Problem Set 6

Norm and co-norm (continued)

1) Deduce from exercise 6) of PS 5 the following:
   a) \( \mathcal{L}_{L|K} \) and \( \mathcal{N}_{L|K} \) map principal divisors to principal divisors, thus they define canonically a co-norm and a norm for the ideal class groups:
   \[
   \mathcal{L}_{L|K} : \mathfrak{C}(R) \to \mathfrak{C}(S), \quad \mathcal{N}_{L|K} : \mathfrak{C}(S) \to \mathfrak{C}(R).
   \]
   b) Prove or disprove: \( \mathcal{L}_{L|K} \) is always injective. \( \mathcal{N}_{L|K} \) is always surjective.
   c) Show that \( \ker(\mathcal{N}_{L|K}) \) is contained in the group of \( n \)-torsion elements, where \( n = [L : K] \). What is the kernel of \( \mathcal{N}_{L|K} \circ \mathcal{L}_{L|K} \)?

Quadratic residues

2) Let \( p \) be an odd prime number, \( \zeta \) a primitive root of unity. Let \( S = \sum_{m=1}^{p-1} \left( \frac{m}{p} \right) \zeta^m \) be the Gauß sum attached to the Legendre symbol. Show that \( S^2 = (\frac{-1}{p})p \). In particular, if \( p^* = (\frac{-1}{p})p \), then \( \sqrt{p^*} \in \mathbb{Z}[\mu_p] \).

3) One defines the Jacobi symbol as follows: Let \( m = p_0 p_1 \ldots p_r \) and \( n = q_1 \ldots q_s \) be integers such that \( p_k \) is \( \pm 1 \) and \( q_j \) are prime numbers, \( n \) being odd. Suppose that \( m \) and \( n \) are relatively prime. Define the Jacobi symbol by \( \left( \frac{m}{n} \right)' = \prod_{i=1}^{r} \left( \frac{m}{q_i} \right) \), where \( \left( \frac{m}{q_i} \right) \) is the usual Legendre symbol. Prove the following:
   a) If \( m_1 \equiv m_2 \pmod{n} \), then \( \left( \frac{m_1}{n} \right)' = \left( \frac{m_2}{n} \right)' \).
   b) \( \left( \frac{n}{m} \right)' \) is multiplicative in both variables \( m \) and \( n \).
   c) One has \( \left( \frac{n}{m} \right)' = (-1)^{(n-1)/2} \). Prove or disprove: \( \left( \frac{2}{n} \right)' = (-1)^{(n^2 - 1)/8} \).
   d) If \( m \) is odd too, then \( \left( \frac{m}{n} \right)' = \left( \frac{m}{n} \right)' (-1)^{(m-1)/2} (-1)^{(n-1)/2} \).
   e) Prove or disprove: \( m \pmod{n} \) is a square in \( \mathbb{Z}/n \) iff \( \left( \frac{m}{n} \right)' = 1 \).

4) Using the properties of the Jacobi symbol try to estimate the number of multiplications needed for checking whether \( x \pmod{p} \) is a square in \( \mathbb{F}_p \). How does this compare with making a list of all the squares in \( \mathbb{F}_p \)?

Different/discriminant/ramification

5) In the usual context \( R, K, L|K, \) and \( S, \) with \( L|K \) finite separable, try to prove the following: A prime \( q \in \mathcal{X}_p \) is ramified in \( S|R \) iff \( q \) divides the different \( \mathfrak{D}_{S|R} \).

Hint: Have none...

6) For every positive bound \( c > 0 \), let \( K_c \) be the set of all the isomorphism types of number fields \( K|\mathbb{Q} \) such that \( |\delta_K| \leq c \). Further, for a given algebraic number \( \alpha \), let \( K^\alpha = \{ K \in K_c \mid \alpha \in K \} \), and finally \( K^\alpha_{\mathbb{Z}_{al}} = \{ K \in K^\alpha \mid K|\mathbb{Q} \text{ Galois extension} \} \).
   a) Prove or disprove: \( K_c \) is finite for all \( c > 0 \) iff \( K^\alpha \) is finite for all \( c > 0 \).
   b) The same question for \( K^\alpha \) versus \( K^\alpha_{\mathbb{Z}_{al}} \).

Hint: For \( K \in K_c \) and \( L = K[\alpha] \), find estimates for \( [L : \mathbb{Q}] \) and \( |\delta_L| \) in terms of \( c \) and \( \alpha \), etc.

Minkowski’s Method

7) Let \( V \) be a real finite dimensional vector space. For points \( P, Q \in V \) we denote by \([P, Q]\) the segment defined by \( P \) and \( Q \). Show the following:
   a) \( X \subset V \) is convex iff \( \forall P, Q \in X \) it holds: \( \frac{1}{2}(P + Q) \in X \) and \([P, Q] \cap X \) is a closed subset of \( V \).
   b) Using this show that the sets \( X \) and \( X_0 \) defined in the lecture are convex subsets of \( V^{r,s} \).
   c) Complete the proof of the assertions: \( \mu(X_\ast) = 2^r \pi^s \prod_i a_i \prod_j b_j^2 \), and \( \mu(X_0) = 2^r \left( \frac{2}{m} \right) \prod_i a_i \prod_j b_j^2 \).

8) Show that the quadratic fields with discriminants \(-11, -8, -7, -4, -3, 5, 8, 13\) are PID. Find the square free \( d \in \mathbb{Z} \) defining these quadratic fields.