Math 288X: Algorithms in Algebra and Number Theory

Fall 2021

Problem set #10

Problem 1. Let $t \in \mathbb{Z}$ be not a square and consider the number field $K = \mathbb{Q}(\sqrt{t})$. For any prime number p, compute the radical $J_p(\mathbb{Z}[\sqrt{t}])$ and the order $T_p(\mathbb{Z}[\sqrt{t}])$ defined in class.

Problem 2 (Dedekind criterion)**.** Let $f \in \mathbb{Z}[X]$ be a monic irreducible polynomial of degree n, let $\alpha \in \mathbb{C}$ be a root of f and $K = \mathbb{Q}(\alpha)$. Let $f(X) \equiv g_1(X)^{e_1} \cdots g_t(X)^{e_t} \mod p$ be the factorization of f modulo p, with monic polynomials $g_1, \ldots, g_t \in \mathbb{Z}[X]$.

a) Show that the ideal $J_p(\mathbb{Z}[\alpha])$ of $\mathbb{Z}[\alpha]$ is generated by p and $g_1(\alpha) \cdots g_t(\alpha)$.

b) Consider the polynomial

$$h(X) = \frac{1}{p}(g_1(X)^{e_1} \cdots g_t(X)^{e_t} - f(X)) \in \mathbb{Z}[X].$$

Show that $\mathbb{Z}[\alpha]$ is p-maximal if and only if no polynomial $g_i(X)$ with $e_i \geqslant 2$ divides $h(X)$ modulo p.
Hint: Let $w_i(X) = g_1(X)^{e_1} \cdots g_t(X)^{e_t}/g_i(X)$. When does $\frac{1}{p}w_i(\alpha)$ lie in $T_p(\mathbb{Z}[\alpha])$?

Problem 3. a) Let M be an $n \times m$-matrix with integer entries. Show that you can compute the Hermite normal form of M in polynomial time (in the total number of digits of the entries of M).
Hint: If the columns of M are linearly independent, work modulo the determinant of an invertible $m \times m$-minor.

b) Let M be an $n \times n$-matrix with integer entries and nonzero determinant. Show that your can compute the Smith normal form of M in polynomial time.
Hint: Work modulo the determinant of M, if it is nonzero.

Problem 4. For a lattice $\Lambda \subseteq \mathbb{R}^n$ of rank n, the *dual lattice* is the set $\widehat{\Lambda}$ of $w \in \mathbb{R}^n$ such that $v \cdot w \in \mathbb{Z}$ for all $v \in \Lambda$.

a) Show that $\widehat{\Lambda}$ is a lattice of rank n.

b) Show that $\widehat{\widehat{\Lambda}} = \Lambda$.

c) Show that $\widehat{\Lambda_1 \cap \Lambda_2} = \widehat{\Lambda_1} + \widehat{\Lambda_2}$ for any lattices $\Lambda_1, \Lambda_2 \subseteq \mathbb{R}^n$ of rank n.

d) Given a basis of a lattice $\Lambda \subseteq \mathbb{Q}^n$ of rank n, show that you can compute a basis of $\widehat{\Lambda} \subseteq \mathbb{Q}^n$ in polynomial time.

e) Explain how to efficiently compute the inverse of a fractional ideal of a number field.