Fonds National de la Recherche Luxembourg

UNIVERSITÉ DU LUXEMBOURG
Mathematics Research Unit (RMATH)

DSSE DOCTORAL SCHOOL IN SCIENCE AND ENGINEERING

http://math.uni.lu/nt/summerschool2018

SUMMER SCHOOL
Explicit and Computational Approaches to Galois Representations

Speakers

Sara Arias-de-Reyna
Henri Cohen
Bas Edixhoven
Davide Lombardo

Organizing Committee

Shaunak Deo
Ilker Inam
Antonella Perucca
Alexander Rahm
Gabor Wiese

3-7 July 2018 University of Luxembourg

UNIVERSITÉ DU LUXEMBOURG

FOUNDATION COMPOSITIO MATHEMATICA

Objective

The aim of the summer school is to provide foundational knowledge necessary for carrying out independent research on explicit and/or computational aspects of Galois representations. It is especially aimed at PhD candidates, but more advanced researchers as well as advanced Master students are welcome.

Organizing Committee

- **Shaunak Deo,** University of Luxembourg, Luxembourg
- **İlker İnam,** Bilecik Şeyh Edebali University, Turkey
- **Antonella Perucca,** University of Luxembourg, Luxembourg
- **Alexander Rahm,** University of Luxembourg, Luxembourg
- **Gabor Wiese,** University of Luxembourg, Luxembourg

Lecturers

- **Sara Arias-de-Reyna,** University of Sevilla, Spain
- **Henri Cohen,** University of Bordeaux, France
- **Bas Edixhoven,** University of Leiden, The Netherlands
- **Davide Lombardo,** University of Pisa, Italy

Location

University of Luxembourg, Belval Campus, Esch-sur-Alzette.
All activities take place in the **Maison du Savoir (MSA)**. It is a huge and long building with an 18 floor tower sitting on top of it. Registration will be close to the lecture room and it will be open well before the start. Lecture rooms and class rooms: MSA 3.110 (main lecture room), MSA 3.040 (lecture room), class rooms MSA 2.240, MSA 2.230, computer room MSA 2.200.

Practical information

HOW TO REACH LUXEMBOURG

- **By plane:** There is an airport in Luxembourg City. You may also want to check the availabilities of nearby airports in Belgium (Brussels Airport, Charleroi), or Germany (Frankfurt Hahn, Frankfurt Main) and look for bus connections to Luxembourg City.
- **By train:** Luxembourg City is 2 hours from Paris by high-speed trains and 3 hours from Brussels. There are also high-speed trains in the direction of Metz/Strasbourg/Marseille.
- **By car:** In the summer, driving inside Benelux is very convenient.

TRANSPORTATION IN LUXEMBOURG

- Maps, and how to reach Campus Belval: `https://wwwen.uni.lu/kontakt/campus_belval`.
- The simplest and usually the best option to get to Campus Belval is by taking the train (even if you are lodged in Esch-sur-Alzette). There are four trains per hour (during day time on working days). The train station at Campus Belval is called "Belval-Université". Campus Belval is connected by direct trains with the City of Luxembourg (30 minutes). The train stops at Bettembourg and Esch-sur-Alzette (and at some other stops). Check train (and bus) times on the CFL website or at mobiliteit.lu.

- We strongly advise you to buy day-tickets. They cost only 4 EUR (per day) and allow you to take any public transport (trains, trams and busses) in the entire country. A single ride is 2 EUR. That may only be interesting on your day of arrival or departure.
- Single rides and day-tickets can be bought at any ticket machine (usually accepting coins, EURO banknotes and bank/credit cards) or at the ticket counter at the main train stations. If you buy a ticket from the machine, it is already validated (i.e. you must buy it before the first ride of the day and cannot buy it the evening before). At the ticket counter and the mobility centers you can get chip cards on which you can load tickets in advance. In that case, it suffices to validate a loaded ticket at the platform before entering the train (or inside the bus).
- There is no centralised number to call a Taxi, but various Taxi companies. For example: Webtaxi, Mondial Taxis. Taking a Taxi may be very expensive (count up to 100 EUR to get from the airport to your hotel; by public transport it is 2 EUR; during heavy traffic you might even be faster by public transport), we recommend you to book a taxi in advance and agree on a flat rate (taxis waiting e.g. at the station do not apply a flat rate).

ACCOMMODATION

Those for who we provide free accommodation are lodged in one of the following hotels:

- Youth Hostel in Esch-sur-Alzette. It has very high standards, and it is conveniently located right at the train station. You can reach Campus Belval by train in 5 minutes (4 trains per hour during day time). The reception is open 24/7. Bedsheets are provided, but towels and soap/shampoo you have to bring yourself.
- Ibis Hotel located on the Campus Belval.
- Hotel Bernini in Bettembourg. It is a little more than a kilometer walk from Bettembourg train station, which connects you to Belval Campus and the City of Luxembourg by direct trains (4 trains per hour during day time). The reception is open from 7:00 to 23:00. If you should arrive later, please call the hotel and make special arrangements.
  To walk to Hotel Bernini, leave Bettembourg train station at the side of the station building where there is also the bus station. Turn left and follow the rails (they are always on your left) until you get to a very large bridge that is for pedestrians only (and does not seem to be on google maps). Cross the train lines via that bridge. You will automatically get to Rue Lentz. Follow that street to its end (i.e. do not turn left at the only possibility). Turn right into the Route de Luxembourg and follow it until you see the pink building Hotel Bernini on your left (on the right hand side there is a Q8 petrol station).
  There are also some buses (none in the evening) going from Bettembourg station to Hotel Bernini. Get bus number 200 at Bettembourg bus station right in front of the train station building in the direction Luxembourg and get off at the second stop "12 Gargullen" after a 3 min ride. You see the pink building of Hotel Bernini on your left.

If we do not provide free accommodation for you, you can also check the availability of other Youth Hostels in Luxembourg. Close to the train station in Esch-sur-Alzette there is also Hotel Acacia. In case you find no accomodation at a reasonable price in Luxembourg, consider that the city Thionville (in France) is only 15 minutes away from Bettembourg by train, and there you have a direct train to Campus Belval.

EATING/DRINKING

- Find out more about the new quarter Belval where the school is held (the site, restaurants, shopping, etc.) `http://www.belval.lu/en/`
- There is a university restaurant on the Campus Belval near the building "Maison du Savoir MSA", the menu is here: `https://portal.education.lu/restopolis/Belval/Todays-menus`. You can buy vouchers at the reception desk of the summer school.
- On the Campus Belval there are several eating/drinking possibilities, some of which are on the main square and in the shopping center (Belval Plaza). There is also a well-furnished supermarket (Del Haize) where you can also find sandwiches, sushi etc.

- In Esch there are various eating possibilities. Near the train station (Place de l'Hôtel de Ville) you have a small Carrefour supermarket.

EMERGENCIES

- To call an ambulance, in Luxembourg you dial **112**. The closest hospital to Campus Belval is the CHEM in Esch:
  `https://www.chem.lu/patients-et-visiteurs/urgences/informations-pratiques`.
- In the night and in the weekends there is always a doctor on duty (this is not for emergencies): you can go to Maison médicale in Esch (70, rue Émile Mayrisch):
  `http://www.sante.public.lu/fr/urgences-gardes/services-garde/maisons-medicales/index.html`
  After midnight, you are expected to call 112 but, if you do not have an emergency, you will be contacted by the doctor on duty (who may even have the possibility to come to you).
- There are no pharmacies on the Campus Belval. There are various pharmacies in Esch (Trierweiler is at the train station): `https://www.pharmacie.lu/pharmacies/?search=Esch`
  Some pharmacies are open at night, see:
  `https://www.pharmacie.lu/service-de-garde/`.

Schedule

Lectures in MSA 3.110. Exercises/Projects in MSA 3.110 and 3.040.

	Tuesday	Wednesday
09.00 - 10.30	Elliptic Curves 1	Modular Forms 1
10.30 - 11.00	Coffee Break	Coffee Break
11.00 - 12.30	Abelian Varieties 1	Galois Reps. 1
	Lunch Break	Lunch Break
14.00 - 15.30	Short Talks 1	Short Talks 2 (start 13.30h!)
15.30 - 15.45	Coffee Break	Coffee Break
15.45 - 18.00	Exercises/Projects 1	Exercises/Projects 2
18.00 - 21.00	Pizza & free/project work	Free/project work

	Thursday	Friday	Saturday
09.00 - 10.30	Elliptic Curves 2	Elliptic Curves 3	Abelian Varieties 3
10.30 - 11.00	Coffee Break	Coffee Break	Coffee Break
11.00 - 12.30	Abelian Varieties 2	Modular Forms 2	Modular Forms 3
	Lunch Break	Lunch Break	Lunch Break
14.00 - 15.30	Galois Reps 2	Galois Reps 3	Project presentation and closing
15.30 - 15.45	Excursion	Coffee Break	Free work
15.45 - 18.00	Excursion	Exercises/Projects 3	Free work
18.00 - 21.00	Excursion	Free/project work	

Contributed talks

TUESDAY, 3 JULY, MSA 3.110

14:00-14:20	Misja Steinmetz	Explicit Serre weights for two-dimensional Galois representations
14:30-14:50	Matthew Bisatt	Root numbers of abelian varieties
15:00-15:20	Jędrzej Garnek	Class numbers of division fields of abelian varieties

TUESDAY, 3 JULY, MSA 3.040

14:00-14:40	Samuele Anni	**Sage Introduction**
14:50-15:30	Henri Cohen	**Pari/GP Introduction**

WEDNESDAY, 4 JULY, MSA 3.110		
13:30-13:50	Antonela Trbovič	Torsion groups of elliptic curves over quadratic fields $\mathbb{Q}(\sqrt{d})$, $0 < d < 100$
14:00-14:20	Gregorio Baldi	Independence of points on elliptic curves coming from modular curves
14:30-14:50	Nirvana Coppola	Inertia action on elliptic curves
15:00-15:20	Emiliano Ambrosi	An explicit bound on l-primary torsion of one dimensional families of abelian varieties in positive characteristic
WEDNESDAY, 4 JULY, MSA 3.040		
13:30-13:50	Shalini Bhattacharya	On the reduction of Galois representations and local constancy with respect to weight
14:00-14:20	Ariel Weiss	Images of Galois representations attached to low weight Siegel modular forms
14:30-14:50	Erhan Gürel	Galois structures of modular forms of even weight
15:00-15:20	Samuele Anni	Congruences, modular Galois representations and Atkin-Lehner signs: an interpretation via graphs

Main lectures

Sara Arias-de-Reyna
(University of Sevilla, Spain)

Elliptic Curves

Contents: Group law, torsion points, isogenies, mod p and p-adic Galois representation, compatible systems, Néron-Ogg-Shafarevich criterion, p-adic uniformization of elliptic curves: Tate's Curve, image of inertia at a prime of multiplicative reduction, conductor, Tate's algorithm, LMFDB - information about elliptic curves.

Henri Cohen
(University of Bordeaux, France)

Modular Forms

Contents: Elliptic functions, modular forms and functions, Hecke operators, Euler products, functional equations, modular forms on subgroups, more general modular forms.

Bas Edixhoven
(University of Leiden, The Netherlands)

Galois Representations Attached to Modular Forms

Contents: Galois representations, modular curves over $\mathbb{C}$, elliptic curves over $\mathbb{C}$, modular forms geometrically, arithmetic moduli of elliptic curves, construction of the Galois representation attached to a Hecke eigenform, local study of the Galois representation, computational aspects.

Davide Lombardo
(University of Pisa, Italy)

Abelian Varieties

Contents: Néron-Ogg-Shafarevich criterion for bad reduction and the semistable reduction theorem, point-counting (especially on Jacobians) via characteristic polynomials of Frobenius, classification of endomorphism algebras, CM abelian varieties and their corresponding representations, polarizations and the Weil pairing.

Contributed Talks

Emiliano Ambrosi

An explicit bound on l-primary torsion of one dimensional families of abelian varieties in positive characteristic

(Ecole Polytechnique, Paris, France)

Abstract: Let $f : Y \to X$ be a one dimensional family of abelian varieties over a smooth geometrically connected base over a field of positive characteristic p. Fix a prime l different from p. Following ideas of Anna Cadoret and Akio Tamagawa we show, as a conseguences of the Weil conjectures, that there exists an explicit constant $C := C(\ell)$ such that, for all but finitely many closed points in X, the fibre of f in x has no k-rational points of order l^C. This result relies on an explit lower bound for the gonality of some étale covers of X.

Samuele Anni

Congruences, modular Galois representations and Atkin-Lehner signs: an interpretation via graphs

(MPIM Bonn, Germany)

Abstract: Congruences between modular forms play a crucial role in understanding links between geometry and arithmetic: cornerstone example of this is the proof of Serre's modularity conjecture by Khare and Wintenberger. Congruences of Galois representations govern many kinds of representations of the absolute Galois group of number fields. Even though our understanding is improving, many aspects remain very mysterious, some are theoretically approachable, many are not; and amongst the latter, some allow numerical studies to reveal first insights. In this talk I will introduce congruence graphs, which are graphs encoding congruence relations between classical newforms (joint work with Vandita Patel). Then I will explain first how to construct analogous graphs for congruences of Galois representations, and then how to use these graphs to study questions regarding Hecke algebras and Atkin-Lehner operators.

Gregorio Baldi

Independence of points on elliptic curves coming from modular curves

(University College London, United Kingdom)

Abstract: Modular curves naturally parametrise elliptic curves, in particular it makes sense to consider isogeny classes inside such curves. Given a correspondence between a modular curve S and an elliptic curve E, we prove that the intersection of any finite rank subgroup of E with the set of points on E coming from an isogney class on S is finite. The proof relies on Serre's open image theorem and various equidistribution results.

Shalini Bhattacharya

On the reduction of Galois representations and local constancy with respect to weight

(MPIM Bonn, Germany)

Abstract: Let p be a prime number. The two-dimensional crystalline representations of the local Galois group $\mathrm{Gal}(\bar{\mathbb{Q}}_p \mid \mathbb{Q}_p)$ are parametrized by the pairs (k, a) up to twists, where $k \geq 2$ is an integer and $a \in m_{\bar{\mathbb{Z}}_p}$, the maximal ideal in the ring of integers of $\bar{\mathbb{Q}}_p$. We are interested in studying the map

$$(k, a) \mapsto \bar{V}_{k,a}$$

where $\bar{V}_{k,a}$ denotes the semisimplified mod p reduction of a typical crystalline representation $V_{k,a}$.
These reductions have been computed when $k \leq 2p+1$ or when a has a small p-adic valuation. Using the theory of Wach modules, Laurent Berger has also shown that the map displayed above is locally constant with respect to both the variables and found an explicit bound on the radius of local constancy when a varies (2012). However, if a is fixed and k varies, nothing more than the existence is known about the radius of local constancy. So we ask the following simple question: for any given p-adic integer a, how close do k and k' need to be in the weight space to ensure that $\bar{V}_{k,a} \cong \bar{V}_{k',a}$? We give a partial answer to this question using some explicit computations in the automorphic side of the p-adic and mod p Local Langlands Correspondences for $\mathrm{GL}_2(\mathbb{Q}_p)$.

Matthew Bisatt

Root numbers of abelian varieties

(Kings College London, United Kingdom)

Abstract: Given an abelian variety over a number field, the Birch and Swinnerton-Dyer conjecture relates its set of rational points to an L-function. A simple consequence is the parity conjecture which states that the parity of the rank should be determined by the root number, which is the expected sign in the functional equation. In this talk, we will show how to explicitly compute the root number and discuss related phenomenon.

Nirvana Coppola

Inertia action on elliptic curves

(University of Bristol, United Kingdom)

Abstract: The starting point of my work is the study of elliptic curves defined over a p-adic field and l-adic Galois representations attached to them. In particular an interesting problem is to describe the action and the possible image of the inertia group under these representations. This action depends first of all on the reduction type of the curve, for example it is trivial if and only if the curve has good reduction modulo p. Another key factor is the residue characteristic p of the field. For the case $p \geq 5$, this problem is completely solved, while for the cases $p = 2$ and 3 there still does not exist a complete description of the Galois action.

Jędrzej Garnek

Class numbers of division fields of abelian varieties

(Adam Mickiewicz University, Poland)

Abstract: Let A be an abelian variety defined over a number field K. Fix a prime p and a natural number n and consider the field K_n, obtained by adjoining to K all the coordinates of the p^n-torsion points of A. We give an effective lower bound on the p-part of the class group of K_n for large n, depending mostly on dimension and Mordell-Weil rank of A. The proof uses Galois representations attached to abelian varieties, in particular the theory of Kummer extensions of an abelian variety of Ribet and Bashmakov.

Erhan Gürel

Galois structures of modular forms of even weight

(METU Northern Cyprus Campus, Northern Cyprus)

Abstract: We calculate the equivariant Euler characteristics of an even power of the canonical sheaf on modular curves over $\mathbb{Z}$ with a tame action of a finite abelian group. As a consequence, we obtain information on the Galois module structure of "twisted" modular forms of even weight having Fourier coefficents in a ring of algebraic integers.

Misja Steinmetz

Explicit Serre weights for two-dimensional Galois representations

(King's College, London, United Kingdom)

Abstract: In their 2010 paper Buzzard, Diamond and Jarvis gave a first precise formulation of a generalisation of Serre's modularity conjecture to the setting of Hilbert modular forms over totally real number fields (in which p is unramified). Analogously to Serre's original recipe of the minimal weight attached to the representation, the authors give a recipe for the set of weights using Hodge-Tate weights and crystalline lifts of the representation. Recently, Dembélé, Diamond and Roberts gave an alternative explicit formulation for the set of weights using local class field theory instead of p-adic Hodge theory, which is much better suited to practical computations. I will talk about their construction as well as some recent work of mine in trying to extend their ideas to the case where p is arbitrarily ramified in the field.

Antonela Trbovič

Torsion groups of elliptic curves over quadratic fields $\mathbb{Q}(\sqrt{d})$, $0 < d < 100$

(University of Zagreb, Croatia)

Abstract: We prove results towards classifying the possible torsion subgroups of elliptic curves over quadratic fields $\mathbb{Q}(\sqrt{d}$, where $0 < d < 100$ is a square-free integer, and obtain a complete classification for 49 out of 60 such fields. Over the remaining 11 quadratic fields, we cannot rule out the possibility of the group $\mathbb{Z}/16\mathbb{Z}$ appearing as a torsion group of an elliptic curve.

Ariel Weiss

Images of Galois representations attached to low weight Siegel modular forms

(University of Sheffield, United Kingdom)

Abstract: Heuristically, the image of a Galois representation coming from an automorphic form should be as large as possible, unless there is an automorphic reason why it shouldn't be. For example, the Ramanujan 691 congruence can be detected in the fact that image of the 691-adic representation of Δ is small - it is residually reducible. In this talk I will discuss the image of Galois representations coming from low weight Siegel modular forms, and give a theoretically checkable condition for when the associated l-adic Galois representation is irreducible.