Algebraic number theory

Problems sheet 4

March 11, 2011

Notation. Let K be a number field of degree n with the ring of integers $\mathcal{O}_K$. Recall that the discriminant D of K is the determinant of the matrix with entries $\mathrm{Tr}_K(\alpha_i\alpha_j)$, where $\alpha_1, \ldots, \alpha_n$ is a basis of $\mathcal{O}_K$ over $\mathbb{Z}$. From lectures we know that there are exactly n distinct injective field homomorphisms

$$\sigma_i : K \hookrightarrow \mathbb{C}, \quad i = 1, \ldots, n.$$

We order them in such a way that the first s embeddings $\sigma_1, \ldots, \sigma_s$ map K into $\mathbb{R}$, and the rest are such that $\sigma_i(K) \not\subset \mathbb{R}$. These remaining $n - s$ embeddings come in pairs of complex conjugate embeddings, in particular $n = s + 2t$ and we order them so that $\sigma_{s+t+i} = \overline{\sigma}_{s+i}$ for $i = 1, \ldots, t$.

1. (a) Find the norms of these ideals in $\mathcal{O}_K$:
$m\mathcal{O}_K$, where $m \in \mathbb{Z}$;
$(2, 1 + \sqrt{-5})$, where $K = \mathbb{Q}(\sqrt{-5})$;
$(2, \frac{1}{2}(1 + \sqrt{-7}))$, where $K = \mathbb{Q}(\sqrt{-7})$;
$(22, 2 + \sqrt{-7})$, where $K = \mathbb{Q}(\sqrt{-7})$;
$(22, 3 + \sqrt{-7})$, where $K = \mathbb{Q}(\sqrt{-7})$.
(b) Find the inverses of the ideals from part (a).
(c) Write the last four ideals in part (a) as products of primes ideals.
(d) Write the fractional ideal $\frac{1}{5}(6 + 7\sqrt{-1}) \subset \mathbb{Q}(\sqrt{-1})$ as a product of integral powers of prime ideals.

2. In lectures we proved that $D = \det(\Sigma)^2$, where Σ is the $n \times n$-matrix with complex entries $\sigma_i(\alpha_j)$. Using this fact prove that the sign of D is $(-1)^t$.

3. Let $f(t) = t^3 + t + 1$. Imitate the argument in lectures to prove that if $K = \mathbb{Q}(\alpha) = \mathbb{Q}[t]/(f(t))$, then $\mathcal{O}_K = \mathbb{Z} \oplus \mathbb{Z}\alpha \oplus \mathbb{Z}\alpha^2$. Find the discriminant of K. (Use the Gauss lemma to prove that $f(t)$ is irreducible

over $\mathbb{Q}$. In lectures we showed that the square of the determinant of the matrix with entries $\sigma_i(\alpha^j)$ equals the discriminant of $f(t)$. Use the fact that the discriminant of $t^3 + at + b$ is $-4a^3 - 27b^2$. Conclude by Remark 6.17.)

4. Prove that the discriminant of any number field K is congruent to 0 or 1 mod 4. (A huge generalisation from the case of quadratic fields!) Proceed in the following steps:

(i) Let S_n be the group of permutations of $\{1, \ldots, n\}$. We have

$$\det(\Sigma) = \sum_{\pi \in S_n} \operatorname{sign}(\pi) \prod_{i=1}^{n} \sigma_{\pi(i)}(\alpha_i),$$

where $\operatorname{sign}(\pi) = \pm 1$ is the signature of the permutation π. Write

$$A = \sum_{\pi \in S_n} \prod_{i=1}^{n} \sigma_{\pi(i)}(\alpha_i), \quad B = \sum_{\pi \in S_n,\ \pi \text{ odd}} \prod_{i=1}^{n} \sigma_{\pi(i)}(\alpha_i),$$

so that $\det(\Sigma) = A - 2B$. Prove that A, $B \in \mathcal{O}_K$.

(ii) If you know Galois theory prove that $A \in \mathbb{Q}$, hence $A \in \mathbb{Z}$. Otherwise take this for granted.

(iii) We have $D = A^2 + 4(B^2 - AB)$. Prove that $B^2 - AB \in \mathbb{Z}$. Deduce that D is 0 or 1 mod 4.

5. In this question $K = \mathbb{Q}(\sqrt{d})$, where d is a square-free integer. Let $\mathrm{Cl}(K)$ be the class group of $\mathcal{O}_K$.

(a) Show that associating to an ideal $I \subset \mathcal{O}_K$ its conjugate ideal $\overline{I}$ preserves equivalence classes of ideals, so that conjugation is a well-defined operation on $\mathrm{Cl}(K)$. Prove that an element of $\mathrm{Cl}(K)$ is fixed by conjugation if and only if it has order at most 2 (that is, is represented by an integral ideal I such that I^2 is principal).

(b) Suppose from now on that $d < 0$. Using Q5 from Sheet 3 prove that any element of order at most 2 in $\mathrm{Cl}(K)$ can be represented by an ideal $I = P_1 \ldots P_r$, where P_i are distinct prime ideals over some of the prime numbers ramified in $\mathbb{Q}(\sqrt{d})$.

(c) Let $I \subset \mathcal{O}_K$ be an ideal from part (b). Determine when I is principal.

(d) Conclude that if $|d|$ is not a prime, then $\mathrm{Cl}(K)$ has an element of exact order 2, in particular $\mathcal{O}_K$ is not a PID.