement de variable, les a_i sont entiers. La régularité peut se vérifier par la non-annulation d'un polynôme Δ en les coefficients. Les points de E sont les solutions de cette équation dans $P^2(\overline{\mathbb{Q}})$.

E peut être munie d'une structure de groupe : on note $Div(E)$ le groupe abélien libre (formellement) engendré par ses points, $Div^0(E)$ le sous-groupe formé des $\sum_{P\in E} n_p(P)$ tels que $\sum_{P\in E} n_P = 0$, et $Pic^0(E)$ le quotient de $Div^0(E)$ par le sous-groupe des diviseurs principaux (si f est une fonction rationnelle sur E, $div(f) = \sum_{P\in E}$ ordre d'annulation de f en $P \in Div^0(E)$ est appelé diviseur principal) ; on a alors une bijection entre l'ensemble des points de E et $Pic^0(E)$, donnée par $P \mapsto [(P) - (O)]$ où (O) est le point $[0, 1, 0]$. Géométriquement, la loi de groupe se visualise de la façon suivante : si $P, Q \in E$, soit R le troisième point d'intersection de la droite PQ avec E (on compte ici les points avec leur multiplicité, donc d'après le théorème de Bézout la droite PQ intersecte E en exactement trois points), alors $P + Q$ est le troisième point d'intersection de la droite OR. Ceci montre que E est un groupe algébrique, et même que la loi de groupe et le passage à l'inverse sont donnés par des fractions rationnelles à coefficients dans $\mathbb{Q}$.

Le sous-groupe de m-torsion de E est isomorphe à $(\mathbb{Z}/m\mathbb{Z})^2$, donc en particulier le sous-groupe de ℓ^n-torsion est isomorphe à $(\mathbb{Z}/\ell^n\mathbb{Z})^2$. Le groupe $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ agit naturellement sur les points de E (puisque l'équation a ses coefficients dans $\mathbb{Q}$), et laisse ces sous-groupes stables (puisque la loi de groupe s'écrit avec des fractions rationnelles à coefficients dans $\mathbb{Q}$). De plus, cette action est compatible avec l'application de multiplication par ℓ allant du sous-groupe de ℓ^{n+1}-torsion dans le sous-groupe de ℓ^n-torsion et commmute à l'action de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ agit donc sur la limite projective de ces sous-groupes, c'est-à-dire $\mathbb{Z}_\ell^2$, et cette action est linéaire et continue.

On a donc défini une représentation ℓ-adique de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

On peut montrer que si la réduction modulo p de E est encore une courbe elliptique (c'est-à-dire si elle reste régulière, ce que l'on détermine à l'aide de Δ), alors cette représentation est non ramifiée en p, et l'image de F_p vérifie une équation du même type que celle du théorème de Deligne.

5. Applications à la fonction τ

5.1. Densité des nombres premiers annulant τ. — Lehmer a conjecturé que la fonction τ ne s'annulait pas sur l'ensemble des nombres premiers. Les congruences du théorème 2.7 montrent que la densité des nombres premiers p annulant τ est inférieure à 10^{-12}, et les essais numériques confortent la conjecture. Cependant, l'existence de la représentation ρ_ℓ donne un résultat concret qui se rapproche du but :

Proposition 5.1. — *Soit K un corps de caractéristique 0 et $\Phi \in K[X,Y]$ non nul. Alors l'ensemble des p tels que $\Phi(p,\tau(p)) = 0$ a une densité nulle. En particulier, les nombres premiers p tels que $\tau(p) = 0$ ont une densité nulle.*

Avant de commencer la preuve, donnons un résultat purement algébrique qui nous sera utile :

Lemme 5.2. — *Soit K un corps de caractéristique 0, $a \in \mathbb{N} - \{0\}$ et $\Phi \in K[X,Y]$ non nul. Alors il existe $\Psi \in K[X,Y]$ tel que $\Psi(X^a, Y)$ soit un multiple de Φ.*

Démonstration. — Soit $f : K[X,Y] \to K[X,Y]$ le morphisme d'algèbre défini par $f(X) = X^a$ et $f(Y) = Y$, et I l'idéal engendré par Φ. On veut montrer que l'idéal $f^{-1}(I)$ est non nul. C'est évident si le degré en X de Φ est nul. Sinon, cela revient à montrer que f n'induit pas une injection de $K[X,Y]$ dans $K[X,Y]/I$. Or, si tel était le cas, on construirait une application linéaire injective $K(Y)[X] \to K(Y)[X]/I$, ce qui, pour des raisons de dimension, est impossible. □

On peut maintenant en venir à la démonstration de la proposition 5.1 :

Démonstration. — D'après le lemme 5.2, on peut se ramener au cas où Φ est de la forme $\Psi(X^{11}, Y)$, avec $\Psi \in \mathbb{Q}[X,Y]$. Soit ℓ un nombre premier, et $H_\ell = \mathrm{Im}(\rho_\ell)$, considéré comme sous-groupe de $\mathrm{GL}_2(\mathbb{Q}_\ell)$. Serre a montré ([**Ser68**], V.1) que H_ℓ est ouvert dans $\mathrm{GL}_2(\mathbb{Q}_\ell)$. Soit alors X l'ensemble des $s \in H_\ell$ tels que $\Psi(\det(s), \mathrm{Tr}(s)) = 0$. L'équation précédente suffit à garantir que X est une hypersurface d'intérieur vide dans la variété ℓ-adique H_ℓ. Dès lors, si μ est la mesure de Haar de H_ℓ, on a $\mu(X) = 0$. Alors, le théorème de Čebotarev montre que l'ensemble des p tels que $F_p \in X$ est de densité nulle. □

5.2. Absence de congruences et indépendance des divers nombres premiers. — Le résultat principal de cette partie est la proposition 5.4 qui sera cruciale pour la partie à venir, car elle permet de reconnaître des situations où toute congruence est impossible. Avant de l'énoncer, énonçons un lemme sur les racines de l'unité ℓ-adiques :

Lemme 5.3. — *Soient $n \in \mathbb{N} - \{0\}$ et ℓ un nombre premier. Alors l'équation $x^n = 1$ possède $\mathrm{pgcd}(n, \ell - 1)$ solutions dans $\mathbb{Z}_\ell^\times$ si $\ell \geqslant 3$, et $\mathrm{pgcd}(n, 2)$ si $\ell = 2$.*

Démonstration. — Cela découle de la structure du groupe $\mathbb{Z}_\ell^\times$:

$$\mathbb{Z}_\ell^\times = \varprojlim_n (\mathbb{Z}/\ell^n\mathbb{Z})^\times \simeq \mathbb{Z}_\ell \times \mathbb{Z}/(\ell-1)\mathbb{Z}$$

pour $\ell \geqslant 3$, et de même $\mathbb{Z}_2^\times \simeq \mathbb{Z}_2 \times \mathbb{Z}/2\mathbb{Z}$. □

Proposition 5.4. — *Supposons que l'image de ρ_ℓ contienne $\mathrm{SL}_2(\mathbb{Z}_\ell)$, et fixons deux ouverts non vides A et B de $\mathbb{Z}_\ell$ et $\mathbb{Z}_\ell^\times$ respectivement. Alors l'ensemble $\{p \in \mathscr{P} | (a_p, p) \in A \times B\}$ a une densité > 0.*

Démonstration. — Tout d'abord, on va montrer que l'image de l'application $\Psi = (\rho_\ell, \chi_\ell)$ contient $\mathrm{SL}_2(\mathbb{Z}_\ell) \times \{1\}$. Or, pour $\ell > 3$, le groupe dérivé de $\mathrm{SL}_2(\mathbb{F}_\ell)$ est $\mathrm{SL}_2(\mathbb{F}_\ell)$ tout entier, donc le résultat en découle par le lemme 6.4. Quant au cas $\ell \in \{2, 3\}$, il provient du fait qu'il n'y a pas dans $\mathbb{Z}_\ell$ de racines $(k-1)$-ièmes de l'unité non triviales par le lemme 5.3 (k est pair), et que pour $\sigma \in \mathrm{Gal}(K_\ell/\mathbb{Q})$ vérifiant $\rho_\ell(\sigma) \in \mathrm{SL}_2(\mathbb{Z}_\ell)$, on a $\chi_\ell(\sigma)^{k-1} = 1$. En effet, on a dès lors $\chi_\ell(\sigma) = 1$.
D'autre part, $\mathbb{Z}$ est dense dans $\mathbb{Z}_\ell$, et $\det(\rho_\ell(\mathrm{Gal}(K_\ell/\mathbb{Q})))$ contient $\{n^{k-1} | n \in \mathbb{Z} - \{0\}\}$ (il contient 1, tous les p^{k-1} est est stable par multiplication) et est fermé dans $\mathbb{Z}_\ell^\times$, donc contient $\{n^{k-1} | n \in \mathbb{Z}_\ell - \{0\}\}$. Ainsi, l'image de Ψ est $\{(\alpha, \beta) \in \mathrm{GL}_2(\mathbb{Z}_\ell) \times \mathbb{Z}_\ell | \det \alpha = \beta^{k-1}\}$. Enfin, comme $\begin{pmatrix} a & b \\ -1 & 0 \end{pmatrix}$ est de trace a et de déterminant b, il existe dans $\mathrm{GL}_2(\mathbb{Z}_\ell)$ des matrices de déterminant dans $\mathbb{Z}_\ell^\times$ et de trace dans $\mathbb{Z}_\ell$ donnés, et on en déduit alors que $\Phi = (\mathrm{tr} \circ \rho_\ell, \chi_\ell) : \mathrm{Gal}(K_\ell/\mathbb{Q}) \to \mathbb{Z}_\ell \times \mathbb{Z}_\ell^\times$ est surjective. Or, comme $\Phi(F_p) = (a_p, p)$ et que les F_p sont distribués uniformément dans $\mathrm{Gal}(K_\ell/\mathbb{Q})$, la proposition s'en déduit. □

Corollaire 5.5. — *Si ℓ n'est pas exceptionnel, alors $a_p \mod \ell^n$ est indépendant de $p \mod \ell^n$.*

D'autre part, le théorème de Čebotarev montre immédiatement que l'ensemble des nombres premiers $p \neq \ell$ tels que a_p soit congru à un entier a donné modulo ℓ^n a une densité, qui par ailleurs est > 0 dès que l'ensemble en question est non vide.

Proposition 5.6. — *Les valeurs de $\tau(p)$ modulo 2^a, 3^b ... sont indépendantes : si la densité des p tels que $\tau(p) \equiv a_i \mod \ell_i^{n_i}$ est d_i, alors celle des p vérifiant toutes ces conditions est le produit des d_i.*
Si $\mathrm{pgcd}(m, n) = 1$, la valeur de $p \mod m$ n'implique rien sur la valeur de $\tau(p) \mod n$.

Démonstration. — Soient $K_1, \ldots, K_n$ les extensions galoisiennes finies de $\mathbb{Q}$, avec K_i non ramifiée en dehors de ℓ_i (les ℓ_i étant distincts), qui correspondent aux noyaux des réductions modulo $\ell_i^{n_i}$ de ρ_{ℓ_i}. Comme $K_1 \ldots K_k \cap K_{k+1} = \mathbb{Q}$ pour tout k (c'est une extension finie de $\mathbb{Q}$, donc si elle est distincte de $\mathbb{Q}$ elle est ramifiée en au moins un nombre premier ℓ, et ℓ doit donc être égal à ℓ_{k+1} et appartenir à $\{\ell_1, \ldots, \ell_k\}$, contradiction), $\mathrm{Gal}(K_1 \ldots K_n/\mathbb{Q})$ s'identifie canoniquement au produit des $\mathrm{Gal}(K_i/\mathbb{Q})$ par restriction, et le théorème de

Čebotarev permet de conclure.
Pour la seconde partie, on regarde également χ_l. □

PARTIE III
CONGRUENCES DE LA FONCTION τ

Avant de commencer, nous allons donner le fil directeur de cette partie. L'idée est de déterminer quelles congruences sur la fonction τ on peut obtenir, mais aussi de savoir lorsqu'il n'en existe pas. Pour cette tâche, le système de représentations (ρ_ℓ) s'avère être un outil extrêmement puissant. En effet, ces dernières transposent toute la complexité de la fonction τ, appartenant au « monde modulaire », dans le « monde linéaire » bien mieux connu. La majeure partie du travail va consister à déterminer le mieux possible l'image de chacune de ses représentations ; si cette dernière est suffisamment grosse, aucune congruence n'est possible, mais sinon, nous pourrons deviner plusieurs types de congruences.
Ajoutons enfin que les congruences que nous établirons seront principalement modulo des nombres premiers, car les congruences modulo des puissances de nombres premiers sont plus délicates à démontrer.

6. Images possibles de ρ_ℓ

6.1. Sous-groupes de $\mathrm{GL}_2(\mathbb{F}_\ell)$. — La classification des sous-groupes de $\mathrm{GL}_2(\mathbb{F}_\ell)$ est en réalité assez fastidieuse, donc nous n'allons donner que les résultats majeurs tirés de [**SD73**] II, pp.12-15, que nous utiliserons dès la partie suivante.

Définition 6.1. — On appelle sous-groupe de Borel de $\mathrm{GL}_2(\mathbb{F}_\ell)$ un sous-groupe conjugué à l'ensemble des matrices triangulaires supérieures.

On a appelle sous-groupe de Cartan de $\mathrm{GL}_2(\mathbb{F}_\ell)$ un sous-groupe abélien maximal de celui-ci.

> ***Remarque 6.***
> Un sous-groupe de Cartan est conjugué dans $\mathrm{GL}_2(\mathbb{F}_{\ell^2})$ au sous-groupe des matrices diagonales. Ceci revient à dire qu'un sous-groupe de Cartan est décrit par deux droites distinctes de $\mathbb{F}_{\ell^2}^2$, ses éléments fixant ces deux droites. Le normalisateur d'un sous-groupe de Cartan est donc constitué du sous-groupe de Cartan lui-même ainsi que des morphismes échangeant ces deux droites.

Théorème 6.2. — *Soit G un sous-groupe de $\mathrm{GL}_2(\mathbb{F}_\ell)$. Si l'ordre de G est divisible par ℓ, alors soit G est contenu dans un sous-groupe de Borel de $\mathrm{GL}_2(\mathbb{F}_\ell)$, soit G contient $\mathrm{SL}_2(\mathbb{F}_\ell)$.*

Théorème 6.3. — *Soit G un sous-groupe de $\mathrm{GL}_2(\mathbb{F}_\ell)$, d'ordre premier avec ℓ. Si PG est l'image de G dans $\mathrm{PGL}_2(\mathbb{F}_\ell)$, alors seuls les trois cas suivants sont possibles :*

(i) *PG est cyclique et G est contenu dans un sous-groupe de Cartan.*

(ii) *PG est dihédral, et G est contenu dans le normalisateur d'un sous-groupe de Cartan, mais pas dans le sous-groupe de Cartan.*
(iii) *PG est isomorphe à $\mathfrak{A}_4$, $\mathfrak{S}_4$, ou $\mathfrak{A}_5$.*

6.2. Image de la représentation ρ_ℓ et congruences. — Une chose importante est que, les éléments de Frobenius étant denses dans $\mathrm{Gal}(K_\ell/\mathbb{Q})$, toute relation entre a_p et p^{k-1} est encore valide entre la trace et le déterminant de chaque élément de l'image de ρ_ℓ. Donc si l'image de $\mathrm{Gal}(K_\ell/\mathbb{Q})$ contient $\mathrm{SL}_2(\mathbb{Z}_\ell)$, elle sera égale à tout $\mathrm{GL}_2(\mathbb{Z}_\ell)_k = \{M \in \mathrm{GL}_2(\mathbb{Z}_\ell) \mid \det(M) \in \mathbb{Z}_\ell^{k-1}\}$, et alors il n'existera aucune congruence en vertu de la propostion 5.4. Cependant, $\mathbb{Z}_\ell$ est un objet assez compliqué, et il serait agréable de pouvoir se ramener à une situation bien connue qui est celle de $\mathbb{F}_\ell$. Dans notre cas, c'est presque toujours possible d'après le lemme suivant :

Lemme 6.4. — *Supposons que $\ell > 3$, et que G est un sous-groupe fermé de $\mathrm{GL}_2(\mathbb{Z}_\ell)$. Si l'image de G par réduction modulo ℓ contient $\mathrm{SL}_2(\mathbb{F}_\ell)$, alors G contient $\mathrm{SL}_2(\mathbb{Z}_\ell)$.*

Démonstration. — Puisque G est fermé, il suffit de montrer que pour tout $n \geqslant 1$, l'image G_n de G dans $\mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$ contient $\mathrm{SL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$. Procédons par récurrence sur n.

Soit $n \geqslant 2$, et supposons que $\mathrm{SL}_2(\mathbb{Z}/\ell^{n-1}\mathbb{Z}) \subset G_{n-1}$. Pour montrer que $\mathrm{SL}_2(\mathbb{Z}/\ell^n\mathbb{Z}) \subset G_n$, il suffit d'établir que le noyau H_n de $\mathrm{SL}_2(\mathbb{Z}/\ell^n\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/\ell^{n-1}\mathbb{Z})$ est inclus dans G_n. Les éléments de H_n sont de la forme $I+\ell^{n-1}u$ où u est à coefficients dans $\mathbb{Z}/\ell\mathbb{Z}$, et pour que le déterminant soit égal à 1 il est nécessaire et suffisant que u soit de trace nulle. De plus $(I+\ell^{n-1}u)(I+\ell^{n-1}v) \equiv I+\ell^{n-1}u+\ell^{n-1}v \mod \ell^n$ car $n \geqslant 2$. H_n est donc naturellement isomorphe au sous-groupe additif de $\mathcal{M}_2(\mathbb{Z}/\ell\mathbb{Z})$ des matrices de trace nulle.

H_n est donc engendré par $I+\ell^{n-1}u$ avec $u = \begin{pmatrix}0&1\\0&0\end{pmatrix}, \begin{pmatrix}0&0\\1&0\end{pmatrix}$ et $\begin{pmatrix}1&-1\\1&-1\end{pmatrix}$, qui sont toutes les trois nilpotentes. Montrons que G_n contient ces trois éléments. $I+\ell^{n-2}u \in \mathrm{SL}_2(\mathbb{Z}/\ell^{n-1}\mathbb{Z})$, donc il existe un élément x de G tel que $x \equiv I+\ell^{n-2}u \mod \ell^{n-1}$, donc $x = I+\ell^{n-2}u+\ell^{n-1}v$ avec v à coefficients dans $\mathbb{Z}_\ell$. Alors :

$$\begin{aligned} x^\ell &= (I+\ell^{n-2}u+\ell^{n-1}v)^\ell \\ &= \sum_{0\leqslant k\leqslant \ell} C_\ell^k(\ell^{n-2}u+\ell^{n-1}v)^k \\ &\equiv I + \sum_{1\leqslant k\leqslant \ell-1} C_\ell^k(\ell^{n-2}u)^k + (\ell^{n-2}u+\ell^{n-1}v)^\ell \mod \ell^n \\ &\equiv I+\ell^{n-1}u \mod \ell^n \end{aligned}$$

car pour $1 \leqslant k \leqslant \ell-1$, l divise C_ℓ^k donc seul le terme $(\ell^{n-2}u)^k$ du développement de $(\ell^{n-2}u+\ell^{n-1}v)^k$ peut donner un résultat non nul modulo ℓ^n, $u^2=0$ et dans le développement de $(\ell^{n-2}u+\ell^{n-1}v)^\ell$, tous les termes sont nuls modulo ℓ^n vu qu'ils contiennent tous u^2 ou deux fois $\ell^{n-1}v$ (ici l'hypothèse $\ell > 3$ est utilisée).

Donc $I + \ell^{n-1}u \in G_n$. □

Évidemment, nous utiliserons ce lemme avec $G = \operatorname{Im}\rho_\ell$, qui est compact donc fermé. On dira alors que ℓ est un *nombre premier exceptionnel* pour la forme parabolique en question si l'image de ρ_ℓ ne contient pas $\mathrm{SL}_2(\mathbb{Z}_\ell)$. Le corollaire suivant répond à notre premier problème :

Corollaire 6.5. — *Supposons $\ell > 3$; alors ℓ est exceptionnel si et seulement si l'image de $\tilde{\rho}_\ell$ ne contient pas $\mathrm{SL}_2(\mathbb{F}_\ell)$.*

Dans toute la suite, on notera de la même manière ρ_ℓ et $\tilde{\rho}_\ell$ par la première expression.

Théorème 6.6. — *Si $G = \operatorname{Im}\rho_\ell$ ne contient pas $\mathrm{SL}_2(\mathbb{F}_\ell)$, alors on est dans l'un des cas suivants :*

(i) *$G \subset$ Borel.*
(ii) *$G \subset$ Normalisateur d'un Cartan mais pas dans le Cartan.*
(iii) *$PG \simeq \mathfrak{S}_4$.*

En d'autres termes, G ne peut pas être contenu dans un sous-groupe de Cartan non déployé sans être aussi contenu dans un Borel, et les cas exceptionnels $PG \simeq \mathfrak{A}_4$ ou $\mathfrak{A}_5$ ne se produisent pas.

Démonstration. — Supposons que $G \subset C$ où C est un Cartan non déployé. Comme C est abélien, ρ_ℓ se factorise à travers $\mathrm{Gal}(K_\ell/\mathbb{Q})^{ab} \simeq \mathbb{Z}_\ell^\times$. De plus l'ordre de C, donc de G, est premier avec ℓ. Ainsi, G s'identifie à un quotient fini de $\mathbb{Z}_\ell^\times$, donc il existe un entier n tel que G se réalise dans $(\mathbb{Z}/\ell^n\mathbb{Z})^\times$ qui est de cardinal $\ell^{n-1}(\ell-1)$. On en déduit que $|\mathrm{G}|$ divise $\ell - 1$. Or C est cyclique d'ordre $\ell^2 - 1$, et $(\ell+1) \wedge (\ell-1) = 2$. Donc G est contenu dans le sous-groupe de C de cardinal $\ell - 1$ constitué des matrices scalaires, donc G est contenu dans un Borel.
Il reste à montrer que PG ne peut-être ni $\mathfrak{A}_4$ ni $\mathfrak{A}_5$, pour quels cas on peut supposer $\ell \neq 2$. Considérons le diagramme commutatif suivant :

$$\begin{array}{ccccc} \mathrm{Gal}(K_\ell/\mathbb{Q}) & \twoheadrightarrow & G & \xrightarrow{\det\rho_\ell} & \mathbb{F}_\ell^\times \\ & & \downarrow & & \downarrow \\ & & PG & \twoheadrightarrow & \mathbb{F}_\ell^\times/(\mathbb{F}_\ell^\times)^2 \end{array}$$

Par le théorème de la progression arithmétique, l'image de G dans $\mathbb{F}_\ell^\times$ contient toutes les puissances $(k-1)$-ièmes. Comme k est pair, l'application $G \to \mathbb{F}_\ell^\times/(\mathbb{F}_\ell^\times)^2$ est surjective, donc $PG \to \mathbb{F}_\ell^\times/(\mathbb{F}_\ell^\times)^2$ l'est aussi. Ainsi, PG possède un sous-groupe d'indice 2, ce qui n'est pas le cas de $\mathfrak{A}_4$ et $\mathfrak{A}_5$. □

Théorème 6.7. — *Dans chacune des trois situations du théorème 6.6, on a les congruences respectives, valables pour tout $p \neq \ell$:*

(i) *Il existe $m \in \mathbb{N}$ tel que $a_p \equiv p^m + p^{k-1-m} \mod \ell$.*
(ii) $a_p \equiv 0 \mod \ell$ *si* $\left(\frac{p}{\ell}\right) = -1$.
(iii) $p^{1-k}a_p^2 \equiv 0, 1, 2$ ou $4 \mod \ell$.

Démonstration. — Commençons par le premier cas. Quitte à changer de base, il existe deux caractères ψ et ψ' de $\mathrm{Gal}(K_\ell/\mathbb{Q})$ tels que :

$$\rho_\ell = \begin{pmatrix} \psi & * \\ 0 & \psi' \end{pmatrix}.$$

Comme ψ est à valeurs dans $\mathbb{F}_\ell^\times$, il existe un entier m tel que $\psi(p) \equiv p^m \mod \ell$. On raisonne de même avec ψ', qui donne un entier m'. La condition sur le déterminant impose alors que $m + m' \equiv k - 1 \mod \ell - 1$.
Pour le cas (ii), on a $\ell \neq 2$. Considérons alors l'homomorphisme

$$\mathrm{Gal}(K_\ell/\mathbb{Q}) \to N \to N/C \simeq \{\pm 1\}.$$

Il est surjectif et d'image d'ordre 2, donc abélien. Donc il se factorise à travers $\mathbb{Z}_\ell^\times$, et même à travers $\mathbb{Z}_\ell^\times/(\mathbb{Z}_\ell^\times)^2$, qui est d'ordre 2 (en effet, $\forall \ell \neq 2, \forall n \in \mathbb{N} - \{0\}$, on a $\left|\{x \in (\mathbb{Z}/p^n\mathbb{Z})^\times \mid x^2 = 1\}\right| = 2$). Ainsi,

$$\begin{aligned} \rho_\ell(F_p) \in C &\iff \left(\frac{p}{\ell}\right) = 1 \\ \rho_\ell(F_p) \in N - C &\iff \left(\frac{p}{\ell}\right) = -1. \end{aligned}$$

Mais alors, si $\left(\frac{p}{\ell}\right) = -1$, $\rho_\ell(F_p)$ est équivalent sur $\mathbb{F}_{\ell^2}$ à une matrice de diagonale nulle (car il permute les sous-espaces propres du Cartan) et donc $a_p = \mathrm{tr}(\rho_\ell(F_p)) = 0$.
Enfin, pour le dernier cas, on commence par remarquer que tout élément de PG est d'ordre $1, 2, 3$ ou 4. Si d est l'ordre d'un élément $\sigma \in PG$ de valeurs propres α et β, alors

$$\sigma^d \sim \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} \text{ donc } \sigma \sim \begin{pmatrix} \alpha & * \\ 0 & \beta \end{pmatrix} \text{ sur } \overline{\mathbb{F}}_\ell,$$

où $\beta = \alpha\zeta$ et $\zeta^d = 1$. Alors $\frac{(\mathrm{tr}\,\sigma)^2}{\det \sigma} = \zeta^{-1} + 2 + \zeta$, et l'énumération des cas conclut.

□

Remarque 7.

Par le même genre d'argument que pour la preuve du point (ii), mais adapté au cas (iii), on peut montrer que l'image de $\rho_\ell(F_p) \notin \mathfrak{A}_4 \iff \left(\frac{p}{\ell}\right) = -1$. Ainsi, il existe une infinité de p premiers tels que $\rho_\ell(F_p)$ soit d'ordre 4, donc tels que p soit un non-résidu quadratique vérifiant $p^{1-k}a_p^2 \equiv 2 \mod \ell$.

Pour finir ce paragraphe, il reste à passer au cas des congruences pour n entier quelconque. Mais en fait, tout le travail est déjà fait vu que les formes modulaires auxquelles nous nous intéressons admettent un produit eulérien. Les fonctions $n \mapsto a_n$ et σ_q ayant des propriétés similaires, un calcul facile donne :

(i) Il existe un entier m tel que pour tout entier n premier à ℓ, on ait : $a_n \equiv n^m \sigma_{k-1-2m}(n) \mod \ell$.
(ii) $a_n \equiv 0 \mod \ell$ dès que n est un non-résidu quadratique modulo ℓ.

7. Congruences et réduction modulo ℓ des formes modulaires

On voudrait maintenant déterminer concrètement, pour chaque ℓ, quelle est l'image de la représentation ρ_ℓ. Comme nous avons en vue les congruences sur les coefficients des formes modulaires en question, on cherche à connaître les nombres premiers exceptionnels. Nous allons montrer un résultat très fort, qui affirme qu'ils sont en nombre fini. De plus, nous arriverons à majorer leur nombre, et, en guise d'exemple, nous les déterminerons explicitement pour la fonction τ. Une idée naturelle à avoir pour trouver des congruences sur les coefficients de formes modulaires, et à laquelle on aurait pu penser dès le début, est de réduire les formes modulaires en question modulo certains nombres premiers. C'est ce que nous allons faire maintenant, et ce sera la dernière étape pour la résolution du problème initial.

7.1. L'algèbre des formes modulaires modulo p. — Comme le titre l'indique déjà, nous allons un peu changer nos notations pour cette partie seulement, en notant p (et non plus ℓ) le nombre premier que l'on utilisera pour réduire. Précisons tout de suite qu'on appellera P, Q, et R les séries d'Eisenstein normalisées de poids $2, 4$ et 6 respectivement.

Soit donc $f = \sum_{n \geqslant 0} a_n q^n$, avec $a_n \in \mathbb{Q}$ une série formelle p-entière, *ie* $\forall n, v_p(a_n) \geqslant 0$. On note $\tilde{f} \in \mathbb{F}_p[[q]]$ sa réduction modulo p, et on désignera par $\widetilde{M_k}$ l'ensemble de $\tilde{f}$, où f parcourt M_k. Remarquons que P, Q, R et Δ sont à coefficients entiers, donc peuvent se réduire modulo tout nombre premier.

Définition 7.1. — La somme $\widetilde{M}$ des $\widetilde{M_k}$ est une sous-algèbre de $\mathbb{F}_p[[q]]$ appelée l'algèbre des formes modulaires modulo p.

On connaît déjà la structure de $M = \mathbb{C}[Q, R]$; on peut se demander ce qu'il en est de $\widetilde{M}$. Pour $p = 2, 3$ sa structure est très simple :

Proposition 7.2. — *Si $p = 2$ ou 3, $\widetilde{M} = \mathbb{F}_p[\widetilde{\Delta}]$ et $\widetilde{\Delta}$ est transcendant sur $\mathbb{F}_p$.*

Démonstration. — Si $f = \sum_{n \geqslant 0} a_n q^n$ est de poids $k \geqslant 4$ et est p-entière, il existe a et b tels que $4a + 6b = k$, donc $f - a_0 Q^a R^b$ est encore de poids k et est parabolique, donc $f = a_0 Q^a R^b + \Delta g$ où g est de poids $k - 12$. La série $g = \sum_{n \geqslant 0} b_n q^n$ est également p-entière,

car sinon en notant m le plus petit entier tel que $v_p(b_m) < 0$, $a_{m+1} - b_m$ est p-entier donc $v_p(a_{m+1}) < 0$. Il s'ensuit qu'on peut réduire g, et $\widetilde{f} = \widetilde{a_0}\widetilde{Q}^a\widetilde{R}^b + \widetilde{\Delta}\widetilde{g} = \widetilde{a_0} + \widetilde{\Delta}\widetilde{g}$ car $\widetilde{Q} = \widetilde{R} = 1$. Par récurrence sur le poids, on en déduit que $\widetilde{M} \subset \mathbb{F}_p[\widetilde{\Delta}]$ et il y a égalité puisque $\widetilde{\Delta} \in \widetilde{M}$.

Enfin, $\widetilde{\Delta}$ est transcendant sur $\mathbb{F}_p$ car si $a_0, a_r \neq 0$, le coefficient de q^r dans $a_0 + a_r\widetilde{\Delta}^r + \ldots + \widetilde{\Delta}^n$ est non nul. □

On suppose dans la suite que p est supérieur à 5.

Proposition 7.3. — *Une forme modulaire de poids k f est p-entière si et seulement si ses coefficients dans la base des Q^aR^b sont p-entiers.*

De plus, la famille des $\widetilde{Q}^a\widetilde{R}^b$ avec $4a + 6b = k$ est une base de $\widetilde{M}_k$.

Démonstration. — Q et R sont à coefficients entiers, donc Q^aR^b également et les combinaisons linéaires à coefficients p-entiers de ces monômes définissent donc des formes modulaires p-entières.

Réciproquement, si f est p-entière, $f = a_0Q^aR^b + \Delta g$ où g est p-entière comme on l'a vu dans la preuve précédente. Comme $\Delta = (Q^3 - R^2)/1728$ et $1728 = 2^63^3$, par récurrence sur k, f est combinaison linéaire à coefficients p-entiers des Q^aR^b.

Montrons par récurrence sur le poids que la famille des $\widetilde{Q}^a\widetilde{R}^b$ avec $4a + 6b = k$ est libre. Si $\widetilde{f} = \sum_i \widetilde{\alpha_i}\widetilde{Q}^{a_i}\widetilde{R}^{b_i} = 0$, $\sum_i \widetilde{\alpha_i} = 0$ donc en prenant a et b tels que $4a + 6b = k$, $f - (\sum_i \alpha_i)Q^aR^b = \Delta g$ où g est une forme modulaire de poids $k - 12$. En outre, $\widetilde{\Delta}\widetilde{g} = 0$, et comme $\mathbb{F}_p[[q]]$ est intègre et $\widetilde{\Delta} \neq 0$, $\widetilde{g} = 0$, ce qui donne une relation de liaison en poids strictement inférieur, donc par hypothèse de récurrence $g = \sum_j \beta_j Q^{c_j}R^{d_j}$ avec $v_p(\beta_j) > 0$. Donc $f = \Delta g + (\sum_i \alpha_i)Q^aR^b$ et comme les α_i sont déterminés par f, il sont de valuation p-adique strictement positive, *ie* $\widetilde{\alpha_i} = 0$ pour tout i. □

Corollaire 7.4. — *Si $\widetilde{f} \in \widetilde{M}_k$, il existe un unique polynôme isobare F de poids k tel que $\widetilde{f} = F(\widetilde{Q}, \widetilde{R})$.*

Déterminer la structure de $\widetilde{M}$ revient donc à déterminer l'idéal $\mathfrak{a} \subset \mathbb{F}_p[Q, R]$ des relations entre $\widetilde{Q}$ et $\widetilde{R}$, et ceci se fera à l'aide d'une dérivation sur $\widetilde{M}$. Nous avons besoin d'un résultat préliminaire, ce sont les congruences de Von Staudt et Kummer, dont la preuve peut être trouvée dans [**Lan76**] (X, §1-2) :

Proposition 7.5. — *Pour un nombre premier p et un entier n, on a les deux cas suivants :*

(i) *Si $(p-1)|2n$ alors $p\, b_{2n} \equiv -1 \mod p$.*
(ii) *Si $(p-1) \nmid 2n$ alors $b_{2n}/2n$ est p-intégral et sa classe modulo p ne dépend que de $2n \mod p-1$.*

Rappelons-nous que $P = E_2$ est presque une forme modulaire de poids 2, à cause de l'absolue convergence de la série qui fait défaut. Cependant, elle vérifie une équation fonctionnelle similaire à celles des formes modulaires car $P(-1/z) = z^2P(z) + \frac{12z}{2i\pi}$. Il n'y a donc pas de moyen agréable, du type multiplication par Δ, d'augmenter le poids d'une forme modulaire de 2. Cela justifie l'introduction d'un opérateur de dérivation sur M que l'on notera θ, défini par $\theta f = q\frac{df}{dq}$.

***Théorème 7.6* (Ramanujan).** — *Si $f \in M_k$, alors $\partial f = 12\theta f - kPf \in M_{k+2}$.*
De plus, on a les formules suivantes : $\theta P = \frac{1}{12}(P^2 - Q)$, $\theta Q = \frac{1}{3}(PQ - R)$ et $\theta R = \frac{1}{2}(PR - Q^2)$.

Démonstration. — La première assertion se montre en dérivant l'identité $f(-1/z) = z^k f(z)$ et en utilisant l'équation fonctionnelle de P. Ainsi $\theta Q - PQ/3$ est une forme modulaire de poids 6 dont le terme constant est $-1/3$, donc c'est $-R/3$. On raisonne de même pour les autres formules. □

Ainsi, ce théorème prouve l'existence d'une algèbre (celle engendrée par P, Q et R) qui contient E_2 et qui soit stable par θ.

> ***Remarque 8.***
> Ce théorème montre qu'on aurait pu définir la dérivation ∂ en lui imposant $\partial Q = -4R$ et $\partial R = -6Q^2$.

Définition 7.7. — On définit la dérivation ∂ sur $\mathbb{F}_p[Q, R]$ en posant $\partial Q = -4R$ et $\partial R = -6Q^2$.

On va maintenant revenir aux formes modulaires modulo p. La formule $12\theta f = k\widetilde{P}f + \partial f$ a encore un sens pour $f \in \widetilde{M}$ car θf est p-entière si f est p-entière, et $\widetilde{P} \in \widetilde{M}$ grâce au théorème qui suit. Le grand avantage de travailler modulo p est que dès lors, P devient une véritable forme modulaire modulo p, de poids $p + 1$:

Théorème 7.8. — *On a $1 \equiv E_{p-1} \mod p$ et $P \equiv E_{p+1} \mod p$. De plus, si A et B sont les polynômes isobares de poids $p-1$ et $p+1$ à coefficients dans $\mathbb{F}_p$ tels que $A(\widetilde{Q}, \widetilde{R}) = \widetilde{E}_{p-1}$ et $B(\widetilde{Q}, \widetilde{R}) = \widetilde{E}_{p+1}$, alors $\partial A = B$ et $\partial B = -QA$.*

Démonstration. — La première assertion découle du développement en série de $\widetilde{E}_{p-1}$ et $\widetilde{E}_{p+1}$ et des congruences de Von Staudt et Kummer, ainsi que du fait que $d^p \equiv d \mod p$ pour la seconde.

D'autre part, puisque $E_{p-1} \equiv 1 \mod p$, on a $\theta E_{p-1} \equiv 0 \mod p$, d'où $(p-1)\widetilde{P}\widetilde{E}_{p-1} + \partial A(\widetilde{Q}, \widetilde{R}) = 0$, *ie* $\partial A(\widetilde{Q}, \widetilde{R}) = \widetilde{P} = \widetilde{E}_{p-1} = B(\widetilde{Q}, \widetilde{R})$ ce qui démontre la première formule. La deuxième se prouve par un argument analogue, en dérivant une nouvelle fois. □

Théorème 7.9. — *L'idéal $\mathfrak{a}$ est l'idéal principal engendré par $A - 1$.*

Démonstration. — On sait déjà que $A-1 \in \mathfrak{a}$. Comme l'anneau des séries formelles sur $\mathbb{F}_p$ est intègre, $\mathfrak{a}$ est un idéal premier de $\mathbb{F}_p[Q,R]$. L'anneau $\mathbb{F}_p[Q,R]$ a pour dimension 2, et est factoriel, donc $\mathfrak{a}$ est maximal ou engendré par un élément irréductible (il est non nul car $A-1 \neq 0$). Si $\mathfrak{a}$ était maximal, $\widetilde{Q}$ et $\widetilde{R}$ seraient algébriques sur $\mathbb{F}_p$, ce qui est impossible car leurs coefficients en q sont $240 = 2^4 \times 3 \times 5$ et $-504 = -2^4 \times 29$, donc l'un des deux est non nul modulo p, par le même argument que pour $\widetilde{\Delta}$

Il reste donc à vérifier que $A-1$ est irréductible. Commençons par montrer que A ne contient pas de facteur carré.

Cherchons la forme possible des diviseurs irréductibles de A dans $\overline{\mathbb{F}}_p[Q,R]$ Introduisons les lettres Z et T telles que $Q = Z^2$ et $R = T^3$. A est donc un polynôme en Z^2 et T^3, homogène en Z,T. Les facteurs irréductibles de A dans $\overline{\mathbb{F}}_p[Z,T]$ sont homogènes, donc de la forme T ou $Z-\lambda T$ avec $\lambda \in \overline{\mathbb{F}}_p$. Si $Z-\lambda T$ divise A, comme $A(-Z,T) = A(Z,T)$ et $Z-\lambda T$ et $Z+\lambda T$ sont premiers entre eux ($p \neq 2$), $Z^2-\lambda^2 T^2$ divise A. De même, en notant j une racine troisième $\neq 1$ de l'unité dans $\overline{F}_p$ ($p \neq 3$), comme $A(Z,T) = A(Z,jT) = A(Z,j^2T)$ et puisque les polynômes $Z^2-\lambda^2T^2$, $Z^2-\lambda^2 j^2T^2$ et $Z^2-\lambda^2 jT^2$ sont deux à deux premiers entre eux, $Z^6-\lambda^6T^6$ divise A. Il s'ensuit que les facteurs irréductibles de A dans $\overline{\mathbb{F}}_p[X,Y]$ sont de la forme Q, R ou $Q^3-\lambda R^2$ avec $\lambda \in \overline{\mathbb{F}}_p^\times$.

Si A est exactement divisible par $(Q^3-\lambda R^2)^n$ avec $n \geqslant 2$ et $\lambda \neq 0$, $\lambda \neq 1$ car $\widetilde{Q}^3-\widetilde{R}^2$ a un terme constant nul tandis que $A(\widetilde{Q},\widetilde{R})$ a pour terme constant 1. Donc $\partial(Q^3-\lambda R^2) = 12(\lambda-1)Q^2R$ est premier avec $Q^3-\lambda R^2$. A étant de poids $p-1$, $n<p$, donc $\partial A = B$ est exactement divisible par $(Q^3-\lambda R^2)^{n-1}$, et puisque $\partial B = -QA$, A est exactement divisible par $(Q^3-\lambda R^2)^{n-2}$, contradiction. Le cas de Q et R est similaire (et plus simple).

Si $P = P_n + \ldots + P_0$ avec $n < p-1$ est un facteur irréductible de $A-1$ dans $\overline{\mathbb{F}}_p[Q,R]$ (avec P_i isobare de poids i), alors $P(\lambda^4 Q, \lambda^6 R)$ (où λ est une racine primitive $(p-1)$-ième de l'unité) est également un facteur irréductible de $A-1$ premier à P car $n<p-1$ et $P_0 \neq 0$. Donc $P_n^2 | A$, contradiction. □

Ainsi $\widetilde{M} = \mathbb{F}_p[X,Y]/\mathfrak{a}$ est une algèbre graduée, de groupe des degrés $\mathbb{Z}/(p-1)\mathbb{Z}$ où l'élément $A-1$ est de poids 0. Alors, en notant $\widetilde{M}^\alpha$ la réunion croissante des $\widetilde{M}_k$ pour $k \equiv \alpha \mod p$, on a :

$$\widetilde{M} = \bigoplus_{\alpha \in \mathbb{Z}/(p-1)\mathbb{Z}} \widetilde{M}^\alpha.$$

En particulier, on peut parler du poids d'une forme modulaire modulo p, qui est défini modulo $p-1$. Cependant, on a vu à quel point l'existence d'un poids pour les formes modulaires était important, et on peut s'attendre à ce qu'il en soit de même pour les formes modulaires modulo p. C'est effectivement le cas, mais il est toujours gênant de traiter non pas avec des entiers mais avec des classes. C'est ce qui justifie l'introduction d'une filtration, que nous allons définir dans le paragraphe suivant.

Corollaire 7.10. — *Les polynômes A et B sont premiers entre eux.*

Démonstration. — Si F irréductible dans $\overline{\mathbb{F}}_p[Q,R]$ divise A, on a vu que ∂F et F sont premiers entre eux et F^2 ne divise pas A donc F ne divise pas $\partial A = B$. □

Définition 7.11. — Si $f \in \widetilde{M}$, on appelle filtration de f, et on note $w(f)$, le plus petit entier k tel que $f \in \widetilde{M}_k$. Si $f = 0$, on convient de $w(f) = -\infty$.

Le théorème 7.9 de structure de $\widetilde{M}$ montre que f est de filtration k si et seulement si f est de la forme $F(\widetilde{Q}, \widetilde{R})$ où F est un polynôme isobare de poids k, à coefficients dans $\mathbb{F}_p$, et non divisible par A.

Corollaire 7.12. — *On a $w(\theta f) \leqslant w(f) + p + 1$, l'égalité se produit si et seulement si $p \nmid w(f)$.*

Démonstration. — On pose $k = w(f)$, F le polynôme isobare de poids k tel que $f = F(\widetilde{Q}, \widetilde{R})$ et g une forme modulaire de poids k telle que $f = \widetilde{g}$. Alors on écrit : $12\theta g = kPg + \partial g$, et en réduisant modulo p, on obtient $12\theta f = kB(\widetilde{Q}, \widetilde{R})f + A(\widetilde{Q}, \widetilde{R})\partial f = \widetilde{h}$ avec $h = kE_{p+1}g + E_{p-1}\partial g$ de poids $p + 1 + k$. En passant aux filtrations, on a l'inégalité recherchée, et on a égalité si et seulement si $kBF + A\partial F$ n'est pas divisible par A. Comme B est premier à A et $A \nmid F$, la conclusion s'ensuit. □

Exemple 7.13. — Prenons $p = 5$ et $f = \widetilde{G}_6 = -\widetilde{R}$. Alors θf est modulaire modulo 5 de poids 12, et son développement commence par q. Donc $\theta f = \widetilde{\Delta}$, d'où la congruence $\tau(n) \equiv n\sigma_5(n) \mod 5$. Le même argument pour $p = 7$ montre que $\theta\widetilde{G}_4 = \widetilde{\Delta}$, d'où $\tau(n) \equiv n\sigma_3(n) \mod 7$.

Ces congruences, directement obtenues de l'étude des formes modulaires modulo des nombres premiers, montre que l'idée naturelle de la réduction était bonne, mais elle a demandé un travail assez conséquent.

7.2. Finitude des nombres premiers exceptionnels. — L'objet de ce paragraphe, qui est le point d'orgue de cet exposé, est de montrer qu'il n'y a qu'un nombre fini de nombres premiers ℓ tels que la fonction τ vérifie une congruence modulo ℓ. De plus, nous arriverons même à donner une sorte de majoration du cardinal des nombres premiers exceptionnels, ce qui nous permettra, par un simple test, de les déterminer tous, résolvant ainsi définitivement notre problème initial.

***Théorème 7.14* (Swinnerton-Dyer)**. — *Soit f vérifiant les hypothèses du théorème de Deligne. Alors l'ensemble des nombres premiers exceptionnels pour f est fini. Plus précisément, les trois types de congruences possibles sont pour les nombres premiers ℓ vérifiant nécessairement :*

(i) *Soit $\ell \leqslant k + 1$, soit ℓ divise le numérateur de $b_k/2k$.*

(ii) $\ell < 2k$.
(iii) *Pour tout nombre premier p, ℓ divise l'un des entiers non nuls p ou $a_p^2 - \alpha p^{k-1}$, pour un $\alpha \in \{0,1,2,4\}$.*

> ***Remarque 9.***
> Le cas (*iii*) montre qu'en l'état actuel de nos connaissances, on ne peut pas donner de borne explicite pour les entiers exceptionnels. En fait, des méthodes très différentes (utilisant en particulier la *conjecture* de l'inertie modérée de Serre) permettent de démontrer que dans ce cas, on a nécessairement $\ell < 4k$.

Démonstration. — Le premier point est le plus délicat. Supposons donc que la première congruence se réalise et que $\ell > k+1$. On a $a_p \equiv p^m + p^{m'} \mod \ell$ si $p \neq \ell$, et m, m' n'étant définis que modulo $\ell - 1$, on peut supposer $0 \leqslant m < m' < \ell - 1$ et $m + m' \equiv k - 1 \mod (\ell - 1)$ (en effet, m et m' ne peuvent être égaux modulo $(\ell - 1)$ sans quoi $\ell = 2$). Alors, on sait que pour tout entier n premier à ℓ, on a $a_n \equiv n^m \sigma_{m'-m}(n) \mod \ell$ ce qui se réécrit $\theta f \equiv \theta^{m+1} G^*_{m'-m+1} \mod \ell$ où on a posé $G^*_{2k} = (-1)^k \frac{B_{2k}}{4k} G_{2k}$. Comme $\ell > k+1$, la filtration de $\theta f \mod \ell$ est $k+\ell+1$; or, celle de $\widetilde{G}^*_{m'-m+1}$ est $m'-m+1$ si $m'-m > 1$, et $\ell+1$ si $m'-m = 1$. Il en résulte que celle de $\theta^{m+1} G^*_{m'-m+1}$ est $m'-m+1+(\ell+1)(m+1)$, et $\ell+1+(\ell+1)(m+1)$ si $m'-m=1$. On doit donc avoir :

$$k+\ell+1 = \begin{cases} m'-m+1+(m+1)(\ell+1) \text{ si } m'-m>1 \\ \ell+1+(\ell+1)(m+1) \text{ si } m'-m=1 \end{cases}.$$

Comme $k < \ell - 1$, ceci n'est possible que si $m = 0$, auquel cas on a $\theta f \equiv \theta G^*_k \mod \ell$, *ie* $\theta(f - G^*_k) = 0 \mod \ell$. Comme k n'est pas divisible par ℓ, on a $f - G^*_k = 0 \mod \ell$ par le corollaire 7.12. Comme f est parabolique, cela entraîne que le terme constant de G^*_k est divisible par ℓ, ou encore que ℓ divise le numérateur de $b_k/2k$.
Passons au cas (*ii*). Si la deuxième congruence se produit, un calcul rapide montre que $\theta f = \theta^{(l+1)/2} f \mod \ell$. Alors, si l'on suppose $\ell \geqslant 2k$, le corollaire 7.12 permet de calculer les filtrations des deux membres, ce qui donne l'identité $k+\ell+1 = k+(\ell+1)^2/2$, d'où la contradiction.
Enfin, pour le cas (*iii*), on choisit p tel que $a_p \neq 0$, et alors, si ℓ est un nombre premier exceptionnel (toujours du type (*iii*)), alors soit $\ell = p$, soit ℓ divise l'un des entiers non nuls $a_p^2 - \alpha p^{k-1}$, pour un $\alpha \in \{0,1,2,4\}$. □

Exemple 7.15. — On va maintenant déterminer les nombres premiers exceptionnels pour la forme parabolique Δ. Voici quelques valeurs de τ, issues d'un programme que nous avons réalisé et qui nous permettront d'éliminer certains cas :

n	$\tau(n) \mod 7$	$\tau(n) \mod 11$	$\tau(n) \mod 13$	$\tau(n) \mod 17$	$\tau(n) \mod 19$	$\tau(n) \mod 23$
1	1	1	1	1	1	1
2	4	9	2	10	14	22
3	0	10	5	14	5	22
4	5	2	10	7	10	0
5	0	1	7	2	4	0
6	0	2	10	4	13	1
7	0	9	0	1	14	0
8	4	0	6	7	6	1
9	2	9	3	2	15	0
10	0	9	1	3	18	0
11	1	1	0	13	9	0
12	0	9	11	13	12	0
13	0	4	8	7	14	22
14	0	4	0	10	6	0
15	0	10	9	11	1	0
16	3	7	7	14	10	22
17	0	9	4	10	15	0
18	1	4	6	3	1	0
19	0	0	3	6	7	0
20	0	2	5	14	2	0
21	0	2	0	14	13	0
22	4	9	0	11	12	0
23	4	10	11	1	16	1
24	0	0	4	13	11	22
25	4	7	2	10	10	1
26	0	3	3	2	6	1
27	0	5	9	15	6	1
28	0	7	0	7	7	0
29	2	0	1	3	13	22
30	0	2	5	8	14	0
31	0	7	12	6	12	22
32	3	8	11	16	12	0
33	0	10	0	12	7	0
34	0	4	8	15	1	0
35	0	9	0	2	18	0
36	3	7	4	14	17	0

FIGURE 1. Valeurs de τ modulo quelques nombres premiers.

- Le cas (i) est impossible pour $\ell > 13$, mis à part 691 qui est le numérateur de b_{12}, et pour lequel la congruence a effectivement lieu (*cf* section 2.3). Il reste les cas $\ell = 2, 3, 5, 7, 11, 13$. Pour $\ell = 2, 3, 5, 7$, on a effectivement une congruence. Pour $\ell = 11$, on regarde $\tau(7) \equiv 9 \mod 11$ et $7^m + 7^{11-m} \mod 11$ pour $m \leqslant 5$. Seul $m = 4$ pourrait convenir, mais on a $\tau(13) \equiv 4 \mod 11$ et $13^4 + 13^7 \equiv 1 \mod 11$, ce qui conclut pour $\ell = 11$. Quant au cas $\ell = 13$, on refait la même opération que précédemment, toujours avec 7, pour lequel aucun m ne convient.
- Le cas (ii) se produit pour $\ell = 2k - 1 = 23$, et le tableau ci-dessus montre que les cas $\ell = 11, 13, 19$ sont exclus, car $\tau \mod \ell$ devrait s'annuler sur tous les non-résidus quadratiques modulo ℓ comme pour 23.
- Enfin, si le cas (iii) se produisait, la remarque 7 montre qu'il existerait des nombres premiers p qui soient des non-résidus quadratiques modulo ℓ tels que ℓ divise $\tau(p)^2 - 2p^{11}$. Ainsi, 2 est un non-résidu quadratique modulo ℓ, donc $\ell \equiv \pm 3 \mod 8$. De plus, en prenant $p = 2$ dans la condition (iii), ℓ doit diviser l'un des nombres $576, -1472, -3520, -7616$, donc $\ell \in \{2, 3, 5, 7, 11, 17, 23\}$. Les congruences pour $2, 3, 5, 7, 23$ ont déjà été remarquées, et la congruence modulo 8 ne laisse plus que le cas $\ell = 11$. On refait ensuite la même opération avec $p = 5$ ce qui élimine ce cas.

Corollaire 7.16. — *Les nombres premiers exceptionnels pour* Δ *sont* $2, 3, 5, 7, 23$ *et* 691.

7.3. Congruences modulo ℓ^n. — Cette théorie étant à notre connaissance encore incomplète, nous allons seulement donner un cas particulier simple qui est celui de 23^2. Par les résultats précédents, comme 23 est exceptionnel de type (ii), c'est à dire que pour tout entier n qui soit un non-résidu modulo 23, alors on a $\tau(n) \equiv 0 \mod 23$. On peut améliorer ce résultat en montrant que, pour $p \neq 23$ premier, on a, modulo 23 :

$$\tau(p) \equiv \begin{cases} 2 \text{ si } p \text{ est de la forme } u^2 + 23v^2 \\ -1 \text{ si } p \text{ est résidu quadratique mais pas de la forme } u^2 + 23v^2 \end{cases}.$$

Voyons comment l'existence, et la connaissance (*cf* exemple 4.6) de ρ_{23} va nous aider pour trouver une congruences modulo 23^2 : prenons en particulier p de la forme $u^2 + 23v^2$. On a alors, modulo 23 :

$$\rho_{23}(F_p) \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

On peut donc écrire :

$$\rho_{23}(F_p) = \begin{pmatrix} 1 + 23a & 23b \\ 23c & 1 + 23d \end{pmatrix},$$

avec $a, b, c, d \in Z_{23}$ et $\tau(p) = 2 + 23(a + d)$, $p^{11} = 1 + 23(a + d) + 23^2(ad - bc)$. En comparant, on en déduit :

Proposition 7.17. — *Si* $p \neq 23$ *est un nombre premier de la forme* $u^2 + 23v^2$, *alors* $\tau(p) \equiv 1 + p^{11} \mod 23^2$.

ANNEXE : EXTENSIONS D'ANNEAUX

8. Éléments entiers sur un anneau

8.1. Définitions et résultats élémentaires. — La situation dans laquelle on se place est celle du théorème suivant :

Théorème 8.1. — *Soit R un anneau commutatif, A un sous-anneau de R, et x un élément de R. Les propriétés suivantes sont équivalentes :*

(i) *Il existe $a_0, \dots, a_{n-1} \in A$ tels que $x^n + a_{n-1}x^{n-1} + \dots + a_1 x + a_0 = 0$;*
(ii) *L'anneau $A[x]$ est un A-module de type fini ;*
(iii) *Il existe un sous-anneau B de R contenant A et x, et qui est un A-module de type fini.*

Ceci amène la définition suivante :

Définition 8.2. — Soit R un anneau, A un sous-anneau de R. Un élément x de R est dit entier sur A s'il satisfait aux conditions équivalentes du théorème précédent.

Corollaire 8.3. — *Soit R un anneau, A un sous-anneau de R. L'ensemble A' des éléments de R qui sont entiers sur A est un sous-anneau de R qui contient A.*

Démonstration. — En effet, si x et y sont deux éléments entiers, alors $A[x, y]$ est un quotient de $A[x] \otimes A[y]$, donc est un module de type fini qui contient $x + y, x - y$ et xy. □

L'anneau A' est appelée la fermeture intégrale de A dans R. Dans le cas où A est un anneau *intègre* et $R = Fr(A)$ est le corps des fractions de A, on l'appelle simplement la clôture intégrale de A. Enfin, si B est un anneau dont A est un sous-anneau, on dit que B est entier sur A si tout élément de B est entier sur A, c'est-à-dire si la fermeture intégrale de A dans B est B lui-même.

Enfin, on dit qu'un anneau A est intégralement clos s'il est intègre et si sa clôture intégrale est A lui-même. Nous verrons par la suite pourquoi cette propriété est importante. Mais avant de finir cette partie, donnons un résultat que nous utiliserons lors de l'étude des anneaux de Dedekind :

Proposition 8.4. — *Soient B un anneau intègre et A un sous-anneau de B, tel que B soit entier sur A. Pour que B soit un corps, il faut et il suffit que A soit un corps.*

Démonstration. — Si A est un corps et $b \in B$ non nul, alors $A[b]$ est un espace vectoriel de dimension finie sur A. Dès lors, la multiplication par b est une application A-linéaire de $A[b]$ dans lui-même qui est injective par intégrité de B. Elle est donc bijective, et atteint $1 \in A[b]$. Inversement, si B est un corps et $a \in A$ non nul, alors a admet un inverse dans

B qui satisfait une équation de dépendance intégrale $a^{-n} + a_{n-1}a^{-n+1} + \ldots + a_0 = 0$. En la multipliant par a^{n-1}, on obtient le résultat recherché. □

8.2. Discriminant. — Dans ce paragraphe, nous allons introduire une notion, celle de discriminant, qui va généraliser celle que l'on connaît pour les polynômes de degré 2, 3 ou 4, et qui va intervenir lorsque nous étudierons la notion de ramification d'un idéal premier dans une extension.

Définition 8.5. — Soit B un anneau et A un sous-anneau de B tel que B est un A-module libre de rang fini n. Pour $(x_1, \ldots, x_n) \in B^n$, on appelle discriminant du système $(x_1, \ldots, x_n)$ l'élément de A défini par $D(x_1, \ldots, x_n) = \det(\mathrm{Tr}_{B/A}(x_i x_j))$.

Un calcul élémentaire donne alors le résultat suivant :

Proposition 8.6. — *Si $(y_1, \ldots, y_n) \in B^n$ est un autre système d'éléments de B tel que $y_i = \sum_{j=1}^n a_{ij}x_j$ avec $a_{ij} \in A$, on a alors : $D(y_1, \ldots, y_n) = \det(a_{ij})^2 D(x_1, \ldots, x_n)$.*

On en déduit la définition suivante :

Définition 8.7. — Sous les hypothèses de la définition précédentes, on appelle discriminant de B sur A et on note $\mathscr{D}_{B/A}$, l'idéal principal engendré par le discriminant dans n'importe quelle base de B sur A.

Le résultat suivant vise à donner un cas particulier où l'on sait que le discriminant n'est jamais nul, résultat qui nous servira par la suite :

Proposition 8.8. — *Soit K un corps, L une extension séparable finie de K, de degré n, et $\sigma_1, \ldots, \sigma_n$ les n K-morphismes distincts de L dans une clôture algébrique de L. Alors, si $(x_1, \ldots, x_n)$ est une base de L sur K, on a $D(x_1, \ldots, x_n) = \det(\sigma_i(x_j))^2 \neq 0$.*

Démonstration. — La première égalité résulte du calcul suivant : $D(x_1, \ldots, x_n) = \det(\mathrm{Tr}(x_i x_j)) = \det(\sum_k \sigma_k(x_i x_j)) = \det(\sigma_k(x_i)).\det(\sigma_k(x_j)) = \det(\sigma_i(x_j))^2$. Quant à la deuxième assertion, elle provient du lemme de Dedekind affirmant l'indépendance linéaire de caractères distincts. □

Remarque 10.
Sous les hypothèses de ce théorème, on montre donc que la forme bilinéaire $(x, y) \mapsto \mathrm{Tr}_{L/K}(xy)$) est non dégénérée, et on obtient donc un isomorphisme canonique entre L (vu comme K espace vectoriel) et son dual. Donc pour toute base $(x_1, \ldots, x_n)$ fixée, il existe une base duale $(y_1, \ldots, y_n)$ telle que $\mathrm{Tr}_{L/K}(x_i y_j)) = \delta_{ij}$ pour tout couple (i, j) convenable.

Théorème 8.9. — *Soit A un anneau intégralement clos, K son corps de fractions, L une extension séparable de degré fini n de K et A' la fermeture intégrale de A dans L. Alors A' est un sous-A-module d'un A-module libre de rang n.*

Démonstration. — Soit $(x_1, \dots, x_n)$ une K-base de L. Chaque x_i est algébrique sur K, donc racine d'un polynôme sur A de degré n, de coefficient dominant a_n. Alors $x_i' = a_n x_i$ est entier sur A, et $(x_1', \dots, x_n')$ est une K-base de L contenue dans A'. Soit $(y_1, \dots, y_n)$ la base duale, et $z \in A'$. Il existe des éléments b_j de K tels que $z = \sum b_j y_j$, et donc pour tout i :

$$\mathrm{Tr}(x_i' z) = \sum_j b_j \mathrm{Tr}(x_i' y_j) = \sum_j b_j \delta_{ij} = b_i.$$

Or, comme $x_i', z \in A$, on a encore $x_i' z \in A$, donc $\mathrm{Tr}(x_i' z) = b_i \in A$, ce qui montre que A' est inclus dans le A-module libre $\bigoplus A y_j$. □

Exemple 8.10. — Soit K un corps et $L = K[x]$ une extension séparable de degré fini n de K, avec F le polynôme minimal de x sur K. Alors on a

$$D(1, x, \dots, x^{n-1}) = (-1)^{\frac{n(n-1)}{2}} \mathrm{N}_{L/K}(F'(x)) = (-1)^{\frac{n(n-1)}{2}} \mathrm{disc}(P).$$

En effet, si $x_1, \dots, x_n$ désignent les racines de $F(X)$ dans une extension de K, alors $D(1, x, \dots, x^{n-1}) = \det(\sigma_i(x^j))^2 = \det(x_i^j)^2$ et d'autre part, on a $(-1)^{\frac{n(n-1)}{2}} \det(x_i^j)^2 = \prod_{i \neq j} (x_i - x_j) = \prod_i (\prod_{j \neq i} (x_i - x_j)) = \prod_i F'(x_i) = \mathrm{N}_{L/K}(F'(x))$ car les $F'(x_i)$ sont les conjugués de $F'(x)$.

9. Anneaux de Dedekind

9.1. Définition et lien avec les anneaux d'entiers. — Dans tout ce paragraphe, les résultats que nous établirons seront là pour montrer que la fermeture intégrale d'un anneau de Dedekind dans une extension finie de son corps de fractions est encore un anneau de Dedekind, et qui plus est un module de type fini. C'est cette propriété - entre autres - qui justifie l'importance particulière accordée aux anneaux de Dedekind. Commençons donc par une propriété concernant finitude, et l'invariance du caractère noethérien par extension convenable :

Proposition 9.1. — *Soient A un anneau noethérien intégralement clos, K son corps de fractions, L une extension de degré fini n de K et A' la fermeture intégrale de A dans L. Si car $K = 0$, alors A' est un A-module de type fini et un anneau noethérien.*

Démonstration. — On sait déjà que A' est un sous-A-module d'un A-module libre de rang n, donc A' est un A-module de type fini. Les idéaux de A' sont des sous-A-modules de A', donc sont également de type fini sur A, et a fortiori sur A'. A' est donc noethérien. □

Remarque 11.
L'anneau des entiers d'un corps de nombres est noethérien, mais l'anneau des entiers de $\overline{\mathbb{Q}}$ ne l'est pas, d'où l'importance de la finitude de l'extension.

Lemme 9.2. — *Dans un anneau noethérien, tout idéal contient un produit d'idéaux premiers. Dans un anneau noethérien intègre A, tout idéal non nul contient un produit d'idéaux premiers non nuls.*

Démonstration. — Démontrons la seconde assertion (la première se démontre de la même façon, en enlevant les "non nul(s)"), et pour cela, raisonnons par l'absurde. La famille Φ des idéaux non nuls de A qui ne contiennent aucun produit d'idéaux premiers non nuls est alors non vide, et admet donc un élément maximal $\mathfrak{b}$. Bien sûr, $\mathfrak{b}$ n'est pas premier, et il existe donc deux élément $x, y \in A - \mathfrak{b}$ tels que $xy \in \mathfrak{b}$.Les idéaux $\mathfrak{b} + Ax$ et $\mathfrak{b} + Ay$ contiennent donc des produits d'idéaux premiers non nuls $\mathfrak{p}_1 \dots \mathfrak{p}_n$ et $\mathfrak{q}_1 \dots \mathfrak{q}_\mathfrak{m}$ respectivement. Comme $xy \in \mathfrak{b}$, on a $\mathfrak{b} \supset (\mathfrak{b} + Ax)(\mathfrak{b} + Ay) \supset \mathfrak{p}_1 \dots \mathfrak{p}_n \mathfrak{q}_1 \dots \mathfrak{q}_\mathfrak{m}$, ce qui est absurde. □

Voilà une dernière définition, généralisant celle d'idéal pour un anneau intègre, dont l'importance se fera sentir dès la section suivante. Soient donc A un anneau intègre et K son corps de fractions. On appelle idéal fractionnaire de A tout sous-A-module I de K tel qu'il existe $d \in A$ non nul tel que $I \subset d^{-1}A$. Les idéaux ordinaires sont un cas particulier d'idéaux fractionnaires et sont parfois qualifiés d'idéaux entiers lorsqu'il convient de les distinguer des idéaux fractionnaires généraux. De même que pour les idéaux, on peut définir le produit et la somme d'idéaux fractionnaires, et l'on obtient alors à nouveau des idéaux fractionnaires.

Définition 9.3. — Un anneau A est appelé anneau de Dedekind s'il est noethérien, intégralement clos, et si tout idéal premier non nul de A est maximal.

Théorème 9.4. — *Soient A un anneau de Dedekind, K son corps de fractions, L une extension séparable de degré fini n de K et A' la fermeture intégrale de A dans L. Alors A' est un anneau de Dedekind et un A-module de type fini.*

Démonstration. — Il reste à montrer que tout idéal premier non nul $\mathfrak{p}'$ de A' est maximal. Soit donc x un élément non nul de $\mathfrak{p}'$, et $x^n + a_{n-1}x^{n-1} + \dots + a_0 = 0$ une équation de dépendance intégrale de x sur A de degré minimal. Ainsi a_0 est non nul, et appartient à $A'x \cap A \subset \mathfrak{p}' \cap A$ donc $\mathfrak{p}' \cap A \neq (0)$. Or, $\mathfrak{p}' \cap A$ est un idéal premier de A, donc est un idéal maximal de A, et alors $A/(\mathfrak{p}' \cap A)$ est un corps. Mais $A/(\mathfrak{p}' \cap A)$ s'identifie à un sous-anneau de $A'/\mathfrak{p}'$, et $A'/\mathfrak{p}'$ est entier sur $A/(\mathfrak{p}' \cap A)$ car A' est entier sur A. Donc $A'/\mathfrak{p}'$ est un corps, ce qui conclut. □

Pour finir ce paragraphe, nous allons donner - sans démonstration - deux résultats dont nous nous resservirons par la suite, mais dont nous avons pensé que la place était ici.

Proposition 9.5. — *Soit S une partie d'un anneau de Dedekind A qui soit multiplicativement stable, contenant 1 mais pas 0. Alors tout anneau fractions $S^{-1}A$ est un anneau de Dedekind.*

Proposition 9.6. — *Soit A un anneau intègre, S une partie multiplicativement stable de A, contenant 1 mais pas 0 et $\mathfrak{m}$ un idéal maximal de A tel que $\mathfrak{m} \cap S = \varnothing$. Alors*

$$S^{-1}A/\mathfrak{m}S^{-1}A \simeq A/\mathfrak{m}.$$

Dans le cas particulier où $S = A - \mathfrak{p}$ avec $\mathfrak{p}$ un idéal premier non nul de A (on dit alors que $A_\mathfrak{p} = S^{-1}A$ est le localisé de A en $\mathfrak{p}$), on peut dire beaucoup plus (cf partie sur les anneaux de valuation discrète).

9.2. Norme d'un idéal. — Nous allons introduire dans cette section une définition relativement importante qui apparaîtra en particulier lors de l'étude des séries L dans des corps de nombres, et qui, selon nous, mérite sa place ci-dessous.

Jusqu'à la fin de ce paragraphe, K désigne un corps de nombres, n est son degré, et A est l'anneau des entiers de K. On écrira $\mathrm{N}(x)$ au lieu de $\mathrm{N}_{K/\mathbb{Q}}(x)$.

Proposition 9.7. — *Si x est un élément non nul de A, alors on a $|\mathrm{N}(x)| = \mathrm{card}(A/Ax)$.*

Démonstration. — A est un $\mathbb{Z}$-module libre de rang n, et Ax est un sous-$\mathbb{Z}$-module de A, également de rang n. Il existe donc une base $(e_1, \dots, e_n)$ du $\mathbb{Z}$-module A, et des éléments $c_i \in \mathbb{N}$ tels que $(c_1e_1, \dots, c_ne_n)$ soit une base de Ax. Alors, $A/Ax \simeq \prod \mathbb{Z}/c_i\mathbb{Z}$ et son cardinal est $c_1c_2 \dots c_n$. Soit u l'application $\mathbb{Z}$-linéaire de A sur Ax envoyant e_i sur c_ie_i. Son déterminant vaut $c_1c_2 \dots c_n$.
D'autre part, $(xe_1, \dots, xe_n)$ est une autre base de Ax, on a donc un automorphisme v du $\mathbb{Z}$-module Ax en posant $v(c_ie_i) = xe_i$. Son déterminant vaut donc ± 1. Or, $v \circ u$ est la multiplication par x, donc finalement, $\mathrm{N}(x) = \det(v \circ u) = \pm c_1c_2 \dots c_n$. □

Définition 9.8. — Étant donné un idéal entier non nul $\mathfrak{a}$ de A, on appelle norme de $\mathfrak{a}$ et on note $\mathrm{N}(\mathfrak{a})$ le nombre $\mathrm{card}(A/\mathfrak{a})$.

Remarquons que $\mathrm{N}(\mathfrak{a})$ est fini : en effet, si a est un élément non nul de $\mathfrak{a}$, alors $Aa \subset \mathfrak{a}$ et $A/\mathfrak{a}$ s'identifie à un quotient de A/aA ; d'où $\mathrm{card}(A/\mathfrak{a}) \leqslant \mathrm{card}(A/Aa)$ qui est fini par la proposition précédente. D'autre part, cette même proposition montre que pour un idéal principal Ab, on a bien $\mathrm{N}(Ab) = |\mathrm{N}(b)|$.
Pour finir, notons qu'on peut montrer que si $\mathfrak{a}$ et $\mathfrak{b}$ sont deux idéaux non nuls de A, alors on a $\mathrm{N}(\mathfrak{ab}) = \mathrm{N}(\mathfrak{a})\mathrm{N}(\mathfrak{b})$.

9.3. Décomposition des idéaux fractionnaires. — Cette section a pour but d'exposer le théorème de décomposition des idéaux fractionnaires en produit d'idéaux premiers non nuls dans un anneau de Dedekind. La démonstration de ce résultat est longue, et nous avons pensé qu'il était plus judicieux, pour la cohérence de l'exposé, de ne pas la présenter. L'idée de base est de commencer par montrer que pour un anneau de Dedekind qui n'est pas un corps, tout idéal maximal de A est inversible dans le monoïde des idéaux fractionnaires de A, avant de passer au cas général. Nous résumons le principal résultat dans le théorème suivant :

Théorème 9.9. — *Soient A un anneau de Dedekind, P l'ensemble des idéaux premiers non nuls de A. Tout idéal fractionnaire non nul $\mathfrak{b}$ de A s'écrit, d'une façon et d'une seule, sous la forme*

$$\mathfrak{b} = \prod_{\mathfrak{p} \in P} \mathfrak{p}^{n_{\mathfrak{p}}(\mathfrak{b})}$$

où les $n_{\mathfrak{p}}(\mathfrak{b})$ sont des entiers relatifs, presque tous nuls.

Corollaire 9.10. — *Si A est un anneau de Dedekind, alors le monoïde des idéaux fractionnaires non-nuls de A est un groupe.*

9.4. Lien avec les anneaux de valuation discrète. —

Définition 9.11. — Un anneau A est appelé anneau de valuation discrète si c'est un anneau principal et s'il possède un idéal premier non nul $\mathfrak{m}(A)$ et un seul. Le corps $A/\mathfrak{m}(A)$ s'appelle le corps résiduel de A.

Les idéaux non nuls de A sont de la forme $\mathfrak{m}(A)^n = \pi^n A$ où $\pi \in A$ est un générateur de $\mathfrak{m}$. Si $x \neq 0$ est un élément de A, on peut écrire $x = \pi^n u$ où u est inversible. L'entier n est appelé valuation de x, et noté $v(x)$. Bien sûr, il ne dépend pas du choix de π.
Ces anneaux étant principaux, ce sont des cas particuliers d'anneaux de Dedekind. On se propose de voir qu'à partir d'un anneau de Dedekind, il est facile de construire des anneaux de valuation discrète :

Proposition 9.12. — *Si A est un anneau intègre noethérien, les deux propriétés suivantes sont équivalentes :*

(i) *Pour tout idéal premier $\mathfrak{p}$ non nul de A, $A_{\mathfrak{p}}$ est un anneau de valuation discrète.*
(ii) *A est un anneau de Dedekind.*

Ceci donne l'existence de valuations sur un anneau de Dedekind, et on remarque que pour tout idéal premier $\mathfrak{p}$ de A, et tout élément $x \in A$, on a : $v_{\mathfrak{p}}(x) = v_{\mathfrak{p}}(Ax)$, où le terme de droite a déjà été défini lors de la décomposition d'un idéal fractionnaire comme produit d'idéaux premiers. Nous allons maintenant donner un lemme, appelé *lemme d'approximation* qui nous sera utile ensuite :

Lemme 9.13. — *Soit A un anneau de Dedekind, K son corps de fractions et k un entier. Pour tout i, $1 \leqslant i \leqslant k$, soient $\mathfrak{p}_i$ des idéaux premiers de A distincts deux à deux, x_i des éléments de K, et n_i des entiers. Il existe alors $x \in K$ tel que $v_{\mathfrak{p}_i}(x - x_i) \geqslant n_i$ pour tout i et $v_{\mathfrak{q}}(x) \geqslant 0$ pour $\mathfrak{q} \neq \mathfrak{p}_1, \dots, \mathfrak{p}_k$.*

Démonstration. — Supposons d'abord que les x_i sont dans A, et cherchons une solution $x \in A$. Par linéarité, on peut supposer que pour $i \geqslant 2$, on a $x_i = 0$, et quitte à augmenter les n_i, on peut les supposer positifs. On pose alors $\mathfrak{a} = \mathfrak{p}_1^{n_1} + \mathfrak{p}_2^{n_2} \dots \mathfrak{p}_k^{n_k}$. On a $v_{\mathfrak{p}}(\mathfrak{a}) = 0$ pour tout $\mathfrak{p}$ d'où $\mathfrak{a} = A$. On en conclut que $x_1 = x + y$ avec $x \in \mathfrak{p}_2^{n_2} \dots \mathfrak{p}_k^{n_k}$ et $y \in \mathfrak{p}_1^{n_1}$. Alors l'élément x convient.
Dans le cas général, on pose $x_i = a_i/s$ avec $a_i, s \in A$, s non nul, et $x = a/s$. L'élément a doit vérifier les conditions $v_{\mathfrak{p}_i}(a - a_i) \geqslant n_i + v_{\mathfrak{p}_i}(s)$ et $v_{\mathfrak{q}}(a) \geqslant v_{\mathfrak{q}}(s)$. Or, ces conditions sont celles du type envisagé ci-dessus en adjoignant à la famille des $\mathfrak{p}_i$ les idéaux premiers $\mathfrak{q}$ tels que $v_{\mathfrak{q}}(s) > 0$, d'où le résultat. □

Remarque 12.
Ce résultat d'apparence complexe n'est qu'en fait qu'une généralisation du lemme chinois bien connu. En particulier, avec les notations du théorème 10.1 à venir, il donne un isomorphisme entre $B/\mathfrak{p}B$ et $\prod_{\mathfrak{P}\,|\,\mathfrak{p}} B/\mathfrak{P}^{e_{\mathfrak{P}}}$.

Corollaire 9.14. — *Un anneau de Dedekind n'ayant qu'un nombre fini d'idéaux premiers est principal.*

10. Ramification

10.1. Généralités. — Dans tout ce paragraphe, on considère A un anneau de Dedekind, K son corps de fractions, et L une extension séparable de degré fini n de K. Pour plus de clarté, on notera B (et non plus A') l'anneau des entiers de L sur A, c'est donc un anneau de Dedekind, et un A-module de type fini.
Si $\mathfrak{P}$ est un idéal premier non nul de B, et si $\mathfrak{p} = \mathfrak{P} \cap A$, on dira que $\mathfrak{P}$ est au-dessus de $\mathfrak{p}$, ou que $\mathfrak{P}$ divise $\mathfrak{p}$. Cette relation équivaut aussi à dire que $\mathfrak{P}$ contient l'idéal $\mathfrak{p}B$ de B engendré par $\mathfrak{p}$. On note alors $e_{\mathfrak{P}}$ l'exposant de $\mathfrak{P}$ dans la décomposition en idéaux premiers de $\mathfrak{p}B$, on a donc :

$$\mathfrak{p}B = \prod_{\mathfrak{P}|\mathfrak{p}} \mathfrak{P}^{e_{\mathfrak{P}}}, \quad e_{\mathfrak{P}} = v_{\mathfrak{P}}(\mathfrak{p}B).$$

L'entier $e_{\mathfrak{P}}$ est appelé indice de ramification de $\mathfrak{P}$ dans l'extension L/K. D'autre part, comme $\mathfrak{P}$ est au-dessus de $\mathfrak{p}$, le corps $B/\mathfrak{P}$ est une extension de $A/\mathfrak{p}$, et B étant de type fini sur A, l'extension en question est de degré fini. Ce degré est appelé degré résiduel de $\mathfrak{P}$ dans l'extension L/K, et noté $f_{\mathfrak{P}}$.

On dit qu'une extension L/K est non ramifiée en $\mathfrak{P}$ si on a à la fois $e_{\mathfrak{P}} = 1$ et $B/\mathfrak{P}$ séparable sur $A/\mathfrak{p}$ (cette dernière condition sera facile à vérifier dans nos cas, car $A/\mathfrak{p}$ sera un corps fini, donc parfait). Enfin, si L/K est non ramifiée pour tous les idéaux premiers $\mathfrak{P}$ au-dessus de $\mathfrak{p}$, on dit que L/K est non ramifiée au-dessus de $\mathfrak{p}$.
Voici maintenant un théorème important, dont la preuve repose en partie sur la remarque 12 :

Théorème 10.1. — *Soit $\mathfrak{p}$ un idéal premier non nul de A. L'anneau $B/\mathfrak{p}B$ est une $A/\mathfrak{p}$-algèbre de degré $n = [L : K]$, isomorphe au produit $\prod_{\mathfrak{P}|\mathfrak{p}} B/\mathfrak{P}^{e_{\mathfrak{P}}}$. On a la formule :*

$$n = \sum_{\mathfrak{P}|\mathfrak{p}} e_{\mathfrak{P}} f_{\mathfrak{P}}.$$

De ce résultat et du corollaire 9.14, on peut déduire que l'anneau des entiers d'une extension finie d'un corps local (*ie* un corps commutatif complet pour une valuation discrète) est toujours principal.

La théorie de la ramification est très vaste, et il existe plusieurs résultats permettant de savoir dans certains cas particuliers, si une extension est non ramifiée, propriété qu'on cherchera souvent à obtenir par la suite.

Exemple 10.2. — Dans le cas où A est un anneau de valuation discrète de corps de fractions K, $f \in A[X]$ un polynôme unitaire irréductible et $L = K[X]/(f)$, on possède un critère de non ramification : si $\overline{f} \in (A/\mathfrak{p})[X]$ ($\mathfrak{p}$ est l'idéal maximal de A) est séparable, alors L/K est non ramifiée.

Un autre cas particulier, très riche, est celui des extensions galoisiennes, que nous développerons après avoir parlé un peu du rapport entre le discriminant et la ramification.

10.2. Discriminant et ramification. — Cette partie vise en priorité à établir le théorème 10.7. Pour cela, on va d'abord énoncer deux lemmes élémentaires sur les discriminants dont les preuves ne comportent pas de difficulté.

Lemme 10.3. — *Soient A un anneau, $B_1, \ldots, B_n$ des anneaux contenant A et qui sont des A-modules libres de rang fini, et $B = \prod B_i$ leur anneau produit. Alors $\mathscr{D}_{B/A} = \prod \mathscr{D}_{B_i/A}$.*

Lemme 10.4. — *Soient A un anneau, B un anneau contenant A et admettant une base finie $(x_1, \ldots, x_n)$ sur A, et $\mathfrak{a}$ un idéal de A. Pour $x \in B$, notons $\overline{x}$ la classe de x dans $B/\mathfrak{a}B$. Alors $(\overline{x}_1, \ldots, \overline{x}_n)$ est une base de $B/\mathfrak{a}B$ sur $A/\mathfrak{a}$ et on a $D(\overline{x}_1, \ldots, \overline{x}_n) = \overline{D(x_1, \ldots, x_n)}$.*

Avant d'énoncer le théorème qui nous intéresse, donnons un dernier résultat, un peu plus difficile, reliant l'existence d'éléments nilpotents dans une algèbre à un certain discriminant :

Lemme 10.5. — *Soient K un corps parfait et L une K-algèbre commutative de dimension finie. Alors L est réduite si et seulement si $\mathscr{D}_{L/K} \neq (0)$.*

Démonstration. — Supposons d'abord L non réduite et soit $x \in L$ un élément nilpotent non nul. On pose $x_1 = x$ et on complète cette famille libre en une base $(x_1, \dots, x_n)$ de L sur K. Alors $x_1 x_j$ est nilpotent, et ainsi sa trace est nulle. Donc $\mathscr{D}_{L/K} = (0)$.
Réciproquement, supposons L réduite, alors l'idéal (0) de L est intersection finie d'idéaux premiers (car les idéaux sont des sous-espaces vectoriels) : $(0) = \bigcap \mathfrak{P}_i$ pour $1 \leqslant i \leqslant q$. Comme $L/\mathfrak{P}_i$ est une algèbre intègre de dimension finie sur K, c'est un corps, et donc $\mathfrak{P}_i$ est un idéal maximal de L, de sorte que $\mathfrak{P}_i + \mathfrak{P}_j = L$ si $i \neq j$. Ainsi, L est isomorphe à $\prod L/\mathfrak{P}_i$ et donc par le lemme 10.3, $\mathscr{D}_{L/K} = \prod \mathscr{D}_{L/\mathfrak{P}_i/K}$. Or, on a montré que pour des extensions séparables, le discriminant était non nul. Donc pour tout i, $\mathscr{D}_{L/\mathfrak{P}_i/K} \neq 0$, et le résultat suit. □

Définition 10.6. — Soient K et L deux corps de nombres avec $K \subset L$, A et B les anneaux des entiers de K et L. On appelle idéal discriminant de B sur A (ou de L sur K) et on note $\mathscr{D}_{B/A}$ ou $\mathscr{D}_{L/K}$ l'idéal de A engendré par les discriminants des bases de L sur K qui sont contenues dans B.

> ***Remarque 13.***
> Lorsque B est un A-module libre, on retrouve la même notion de discriminant que celle définie auparavant.

Si $(x_1, \dots, x_n)$ est une base de L sur K contenue dans B, alors $\mathrm{Tr}_{L/K}(x_i x_j) \in A$, donc $D(x_1, \dots, x_n) \in A$ est ainsi, $\mathscr{D}_{B/A}$ est un idéal *entier* de A, non nul.
Nous pouvons maintenant énoncer le théorème recherché (les notations précédentes sont conservées) :

Théorème 10.7. — *Pour qu'un idéal premier $\mathfrak{p}$ de A se ramifie dans B, il faut et il suffit qu'il contienne l'idéal discriminant $\mathscr{D}_{B/A}$. Les idéaux premiers de A qui se ramifient dans B sont en nombre fini.*

Démonstration. — Il suffit de montrer la première assertion. Comme $B/\mathfrak{p}B \simeq \prod B/\mathfrak{P}_i^{e_i}$, $\mathfrak{p}$ se ramifie si et seulement si $B/\mathfrak{p}B$ est non réduit ou encore $\mathscr{D}_{(B/\mathfrak{p}B)/(A/\mathfrak{p})} = (0)$ car $A/\mathfrak{p}$ est un corps fini. Posons $S = A - \mathfrak{p}$, $A' = A_{\mathfrak{p}} = S^{-1}A$, $B' = S^{-1}B$ et $\mathfrak{p}' = \mathfrak{p}A'$. Alors A' est un anneau principal, B' est un A-module libre, et on a $A'/\mathfrak{p}' \simeq A/\mathfrak{p}$ et $B'/\mathfrak{p}'B' \simeq B/\mathfrak{p}B$. En désignant par $(e_1, \dots, e_n)$ une base de B' sur A', la relation $\mathscr{D}_{(B/\mathfrak{p}B)/(A/\mathfrak{p})} = (0)$ équivaut à $D(e_1, \dots, e_n) \in \mathfrak{p}'$ par le lemme 10.4. Ceci étant, si $D(e_1, \dots, e_n) \in \mathfrak{p}'$ et si $(x_1, \dots, x_n)$ est une base de L sur K contenue dans B, on a $D(x_1, \dots, x_n) \in \mathfrak{p}' \cap A = \mathfrak{p}$ donc $\mathscr{D}_{B/A} \subset \mathfrak{p}$.

Réciproquement, si $\mathscr{D}_{B/A} \subset \mathfrak{p}$, alors on a $D(e_1, \ldots, e_n) \in \mathfrak{p}'$ car on peut écrire $e_i = y_i/s$ avec $y_i \in B$ et $s \in S$ pour tout i, d'où :

$$D(e_1, \ldots, e_n) = s^{-2n} D(x_1, \ldots, x_n) \in A' \mathscr{D}_{B/A} \subset A'\mathfrak{p} = \mathfrak{p}'.$$

□

10.3. Cas galoisien. — Gardant les notations du paragraphe précédent, on va supposer de plus que l'extension L/K est galoisienne. Le résultat suivant, bien que n'étant pas particulièrement compliqué, va être le point de départ pour toute la suite.

Proposition 10.8. — *Le groupe* $\mathrm{Gal}(L/K)$ *opère transitivement sur l'ensemble de idéaux premiers* $\mathfrak{P}$ *de* B *divisant un idéal premier donné* $\mathfrak{p}$ *de* A.

Démonstration. — Soit $\mathfrak{P}|\mathfrak{p}$, et supposons qu'il existe un idéal premier $\mathfrak{P}'$ de B au-dessus de $\mathfrak{p}$ distinct des $\sigma(\mathfrak{P}), \sigma \in \mathrm{Gal}(L/K)$. D'après le lemme d'approximation, il existe $a \in \mathfrak{P}', a \notin \sigma(\mathfrak{P})$ pour tout σ. Si $x = \mathrm{N}_{L/K}(a)$, on a $x \in A$, et $x = \prod \sigma(a)$, d'où $x \notin \mathfrak{P}$, $x \in \mathfrak{P}'$ ce qui est absurde car $\mathfrak{P} \cap A = \mathfrak{P}' \cap A$. □

Corollaire 10.9. — *Soit* $\mathfrak{p}$ *un idéal premier non nul de* A. *Les entiers* $e_\mathfrak{P}$ *et* $f_\mathfrak{P}$ *(pour* $\mathfrak{P}|\mathfrak{p}$*) ne dépendent que de* $\mathfrak{p}$. *Si on les note* $e_\mathfrak{p}$, $f_\mathfrak{p}$, *et si* $g_\mathfrak{p}$ *est le nombre des idéaux premiers divisant* $\mathfrak{p}$, *alors on a* $n = e_\mathfrak{p} f_\mathfrak{p} g_\mathfrak{p}$.

Voici maintenant deux nouveaux objets propres au cas galoisien, et dont les propriétés montrent la richesse des extensions galoisiennes.

Définition 10.10. — Le groupe de décomposition de $\mathfrak{P}$ dans L/K est $D_\mathfrak{P}(L/K) = \{\sigma \in \mathrm{Gal}(L/K) | \sigma(\mathfrak{P}) = \mathfrak{P}\}$.

Pour $\sigma \in D := D_\mathfrak{P}(L/K)$, les relations $\sigma(B) = B$ et $\sigma(\mathfrak{P}) = \mathfrak{P}$ passent au quotient pour donner un morphisme $\epsilon : D \to \mathrm{Gal}((B/\mathfrak{P})/(A/\mathfrak{p}))$.

Définition 10.11. — Le groupe d'inertie de $\mathfrak{P}$ dans L/K est $I_\mathfrak{P}(L/K) = \mathrm{Ker}\,(\epsilon) = \{\sigma \in D \,|\, \forall x \in B, \sigma(x) - x \in \mathfrak{P}\}$.

Le résultat suivant, dans le prolongement direct de ce qui précède, nous permettra d'arriver au principal but de cette section qui est la construction d'un élément particulier de $\mathrm{Gal}(L/K)$ qui s'appelle le Frobenius. Pour plus de clarté, on va adopter une notation plus concise pour les corps résiduels, en notant $\overline{K} = A/\mathfrak{p}$ et $\overline{L} = B/\mathfrak{P}$.

Proposition 10.12. — *L'extension* $\overline{L}/\overline{K}$ *est normale et l'homomorphisme* ϵ *définit un isomorphisme de* D/I *sur* $\mathrm{Gal}(\overline{L}/\overline{K})$.

Démonstration. — Soit $\overline{a} \in \overline{L}$, et soit $a \in B$ un de ses représentants. $P(X) = \prod(X - \sigma(a))$ où σ parcourt $\mathrm{Gal}(L/K)$ est un polynôme unitaire de $A[X]$ qui admet a pour racine. Sa réduction $\overline{P}(X)$ a pour racine les $\overline{\sigma(a)} \in \overline{L}$ car L est galoisienne, ce qui montre que les conjugués de $\overline{a}$ sont dans $\overline{L}$ ou encore que l'extension $\overline{L}/\overline{K}$ est normale.
Choisissons pour $\overline{a}$ un élément primitif de la plus grande extension séparable $\overline{L}_s$ de $\overline{K}$ contenue dans $\overline{L}$. Le lemme d'approximation montre qu'il existe un représentant a de $\overline{a}$ qui appartient à tous les idéaux premiers $\sigma(\mathfrak{P}), \sigma \notin D$. En effet, en notant $\mathfrak{P}_1 = \mathfrak{P}$ et $\mathfrak{P}_\sigma = \sigma(\mathfrak{P})$ pour $\sigma \notin D$, il suffit de prendre, avec les notations de ce lemme, $x_\sigma = 0, n_\sigma \geqslant 1$ pour $\sigma \notin D$, puis, si b est un relèvement de $\overline{a}$, $x_1 = b, n_1 \geqslant 1$.

En considérant le même polynôme $P(X) = \prod(X - \sigma(a))$ (σ parcourt $\mathrm{Gal}(L/K)$) que précédemment, alors les racines non nulles de $\overline{P}(X)$ sont de la forme $\overline{\sigma(a)}$ avec $\sigma \in D$. En effet, $\overline{\sigma(a)} = 0$ est équivalent à $a \in \sigma^{-1}(\mathfrak{P})$, et alors $\sigma^{-1}(\mathfrak{P}) \subset \mathfrak{P}$ équivaut à $\sigma \in D$.

On en conclut que tout conjugué de $\overline{a}$ est égal à l'un des $\overline{\sigma(a)}$ avec $\sigma \in D$, donc pour tout conjugué $\overline{b}$ de $\overline{a}$, il existe $\sigma \in D$ tel que $\epsilon(\sigma)(\overline{a}) = \overline{b}$. Comme $\overline{a}$ est un élément primitif de $\overline{L}_s/\overline{K}$, une telle condition caractérise un et un seul élément de $\mathrm{Gal}(\overline{L}/\overline{K})$, ce qui démontre la surjectivité de ϵ. □

Remarque 14.
Ce résultat, permettant de définir le Frobenius, est aussi très utile en théorie de Galois : il montre, avec l'exemple 10.2, comment relier le groupe de Galois d'un polynôme sur $\mathbb{Z}$ à celui de ses réductions modulo certains nombres premiers.

Corollaire 10.13. — *Pour que $\mathfrak{p}$ ne se ramifie pas dans B, il faut et il suffit que I soit réduit à l'identité.*

Démonstration. — En effet, on a $ef/|I| = |D/I| = |\mathrm{Gal}(\overline{L}/\overline{K})| = [\overline{L} : \overline{K}] = f$, d'où $|I| = e$. □

Nous pouvons maintenant définir ce qu'est l'élément de Frobenius pour un idéal $\mathfrak{P}$. On garde toujours les mêmes notations, et on fait l'hypothèse $\overline{K} \simeq \mathbb{F}_q$ et que l'extension L/K est non ramifiée en $\mathfrak{P}$ ou encore que le groupe d'inertie $I_\mathfrak{P}$ est trivial. Alors $D_\mathfrak{P}$ s'identifie à $\mathrm{Gal}(\overline{L}/\overline{K})$ via ϵ. Or, $\overline{K}$ étant fini, ce dernier groupe est cyclique engendré par l'automorphisme $x \mapsto x^q$. On va noter $F_\mathfrak{P}$ l'élément de $D_P(L/K)$ correspondant à ce générateur, il est caractérisé par la propriété suivante :

$$\forall\, b \in B,\ F_\mathfrak{P}(b) \equiv b^q \bmod \mathfrak{P}.$$

Définition 10.14. — L'élément $F_\mathfrak{P}$ est appelé élément de Frobenius de $\mathfrak{P}$. C'est un générateur du groupe de décomposition de $\mathfrak{P}$, d'ordre $f_\mathfrak{P}$. On le note aussi $(\mathfrak{P}, L/K)$.

Pour conclure, remarquons que si on ne donne que $\mathfrak{p}$ idéal de A, alors l'élément de Frobenius en $\mathfrak{p}$ est défini à conjugaison près (car $(\sigma(\mathfrak{P}), L/K) = \sigma(\mathfrak{P}, L/K)\sigma^{-1}$).

Enfin, tout ce que nous avons fait vaut pour des extensions *finies*, et nous verrons que lors de l'étude des représentations ℓ-adiques de groupes de Galois, nous travaillerons sur des extensions infinies. En fait, bon nombre des résultats établis ici possèdent une extension naturelle, mais d'autres non (par exemple le fait que $\overline{\mathbb{Z}}$ ne soit pas un anneau de Dedekind).

10.4. Complétude, complétion et ramification. — Nous allons maintenant nous intéresser aux propriétés topologiques des extensions dans l'étude de la ramification. Une des réductions possibles que nous avons brièvement suggérée est la localisation, et nous avons vu que la situation était plus simple pour des anneaux de valuation discrète. Le but de ce paragraphe est de montrer que l'on peut se ramener à une extension de corps valués complets, ce qui facilite encore plus cette étude.

Soit K un corps muni d'une valuation discrète, c'est-à-dire $v : K \setminus \{0\} \to \mathbb{Z}$ un morphisme de groupes tel que $v(x+y) \geqslant \min(v(x), v(y))$ pour tous x, y. Soit A l'anneau local $v^{-1}([0, +\infty[)$, d'idéal maximal $v^{-1}([1, +\infty[)$. Si $a \in \mathbb{R}$ avec $0 < a < 1$, alors la formule $||x|| = a^{v(x)}$ si $x \neq 0$ et $||0|| = 0$ définit une valeur absolue ultramétrique sur K. Soit $\hat{K}$ le complété de K pour la topologie définie par sa valeur absolue (qui ne dépend pas de a). Alors $\overline{K}$ est un corps valué dont la valeur absolue prolonge celle de K. D'autre part $\hat{v}$ est à valeurs entières, c'est même une valuation discrète sur $\hat{K}$ dont l'anneau de valuation est l'adhérence $\hat{A}$ de A dans $\hat{K}$. Si π est une uniformisante locale de A, alors on a :

$$\hat{A} = \varprojlim A/\pi^n A.$$

En particulier, les corps résiduels de A et $\hat{A}$ coïncident.
Voici un résultat de nature topologique qui permet de savoir si K n'est pas "trop gros" :

Proposition 10.15. — *Pour que K soit localement compact, il faut et il suffit qu'il soit complet et que son corps des résiduels soit fini.*

Démonstration. — Si K est localement compact, il est complet (car c'est un corps topologique). De plus, les $\pi^n A$ forment un système fondamental de voisinages fermés de 0, donc l'un d'eux est compact, et par homothétie, A aussi. Dès lors, $\overline{K} = A/\pi A$ est compact et discret donc fini.
Réciproquement, si $\overline{K}$ est fini, alors les $A/\pi^n A$ sont finis aussi, donc $\hat{A}$ est compact. Si de plus K est complet, alors $A = \hat{A}$ et K est bien localement compact. □

Exemple 10.16. — Le corps $\mathbb{Q}_p$ est un corps localement compact de corps de résiduels $\mathbb{F}_p$. Dans un autre genre, si $\mathbb{F}$ est un corps fini, alors le corps des séries formelles $\mathbb{F}((T))$ est localement compact.

Voici un premier résultat qui montre que la complétude est conservée par extension sous de bonnes hypothèses.

Proposition 10.17. — *Soit K un corps muni d'une valuation discrète v d'anneau A, et complet pour la topologie définie par v. Soit L/K une extension finie de K, et soit B la fermeture intégrale de A dans L. Alors B est un anneau de valuation discrète ; c'est un A-module libre de rang $n = [L : K]$, et L est complet pour la topologie définie par B.*

La démonstration de ce résultat se traite en montrant que toutes les valuations associées aux idéaux premiers de B donnent lieu à une seule topologie sur B. On peut d'ailleurs noter quelques similitudes avec le cas des espaces vectoriels normés de dimension finie sur un corps complet pour une valeur absolue archimédienne.

Corollaire 10.18. — *Il existe une valuation w et une seule de L qui prolonge v. Elle est donnée par $w(x) = \frac{1}{f} v(\mathrm{N}_{L/K}(x))$ pour tout $x \in L$.*

Nous ne voulons pas nous étendre trop sur la complétion ou la structure des anneaux de valuation discrète complets. Ainsi, nous allons finir là cette section avec un théorème important qui nous sera très utile au moment de la construction de l'extension maximale de $\mathbb{Q}$ non ramifiée en dehors d'un certain nombre premier ℓ, car il nous autorise à regarder des extensions de corps valués complets, que nous connaissons bien d'après la propositon précédente.
Au stade où nous en sommes, ce théorème s'apparente presque à un résumé de nos connaissances, donc se passe de démonstration.

Théorème 10.19. — *Soit L/K une extension séparable de degré fini n, v une valuation discrète de K d'anneau A, et B la fermeture intégrale de A dans L. Soient w_i les différents prolongements de v à L, et soient e_i, f_i les nombres correspondants. Si $\hat{K}$ et $\hat{L}_i$ désignent les complétés de K et L pour v et w_i respectivement, alors :*

(a) *Le corps $\hat{L}_i$ est une extension de $\hat{K}$ de degré $n_i = e_i f_i$;*
(b) *La valuation w_i est l'unique valuation de $\hat{L}_i$ prolongeant la valuation $\hat{v}$, et on a : $e_i = e(\hat{L}_i/\hat{K})$ et $f_i = f(\hat{L}_i/\hat{K})$.*

10.5. Cas des extensions cyclotomiques. — Ce paragraphe va servir à résumer les idées déjà vues au travers d'un exemple relativement riche, et d'autre part, à construire dès la partie suivante le caractère de Dirichlet, cas particulier d'une représentation ℓ-adique de groupes de Galois. On rappelle qu'une extension cyclotomique de degré n (de $\mathbb{Q}$) est le corps de décomposition sur $\mathbb{Q}$ de $X^n - 1$, ou encore $\mathbb{Q}(\zeta)$ où ζ est une racine primitive n-ième de l'unité (complexe). Nous voulons regrouper les résultats principaux dans un seul théorème, pour plus de clarté :

Théorème 10.20. — *Soit $n \geqslant 2$ un entier. Alors :*

(a) *L'anneau des entiers du corps cyclotomique $\mathbb{Q}(\zeta)$ est $\mathbb{Z}[\zeta]$, de base $(1, \zeta, \ldots, \zeta^{\phi(n)-1})$.*
(b) *Aucun nombre premier qui ne divise pas n ne se ramifie dans $\mathbb{Z}[\zeta]$.*

Démonstration. — La démonstration du premier point n'est pas très intéressante donc nous nous concentrerons sur la seconde assertion. D'après les résultats de la section 10.2 et l'exemple 8.10, cela revient à calculer la norme de $F'(\zeta)$ où F est le polynôme minimal de ζ (sur $\mathbb{Q}$). Notons d le degré de F. On écrit $X^n-1=F(X)G(X)$ et donc $n\zeta^{n-1}=F'(\zeta)G(\zeta)$ d'où $N(F'(\zeta))|n^d$. Enfin, comme ζ est un entier de $\mathbb{Q}(\zeta)$, le discriminant absolu de $\mathbb{Q}(\zeta)$ divise $D(1,\zeta,\ldots,\zeta^{n-1})$ et donc n^d. □

Références

[Ami75] Y. Amice – *Les nombres p-adiques*, PUF, 1975.

[Bre07] C. Breuil – « Represention of Galois ans of GL_2 in characteristic p », Graduate course at Columbia University, 2007.

[Col] P. Colmez – « Périodes et représentations galoisiennes », Notes du cours de M2 à Orsay.

[DS05] F. Diamond & J. Shurman – *A first course in modular forms*, Springer, 2005.

[Kob77] N. Koblitz – *p-adic Numbers, p-adic Analysis, and Zeta-Functions*, Springer, 1977.

[Lan65] S. Lang – *Algebra*, Addison-Wesley, 1965.

[Lan76] ———, *Introduction to modular forms*, Springer, 1976.

[Neu99] J. Neukirch – *Algebraic Number Theory*, Springer, 1999.

[Sam03] P. Samuel – *Théorie algébrique des nombres*, Hermann, 2003.

[SD73] H. Swinnerton-Dyer – « On ℓ-adic representations and congruences for coefficients of modular forms », in *Antwerp Conference*, Springer Lectures Notes, **350**, 1973.

[Ser68a] J.-P. Serre – *Abelian $\ell-$adic Representations and Elliptic Curves*, Hermann, 1968.

[Ser68b] ———, *Corps locaux*, Hermann, 1968.

[Ser70] ———, *Cours d'arithmétique*, PUF, 1970.

[Ser68] ———, « Une interprétation des congruences relatives à la fonction τ de Ramanujan », in *Séminaire Delange-Pisot-Poitou*, 1967/68, n°14.

[Ser72] ———, « Congruences et formes modulaires (d'après H.P.F. Swinnerton-Dyer) », in *Séminaire Bourbaki*, 1971/72, n°416.

[Sil86] J. H. Silvermann – *The arithmetic of elliptic curves*, Springer, 1986.

Henri GUENANCIA
Olivier TAÏBI