Algebraic Number Theory
Solutions to Example Sheet 3

3. Let $K = \mathbb{Q}(\sqrt{-5})$. In $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$ let

$$\mathfrak{a} = \langle 2, 1+\sqrt{-5}\rangle, \qquad \mathfrak{b} = \langle 3, 1+\sqrt{-5}\rangle, \qquad \mathfrak{b}' = \langle 3, 1-\sqrt{-5}\rangle.$$

(i) Show that

$$\mathfrak{a}^2 = \langle 2\rangle, \qquad \mathfrak{b}\mathfrak{b}' = \langle 3\rangle, \qquad \mathfrak{a}\mathfrak{b} = \langle 1+\sqrt{-5}\rangle, \qquad \mathfrak{a}\mathfrak{b}' = \langle 1-\sqrt{-5}\rangle.$$

This shows that the Algebra II example of non-unique factorisation $6 = 2\cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$ comes from grouping the ideal factorization of 6 in two different ways: $(\mathfrak{a}^2)\cdot(\mathfrak{b}\mathfrak{b}')$ and $(\mathfrak{a}\mathfrak{b})\cdot(\mathfrak{a}\mathfrak{b}')$.

(ii) Show that $\mathfrak{a}$, $\mathfrak{b}$ and $\mathfrak{b}'$ are non-principal.

Answer:

(i)

$$\begin{aligned}
\mathfrak{a}^2 &= \langle 4, 2+2\sqrt{-5}, -4+2\sqrt{-5}\rangle \qquad (\text{as } (1+\sqrt{-5})^2 = -4+2\sqrt{-5})\\
&= \langle 4, 2+2\sqrt{-5}, 2\sqrt{-5}\rangle \qquad (\text{adding first generator to the last})\\
&= \langle 4, 2, 2\sqrt{-5}\rangle \qquad (\text{subtracting third generator from second})\\
&= \langle 2\rangle \qquad (\text{since 4 and } 2\sqrt{-5} \text{ are multiples of 2}).
\end{aligned}$$

$$\begin{aligned}
\mathfrak{b}\mathfrak{b}' &= \langle 9, 3+3\sqrt{-5}, 3-3\sqrt{-5}, 6\rangle \qquad (\text{as } (1+\sqrt{-5})(1-\sqrt{-5}) = 6)\\
&= \langle 3, 3+3\sqrt{-5}, 3+3\sqrt{-5}\rangle \qquad \text{as } 3 = 9-6 \text{ and } 3 \mid 9,\ 3 \mid 6\\
&= \langle 3\rangle \qquad \text{as } 3 \pm 3\sqrt{-5} \text{ are multiples of 3}
\end{aligned}$$

$$\begin{aligned}
\mathfrak{a}\mathfrak{b} &= \langle 6, 3+3\sqrt{-5}, 2+2\sqrt{-5}, -4+2\sqrt{-5}\rangle\\
&= \langle 6, 3+3\sqrt{-5}, 2+2\sqrt{-5}\rangle \qquad \text{as } -4+2\sqrt{-5} = 2+2\sqrt{-5}-6\\
&= \langle 6, 1+\sqrt{-5}\rangle\\
&= \langle 1+\sqrt{-5}\rangle \qquad \text{as } 6 = (1+\sqrt{-5})(1-\sqrt{-5})
\end{aligned}$$

Next we compute $\mathfrak{a}\mathfrak{b}'$. We can do this as above, or note that $\overline{\mathfrak{a}} = \mathfrak{a}$ and $\overline{\mathfrak{b}} = \mathfrak{b}'$ (where the bar denotes complex conjugation). Thus

$$\mathfrak{a}\mathfrak{b}' = \overline{\mathfrak{a}\mathfrak{b}} = \langle 1-\sqrt{-5}\rangle.$$

(ii) Suppose $\mathfrak{a}$ is principal.

$$\mathfrak{a} = \beta\cdot\mathcal{O}_K$$

for some $\beta \in \mathcal{O}_K$. Since $\beta \mid 2$ and $\beta \mid (1+\sqrt{-5})$ we have $\mathrm{Nm}_{K/\mathbb{Q}}(\beta) \mid 4$ and $\mathrm{Nm}_{K/\mathbb{Q}}(\beta) \mid 6$ and so $\mathrm{Nm}_{K/\mathbb{Q}}(\beta) \mid 2$. Write $\beta = u + v\sqrt{-5}$ where u, v are integers. Thus $u^2+5v^2 = \pm 1$ or ± 2. It follows that $v = 0$ and $u = \pm 1$, so $1 = \pm\beta \in \mathfrak{a}$ (and so $\mathfrak{a} = \langle 1\rangle$). Thus $\mathfrak{a}^2 = \langle 1\rangle$ contradiction. Therefore $\mathfrak{a}$ is non-principal.

Similarly if $\mathfrak{b} = \beta\mathcal{O}_K$ then $\mathrm{Nm}_{K/\mathbb{Q}}(\beta) \mid 9, 6$, so $\mathrm{Nm}_{K/\mathbb{Q}}(\beta) = \pm 1$ or ± 3. Writing $\beta = u+v\sqrt{-5}$, we get $u^2+5v^2 = \pm 1$ or ± 3. Hence $v = 0$ or $\beta = u = \pm 1$. So $\mathfrak{b} = \langle 1\rangle$. But $\mathfrak{b}' = \overline{\mathfrak{b}}$ so $\langle 3\rangle = \mathfrak{b}\mathfrak{b}' = \langle 1\rangle$ also giving a contradiction. Therefore $\mathfrak{b}$ is non-principal.

As $\mathfrak{b}' = \overline{\mathfrak{b}}$, $\mathfrak{b}'$ is non-principal.

7. Let $K = \mathbb{Q}(\sqrt{3})$. Use the Dedekind–Kummer theorem to factorise the following ideals of $\mathcal{O}_K$ into prime ideals:

$$\langle 2\rangle, \quad \langle 3\rangle, \quad \langle 5\rangle.$$

Correction. You should also factorise $\langle 11\rangle$ into prime ideals of $\mathcal{O}_K$.
Deduce the factorisation of the following ideals of $\mathcal{O}_K$ into prime ideals:

$$\langle 10\rangle, \quad \langle 30\rangle.$$

For each prime ideal $\mathfrak{p}$ which appears as a factor of any of $\langle 2\rangle$, $\langle 3\rangle$, $\langle 5\rangle$ or $\langle 11\rangle$, show that it is principal by writing down an element $\pi \in \mathcal{O}_K$ such that $\mathfrak{p} = \langle \pi\rangle$.

Answer:

We have $\mathcal{O}_K = \mathbb{Z}[\sqrt{3}]$, so we can apply the Dedekind–Kummer theorem with $\alpha = \sqrt{3}$. The minimal polynomial of $\sqrt{3}$ is $f(X) = X^2 - 3$.

For $p = 2$: $f(X) \equiv (X-1)^2 \bmod 2$. Hence

$$\langle 2\rangle = \mathfrak{p}_2^2 \text{ where } \mathfrak{p}_2 = \langle 2, \sqrt{3}-1\rangle^2.$$

For $p = 3$: $f(X) \equiv X^2 \bmod 3$. Hence

$$\langle 3\rangle = \mathfrak{p}_3^2 \text{ where } \mathfrak{p}_3 = \langle 3, \sqrt{3}\rangle^2.$$

For $p = 5$: $f(X)$ is irreducible mod 5, because it is quadratic and has no roots (3 is not a quadratric residue mod 5). Hence $\langle 5\rangle$ is a prime of $\mathcal{O}_K$.

For $p = 11$: $f(X) \equiv (X-5)(X+5) \bmod 11$. Hence

$$\langle 11\rangle = \mathfrak{p}_{11}\mathfrak{q}_{11} \text{ where } \mathfrak{p}_{11} = \langle 11, -5+\sqrt{3}\rangle \text{ and } \mathfrak{q}_{11} = \langle 11, 5+\sqrt{3}\rangle.$$

We have

$$\langle 10\rangle = \langle 2\rangle\langle 5\rangle = \mathfrak{p}_2^2\langle 5\rangle,$$
$$\langle 30\rangle = \langle 2\rangle\langle 3\rangle\langle 5\rangle = \mathfrak{p}_2^2\mathfrak{p}_3^2\langle 5\rangle.$$

Recall that $\mathrm{Nm}_{K/\mathbb{Q}}(a+b\sqrt{3}) = a^2 - 3b^2$.

For $\mathfrak{p}_2$: $\mathrm{Nm}(\sqrt{3}-1) = 1-3 = -2 = -\mathrm{Nm}(\mathfrak{p}_2)$ and $\sqrt{3}-1 \in \mathfrak{p}_2$, so $\langle \mathfrak{p}_2\rangle = \langle \sqrt{3}-1\rangle$.

For $\mathfrak{p}_3$: $\mathrm{Nm}_{K/\mathbb{Q}}(\sqrt{3}) = -3 = -\mathrm{Nm}(\mathfrak{p}_3)$ and $\sqrt{3} \in \mathfrak{p}_3$, so $\langle \mathfrak{p}_3\rangle = \langle \sqrt{3}\rangle$.

The only prime ideal dividing $\langle 5\rangle$ is $\langle 5\rangle$ itself, which is clearly principal!

For $\mathfrak{p}_{11}$: we need an integer solution to the equation $a^2 - 3b^2 = \pm 11$. Since 11 is not a quadratic residue mod 3, in fact we need to look for a solution to $a^2 - 3b^2 = -11$. A solution is given by $a = 1, b = 2$ (the easiest way to find this is to work out $3b^2 - 11$ for small values of b, until you get a square). Now

$$1 + 2\sqrt{3} = 11 + 2(-5+\sqrt{3}) \in \langle 11, -5+\sqrt{3}\rangle = \mathfrak{p}_{11}.$$

Thus $\mathfrak{p}_{11} = \langle 1+2\sqrt{3}\rangle$.

Similarly, $\mathrm{Nm}_{K/\mathbb{Q}}(1-2\sqrt{3}) = 1-12 = -11$ and

$$1-2\sqrt{3} = 11-2(5+\sqrt{3}) \in \mathfrak{q}_{11}.$$

Thus $\mathfrak{q}_{11} = \langle 1-2\sqrt{3}\rangle$.

11. Let $K = \mathbb{Q}(\sqrt{11})$. Factorise the ideals $\langle 2\rangle$ and $\langle 3\rangle$ of $\mathcal{O}_K$ into prime ideals. Show that $\mathcal{O}_K$ has a unique proper ideal of norm ≤ 3, and that this ideal is principal. Use Minkowski's theorem on ideal classes to deduce that $\mathbb{Z}[\sqrt{11}]$ is a principal ideal domain.

Answer:

Since $11 \equiv 3 \bmod 4$, we have $\mathcal{O}_K = \mathbb{Z}[\sqrt{11}]$ so we can apply the Dedekind–Kummer theorem with $\alpha = \sqrt{11}$. The minimal polynomial of $\sqrt{11}$ is $f(X) = X^2 - 11$.

For $p = 2$: $f(X) \equiv (X-1)^2 \bmod 2$ so

$$\langle 2\rangle = \mathfrak{p}_2^2 \text{ where } \mathfrak{p}_2 = \langle 2, \sqrt{11}-1\rangle.$$

For $p = 3$: $f(X)$ is irreducible mod 3 because it is quadratic and has no roots (11 is not a quadratic residue mod 3). Hence $\langle 3\rangle$ is a prime ideal of $\mathcal{O}_K$.

Any ideal $\mathfrak{a}$ of $\mathcal{O}_K$ with norm ≤ 3 must be a product of prime ideals dividing $\langle 2\rangle$ or $\langle 3\rangle$. Thus $\mathfrak{a}$ must be a product of $\mathfrak{p}_2$ and $\langle 3\rangle$. But $\mathrm{Nm}(\langle 3\rangle) = 9 > 3$. Thus $\mathfrak{a}$ must be a power of $\mathfrak{p}_2$. Since $\mathrm{Nm}(\mathfrak{p}_2) = 2$, $\mathrm{Nm}(\mathfrak{p}_2^2) = 4 > 3$. Thus the only possibility for $\mathfrak{a}$ is $\mathfrak{p}_2$ itself.

To show that $\mathfrak{p}_2$ is principal, we must find an element of $\mathfrak{p}_2$ with norm ± 2 i.e. we must find an integer solution to the equation $a^2 - 11b^2 = \pm 2$. A solution is given by $a = 3, b = 1$. Thus we have $\mathrm{Nm}_{K/\mathbb{Q}}(3+\sqrt{11}) = 9-11 = -2$ and

$$3+\sqrt{11} = 2\times 2 + (\sqrt{11}-1) \in \mathfrak{p}_2.$$

So $\mathfrak{p}_2 = \langle 3+\sqrt{11}\rangle$.

The signature of K is $(r,s) = (2,0)$ and the discriminant is $\Delta_K = 4\times 11 = 44$. Hence the Minkowski bound is

$$B_K = \left(\frac{4}{\pi}\right)^0 \frac{2!}{2^2}\sqrt{|44|} = \tfrac{1}{2}\sqrt{44} = \sqrt{11} < 4.$$

By Minkowski's theorem, every class in $\mathrm{Cl}(K)$ is represented by an ideal of norm $< B_K$, i.e. by an ideal of norm ≤ 3. We have shown that the only proper ideal of norm ≤ 3 is $\mathfrak{p}_2$, and $\mathfrak{p}_2$ is principal. Thus $\mathrm{Cl}(K)$ is trivial i.e. $\mathcal{O}_K$ is a PID.