Köln, Oktober 02

Vortrag: Die diesjährigen Fields-Medaillen

Fieldsmedaille ≈ Nobelpreis der Mathematik, seit 30-er Jahren

Abb

wird verliehen auf dem ICM, der alle 4 Jahre stattfindet

Bedingung: < 40 J, etwas Talent, kein Geld.

Liste der bisherigen Preisträger:

Diesjähriger ICM: Peking

Fieldsmedaillen an: L. Laffargue (Fakt) Schüler von Lemonon, jetzt IHES

V. Voevodsky (R/USA) — Suslin, jetzt IAS.

Foto beschriften

Nevanlinnapreis an: Madhu Sudan (MIT)

Idee erklären, worin die Leistung der Preisträger besteht.

Dabei natürlich nicht alles verständlich – aber ich wollte unbedingt sowohl Studenten, als auch informierte Kollegen ansprechen. Als Trost ein Thomas-Mann-Zitat.

Beide Fieldsmedaillen für „Verbindung zwischen Struktur eines Körpers F und Struktur seiner Galoisgruppe Gal($\bar{F}$/F)".

Dabei: Laffargue zur alg. Geom / Analysis

Voevodsky ——— / Topologie.

Prototyp eines solchen Resultats ist

<u>Hauptsatz der Galoistheorie</u>: Sei F ein Körper, $\bar{F}$ sein algebraischer Abschluss. Dann 1:1-Beziehung zwischen

$$\left\{ \begin{array}{l} \text{endl. Untergr. von endl. Index} \\ \text{von } Gal(\bar{F}/F) \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{l} \text{endl. separable} \\ \text{Zwischenkörper } F' \\ \text{von } \bar{F}/F \end{array} \right\}$$

mit allen möglichen guten Eigenschaften.

Laurent Lafforgue

geehrt für seine Beweis der Langlandsvermutung für Fkt.-körper.

Ursprung folg. experimentell gefundenes Resultat von Fermat, Euler.

Südbl. 2 von 21.8.: Seien p, q ungerade Primzahlen.

Dann

$\exists\, x \in \mathbb{Z}$ mit $x^2 \equiv p \bmod q$ gdw. $\exists\, y \in \mathbb{Z}$ mit $y^2 \equiv q \bmod p$.

Fast richtig, nur anders falls $p \equiv q \equiv -1\ (4)$.

- Erster Beweis von Gauß als 19-Jähriger, hat selbst insges. 8 Beweise geliefert (heute ca. 250 Beweise bekannt)
- Danach Suche nach höheren Rez.-ges.: 3., 4., .. Potenzen Gauß, Jacobi, Eisenstein, Kummer, Kronecker – ganzes 19. Jhd.
- Hilbert bringt strukturelle Gesichtspkt hinein, formuliert als ein „H. P.".
- mündet in „Allg. Rezipr.-gesetz von Takagi et Artin"

(KKT) – 1925

Sei F = globaler Körper, d.h. $[F:\mathbb{Q}] < \infty$ Zahlk.-fall, $[F:\mathbb{F}_q(t)] < \infty$ Fkt.-k.-fall.

Sei $\mathbb{A} = \mathbb{A}_F$ = Adelering von F

$= \prod F_x$ alle Vervollst. von F.

Dann ex. 1:1 - Bez. zwischen

$$\left\{ \begin{array}{l} \text{Charaktere von} \\ \mathrm{Gal}(\bar{F}/F), \\ \varrho : \mathrm{Gal}(\bar{F}/F) \to \mathbb{C}^\times \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{l} \text{endl. Faktorgruppen von} \\ \text{Idelekl.-gruppe } \mathbb{A}_F^\times / F^\times \end{array} \right\}$$

mit guter Eigensch.

Beweis sehr schwierig, stromlinienförmig bis Ende der 40-Jahre.

Dann klar, daß neue Idee benötigt, um nichtabelschen Charaktere von $\mathrm{Gal}(\bar{F}/F)$ gerecht zu kom.

- Entscheidende Idee Ende der 60-Jahre von Langlands.

Sei $r \geq 1$. Postuliert Bez. zwischen

$$\left\{ \begin{array}{l} \text{Irredz. Darst. der Dim. } r \\ \text{von } \mathrm{Gal}(\bar{F}/F), \\ \varrho : \mathrm{Gal}(\bar{F}/F) \to GL_r(\mathbb{C}) \end{array} \right\} \text{ und } \left\{ \begin{array}{l} \text{cuspid. Darst. von} \\ GL_r(\mathbb{A}) \end{array} \right\}.$$

<u>Im Zahlkörperfall vor Teilresultate</u> (i.w. $r = 2$), aber bereits diese so tiefliegend, daß sie Wesentl. Input bei Wiles's Bew. von FLT.

Sei jetzt F ein globaler Körper. Dann

<u>cuspidale Darst von</u> $GL_r(\mathbb{A})$ = wiederk. Teildarst der regulären Darst von $G(\mathbb{A})$ auf

$$\{ f \in L^2(G(\mathbb{A})/G(F)); \forall P \subsetneq G \text{ ist } f_P \equiv 0 \}$$

$$f_p(x) = \int_{U_p(\mathbb{A})} f(ux)\,du$$

Spektralzerlegung des Raums L^2 großes Hyperbolicum.

Zum Satz von Lefschetz: Sei jetzt $\bar{F}$ = Fkt.-körper. der Char. p. Sei $(\ell, p) = 1$. Sei $r \geq 1$. Sei

$\mathcal{G}_r = \{$ irreduz. Darst. ϱ. $\mathrm{Gal}(\bar{F}/F) \to GL_r(\bar{\mathbb{Q}}_\ell)\}$

$\mathcal{A}_r = \{$ cusp. Darst. π von $GL_r(\mathbb{A}_F)\}$.

Zu $\varrho \in \mathcal{G}_r$ $\overset{\text{Grothendieck}}{\mapsto}$ $L(\varrho, s)$ L-Fkt.,

- ist rat. Fkt in p^{-s} mit Fktl-gl.

$$L(\varrho, s) = \varepsilon(\varrho, s) \cdot L(\varrho^\vee, 1-s)$$

- ist Eulerprodukt über alle Stellen von F

$$L(\varrho, s) = \prod_x L_x(\varrho, s), \quad \text{wobei}$$

$\forall x$, wo ϱ unverzw. ($\Rightarrow \forall\forall x$) ist

$$L_x(\varrho, s) = \prod_{i=1}^{r} \frac{1}{1 - z_i \cdot p^{-\deg(x)\cdot s}}$$

Hier $z_1, \dots, z_r$ Frobeniuseigenw.

Entspr. für $\pi \in \mathcal{A}_r$ $\overset{\text{Godement, Jacquet}}{\mapsto}$ $L(\pi, s)$

Hier $z_1, \dots, z_r$ Heckeeigenwerte. (Spektralwert von π).

Sätze auflegen.

Kommentar: Kenne von $\mathcal{G}_r$ oder $\mathcal{A}_r$ ist einfacher als andere, aber Satz 3 folgt aus Satz 2 u. H. von Bez. Ungekehrt erlaubt Bez. Konstr. von $\pi_1 \boxtimes \pi_2$ via $\sigma(\pi_1) \otimes \sigma(\pi_2)$ usw.

Zum Beweis: Konstr. der Abb. $\pi \longmapsto \sigma(\pi)$ durch Analyse der ℓ-adischen Kohom. von

$$H^* (Sht_r \otimes_{(F \otimes F)} (\overline{F} \otimes \overline{F}), \overline{\mathbb{Q}}_\ell)$$

Man sucht Komponente der Form

$$\pi \otimes \sigma(\pi) \otimes \sigma(\pi)^\vee .$$

Dabei Sht_r = Modulstack der Shtukas vom Rang r

Grob gesprochen: Sei X = glatte proj. Kurve mit $\mathbb{F}_q(X) = F$. Ein Shtuka von Rang r über $\overline{\mathbb{F}}_q$ = Vektorbündel von Rang r auf $X \otimes_{\mathbb{F}_q} \overline{\mathbb{F}}_q$ + meromorpher Abstieg nach $\mathbb{F}_q$, d.h. fast ein Iso $\tau^* \mathcal{E} \longrightarrow \mathcal{E}$. (das wäre exakt ein VB auf X sein, also keine Moduli besitzen).

Methode wie bei Th. der Shimuravarietäten: Vgl. von L-F-Formel und Selberg'scher Spurformel.

Wesentl. Schwierigk.: Sht_r nicht kompakt, noch nicht einmal Ecke o.e.T.!

(≈ 600 Seiten lang)

Vladimir Voevodsky

Sei F bel. Körper. Die Milnor-K-Theorie von F =

graduierte assoz. $\mathbb{Z}$-Algebra mit 1,

$$\mathbb{Z} \oplus F^\times \oplus (F^\times \otimes F^\times) \oplus \ldots \Big/ \left(\text{Ideal erz. von } \{ a \otimes (1-a),\ a \in F \setminus \{0,1\} \} \right)$$

Also

$$K_1(F) = F^\times$$

$$K_2(F) = F^\times \otimes F^\times / \{ a \otimes (1-a);\ a \neq 0,1 \}$$

usw.

Andererseits sei $H^*(\mathrm{Gal}(\bar{F}/F), \mathbb{Z}/2) = \mathbb{Z}$-Alg.

der Galoiskoh. mit Werten in trivialer Gal.-Modul $\mathbb{Z}/2$,

also

$$H^1(\quad) = \mathrm{Hom}(\mathrm{Gal}(\bar{F}/F), \mathbb{Z}/2)$$
$$= \text{Charakt. der Ord. } 2.$$

$$H^2(\quad) = \text{gekreuzte Homo's.}$$

Kummertheorie definiert

$$F^\times \longrightarrow \mathrm{Hom}(\mathrm{Gal}(F/F), \mathbb{Z}/2)$$

$$a \longmapsto \text{Aktion von } \mathrm{Gal}(\bar{F}/F) \text{ auf } \sqrt{a}.$$

Theorem 1, 2 zeigen.

Erklärungen zu Theorem 2. • Sei $\hat{GW}(F)$ = Ring aller formalen Differenzen $M - N$, wobei M, N nichtausg. symm. Bil.-formen.

Sei $GW(F) = \hat{G}W(F) \,/\, \mathbb{Z} \cdot \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. Wittring.

• Die Abb. in Satz gibt kohom. Invar. von quadr. Formen,

deg 0 : $rg(M) \mod 2$

deg 1 : discr (M)

deg 2 : Wittindex

deg ≥ 3 : höhere Stiefel-Whitney-Invar.

Somit Satz 2 eine partielle Klassifik von quadr. Formen /F.

Zerfallskörper durch Kl-körperth.

Zum Beweis von Theorem 1: Sei $\underline{a} = a_1 \otimes \ldots \otimes a_n \in F^\times \otimes \ldots \otimes F^\times$.

Konstruiere jetzt „universelle Zerfällungsvarietät des entspr. Elements in $H^n(Gal(\bar{F}/F), \mathbb{Z}/2)$" – alle Zerf.-körper sind Spezialisierungen: Voevodsky zeigt, daß die Pfisterquadrik $X_{\underline{a}}$ eine solche ist. Man muß jetzt „K-Theorie" von $X_{\underline{a}}$ verstehen, sehr schwer weil $\dim X_{\underline{a}} = 2^n - 1$ sehr groß. Für kleine n OK (Merkurjev, Suslin, Rost), aber für großes n zu schwierig.

Stattdessen konstruiert Voevodsky eine neue Kohom.-theorie

(motivische Kohomologie), über Homotopietheorie von algebraischen Varietäten. Diese ist schwer zu konstruieren, aber Gerbes zu berechnen – führt zum Ziel.

Weitere Literatur

Schluß: Hoffe, Einblick gegeben zu haben.

Seitenblick → Enthusiasmus im anlaufenden Semester.

Fields Medal and Rolf Nevanlinna Prizes

Fields Medal

At the 1924 International Congress of Mathematicians in Toronto, a resolution was adopted that at each ICM, two gold medals should be awarded to recognize outstanding mathematical achievement. Professor J. C. Fields, a Canadian mathematician who was Secretary of the 1924 Congress, later donated funds establishing the medals which were named in his honor. Consistent with Fields's wish that the awards recognize both existing work and the promise of future achievement, it was agreed to restrict the medals to mathematicians not over forty at the year of the Congress. In 1966 it was agreed that, in light of the great expansion of mathematical research, up to four medals could be awarded at each Congress.

For more details about the origins of the Fields Medal we recommend the article:

Henry S. Tropp, "*The Origins and History of the Fields Medal*", Historia Mathematica 3 (1976) 167-181.

The following text by Eberhard Knobloch describes the design of the medal:

The Fields Medal

Obverse:

The head represents Archimedes facing right.

(1) In the field is the word ΑΡΧΙΜΗΔΟΥΣ in Greek capitals and
(2) the artist's monogram and date RTM, MCNXXXIII.
(3) The inscription reads: TRANSIRE SUUM PECTUS MUNDOQUE POTIRI.

The inscriptions mean:
(1) "of Archimedes", namely the face of Archimedes.
(2) R(obert) T(ait) M(cKenzie), that is the name of the Canadian sculptor who designed the medal. The correct date would read: "MCMXXXIII" or 1933. The second letter M has to be substituted for the false N.
(3) "To transcend one's spirit and to take hold of (to master) the world".

Reverse:

The inscription on the tablet reads:

CONGREGATI
EX TOTO ORBE
MATHEMATICI
OB SCRIPTA INSIGNIA
TRIBUERE

It means: "The mathematicians having congregated from the whole world awarded (this medal) because of outstanding writings". The verb form "tribuere" (the first "e" is a long vowel) is a short form of "tribuerunt".
In the background there is a representation of Archimedes' sphere being inscribed in a cylinder.

Eberhard Knobloch, August 5, 1998

The photos show the Fields Medal presented to Maxim Kontsevich at ICM'98 in Berlin. The name of the Medalist, not visible on the photos, is engraved on the rim of the medal.

Rolf Nevanlinna Prize

The Rolf Nevanlinna Prize in mathematical aspects of information science was established by the Executive Committee of the International Mathematical Union IMU in April 1981. It was decided that the prize should consist of a gold medal and a cash prize similar to the ones associated with the Fields Medal and that one prize should be given at each International Congress of Mathematicians.

One year later, in April 1982, the IMU acepted the offer by the University of Helsinki to

finance the prize. The prize was named the Rolf Nevanlinna Prize in honor of Rolf Nevanlinna (1895-1980), who had been Rector of the University of Helsinki and President of the IMU and who in the 1950s had taken the initiative to the computer organization at Finnish universities.

On its obverse side, the medal represents Nevanlinna and bears the text "Rolf Nevanlinna Prize". In addition, there is in very small characters "RH 83". RH refers to the Finnish sculptor Raimo Heino (1932-95) who designed the medal, and 83 to the year 1983 when the first medal was minted. On the reverse side, the two figures are related to the University of Helsinki. On the University's seal in the lower right, the text "Universitas Helsingiensis" is readable. The seal is from the 17th century, except for the Cross of Liberty which was added to it in 1940. In the upper left part, the word "Helsinki" is in coded form. The name of the prize winner is engraved on the rim of the medal.

Olli Lehto, August 12, 1998

More recently, the Executive Committee of IMU clarified that the Nevanlinna Prize is to be awarded for outstanding contributions in Mathematical Aspects of Information Sciences, including:

1) All mathematical aspects of computer science, e.g. complexity theory, logic of programming languages, machine models, cryptography.

2) Scientific computing, numerical analysis and optimization.

3) Information theory, signal processing, control theory and the modeling of intelligence.

Fields Medals Awarded:

1936

Lars Valerian AHLFORS
Jesse DOUGLAS

1950

Laurent SCHWARTZ
Atle SELBERG

1954

Kunihiko KODAIRA
Jean-Pierre SERRE

1958

Klaus Friedrich ROTH
René THOM

1962

Lars HÖRMANDER
John Willard MILNOR

1966

Michael Francis ATIYAH
Paul Joseph COHEN
Alexander GROTHENDIECK
Stephen SMALE

1970

Alan BAKER
Heisuke HIRONAKA
Serge NOVIKOV
John Griggs THOMPSON

1974

Enrico BOMBIERI
David Bryant MUMFORD

1978

Pierre René DELIGNE
Charles Louis FEFFERMAN
Gregori Alexandrovitch MARGULIS
Daniel G. QUILLEN

1982

Alain CONNES
William P. THURSTON
Shing-Tung YAU

1986

Simon K. DONALDSON
Gerd FALTINGS
Michael H. FREEDMAN

1990

Vladimir DRINFELD
Vaughan F.R. JONES
Shigefumi MORI
Edward WITTEN

1994

Jean BOURGAIN
Pierre-Louis LIONS
Jean-Christophe YOCCOZ
Efim ZELMANOV

1998

Richard E. Borcherds

W. Timothy Gowers
Maxim Kontsevich
Curtis T. McMullen

A silver plate was offered to Andrew J. Wiles as a special tribute from IMU

2002

Vladimir Voevodsky
Laurent Lafforgue

Nevanlinna Prizes Awarded:

1982

Robert TARJAN

1986

Leslie VALIANT

1990

A.A. RAZBOROV

1994

Avi WIGDERSON

1998

Peter W. Shor

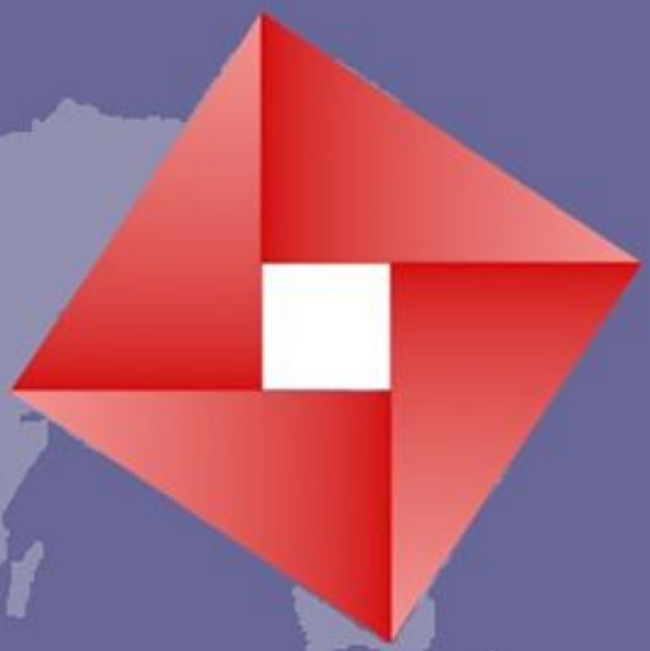
2002

Madhu Sudan

International Congress of Mathematicians

Welcome
What's New
General Information
Organization
Registration
Publication
Satellite Conference
Mail & Circular Letters
Local Information
Tours
Sponsors
FAQ

中文版



ICM 2002

Beijing

August 20-28, 2002

V. Vernadsky

L. Lafforgue

Ich unterbreche mich in meiner Wiedergabe, nur, um aufmerksam zu machen, daß der Vortragende da von Dingen, Angelegenheiten, Kunstverhältnissen sprach, die noch gar nicht in unseren Gesichtskreis fielen und nur am Rande desselben ... schattenhaft für uns auftauchten...; daß wir ... dem allen mit der dunkel erregten Phantasie von Kindern zuhörten, die Märchen lauschten, welche sie nicht verstehen, während ihr zarter Geist sich doch auf eine eigentümlich traumhaft ahnungsvolle Weise dadurch bereichert und gefördert sieht.
"Fuge", "Kontrapunkt", ..., "Verwirrung durch überfärbte Modulationen", "strenger Stil", - das war im Grunde alles noch Märchengeraun für uns, aber wir hörten es so gern und mit so großen Augen, wie Kinder das Unverständliche, eigentlich noch ganz Unzukömmliche hören - und zwar mit viel mehr Vergnügen, als das Nächste, Wohlentsprechende, Angemessene ihnen gewährt. Will man glauben, daß dies die intensivste und stolzeste, vielleicht förderlichste Art des Lernens ist - das antizipierende Lernen, das Lernen über weite Strecken von Unwissenheit hinweg? Als Pädagoge sollte ich ihm wohl nicht das Wort reden, aber ich weiß nun einmal, daß die Jugend es außerordentlich bevorzugt, und ich meine, der übersprungene Raum füllt sich auch mit der Zeit wohl von selber aus.

Theorem 1 (the Langlands conjecture): There is a bijection $\pi \mapsto \sigma(\pi)$ between $\mathcal{A}_r$ and $\mathcal{G}_r$ characterized by the fact that $L_x(\pi, s) = L_x(\sigma(\pi), s)$ for every place x of F.

Theorem 2 (the Ramanujan-Petersson conjecture): Let $\pi \in \mathcal{A}_r$ with central character of finite order. Then for every place x of F where π is unramified, the Hecke eigenvalues $z_1, \ldots, z_r \in \mathbf{C}$ are all of absolute value 1.

Theorem 3 (the Deligne conjecture): Let $\sigma \in \mathcal{G}_r$ with determinant character of finite order. Then σ is pure of weight 0, i.e. for any place x of F where σ is unramified, the images of the Frobenius eigenvalues $z_1, \ldots, z_n$ under any embedding of $\bar{\mathbf{Q}}_\ell$ into $\mathbf{C}$ are of absolute value 1.

Theorem 1: Let char $F \neq 2$. Then have isomorphism of graded $\mathbf{Z}/2$-algebras

$$K_*(F)/2K_*(F) \xrightarrow{\sim} H^*(\mathrm{Gal}(\overline{F}/F), \mathbf{Z}/2) \quad .$$

In particular, the graded $\mathbf{Z}/2$-algebra $H^*(\mathrm{Gal}(\overline{F}/F), \mathbf{Z}/2)$ is generated by its elements of degree 1.

Theorem 2: Let char $F \neq 2$. Then have isomorphism of graded $\mathbf{Z}/2$-algebras

$$\bigoplus_{n \geq 0} I^n/I^{n+1} \xrightarrow{\sim} H^*(\mathrm{Gal}(\overline{F}/F), \mathbf{Z}/2) \quad .$$

Here

$$I = \ker(\acute{G}W(F) \xrightarrow{\mathrm{rg}} \mathbf{Z}/2)$$

ideal in Grothendieck Witt ring of quadratic forms over F.

- ICM 2002 Proceedings (Reports von G. Laumon bzw. C. Soulé)

- Über Lafforgue:
  - Homepage Rapoport
  - Maurice Mashaal: De Langlands à Lafforgue (Internet)

- **Ausführlichere Darstellungen:**

  Über Lafforgue:
  - G. Laumon, Bourbaki-Seminar Nr. 873 (2000)

  Über Voevodsky:
  - B. Kahn, Bourbaki-Seminar Nr. 834 (1997)
  - F. Morel, Bull. AMS 35 (1998)

ICM 2002 · Vol. III · 1–3

The Work of Vladimir Voevodsky

Christophe Soulé*

Vladimir Voevodsky was born in 1966. He studied in Moscow and Harvard universities. He is now Professor at the Institute for Advanced Study in Princeton.

Among his main achievements are the following ones: he defined and developed motivic cohomology and the $\mathbf{A}^1$-homotopy theory of algebraic varieties; he proved the Milnor conjectures on the K-theory of fields.

Let us state the first Milnor conjecture. Let F be a field and n a positive integer. The *Milnor K-group* of F is the abelian group $K_n^M(F)$ defined by the following generators and relations. The generators are sequences $\{a_1, \dots, a_n\}$ of n units $a_i \in F^*$. The relations are

$$\begin{aligned} & \{a_1, \dots, a_{k-1}, xy, a_{k+1}, \dots, a_n\} \\ = \; & \{a_1, \dots, a_{k-1}, x, a_{k+1}, \dots, a_n\} + \{a_1, \dots, a_{k-1}, y, a_{k+1}, \dots, a_n\} \end{aligned}$$

for all $a_i, x, y \in F^*$, $1 \leq k \leq n$, and the *Steinberg relation*

$$\{a_1, \dots, x, \dots, 1-x, \dots, a_n\} = 0$$

for all $a_i \in F^*$ and $x \in F - \{0, 1\}$.

On the other hand, let $\overline{F}$ be an algebraic closure of F and $G = \mathrm{Gal}(\overline{F}/F)$ the absolute Galois group of F, with its profinite topology. The *Galois cohomology* of F with $\mathbf{Z}/2$ coefficients is, by definition,

$$H^n(F, \mathbf{Z}/2) = H^n_{\text{continuous}}(G, \mathbf{Z}/2)\,.$$

Theorem 1. (Voevodsky 1996 [4]) *Assume* $1/2 \in F$ *and* $n \geq 1$. *The Galois symbol*

$$h_n : K_n^M(F)/2K_n^M(F) \to H^n(F, \mathbf{Z}/2)$$

is an isomorphism.

*CNRS and Institut des Hautes Etudes Scientifiques, 35, route de Chartres, 91440 Bures-sur-Yvette, France.

This was conjectured by Milnor in 1970 [1]. When $n = 2$, Theorem 1 was proved by Merkurjev in 1983. The case $n = 3$ was then solved independently by Merkurjev-Suslin and Rost.

There exists also a Galois symbol on $K_n^M(F)/p\,K_n^M(F)$ for any prime p invertible in F. When $n = 2$ and F is a number field, Tate proved that it is an isomorphism. In 1983 Merkurjev and Suslin proved that it is an isomorphism when $n = 2$ and F is any field. Both Voevodsky and Rost have made a lot of progress towards proving that, for any F, any $n > 0$ and any p invertible in F, the Galois symbol is an isomorphism.

The map h_n in Theorem 1 is defined as follows. When $n = 1$, we have $K_1^M(F) = F^*$ and $H^1(F, \mathbf{Z}/2) = \mathrm{Hom}(G, \mathbf{Z}/2)$. The map

$$h_1 : F^*/(F^*)^2 \to \mathrm{Hom}(G, \mathbf{Z}/2)$$

maps $a \in F^*$ to the quadratic character χ_a defined by

$$\chi_a(g) = g(\sqrt{a})/\sqrt{a} = \pm 1$$

for any $g \in G$ and any square root $\sqrt{a}$ of a in $\overline{F}$. That h_1 is bijective is a special case of Kummer theory. When $n \geq 2$, we just need to define h_n on the generators $\{a_1, \ldots, a_n\}$ of $K_n^M(F)$. It is given by a cup-product:

$$h_n(\{a_1, \ldots, a_n\}) = \chi_{a_1} \cup \cdots \cup \chi_{a_n}\,.$$

The fact that h_n is compatible with the Steinberg relation was first noticed by Bass and Tate.

Theorem 1 says that $H^n(F, \mathbf{Z}/2)$ has a very explicit description. In particular, an immediate consequence of Theorem 1 and the definition of h_n is the following

Corollary 1. *The graded* $\mathbf{Z}/2$*-algebra* $\bigoplus_{n \geq 0} H^n(F, \mathbf{Z}/2)$ *is spanned by elements of degree one.*

This means that absolute Galois groups are very special groups. Indeed, it is seldom seen that the cohomology of a group or a topological space is spanned in degree one.

Corollary 2. (Bloch) *Let X be a complex algebraic variety and $\alpha \in H^n(X(\mathbf{C}), \mathbf{Z})$ a class in its singular cohomology. Assume that $2\alpha = 0$. Then, there exists a nonempty Zariski given subset $U \subset X$ such that the corestriction of α to U vanishes.*

If Theorem 1 was extended to $K_n^M(F)/p\,K_n^M(F)$ for all n and p, Corollary 2 would say that any torsion class in the integral singular cohomology of X is supported on some hypersurface. (Hodge seems to have believed that such a torsion class should be Poincaré dual to an analytic cycle, but this is not always true.)

With Orlov and Vishik, Voevodsky proved a second conjecture of Milnor relating the Witt group of quadratic forms over F to its Milnor K-theory [3].

A very serious difficulty that Voevodsky had to overcome to prove Theorem 1 was that, when $n = 2$, Merkurjev made use of the algebraic K-theory of conics over F, but, when $n \geq 2$, one needed to study special quadric hypersurfaces of dimension $2^{n-1} - 1$. And it is quite hard to compute the algebraic K-theory of varieties of such a high dimension. Although Rost had obtained crucial information about the K-theory of these quadrics, this was not enough to conclude the proof when $n > 3$. Instead of algebraic K-theory, Voevodsky used *motivic cohomology*, which turned out to be more computable.

Given an algebraic variety X over F and two integers $p, q \in \mathbf{Z}$, Voevodsky defined an abelian group $H^{p,q}(X, \mathbf{Z})$, called motivic cohomology. These groups are analogs of the singular cohomology of CW-complexes. They satisfy a long list of properties, which had been anticipated by Beilinson and Lichtenbaum. For example, when n is a positive integer and X is smooth, the group

$$H^{2n,n}(X, \mathbf{Z}) = \mathrm{CH}^n(X)$$

is the Chow group of codimension n algebraic cycles on X modulo linear equivalence. And when X is a point we have

$$H^{n,n}(\text{point}) = K_n^M(F)\,.$$

Earlier constructions of motivic cohomology are due to Bloch (at the end of the seventies) and, later, to Suslin. The way Suslin modified Bloch's definition was crucial to Voevodsky's approach and, as a matter of fact, several important papers on this topic were written jointly by Suslin and Voevodsky [6]. There exist also two very different definitions of $H^{p,q}(X, \mathbf{Z})$, due to Levine and Hanamura; according to the experts they lead to the same groups. But it seems fair to say that Voevodsky's approach to motivic cohomology is the most complete and satisfactory one.

A larger context in which Voevodsky developed motivic cohomology is the $\mathbf{A}^1$-homotopy of algebraic manifolds [5], which is a theory of "algebraic varieties up to deformations", developed jointly with Morel [2]. Starting with the category of smooth manifolds (over a fixed field F), they first embed this category into the category of *Nisnevich sheaves*, by sending a given manifold to the sheaf it represents. A Nisnevich sheaf is a sheaf of sets on the category of smooth manifolds for the Nisnevich topology, a topology which is finer (resp. coarser) than the Zariski (resp. étale) topology. Then Morel and Voevodsky define a homotopy theory of Nisnevich sheaves in much the same way the homotopy theory of CW-complexes is defined. The parameter space of deformations is the affine line $\mathbf{A}^1$ instead of the real unit interval $[0, 1]$. Note that, in this theory there are *two circles* (corresponding to the two degrees p and q for motivic cohomology)! The first circle is the sheaf represented by the smooth manifold $\mathbf{A}^1 - \{0\}$ (indeed, $\mathbf{C} - \{0\}$ has the homotopy type of a circle). The second circle is $\mathbf{A}^1/\{0, 1\}$ (note that $\mathbf{R}/\{0, 1\}$ is a loop). The latter is not represented by a smooth manifold. But, if we identify 0 and 1 in the sheaf of sets represented by $\mathbf{A}^1$ we get a presheaf of sets, and $\mathbf{A}^1/\{0, 1\}$ can be defined

as the sheaf attached to this presheaf. This example shows why it was useful to embed the category of algebraic manifolds into a category of sheaves.

It is quite extraordinary that such a homotopy theory of algebraic manifolds exists at all. In the fifties and sixties, interesting invariants of differentiable manifolds were introduced using algebraic topology. But very few mathematicians must have anticipated that these "soft" methods would ever be successful for algebraic manifolds. It seems now that any notion in algebraic topology will find a partner in algebraic geometry. This has long been the case with Quillen's algebraic K-theory, which precisely analogous to topological K-theory. We mentioned that motivic cohomology is an algebraic analog of singular cohomology. Voevodsky also computed the algebraic analog of the Steenrod algebra, i.e. cohomological operations on motivic cohomology (this played a decisive role in the proof of Theorem 1). Morel and Voevodsky developed the (stable) $\mathbf{A}^1$-homotopy theory of algebraic manifolds. Voevodsky defined *algebraic cobordism* as homotopy classes of maps from the suspension of an algebraic manifold to the classifying space MGL. There is also a direct geometric definition of algebraic cobordism, due to Levine and Morel (see Levine's talk in these proceedings), which should compare well with Voevodsky's definition. An the list is growing: Morava K-theories, stable homotopy groups of spheres, etc...

Vladimir Voevodsky is an amazing mathematician. He has demonstrated a unique talent for creating new abstract theories, about which he proved highly nontrivial theorems. He could use these theories to solve several of the main long standing problems in algebraic K-theory. The field is completely different after his work. He opened large new avenues and, to use the same word as Laumon, he is leading us close to the world of *motives* that Grothendieck was dreaming about in the sixties.

References

[1] John Milnor, Algebraic K-theory and quadratic forms, *Inv. Math.*, 9 (1970), 318–344.

[2] Fabien Morel & Vladimir Voevodsky, $\mathbf{A}^1$-homotopy theory of schemes, *Publ. Math. IHES*, 90 (1999), 45-143.

[3] D. Orlov, A. Vishik & Vladimir Voevodsky, An exact sequence for Milnor's K-theory with applications to quadratic forms (2000), to appear.

[4] Vladimir Voevodsky, On 2-torsion in motivic cohomology (2001), to appear.

[5] Vladimir Voevodsky, The $\mathbf{A}^1$-homotopy theory. In *Proceedings of the international congress of mathematians*, Volume 1, pp. 579-604, Berlin, 1998.

[6] Vladimir Voevodsky, Andrei Suslin & Eric Friedlander, Cycles, transfers and motivic homology theories, *Annals of Maths. Studies* 143, Princeton University Press (2000).

Dossier scientifique

De Langlands à Lafforgue

Par Maurice Mashaal

En l'an 2000, le mathématicien Laurent Lafforgue achevait sa démonstration d'une conjecture rattachée à la "correspondance de Langlands". Cette expression désigne un tissu de conjectures, énoncées à la fin des années 1960, qui a inspiré une partie importante des recherches modernes en géométrie algébrique et en théorie des nombres. Pour ses résultats, fruits d'environ sept ans de travail, Laurent Lafforgue s'est vu décerner le 20 août 2002 la récompense la plus prestigieuse pour un mathématicien de moins de quarante ans : une médaille Fields.

En 1967, le mathématicien canadien Robert P. Langlands n'avait que 31 ans et était en poste à l'université de Yale, aux Etats-Unis. En janvier de cette année-là, il écrivit une lettre manuscrite de 17 pages à un mathématicien de l'Institute for Advanced Study de Princeton, André Weil (1906-1998). Ce Français émigré aux Etats-Unis, frère de la philosophe Simone Weil et cofondateur du groupe Nicolas Bourbaki, était l'un des grands noms de la théorie des nombres et de la géométrie algébrique. La lettre avait pour but de développer et formuler plus précisément une question que Langlands avait posée oralement à Weil quelque temps auparavant. En fait, Langlands y présentait un certain nombre d'hypothèses et d'idées profondes, qui esquissaient des liens étroits et surprenants entre des classes d'objets mathématiques de natures différentes. En caricaturant, il s'agissait de correspondances entre "représentations galoisiennes", objets qui relèvent de l'algèbre, et "formes automorphes", classe de fonctions qui relèvent de l'analyse.

Weil ne fit pas de réponse écrite à Langlands, mais il reconnut l'intérêt des idées exposées par le jeune mathématicien canadien. Il fit dactylographier le texte de la lettre, qui se diffusa largement. Le contenu mathématique de cette lettre forme, avec certains ajouts ultérieurs de la part de Langlands lui-même ou d'autres mathématiciens, ce que l'on a appelé la "correspondance de Langlands" (ou le "programme de Langlands", ou encore tout simplement les "conjectures de Langlands"). Les idées et conjectures en question ont, depuis, stimulé de nombreuses recherches dans les domaines de la théorie des nombres et de la géométrie algébrique.

Comme souvent en mathématiques, l'importance du programme de Langlands est due au fait qu'il relie des parties très différentes de cette science. En effet, lorsque des objets *a priori* distincts se révèlent être des facettes différentes d'un même objet plus général, il en résulte une compréhension plus profonde et une plus grande richesse conceptuelle ; il en naît de nouvelles stratégies pour résoudre les problèmes posés au mathématicien, et de nouvelles questions émergent à leur tour. Ainsi avancent les idées.

Même si le prix à payer est une technicité et une abstraction plus grandes, de telles unifications permettent de temps à autre de résoudre des problèmes plus terre à terre mais qui résistent depuis longtemps aux efforts des chercheurs. La correspondance de Langlands en fournit un exemple célèbre avec le théorème de Fermat[1]. La démonstration de ce théorème, en 1994, passait en effet par la démonstration d'une partie d'une autre conjecture

beaucoup plus technique, appelée conjecture de Shimura-Taniyama-Weil[2]. Or celle-ci, qui a été prouvée dans son intégralité en 1999, peut être considérée comme l'un des éléments du programme de Langlands. D'un autre côté, des théories mathématiques abstraites d'ordre fondamental peuvent aussi avoir des répercussions d'ordre technologique, voire économique : on sait que, depuis plusieurs décennies, les recherches en théorie des nombres et en géométrie algébrique jouent un rôle important dans les domaines de la cryptographie et du codage numérique de l'information.

Une histoire ancienne, mais qui prend son véritable essor au XIX^{e} siècle

Pour comprendre en quoi consistent la correspondance de Langlands et les travaux qu'elle a suscités — et ceux de L. Lafforgue en font partie — il faudrait des connaissances préalables qui dépassent de beaucoup celles que peut posséder un non-mathématicien. Essayons cependant de donner un parfum de l'histoire de ces développements et de leurs motivations.

Comme c'est souvent le cas en mathématiques, les débuts appartiennent à un passé lointain. Dès l'Antiquité, les mathématiciens se sont intéressés à la résolution de problèmes qui, dans la terminologie d'aujourd'hui, sont appelées *équations diophantiennes*. Il s'agit tout simplement d'équations polynomiales, à coefficients entiers, dont on cherche les solutions parmi les nombres entiers. Par exemple, $x^2 + 3y^3 = 7$ est une équation diophantienne, et l'une de ses solutions entières est donnée par $x = 2$, $y = 1$. Un autre exemple d'équation diophantienne est celle intervenant dans le théorème de Fermat. Malgré leur apparence anodine, l'étude de telles équations est, en général, bien difficile.

Les attaques directes se sont révélées assez peu fructueuses. Depuis le début du XIX^{e} siècle et sous l'impulsion du grand Carl Friedrich Gauss (1777-1855), les mathématiciens se sont mis à explorer des voies détournées. En particulier, il s'est avéré intéressant et utile de considérer non pas des égalités au sens ordinaire, mais des égalités définies à un multiple entier d'un nombre premier[3] près. Par exemple, étant donné un nombre premier p, existe-t-il un entier x tel que $x^2 + 1$ soit divisible par p, c'est-à-dire un entier x tel que $x^2 + 1$ soit égal à 0 à un multiple de p près ? Dans ce domaine, un résultat profond — et fort utile pour les équations diophantiennes du second degré — est la *loi de réciprocité quadratique*, que Gauss a été le premier à prouver correctement (étant donnés deux nombres premiers p et q, cette loi arithmétique relie par une formule simple deux propriétés : l'existence (ou la non-existence) d'un entier x tel que $x^2 – p$ est divisible par q, et l'existence d'un entier y tel que $y^2 – q$ est divisible par p).

Une bonne partie des développements ultérieurs de l'arithmétique et de l'algèbre sont issus de la recherche de lois de réciprocité analogues allant au-delà du cas quadratique, c'est-à-dire s'appliquant à des puissances d'entiers supérieures à 2. La route était semée d'obstacles. C'est notamment pour les surmonter que Gauss, puis d'autres, sont sortis du cadre trop strict des nombres ordinaires et ont essayé d'étendre les lois de l'arithmétique[4] des nombres entiers à des ensembles de nombres plus généraux ; par exemple les "entiers de Gauss" qui sont les nombres de la forme $a + ib$, où a et b sont des entiers ordinaires et $i = \sqrt{(–1)}$, ou encore l'ensemble noté $\mathbf{Q}[\sqrt{5}]$ des nombres de la forme $x + y\sqrt{5}$ où x et y sont des nombres rationnels (quotients d'entiers).

Quand l'algèbre abstraite se marie avec la théorie des nombres

L'étude des propriétés arithmétiques et algébriques de tels ensembles de nombres et la recherche de lois de réciprocité autres que la loi quadratique ont progressivement fait

émerger la théorie algébrique des nombres. Parmi ses principaux artisans, dans la deuxième moitié du XIX^{e} siècle, on compte les Allemands Ernst Kummer, Richard Dedekind, Leopold Kronecker. La montée en généralité de la théorie des nombres s'est accompagnée d'une montée en abstraction. Ce faisant, plusieurs concepts importants se sont forgés. Deux de ces ingrédients essentiels de l'algèbre et de la théorie des nombres sont la notion de *corps* et la *théorie de Galois*, dont il faut dire quelques bribes avant de parler de la correspondance de Langlands.

Un *corps* est tout simplement un ensemble d'éléments qui peuvent s'additionner, se soustraire, se multiplier et se diviser (sauf par zéro) comme les nombres réels ordinaires, avec des règles semblables. L'ensemble **Q** des nombres rationnels, l'ensemble **R** des nombres réels, l'ensemble **C** des nombres complexes, l'ensemble **Q**[$\sqrt{5}$] mentionné plus haut sont des exemples de corps[5]. L'ensemble **Q**[$\sqrt{5}$] constitue d'ailleurs un exemple d'"extension" du corps **Q** des nombres rationnels, car c'est un corps qui contient **Q** et qui est construit à partir de ce dernier. Pour déterminer les propriétés arithmétiques et algébriques des corps et de leurs extensions, les mathématiciens disposent d'une arme à la fois puissante et abstraite : la théorie de Galois. Celle-ci tire son nom et ses idées de base des travaux d'Evariste Galois (1811-1832), mathématicien de génie, mort très jeune dans un duel aux circonstances obscures.

Galois lui-même s'était focalisé sur les équations polynomiales ; il avait démontré qu'il n'est pas possible de trouver pour les équations à une inconnue, de degré supérieur ou égal à 5, une solution générale exprimable à l'aide de radicaux (c'est-à-dire un équivalent de la fameuse formule $x = [-b \pm \sqrt{(b^2 - 4ac)}]/(2a)$ qui donne la solution de l'équation générale du second degré $ax^2 + bx + c = 0$). En fait, la théorie de Galois ne se limite pas aux équations polynomiales ; convenablement généralisée, elle s'applique à l'étude de nombreuses autres structures algébriques, notamment à des extensions de corps quelconques. Quelle en est l'idée essentielle ? En termes modernes et de façon vague, elle est, étant donnée une extension K* d'un corps K, d'associer à cette extension un certain *groupe*[6] de transformations, dénommé son *groupe de Galois*[7]. L'analyse du groupe de Galois de l'extension K* de K permet ensuite d'accéder aux propriétés algébriques et arithmétiques de cette extension, alors qu'une étude directe de celle-ci serait trop ardue.

La correspondance de Langlands, une généralisation de la "théorie des corps de classes"

Quel rapport tout cela a-t-il avec la correspondance de Langlands ? Celle-ci est une généralisation de ce qu'on appelle la "théorie des corps de classes", édifiée depuis la fin du XIX^{e} siècle et jusque vers 1950 par des mathématiciens comme Heinrich Weber, David Hilbert, Teiji Takagi, Emil Artin, Helmut Hasse et d'autres. Cette théorie, réputée complexe et difficile, est l'un des grands exploits de la théorie algébrique des nombres du XX^{e} siècle. On peut la caractériser à l'aide des notions évoquées plus haut. En simplifiant, la théorie des corps de classes cherche, partant d'un corps K, à décrire certaines extensions K* de K dont le groupe de Galois est commutatif ("commutatif" signifie que dans l'opération interne du groupe, le résultat ne dépend pas de l'ordre dans lequel sont pris les éléments du groupe : $a\ b = b\ a$ quels que soient les éléments a et b du groupe de Galois). En d'autres termes, cette théorie consiste, par l'intermédiaire du groupe de Galois, à dégager les propriétés de certains "surcorps" K* à partir des propriétés arithmétiques du corps de base K. C'est dans ce cadre qu'Emil Artin a obtenu en 1927 une loi de réciprocité générale, formulée de manière abstraite mais qui englobe toutes les lois de réciprocité trouvées précédemment (dont la plus simple est la loi de réciprocité quadratique mentionnée au début de ce texte).

Il était naturel de vouloir étendre la théorie des corps de classes aux cas où le groupe de Galois n'est pas commutatif. Des pistes pour ce faire n'ont été trouvées que dans les années 1960, en particulier par Langlands. Le principe était non pas d'étudier le groupe de Galois lui-même, mais de passer par ses *représentations*[8] (des « images » du groupe constituées de transformations linéaires agissant sur un espace de dimension fixée, finie ou infinie). Langlands a conjecturé l'existence d'une correspondance bijective entre certaines représentations de dimension finie *n* du groupe de Galois attaché à l'extension d'un corps K et certaines représentations dites automorphes associées au "groupe linéaire" GL(*n*, K), un groupe familier à tous les étudiants qui débutent en mathématiques[9]. Un peu plus précisément, les conjectures de Langlands établissent ces correspondances *via* des fonctions particulières (d'une part, on sait rattacher les représentations galoisiennes à certaines fonctions dénommées "fonctions L"[10] ; d'autre part, les représentations automorphes définissent des fonctions dénommées « formes automorphes », auxquelles on sait attacher des fonctions L ; prouver la correspondance de Langlands implique donc de démontrer que les fonctions L liées aux représentations galoisiennes de l'extension de K sont les mêmes que les fonctions L rattachées à GL(n, K)).

Peu à peu, le programme de Langlands s'accomplit

Quelle est la contribution de Laurent Lafforgue à ce programme ? La correspondance de Langlands comporte en fait de nombreux cas et sous-cas distincts, selon la valeur de l'entier positif *n* et selon la nature du corps K. Le cas *n* = 1 correspond à un groupe de Galois commutatif et équivaut à la théorie des corps de classes ; il est donc réglé depuis plus d'une cinquantaine d'années. Pour les autres valeurs de *n*, correspondant à des groupes non commutatifs, plusieurs cas particuliers des conjectures de Langlands ont été démontrés au fil des ans. Des résultats plus généraux ont été obtenus dans la dernière décennie. En particulier, en 1993, Gérard Laumon (université Paris XI), Michael Rapoport (université de Cologne) et Ulrich Stuhler (université de Göttingen) prouvaient la correspondance de Langlands pour tout entier positif *n*, mais pour des corps K particuliers — les "corps de séries formelles définies sur un corps fini". En 1998, Michael Harris (université Paris VII) et Richard Taylor (université de Harvard) démontraient la correspondance (pour tout *n*) pour les "corps *p*-adiques" ; quelques mois plus tard, Guy Henniart (université Paris XI) fournissait du même énoncé une preuve un peu moins informative, mais plus directe.

Deux ans plus tard, Laurent Lafforgue prouvait la correspondance de Langlands (pour tout *n*) pour les "corps de fonctions rationnelles sur une courbe définie sur un corps fini"[11]. Sa démonstration occupe 240 pages de la revue professionnelle *Inventiones mathematica*, à quoi il faut ajouter les nombreux et volumineux travaux déjà publiés sur lesquels elle s'appuie. Pour aboutir à son résultat, L. Lafforgue a étendu la méthode du mathématicien ukrainien Vladimir Drinfeld (médaille Fields en 1990) qui, dans les années 1970, était parvenu à démontrer cette même partie du programme de Langlands, mais uniquement pour la valeur particulière *n* = 2.

Les travaux de Lafforgue apportent ainsi l'une des pièces maîtresses du vaste édifice imaginé par Langlands il y a plus de trente ans. Cet édifice — d'une complexité, d'une technicité et d'une abstraction assez effroyables — dresse de larges ponts entre la théorie des nombres (l'arithmétique des corps), l'algèbre (la théorie de Galois, la théorie des représentations des groupes) et l'analyse (les fonctions automorphes), pour ne citer que ces domaines. Il n'est pas achevé : paradoxalement, les conjectures de Langlands restent à prouver pour les corps de base les plus familiers, comme **Q** (les nombres rationnels), **R** (les nombres réels) ou **C** (les nombres complexes). Ce sont les cas de figure qui auront, *a priori*, le plus d'impact sur les problèmes d'apparence élémentaire, comme les équations diophantiennes. Mais jusqu'ici, les

progrès dans cette direction ont été rares, hormis ce qui a été fait en liaison avec le théorème de Fermat. De nouvelles idées sont donc attendues. Par ailleurs, Drinfeld a imaginé une version un peu plus géométrique de la correspondance de Langlands, impliquant des courbes définies sur le corps des nombres complexes et non sur un corps fini. Ce programme tentaculaire n'a donc pas fini de faire parler de lui.

Communiqué de presse
Dossier de presse

Références

Sur le programme de Langlands et les thèmes qui s'y rattachent, il n'existe quasiment pas de documents accessibles à des non-spécialistes. Même quand ils existent, ils exigent généralement un minimum de connaissances mathématiques de niveau universitaire. Les propositions suivantes sont rangées dans l'ordre croissant de difficulté.

• C. Goldstein, "Le théorème de Fermat", *La Recherche*, mars 1994, pp. 268-275 ; "Autour du théorème de Fermat", *Mnémosyne, 7*, 1994, pp. 34-61.

• R. P. Langlands, "Representation theory — its rise and its role in number theory", *Proceedings of the Gibbs Symposium*, American Mathematical Society, 1990 (article à télécharger).

• S. Gelbart, "An elementary introduction to the Langlands program", *Bulletin of the American Mathematical Society, 10*, 2, 1984, pp. 177-219.

• G. Laumon, "Chtoucas de Drinfeld et correspondance de Langlands", *Gazette des mathématiciens n°88*, avril 2001, pp. 11-33.

• L. Lafforgue, "Chtoucas de Drinfeld et correspondance de Langlands", *Inventiones mathematicae, 147*, 2002, pp. 1-241.

Notes

1- Le théorème de Fermat affirme que pour tout entier *n* supérieur ou égal à 3, il n'existe pas d'entiers positifs *x*, *y*, *z* vérifiant l'équation $x^n + y^n = z^n$. Il a été démontré par le chercheur britannique Andrew Wiles en 1994, près de trois siècles et demi après avoir été énoncé.

2- La démonstration de la conjecture complète de Shimura-Taniyama-Weil, en 1999, est due au Français Christophe Breuil et aux Américains Brian Conrad, Fred Diamond et Richard Taylor.

3- Un nombre premier est un entier positif qui n'est divisible que par 1 et par lui-même, comme 5, 13 ou 17.

4- Un exemple de loi arithmétique fondamentale est la décomposition unique d'un nombre en facteurs premiers : tout entier positif se décompose de façon unique (à l'ordre près) en un produit de nombres premiers (ainsi, par exemple, $3234 = 2 \times 3 \times 7 \times 7 \times 11$).

5- En revanche, l'ensemble **Z** des entiers n'est pas un corps (car l'inverse d'un entier autre que 1 ou –1 n'est pas un entier). Il existe aussi des corps dont les éléments ne sont pas des nombres : par exemple le corps des fonctions rationnelles définies sur un corps K, c'est-à-dire l'ensemble des expressions de la forme P/Q où P et Q sont des polynômes à coefficients appartenant à K. Enfin, si tous les exemples ci-dessus sont des corps ayant une infinité d'éléments, on définit également des corps finis, qui n'ont qu'un nombre fini d'éléments (l'exemple sans doute le plus simple, qui joue d'ailleurs un rôle central en informatique, est le corps constitué par les deux nombres 0 et 1, avec la multiplication habituelle et l'addition "modulo 2", c'est-à-dire que l'on pose 1 + 1 = 0).

6- Le terme de *groupe* désigne une structure algébrique que l'on rencontre fréquemment et partout en mathématiques. Un groupe est un ensemble G d'éléments muni d'une opération interne, notée par exemple *, avec les trois propriétés suivantes valables pour tous éléments a, b, c de G :
- associativité : $(a * b) * c = a * (b * c)$;
- existence d'un élément neutre e tel que $a * e = e * a = a$ pour tout a ;
- existence d'un élément inverse a' pour tout a, vérifiant $a' * a = a * a' = e$.
L'ensemble **Z** des entiers relatifs, muni de l'addition, est un exemple de groupe. Les rotations géométriques autour d'un point du plan ou de l'espace constituent un autre exemple de groupe (l'opération interne étant ici la composition des applications).

7- Le *groupe de Galois* d'une extension L d'un corps K (c'est-à-dire que L est un corps qui contient le corps K) est constitué des *automorphismes* sur L qui laissent inchangés les éléments de K. Par définition, un automorphisme f sur un corps L est une application bijective $f : L \longrightarrow L$ telle que $f(a + b) = f(a) + f(b)$ et $f(ab) = f(a)f(b)$, quels que soient les éléments a et b de L. L'ensemble des automorphismes de L, muni de la loi de composition des applications, forme un groupe ; les automorphismes de L qui laissent inchangés les éléments de K en forment un sous-groupe.

8- Etant donné un groupe G, une représentation (linéaire) de G de dimension finie n consiste à associer à tout élément x de G une matrice $R(x)$ à $n \times n$ composantes, c'est-à-dire un tableau de nombres comprenant n lignes et n colonnes, de manière à vérifier la propriété : $R(x * y) = R(x)R(y)$ quels que soient les éléments x et y du groupe G. (Les matrices $n \times n$ représentent des transformations linéaires opérant sur un espace vectoriel de dimension n ; elles s'additionnent et se multiplient selon des règles assez simples). La théorie de la représentation des groupes joue un rôle essentiel notamment en physique, en relation avec les symétries.

9- Le "groupe linéaire" GL(n, K) est le groupe constitué par les matrices à n lignes et n colonnes dont les n^2 composantes sont des éléments du corps K et qui sont inversibles (pour la loi de mutiplication des matrices, qui n'est en général pas commutative). Par exemple, pour $n = 2$ et K = **R**, il s'agit des matrices inversibles à 2×2 composantes, ces composantes étant des nombres réels. Pour $n = 1$ et K = **R**, le groupe linéaire équivaut à l'ensemble des nombres réels, muni de la multiplication ordinaire (qui est commutative).

10- Les fonctions L constituent une classe particulière de fonctions d'une variable complexe s. Elles permettent d'étudier des propriétés arithmétiques par des méthodes qui relèvent de

l'analyse. L'archétype des fonctions L est la fonction ζ (dzêta) de Riemann, définie pour s > 1 par $\zeta(s) = 1 + 1/2^s + 1/3^s + 1/4^s + ...$ Un calcul assez simple montre qu'elle est égale au produit de tous les termes de la forme $1/(1 – 1/p^s)$ où p est un nombre premier, ce qui fait apparaître son lien avec l'arithmétique.

11- Un peu plus explicitement, un tel corps est constitué des fonctions de la forme $P(x, y)/Q(x, y)$, où *P* et *Q* sont des polynômes en *x* et en *y*, et où *x* et *y* sont les coordonnées des points appartenant à une "courbe définie sur un corps fini". Etant donné un corps fini F (c'est-à-dire un corps comportant un nombre fini d'éléments), une telle courbe est représentée par une équation algébrique reliant *x* et *y*, dans laquelle les coefficients et les inconnues *x* et *y* doivent être des éléments de F.