Laurent Lafforgue
Institut des hautes études scientifiques (IHES),
Le Bois-Marie, 35 route de Chartres,
Bures-sur-Yvette, Frankrijk
laurent@ihes.fr

Mathieu Florence
Avenue de la Poste 24
1020 Renens, Zwitserland
mathieu.florence@gmail.com

Overzichtsartikel

Galois Theory and Arithmetic

At the age of twenty, in the night before the duel that would end his life, Evariste Galois (1811–1832) wrote an account of his thoughts of the previous years. These concerned a theory of algebraic equations that now bears his name: Galois theory. Now more than ever, it is central to arithmetic, where it brings together algebra, geometry, topology, and harmonic analysis. In this article, Laurent Lafforgue, professor at the Institut des Hautes Etudes Scientifiques (IHES) and Field Medalist in the year 2002, connects the classical theory with the contemporary state of the research area. His text is supplemented with frames by Mathieu Florence, post-doc at the Ecole Polytechnique Fédérale de Lausanne (EPFL). The French version appeared in the collection 'Images des Mathématiques 2004' published by the Centre National de la Recherche Scientifique. Translation: Reinie Erné.

An algebraic equation in an unknown X can be written as $a_d X^d + a_{d-1}X^{d-1} + \cdots + a_1 X + a_0 = 0$. When the degree d is 1, this equation has the solution $-a_0/a_1$ whenever the coefficients a_0, a_1 are elements of a set F in which the four operations $+, -, \times$, and $/$ are defined; such an F is called a field. When $d = 2$, the solutions are

$$\left(-a_1 \pm \sqrt{a_1^2 - 4a_0a_2}\right)/2a_2\,.$$

Likewise, for $d = 3$ or 4, the solutions can be expressed in terms of the four operations and the taking of the roots $\sqrt{a}$, $\sqrt[3]{a}$, $\sqrt[4]{a}$ of the equations $X^2 = a$, $X^3 = a$, and $X^4 = a$. Abel showed that this is impossible from $d = 5$ on. Galois theory answers the most general question of determining all relations between algebraic equations with coefficients in a field F. To each we associate the finite set of its solutions endowed with the action of a group G_F, the Galois group of F. The relations between equations then correspond to maps between the associated finite sets that respect the action of G_F.

Between 1958 and 1970, the French mathematician Alexander Grothendieck brought a new vision and two important generalizations to Galois theory, in the setting of his recasting of algebraic geometry into *theory of schemes*. He first defines the coverings of a scheme S: these are the schemes S' fibered over S that locally, in the sense of his 'étale topology', can be written as stacks of copies of S, like the floors in an apartment building. Then he shows that the category of coverings of S is equivalent to that of the finite sets endowed with the action of a group π_S, the 'fundamental group of S'. To each field F corresponds a scheme of dimension 0, its 'spectrum', $S = \operatorname{Spec}(F)$, and the algebraic equations in one variable with coefficients in F correspond to the coverings of S. The fundamental group π_S is none other than the group G_F. Thus we have a common generalization of Galois theory and of the theory of the topological fundamental group of Henri Poincaré (1854–1912).

In the same way as there are schemes of all dimensions, there are fibrations of all relative dimensions above a scheme S, and not only the relative dimension 0 of the coverings. When $S = \operatorname{Spec}(F)$, these are 'varieties' defined by algebraic equations in more than one variable. In this vertical direction, Grothendieck also gave a partial generalization of Galois theory, the 'ℓ-adic cohomology' of fibrations. The cohomology, or rather the homo-

Polynomial Equations and Galois Theory

Classically, the general degree three equation with, say, real coefficients is resolved in two steps. First you reduce the equation to the form

$$P(X) = X^3 - pX + q = 0 \quad p, q \text{ real}$$

by eliminating the X^2 term. Then you look for a root x of P of the form

$$x = u + v \quad \text{where } 3uv = p\,.$$

By expanding $P(u+v)$, we obtain the system

$$\begin{cases} u^3 + v^3 = -q \\ \quad u^3 v^3 = p^3/27, \end{cases}$$

which we know how to solve: u^3 and v^3 are the roots of the polynomial $X^2 + qX + p^3/27$. Finally, we arrive at Cardano's Formula:

$$x = \sqrt[3]{\frac{-q}{2} + \sqrt{\frac{q^2}{4} - \frac{p^3}{27}}} + \sqrt[3]{\frac{-q}{2} - \sqrt{\frac{q^2}{4} - \frac{p^3}{27}}}\,,$$

which gives all three roots of P. The choice of the first cube root of unity fixes the choice of the second because of the relation $3uv = p$. The degree four equation can be reduced by a similar method to that of degree three.

Galois theory allows us to show the absence of a formula similar to the one above for the equations of degree five or more, that is, of the form $P(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0 = 0$, where $n \geq 5$ and the a_i are in a field K. For simplicity, we will assume here that the characteristic of K is zero. The equation $P(X) = 0$ is then said to be *solvable by radicals* if there is a formula using the elements of K and the operations $+, -, \times, /$, and $\sqrt[k]{}$ that gives the roots of P. Let us give two essential definitions. A *splitting field* for P is a field L containing K, in which P has all its roots:

$$P(X) = \prod_{i=1}^{n}(X - \alpha_i)$$

with $\alpha_i \in L$, and such that $L = K(\alpha_1, \ldots, \alpha_n)$. Such a field L is unique up to isomorphism. For example, the splitting field of $X^3 - 2$ for $K = \mathbf{Q}$ is $\mathbf{Q}(\sqrt[3]{2}, e^{2\pi i/3})$. The Galois group of this extension L/K, denoted $\mathrm{Gal}_{L/K}$, is the group $\mathrm{Aut}_K L$ of automorphisms of L that leave the elements of K invariant. In the example above, this group is the symmetric group with three elements. An essential result due to Galois states that the equation $P = 0$ is solvable by radicals if and only if $\mathrm{Gal}_{L/K}$ is solvable. (A group G is called *solvable* if there exist subgroups $G = H_0 \supset H_1 \supset \ldots \supset H_n = \{e\}$ such that H_{i+1} is a normal subgroup of H_i and H_i/H_{i+1} is Abelian.)

In particular, if we consider the coefficients a_i of P as variables, we can apply this result to the field $K = \mathbf{C}(a_0, \ldots, a_{n-1})$. The group $\mathrm{Gal}_{L/K}$ can then be identified with the group of permutations of the roots α_i. Now, this group is not solvable for $n \geq 5$, whence the impossibility of solving the general equation of degree $n \geq 5$ by radicals, as was shown by the Norwegian mathematician Niels Hendrik Abel (1802–1829).

logy, of a topological space had been invented by Poincaré, and as soon as the 1940's, André Weil was interested in adapting it to algebraic geometry. After pioneering work by Jean-Pierre Serre, Grothendieck realized this adaptation, associating to every fibration of a scheme S the ℓ-adic cohomology spaces that are continuous linear representations of the fundamental group π_S; we call these Galois representations of S. We would have a complete generalization of Galois theory if we could have moved back up from these to algebraic varieties; this is the object of Grothendieck's theory of 'motives', which, even today, remains conjectural. Outside of relative dimension 0, we know only the case of the varieties called 'Abelian' conjectured by John Tate and proved by Gerd Faltings in 1983: when two Abelian varieties have the same ℓ-adic cohomology, each parametrizes the other. But if it is true that the category of fibrations, or rather of 'motives', over a base scheme S is equivalent to that of the Galois representations of S, determining these representations and their mutual relations is crucial.

Arithmetic is the study of algebraic varieties, and therefore of Galois representations, over the field $\mathbf{Q}$ of rational numbers. Grothendieck associates the point $\mathrm{Spec}\,\mathbf{Q}$ to this field, but also a scheme of dimension 1, $\mathrm{Spec}\,\mathbf{Z}$, whose points are the prime numbers and whose regular functions are the elements of $\mathbf{Q}$. This makes $\mathbf{Q}$ similar to the fields of algebraic functions on curves. Just as we can associate to a function f on a curve the order $v_p(f)$ of the zero or pole at every point p, likewise for every prime number p a rational number f has a unique integer $v_p(f)$ such that $f/p^{v_p(f)}$ has no factor p. The field $\mathbf{Q}$ and the function fields $F(C)$ of algebraic curves C over a field whose number of elements is finite are called global fields. To every Galois representation of such a field we can associate an analytic function L that is an infinite product of factors indexed by the points of $\mathrm{Spec}\,\mathbf{Z}$ or C. These are generalizations of the Riemann ζ-function $\zeta(s) = \prod_p (1 - p^{-s})^{-1}$ and we expect that, as is the case for the Riemann ζ-function, they admit analytic continuations and functional equations linking their values in s and $1 - s$. Grothendieck proved this for the function fields as a consequence of a result coming from topology, the 'Poincaré duality'. But we still have no duality on $\mathrm{Spec}\,\mathbf{Z}\ldots$

According to the predictions of the Canadian mathematician Robert Langlands, it is through the L functions that Galois theory meets harmonic analysis. This is a branch of mathematics created in the 19th century by Joseph Fourier to analyze waves, that studies periodic functions, for example $\cos()$ and $\sin()$ on $\mathbf{R}$ with period group $2\pi\mathbf{Z}$. To a global field $F = \mathbf{Q}$ or $F(C)$ we associate its 'ring of adèles' $\mathbf{A}_F$ that is an infinite product of fields $\mathbf{F}_p$, 'localizations of F', in all points p of $\mathrm{Spec}\,(F)$ or C. The functions on the group $GL_r(\mathbf{A}_F)$ of invertible $r \times r$ matrices with coefficients in $\mathbf{A}_F$ with period group $GL_r(F)$ are called *automorphic*. In a different form, these were first studied by Poincaré. To every automorphic representation of $GL_r(\mathbf{A}_F)$, Langlands associated an analytic

Algebraic Varieties and Schemes

The simplest object studied in algebraic geometry is the affine space A_K^n, where K is an algebraically closed field. As set, A_K^n is equal to K^n. It is endowed with a topology called the *Zariski topology*, whose closed subsets are the sets $V(I)$ of zeros in K^n of an ideal I of $K[X_1, \ldots, X_n]$.

However, this topology is too coarse to distinguish sufficiently many algebraic varieties. We must therefore add some structure. For every open subset $U \subset A_K^n$, we define the *regular functions* on U as the maps from U to K that can be written as P/Q for polynomials P and Q, where Q has no zeros on U. These functions have a remarkable property. Indeed, giving a regular function f on U is equivalent to giving a covering $\{U_i\}$ of U by open subsets, and regular functions f_i on U_i such that $f_i = f_j$ on $U_i \cap U_j$.

We call the map $U \mapsto \{\text{regular functions on } U\}$ a *sheaf* on A_K^n (note the analogy with the sheaf of C^∞ functions on a C^∞ variety).

More generally, to every commutative ring A, Grothendieck's theory of schemes associates a topological space whose points are the prime ideals of A, and whose closed subsets are the sets $V(I)$ of prime ideals containing an ideal $I \subset A$. This space is endowed with a sheaf of rings constructed in such a way that, loosely speaking, A corresponds to the regular functions on this space. The resulting object is called the *spectrum* of A, and is denoted Spec (A). This is an affine scheme. General schemes are obtained by gluing such affine schemes together.

Let us consider Spec $(\mathbf{Z})$ and Spec $(K[X])$ more closely. We can draw them as follows:

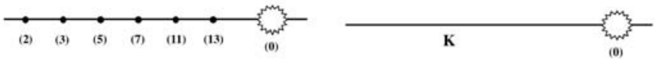


Figure 1 Spec $(\mathbf{Z})$ and Spec $(K[X])$

In both cases, the topological space in question resembles a straight line with the cofinite topology, plus a dense point η corresponding to the zero ideal. If K is countable, these two spaces are homeomorphic. Nevertheless, the schemes are not isomorphic: their sheaves of regular functions are completely different.

Consider the scheme $S = \text{Spec}\,(K[X_1, \ldots, X_n]/(P))$, where P is an irreducible polynomial. The closed points of S correspond to the maximal ideals of $K[X_1, \ldots, X_n]$ containing P, which according to Hilbert's Nullstellensatz are in bijection with the solutions of the equation $P = 0$ in K^n. It follows that S is an *algebraic hypersurface*.

This example together with that of Spec $(\mathbf{Z}[i])$, studied in the frame *Etale Coverings and Fundamental Group*, shows how the theory of schemes is a common generalization of arithmetic and algebraic geometry.

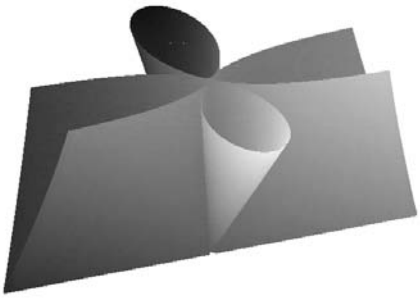


Figure 2 Algebraic hypersurface

function L, also defined by an infinite product of factors indexed by p, that admits an analytic continuation and a functional equation. He conjectured the following fantastic statement: for every $r \geq 1$, there exists a unique correspondence preserving the L functions, $\sigma \mapsto \pi_\sigma$, $\pi \mapsto \sigma_\pi$ between the set of Galois representations σ of dimension r of F and the set of automorphic representations π of $GL_r(\mathbf{A}_F)$.

The case $r = 1$ is a reformulation, already known to Emil Artin (1898–1962), of the theory of class fields, which kept all arithmeticians busy in the 19th century, up tot the 1930's. The case $r \geq 2$ is more subtle, as the groups $GL_r(\mathbf{A}_F)$ are no longer commutative.

For $F = F(C)$, and thanks to the functional equations of Grothendieck, we have been able to show that if there are maps $\pi \mapsto \sigma_\pi$ in ranks $< r$, there are maps in the other direction $\sigma \mapsto \pi_\sigma$ for ranks $\leq r$. For $F = \mathbf{Q}$ and $r \neq 1$, the most important construction $\sigma \mapsto \pi_\sigma$ to date is due to Andrew Wiles: it is when σ comes from an elliptic curve, an Abelian variety of dimension 1. By the theorem of Faltings mentioned before, this means that every elliptic curve over $\mathbf{Q}$ can be parametrized by what we call a modular curve. This result, as everyone knows, implies Fermat's theorem.

In the other direction, $\pi \mapsto \sigma_\pi$, we are looking for the σ_π in the ℓ-adic cohomology of suitable varieties over F. For $F = F(C)$, the Ukrainian mathematician Vladimir Drinfeld proposed a conjectural answer to the question at the beginning of the 1970's, the 'chtoucas' varieties; he later proved the case $r = 2$. Recently, the author of this article generalized the proof of Drinfeld to arbitrary dimension, so that at this moment, the Langlands correspondence on functions fields has been proved. On $F = \mathbf{Q}$, a partial answer is given conjecturally by the varieties that generalize modular curves, introduced by the Japanese mathematician Shimura even before Langlands stated his program. However, the cohomology of these varieties can only contain part of the Galois representations, and in general, we do not know yet how to determine it explicitly.

The theories of Galois and Grothendieck and the Langlands program that completes them are a great and beautiful product of the human mind. No one doubts that the yet to be resolved problems that they pose — the motives, the cohomology of Shimura varieties, and other more general varieties that must still be

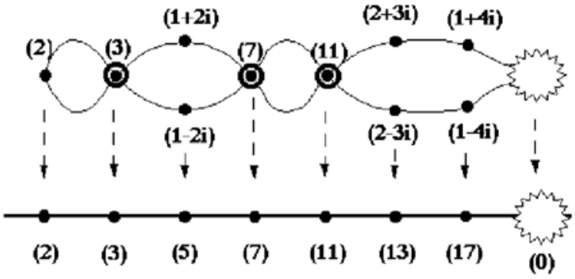
Etale Coverings and Fundamental Group

We will now explain how the notion of covering, well-known for 'nice' topological spaces, generalizes to schemes. For simplification, all schemes we consider here are supposed connected. We must translate the notion of local isomorphism to algebraic geometry; if we do this naïvely, we obtain nothing. A surjective morphism of schemes that is a local isomorphism is in fact an isomorphism, because the Zariski open subsets are dense for a large class of schemes. We must therefore refine this topology to obtain a new one, called *étale topology*. This is not a topology in the usual sense: for every scheme we have a family of morphisms of schemes $\{f_i : U_i \to X\}$ satisfying certain properties that axiomatize the notion of 'covering of X by open $U_i \hookrightarrow X$'. The maps $\{f_i : U_i \to X\}$ considered here are étale morphisms. A good definition of these morphisms is that of the Jacobian criterion: $\{f : U \to X\}$ is called étale if locally, f represents U by polynomial equations $P_1(X_1, \ldots, X_n) = \ldots = P_n(X_1, \ldots, X_n) = 0$ with $\det(\delta P_i / \delta P_j)$ invertible. You might think of U as a horizontal strip stretched over X without folds.

However, this does not reflect the richness of this notion. For example, if $X = \operatorname{Spec}(K)$, U will be of the type $\operatorname{Spec}(L)$, where L is a field that is a finite separable extension of K.

A covering between schemes is, up to details, a surjective étale morphism $U \to X$. For example, $\mathbf{C}^* \to \mathbf{C}^*$, $x \mapsto x^n$ is an étale covering of the scheme $\mathbf{C}^* = \operatorname{Spec}(\mathbf{C}[X, 1/X])$. As in topology, we have the notion of Galois covering. Moreover, if $X = \operatorname{Spec}(K)$, the Galois coverings correspond to Galois field extensions.

Even though in general there is no universal covering of a given scheme S, there does exist a *fundamental group* π_S whose finite quotients are the automorphism groups of the Galois coverings. A non-trivial result is that $\pi_{\operatorname{Spec}(\mathbf{Z})} = \{e\}$, that is, that every number field K is ramified at at least one prime number p. For example, the canonical map $\operatorname{Spec}(\mathbf{Z}[i]) \to \operatorname{Spec}(\mathbf{Z})$ is ramified at the point $(1+i)$: if we remove this point, the resulting morphism is étale. This morphism can be drawn as follows:



Class Field Theory

A major problem of modern mathematics is the description of the Galois group of $\overline{\mathbf{Q}}/\mathbf{Q}$. This question is extremely delicate. Nevertheless, class field theory gives a partial answer. It has two facets.

The first is local: we consider *local fields*, for example the p-adic numbers or the formal series over a finite field. The principal result is the following: the correspondence

$$\begin{gathered}\{\text{finite Abelian extensions of K}\} \to \\ \{\text{subgroups of K}^* \text{ with finite index}\}, \\ L \mapsto \mathrm{N}_{L/K}(L^*)\end{gathered}$$

is bijective, where $\mathrm{N}_{L/K}$ denotes the norm of the extension L/K. Moreover, for every Galois extension L/K we have an isomorphism

$$(\alpha, L/K) : K^*/\mathrm{N}_{L/K}(L^*) \xrightarrow{\sim} \mathrm{Gal}^{\mathrm{ab}}_{L/K}$$

with a good number of functorial properties. This gives us a description of $\mathrm{Gal}^{\mathrm{ab}}_{L/K}$, the largest Abelian quotient of $\mathrm{Gal}_{L/K}$. These results can be obtained in various ways, in particular thanks to the Nakayama-Tate duality between certain Galois cohomology groups.

The other facet of class field theory deals with *global fields*. To fix some ideas, K now denotes a number field. The role that K^* plays in the local case is now held by the group $\mathrm{C}_K = \mathrm{I}_K/K^*$, the *idèle class group* of K. We denote by I_K the group of idèles, which for $K = \mathbf{Q}$ is defined as $\mathrm{I}_{\mathbf{Q}} = \mathbf{R}^* \times \prod'_{p \in P} \mathbf{Q}_p^*$, where P denotes the set of prime numbers, $\mathbf{Q}_p$ is the field of p-adic numbers, and $\prod'$ is the restricted product, that is, the set of elements of the usual product that are almost everywhere units. In general, the factors of the product defining I_K are the completions of K for all absolute values of K. These fields are $\mathbf{R}$ or $\mathbf{C}$ for the Archimedian absolute values, and finite extensions of p-adic fields for the others. We then have two theorems analogous to the ones above, obtained by replacing K^* respectively L^* by C_K respectively C_L. The ingredients of the proof are still of cohomologic nature, but also analytic: the Chebotarev density theorem, a vast generalization of the theorem of Dirichlet on arithmetic progressions, comes in at a crucial point in the proof. In fact, class field theory even gives a description of the abelianization of $\mathrm{Gal}(\overline{K}/K)$ for every global field K. This comes down to describing all continuous representations of dimension 1 of $\mathrm{Gal}(\overline{K}/K)$; this is where this theory coincides with the Langlands program for $r = 1$.

defined, the properties of L functions of Galois representations — will for a long time remain on the horizon of algebraic and arithmetic geometry.

Automorphic Representations

We will now describe in detail the notion of *automorphic representation* of the group $\mathrm{GL}_r(\mathbf{A})$. To simplify this discussion, we consider a function field F over an algebraic curve C defined over a finite field, for example $F = \mathbf{F}_p(t)$. The ring of adèles of F is $\mathbf{A} = \prod'_{x \in C} F_x$, where F_x denotes the local field obtained by completing F at the point $x \in C$, and $\prod'$ is the set of elements of the usual product that are almost everywhere integers, that is, elements of the ring of integers $O_x \subset F_x$.

The ring $\mathbf{A}$ is endowed with a topology whose basis of open neighborhoods of 0 is given by the sets $\prod_{x \in S} H_x \times \prod_{x \notin S} O_x$, where $S \subset C$ is finite and $H_x \subset F_x$ is open for $x \in S$. We have a natural injection $F \hookrightarrow \mathbf{A}$. We call a function $f : \mathrm{GL}_r(\mathbf{A}) \to \mathbf{C}$ with the following properties an *automorphic form on* $\mathrm{GL}_r(\mathbf{A})$:

- f is left-invariant for $\mathrm{GL}_r(F)$: $f(\gamma x) = f(x)$ for $\gamma \in \mathrm{GL}_r(F)$, $x \in \mathrm{GL}_r(\mathbf{A})$,
- f is right-invariant for an open subgroup $H \subset \mathrm{GL}_r(\mathbf{A})$: $f(x) = f(xh)$ for $h \in H$, $x \in \mathrm{GL}_r(\mathbf{A})$.

Strictly speaking, we should add a third condition that we leave out here.

The group $\mathrm{GL}_r(\mathbf{A})$ acts on the space A of automorphic forms by $(g.f)(x) = f(xg)$ for $f \in A$ and $x, g \in \mathrm{GL}_r(\mathbf{A})$.

An *automorphic representation* is an irreducible representation of $\mathrm{GL}_r(\mathbf{A})$ that occurs in the space A. Let us recall that a representation $\rho : G \to \mathrm{GL}(V)$ is called *irreducible* if the only subspaces of V that are stable under ρ are $\{0\}$ and V. An automorphic representation can always be written as an infinite tensor product of local factors that are irreducible representations of the groups $\mathrm{GL}_r(F_x)$. This is the local aspect of this theory. The global aspect is contained in the left-invariance of the automorphic forms for the subgroup $\mathrm{GL}_r(F)$.

Some Definitions

- A group is a set endowed with a law of composition $(g_1, g_2) \mapsto g_1 g_2$, a unit element, and an inverse map $g \mapsto g^{-1}$. It is commutative or Abelian if we always have $g_1 g_2 = g_2 g_1$. An action of a group on a finite set consists of associating to every element of the group a permutation of the elements of the set, in a way that is compatible with the laws of composition.
- A category is a collection of objects and relations between the objects.
- A linear representation of a group is a vector space endowed with linear transformations indexed by the elements of the group, in a way that is compatible with the laws of composition.
- A ring is a set in which the three operations $+$, $-$, and $\times$ are defined, but not necessarily the division $/$.