Algebraic number theory

Solutions sheet 5

March 11, 2011

1. Let $z \in A(d)^*$ be a unit. Write $2z = a + b\sqrt{d}$ for some a and b in $\mathbb{Z}$. We now show that the equation $a^2 - db^2 = -4$ has no solutions in $\mathbb{Z}$. Let $p|d$ be congruent to 3 modulo 4. Then -4 is a square modulo p. This is equivalent to -1 being a square modulo p, which for odd p is equivalent to the condition that p is congruent to 1 modulo 4. This is a contradiction.

2. We have $\lambda(5) = \sqrt{5}/2 < 2$. Hence every ideal class is represented by an integral ideal of norm 1, that is, $A(-5)$ itself. Thus the class group is trivial.

We have $\lambda(6) = \sqrt{6} < 3$, hence it is enough to consider ideals $I \subset A(6)$ of norm 2. These are necessarily prime ideals lying over 2. But 2 is ramified, hence $I = (2, \sqrt{6})$. If it is principal, then the norm of the generator must be ± 2. (Since $||zA(d)|| = |N_K(z)|$.) Indeed, $a^2 - 6b^2 = -2$ has a solution $a = 2$, $b = 1$. One checks immediately that we have $(2, \sqrt{6}) = (2 + \sqrt{6})$. Hence all the ideal classes are represented by principal ideals, thus the class group is trivial.

3. We have $\lambda(-163) < 9$, hence we must look at the prime ideals over 2, 3, 5 and 7. By computing the Legendre symbols one observes that 3, 5 and 7 are all inert in $\mathbb{Q}(\sqrt{-163})$, so the corresponding prime ideals are principal. Since -163 is congruent to 5 modulo 8, by the result from the lectures we know that 2 is also inert! Hence all prime ideals lying over 2, 3, 5 and 7 are principal, hence every ideal of norm less than 9 is principal. The class number is 1. [It is a difficult result that if $d < -163$, then the class number is greater than 1.]

Notation. We write the operation in the class group $\mathrm{Cl}(\mathbb{Q}(\sqrt{d}))$ as multiplication, and denote the equivalence class of an ideal $I \subset A(d)$ by $[I]$

4. Let $d = -p_1 \dots p_n$, where $p_1, \dots, p_n$ are different prime numbers, $n > 2$. To fix ideas assume that $2|p$. Consider the ideal $J_i = (p_i, \sqrt{d})$. This is a prime ideal lying over p_i, which is ramified in $\mathbb{Q}(\sqrt{d})$. Hence $J_i^2 = p_i A(d)$, and $J_i^{-1} = p_i^{-1}(p_i, \sqrt{d})$. Thus we have $J_i J_k^{-1} = p_k^{-1} J_i J_k = p_k^{-1}(p_i p_k, p_i\sqrt{d}, p_k\sqrt{d}, d) = p_k^{-1}(p_i p_k, \sqrt{d})$, because $(p_i, p_k) = 1$. I claim that the ideals $J_i = (p_i, \sqrt{d})$ and $(p_i p_j, \sqrt{d})$ for $i \neq j$ are not principal. Let us assume this for a moment. Then the classes $[J_i]$ in the class group of $\mathbb{Q}(\sqrt{d})$ are all non-trivial since J_i are not principal. These classes are also pairwise distinct since $J_i J_k^{-1}$ are not principal. This produces n different non-trivial elements in the class group, hence the result.

It remains to show that $(p_i, \sqrt{d})$ and $(p_i p_j, \sqrt{d})$ are not principal. The norms of these ideals are p_i and $p_i p_j$, respectively. But there are no elements with such norms in $A(d)$, since the equations $x^2 + |d|y^2 = p_i$ and $x^2 + |d|y^2 = p_i p_j$ have no integer solutions. Indeed, $|d| > p_i p_j$, hence $y = 0$, and now it is clear that there are no solutions (recall that $p_i \neq p_j$). This completes the proof.

5. We have $\lambda(-21) < 7$, so we look into prime ideals over 2, 3 and 5. Since 2 and 3 are ramified, the corresponding prime ideals are $P = (2, \sqrt{-21} - 1)$ and $Q = (3, \sqrt{-21})$, respectively. Using the same method as before, we show that there are no elements in $A(-21)$ with norm 2 or 3, hence P and Q are not principal. In other words, $[P] \neq 1$, $[Q] \neq 1$. It is clear that $P^2 = (2)$ and $Q^2 = (3)$, hence $[P]^2 = 1$ and $[Q]^2 = 1$. Next we study the product PQ. The norm of PQ is 6, and the same usual method shows that there are no elements in $A(-21)$ with norm 6. Hence PQ is not principal. Thus the subgroup of the class group generated by $[P]$ and $[Q]$ is isomorphic to $(\mathbb{Z}/2)^2$.

The prime 5 is split (-21 is a square modulo 5), $(5) = (5, 2-\sqrt{-21})(5, 2+\sqrt{-21})$. Let $R = (5, 2 - \sqrt{-21})$, $S = (5, 2 + \sqrt{-21})$. Since $RS = (5)$ we have $[R][S] = 1$. Let us show that PQR is principal, then $[P][Q][R] = 1$, and every element of the class group can be expressed in terms of $[P]$ and $[Q]$ alone. Indeed, the norm of PQR is 30, and the only elements of $A(-21)$ with norm 30 are $\pm 3 \pm \sqrt{-21}$. The ideal $(3 \pm \sqrt{-21})$ factors into prime ideals either as PQR or as PQS. In any of these cases our statement is clear.

Therefore the class group is isomorphic to $(\mathbb{Z}/2)^2$.