Shimura Varieties: Problem sheet 2

15 October 2014

1. **Computing class groups of quadratic fields**

   Let K be a number field.

   We define the **norm** of an ideal $\mathfrak{a} \subset \mathfrak{o}_K$ to be the cardinality of the quotient ring $\mathfrak{o}_K/\mathfrak{a}$. If $\mathfrak{p}$ is a prime ideal in $\mathfrak{a}$, then $\mathrm{Nm}(\mathfrak{p}) = p^r$ for some rational prime p and positive integer r, and $\mathfrak{p}$ divides the ideal (p) in $\mathfrak{o}_K$.

   The **discriminant** d_K is the square of the determinant of the matrix $(\sigma_i(\alpha_j))_{1\leq i,j\leq n}$ where $\{\sigma_1, \ldots, \sigma_n\}$ is the set of embeddings $K \to \mathbb{C}$ and $\{\alpha_1, \ldots, \alpha_n\}$ is a basis for $\mathfrak{o}_K$ as a $\mathbb{Z}$-module.

   Theorem (Minkowski)**.** *The class group of $\mathfrak{o}_K$ is generated by ideals of norm at most*
   $$\frac{n!}{n^n}\Big(\frac{4}{\pi}\Big)^s\sqrt{|d_K|},$$
   where s is the number of complex-conjugate pairs of embeddings $K \to \mathbb{C}$ whose images are not contained in $\mathbb{R}$. (Thus $s = 1$ for an imaginary quadratic field and $s = 0$ for a real quadratic field.)

   Theorem (Dedekind)**.** *Suppose that $\mathfrak{o}_K = \mathbb{Z}[\alpha]$, and let $f(X)$ be the minimal polynomial of α. (Not all number fields contain an α such that $\mathfrak{o}_K = \mathbb{Z}[\alpha]$; there is a slightly more complicated version of the theorem without this condition.)*

   Let p be a rational prime. Let the factorisation of $f(X) \pmod p$ into irreducibles in $\mathbb{F}_p[X]$ be
   $$\bar{f}_1(X)^{e_1}\cdots\bar{f}_r(X)^{e_r},$$
   and choose monic polynomials $f_1(X), \ldots, f_r(X) \in \mathbb{Z}[X]$ which reduce to $\bar{f}_1, \ldots, \bar{f}_r$ mod p. Then the ideals
   $$\mathfrak{p}_j = (p, f_j(\alpha))$$
   are distinct prime ideals in $\mathfrak{o}_K$ and the prime factorisation of (p) in $\mathfrak{o}_K$ is
   $$(p) = \mathfrak{p}_1^{e_1}\cdots\mathfrak{p}_r^{e_r}.$$

   We can thus obtain a set of generators for the class group of $\mathfrak{o}_K$ by looking at each rational prime up to the Minkowski bound and using Dedekind's theorem to factorise these into prime ideals of $\mathfrak{o}_K$. To fully compute the class group, we then have to determine which combinations of these generating ideals are principal.

   Let D be a square-free integer not divisible by 4 and not equal to 1 (D may be positive or negative). We will look at the field $\mathbb{Q}(\sqrt{D})$.

   You will need the following fact:

Lemma. *If $\mathfrak{a} = (a + b\sqrt{D})$ is a principal ideal in $\mathfrak{o}_K$, where $K = \mathbb{Q}(\sqrt{D})$ and $a, b \in \mathbb{Q}$, then*

$$\mathrm{Nm}(\mathfrak{a}) = \left|a^2 - Db^2\right|.$$

(a) (Optional preliminary) Show that:

i. If $D \equiv 1 \mod 4$, then the ring of integers of $\mathbb{Q}(\sqrt{D})$ is $\mathbb{Z}[\frac{1}{2}(1+\sqrt{D})]$, the minimum polynomial of $\frac{1}{2}(1+\sqrt{D})$ is $X^2 - X + \frac{1}{4}(1-D)$ and the discriminant of $\mathbb{Q}(\sqrt{D})$ is D.

ii. If $D \equiv 2$ or $3 \mod 4$, then the ring of integers of $\mathbb{Q}(\sqrt{D})$ is $\mathbb{Z}[\sqrt{D}]$, the minimum polynomial of $\sqrt{D}$ is $X^2 - D$ and the discriminant of $\mathbb{Q}(\sqrt{D})$ is $4D$.

(b) Read off from Minkowski's theorem that $\mathbb{Q}(\sqrt{D})$ has class number 1 if $D = 2, 3, 5, 13, -1, -2, -3$ or -7.

(c) Use Minkowski's and Dedekind's theorems to show that $\mathbb{Q}(\sqrt{D})$ has class number 1 if $D = 17, 21, 29, 33, -11$ or -19.

(d) Show that the class group of $\mathbb{Q}(\sqrt{6})$ is generated by the ideal $\mathfrak{a} = (2, 1+\sqrt{6})$, which has norm 2.

Find an integer solution to the equation $a^2 - 6b^2 = -2$, and deduce that $\mathfrak{a}$ is principal. Hence $\mathbb{Q}(\sqrt{6})$ has class number 1.

(e) Show that the class group of $\mathbb{Q}(\sqrt{-5})$ is generated by the ideal $\mathfrak{a} = (2, 1+\sqrt{-5})$, and that $\mathfrak{a}^2 = (2)$ is principal.

Show that there are no integer solutions to $a^2 + 5b^2 = \pm 2$ and deduce that $\mathbb{Q}(\sqrt{-5})$ has class number 2.

(f) Show that the class group of $\mathbb{Q}(\sqrt{-6})$ is generated by the ideals $\mathfrak{a} = (2, \sqrt{6})$ and $\mathfrak{b} = (3, \sqrt{6})$ and that $\mathfrak{a}^2$ and $\mathfrak{b}^2$ are each principal.

Show that $\mathfrak{a}$ and $\mathfrak{b}$ are not principal, but that $\mathfrak{a}\mathfrak{b} = (\sqrt{-6})$ is principal. Conclude that $\mathbb{Q}(\sqrt{-6})$ has class number 2.

(g) Show that the class group of $\mathbb{Q}(\sqrt{-31})$ is generated by the ideals $\mathfrak{a} = (2, \alpha)$ and $\mathfrak{b} = (2, 1+\alpha)$ where $\alpha = \frac{1}{2}(1+\sqrt{-31})$, with $\mathfrak{a}\mathfrak{b} = (2)$.

Show that the only principal ideal in $\mathbb{Z}[\alpha]$ with norm ± 4 is (2). (Remember that $\mathbb{Z}[\alpha]$ is bigger than $\mathbb{Z} + \mathbb{Z}\sqrt{-31}$.)

Since $\mathfrak{a}^2 \neq (2)$, conclude that $\mathfrak{a}$ has order 3 in the class group and hence that the class number of $\mathbb{Q}(\sqrt{-31})$ is 3.

(h) Determine the class numbers of $\mathbb{Q}(\sqrt{10})$, $\mathbb{Q}(\sqrt{14})$ and $\mathbb{Q}(\sqrt{15})$. (For $\mathbb{Q}(\sqrt{15})$, find a principal ideal of norm 6 in order to copy the method of (f).)

(i) Show that the class number of $\mathbb{Q}(\sqrt{-23})$ is 3.

(j) Let p be a prime $\equiv 11 \mod 12$. If $p > 3^n$, show that the class group of $\mathbb{Q}(\sqrt{-p})$ contains an element of order greater than n.