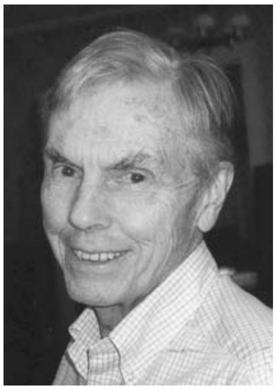
Le prix Wolf 2003 attribué à John Tate

Antoine Chambert-Loir

Le prix Wolf 2002/2003 a été attribué conjointement à l'analyste Mikio Sato et à l'arithméticien John T. Tate, ce dernier « pour sa céation de concepts fondamentaux en théorie algébrique des nombres ».



© AMS

John Tate

John Torrence Tate est né en 1925 à Minneapolis (États-Unis). En 1950, il a obtenu son Ph.D. à l'université de Princeton en 1950 sous la direction d'Emil Artin. De 1954 à 1990, il a été professeur à l'université de Harvard. Il a eu plus de 30 étudiants. Depuis 1990, il est professeur à l'université du Texas à Austin où il détient la chaire Sid W. Richardson. En 1995, la Société mathématique américaine (AMS) lui a décerné le prix Steele pour l'ensemble de son œuvre (« *lifetime achievement* »). À cette occasion, les *Notices* ont publié dans leur numéro de novembre 1995 une brève présentation chronologique des travaux de J. Tate.

Cependant, la seule lecture des titres des articles, dans l'ordre chronologique, peut donner l'impression (d'ailleurs fausse) que les articles de Tate se suivent, sans liens précis ; à leur étude se dégage au contraire une unité assez impressionnante. Je me limiterai aux travaux concernant la géométrie algébrique et l'arithmétique et, par commodité, je les répartirai en quatre groupes : sa thèse, puis ses travaux autour de la théorie du corps de classes, ceux concernant les courbes elliptiques et variétés abéliennes, et enfin ceux consacrés aux théories p-adiques.

La thèse de Tate

La fonction zêta de Riemann possèdait à la fin du XIX$^{\text{e}}$ siècle deux sortes de généralisations. Pour démontrer l'existence d'une infinité de nombres premiers dans une progression arithmétique $a, a+n, a+2n, \ldots$, a et n étant deux entiers premiers entre eux, Dirichlet avait introduit des séries de la forme

$$L(\chi, s) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s},$$

où χ est un *caractère* modulo n, c'est-à-dire une fonction $\chi\colon \mathbf{Z} \to \mathbf{C}$ telle que $\chi(ab) = \chi(a)\chi(b)$, $\chi(1) = 1$, $\chi(a+n) = \chi(a)$, et telle que $\chi(a) = 0$ si a n'est pas premier à n. Ces séries convergent pour $\mathrm{Re}(s) > 1$ et ont des prolongements méromorphes à $\mathbf{C}$ tout entier. Si le caractère χ est *primitif*, $L(\chi, s)$ vérifie l'équation fonctionnelle

$$\Lambda(\chi, 1-s) = \varepsilon(\chi)\Lambda(\chi, s) \quad \text{avec} \quad \Lambda(\chi, s) = (n/\pi)^{s/2}\Gamma((s+c)/2)L(\chi, s),$$

Γ désignant la fonction Γ d'Euler, avec $c = 0$ si $\chi(-1) = 1$, $c = 1$ si $\chi(-1) = -1$, et dans laquelle $\varepsilon(\chi)$ est un nombre complexe explicite.

L'autre généralisation, introduite par Dedekind, concerne les *corps de nombres*, c'est-à-dire les sous-corps de $\mathbf{C}$ qui sont de dimension finie sur $\mathbf{Q}$. Un élément d'un tel corps K est racine d'un polynôme unitaire à coefficients rationnels. Par définition, les entiers de K sont ceux dont un tel polynôme annulateur est à coefficients entiers ; ils forment un anneau R_K. Si I est un idéal non nul de R_K, l'anneau quotient R_K/I est fini ; notons $N(I)$ son cardinal (*norme* de l'idéal I). La fonction zêta de Dedekind est alors définie par la série

$$\zeta_K(s) = \sum_{I \neq 0} \frac{1}{N(I)^s}, \quad \mathrm{Re}(s) > 1,$$

où I parcourt l'ensemble des idéaux non nuls de R_K. En 1917, E. Hecke a montré qu'elle possède un prolongement méromorphe à tout le plan complexe, avec un unique pôle simple en $s = 1$ et admet une équation fonctionnelle reliant $\zeta_K(s)$ à $\zeta_K(1-s)$. Un peu après, il a généralisé les fonctions L de Dirichlet pour les corps de nombres et démontré que les fonctions qu'il avait définies possèdent des propriétés analogues.

La fonction zêta de Riemann est définie indifféremment par la série $\sum_{n=1}^{\infty} n^{-s}$ ou par le produit $\prod_p (1 - p^{-s})^{-1}$, indexé par les nombres premiers. L'égalité de ces deux formules est un reflet analytique de l'unicité de la décomposition d'un entier en facteurs premiers. Un anneau tel que R_K n'est en général pas factoriel mais, ainsi que Kummer l'a découvert, il subsiste une décomposition des idéaux en produit d'idéaux maximaux ; c'est même de là que vient la notion d'idéal. Il en résulte que la fonction zêta de Dedekind admet une expression comme un produit indexé sur les idéaux maximaux, et il en est de même des fonctions L de Hecke.

Dans sa thèse, J. Tate redémontre les résultats de Hecke en se plaçant dans le cadre de l'*analyse de Fourier* sur le groupe topologique localement compact des adèles $\mathbf{A}_K$ du corps K. L'analyse harmonique, via la formule de Poisson, jouait déjà certainement un rôle dans les travaux antérieurs, mais de nombreuses complications provenaient de l'arithmétique, notamment parce que l'anneau R_K n'est pas forcément principal. De fait, le mélange des structures multiplicative et additive de K est plus aisé à manipuler dans le langage adélique : les transformées de Fourier sont des *produits* de transformées de Fourier « locales », chacune étant relativement facile à calculer. La « recombinaison » s'effectue via la formule sommatoire de Poisson adélique.

Ce point de vue s'avérera crucial pour la théorie des nombres de la seconde moitié du siècle, jusque dans la formulation même des conjectures de Langlands dont la thèse de Tate apparaît comme le cas le plus simple possible.

Théorie du corps de classes et cohomologie galoisienne

La théorie du corps de classes décrit les extensions abéliennes d'un corps, mais la solution n'est pas si explicite que cela. Il y a pourtant des énoncés très concrets. Par exemple, d'après le théorème de Kronecker–Weber, pour toute extension galoisienne $\mathbf{Q} \subset K$ dont le groupe de Galois est abélien, il existe un entier $n \geqslant 2$ (explicite) tel que K soit contenu dans le corps obtenu en adjoignant à $\mathbf{Q}$ les racines n-ièmes de l'unité. Le même énoncé vaut lorsque le corps $\mathbf{Q}$ est remplacé par le corps $\mathbf{Q}_p$ des nombres p-adiques.

Avec J. Lubin, Tate utilise la théorie des groupes formels pour construire explicitement les extensions abéliennes d'une extension finie K de $\mathbf{Q}_p$. Notons R l'anneau de valuation de K, π un générateur de l'idéal maximal de R et q le cardinal du corps fini $R/(\pi)$. Soit $f = X^q + a_{q-1}X^{q-1} + \cdots + a_2x + \pi x$ un polynôme à coefficients dans R tel que a_i soit divisible par π si $2 \leqslant i \leqslant q-1$. Définissons par récurrence sur n un élément π_n de $\bar{K}$ en prenant pour π_1 une racine non nulle de f et pour π_{n+1} une solution de l'équation $f(x) = \pi_n$ si $n \geqslant 1$. Alors, Lubin et Tate démontrent que toute extension abélienne de K est contenue dans l'extension engendrée par les racines de l'unité d'ordre premier à p et les π_n, $n \geqslant 1$. Les π_n s'interprètent naturellement comme des points de torsion d'un groupe formel (dit *de Lubin-Tate*) associé à f. Lorsque $K = \mathbf{Q}_p$ et $f = (1+X)^p - 1 = pX + \binom{p}{2}X^2 + \cdots + X^p$, ce groupe formel est le groupe multiplicatif et $1+\pi_n$ est une racine primitive de l'unité d'ordre p^n ; on retrouve ainsi la version locale du théorème de Kronecker–Weber.

Une description aussi explicite que cela reste inconnue dans le cas des corps de nombres généraux. Cela fait partie des problèmes de Hilbert non encore résolus. Une réponse partielle est donnée par les conjectures de Stark. Citons à ce propos un livre de Tate sur *les conjectures de Stark sur les fonctions L d'Artin en* $s = 0$ (Birkhäuser, 1984), dans lequel il approfondit les conjectures en question.

Dans un court article publié en 1952, J. Tate a calculé la *cohomologie galoisiene des classes d'idèles.* Les résultats qu'il obtient permettent de reformuler de manière très compacte certains énoncés de la théorie du corps de classes en termes de cohomologie galoisienne et de démontrer directement l'existence des « groupes de Weil », *cf.* le livre *Class field theory*, par Artin et Tate. Ce sont d'ailleurs les représentations de ces groupes, plutôt que celles des groupes de Galois, que le programme de Langlands a pour but d'élucider.

Tate a par la suite étudié systématiquement la cohomologie galoisienne des corps de nombres et des corps locaux. Il y démontre en particulier des théorèmes de dualité (dualité de Poitou–Tate) qui jouent un rôle fondamental dans toutes sortes de questions (conjecture de Birch et Swinnerton-Dyer, conjecture de Bloch–Kato, méthode des systèmes d'Euler introduite par Kolyvagin, travaux de Wiles,...).

La théorie du corps de classe entre aussi en jeu comme *outil* fondamental dans de nombreux travaux de Tate, par exemple lorsqu'il calcule le K_2 d'un corps de nombres en termes de cohomologie galoisienne, démontrant dans ce cas une conjecture de Milnor (finalement établie par les travaux de Voevodsky et Rost).

Courbes elliptiques et variétés abéliennes

Une courbe elliptique E est définie le plus souvent par une équation « affine » de la forme $Y^2 = X^3 + aX + b$, a et b dans un corps K, où l'on exige que le discriminant $\Delta = -4a^3 - 27b^2$ soit non nul. En ajoutant un point à l'infini, on sait depuis bien longtemps munir l'ensemble $E(K)$ des solutions *rationnelles*, c'est-à-dire dont les coordonnées sont dans K, d'une structure de groupe abélien dont la définition repose sur le fait que la droite passant par deux solutions rationnelles recoupe la courbe en une troisième. On obtient ainsi un groupe abélien, noté $E(K)$.

Lorsque K est le corps $\mathbf{Q}$ des nombres rationnels, L. Mordell a démontré que ce groupe est de type fini. Dit géométriquement, on peut obtenir toutes les solutions à partir d'un nombre fini d'entre elles par sécantes et tangentes. A. Weil a étendu ce résultat aux variétés abéliennes de dimension quelconque sur un corps de nombres arbitraire.

L'une des deux étapes de la démonstration repose sur des propriétés de la taille des solutions : les coordonnées $(x, y) \in \mathbf{Q}^2$ d'un point P ont un plus petit dénominateur commun $d \geqslant 1$. Posons alors $h(P) = \log \max(d, |dx|, |dy|)$ — c'est la *hauteur logarithmique* du point P ; la définition se généralise au cas d'un corps de nombres K. Restreinte à $E(K)$, cette hauteur possède une remarquable propriété de quadraticité : il existe une constante c telle que pour tous points P, Q, $R \in E(K)$,

$$|h(P+Q) + h(P-Q) - 2h(P) - 2h(Q)| \leqslant c.$$

Il est alors naturel de chercher une forme quadratique $q \colon E(K) \to \mathbf{R}$ telle que $h - q$ soit bornée ; elle induirait en effet une produit scalaire sur l'espace vectoriel $E(K) \otimes_{\mathbf{Z}} \mathbf{R}$.

A. Néron a montré qu'il existe effectivement une telle forme ; sa démonstration est à la fois très précise et relativement compliquée. La solution que J. Tate donne à ce problème est étonnamment simple : il suffit de poser

$$q(P) = \lim_{n\to\infty} h(nP)/n^2.$$

Cette forme quadratique est appelée depuis *hauteur de Néron-Tate*. Elle intervient de manière cruciale dans la formulation précise de la conjecture de Birch et Swinnerton-Dyer (BSD) concernant le terme principal de la fonction L d'une courbe elliptique sur $\mathbf{Q}$ en $s = 1$.

Soit $y^2 = x^3 + ax + b$ l'équation affine d'une courbe elliptique, où a et b sont deux entiers. La fonction L (partielle) d'une telle courbe est définie par le produit, indexé par les nombres premiers p qui ne divisent pas le discriminant $\Delta = -4p^3 - 27q^2$,

$$L_\Delta(s) = \prod_{p \nmid \Delta} \frac{1}{1 - a_p p^{-s} + p^{1-2s}},$$

où $a_p \in \mathbf{Z}$ est tel que l'équation $y^2 = x^3 + ax + b$ ait $p - a_p$ solutions dans $\mathbf{Z}/p\mathbf{Z}$. D'après un théorème de Hasse, on a $|a_p| \leqslant 2\sqrt{p}$ si bien que ce produit converge pour $\mathrm{Re}(s) > 3/2$ et y définit une fonction analytique de s. En complétant les travaux de Wiles qui ont mené à la solution du problème de Fermat, Breuil, Conrad, Diamond et Taylor ont montré en 2001 que cette fonction s'étend à tout le plan complexe et y admet une équation fonctionnelle, très jolie dès qu'on lui ajoute des facteurs convenables pour les p divisant le discriminant Δ. La conjecture (BSD), pour la fonction L complète, affirme que

$$\lim_{s\to 1} \frac{1}{(s-1)^r} L(s) = \big(\#\text{Ш}(E)\big) \frac{\det\langle P_i, P_j\rangle}{\#\mathrm{Tors(E)}^2} \alpha \prod_{p|\Delta} c_p.$$

Expliquons-en rapidement les divers ingrédients : Rappelons que $E(\mathbf{Q})$ est un groupe abélien de type fini, $\mathrm{Tors}(E)$ désigne son sous-groupe de torsion, r est son rang, $P_1, \ldots, P_r$ sont des points de $E(\mathbf{Q})$ tels que $E(\mathbf{Q}) = \mathbf{Z}P_1 \oplus \cdots \oplus \mathbf{Z}P_r \oplus$ Tors. On a désigné par $\langle \cdot, \cdot\rangle$ la forme bilinéaire associée à la forme quadratique de Néron-Tate et $\det\langle P_i, P_j\rangle$ désigne le déterminant de Gram correspondant. Intervient aussi l'ordre du groupe $\text{Ш}(E)$, dit de Tate-Shafarevich. En fait, même s'il y a des résultats partiels (Kolyvagin, Rubin), on ne sait pas si ce groupe est fini en général ! Finalement, α est l'intégrale elliptique

$$2\int \frac{dx}{\sqrt{x^3+ax+b}}$$

(on intègre là où le radicande est positif) et les c_p sont des entiers.

On doit à J. Tate plusieurs articles d'intérêt général concernant l'arithmétique des courbes elliptiques. Outre les exposés dans le tome IV des comptes-rendus de la conférence à Anvers en 1972, *Modular forms in one variable*, son article intitulé *The arithmetic of elliptic curves*, paru aux *Inventiones Math.* en 1974, présente un double point de vue théorique et pratique sur le sujet, notamment en ce qui concerne la détermination du *rang* de $E(K)$. Sur la base d'un cours professé en 1961, il a publié avec J. Silverman un livre sur le sujet, *Rational points on elliptic curves* (Undergraduate Texts in Mathematics, Springer-Verlag, 1992).

Les variétés abéliennes sont la généralisation des courbes elliptiques en dimension supérieure. Du point de vue de la géométrie algébrique complexe, ce sont les tores complexes (quotient de $\mathbf{C}^n$ par un réseau $\Lambda \simeq \mathbf{Z}^{2n}$) qui sont aussi des variétés algébriques. Leur existence même n'est pas triviale : pour un réseau arbitraire, il n'existe en général pas de fonction méromorphe Λ-périodique non constante sur $\mathbf{C}^n$!

Mais on peut aussi définir la notion de variété abélienne sur un corps K arbitraire : c'est un groupe algébrique projectif sur K. Lorsque le corps K est fini, J. Tate en a fourni une classification *à isogénie près* — dans l'analogie complexe, cela revient à considérer deux réseaux commensurables comme équivalents — et le résultat final est très simple : deux variétés abéliennes définies sur un corps fini sont isogènes dès qu'elles ont même nombre de points sur toute extension finie (c'est-à-dire même fonction zêta) !

La démonstration que Tate donne a servi de modèle à la démonstration par Faltings (1983) de l'énoncé analogue sur les corps de nombres — une des étapes dans sa preuve de la conjecture de Mordell. En particulier, deux courbes elliptiques sur $\mathbf{Q}$ sont $\mathbf{Q}$-isogènes si et seulement si elles ont même fonction L. À noter que Serre avait démontré un cas particulier de ce dernier énoncé, grâce aux propriétés de la courbe de Tate dont je parle plus bas !

Ce résultat est intimement lié à des analogues géométriques de la conjecture de Birch et Swinnerton-Dyer et à des travaux de Tate concernant la question plus vaste de détecter les classes de cycles dans la cohomologie ℓ-adique, ce qui est une sorte d'analogue arithmétique de la conjecture de Hodge. Mystérieusement, le simple cas des diviseurs n'est pas résolu, alors que le résultat analogue pour la conjecture de Hodge est un théorème classique de Lefschetz.

De là est apparue la conjecture de Sato-Tate que je vais rapidement évoquer. Si E est une courbe elliptique comme ci-dessus, rappelons que l'on a défini pour tout nombre premier p ne divisant pas Δ un entier a_p tel que $|a_p| \leqslant 2\sqrt{p}$. On peut donc l'écrire sous la forme $a_p = 2\sqrt{p}\cos\theta_p$, où $\theta_p \in [0,\pi]$ est « l'angle de Frobenius ». Appliquées aux puissances de la courbe elliptique sur $\mathbf{Q}$ donnée, les conjectures de Tate sur les cycles algébriques l'amèneront à postuler une répartition très précise de ces angles. Par exemple, lorsque la courbe elliptique n'a pas de multiplication complexe, il prédit que pour tout intervalle $[a,b] \subset [0,\pi]$, la densité des nombres premiers p tels que $\theta_p \in [a,b]$ est égale à

$$\frac{2}{\pi}\int_a^b \sin^2 t\,dt.$$

Il est remarquable que le mathématicien japonais M. Sato, second récipiendaire de ce prix Wolf, ait lui aussi prédit cette répartition, en se fondant sur des exemples numériques.

Théories p-adiques

De nombreux articles de J. Tate sont consacrés à la géométrie algébrique sur un corps complet non archimédien. Ce sont des corps où l'on peut faire de l'analyse, mais leur topologie totalement discontinue rend le point de vue classique trop naïf.

Dans un manuscrit écrit en 1959 et publié dans la première partie de l'article « A review of non-archimedean elliptic functions », *Elliptic curves, modular forms, & Fermat's last theorem* (Hong Kong, 1993), Internat. Press, 1995, p. 162–184, Tate introduit ce que l'on appelle aujourd'hui courbe de Tate. Sur le corps des nombres complexes, une courbe elliptique peut s'uniformiser sous la forme $\mathbf{C}/(\mathbf{Z}+\mathbf{Z}\tau)$, où τ est un nombre complexe de partie imaginaire strictement positive. Grâce à l'exponentielle $\mathrm{e}\colon z \mapsto \exp(2\mathrm{i}\pi z)$, on peut aussi l'écrire $\mathbf{C}^*/q^{\mathbf{Z}}$, avec $q = \mathrm{e}(\tau)$. Si q est un élément d'un corps complet non archimédien K tel que $|q| < 1$, Tate construit une courbe elliptique E_q sur K avec un isomorphisme de groupes analytiques $K^*/q^{\mathbf{Z}} \simeq E_q(K)$.

C'est le début d'une géométrie analytique non archimédienne. Début, car la géométrie analytique p-adique naïve n'a pas toutes les propriétés qu'on attend. Il y a par exemple beaucoup plus de fonctions localement analytiques sur le disque de rayon 1 que de fonctions analytiques définies par une série entière qui converge sur ce disque. Dans un article rédigé en 1962 et paru presque 10 ans après (« Rigid analytic spaces », *Invent. Math.* **12**, p. 257–289, 1971), Tate a jeté les bases d'une géométrie analytique, dite *rigide*, exempte de ce défaut et dans laquelle existe un analogue du théorème « gaga » de Serre de comparaison entre géométrie algébrique et géométrie analytique.

Cette géométrie rigide a eu de nombreuses applications, non seulement en arithmétique (uniformisation des courbes elliptiques et des variétés abéliennes, plus récemment en théorie des formes modulaires), mais elle a aussi servi dans des contextes de pure géométrie algébrique. Par exemple, Raynaud l'utilise de manière cruciale dans sa démonstration de la conjecture d'Abhyankar sur les revêtements de la droite affine (en caractéristique positive, elle en a de nombreux !).

Dans le cas d'une variété abélienne A sur un corps p-adique K, Tate a montré en 1966 l'existence d'une espèce d'analogue de la décomposition de Hodge :

$$\mathrm{Hom}_{\mathbf{Z}_p}(T_p(A), \mathbf{C}_p) \simeq \big(H^1(A, \mathcal{O}_A) \otimes_K \mathbf{C}_p\big) \oplus \big(H^0(A, \Omega^1) \otimes_K \mathbf{C}_p(-1)\big) .$$

Dans cette formule, le corps $\mathbf{C}_p$ est le complété de $\bar{K}$; il est muni d'une action de $\mathrm{Gal}(\bar{K}/K)$. Le module de Tate de A, noté $T_p(A)$, est un $\mathbf{Z}_p$-module libre de dimension $2 \dim A$, muni d'une action (continue) du groupe de Galois $\mathrm{Gal}(\bar{K}/K)$, si bien que le membre de gauche est un $\mathbf{C}_p$-espace vectoriel de dimension $2 \dim A$ muni d'une action (semi-linéaire) de $\mathrm{Gal}(\bar{K}/K)$. C'est ainsi l'analogue de la cohomologie singulière $H^1(A, \mathbf{C})$. Au membre de droite figure un objet du même type ; on y reconnaît dans $H^0(A, \Omega^1)$ et $H^1(A, \mathcal{O}_A)$ les blocs $H^{0,1}(A)$ et $H^{1,0}(A)$ de la décomposition de Hodge classique. On les tensorise par le corps $\mathbf{C}_p$; le (-1) dans le second produit tensoriel est ce qu'on appelle une « torsion à la Tate ». La décomposition de Hodge p-adique est l'isomorphisme écrit ci-dessus entre ces deux objets, d'apparence assez barbare au début.

Un des ingrédients pour l'existence de cette décomposition est le calcul de la cohomologie galoisienne de $\mathbf{C}_p$, en particulier le fait que les éléments de $\mathbf{C}_p$ fixés par $\mathrm{Gal}(\bar{K}/K)$ soient réduits à K. (Malgré les apparences, ce n'est pas évident.) Tate a conjecturé l'existence de décompositions analogues pour la cohomologie de toute variété algébrique projective lisse sur un tel corps. Cette conjecture a été démontrée par Faltings (1988).

L'unicité d'une telle décomposition est liée au fait que les invariants de $\mathbf{C}_p(1)$ sous $\mathrm{Gal}(\bar{K}/K)$ se réduisent à 0 : de manière imagée, le corps $\mathbf{C}_p$ ne contient pas d'analogue de $2\mathrm{i}\pi$. Ceci a conduit J.-M. Fontaine à introduire des anneaux $\mathbf{B}_{\mathrm{cris}}$, $\mathbf{B}_{\mathrm{st}}$ et $\mathbf{B}_{\mathrm{dR}}$ contenant un tel élément $2\mathrm{i}\pi$ et à formuler des raffinements de la conjecture de Tate traduisant l'appartenance des périodes de variétés algébriques à ces anneaux. L'ensemble des travaux suscités par cette conjecture de Tate permet aujourd'hui une compréhension profonde des représentations p-adiques d'un corps p-adique et d'un corps de nombres : signalons à ce sujet la conjecture de Fontaine–Mazur décrivant, via l'anneau $\mathbf{B}_{\mathrm{dR}}$, les représentations p-adiques d'un corps de nombres provenant de la géométrie.

Si le lecteur se reporte à la liste des articles de John Tate, il constatera que cette évocation de son œuvre impressionnante en a négligé beaucoup (par exemple, ses travaux sur les algèbres de Sklyanin) et les spécialistes regretteront certainement telle ou telle omission. J'espère cependant avoir bien montré comment les travaux de Tate ont irrigué la géométrie algébrique et l'arithmétique de toute la moitié du XX$^{\mathrm{e}}$ siècle, fournissant tout à la fois conjectures, théorèmes, outils théoriques et parfois algorithmes.