SUMMER SCHOOL GALOIS THEORY AND NUMBER THEORY

Course no. 1: Specializations in Inverse Galois Theory

Speakers: Pierre Dèbes, Joachim König, Danny Neftin, Umberto Zannier.

General outline: Specialization is one of the few general tools that provide a bridge between geometry and arithmetic. Given a geometric system involving some independent parameters, it makes it possible to specialize the parameters in the base field (the field $\mathbb{Q}$ of rationals for example) and still preserve the structure of the system. This is the so-called Hilbert Property. The system structure can be for instance the Galois group of a field extension; the Hilbert Property follows then from Hilbert's celebrated irreducibility theorem from 1892. The course is aimed at reviewing the specialization process and revisiting it towards some modern developments: some very recent results by Corvaja–Zannier on the Hilbert Property of certain unirational varieties, others by Dèbes–König–Legrand–Neftin on the specialization set of covers of the line, finally some on different aspects of the Grunwald Problem including work by Harpaz–Wittenberg on the Brauer–Manin obstruction.

Lecture 1: The specialization process in Galois theory (Pierre Dèbes – Saturday, 9:00-10:30).

Abstract: We will present the main definitions around the notion of specialization: specialized field extensions, Hilbert subset, thin subset, the Hilbert specialization property, Hilbertian field, etc. We will then introduce three situations in Galois theory where specialization plays a major role, and which will be developed in next lectures. These are the Regular Inverse Galois Problem, the study of regularly parametric covers, and the Noether Program.

Lecture 2: Specialization tools and first results (Pierre Dèbes – Sunday, 9:00-10:30).

Abstract: We will present some basic tools for specializing Galois function field extensions along with some first applications, including a proof of Hilbert's irreducibility theorem. We will also discuss some generalizations leading to the Colliot-Thélène approach to the Noether Program.

Lecture 3: About the Hilbert Property and the topology of algebraic varieties (Umberto Zannier – Sunday, 14:30-16:00).

Abstract: After recalling some standard motivations and definitions concerning the Hilbert Property and its applications, I shall illustrate some new examples in both cases of failure and attainment of it. They come from the observation that the HP can possibly hold for a smooth complete variety only if it is algebraically simply connected. The examples I shall present concern surfaces of Enriques type (failure) and the Fermat quartic surface $x^4 + y^4 = z^4 + w^4$ (which has the HP/$\mathbb{Q}$). I will also illustrate a link with "weak approximation". Most of this has been obtained in joint work with P. Corvaja (and extended to further cases by J. Demeio by similar principles).

Lecture 4: A modified Hilbert Property for group varieties (Umberto Zannier – Monday, 9:00-10:30).

Abstract: The limitations pointed out in the previous talk for a variety to have the Hilbert Property can be overcome if one considers merely ramified covers, which is not very restrictive for the applications. So it seems worth studying whether a "modified HP" in this sense may hold. Group varieties are natural to look at, because they often have many rational points, so there is not an 'a priori' obstruction for the HP. I will illustrate a method to prove such a HP for tori (this was later extended by Corvaja to linear algebraic groups). This yields some applications, as for instance a proof of the so-called "Pisot d-th root conjecture" for linear recurrences, actually in strengthened form.

Lecture 5: Gathering extensions into families (Danny Neftin – Tuesday, 9:00-10:30).

Abstract: Parametrizing a set of Galois extensions by a single extension with parameters is a common approach in computational Galois theory, and statistical Galois theory. We shall discuss the problem of parametrizing all or part of the extensions with a given Galois group G using one or two parameters, and a mod-p approach to this problem.

Lecture 6: Rational pullbacks of Galois covers of the line (Joachim König – Wednesday, 9:00-10:30).

Abstract: I will introduce the notion of the pullback of a Galois cover $f : X \to \mathbb{P}^1$ by a rational function. In many ways, the pullback is a natural "geometric" analog of the specialization of a Galois cover (defined over a field k) at a value $t_0 \in k$. We may then formulate analogs of many famous specialization problems in the world of pullbacks. This is meaningful because
a) pullbacks are "rich" even over algebraically closed fields (whereas specializations are not), reflecting the fact that the RIGP is of interest over all fields, and
b) because results about pullbacks may serve as test models for what might be expected about some open problems on specialization sets over number fields.
After introducing some basic machinery on covers and their pullbacks, I will discuss some recent joint results with Dèbes, Legrand, and Neftin. In particular, we introduce a pullback analog of the problem of "parametric extensions" ("Regular Parametricity") and of the Beckmann–Black Problem. Over a base field such as $k = \mathbb{C}$, we solve these regular analogs in full, showing, e.g., that the set of all pullbacks of a fixed G-cover is usually "tiny" (in a well-defined sense) in the set of all G-covers. I will also discuss what these results might indicate regarding the parametricity problem over number fields, and compare the different but related notions of (regularly or not) parametric and generic extensions.

Lecture 7: The Brauer–Manin obstruction (Danny Neftin – Thursday, 9:00-10:30).

Abstract: The validity of the local global principle is a main theme in number theory. We shall discuss the role of the Brauer group as the "only obstruction" to the local global principle, to weak approximation, and lifting problems. Finally, we discuss recent breakthroughs in studying these properties following a better understanding of the structure of the Brauer group.

Course no. 2: Random Polynomials

Speakers: Lior Bary-Soroker, Ofir Gorodetsky, Joachim König, Dimitris Koukoulopoulos.

General outline: The aim of this course is the study of random polynomials, putting the emphasis on integral polynomials. The questions we are interested in are the number of real roots, irreducibility over the rationals, and the typical Galois group. One model we will study is the so-called large box model in which the size of the coefficients is much larger than the degree. A more difficult model, in which there are several recent breakthroughs, is the bounded height model, in which we choose the coefficients from a fixed set and let the degree grow.

Lecture 1: Methods for computing Galois groups (Joachim König – Saturday, 11:00-12:30).

Abstract: We will present several methods to compute Galois groups, via inertia groups, decomposition groups, Newton polygons, resolvents, function field methods, etc. The methods will be exemplified via several classical and modern examples.

Lecture 2: Roots of random polynomials (Ofir Gorodetsky – Monday, 11:00-12:30).

Abstract: The talk will cover the following topics: the number of real roots of a random polynomial (Littlewood–Offord Theorem, Kac Theorem, etc.), the model of random polynomials of bounded height, and low degrees of a random integral polynomial.

Lecture 3: Irreducibility of polynomials of bounded height (Dimitris Koukoulopoulos – Wednesday, 11:00-12:30).

Abstract: The talk will present the recent progress on the following question: what is the probability that a random polynomial of large degree all of whose coefficients lie in a given fixed set is irreducible?

Lectures 4 and 5: Probabilistic Galois theory (Lior Bary-Soroker – Thursday, 11:00-12:30 and Friday, 9:00-10:30).

Abstract: We will study the Galois group of random polynomials in the large box model. The talks will include classical results such as theorems saying that most polynomials have Galois group S_n (Van der Waerden theorem, Gallagher theorem, and others), Kuba's sharp counts of irreducibles, polynomials in families, etc.

Course no. 3: Number Theory in Function Fields

Speakers: Alexei Entin, Dimitris Koukoulopoulos.

General outline: Number theory in function fields studies the arithmetic of polynomials over a finite field, and more generally the function fields over a finite field. This world shares a lot with the classical setting of the integers and number fields, but is also equipped with other tools coming from algebraic geometry. The course will focus on the statistical point of view of number theory in which we study statistical features of arithmetic functions (such as mean values, correlations, etc.). We will see classical results in the integers and their analogues to polynomials as well as novel approaches using monodromy, Galois groups, and equidistribution theorems.

Lecture 1: Introduction to number theory in function fields (Alexei Entin – Saturday, 14:30-16:00).

Abstract: The talk will cover the following topics: the analogy between the ring of integers $\mathbb{Z}$ and the ring of polynomials $\mathbb{F}_q[t]$, basic parallels, the Prime Polynomial Theorem, function fields and curves, ζ-functions of curves, and the Riemann Hypothesis.

Lectures 2 and 3: Anatomy of integers, permutations, and polynomials (Dimitris Koukoulopoulos – Sunday, 11:00-12:30 and Monday, 14:00-15:30).

Abstract: These talks will discuss probabilistic methods in number theory. Specifically, we will introduce the Kubilius model of the integers and use it to study the anatomy of a 'typical' integer. Some results we will sketch the proof of are the Erdős–Kac theorem, the Hardy–Ramanujan inequality, and a theorem determining the size of the prime factors of a typical integer. In addition, we will use this point of view to study the distribution of the divisors of a typical integer. All these results have analogues in the permutation and polynomial setting, which we will explain. Finally, we will show how using this analogy can answer questions about transitive subgroups and invariable generation of S_n.

Lectures 4 and 5: Galois groups and arithmetic statistics in function fields (Alexei Entin – Wednesday, 14:00-15:30 and Thursday, 14:00-15:30).

Abstract: The goal of these talks is to present methods for solving problems on arithmetic statistics (e.g., the distribution of primes) in function fields in the large finite field limit. Our main tools will be a Chebotarev density theorem and calculation of Galois groups of function field extensions in several variables (or, equivalently, monodromy of covers of varieties).

In the first talk, we will discuss varieties over finite fields, the Frobenius map, descent over finite fields, étale covers, monodromy and Galois groups, complexity of varieties and morphisms, and the Chebotarev density theorem for a cover of varieties. In the second talk, we cover the use of ramification and inertia groups, example: the monodromy of a Morse function, sectional monodromy of projective curves, applications: function field analogues of Hardy–Littlewood, Bateman–Horn conjectures, and more.