D-MATH
Prof. Richard Pink

Algebraic Number Theory

FS 2018

Exercise Sheet 4

Lattices, Units

1. Suppose that the equation $y^2 = x^5 - 2$ has a solution with $x, y \in \mathbb{Z}$.
   (a) Write down the ring of integers and the class number of $K := \mathbb{Q}(\sqrt{-2})$.
   (b) Show that y is odd and that the two ideals $(y \pm \sqrt{-2})$ of $\mathcal{O}_K$ are coprime.
   (c) Prove that $y + \sqrt{-2}$ is a 5-th power in $\mathcal{O}_K$.
   (d) Deduce a contradiction, proving that the equation has no integer solution.

2. (a) A *cone* in a real vector space is a subset that is invariant under multiplication by $\mathbb{R}^{>0}$. Let C be a non-empty open convex cone in a finite dimensional real vector space V. Prove that for any complete lattice $\Gamma \subset V$ there exists a point in $\Gamma \cap C$.
   (b) Let K be a totally real number field, i.e., one with $\Sigma := \mathrm{Hom}(K, \mathbb{C}) = \mathrm{Hom}(K, \mathbb{R})$. Let T be any nonempty proper subset of Σ. Show that there exists a unit $\varepsilon \in \mathcal{O}_K^\times$ such that $\sigma(\varepsilon) > 1$ for all $\sigma \in T$ and $0 < \sigma(\varepsilon) < 1$ for all $\sigma \in \Sigma \smallsetminus T$.

*3. (a) Let M be a bounded subset of a finite dimensional real vector space V. Construct another bounded subset $N \subset V$ such that for any complete lattice $\Gamma \subset V$ with $V = \Gamma + M$, the subset $\Gamma \cap N$ generates Γ.
   (b) Deduce that, in principle, for every number field K one can effectively find generators of $\mathcal{O}_K^\times$.

4. (a) For any number field K, any subring $\mathcal{O} \subset \mathcal{O}_K$ of finite index is called an *order in* $\mathcal{O}_K$. For any such order prove that $\mathcal{O}^\times$ is a subgroup of finite index in $\mathcal{O}_K^\times$.
   (b) Consider a squarefree integer $d > 1$ with $d \equiv 1 \bmod (4)$, so that $K := \mathbb{Q}(\sqrt{d})$ has the ring of integers $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$. Explain the precise relation between $\mathbb{Z}[\sqrt{d}]^\times$ and $\mathcal{O}_K^\times$.

5. Show that the equation $a^2 - b^2 d = -1$ has infinitely many solutions $(a, b) \in \mathbb{Z}^2$ for $d = 2$, but none for $d = 3$. Explain the answer with algebraic number theory.