Algebraic number theory

Solutions sheet 4

March 11, 2011

1. (a) m^n, 2, 2, 11 (this ideal is $(2+\sqrt{-7})$), 4 (this ideal is (2)).
(b) $m^{-1}\mathcal{O}_K$, $\frac{1}{2}(2, 1+\sqrt{-5})$, $(2, \frac{1}{2}(1-\sqrt{-7}))$, $\frac{1}{11}(2-\sqrt{-7})$, $(\frac{1}{2})$.
(c) All except the last one are prime ideals. The last one is

$$(2) = (2, \frac{1}{2}(1+\sqrt{-7}))(2, \frac{1}{2}(1-\sqrt{-7})).$$

(d) $6+7\sqrt{-1}$ has norm $85 = 5 \times 17$, so we find that this is the product of $2-\sqrt{-1}$ and $1+4\sqrt{-1}$. These elements are irreducible in the PID $\mathbb{Z}[\sqrt{-1}]$, hence $(2-\sqrt{-1})$ and $(1+4\sqrt{-1})$ are prime ideals. On the other hand, $5 = (2+\sqrt{-1})(2-\sqrt{-1})$, so that finally $\frac{1}{5}(6+7\sqrt{-1}) = (1+4\sqrt{-1})(2+\sqrt{-1})^{-1}$ (a ratio of two principal prime ideals).

2. The complex conjugation swaps t pairs of rows of Σ, hence it sends $\det(\Sigma)$ to $(-1)^t\det(\Sigma)$. Thus $\det(\Sigma) = c(\sqrt{-1})^t$ for some $c \in \mathbb{R}^*$. Square this to find the sign of D.

3. The discriminant of $f(t)$ is -31, and this is not divisible by a square, so we have $\mathcal{O}_K = \mathbb{Z} \oplus \mathbb{Z}\alpha \oplus \mathbb{Z}\alpha^2$ by Remark 6.17. Hence $D = -31$.

4. The only fact you need to use is that algebraic integers form a subring of $\mathbb{C}$.

5. (a) The first statement is obvious. Every element of $\mathrm{Cl}(K)$ has a representative which is an ideal $I \subset \mathcal{O}_K$. Write $I = P_1 \dots P_r$, where the P_i's are prime ideals. Since $P\overline{P} = (p)$ or (p^2), where P is a prime ideal over p, we have $I\overline{I} = (a)$ for some $a \in \mathbb{Z}$. Hence the class of $\overline{I}$ in $\mathrm{Cl}(K)$ is the inverse of the class of I, so that the classes of I and $\overline{I}$ in $\mathrm{Cl}(K)$ are equal if and only if the order of I in $\mathrm{Cl}(K)$ is at most 2.

(b) By part (a) if the class of I has order at most 2 in $\mathrm{Cl}(K)$, then $\overline{I} = xI$ for some $x \in K^*$. Write $x = \alpha/\beta$, where α, $\beta \in \mathcal{O}_K$. Then $\alpha I = \beta\overline{I}$. Taking norms and using the fact that $||I|| = ||\overline{I}||$ we obtain $N_K(x) = \pm 1$. The negative sign is not possible because $d < 0$. By Q5 of Sheet 4 we can write $x = a/\overline{a}$, where $a \in K^*$. Let $J = aI$. This is a fractional ideal of K such that $J = \overline{J}$. Hence conjugate prime ideals in the decomposition of J have the same power. Thus $J = bP_1 \dots P_r$, where P_i are distinct prime ideals over ramified primes, and $b \in \mathbb{Q}^*$.

(c) Let $I = P_1 \dots P_r$, where P_i are distinct prime ideals over ramified primes, $r \geq 1$. If $I = (a)$, $a \in \mathcal{O}_K$, then $N_k(a) = ||I|| = p_1 \dots p_r$, where P_i is the unique prime ideal of $\mathcal{O}_K$ over the prime p_i. Note that $p_1 \dots p_r$ divides d or $2d$ (the last case occurs if d is 3 mod 4, and 2 is one of the $p_1, \dots, p_r$). Let's assume that $d \neq -1$: in this case $\mathcal{O}_K$ is a PID, so all ideals are principal.

If $d < -1$ is 2 or 3 mod 4, it is easy to check that there are no elements of norm $p_1 \dots p_r$ in $\mathcal{O}_K$ unless $p_1 \dots p_r = -d$. In the last case the only element of norm d is $\pm\sqrt{d}$. The case when d is 1 mod 4 is similar. Thus the only possibility for I to be principal is $I = (\sqrt{d})$, so I must be the product of all prime ideals over the ramified primes when d is 2 mod 4, and of all ideals over odd ramified primes when d is 1 or 3 mod 4.

(d) The unique ideal P over a prime factor $p|d$ is not principle, but $P^2 = p\mathcal{O}_K$ is principal.