Number Fields: Example Sheet 3

(1) Let $D > 1$ be a square-free integer and put $K = \mathbb{Q}(\sqrt{D})$. Recall that *the* fundamental unit of K is an element $\varepsilon_0 \in \mathcal{O}_K^*$ such that $\varepsilon_0 = \min\{\varepsilon \in \mathcal{O}_K^* \mid \varepsilon > 1\}$. Use the algorithm explained in the lectures to determine the fundamental unit of K for $D = 13, 17, 26, 29, 35, 37, 53$ and 77.

(2) Let $m \geq 1$ and $D_1, \ldots, D_m$ be pairwise co-prime integers, $D_i \notin \{0, 1\}$ for all i. Put $K = \mathbb{Q}(\sqrt{D_1}, \ldots, \sqrt{D_m})$. Show by induction over m that $[K : \mathbb{Q}] = 2^m$.

(3) For a number field K let as usual r and s denote the number of real and half the number of complex embeddings, respectively. Determine r and s in the following cases:

(a) $K = \mathbb{Q}(\sqrt{D_1}, \ldots, \sqrt{D_m})$ as in the preceding exercise.

(b) $K = \mathbb{Q}(\sqrt[m]{D})$, where $D > 1$ is a square-free integer and $m \geq 2$.

(4) Let K be a number field. Recall that a prime number p is called *ramified* in K if in the prime ideal decomposition $[p] = p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$ at least one of the exponents e_i is > 1. Now let $K = \mathbb{Q}(\sqrt{D})$ for some square-free integer $D \notin \{0, 1\}$. On a previous example sheet we have seen that $\mathcal{O}_K = \mathbb{Z}[\theta]$ for some $\theta \in \mathcal{O}_K$. Use the explicit description of θ and Dedekind's theorem to give a direct proof that the primes which ramify in K are the prime divisors of the discriminant of K.

(5) Let $K = \mathbb{Q}(\sqrt{26})$ and let $\varepsilon = 5 + \sqrt{26}$. Use Dedekind's theorem to show that the ideal equations

$$[2] = [2, \varepsilon + 1]^2\,,\ [5] = [5, \varepsilon + 1][5, \varepsilon - 1]\,,\ [\varepsilon + 1] = [2, \varepsilon + 1][5, \varepsilon + 1]$$

hold in K. Deduce that K has class number two. (Argue with the Minkowski constant.)

ε is the fundamental unit of K, by a preceding exercise. Use this fact to show that all solutions in integers x, y of the equation $x^2 - 26y^2 = \pm 10$ are given by

$$x + \sqrt{26}y = \pm\varepsilon^n(\varepsilon \pm 1)\,,\ n = 0, \pm 1, \pm 2, \ldots$$

(6) Show that $\varepsilon = \frac{3+\sqrt{7}}{3-\sqrt{7}}$ is a unit in $K = \mathbb{Q}(\sqrt{7})$. Show further that $[2]$ is the square of the principal ideal in $\mathcal{O}_K$ generated by $3 + \sqrt{7}$. Use the Minkowski constant to show that K has class number one.

Assuming further that ε is the fundamental unit in K, show that all solutions in integers x, y of the equation $x^2 - 7y^2 = 2$ are given by

$$x + \sqrt{26}y = \pm\varepsilon^n(3 + \sqrt{7})\,,\ n = 0, \pm 1, \pm 2, \ldots$$

(7) Let $K = \mathbb{Q}(\sqrt{35})$. By Dedekind's theorem, or otherwise, show that the ideal equations

$$[2] = [2, \omega]^2\,,\ [5] = [5, \omega]^2\,,\ [\omega] = [2, \omega][5, \omega]$$

hold in K, where $\omega = 5 + \sqrt{35}$. Deduce that K has class number two. (Argue with the Minkowski constant.)

$\omega + 1$ is the fundamental unit of K, by a preceding exercise. Hence show that all solutions in integers x, y of the equation $x^2 - 35y^2 = -10$ are given by

$$x + \sqrt{35}y = \pm\omega(\omega + 1)^n\,,\ n = 0, \pm 1, \pm 2, \ldots$$

Calculate the particular solution x, y for $n = 1$.

(8) Let $K = \mathbb{Q}(\sqrt{-34})$. By Dedekind's theorem, or otherwise, factorise 2, 3, 5 and 7 into prime ideals in $\mathcal{O}_K$. Show that the ideal equations

$$[\omega] = [5, \omega][7, \omega]\,, \;\; [\omega + 3] = [2, \omega + 3][5, \omega + 3]^2$$

hold in K, where $\omega = 1 + \sqrt{-34}$. Deduce that the class group of K is cyclic of order four. (Argue with the Minkowski constant.)

(9) By exercises (6) and (7) of example sheet 2, we know the class groups of the imaginary quadratic fields $\mathbb{Q}(\sqrt{-5})$ and $\mathbb{Q}(\sqrt{-11})$. Use this information to find all solutions in integers of the diophantine equations

$$y^2 + 5 = x^3\,, \qquad y^2 + 11 = x^3\,.$$

(10) Let K be a number field of degree $n = r + 2s$. Denote by $\rho_1, \ldots, \rho_r$ the real embeddings of K and by $\sigma_1, \bar{\sigma}_1, \ldots, \sigma_s, \bar{\sigma}_s$ the complex embeddings of K into $\mathbb{C}$. Recall the map λ as introduced in the lectures

$$\lambda : \mathcal{O}_K^* \longrightarrow \mathbb{R}^{r+s}\,, \;\; \alpha \mapsto (\log(|\tau_1(\alpha)|, \ldots, \log(|\tau_r(\alpha)|), \log(|\sigma_1(\alpha)|^2), \ldots, \log(|\sigma_s(\alpha)|^2))\,.$$

The image of λ is a complete lattice in the hyperplane

$$H = \{(x_1, \ldots, x_r, \xi_1, \ldots, \xi_s) \in \mathbb{R}^{r+s} \mid \sum_{i=1}^{r} x_i + \sum_{j=1}^{s} \xi_j = 0\}\,.$$

We consider $\mathbb{R}^{r+s}$ with its standard scalar product and restrict it to H, thereby getting a well-defined notion of volume on H. Show that the volume of a fundamental mesh of the lattice $\Gamma = \lambda(\mathcal{O}_K^*)$ is equal to $\sqrt{r+s}R_K$ where R_K is the absolute value of the determinant of an arbitrary minor of rank $t = r + s - 1$ of the following matrix

$$\begin{pmatrix} \lambda_1(\varepsilon_1) & \cdots & \lambda_1(\varepsilon_t) \\ \vdots & & \vdots \\ \lambda_{t+1}(\varepsilon_1) & \cdots & \lambda_{t+1}(\varepsilon_t) \end{pmatrix}$$

Here $\varepsilon_1, \ldots, \varepsilon_t$ is a system of fundamental units and $(\lambda_1(\varepsilon_i), \ldots, \lambda_{t+1}(\varepsilon_i))^t = \lambda(\varepsilon_i)$, in the standard coordinates on $\mathbb{R}^{r+s}$. R_K is called the *regulator* of K. (Hint: The column vector $\lambda_0 = \frac{1}{\sqrt{r+s}}(1, \ldots, 1)^t$ is perpendicular to H and of length one; the volume of a fundamental mesh of Γ is thus given by the absolute value of the determinant of the matrix $(\lambda_0\, \lambda(\varepsilon_1) \cdots \lambda(\varepsilon_t))$. Then add all rows to a fixed one.)

(11) Let $K \subset L$ be number fields and $L = K(\theta)$ for some $\theta \in \mathcal{O}_L$. Let $f(X) \in \mathcal{O}_K[x]$ be the minimal polynomial of θ over K, and put $\mathfrak{c} = \{\alpha \in \mathcal{O}_L \mid \alpha \cdot \mathcal{O}_L \subset \mathcal{O}_K[\theta]\}$. This is a non-zero ideal of $\mathcal{O}_L$. Generalise Dedekind's theorem as follows: if the prime ideal $\mathfrak{p} \subset \mathcal{O}_K$ is co-prime to $\mathfrak{c}$ (i.e. $\mathfrak{p}\mathcal{O}_L + \mathfrak{c} = \mathcal{O}_L$), and $\bar{f}(x) = \bar{f}_1(x)^{e_1} \cdots \bar{f}_r(x)^{e_r}$ is the decomposition of $\bar{f}(x) = f(x) \mod \mathfrak{p}$ in $(\mathcal{O}_K/\mathfrak{p})[x]$ into irreducible monic polynomials, then $\mathfrak{P}_1 = [f_1(\theta), \mathfrak{p}], \ldots, \mathfrak{P}_r = [f_r(\theta), \mathfrak{p}]$ are the r different prime ideals of $\mathcal{O}_L$ containing $\mathfrak{p}\mathcal{O}_L$ and $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$. (Here $f_i(x) \in \mathcal{O}_K[x]$ is a monic polynomial whose reduction modulo $\mathfrak{p}$ is $\bar{f}_i$.)

(12) Let $K = \mathbb{Q}(\sqrt{D_1}, \ldots, \sqrt{D_m})$ with $D_1, \ldots, D_m$ be pairwise co-prime integers, $D_i \notin \{0, 1\}$ for all i. Use the assertion of the preceding exercise that, up to at most finitely many exceptions, a prime number p *splits completely* in $\mathcal{O}_K$, i.e. $[p] = \mathfrak{p}_1 \cdots \mathfrak{p}_n$ with $n = 2^m$ and pairwise different prime ideals $\mathfrak{p}_i$, if and only if all the congruences $X_1^2 \equiv D_1, \ldots, X_m^2 \equiv D_m$ have a solution modulo p.

(13) Use the preceding exercise and the quadratic reciprocity law to show that, up to at most finitely many exceptions, a prime p splits completely in $\mathbb{Q}(i, \sqrt{3})$ if and only if $p \equiv 1$ modulo 12.

Comments, corrections and queries can be send to me at M.Strauch@dpmms.cam.ac.uk