Online Number Theory Seminar

8 December 2023. – 17:00-17:50

J-H. Evertse: Orders with few rational monogenizations

Recall that a monogenic order is an order of the shape $\mathbb{Z}[\alpha]$, where α is an algebraic integer. This is generalized to orders $\mathbb{Z}_\alpha$ for not necessarily integral algebraic numbers α as follows. For an algebraic number α of degree n, let $\mathcal{M}_\alpha$ be the $\mathbb{Z}$-module generated by $1, \alpha, \ldots, \alpha^{n-1}$; then $\mathbb{Z}_\alpha := \{\xi \in \mathbb{Q}(\alpha) : \xi\mathcal{M}_\alpha \subseteq \mathcal{M}_\alpha\}$ is the ring of scalars of $\mathcal{M}_\alpha$. We call an order of the shape $\mathbb{Z}_\alpha$ *rationally monogenic*. If α is an algebraic integer, then $\mathbb{Z}_\alpha = \mathbb{Z}[\alpha]$ is monogenic. Rationally monogenic orders are special types of invariant orders of polynomials, which were introduced by Birch and Merriman (1972), Nakagawa (1989), and Simon (2001).

If α, β are two $\mathrm{GL}_2(\mathbb{Z})$-equivalent algebraic numbers, i.e., $\beta = (a\alpha + b)/(c\alpha + d)$ for some $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Z})$, then $\mathbb{Z}_\alpha = \mathbb{Z}_\beta$. Given an order $\mathcal{O}$ of a number field, we call a $\mathrm{GL}_2(\mathbb{Z})$-equivalence class of α with $\mathbb{Z}_\alpha = \mathcal{O}$ a *rational monogenization* of $\mathcal{O}$.

It is known that every order of a number field has at most finitely many rational monogenizations. Among other things, we discuss our new result that if K is a number field of degree $n \geq 5$ with normal closure having maximal Galois group S_n, then apart from at most finitely many exceptions, every order of K has at most one rational monogenization.