ALGEBRAIC NUMBER THEORY

MIDTERM 2

(1) Compute the ideal class group of $K = \mathbb{Q}(\sqrt{-55}\,)$. We have disc $K = 55$, hence every ideal class contains an ideal with norm $< \sqrt{55/3} < 5$, that with norm ≤ 5. Thus the ideal class group of K is generated by the prime ideals of norm ≤ 3.

Clearly $(2) = \mathfrak{p}_2\mathfrak{p}_2'$ for $\mathfrak{p}_2 = (2, \omega)$, where $\omega = \frac{1+\sqrt{-55}}{2}$.[1] Since $(\frac{-55}{3}) = -1$, there is no ideal of norm 3.

Now we know that $\mathrm{Cl}\,(K)$ is generated by $[\mathfrak{p}_2]$. Now we will determine the smallest power of $\mathfrak{p}_2$ that is principal. If $\mathfrak{p}_2 = (\alpha)$, then $N\alpha = 2$, and writing $\alpha = \frac{a+b\sqrt{-55}}{2}$ shows that we must have $a^2 + 55b^2 = 4 \cdot 2 = 8$, which is impossible. Thus $\mathfrak{p} \not\sim (1)$. A similar argument shows that $\mathfrak{p}^3 \not\sim (1)$.

What about $\mathfrak{p}^2$? If it is principal, then $N\alpha = 4$ must have a solution. This equation is indeed solvable, and the only solutions are $\alpha = \pm 2$. But $(2) = \mathfrak{p}\mathfrak{p}' \neq \mathfrak{p}^2$, hence $\mathfrak{p}^2 \not\sim (1)$.

Finally, if $\mathfrak{p}^4$ is principal, then $a^2 + 55b^2 = 4 \cdot 16 = 64$ must be solvable. In fact, $a = 3$ and $b = 1$ is such a solution, and $\alpha = \frac{3+\sqrt{-55}}{2}$ is an element with norm $N\alpha = 16$. What is its prime ideal factorization? (α) cannot be divisible by both $\mathfrak{p}_2$ and $\mathfrak{p}_2'$, since then it would be divisible by 2, which it isn't. Thus either $(\alpha) = \mathfrak{p}_2^4$ or $(\alpha) = {\mathfrak{p}_2'}^4$. Since $\alpha = 1 + \omega$ is not in $\mathfrak{p}_2$, the second possibility must hold, and we have $(\alpha') = \mathfrak{p}_2^4$.

Thus we have seen that $[\mathfrak{p}_2]$ has order 4 in the class group, and we conclude that $\mathrm{Cl}\,(K) \simeq \mathbb{Z}/4\mathbb{Z}$.

(2) Compute the ideal class group of $\mathbb{Q}(\sqrt{30}\,)$.

The only prime ideals with norms below the Gauss bound are $\mathfrak{p} = (2, \sqrt{30}\,)$ and $\mathfrak{q} = (3, \sqrt{30}\,)$ with $\mathfrak{p}^2 = (2)$ and $\mathfrak{p}^2 = (3)$.

If $\mathfrak{p} \sim (1)$, there must exist an element of norm ± 2. But $x^2 - 30y^2 = \pm 2$ yields $x^2 \equiv \pm 2 \bmod 5$, which is impossible. Thus $[\mathfrak{p}]$ has order 2.

Next $(6 + \sqrt{30}\,) = \mathfrak{p}\mathfrak{q}$ shows that $\mathfrak{q} \sim \mathfrak{p}^2\mathfrak{q} \sim \mathfrak{p}$, hence $\mathrm{Cl}\,(K)$ contains two classes, namely $[(1)]$ and $[\mathfrak{p}]$, and we have $\mathrm{Cl}\,(K) \simeq \mathbb{Z}/2\mathbb{Z}$.

[1] Observe that $(2, 1 + \sqrt{-55}) = (2)(1, \omega) = (2)$.

(3) Show that every prime $p \equiv \pm 1 \bmod 5$ can be written in the form $p = x^2 - 5y^2$ for integers x, y. Hints:

(a) Show that p splits into principal prime ideals in $K = \mathbb{Q}(\sqrt{5})$, and deduce that $N\pi = \pm p$ for some $\pi \in \mathcal{O}_K$.
Since $p \equiv \pm 1 \bmod 5$, we have $(\frac{5}{p}) = (\frac{p}{5}) = (\frac{\pm 1}{5}) = +1$, hence $(5) = \mathfrak{p}\mathfrak{p}'$ in $K = \mathbb{Q}(\sqrt{5})$. The Gauss bound of K is 1, hence all ideals are principal. With $\mathfrak{p} = (\pi)$ we then find $N\pi = \pm 5$.

(b) Show that we may assume that $N\pi = p$ by using the fundamental unit ε of $\mathcal{O}_K$.
The fundamental unit corresponds to the smallest solution of the Pell equation $t^2 - 5u^2 = \pm 4$, which is $(t, u) = (1, 1)$. Thus $\varepsilon = \frac{1+\sqrt{5}}{2}$, and $N\varepsilon = -1$. Note that $\varepsilon^2 = \frac{3+\sqrt{5}}{2}$.
If $N\pi = p$, we are done; if $N\pi = -p$, then $N(\varepsilon\pi) = p$.

(c) Show that one of the elements π, $\pi\varepsilon^2$, $\pi\varepsilon^{-2}$ can be written in the form $\pi = x + y\sqrt{5}$.
Write $\pi = \frac{a+b\sqrt{5}}{2}$. If a and b are even, we can write $a = 2x$ and $b = 2y$, and get $\pi = x + y\sqrt{5}$.
If a and b are odd, there are two cases: $a \equiv b \bmod 4$ or $a \equiv -b \bmod 4$. In the first case, $\pi\varepsilon^2 = \frac{3a+5b+(a+3b)\sqrt{5}}{4}$; now $a + 3b \equiv a - b \equiv 0 \bmod 4$, hence $a+3b = 4y$; next $3a+5b \equiv -a+b \equiv 0 \bmod 4$, hence $3a+5b = 4x$. This shows that $\pi\varepsilon^2 = x + y\sqrt{5}$. In the second case, consider $\pi\varepsilon^{-2}$.

(4) Let $p \equiv 1 \bmod 4$ be prime, and write $2p = a^2 + b^2$. Assume that $a \equiv \pm 3 \bmod 8$. Show that the ideal class generated by $\mathfrak{a} = (a, b + \sqrt{2p})$ has order 2 in the ideal class group of $\mathbb{Q}(\sqrt{2p})$.

First we show that $\mathfrak{a}$ is not principal. In fact, if $x^2 - 2py^2 = \pm a$, then $2py^2 \equiv 0, 2 \bmod 8$, hence $\pm a = x^2 - 2py^2 \equiv \pm 1 \bmod 8$.

Next I claim that $\mathfrak{a}^2$ is principal. This is a simple calculation:

$$\begin{aligned}
\mathfrak{a}^2 &= (a^2, a(b + \sqrt{2p}), (b + \sqrt{2p})^2) \\
&= (2p - b^2, a(b + \sqrt{2p}), (b + \sqrt{2p})^2) \\
&= (b + \sqrt{2p})(\sqrt{2p} - b, a, b + \sqrt{2p}) \quad = \quad (b + \sqrt{2p}).
\end{aligned}$$

Here we have used that $a^2 = 2p - b^2$ and that $(a, 2b) = (1)$. Alternatively, you may observe that $\mathfrak{a}^2 \subseteq (b + \sqrt{2p})$ and then use the fact that both ideals have the same norm, hence must be equal.

(5) (a) Complete the definition: Ideals $\mathfrak{a}, \mathfrak{b}$ in the ring $\mathcal{O}_K$ of integers of an algebraic number field K are called equivalent ($\mathfrak{a} \sim \mathfrak{b}$) if there exist $\alpha, \beta \in \mathcal{O}_K$ such that

$$\alpha\mathfrak{a} = \beta\mathfrak{b}.$$

(b) Show that $\mathfrak{a} \sim (1)$ if and only if $\mathfrak{a}$ is principal.

$\mathfrak{a} \sim (1) \iff \alpha\mathfrak{a} = \beta(1) = (\beta)$ for some $\alpha, \beta \in \mathcal{O}_K$. But then $\mathfrak{a} = (\beta/\alpha)$ is principal.
Conversely, if $\mathfrak{a}$ is principal, say $\mathfrak{a} = (\gamma)$, then $\alpha\mathfrak{a} = \beta(1)$ for $\alpha = 1$ and $\beta = \gamma$.

(c) Show that $\sim$ is an equivalence relation.

(i) $\mathfrak{a} \sim \mathfrak{a}$ since we only need to pick $\alpha = \beta = 1$.
(ii) $\mathfrak{a} \sim fb$ is equivalent to $\alpha\mathfrak{a} = \beta\mathfrak{b}$. This clearly implies $\mathfrak{b} \sim \mathfrak{a}$.
(iii) $\mathfrak{a} \sim \mathfrak{b}$ and $\mathfrak{b} \sim \mathfrak{c}$ imply that $\mathfrak{a} \sim \mathfrak{c}$. In fact, if $\alpha\mathfrak{a} = \beta\mathfrak{b}$ and $\gamma\mathfrak{b} = \delta\mathfrak{c}$, then $\alpha\gamma\mathfrak{a} = \beta\gamma\mathfrak{b} = \beta\delta\mathfrak{c}$,