Update: *September 23, 2012*

February 4-8, 2013, Calicut (Kozhikode, Kerala, India).

The Kerala School of Mathematics (KSoM)

Workshop on number theory and dynamical systems

1. Linear recurrent sequences and iterations of linear maps

The problems. By *dynamical system* we usually mean the datum of a space X and an endomorphism $\Phi : X \to X$, where we are interested in studying the properties of the orbits of the points of X under the iterations of Φ.

Many problems can be dealt with in dynamics, according to the properties of the orbits we are interested in. In this course, we shall be mainly interested in the following problem:

Given a vector space X, a linear endomorphism $\Phi \in \mathrm{End}(X)$, a point $P \in X$ and an algebraic variety $Y \subset X$, describe the intersection $\{\Phi^n(P) : n = 0, 1, 2 \ldots\} \cap Y$. In particular,when does $\Phi^n(P)$ belong to Y for infinitely many n?

Let us see particular instances of this problem.

`Example 1`. Given an algebraic number, decide when it is a root of unity. If α is this algebraic number, and $d = [\mathbb{Q}(\alpha) : \mathbb{Q}]$ its degree, consider the vector space $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$. Multiplication by α defines an automorphism of $\mathbb{Q}(\alpha)$ which has finite order if and only if α is a root of unity. Hence the problem is reduced to deciding when has a square matrix with rational entries finite order. In this case, it turns out to be equivalent to finding when is the orbit of any non zero vector infinite. Although it looks like a purely geometrical problem, its solution needs methods from number theory. A concrete example: the complex number $\frac{3}{5} + \frac{4}{5}i$ is not a root of unity, i.e. the matrix $\begin{pmatrix} 3/5 & -4/5 \\ 4/5 & 3/5 \end{pmatrix} \in \mathrm{SO}(2)$ has infinite order. Another formulation of the same problem: the powers $(2+i)^n$ are never real numbers. In other words, the orbit of the complex number 1 under multiplication by $2 + i$ will never meet the real axis again. Still another formulation: the projective automorphism given by the matrix $\begin{bmatrix} 2 & -1 \\ 1 & 2 \end{bmatrix} \in \mathrm{PGL}_2(\mathbb{R})$ has infinite order.

`Example 2`. Given a linear endomorphism $\Phi : \mathbb{C}^m \to \mathbb{C}^m$ and a hypersurface Y of equation $f(x_1, \ldots, x_m) = 0$, for a polynomial $f(x_1, \ldots, x_m) \in \mathbb{C}[x_1, \ldots, x_m]$, for every point $P \in \mathbb{C}^m$, consider the Diophantine equation

$$f(\Phi^n(P)) = 0$$

to be solved in positive integers n. It corresponds to the problem of finding the intersection of the orbit of P with Y. Again, a Diophantine equation is equivalent to a geometrical problem.

One can also consider non-commutative dynamical systems, i.e. non-commutative finitely generated semi-groups of endomorphisms. For instance, take two endomorphisms

Φ, Ψ and consider the set of endomorphisms $\Gamma := \{\Phi, \Psi, \Phi^2, \Phi \circ \Psi, \Psi \circ \Phi, \Psi^2, \Phi^3, \ldots\}$. Then the orbit of a point P under the semigroup Γ contains in particular the orbits of P under Φ and Ψ.

It turns out that the above problem reduce to studying Diophantine equations involving *linear recurrent sequences*. These are sequences $u : \mathbb{N} \to \mathbb{C}$ satisfying, for a certain integer $d > 0$ and coefficients $a_1, \ldots, a_d \in \mathbb{C}$, the linear relations

$$u(n+d) = a_1 u(n+d-1) + \ldots + a_d u(n).$$

The typical example is the Fibonacci sequence. Every linear recurrent sequence admits a (unique) representation as an exponential polynomial, i.e. can be written as

$$u(n) = p_1(n)\alpha_1^n + \ldots + p_h(n)\alpha_h^n,$$

where the *roots* $\alpha_1, \ldots, \alpha_h$ are non-zero complex numbers and the 'coefficients' $p_1(X), \ldots, p_h(X) \in \mathbb{C}[X]$ are polynomials.

The aim of these courses is two-fold. On one hand, we plan to show several results on the arithmetic of linear recurrence sequences, developing various Diophantine techniques; on the other hand, we show the application of the Diophantine theory to problem of dynamical origin.

Typical Diophantine results which will be treated include: Skolem-Mahler-Lech theorem on zeros of linear recurrent sequences, the solutions to Pisot's conjecture on perfect powers in a linear recurrent sequence (Zannier's theorem); more generally, equations of the form $f(x, u(n)) = 0$, where $f(X, Y) \in \mathbb{Q}[X, Y]$ is a polynomial, $u : \mathbb{N} \to \mathbb{Q}$ is a given linear recurrent sequence, and the solutions x, n are to be found in $\mathbb{Q} \times \mathbb{N}$, will be treated. The methods involve both Diophantine approximations, e.g. the Subspace theorem and the theory of linear forms in logarithms, and reduction modulo p and the theory of algebraic equations over finite fields (method of Ferretti-Zannier).

A possibility for the list of lectures:

(1) Linear recurrent sequences. Exponential polynomials. Iterations of linear endomorphisms, rational functions. [Equivalent definitions of linear recurrent sequences, algebraic theory, no arithmetic yet].

(2) Zeros of linear recurrent sequences. The binary case. Effective methods to decide whether an algebraic number is a root of unity. Solving $a\alpha^n + b\beta^n = 0$. [Example: $(2+i)^n$ is never (i.e. for any $n > 0$) a real number]

(3) Zeros of linear recurrent sequences: the ternary case. Linear forms in logarithms and effective solution of $a\alpha^n + b\beta^n = c$. [Giving for granted estimates for linear forms in logs].

(4) Zeros of linear recurrent sequences: the general case. P-adic methods. Skolem-Mahler-Lech theorem.

(5) General equations involving linear recurrent sequences. Subspace theorem approach. Perfect powers in linear recurrent sequences. [Applying the Subspace theorem without proving it]

(6) Pisot's conjecture, its generalizations and its solutions. [Idea of the proof by Zannier and Ferretti-Zannier]

(7) Applications: Diophantine equations on linear algebraic groups; Hilbert irreducibility over algebraic groups. [Corvaja, Annali SNS]

(8) Applications: Spectra of matrices in finitely generated sub-semigroups of linear groups. Non commutative dynamical systems, i.e. non commutative semigroups of endomorphisms. [Application of (7)].

(9) Applications: iterations of linear endomorphisms, intersection of orbits with algebraic subvarieties. [Geometric applications of Skolem-Mahler-Lech]

2. Diophantine approximation and dynamical systems

There is an other topic of number theory which strongly interplays with dynamical systems, namely several aspects of Diophantine approximation. To illustrate this feature, let us now consider the linear torus $X = (\mathbb{R}/\mathbb{Z})^m$ and let $\Phi = \Phi_\alpha$ be the translation map

$$\Phi(x) = x + \alpha$$

on X, where $\alpha = (\alpha_1, \ldots, \alpha_m)$ is a fixed point in X. We are again concerned with the density of an orbit $\{\Phi^n(P) \, : \, n = 0, 1, 2 \ldots\}$. Here density is understood with respect to the usual topology on the real torus, not the Zariski one as in part 1.

A reformulation in this setting of the classical Kronecker's density Theorem is the following statement :

Suppose that the real numbers $1, \alpha_1, \ldots, \alpha_m$ are linearly independent over $\mathbb{Q}$. Then, any orbit $\{\Phi^n(P) \, : \, n = 0, 1, 2 \ldots\}$ is dense in X.

A major problem is to understand how such an orbit fills the whole space X. As an example, equidistribution of the sequence $\{\Phi^n(P) \, : \, n = 0, 1, 2 \ldots\}$ follows from Birkhoff's ergodic Theorem. We are mainly concerned with effective properties of Diophantine approximation of a fixed point in X, which may be taken as the origin by changing eventually the initial point P.

For simplicity, we shall restrict to the dimension $n = 1$, although we may possibly explain without proof what happens in higher dimension and groups of higher rank [paper of Michel Laurent with Yann Bugeaud in Moscow Journal using "hat" exponents]. A classical statement on the density in $\mathbb{R}$ of the group $\mathbb{Z}\alpha + \mathbb{Z}$ is Minkowski Theorem:

Let α be an irrational number and let β be any real number not belonging to $\mathbb{Z}\alpha + \mathbb{Z}$. Then, there exists infinitely many integers p, q such that

$$|q\alpha + p - \beta| \leq \frac{1}{4|q|}.$$

We shall give a detailed proof of the following metrical version of Minkowski Theorem, essentially going back to Khintchine, using a zero-one law based on dynamical ideas such as the ergodicity of the multiplication by a non-zero integer in the torus:

Let β be a real number and let $\psi : \mathbb{N} \mapsto \mathbb{R}^+$ be a decreasing function such that

$$\sum_{\ell \geq 1} \psi(\ell) = +\infty.$$

Then, there exists infinitely many integers p, q such that

$$|q\alpha + p - \beta| \leq \psi(|q|).$$

Depending on the time and the level of the course, non-commutative dynamical systems could possibly be presented following the same pattern. For instance $X = \mathbb{R}^n$ on which we have the action of $\mathrm{SL}(n, \mathbb{Z})$, or a lattice.

Interesting problem : $X = \mathbb{R}^n/\mathbb{Z}^n$ with the action of $\mathrm{SL}(n, \mathbb{Z})$.

A possibility for the list of lectures:

(1) The box principle for homogeneous approximation. A simple proof of Minkowski Theorem (with 1/4 replaced by 1/2) using continued fractions [possibly an overview over continued fractions].
(2) Metrical theory. Borel-Cantelli Lemma and its converse for limsup sets.
(3) Zero-one laws and a complete proof of Khintchine Theorem.
(4) More advanced results [possibly describing a paper by Nogueira and Laurent on $\mathrm{SL}(2, \mathbb{Z})$ -orbits].

3. Continued fractions and the geodesic flow

It was seen in part 2 that for an irrational α, every real number can be approximated arbitrarily closely by one of the form $p + q\alpha$, with $p, q \in \mathbb{Z}$, and one proceeded towards getting better control on the approximations.

On the other hand if we consider a quadratic expression of the form $(p + q\alpha)(p + q\beta)$, assuming one or both of α, β to be irrational does not ensure that the values, as p and q run over integers, will approximate all real numbers, namely do not form a dense subset of $\mathbb{R}$. In the first place there exist irrational numbers α, such that $|(p+q\alpha)q|$ is bounded away from 0; these are so called badly approximable numbers, a property that holds whenever (and only when) the partial quotients in the continued fraction expansion of α are bounded;

in particular every quadratic irrational, e.g. $\sqrt{2}$, is badly approximable. Similarly, if α and β are both badly approximable numbers the values of $(p+q\alpha)(p+q\beta)$ do not form a dense subset of $\mathbb{R}$. Generalizations of this to the case of complex numbers, namely continued fractions for complex numbers and values of binary forms with complex coefficients will be discussed.

The question of the set of values as above being dense is related to that of density of orbits of the geodesic flow on the modular surface, namely the flow defined on $\mathrm{SL}(2,\mathbb{R})/\mathrm{SL}(2,\mathbb{Z})$ by the action of the one parameter subgroup $\{\mathrm{diag}\,(e^{t/2}, e^{-t/2})\}_{t\in\mathbb{R}}$. The latter were characterized by E. Artin and his result translates to the question at hand as follows: Call an irrational number *generic* if every block (finite sequence) $(b_1,\ldots,b_l)$ of positive integers occurs in the continued fraction expansion of $\{a_n\}$ of α, namely there exists k such that $a_k = b_1,\ldots,a_{k+l-1} = b_l$. Artin's theorem implies that if either α or β is a generic irrational number the set of values of $(p+q\alpha)(p+q\beta)$, with $p,q\in\mathbb{Z}$, is dense in $\mathbb{R}$. This provides a "generic" class of quadratic forms for which the desired assertion holds.

In these lectures we shall give a detailed proof of the above result, via an approach different from that of Artin (based on the joint work of S.G. Dani with Arnaldo Nogueira). This involves considering the action of $\mathrm{SL}(2,\mathbb{Z})$ on $\mathbb{P}\times\mathbb{P}$, where $\mathbb{P}$ is the projective space consisting of lines in $\mathbb{R}^2$ and the action is the one induced by the natural action of $\mathrm{SL}(2,\mathbb{Z})$ on $\mathbb{R}^2\backslash\{0\}$. We study the orbits of the action using the Euclidean algorithm, and then relate it to the question of values of the binary quadratic forms as above.

We shall also discuss the set of badly approximable numbers, involved in the quadratic forms for which density does not hold. We recall a two-player game introduced by W.M. Schmidt and apply it to show that the set of badly approximable numbers is "large" in the sense of having Hausdorff dimension 1. The relation of this with the dynamics of the geodesic flow as above will be brought out.

Analogous results for flows on more general homogeneous spaces, including in particular on $\mathrm{SL}(d,\mathbb{R})/\mathrm{SL}(d,\mathbb{Z})$, their applications to the theory of Diophantine approximation such as the Oppenheim conjecture, Littlewood conjecture, etc will be briefly indicated along with some open questions in the area.

A possibility for the list of lectures:

(1) Introduction to the issue of values of quadratic forms, badly approximable numbers, relation with hyperbolic geometry.

(2) Schmidt game, Hausdorff dimension and application to the set of badly approximable numbers.

(3) Euclidean algorithm on $\mathbb{R}^2$ and its application to studying the orbits of $\mathrm{SL}(2,\mathbb{Z})$ on $\mathbb{P}\times\mathbb{P}$.

(4) Proof of Artin's theorem and application to values of binary quadratic forms. Discussion on generalizations.

Pietro Corvaja, S.G. Dani, Michel Laurent, Michel Waldschmidt