Problem set 5 – Math 699 – Algebraic number theory

(1) In this exercise, you will determine the factorization of all primes in all quadratic extensions. Let $K = \mathbf{Q}(\sqrt{d})$ where $d \in \mathbf{Z}$ is squarefree. We saw that

$$\Delta(K) = \begin{cases} d & \text{if } d \equiv 1 \pmod 4 \\ 4d & \text{if } d \equiv 2, 3 \pmod 4. \end{cases}$$

Define the *Kronecker symbol* as an extension of the Legendre symbol: for $a, n \in \mathbf{Z}$, if $n = u \prod p_i^{e_i}$, where $u = \pm 1$, let

$$\left(\frac{a}{n}\right) = \left(\frac{a}{u}\right) \prod \left(\frac{a}{p_i}\right)^{e_i},$$

where

$$\left(\frac{a}{1}\right) = 1, \quad \left(\frac{a}{-1}\right) = \begin{cases} 1 & \text{if } a \geq 0, \\ -1 & \text{if } a < 0, \end{cases} \quad \left(\frac{a}{2}\right) = \begin{cases} 1 & \text{if } a \equiv \pm 1 \pmod 8, \\ -1 & \text{if } a \equiv \pm 3 \pmod 8, \\ 0 & \text{if } a \text{ is even}, \end{cases}$$

and $\left(\frac{a}{p}\right)$ is the Legendre symbol if p is an odd prime. Let $\left(\frac{a}{0}\right) = 0$, unless $a = \pm$, in which case it is 1. Note that for a, n non-zero, we can extend quadratic reciprocity to say that

$$\left(\frac{a}{n}\right) = \left(\frac{n}{a}\right), \text{ unless } a', n' \equiv 3 \pmod 4, \text{ in which case } \left(\frac{a}{n}\right) = -\left(\frac{n}{a}\right),$$

where m' is the odd part of m.

Prove that

$$\left(\frac{\Delta(K)}{p}\right) = \begin{cases} 1 & \text{if } p \text{ splits}, \\ -1 & \text{if } p \text{ is inert}, \\ 0 & \text{if } p \text{ ramifies}. \end{cases}$$

(2) Let $K = \mathbf{Q}(2^{1/3})$.

(a) Which primes ramify and what is their factorization? We'll show later that $\mathcal{O}_K$ is a PID. For now assume this and write the primes in the previous factorizations as principal ideals.

(b) For each of the unramified factorization types of K, find a rational prime p with that type and write down its factorization. Write the primes in the previous factorizations as principal ideals.

(3) (a) Let $K = \mathbf{Q}(\theta)$ and p a rational prime. Suppose the minimal polynomial of θ, denoted f_θ, is Eisenstein at p. Show that p is totally ramified in K.

(b) Let $K_n = \mathbf{Q}(\zeta_n)$, where $n = \ell^\nu$ is a prime power ($\nu \geq 1$). Show that ℓ is totally ramified in K_n. Show that the unique prime ideal dividing $\ell \mathcal{O}_{K_n}$ is generated by $\lambda := 1 - \zeta_n$.

(4) Let K be a number field and let $\mathcal{D}_K^{-1} := \{\alpha \in K : \mathrm{tr}_{K/\mathbf{Q}}(\alpha \mathcal{O}_K) \subseteq \mathbf{Z}\}$. Show that $\mathcal{D}_K^{-1}$ is a fractional ideal of K (it's called the *inverse different of* K). Let $\mathcal{D}_K$ be its inverse. Show that $\mathcal{D}_K$ is an integral ideal of $\mathcal{O}_K$ (it's called the *different of* K).

(5) Let $\mathcal{O}$ be a Dedekind domain and K its field of fractions. Some standard arithmetic operations on elements of a UFD can be ported over to the fractional ideals in $\mathcal{O}$. Let

$$I = \prod_{\mathfrak{p}} \mathfrak{p}^{a_\mathfrak{p}}$$

be the prime factorization of the fractional ideal I. Define the $\mathfrak{p}$*-adic valuation of* I to be $\mathrm{ord}_\mathfrak{p}(I) := a_\mathfrak{p}(I)$. For an element $\alpha \in K^\times$, define $\mathrm{ord}_\mathfrak{p}(\alpha) := \mathrm{ord}_\mathfrak{p}((\alpha))$. For two integral ideals I and J, define

$$\gcd(I, J) = \prod_{\mathfrak{p}} \mathfrak{p}^{\min(\mathrm{ord}_\mathfrak{p}(I), \mathrm{ord}_\mathfrak{p}(J))} \quad \text{and} \quad \mathrm{lcm}(I, J) = \prod_{\mathfrak{p}} \mathfrak{p}^{\max(\mathrm{ord}_\mathfrak{p}(I), \mathrm{ord}_\mathfrak{p}(J))}.$$

(a) Show that $\gcd(I, J) = I + J$ and $\mathrm{lcm}(I, J) = I \cap J$.

(b) We say that I *divides* J, $I \mid J$, if there is an integral ideal M such that $J = IM$. Show that $I \mid J$ if and only if $\mathrm{ord}_\mathfrak{p}(I) \leq \mathrm{ord}_\mathfrak{p}(J)$ for all $\mathfrak{p}$. Also, if and only if $I \supseteq J$.

(c) Let $\alpha \in K$ and let I be a fractional ideal. Show that $\alpha \in I$ if and only if $\mathrm{ord}_\mathfrak{p}(\alpha) \geq \mathrm{ord}_\mathfrak{p}(I)$ for all $\mathfrak{p}$.

(d) Show that $\mathrm{ord}_\mathfrak{p}$ behaves like an ultrametric valuation, i.e. for two fractional ideals

$$\mathrm{ord}_\mathfrak{p}(IJ) = \mathrm{ord}_\mathfrak{p}(I) + \mathrm{ord}_\mathfrak{p}(J) \quad \text{and} \quad \mathrm{ord}_\mathfrak{p}(I + J) = \min(\mathrm{ord}_\mathfrak{p}(I), \mathrm{ord}_\mathfrak{p}(J)).$$

For elements $\alpha, \beta \in K^\times$ such that $\alpha + \beta \neq 0$, show that $\mathrm{ord}_\mathfrak{p}(\alpha + \beta) \geq \min(\mathrm{ord}_\mathfrak{p}(\alpha), \mathrm{ord}_\mathfrak{p}(\beta))$. Give an example where the inequality is strict.

(e) Let I be a fractional ideal and $\alpha, \beta \in \mathcal{O}$. Say $\alpha \equiv \beta \pmod{I}$ if $I \mid (\alpha - \beta)$. Prove the Chinese Remainder Theorem: Let $I_1, \ldots, I_k$ be pairwise relatively prime integral ideals of $\mathcal{O}$ and let $\alpha_1, \ldots, \alpha_k \in \mathcal{O}$. Show that there is $\alpha \in \mathcal{O}$ such that $\alpha \equiv \alpha_i \pmod{I_i}$. Also show the natural map

$$\mathcal{O} \to \prod_{i=1}^{k} \mathcal{O}/I_i$$

yields an isomorphism

$$\mathcal{O} \Big/ \prod_{i=1}^{k} I_i \cong \prod_{i=1}^{k} \mathcal{O}/I_i.$$

(6) Let $\mathcal{O}$ be a Dedekind domain.

(a) Show that if $\mathcal{O}$ is a UFD, then it is a PID. (Hint: first show that it suffices to prove all prime ideals are principal.)

(b) Let $\mathfrak{p}$ be a non-zero prime ideal of $\mathcal{O}$ and let $r \in \mathbf{Z}$. Show that $\mathcal{O}/\mathfrak{p} \cong \mathfrak{p}^r/\mathfrak{p}^{r+1}$ as additive groups. (Hint: take $a \in \mathfrak{p}^r/\mathfrak{p}^{r+1}$ and study the map $x \mapsto ax$.)

(c) Show that every fractional ideal is generated by at most two elements. (Hint: for an integral ideal I of $\mathcal{O}$, find an element α of $\mathcal{O}$ whose valuation at all primes dividing I is the same as that of I (try CRT). Show that I is generated by α and any other non-zero element β of I).