NUMBER FIELDS, EXX. SHEET 3

N. I. SHEPHERD-BARRON

(1) Suppose that K is a number field. Define the *inverse different* $\mathcal{D}_K^{-1}$ by

$$\mathcal{D}_K^{-1} = \{x \in K : \mathrm{Tr}(xy) \in \mathbb{Z}\ \forall y \in \mathcal{O}_K\}.$$

(i) Show that $\mathcal{D}_K^{-1}$ is a fractional ideal of K.

The *different* $\mathcal{D}_K$ is defined as the inverse of $\mathcal{D}_K^{-1}$, $\mathcal{D}_K = (\mathcal{D}_K^{-1})^{-1}$.

(ii) Show that $\mathcal{D}_K$ is an integral ideal of $\mathcal{O}_K$.

(iii) Show that $N_{K/\mathbb{Q}}(\mathcal{D}_K) = |d_K|$, where d_K is the discriminant of K.

(iv) Assume that $\mathcal{O}_K = \mathbb{Z}[x]$ for some x, and that $f \in \mathbb{Z}[X]$ is the minimal polynomial of x. Suppose that $x = x_1, ..., x_n$ are the conjuigates of x. Show that

$$\frac{1}{f(T)} = \sum_1^n \frac{1}{f'(x_i)(T - x_i)}.$$

(v) Deduce that $\mathrm{Tr}_{K/\mathbb{Q}}(\frac{x^r}{f'(x)}) = 0$ if $0 \le r < n-1$ and $= 1$ if $r = n-1$.

(vi) Deduce that $\mathcal{D}_K = (f'(x))$.

(2) (i) Suppose that $m > 0$ is even and square-free. Show that, if the class number of $\mathbb{Q}(\sqrt{-m})$ is prime to 3, then the equation $y^3 = x^2 + m$ has at most two solutions in integers.

(ii) Compute the class group of $\mathbb{Q}(\sqrt{-47})$.

(iii) Find all integer solutions to $4y^3 = x^2 + 1175$.

(3) Suppose that $m > 0$ is the product of k distinct primes p_i and that $K = \mathbb{Q}(\sqrt{-m})$. Show that $(p_i) = P_i^2$ for a prime ideal P_i of $\mathcal{O}_K$, and determine when two ideals $\prod_1^k P_i^{r_i}$, $\prod_1^k P_i^{s_i}$ are in the same class. Deduce that the class number h_K is divisible by 2^{k-1}.

(4*) (i) Suppose that I is an integral ideal in a ring of integers $\mathcal{O}_K$ and that $N(I) = p_1...p_k = N$, the product of k primes (not necessarily distinct). Show that I is the product of at most k prime ideals (not necessarily distinct).

(ii) Find an upper bound, in terms of N and the degree $[K : \mathbb{Q}]$, for the number of integral ideals of norm N in $\mathcal{O}_K$.

(5*) Compute the class groups of $\mathbb{Q}(\sqrt{-6})$ and $\mathbb{Q}(\sqrt{6})$.

(6) Suppose that p, q are distinct odd primes such that p is a square modulo q and q is a square modulo p. Show that $x^2 - py^2 - qz^2 = 0$ has a non-trivial solution in integers.

[The natural way to do this is via the Hasse principle, which is a theorem to the effect that a quadratic form over a number field K has a non-trivial zero if

and only if it has one over every completion of K. It's worth learning about completions, local fields and the Hasse principle (e.g., Serre, A Course in Arithmetic, ch. IV).]
(i) Show that at least one of p, q is congruent to 1 mod 4 and that there are integers u, v with

$$u^2 \equiv p \pmod{4q},\ u \equiv 0 \pmod{p},\ v^2 \equiv q \pmod{p},\ v \equiv 0 \pmod{q}.$$

(ii) Define

$$\Lambda = \{(x, y, z) \in \mathbb{Z}^3 : z \equiv 0 \pmod{2}, x \equiv uy + vz \pmod{2pq}\}.$$

Show that Λ is a lattice in $\mathbb{R}^3$ and that if $(x, y, z) \in \Lambda$, then $x^2 - py^2 - qz^2 \equiv 0 \pmod{4pq}$.
(iii) Now use the ellipsoid $X = \{(x, y, z) \in \mathbb{R}^3 : x^2 + py^2 + qz^2 < 4pq\}$ show that $x^2 - py^2 - qz^2 = 0$ has a non-trivial solution in integers.

[Hint: The covolume of Λ and the volume of X will be useful. Further hint: the right answers are $4pq$ and $32\pi pq/3$. And the phrase "Minkowski's convex bodies theorem" is helpful.]

References

E-mail address: `nisb@dpmms.cam.ac.uk`

Version: 1, Date: Mar 9, 2010