Géométrie arithmétique / Arithmetic geometry

ENS de Lyon · Master 2 · 2027–2028

Programme

1 Premier semestre / First semester **1**
- 1.1 Introduction à la théorie des schémas / Introduction to schemes (Benjamin Schraen) 1
- 1.2 Corps p-adiques / p-adic fields (Laurent Berger) 1
- 1.3 Courbes elliptiques / Elliptic curves (Olivier Taïbi) 1

2 Second semestre / Second semester **2**
- 2.1 Courbes elliptiques en théorie algorithmique des nombres / Elliptic curves in computational number theory (Benjamin Wesolowski) 2
- 2.2 Introduction aux schémas en groupes (Philippe Gille) 2
- 2.3 Théorie de Hodge p-adique / p-adic Hodge theory (Gabriel Dospinescu) 3

1 Premier semestre / First semester

1.1 Introduction à la théorie des schémas / Introduction to schemes

Benjamin Schraen

FR Le but de ce cours est de donner une introduction à la théorie des schémas. Dans une première partie nous introduirons le vocabulaire des schémas : schémas affines, projectifs, ainsi qu'une introduction au point de vue fonctoriel. La suite du cours sera consacrée à l'étude des diviseurs, du groupe de Picard et aux notions de platitude et lissité en géométrie algébrique.

EN The goal of this course is to give an introduction to the theory of schemes. We will first introduce the basic vocabulary of schemes (affine schemes, projective schemes), and give an introduction to the functorial point of view. The rest of the course will focus on divisors and the Picard group, as well as on the concepts of flatness and smoothness in algebraic geometry.

Références / References.
- Mumford, *The Red Book of Varieties and Schemes*;
- Eisenbud–Harris, *The Geometry of Schemes*;
- Hartshorne, *Algebraic Geometry*.

1.2 Corps p-adiques / p-adic fields

Laurent Berger

EN This course is an introduction to arithmetic and analysis in p-adic fields. The following topics will be covered: local fields, Galois theory, ramification theory, p-adic analysis, formal groups, local class field theory and an introduction to p-adic periods. Additional topics may be treated depending on the needs of the other courses.

1.3 Courbes elliptiques / Elliptic curves

Olivier Taïbi

FR Ce cours est une introduction aux courbes elliptiques, plus particulièrement aux aspects arith-

métiques. Les courbes elliptiques (courbes « de genre 1 ») sont les premières que l'on rencontre au-delà des coniques (« de genre 0 »), pourtant leur arithmétique recèle encore de nombreux mystères. Après les définitions et propriétés générales (courbes elliptiques analytiques et algébriques, loi de groupe, morphismes) nous étudierons de plus près les courbes elliptiques sur les corps finis (théorème de Hasse sur le nombre de points, théorème d'isogénie de Tate), les corps locaux (critère de bonne réduction de Néron–Ogg–Shafarevich) et les corps de nombres (théorèmes de finitude de Mordell et de Siegel).

EN This course is an introduction to elliptic curves, more specifically their arithmetic properties. Elliptic curves ("genus 1" curves) are the first curves one encounters beyond conics ("genus 0"), yet their arithmetic still holds many mysteries. After general definitions and properties (analytic and algebraic elliptic curves, group law, morphisms) we will study more closely elliptic curves on finite fields (Hasse's theorem on the number of points, Tate's isogeny theorem), local fields (Néron–Ogg–Shafarevich criterion for good reduction) and number fields (finiteness theorems of Mordell and Siegel).

Références / References.

- Joseph H. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics 106.

2 Second semestre / Second semester

2.1 Courbes elliptiques en théorie algorithmique des nombres / Elliptic curves in computational number theory

Benjamin Wesolowski

EN This course will explore computational aspects of elliptic curves, and their many applications. Computing with elliptic curves has long been of interest for an experimental approach to number theory and testing conjectures. Beyond such theoretical endeavors, the field has developed around important applications in information and communication sciences: elliptic curves play a central part in ensuring the security of our everyday communications.

This course will cover:

1. Fundamental aspects of the field: how to compute the group law, count points over finite fields, compute isogenies;
2. Applications to seemingly unrelated computational questions in number theory: how to factor integers, or prove that an integer is prime;
3. Applications in cryptography: how to design or break cryptosystems with elliptic curves and isogenies;
4. Along the way, various aspects of the theory of elliptic curves will be developed or revisited, including endomorphism rings, isogeny graphs and random walks, complex multiplication.

2.2 Introduction aux schémas en groupes

Philippe Gille

FR Les schémas en groupes sont les objets en groupes dans la catégorie des schémas, ce sont donc des « familles de groupes algébriques ». Un exemple sur l'anneau $\mathbb{Z}$ est donné par le cercle $x^2 + y^2 = 1$, qui modulo 2, devient $(x + y + 1)^2 = 0$, c'est-à-dire une droite de multiplicité 2. Cet exemple indique que l'on ne peut pas se limiter aux objets lisses et que le cadre « plat » est

plus naturel. Le schéma en groupes orthogonaux de la forme quadratique entière $x_1^2 + \cdots + x_n^2$ est un exemple de $\mathbb{Z}$-schéma en groupes non commutatif pour $n \geq 2$, lié à la théorie des formes quadratiques entières.

Le cours porte sur les schémas en groupes affines, leurs représentations linéaires et leurs algèbres de Lie, avec une attention particulière aux schémas en groupes diagonalisables et à leurs actions. Cela conduit à la cohomologie de Hochschild des schémas en groupes plats. Nous présentons aussi l'exemple récent [3] d'un schéma en groupes affine non linéaire sur les nombres duaux trouvé en 2026 par l'IA.

EN Group schemes are the group objects in the category of schemes; they are therefore "families of algebraic groups". An example over the ring $\mathbb{Z}$ is given by the circle $x^2+y^2=1$, which modulo 2 becomes $(x+y+1)^2=0$, that is, a line of multiplicity 2. This example indicates that one cannot restrict to smooth objects and that the flat setting is more natural. The orthogonal group scheme of the integral quadratic form $x_1^2 + \cdots + x_n^2$ is an example of a non-commutative $\mathbb{Z}$-group scheme for $n \geq 2$, connected to the theory of integral quadratic forms.

The course deals with affine group schemes, their linear representations and their Lie algebras, with particular attention to diagonalizable group schemes and their actions. This leads to the Hochschild cohomology of flat group schemes. We also present the recent example [3] of a non-linear affine group scheme over the dual numbers found in 2026 by AI.

Références / References.

[1] Demazure–Gabriel, *Groupes algébriques*, Masson, 1970.
[2] J.S. Milne, *Basic Theory of Affine Group Schemes*, lien.
[3] Exemple de 2026.

2.3 Théorie de Hodge p-adique / p-adic Hodge theory

Gabriel Dospinescu

FR Ce cours propose une introduction à la théorie de Hodge p-adique à travers la géométrie des espaces perfectoïdes, développée par Peter Scholze. Il s'agit de comprendre comment la cohomologie étale p-adique d'une variété est reliée à ses formes différentielles et à sa cohomologie de de Rham. Nous introduirons les bases de la géométrie analytique p-adique, puis les espaces perfectoïdes et le basculement, qui établit un lien entre les caractéristiques zéro et p. Le site pro-étale permettra ensuite d'aborder les théorèmes de comparaison : les espaces perfectoïdes y jouent le rôle de modèles locaux sur lesquels les calculs cohomologiques se simplifient. L'objectif principal sera la construction de la suite spectrale de Hodge–Tate pour les variétés propres et lisses. Les calculs sur les tores et leurs revêtements fourniront des exemples explicites. Selon le temps disponible, nous aborderons la comparaison de de Rham ou les applications de périodes de Hodge–Tate.

EN This course offers an introduction to p-adic Hodge theory through the geometry of perfectoid spaces, developed by Peter Scholze. Its aim is to explain how the p-adic étale cohomology of a variety relates to its differential forms and de Rham cohomology. We will introduce the foundations of p-adic analytic geometry, followed by perfectoid spaces and tilting, which provides a bridge between characteristic zero and characteristic p. The pro-étale site will then provide the framework for studying comparison theorems: perfectoid spaces serve as local models on which cohomological calculations become simpler. The main goal will be the construction of the Hodge–Tate spectral sequence for smooth proper varieties. Calculations on tori and their coverings will provide explicit examples. Depending on the time available, we will also discuss the de Rham comparison theorem or Hodge–Tate period maps.