Seminari de Teoria de Nombres (UB-UAB-UPC)
STNB2026, 39a ed.

Abstracts of the STNB2026

Facultat de Matemàtiques i Informàtica, Universitat de Barcelona
January 26 - 30, 2026

Organising Committee:
F. Bars, L.V. Dieulefait, B. Plans, A. Travesa

Introduction

The *Seminari de Teoria de Nombres (UB-UAB-UPC)* would like to extend a warm welcome to all the participants to the 39th edition of our annual Seminar. The *Seminari* is mainly formed by researchers in Number Theory from the metropolitan area of Barcelona, mostly of the Universitat de Barcelona (UB), the Universitat Autònoma de Barcelona (UAB) or the Universitat Politècnica de Catalunya (UPC), and also attracts people from other places and foreign countries.

This edition of the Seminari de Teoria de Nombres de Barcelona, STNB2026, contains **two main courses** and also several sessions for **conferences** or **research talks** to present works by some participants to this event. The two main courses are dedicated to **Hopf-Galois Theory and applications to Number Theory**, and to **Four lectures on p-adic Hodge-Tate Theory and applications**.

The afternoon of Thursday, January 29th, is devoted to a **special session** in occasion of the 60-th birthday of Xavier Xarles. We would like to specially thank the speakers of this session. **Per molts anys, Xavier!**

Breaks between sessions or talks are scheduled as "Pausa"; it is possible to have a coffee there.

We thank Daniel Gil Muñoz, Cornelius Greither, and Josu Pérez Zarraonandia for coordinating the main courses; also, all the speakers of these courses, and also, finally, all the speakers of the communications; without them, this Seminari would not be possible.

This booklet contains the abstracts of the scheduled talks, as provided by their respective authors. We hope that you find this information helpful and that you enjoy the Seminari as much as possible.

Barcelona, January 2026

F. Bars, L.V.Dieulefait, B. Plans, A. Travesa

Contents

Abstracts for: Hopf-Galois theory and applications to number theory

(main course)

Coordinators: Daniel Gil Muñoz, Cornelius Greither

In this course we offer a detailed introduction to Hopf-Galois theory, which is a generalization of Galois theory involving the use of Hopf algebras. We shall start with the study of Hopf algebras and their duals, as well as their actions on rings, introducing the equivalent notions of Hopf-Galois extensions, which are generalizations of Galois extensions, and Hopf-Galois objects, which can be regarded as their dual counterpart. The former notion involves Hopf-Galois structures on a field extension, defined as pairs of a Hopf algebra and a linear action on the extension. Among the very basics of Hopf-Galois theory, there is the Greither-Pareigis theorem, which establishes a bijective correspondence between the Hopf-Galois structures on a separable extension and a subclass of permutation subgroups of n letters, where n is the degree of the extension. The study of the Hopf-Galois structures using these techniques is the so-called Greither-Pareigis theory, of which we shall also see some applications. Finally, we shall study the use of Hopf-Galois extensions in number theory, and more concretely in studying the module structure of the ring of integers in extensions of number fields and p-adic fields.

References:

S. U. Chase and M. E. Sweedler. *Hopf Algebras and Galois Theory.* 1st ed. Lecture Notes in Mathematics. Springer, 1969.

L. N. Childs. *Taming Wild Extensions: Hopf Algebras and Local Galois Module Theory.* 1st ed. Mathematical Surveys and Monographs 80. American Mathematical Society, 2000. ISBN: 0-8218-2131-8.

L. N. Childs, C. Greither, K. P. Keating, A. Koch, T. Kohl, P. J. Truman, and R. G. Underwood. *Hopf Algebras and Galois Module Theory.* 1st ed. Mathematical Surveys and Monographs 260. American Mathematical Society, 2021.

C. Greither and B. Pareigis. Hopf Galois theory for separable field extensions. *Journal of Algebra* **106** n.1 (1987), pp. 239–258. ISSN: 0021-8693. DOI: https://doi.org/10.1016/0021-8693(87)90029-9

S. Montgomery. *Hopf algebras and their actions on rings.* Conference Board of the Mathematical Science. American Mathematical Society, 1993.

P. J. Truman. *Hopf-Galois Module Structure of Some Tamely Ramified Extensions.* PhD thesis. University of Exeter, 2009.

R. G. Underwood. *Fundamentals of Hopf Algebras.* 1st ed. Universitext. Springer, 2015. ISBN: 978-3-319-18990-1. DOI: 10.1007/978-3-319-18991-8.

Hopf algebras and their actions on modules

Daniel Gil Muñoz
Universitat de Barcelona
Wednesday, January 28th, 10:00-11:30

We start by an introduction to the theory of Hopf algebras over rings that will be eventually needed in Hopf-Galois theory. A Hopf algebra is a module that is a bialgebra (it admits compatible structures of algebra and coalgebra) and is equipped with a coinverse map or antipode. The prototypical example of Hopf algebra is the one of a group algebra, consisting in the linear combinations of elements of a group with scalars in a ring. We shall see the notion of duality in the theory of modules and we will study the dual of a Hopf algebra. In addition, we shall study the notion of module and comodule algebras over Hopf algebras, which is the setting where Hopf-Galois extensions will be defined.

Hopf-Galois extensions and Hopf-Galois objects

Cornelius Greither
Bundeswehr University Munich
Thursday, January 29th, 10:00-11:30

This is the first of two lectures in which will try to give an overview of some basic topics in Hopf Galois theory. Building on the introductory

lecture by Daniel Gil Muñoz, we start by introducing Hopf Galois situations, where a K-Hopf algebra H provides "symmetries" on a (finite-dimensional commutative) K-algebra A. This is explained in two versions, which will turn out to be essentially equivalent. First we describe H-Galois extensions, where H acts on A (this is closer to the classical Galois situation), and second we present H-Galois objects, where A is an H-comodule algebra; this setup is closer in spirit to the action of algebraic groups on varieties. We will recall a very explicit description of algebras and Hopf Galois objects in the language of finite Γ_K-sets and Γ_K-groups. In other words we try to understand zerodimensional varieties and group varieties over K (which is usually a number field, hence far from algebraically closed), and the actions of the latter on the former. A generalized Galois correspondence will be discussed briefly.

Hopf-Galois structures on separable extensions

Cornelius Greither
Bundeswehr University Munich
`Friday, January 30th, 9:45-11:15`

This second lecture builds on the concepts introduced in the first; its essential topics are the so-called Greither-Pareigis correspondence, and the Byott translation. The former assumes that the K algebra $A = L$ is a field, and describes all Hopf Galois situations involving L in terms of G (the Galois group of the normal closure of L), G' (the subgroup fixing L), and the group of permutations of the G-set G/G'. This is nice in principle and totally explicit, but it involves groups which are often unwieldy because of their size. Byott's translation reformulates this correspondence in a different and potentially more manageable way, which also involves groups and actions, a key notion being the holomorph of a finite group. We will try to give typical and meaningful examples all along. In particular we will see that for example, field extensions obtained by adjoining cube roots are typically not classically Galois, but can be endowed with a nice Hopf Galois structure. This example belongs to the larger class of so-called "almost classically Galois extensions"; those will be treated

more generally if time permits. This lecture will be followed by a final lecture, given by Daniel Gil Muñoz.

Hopf-Galois extensions in number theory

Daniel Gil Muñoz
Universitat de Barcelona
`Friday, January 30th, 11:30-13:00`

It was at the end of the eighties when Childs suggested that Hopf-Galois theory could be applied in order to generalize Galois module theory, which consists in the study of the module structure of the ring of algebraic integers over the Galois group algebra in a Galois extension of number or p-adic fields. This idea led to the development of Hopf-Galois module theory, which considers instead Hopf-Galois extensions of number or p-adic fields, and the ground ring for the module structure of the algebraic integers is an object depending on a Hopf-Galois structure on the extension. This problem contains the one corresponding to classical Galois module theory and has been useful to broaden the information provided by the latter. In this lecture, we shall present the main research directions in this topic. In particular, the positive results obtained so far will illustrate how the behavior of the module structure of the ring of integers depends on arithmetic invariants on the extension.

Abstracts for: Four lectures on p-adic Hodge-Tate theory and applications

(main course)

Coordinator: Josu Pérez Zarraonandia

The classical theory of Hodge provides isomorphisms which compare the de Rham cohomology and the singular cohomology of smooth real manifolds. The p-adic version of this theory provides similar isomorphisms, which compare the étale and de Rham cohomology of smooth proper schemes over p-adic fields. This is achieved by constructing suitable comparison rings and linearization functors, which in turn have applications to the classification of p-adic representations. The contents of our series of four lectures are as follows. In the first lecture we will give an overview of the theory. In the second lecture we will discuss the case of Hodge-Tate representations, the fundamental example of Fontaine's formalism, which will guide us when we discuss more general representations in the third lecture, such as the de Rham and crystalline. In the last session, we will apply this theory to classify p-adic representations arising from elliptic curves.

References:

Olivier Brinon and Brian Conrad: CMI summer school notes on p-adic Hodge theory,
`https://math.stanford.edu/~conrad/papers/notes.pdf`

Abhinandan: p-adic Galois representations and elliptic curves,
`https://www.math.u-bordeaux.fr/~ybilu/algant/documents/theses/Abhinandan.pdf`

The four lectures are the following.

Overview and Motivation

Josu Pérez Zarraonandia
Universitat de Barcelona

`Tuesday, January 27th, 10:00-11:30`

Hodge-Tate Representations

Matilde Vieira Lino da Costa
Universitat de Barcelona
Tuesday, January 27th, 11:45-13:15

Three Period Rings for the Elven-kings

Filip Gawron
Universitat de Barcelona
Wednesday, January 28th, 11:45-13:15

Classification of p-adic Representations of Elliptic Curves

José Castro Moreno
ICMat, Madrid
Thursday, January 29th, 11:45-13:15

Abstracts for the Special session for the 60th birthday of Xavier Xarles

Coordinator: Francesc Bars

Paraules

Francesc Bars
Universitat Autònoma de Barcelona
Thursday, January 29th, 16:00-16:30

Squares in arithmetic progression over number fields

Enrique González-Jiménez
Universidad Autónoma de Madrid
Thursday, January 29th, 15:00-15:50

Abstracts for contributed conferences or communications

(in alphabetical order of speakers)
Coordinator: Bernat Plans

Modular Entanglement

Samuele Anni
Université Aix-en-Marseille
`Monday, January 26th, 17:55-18:45`

We study entanglement phenomena between residual Galois representations attached to modular forms and modular abelian varieties, focusing on whether two such representations—possibly in different residual characteristics—can correspond to the same number field or share a common non-trivial subfield. These questions are closely related to inverse Galois theory and to congruences between modular forms. We present explicit examples arising from elliptic curves: for levels N_1, N_2 in $\{3, 4, 5\}$, we describe one-dimensional families of pairs of elliptic curves whose N_1- and N_2-torsion Galois representations exhibit projective A_4-entanglement. We also give explicit models for the associated modular surfaces over suitable cyclotomic extensions of $\mathbb{Q}$. This is joint work with David Kohel (AMU) and Zoé Yvon (Toulouse), and ongoing work with Luis Dieulefait (UB) and Gabor Wiese (Université du Luxembourg).

Exploring extensions of Dirichlet and Green-Tao theorems on arithmetic progressions over polynomial and formal power series rings

Alberto Fernández-Boix
Universitat Politècnica de Catalunya
Monday, January 26th, 10:00-10:50

Dirichlet's Theorem on primes in arithmetic progressions asserts that, if a and b are relatively prime positive integers, then there are infinitely many primes in the arithmetic progression $a(-)+b$, $-$ running over the positive integers. On the other hand, the so–called Green–Tao Theorem asserts that, given any $k \in \mathbb{N}$, there are coprime integers a and b such that all the numbers $a+b$, $a+2b$, $\ldots$, $a+kb$ are primes. The goal of this talk is to explore the validity of Dirichlet's and Green–Tao' statements over polynomial and formal power series rings. More precisely, we will see that Dirichlet's Theorem also holds replacing the ring of integers by the polynomial ring $\mathbb{Z}[x_1, \ldots, x_n]$; in contrast, we will exhibit a counterexample for the validity of this statement over the formal power series ring $\mathbb{Z}[[x]]$. On the other hand, we provide a Green–Tao type result that works over the polynomial ring $A[x_1, \ldots, x_n]$, where A can be either $\mathbb{Z}$ or a field of characteristic zero. The content of this talk is based on [GRB26], where the reader can find all the details.

References

[GRB26] D. A. J. Gómez-Ramírez and A. F. Boix. On extensions of Dirichlet and Green–Tao theorems and Goldbach–Dirichlet representations over certain families of commutative rings with unity. *Math. Nachr.*, **229** n.1 (2026), pp. 117–128.

Corbes el·líptiques associades a varietats abelianes 3-dimensionals amb multiplicació imaginària

Francesc Fité
Universitat de Barcelona
Wednesday, January 28th, 17:30-18:20

Sigui A una varietat abeliana 3-dimensional definida sobre els nombres racionals. L'aparellament de Weil mostra el seu primer grup

de cohomologia étale $H^1(A)$ com una subrepresentació de $H^3(A)(1)$. Si l'anell d'endomorfismes geomètrics d'A consisteix únicament de les multiplicacions enteres, aleshores el teorema d'imatge oberta de Serre garanteix que cap altra part de $H^3(A)$ prové de l'H^1 d'una varietat abeliana. Suposem que l'àlgebra d'endomorfismes geomètrics d'A és un cos quadràtic imaginari M. El resultat explicat a la xerrada d'en Pip Goodman associa a A una corba el·líptica E definida sobre els racionals, amb multiplicació complexa potencial per M, tal que $H^1(E)$ apareix com una subrepresentació de $H^3(A)(1)$. En aquesta xerrada explicaré treballs en curs en col·laboració amb S. Chidambaram, P. Goodman i F. Pedret que determinen la classe d'isogènia d'E quan A recorre certes famílies de varietats abelianes amb multiplicació imaginària per l'arrel quadrada de -1, -2 i -3, respectivament.

Recognizing fake elliptic curves

Enric Florit
Universitat de Barcelona

`Monday, January 26th, 12:40-13:00`

The system of Galois representations attached to an abelian surface with quaternionic multiplication looks remarkably similar to the one attached to an elliptic curve. The two systems are two-dimensional and have rational traces, and they both satisfy an open-image theorem. For this reason, QM surfaces are sometimes called fake elliptic curves. In this talk, I will explain a result over imaginary quadratic fields that separates fake elliptic curves from actual ones by studying the non-surjective primes of the residual representations.

Hasse principle and twists of the modular curve $X(p)$

Nuno Freitas
ICMat, Madrid

`Monday, January 26th, 11:10-12:00`

The Hasse principle is the idea that a Diophantine equation over the rational numbers should have a rational solution if and only if it has solutions in all of its completions, namely, the real numbers and all p-adic fields. In recent work of Lorenzo and Vullers, they give twists of the modular curve $X(7)$ that are counterexamples to the Hasse principle. In this talk, we will discuss generalizations of their result, for example, that there are infinitely many counterexamples to the Hasse principle that are twists of the modular curve $X(p)$ for primes p congruent to 1 (mod 4). This is joint work with Diana Mocanu.

Primes ramified in coefficient fields of modular forms

Filip Gawron
Universitat de Barcelona

`Monday, January 26th, 16:40-17:00`

Let $f \in \mathbf{S}_k(\Gamma_0(N), \chi)^{\text{new}}$ be a newform of level N and nebentypus χ. Knowing N and χ, what can we say about the field $\mathbb{Q}_f$ generated by the Fourier coefficients of f? In particular, what can we say about primes ramifying in $\mathbb{Q}_f$? In the talk, I will show some numerical calculations in the case $k = 2$ and trivial nebentypus. I will also discuss some existing results. Finally, I will comment on my recent work about ramification occurring when the level N is non-optimal.

Elliptic curves attached to abelian threefolds with imaginary multiplication

Pip Goodman
Universitat de Barcelona
Wednesday, January 28th, 17:05-17:25

Let A be an abelian threefold defined over a number field K with geometric endomorphism algebra an imaginary quadratic field M. In this talk, I will prove the existence of an elliptic curve E/K with CM by M whose associated Galois representations are determined by those of A. This is joint work with Francesc Fité.

Explicit base-change lifts of modular forms

Antti Haavikko
Universidad of Alcalá de Henares
Monday, January 26th, 17:05-17-25

In this talk, we introduce explicit formulas for two known Langlands base-change results: Doi-Naganuma lifting in the case of real quadratic number fields and its generalisation to totally real cyclic number fields of prime degree by Saito. Moreover, we talk about the on-going work of generalising Saito's results to the compositum of two totally real cyclic extensions of prime degrees. We call the results above explicit since they provide the Fourier coefficients for the base-change lifted Hilbert modular forms, which we know exist thanks to Arthur and Clozel in the cyclic case, or more in general, thanks to Dieulefait.

Todo entero se puede escribir como suma de un cuadrado y un libre de cuadrados

Jorge Jiménez Urroz
Universidad Politécnica de Madrid
`Monday, January 26th, 16:10-16:30`

En 1931 Estermann establece que cualquier número suficientemente grande se puede escribir como suma de un cuadrado y un libre de cuadrados. En la charla vamos a probar que cualquier entero sin restricción se puede representar de esa manera, dando la fórmula asintótica y acotando de forma explícita el término de error. A diferencia del artículo original, la prueba es básicamente elemental, cribando los cuadrados, y dando cotas concretas del número de divisores sobre cuerpos cuadráticos y sobre los enteros. La cota sobre la función divisor es ligeramente mejor que las conocidas hasta el momento.

Fermat curves over number fields and the Hasse principle

Alain Kraus
Institute Jussieu, Paris, France
`Wednesday, January 28th, 15:00-15:50`

Let p be a prime number. A Fermat curve over $\mathbb{Q}$ of exponent p is defined by an equation of the shape $ax^p + by^p + cz^p = 0$ where a, b, c are non-zero rational numbers. The aim of this talk is to discuss the following recent result. Let $d \geq 1$ be an integer. If p is large enough with respect to d, for instance $p > 1 + d(d+1)$, then there exist infinitely many Fermat curves over $\mathbb{Q}$ of exponent p such that, for any number field K of degree $[K : \mathbb{Q}] \leq d$, these curves contradict the Hasse principle over K and are pairwise non K-isomorphic.

Extension of root-based attacks against fully-split PLWE instances via isomorphisms

Rodrigo Martín Sánchez-Ledesma
Universidad Complutense de Madrid
`Wednesday, January 28th, 16:40-17:00`

In this talk, we present some results concerning the generalization of attacks on the Polynomial Learning With Errors problem that we provisionally offered in [1]. In these attacks, knowledge of a root of the generating polynomial of the polynomial ring over a certain (finite) base field is used to obtain algorithms that can solve, under certain conditions, the PLWE problem in its decision variant. Now our goal is to extend these attacks by constructing morphisms based on instances vulnerable to the attacks described above. Our results indicate that if the generating polynomial is totally factorizable over the base field, it is not possible to find new vulnerabilities.

To prove this, the key idea is to construct explicit isomorphisms between fully factorizable polynomials and show that such isomorphisms always distort the samples in such a way that the transformed samples cannot be used as an advantage for the decision-making attack. In other words, they do not allow us to distinguish whether such samples come from a PLWE-type distribution or from a purely uniform distribution, so that the attack is ineffective. Furthermore, we show that any isomorphism must be one of the explicitly constructed, thus showing that this approach cannot yield any new vulnerabilities, in a fully-split setting.

[1] I. Blanco Chacón, R. Durán Díaz, R. Martín Sánchez-Ledesma, A Generalized Approach to Root-based Attacks against PLWE, Cryptography and Communications (QuRCry). doi:10.1007/s12095-025-00849-9.

Revisiting the Fermat equation of exponents $(3, 3, p)$

Diana Mocanu
Max Planck Institute, Bonn, Germany
`Monday, January 26th, 12:10-12:30`

Wiles' famous proof of Fermat's Last Theorem opened up the possibility of tackling many Diophantine equations using the same method, called the modular method. In this talk, I will give a brief sketch of the modular method and then use it to show that the equation $x^3 + y^3 = 5^\alpha c^p$ has no non-trivial coprime solutions for p in a given list of primes. In the elimination step, I will use a recent joint work with Nuno Freitas on local points on twists of the modular curve $X(p)$.

Explicit lower bounds on the conductors of elliptic curves and abelian varieties over number fields

Pierre Tchamitchian
Université Aix-en-Marseille
`Wednesday, January 28th, 16:10-16:35`

Following the work of Mestre, we use Weil's explicit formulas to compute explicit lower bounds on the conductors of elliptic curves and abelian varieties over number fields. Moreover, we obtain bounds for the conductor of elliptic curves and abelian varieties over $\mathbb{Q}$ with specified bad reduction and over number fields. As an application, for specific fields, we prove the non-existence of abelian varieties with everywhere good reduction.

Additively indecomposable quadratic forms over totally real number fields

Magdaléna Tinková
Czech Technical University, Prague
Monday, January 26th, 17:30-17:50

Additively indecomposable quadratic forms with integer coefficients were studied, for example, by Mordell (1930, 1937) and Erdős and Ko (1938, 1939). However, we know much less about them if their coefficients belong to the ring of algebraic integers of a totally real number field. Some of our new results are general, but one part is restricted to the case of binary quadratic forms over real quadratic fields. For them, we provide some bounds on the number of such additively indecomposable quadratic forms, show that their number is rather large for almost all quadratic fields, or give their whole structure for several examples of these fields. We also show a relation between them and the problem of n-universal quadratic forms. This is joint work with Pavlo Yatsyna.

Divertiment aritmètic per a relax

Artur Travesa
Universitat de Barcelona
Friday, January 30th, 13:15-13:45

Acabem el Seminari amb una picada d'ullet a l'aritmètica bàsica, a nivell de primer curs.

Correspondence theorems for infinite Hopf–Galois extensions

Gabor Wiese
Université du Luxembourg
`Monday, January 26th, 15:00-15:50`

In this talk, I will speak on joint work with Hoan-Phung Bui and Joost Vercruysse, which extends Hopf–Galois theory to infinite field extensions. We provide a natural definition of subextensions and for separable (possibly infinite) Hopf–Galois extensions, we obtain a Galois correspondence.