COURSE DESCRIPTION FOR SKEW BASES OF "SIMPLE" FIELDS (RESEARCH)

1. The topic

Recently, in a joint paper with Fraczyk and Harcos, we managed to show that cylinders of the Minkowski space contain bases of number fields under the only assumption that their volume is large enough. It turns out that for real quadratic fields, our bound up to constant is optimal for general cylinders, but improvable for special ones. The goal of the research class is to investigate what happens for other simple special classes of number fields, e.g. totally real biquadratic or cubic fields.

Prerequisite: classical algebraic number theory (finite extensions of $\mathbb{Q}$, algebraic integers, notion of discriminant, etc.).

2. Preliminary assignment

Please send the solutions of the problems below to `magapeter@gmail.com`. Participation in the research is conditional to a good result on these problems.

1. Let k be a real quadratic extension of $\mathbb{Q}$, $\mathfrak{o}$ its ring of integers, Δ its discriminant. Prove that there is a set
$$C = [-a, a] \times [-b, b] \subseteq \mathbb{R}^2$$
such that $\mathrm{vol}(C) > |\Delta|/100$ and C does not contain a $\mathbb{Z}$-basis of $\mathfrak{o}$.
2. Let k be a real quadratic extension of $\mathbb{Q}$, $\mathfrak{o}$ its ring of integers, Δ its discriminant. Prove that the set
$$C = [-2, 2] \times [-100|\Delta|^{1/2}, 100|\Delta|^{1/2}] \subseteq \mathbb{R}^2$$
contains a $\mathbb{Z}$-basis of $\mathfrak{o}$.
3. Let k be a cubic extension of $\mathbb{Q}$. Prove that if $\mathrm{Gal}[k : \mathbb{Q}]$ is the cyclic group on three elements, then
   a) k is totally real,
   b) the discriminant of k is a perfect square in $\mathbb{Q}$.

Explanation to the first two problems: since k is a real quadratic extension of $\mathbb{Q}$, it is $\mathbb{Q}(\sqrt{d})$ for some $d > 1$ square-free, i.e.
$$k = \{a + b\sqrt{d} : a, b \in \mathbb{Q}\}.$$
Then k embeds into $\mathbb{R}^2$ via
$$k \ni a + b\sqrt{d} \mapsto (a + b\sqrt{d}, a - b\sqrt{d}) \in \mathbb{R}^2.$$
Under this embedding, $\mathfrak{o}$ is a lattice in $\mathbb{R}^2$ (a discrete additive subgroup of $\mathbb{R}^2$ generated by two elements). By a $\mathbb{Z}$-basis of $\mathfrak{o}$, we understand a two-element generating system of the lattice as an additive group.

Example: when $k = \mathbb{Q}(\sqrt{2})$, $\mathfrak{o} = \mathbb{Z} + \mathbb{Z}\sqrt{2}$ (warning: it is not always this much simple!), and then $1 \mapsto (1, 1)$, $\sqrt{2} \mapsto (\sqrt{2}, -\sqrt{2})$ form a $\mathbb{Z}$-basis of $\mathfrak{o}$.