Elliptic Functions and related topics

Problem sheet 10

Dr. L. Rolen, Dr. M. H. Mertens

Exercise 1. (4 points)
Let $R := \mathbb{Z}[i]$ denote the ring of Gaussian integers. For all rational primes p determine whether p is inert (i.e. p is a prime in R as well), split (i.e. p factors into two distinct primes in R, $p = \pi\pi'$), or ramified (i.e. $p = \varepsilon\pi^2$ for some prime π and some unit ε in R) in R.

Exercise 2. (4 points)
Let d be a square-free integer and let $K := \mathbb{Q}(\sqrt{d})$.

(a) Show that the ring of integers in K, which is defined as

$$\mathbb{Z}_K := \{\alpha \in K : \alpha \text{ is the root of a monic polynomial with integer coefficients}\}$$

is given by

$$\mathbb{Z}_K = \begin{cases} \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] & \text{if } d \equiv 1 \pmod 4 \\ \mathbb{Z}[d] & \text{if } d \equiv 2,3 \pmod 4). \end{cases}$$

(b) For $d < 0$, find generators of the group $\mathbb{Z}_K^*$.

Exercise 3. (4 points)
Let $\mathbb{Z}_K$ be the ring of integers in a number field K and $\mathfrak{a} \trianglelefteq \mathbb{Z}_K$ be an ideal of $\mathbb{Z}_K$. Then $\mathbb{Z}_K/\mathfrak{a}$ is a finite ring whose cardinality is called the *norm* of $\mathfrak{a}$, denoted by $N\mathfrak{a}$ (no proof required). Let $\psi : \mathbb{Z}_K/\mathfrak{a} \to \mathbb{C}^*$ be an additive charcter which is non-trivial on any subgroup $\mathfrak{b}/\mathfrak{a}$ of $\mathbb{Z}_K/\mathfrak{a}$, where $\mathfrak{b} \trianglelefteq \mathbb{Z}_K$ is an ideal properly containing $\mathfrak{a}$. Let $\chi : (\mathbb{Z}_k/\mathfrak{a}) \to \mathbb{C}^*$ be a multiplicative character and take $\chi(x) = 0$ whenever $x \in \mathbb{Z}_K/\mathfrak{a}$ is not comprime to $\mathfrak{a}$. Finally, define the generalized Gauß sum

$$g(\chi) = g(\chi, \psi) := \sum_{x \in \mathbb{Z}_K/\mathfrak{a}} \chi(x)\psi(x).$$

Show that $\sum_{x \in \mathbb{Z}_K/\mathfrak{a}} \chi(x)\psi(ax) = \overline{\chi}(a)g(\chi,\psi)$ for all $a \in (\mathbb{Z}_K/\mathfrak{a})^*$.

Exercise 4. (4 points)
Assume the notation and definitions in Exercise 3. We call a multiplicative character χ *primitive* modulo $\mathfrak{a}$, if χ is non-trivial on any subgroup of $\mathbb{Z}_K/\mathfrak{a}$ consisting of elements which are congruent to 1 mod $\mathfrak{b}$ ($\mathfrak{b}$ as above). For this exercise, let χ be primitive modulo $\mathfrak{a}$.

(a) Show that, the formula in Exercise 3 (a) holds for all $a \in \mathbb{Z}_K/\mathfrak{a}$.

(b) Prove that $g(\chi,\psi)g(\overline{\chi},\psi) = \chi(-1)N\mathfrak{a}$ and $|g(\chi,\psi)| = \sqrt{N\mathfrak{a}}$.

Deadline: Tuesday, Dec. 16, 2014 at the beginning of the lecture.