ALGEBRAIC NUMBER THEORY

FINAL

(1) Compute all reduced forms of discriminant $\Delta = -4{\cdot}17$. (The form (A, B, C) with $A > 0$ is reduced if $-A < B \leq A \leq C$, with $B > 0$ if $A = C$).

From $-68 = \Delta = B^2 - 4AC$ we see that $B = 2b$ must be even, and that $b^2 - AC = -17$. Moreover, $0 < A < \sqrt{-\Delta/3} < 5$. Now we compute

A	B	forms
1	0	$(1, 0, 17)$
2	2	$(2, 2, 9)$
3	± 2	$(3, \pm 2, 6)$

Thus the class number is 4.

(2) Compute the ideal class group of $\mathbb{Q}(\sqrt{-17}\,)$. The primes below the Gauss bound split as follows:

- $(2) = \mathfrak{p}^2$ for $\mathfrak{p} = (2, 1 + \sqrt{-17}\,)$;
- $(3) = \mathfrak{q}\mathfrak{q}'$ for $\mathfrak{q} = (3, 1 + \sqrt{-17}\,)$;
- $(5) = (5)$ is inert.

Thus the class group is generated by the classes of $\mathfrak{p}$ and $\mathfrak{q}$ (note that $[\mathfrak{q}'] = [\mathfrak{q}]^{-1}$.

Obviously, $[\mathfrak{p}]$ has order 2 in the class group. Now $(1 + \sqrt{-17}\,) = \mathfrak{p}\mathfrak{q}^2$ shows that $\mathfrak{p}\mathfrak{q}^2 \sin(1)$, hence $\mathfrak{q}^2 \sim \mathfrak{q}^2\mathfrak{p}^2 \sim \mathfrak{p}$. Thus $\mathrm{Cl}\,(K)$ is generated by $[\mathfrak{q}]$. This element has order 4 (because $[\mathfrak{q}]^2 = [\mathfrak{p}]$ has order 2), and in fact $\mathfrak{q}^4 = (8 - \sqrt{-17}\,)$.

Thus we have shown that $\mathrm{Cl}\,(K) \simeq \mathbb{Z}/4\mathbb{Z}$.

Determine the ideal class to which the ideal $\mathfrak{a} = (7, 2 + \sqrt{-17}\,)$ belongs.

This ideal $\mathfrak{a}$ has norm 7; it is equivalent to some power of $\mathfrak{q}$. Now $\mathfrak{a}$ is not principal since $x^2 + 17y^2 = 7$ is not solvable. But $2 + \sqrt{-17}$ is an element of norm 21, and we find $(2 + \sqrt{-17}\,) = \mathfrak{q}'\mathfrak{a}$. Thus $\mathfrak{a}\mathfrak{q}' \sim (1)$, hence $\mathfrak{a} \sim \mathfrak{a}\mathfrak{q}'\mathfrak{q} \sim \mathfrak{q}$, and we have shown that $\mathfrak{a} \in [\mathfrak{q}]$.

(3) Compute the class group and the fundamental unit of $K = \mathbb{Q}(\sqrt{10}\,)$.

The Gauss bound is < 4, $(2) = \mathfrak{p}^2$ for $\mathfrak{p} = (2, \sqrt{10}\,)$ and $(3) = \mathfrak{q}\mathfrak{q}'$ for $\mathfrak{q} = (3, 1 + \sqrt{10}\,)$.

If $\mathfrak{p}$ is principal, then $a^2 - 10b^2 = \pm 2$ must be solvable. Reduction modulo 5 gives a contradiction. Thus $[\mathfrak{p}]$ has order 2 in the class group.

Now $2 + \sqrt{10}$ has norm -6, hence $(2 + \sqrt{10}\,) = \mathfrak{p}\mathfrak{q}'$. This shows that $\mathfrak{p}\mathfrak{q}' \sim (1)$, hence $\mathfrak{q} \sim \mathfrak{p}\mathfrak{q}'\mathfrak{q} \sim \mathfrak{p}$, and the class group is generated by the class $[\mathfrak{p}]$ of order 2. Thus $\mathrm{Cl}\,(K) \simeq \mathbb{Z}/2\mathbb{Z}$.

The fundamental unit comes from the minimal solution of the Pell equation $t^2 - 10u^2 = \pm 1$, hence is given by $\varepsilon = 3 + \sqrt{10}$.

(4) Compute the class group and a unit > 1 of $K = \mathbb{Q}(\sqrt{89}\,)$.

The Gauss bound is $\mu \approx 4.2$, hence we need to look at the primes 2 and 3. We find $(2) = \mathfrak{p}\mathfrak{p}'$ for $\mathfrak{p} = (2, \omega)$, where $\omega = \frac{1+\sqrt{89}}{2}$, and (3) is inert. Since $N(4+\omega) = N(\frac{9+\sqrt{89}}{2}) = -2$, $\mathfrak{p} = (4+\omega)$ is principal. This shows that K has class number 1.

For computing a unit we need more elements of small norm. We immediately find $N(5+\omega) = 8$, hence $(5+\omega) = \mathfrak{p}'^3$. Taking conjugates and using $\omega' = 1 - \omega$ we find $(6-\omega) = \mathfrak{p}^3$. This shows that

$$\varepsilon = \frac{(4+\omega)^3}{6-\omega}$$

is a unit (since $\omega \approx 5$, we clearly have $\varepsilon > 1$). Actual calculation gives $\varepsilon = 447 + 106\omega$.

(5) Assume that $m \equiv 3 \bmod 4$ is squarefree.

(a) Show that $[2, 1+\sqrt{m}\,] = (2, 1+\sqrt{m}\,)$.

The $\mathbb{Z}$-module $[2, 1+\sqrt{m}\,]$ is an ideal because 2 divides $N(1+\sqrt{m}\,) = 1 - m$. Thus it contains all $\mathcal{O}_K$-linear combinations of 2 and $1+\sqrt{m}$, and this implies the claim.

(b) Find integers a and b such that $[a, b+\sqrt{m}\,] \neq (a, b+\sqrt{m}\,)$, and explain why.

We have $[2, \sqrt{m}\,] \neq (2, \sqrt{m}\,)$. In fact, the ideal contains 2 and m, hence 1, so $(2, \sqrt{m}\,) = (1)$.

On the other hand, $1 \notin [2, \sqrt{m}\,]$ because $1 = 2x + y\sqrt{m}$ for integers x, y implies $1 - 2x = y\sqrt{m}$; this is only possible for $y = 0$, and then we get a contradiction.

(6) Explain how the ideal (2) splits in quadratic number fields $\mathbb{Q}(\sqrt{m}\,)$. We have

$$\begin{aligned}
(2) &= (2,\omega)(2,\omega') && \text{if } m \equiv 1 \bmod 8,\\
(2) &= (2) \quad \text{(inert)} && \text{if } m \equiv 5 \bmod 8,\\
(2) &= (2, \sqrt{m}\,)^2 && \text{if } m \equiv 0 \bmod 2,\\
(2) &= (2, 1+\sqrt{m}\,)^2 && \text{if } m \equiv 3 \bmod 4.
\end{aligned}$$

Here $\omega = \frac{1+\sqrt{m}}{2}$.