DES ADÈLES: POURQUOI?

DES ADÈLES: POURQUOI ? [1]

par Alain ROBERT

C'est en 1897 que Hensel introduit formellement pour la première fois les nombres p-adiques. Il désire appliquer aux nombres algébriques les techniques de développement en série de Laurent (ou de Puiseux dans le cas ramifié) qui s'utilisent couramment dans la théorie des fonctions algébriques sur les surfaces de Riemann. Par exemple, un nombre rationnel $a \in \mathbf{Q}$ admet un développement en série

$$(1) \qquad \sum_{n \geq n_0} a_n p^n \qquad (0 \leqslant a_n < p)$$

(n'ayant qu'un nombre fini de coefficients $a_n \neq 0$ d'indices n négatifs) pour chaque nombre premier p. L'indice n_0 du premier coefficient non nul (si $a \neq 0$) est appelé ordre de a en p et dénoté par $\mathrm{ord}_p(a)$. Cet entier rationnel est l'exposant de p dans la décomposition de a en nombres premiers : $a = \prod_p p^{ord_p(a)}$. Lorsque $\mathrm{ord}_p(a) < 0$, on dit que a présente un pôle en p tandis que si $\mathrm{ord}_p(a) > 0$, on dit au contraire que a possède un zéro en p. Hensel a d'ailleurs utilisé très tôt des développements du type (1) même s'ils ne provenaient plus d'un nombre rationnel (en analogie avec les développements de fonctions transcendantes sur les surfaces de Riemann), et il a développé une algèbre de ces développements formels (rappelons que la théorie générale des anneaux et des corps est précisément née au début du XX^e siècle, en particulier sous l'impulsion des idées de Hensel). Mais si Hensel avait bien senti les simplifications qu'il pouvait apporter à certaines démonstrations de théorie des nombres à l'aide de cette localisation, il n'avait pas encore à disposition les notions topologiques (liées à celles d'espace métrique) qui clarifient l'étude des nombres p-adiques. Dès 1910 néanmoins, il peut calquer la théorie de Cauchy et faire de l'analyse p-adique, en définissant en particulier, exponentielle et logarithmes p-adiques.

L'utilité des nombres p-adiques apparaît clairement dans la recherche de solutions d'équations diophantiennes. Par exemple soit F un polynôme à n variables et à coefficients entiers. L'existence d'une solution entière

---

[1] Exposé présenté au groupe des mathématiciens rhodaniens le 6 mai 1973.

$(x_1, ..., x_n)$ de l'équation $F(x_1, ..., x_n) = 0$ implique l'existence de solutions pour toutes les congruences

$$F(x_1, ..., x_n) \equiv 0 \bmod m \qquad (m \geqslant 2). \tag{2}$$

Comme on sait bien, il suffit de considérer ces congruences modulo les puissances p^k de nombres premiers. Or il se trouve que les congruences

$$F(x_1, ..., x_n) \equiv 0 \bmod p^k \tag{3}$$

peuvent être résolues pour tout $k \geqslant 1$ si et seulement si $F(x_1, ..., x_n) = 0$ a une solution $(x_1, ..., x_n)$ à coordonnées dans l'anneau des entiers p-adiques $\mathbf{Z}_p$ (lemme de Hensel). L'anneau des entiers p-adiques $\mathbf{Z}_p$ apparaît comme limite des anneaux $\mathbf{Z}/p^k\mathbf{Z}$: $\mathbf{Z}_p = \varprojlim \mathbf{Z}/p^k\mathbf{Z}$. L'avantage est ici que $\mathbf{Z}_p$ est intègre (alors que $\mathbf{Z}/p^k\mathbf{Z}$ avait des éléments nilpotents ...) et admet un corps de fractions

$$\mathbf{Q}_p = \mathbf{Z}_p \underset{\mathbf{Z}}{\otimes} \mathbf{Q} = \mathbf{Z}_p[p^{-1}]. \tag{4}$$

Dans une première étape de la recherche de solutions entières, on pourra essayer de résoudre $F(x_1, ..., x_n) = 0$ dans tous les corps p-adiques $\mathbf{Q}_p$. Il peut aussi être intéressant d'en rechercher les solutions réelles, par exemple l'équation $x^2 + y^2 + 1 = 0$ ne saurait avoir de solutions entières ! Il arrive que l'existence de solutions *locales* pour tout p (c'est-à-dire dans $\mathbf{Q}_p$ pour tout p) implique l'existence d'une solution globale (dans $\mathbf{Q}$). C'est par exemple le cas si F est une forme quadratique. Plus précisément, dénotons par P l'ensemble des nombres premiers, par $\bar{P}$ la réunion de P et d'un symbole ∞, et par $\mathbf{Q}_\infty = \mathbf{R}$. Alors si F est une forme quadratique à coefficients rationnels en n variables, pour que $F(x_1, ..., x_n) = 0$ ait une solution non triviale $x = (x_1, ..., x_n) \neq 0$ à coordonnées x_i entières (ou rationnelles), il faut et il suffit que l'on puisse en trouver des solutions non triviales à coordonnées dans $\mathbf{Q}_p$: $0 \neq x = (x_1, ..., x_n) \in \mathbf{Q}_p^n$ *pour tout* $p \in \bar{P}$. C'est le théorème de Hasse-Minkowski (cf. [5] Chap. IV, Théorème 8). On voit ici que les nombres p-adiques doivent être placés sur un pied d'égalité avec les nombres réels. En fait si on dénote par $|\ldots|_p$ la valeur absolue p-adique de $\mathbf{Q}$ définie par

$$|a|_p = p^{-ord_p(a)} \qquad (0 \neq a \in \mathbf{Q}), \tag{5}$$

le corps $\mathbf{Q}_p$ est le complété de $\mathbf{Q}$ pour la topologie définie par la métrique p-adique $d_p(a, b) = |a - b|_p$. On voit ainsi mieux l'analogie entre les corps p-adiques ($p \in P$) et le corps des nombres réels $\mathbf{Q}_\infty = \mathbf{R}$ complété de

$\mathbf{Q}$ pour la distance définie par la valeur absolue usuelle $|a|_\infty = |a|$. Pour obtenir des énoncés complets, il est souvent nécessaire de regarder simultanément toutes les places $p \in \bar{P}$ et d'associer à un nombre rationnel la famille de ses développements en tous les nombres premiers $p \in P$ et sa coordonnée réelle. Cela revient à plonger $\mathbf{Q}$ dans le produit de ses complétés $\prod_{\bar{P}} \mathbf{Q}_p$ à l'aide de l'application diagonale.

Prenons encore un exemple tiré de l'analyse classique pour illustrer l'importance des nombres p-adiques, considérés simultanément avec des nombres complexes. Partons d'une fonction analytique

$$f(z) = \sum_{n \geqq 0} a_n z^n \qquad (a_n \in \mathbf{Z}) \tag{6}$$

dont le développement de Taylor à l'origine a tous ses coefficients entiers. Il y a beaucoup de telles fonctions, par exemple $f(z) = 1/(1-z)$ ou bien le discriminant Δ de la théorie des fonctions elliptiques $\Delta(z) = z \prod_{n \geqq 1} (1-z^n)^{24} = \sum_{n \geqq 1} \tau(n) z^n$ (les coefficients $\tau(n)$ étant par définition les coefficients de Ramanujan). Remarquons que si le rayon de convergence ρ de la série (6) est strictement plus grand que 1, la convergence en $z = 1$ implique que a_n tend vers 0 (par valeurs entières !), donc est nul pour n assez grand. Dans ce cas donc, f est nécessairement une fonction polynomiale. E. Borel a donné la variante plus intéressante suivante de cet énoncé:

(7) *Si une fonction analytique f, définie par un développement* (6) *à coefficients entiers se prolonge en fonction méromorphe dans un cercle de rayon $\rho > 1$, alors f se prolonge en fonction rationnelle sur* $\mathbf{C}$. [1])

Comme on le prévoit facilement, ce critère n'est pas très maniable dans les applications et Dwork l'a grandement généralisé à l'occasion de sa démonstration de rationalité de la fonction zêta d'une variété algébrique définie sur un corps fini (cf. [3] § 4, Théorèmes 2 et 3). Le critère de Dwork s'applique aux fonctions analytiques f définies par un développement de Taylor à l'origine ayant tous ses coefficients rationnels (et non plus seulement entiers). Pour l'énoncer, il faut considérer les fonctions analytiques p-adiques f_p $(p \in P)$ ayant même développement que f mais où la variable $z = x_p$ appartient à un complété Ω_p d'une clôture algébrique $\bar{\mathbf{Q}}_p$ de $\mathbf{Q}_p$ (ces

[1] Citons peut-être à ce propos le théorème de Nagy-Carlson: Si une fonction analytique f admet un développement $\Sigma a_n z^n$ à cœfficients entiers de rayon de convergence 1, alors ou bien f est rationnelle, ou bien $|z| = 1$ est frontière naturelle de f. Nous ne nous intéresserons qu'au cas ou f est rationnelle, aussi laisserons-nous de côté cet aspect de la question.

corps Ω_p sont complets et algébriquement clos, et jouent un rôle de domaine universel analogue au corps $\mathbf{C}$ des nombres complexes). Une remarque préliminaire s'impose. Si $f(z) = \sum a_n z^n$ est une fonction analytique donnée par un développement ayant tous ses coefficients rationnels, et si f se prolonge comme fonction rationnelle, alors, elle est quotient de deux polynômes à coefficients rationnels (ou même entiers). C'est un théorème de Fatou. Par conséquent l'algorithme de division des polynômes suivant les puissances croissantes montre que seuls les facteurs premiers du terme constant du dénominateur peuvent apparaître dans les dénominateurs des coefficients a_n. En dénotant donc par S l'ensemble fini des diviseurs premiers de ce terme constant, on voit que les coefficients a_n sont tous dans l'anneau $\mathbf{Z}[S]^{-1}$ engendré par les entiers et les inverses des nombres premiers $p \in S$. Le théorème de Dwork est alors le suivant.

(8) *Pour qu'une fonction analytique f définie par un développement $\sum a_n z^n$ à coefficients rationnels représente une fonction rationnelle, il faut et il suffit qu'il existe une partie finie $S \subset P$ avec $a_n \in \mathbf{Z}[S]^{-1}$ $(n \geqslant 0)$ et des nombres positifs r_p $(p \in \bar{S} = S \cup \{\infty\})$ avec $\prod_{\bar{S}} r_p > 1$, tels que f_p se prolonge comme fonction méromorphe (quotient de deux holomorphes) dans le disque $|x_p|_p < r_p$ de Ω_p pour tout $p \in \bar{S}$ $(\Omega_\infty = \mathbf{C})$.*

La condition $a_n \in \mathbf{Z}[S]^{-1}$ exprime simplement le fait que les nombres rationnels $a_n \in \mathbf{Z}_p$ sont des entiers p-adiques pour les nombres premiers $p \notin S$, ou encore que $|a_n|_p \leqslant 1$ pour $p \in P - S$. Donc les fonctions analytiques f_p sont holomorphes dans le disque unité $|x_p|_p < 1$ de Ω_p pour $p \in P - S$. En choisissant $r_p = 1$ pour $p \in P - S$, la condition de produit s'exprime plus symétriquement par $\prod_{\bar{P}} r_p > 1$. D'autre part, lorsque tous les coefficients a_n sont entiers, on pourra prendre pour S l'ensemble vide, et le critère ci-dessus redonne le résultat de Borel (7). En général au contraire, on aura avantage à prendre dans (8) $r_\infty = \rho$ (rayon de convergence de la série complexe de $f = f_\infty$), et d'aller « plus loin » dans un corps p-adique Ω_p qui s'y prête ! Dwork lui-même utilise (8) sous la forme suivante: une série à coefficients entiers qui a un rayon de convergence complexe $\rho \neq 0$ et qui se prolonge comme fonction méromorphe sur un corps p-adique Ω_p, représente une fonction rationnelle.

J'espère que les exemples précédents montrent l'opportunité de tenir compte de tous les complétés p-adiques de $\mathbf{Q}$ et non seulement du complété privilégié $\mathbf{R} = \mathbf{Q}_\infty$, et d'introduire un anneau contenant $\mathbf{Q}$ et tous les

$\mathbf{Q}_p$ ($p \in \bar{P}$). Malheureusement, le premier candidat qui se présente à l'esprit, le produit $\prod_{\bar{P}} \mathbf{Q}_p$, n'est pas localement compact (un produit d'espaces localement compacts ne peut être localement compact que si tous ses facteurs sauf un nombre fini, sont compacts). L'astuce (complétement négligée par Hensel et ses successeurs immédiats) consiste à se restreindre au sous-anneau formé des familles $(x_p)_{p\in\bar{P}}$ ne présentant qu'un nombre fini de pôles: $x_p \in \mathbf{Z}_p$ pour presque tous les $p \in P$. Ce produit restreint [1])

$$\mathbf{A} = \{(x_p) \in \prod_{P} \mathbf{Q}_p : x_p \in \mathbf{Z}_p \text{ pour presque tout } p \in P\} \tag{9}$$

est l'anneau des *adèles*. C'est le plus petit anneau contenant (des sous-anneaux isomorphes à) $\mathbf{Q}_p$ ($p \in \bar{P}$) et $\prod_{P} \mathbf{Z}_p$. On munit $\mathbf{A}$ de la topologie de groupe additif qui induit sur le sous-groupe $\mathbf{R} \times \prod_{P} \mathbf{Z}_p$ la topologie produit. Ce sous-groupe est à la fois ouvert et fermé dans $\mathbf{A}$ (et localement compact puisque les anneaux d'entiers p-adiques sont compacts), et la multiplication de $\mathbf{A}$ est continue. Puisqu'un nombre rationnel n'a qu'un nombre fini de pôles (nombres premiers divisant son dénominateur), l'injection diagonale canonique applique $\mathbf{Q}$ dans $\mathbf{A}$, et il est facile de voir que la topologie induite par $\mathbf{A}$ sur $\mathbf{Q}$ est la topologie discrète (canonique...). En effet, $V =]-1, +1[\times \prod \mathbf{Z}_p$ est un voisinage ouvert de 0 dans $\mathbf{A}$ par définition, et les nombres rationnels qui tombent dans V doivent *primo :* être des entiers p-adiques pour tout $p \in P$, donc ne pas avoir de dénominateur, c'est-à-dire être des entiers, *secundo :* avoir une image réelle dans l'intervalle ouvert $]-1, +1[$.

Ainsi on a bien $\mathbf{Q} \cap V = \{0\}$. Une propriété fondamentale de l'anneau localement compact des adèles est la suivante: $\mathbf{A}$ est isomorphe (en tant que groupe localement compact abélien additif) à son dual de Pontryagin. Plus précisément, la suite exacte

$$0 \to \mathbf{Q}_{discr.} \to \mathbf{A} \to \mathbf{A}/\mathbf{Q} \to 0 \tag{10}$$

admet pour duale (de Pontyagin) la suite exacte

$$0 \leftarrow \mathbf{A}/\mathbf{Q} \leftarrow \mathbf{A} \leftarrow \mathbf{Q}_{discr.} \leftarrow 0.$$

Le quotient $\mathbf{A}/\mathbf{Q}$ est donc compact (dual du groupe additif discret $\mathbf{Q}$). On pourra comparer la suite précédente aux suites autoduales

$$0 \to \mathbf{Z}_p \to \mathbf{Q}_p \to \mathbf{Q}_p/\mathbf{Z}_p \to 0 \qquad (p \in \bar{P}) \tag{11}$$

---

[1] La notion générale de produit restreint est due à Braconnier.

(on a posé $\mathbf{Z}_\infty = \mathbf{Z}$). D'ailleurs, la suite (10) n'est pas sans présenter une analogie frappante avec la suite $(11)_\infty$

$$0 \to \mathbf{Z} \to \mathbf{R} \to \mathbf{R}/\mathbf{Z} \to 0\,, \tag{12}$$

puisque $\mathbf{Q}$ est discret dans $\mathbf{A}$ comme $\mathbf{Z}$ l'est dans $\mathbf{R}$. On a mieux puisque $\mathbf{A}/\mathbf{Q}$ est connexe comme $\mathbf{R}/\mathbf{Z}$ (une petite surprise puisque dans la définition de l'anneau des adèles par l'égalité (9), tous les facteurs sauf $\mathbf{Q}_\infty = \mathbf{R}$ sont totalement discontinus; il se trouve que ce facteur connexe a une image dense dans le quotient), et on peut identifier $\mathbf{A}/\mathbf{Q}$ au solénoïde $\varprojlim_N \mathbf{R}/N\,\mathbf{Z}$, lui-même limite projective des revêtements du cercle (la relation d'ordre filtrante sur l'ensemble des indices est fournie par la divisibilité puisqu'on a des applications canoniques de transition $\mathbf{R}/N\,\mathbf{Z} \to \mathbf{R}/M\,\mathbf{Z}$ lorsque N est multiple de M). Il est aussi intéressant de considérer le groupe multiplicatif $\mathbf{A}^\times$ des unités de $\mathbf{A}$. Comme la topologie induite par $\mathbf{A}$ sur $\mathbf{A}^\times$ ne rend pas continue l'application $x \mapsto x^{-1}$, on préfère munir $\mathbf{A}^\times$ de la topologie induite par l'injection $x \mapsto (x, x^{-1})$ de $\mathbf{A}^\times$ dans $\mathbf{A}^2$. (Ainsi $\mathbf{A}^\times = G\,L_1\,(\mathbf{A})$ est muni de la topologie initiale relativement aux applications $x \mapsto x$ et $x \mapsto x^{-1}$ de $\mathbf{A}^\times$ dans $\mathbf{A}$: on force l'inverse à être continu). C'est ce groupe topologique $\mathbf{A}^\times$ qui est le groupe des *idèles*. Il est clair que tout nombre rationnel non nul définit une unité de $\mathbf{A}$ et que par conséquent $\mathbf{Q}^\times$ s'identifie à un sous-groupe discret de $\mathbf{A}^\times$. Le quotient $\mathbf{A}^\times/\mathbf{Q}^\times$ n'est pas compact pour la raison suivante. Tout idèle $x = (x_p)_{\bar{P}}$ a des composantes $x_p \in \mathbf{Q}_p^\times$ satisfaisant $x_p \in \mathbf{Z}_p^\times$ presque pour tout $p \in P$. Donc le produit infini $\prod_{\bar{P}} |\,x_p\,|_p$ converge (il n'a qu'un nombre fini de facteurs $\neq 1$) et on a un morphisme continu surjectif

$$\mathbf{A}^\times \to \mathbf{R}^\times \textit{ defini par } x \mapsto |\,x\,|_{\mathbf{A}} = \prod_{\bar{P}} |\,x_p\,|_p\,. \tag{13}$$

Le noyau de ce morphisme contient $\mathbf{Q}^\times$: par exemple d'après (5)

$|\,2/15\,|_2 = \frac{1}{2}$ (zéro simple en $p = 2$),

$|\,2/15\,|_3 = 3$ (pôle simple en $p = 3$),

$|\,2/15\,|_5 = 5$ (pôle simple en $p = 5$),

$|\,2/15\,|_p = 1$ si $p \in P$ et $p \neq 2, 3, 5$ (unité p-adique),

$|\,2/15\,|_\infty = 2/15$,

de sorte que le produit vaut bien 1. On entrevoit bien que ce genre d'argument est général. Le module idèlique définit ainsi un morphisme continu

surjectif $\mathbf{A}^\times/\mathbf{Q}^\times \to \mathbf{R}$ qui empêche le quotient $\mathbf{A}^\times/\mathbf{Q}^\times$ d'être compact. Par contre si on se restreint au sous-groupe $\mathbf{A}^1/\mathbf{Q}^\times$ formé des classes d'idèles de module 1 (noyau du morphisme précédent), on obtient un groupe compact.

Le terme *idèle* a été introduit par Chevalley en 1936 dans une rédaction algébrique de la théorie du corps de classes. Il était suggéré par la façon dont les idèles représentent un raffinement de la notion d'idéal. Indiquons sommairement comment les idèles apparaissent dans ce contexte. Partons d'un corps de nombres algébriques $k : [k: \mathbf{Q}] < \infty$. Le groupe de Galois $G = \mathrm{Gal}\,(\bar{k}/k)$ peut être topologisé de façon à avoir une correspondance biunivoque entre sous-groupes fermés et extensions intermédiaires de $\bar{k}/k$ (topologie de Krull). Ce groupe topologique G est compact et totalement discontinu, et seul son abélianisé est relativement bien connu. On remarque que le sous-groupe fermé $\overline{[G, G]}$ engendré par les commutateurs correspond à la plus grande extension k_{ab} de k (contenue dans $\bar{k}$) ayant un groupe de Galois abélien sur k:

$$\mathrm{Gal}\,(k_{ab}/k) = G/\overline{[G, G]} = G_{ab}\,.$$

La théorie du corps de classes a pour premier but d'établir un isomorphisme canonique entre ce groupe topologique G_{ab} et un groupe de classes d'idèles de k, plus précisément le groupe totalement discontinu des composantes connexes de $k_{\mathbf{A}}^\times/k^\times$ ou de $k_{\mathbf{A}}^1/k^\times$. On a posé $k_{\mathbf{A}} = k \underset{\mathbf{Q}}{\otimes} \mathbf{A}$ (ces adèles de k pourraient aussi être définis directement à l'aide des idéaux premiers de k et des places « à l'infini », comme produit restreint de tous les complétés de k.) Comme par exemple le groupe des classes d'idéaux de l'anneau des entiers de k (modulo les idéaux principaux) est un quotient de $k_{\mathbf{A}}^\times/k^\times$, il en résulte qu'à ce groupe $C\,(k)$ de classes d'idéaux fractionnaires de k correspond une extension abélienne $k_{nr} \subset k_{ab}$ bien déterminée de k (de degré fini) avec

$$\mathrm{Gal}\,(k_{nr}/k) = C\,(k)\,,$$

Cette extension k_{nr} (corps de classes absolu de Hilbert) peut être caractérisée intrinsèquement (par des propriétés de non ramification sur k), d'où son intérêt dans la recherche de la structure du groupe $C\,(k)$. L'analogue additif des idèles, *les adèles*, n'a été introduit qu'ultérieurement et J. Tate utilise encore dans sa thèse (1950) le terme « valuation vector » pour ce qu'on appelle aujourd'hui « adèle ».

Les adèles constituent un langage (voire un outil) idéal pour la formulation de tous les problèmes qui traitent d'une connexion entre local et global, ces termes étant bien entendu pris dans leur acception en algèbre commutative, inspirée par le modèle géométrique Spec (A) d'un anneau commutatif A. En un certain sens, on peut comparer les adèles en arithmétique aux faisceaux en géométrie analytique, à condition de remplacer la cohomologie des faisceaux par l'analyse (analyse harmonique, transformations intégrales, ...) Par exemple, la suite exacte (10) (et les suites analogues qu'on en dérive) effectue une liaison entre une situation rationnelle (ou globale, sur $\mathbf{Q}$) et une situation comparable adélique (ou locale, sur $\mathbf{A}$) grâce à la présence du terme « correcteur » $\mathbf{A}/\mathbf{Q}$ de nature mixte. Les groupes $\mathbf{A}$ et $\mathbf{A}/\mathbf{Q}$ se prêtent mieux à l'analyse que le groupe $\mathbf{Q}$ discret. Un nouvel exemple illustrera probablement mieux que des phrases ce phénomène. Nous partirons de la thèse de Tate (publiée pour la première fois en 1967 dans [2]) où le problème était de dériver les équations fonctionnelles de la fonction zêta et des fonctions L d'un corps de nombres par des méthodes locales. Choisissons le cas le plus simple de la fonction zéta de $\mathbf{Q}$ (fonction zêta de Riemann). On peut définir une fonction canonique $\Phi : \mathbf{A} \to \mathbf{R}$ par produit de fonctions locales $\Phi_p : \mathbf{Q}_p \to \mathbf{R}$ où

$$\Phi_\infty(t) = \exp(-\pi t^2),$$
$$\Phi_p = \text{fonction caractéristique de } \mathbf{Z}_p \subset \mathbf{Q}_p \ (p \in P).$$

En effet, $x = (x_p) \in \mathbf{A}$ implique $x_p \in \mathbf{Z}_p$ pour presque tout $p \in P$ et le produit infini

$$\Phi(x) = \prod_{p \in \bar{P}} \Phi_p(x_p)$$

converge (presque tous ses facteurs valent 1). Les fonctions Φ_p sont caractérisées par la propriété d'être égales à leur transformées de Fourier (pour la mesure de Haar autoduale sur $\mathbf{Q}_p$) pour tout $p \in \bar{P}$. La transformée de Mellin de cette fonction canonique

$$Z(s) = Z_{\mathbf{Q}}(s) = \int_{\mathbf{A}^\times} \Phi(x) \, |x|_{\mathbf{A}}^{s} \, d^\times x \quad (s \in \mathbf{C}), \tag{14}$$

est une fonction d'une variable complexe s, définie dans un domaine qu'on va préciser. On doit considérer cette fonction comme un invariant attaché à $\mathbf{Q}$ (invariant que l'on pourra éventuellement comparer aux autres Z_k associés à des corps de nombres k puisque toutes ces fonctions sont définies dans le même plan complexe $\mathbf{C}$). Voyons comment on peut calculer cet invariant (dans un domaine de convergence absolue de l'intégrale). Une méthode *locale* s'impose premièrement puisque l'intégrant est un produit

de fonctions ne dépendant chacune que d'une coordonnée p-adique. Le produit restreint sur lequel on intègre se décompose lui aussi et une analyse précise des définitions justifie le calcul de (14) par produit d'intégrales locales

$$Z(s) = \prod_P Z_p(s) = \prod_P \int_{\mathbf{Q}_p^\times} \Phi_p(x_p) \mid x_p \mid_p^s d^\times x_p$$

qui peuvent se calculer individuellement. On a

$$Z_\infty(s) = \int_{\mathbf{R}^\times} \exp(-\pi t^2) \mid t \mid^s d^\times t =$$

$$= 2 \int_0^\infty \exp(-\pi t^2)\, t^{s-1}\, dt = \pi^{-s/2}\, \Gamma(s/2),$$

et aussi

$$Z_p(s) = \int_{\mathbf{Z}_p - 0} \mid x_p \mid_p^s d^\times x_p =$$

$$= \int_{\bigcup_{k \geqq 0} p^k \mathbf{Z}_p^\times} \mid x_p \mid_p^s d^\times x_p =$$

$$= \sum_{k \geqq 0} p^{-ks} = (1 - p^{-s})^{-1}$$

(en choisissant la mesure multiplicative sur $\mathbf{Q}_p^\times$ normalisée par la condition de donner volume unité à $\mathbf{Z}_p^\times$ et donc aussi aux classes $p^k \mathbf{Z}_p^\times$). Ces intégrales locales existent pour $Re(s) > 0$ et leur produit

$$(15) \qquad Z(s) = \prod_P Z_p(s) = \pi^{-\frac{1}{2}s}\, \Gamma(\tfrac{1}{2}s) \prod_P (1 - p^{-s})^{-1} =$$

$$= \pi^{-\frac{1}{2}s}\, \Gamma(\tfrac{1}{2}s)\, \zeta(s)$$

est absolument convergent pour $Re(s) > 1$. C'est le domaine de convergence absolue de l'intégrale (14).

Il y a une méthode plus *globale* de traiter l'intégrale (14) qui conduit à son prolongement analytique. Séparons l'intégrale en deux portions $Z(s) = Z'(s) + Z''(s)$ où

$$Z'(s) = \int_{\mid x \mid_{\mathbf{A}} \geqq 1} \Phi(x) \mid x \mid_{\mathbf{A}}^s d^\times x$$

est une fonction entière de s, et

$$Z''(s) = \int_{\mid x \mid_{\mathbf{A}} \leqq 1} \Phi(x) \mid x \mid_{\mathbf{A}}^s d^\times x\,.$$

Pour calculer cette dernière intégrale, on peut commencer à rendre son intégrant invariant sous $\mathbf{Q}^\times$ (le module idélique est déjà invariant par les multiplications rationnelles). Il ne reste ensuite plus qu'à intégrer sur les classes d'idèles mod $\mathbf{Q}^\times$

$$Z''(s) = \int_{\mid \dot{x} \mid \leqq 1} \sum_{\mathbf{Q}^\times} \Phi(\xi x) \mid \dot{x} \mid^s d^\times \dot{x}\,.$$

La formule sommatoire de Poisson va nous permettre de transformer l'intégrant. En effet, avec $\Phi_x(\xi) = \Phi(\xi x)$, elle s'écrit

$$\sum_{\mathbf{Q}} \Phi_x(\xi) = \sum_{\mathbf{Q}} \widehat{\Phi}_x(\xi)$$

où l'on a introduit la transformée de Fourier $\widehat{\Phi}_x$ de Φ_x. Cette transformée de Fourier se calcule en complète analogie avec le cas classique en introduisant une exponentielle normalisée $\underline{e}$ qui permet d'identifier $\mathbf{A}$ à son dual de Pontryagin

$$\mathbf{A} \times \mathbf{A} \to \mathbf{C}^1$$
$$(x, y) \mapsto \underline{e}(xy).$$

Ainsi

$$\widehat{\Phi}_x(\xi) = \int_{\mathbf{A}} \Phi_x(y)\, \underline{e}(\xi y)\, dy = \int \Phi(xy)\, \underline{e}(\xi y)\, dy =$$
$$= \int \Phi(y)\, \underline{e}(\xi x^{-1} y)\, |x|_{\mathbf{A}}^{-1}\, dy = |x|_{\mathbf{A}}^{-1}\, \Phi(x^{-1}\xi).$$

En mettant hors de la somme les termes d'indice $\xi = 0$ dans la formule de Poisson, et en tenant compte du fait que ϕ a été choisie de façon à être égale à sa transformée de Fourier avec $\widehat{\Phi}(0) = \Phi(0) = 1$ on voit que

$$1 + \sum_{\mathbf{Q}^\times} \Phi(\xi x) = |x|_{\mathbf{A}}^{-1} + |x|_{\mathbf{A}}^{-1} \sum_{\mathbf{Q}^\times} \Phi(x^{-1}\xi).$$

On a donc montré que

$$Z''(s) = \int_{|\dot{x}| \leq 1} \{ |\dot{x}|^{-1} - 1 + |\dot{x}|^{-1} \sum_{\mathbf{Q}^\times} \Phi(x^{-1}\xi) \}\, |\dot{x}|^s\, d^\times \dot{x}.$$

D'abord il s'agit de calculer

$$\int_{|\dot{x}| \leq 1} |\dot{x}|^{s-1}\, d^\times \dot{x} = \int_0^1 t^{s-1}\, d^\times t \int_{\mathbf{A}/^1\mathbf{Q}^\times} d^\times \dot{x} =$$
$$= \int_0^1 t^{s-1}\, dt/t = \left[\frac{t^{s-1}}{s-1}\right] = \frac{1}{s-1}.$$

Ensuite il reste une intégrale à estimer:

$$\int_{|\dot{x}| \leq 1} |\dot{x}|^{-1} \sum_{\mathbf{Q}^\times} \Phi(x^{-1}\xi)\, |\dot{x}|^s\, d^\times \dot{x} =$$
$$= \int_{|\dot{y}| \geq 1} \sum_{\mathbf{Q}^\times} \Phi(y\xi)\, |\dot{y}|^{1-s}\, d^\times \dot{y} = Z'(1-s),$$

et cette intégrale se prolonge en fonction entière. En résumé, on a trouvé

$$Z(s) = Z'(s) + Z''(s) = Z'(s) + \frac{1}{s-1} - \frac{1}{s} + Z'(1-s).$$

On voit ici que $Z(s)$ se prolonge comme fonction méromorphe en $s \in \mathbf{C}$ avec un pôle simple en $s = 1$ (résidu 1) et un pôle simple en $s = 0$ (résidu -1). De plus cette fonction prolongée satisfait l'équation fonctionnelle

$$(16) \qquad Z(s) = Z(1-s), \quad Z(s) = \pi^{-\frac{1}{2}s}\Gamma(\tfrac{1}{2}s)\zeta(s),$$

qui n'est autre que l'équation fonctionnelle de Riemann.

Dans sa thèse, Tate a même montré comment on peut dériver cette équation fonctionnelle par une méthode locale, en démontrant des équations fonctionnelles locales pour toutes les $Z_p(s)$ $(p \in \bar{P})$. Ses méthodes ont été généralisées par Jacquet et Langlands pour le groupe Gl_2 (au lieu de Gl_1).

Donnons une application frappante du principe de calcul de fonctions zêta où une intégrale adélique (transformée de Mellin) permet de passer de données *locales* à un résultat *global.* Il s'agit du résultat de base de la théorie du groupe de Brauer:

(17) *Soient M et M' deux algèbres centrales simples de rang n^2 fini sur $\mathbf{Q}$. On suppose que pour tout $p \in \bar{P}$, $M_p = M \otimes_{\mathbf{Q}} \mathbf{Q}_p$ est isomorphe à la localisée correspondante M'_p de M'. Alors M et M' sont (globalement) isomorphes.*

Le principe de démonstration est le suivant. En se plaçant dans le groupe de Brauer (où on considère comme triviales les algèbres centrales simples isomorphes aux algèbres de matrices $M(n, \mathbf{Q})$, on voit qu'on est ramené à voir que si une algèbre à division M centrale sur $\mathbf{Q}$ est localement triviale, i.e. isomorphe à une algèbre de matrices pour tout $p \in \bar{P}$, alors $M = \mathbf{Q}$:

$$\left.\begin{array}{l} M \text{ corps gauche de centre } \mathbf{Q} \\ M_p \text{ isomorphe à } \mathrm{M}(n, \mathbf{Q}_p) \text{ pour } p \in \bar{P} \end{array}\right\} \Rightarrow \mathrm{M} = \mathbf{Q} \ (n=1).$$

Pour cela, on compare les invariants

$$Z_M(s) \ (M \text{ corps gauche de centre } \mathbf{Q}) \text{ et } Z_{M(n, \mathbf{Q})}(s).$$

Puisque ces invariants peuvent se calculer par une méthode locale, l'hypothèse implique l'égalité $Z_M = Z_{M(n, \mathbf{Q})}$. D'autre part, le calcul global que nous avons fait pour prolonger analytiquement $Z_{\mathbf{Q}}$ s'applique avec quelques modifications pour le prolongement de Z_M et montre que cette

fonction se prolonge en fonction méromorphe ayant deux pôles simples en $s = 0$ et $s = n$. Mais le calcul local de la fonction zêta d'une algèbre de matrices peut être effectué complètement en utilisant le théorème des diviseurs élémentaires et conduit à

$$Z_{M(n,\mathbf{Q})}(s) = Z(s)Z(s-1)\cdot\ldots\cdot Z(s-(n-1)) \quad (Z = Z_{\mathbf{Q}}),$$

et montre donc que $Z_{M(n,\mathbf{Q})}$ possède des pôles simples en $s = 0$ et $s = n$ *et des pôles doubles en* $s = 1, 2, \ldots, n-1$. Cette fonction zêta ne peut donc être égale à la fonction zêta d'une algèbre à division que si $n = 1$, et cela prouve que $M = \mathbf{Q}$ est triviale. C'est cette méthode que A. Weil a choisie dans [8] pour montrer que l'homomorphisme canonique de localisation $Br(\mathbf{Q}) \to \prod_P Br(\mathbf{Q}_p)$ est injectif.

* * *

En conclusion, les adèles fournissent un langage pour traiter de problèmes d'arithmétique à l'aide d'analyse (entendue au sens d'analyse harmonique dans les groupes abéliens localement compacts par exemple). Les intégrales adéliques globales permettent parfois une comparaison profonde entre propriétés locales et globales d'objets algébriques, et dans ce sens, on peut comparer leur utilisation à celle de la cohomologie des faisceaux sur les variétés analytiques. Mais ce langage, même s'il permet une bonne formulation des problèmes, ne permet pas toujours de les résoudre. Il arrive au contraire qu'une généralisation suggérée par son utilisation défie — et de loin — toutes les méthodes connues et initie un vaste champ de conjectures ... D'autre part, il est probable que l'utilisation des adèles va continuer à se répandre et à influencer d'autres domaines mathématiques, comme elle l'a fait récemment en topologie algébrique.

BIBLIOGRAPHIE

[1] Bourbaki, N. *Algèbre Commutative, Chap. 7, Note Historique.* Paris, Hermann (1965), Act. Sc. et Ind. 1314.

[2] Cassels, J. W. L. and A. Frölich. *Algebraic Number Theory.* Washington D.C., Thompson Book Company Inc. (1967).

[3] Dwork, B. On the Rationality of the Zeta Function of an Algebraic Variety. *Amer. J. of Math., 82* (1960), pp. 630-648.

[4] JACQUET, H. and R. P. LANGLANDS. *Automorphic Forms on GL_2*. Berlin, Springer-Verlag (1970). Lecture Notes in Maths. 114.
[5] SERRE, J.-P. *Cours d'Arithmétique*. Paris, P.U.F. (1970), Collection Sup « Le Mathématicien ».
[6] TAMAGAWA, T. Adèles. *in Proc. of Symp. in Pure Mathematics, vol. IX*, Amer. Math. Soc., Providence R. I. (1966), pp. 113-121.
[7] WEIL, A. *Adeles and Algebraic Groups*. The Institute for Advanced Study, Princeton N.J. (1961).
[8] ——. *Basic Number Theory*. Berlin, Springer-Verlag (1967), Die Grundlehren..., Bd. 144.

(Reçu le 5 juin 1973)

Alain Robert
Institut de Mathématiques
Chantemerle 20
CH-2000 Neuchâtel 7