Algebraic Number Theory 2019
Solutions to Example Sheet 4

6. Let $K = \mathbb{Q}(\sqrt{-11})$. Let x, y be rational integers satisfying $x^3 = y^2 + 11$.
   (i) Prove that the ring of integers of $\mathbb{Q}(\sqrt{-11})$ is a PID.
   (ii) Prove that if $x, y \in \mathbb{Z}$ satisfy $x^3 = y^2 + 11$, then there exist $u, v \in \mathbb{Z}$ such that
   $$\Big(\frac{u + v\sqrt{-11}}{2}\Big)^3 = y + \sqrt{-11}.$$
   (iii) Show that the equation $x^3 = y^2 + 11$ has exactly four solutions in rational integers. Verify that two of these solutions are $(15, \pm 58)$; find the other two.

Answer:
(i) Since $-11 \equiv 1 \bmod 4$, we have $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{-11}}{2}]$ and $\Delta_K = -11$. The Minkowski bound is
$$B_K = \Big(\frac{4}{\pi}\Big)^1 \frac{2!}{2^2}\sqrt{|-11|} = \frac{2}{\pi}\sqrt{11} < \frac{2}{3} \times 4 < 3.$$
Hence $\mathrm{Cl}(K)$ is generated by the classes of prime ideals dividing 2.

The minimal polynomial of $\frac{1+\sqrt{-11}}{2}$ is $X^2 + X + 3$. This is irreducible mod 2. Hence by the Dedekind–Kummer theorem, $\langle 2\rangle$ is a prime ideal in $\mathcal{O}_K$. So all prime ideals dividing 2 are principal (**or**: there are no prime ideals of norm 2). Hence $\mathcal{O}_K$ is a PID.

(ii) If y is odd, then $y^2 \equiv 1 \bmod 8$ so $y^2 + 11 \equiv 4 \bmod 8$. It follows that x is even, but then $x^3 \equiv 0 \bmod 8$ which is a contradiction.

Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$ which divides both $\langle y + \sqrt{-11}\rangle$ and $\langle y - \sqrt{-11}\rangle$. Then also $\mathfrak{p}$ divides $\langle 2\sqrt{-11}\rangle$. Consequently $\mathrm{Nm}(\mathfrak{p})$ divides $\mathrm{Nm}_{K/\mathbb{Q}}(2\sqrt{-11}) = 44$. Since $\mathrm{Nm}(\mathfrak{p})$ is a prime power, it is either 2, 4 or 11.

If $\mathrm{Nm}(\mathfrak{p}) = 2$ or 4, then 2 divides $\mathrm{Nm}_{K/\mathbb{Q}}(y + \sqrt{-11}) = y^2 + 11$. Hence y is odd, contradicting (ii).

If $\mathrm{Nm}(\mathfrak{p}) = 11$, then 11 divides $y^2 + 11 = x^3$. Hence 11 divides both x and y. So 11^2 divides both x^3 and y^2, contradicting the fact that $x^3 - y^2 = 11$.

Since
$$\langle x\rangle^3 = \langle y + \sqrt{-11}\rangle\langle y - \sqrt{-11}\rangle$$
and the ideals $\langle y + \sqrt{-11}\rangle$, $\langle y - \sqrt{-11}\rangle$ are coprime, there exists an ideal $\mathfrak{a}$ such that
$$\mathfrak{a}^3 = \langle y + \sqrt{-11}\rangle.$$
Since $\mathcal{O}_K$ is a PID, $\mathfrak{a}$ is a principal ideal and so
$$\mathfrak{a} = \frac{u + v\sqrt{-11}}{2}$$
for some $u, v \in \mathbb{Z}$. The only units in $\mathcal{O}_K$ are ± 1, so
$$\frac{u + v\sqrt{-11}}{2} = \pm(y + \sqrt{-11}).$$

After switching the sign of u and v if necessary,

$$\frac{u+v\sqrt{-11}}{2} = y + \sqrt{-11}.$$

Alternatively: Since $\mathcal{O}_K$ is a PID, it is a UFD. Therefore the equation

$$x^3 = (y+\sqrt{-11})(y-\sqrt{-11})$$

in $\mathcal{O}_K$, and the fact that $y+\sqrt{-11}$ and $y-\sqrt{-11}$ are coprime, imply that there is exist $\alpha \in \mathcal{O}_K$ and $\gamma \in \mathcal{O}_K^\times$ such that

$$y + \sqrt{-11} = \gamma\alpha^3.$$

Since $\mathcal{O}_K^\times = \{\pm 1\}$, after replacing α by $-\alpha$ if necessary, we have

$$y + \sqrt{-11} = \alpha^3.$$

We may write

$$\alpha = \frac{u+v\sqrt{-11}}{2}, \quad u, v \in \mathbb{Z}.$$

(iii) Expanding out the equation from (iv), we get

$$\frac{u^3 + 3u^2v\sqrt{-11} - 33uv^2 - 11v^3\sqrt{-11}}{8} = y + \sqrt{-11}.$$

Since 1 and $\sqrt{-11}$ are $\mathbb{Q}$-linearly independent, this implies

$$u(u^2 - 33v^2) = 8y,$$
$$v(3u^2 - 11v^2) = 8.$$

From the second of these equations, v must be an integer factor of 8. We go through the cases:

- $v = \pm 1$. Then $3u^2 - 11 = \pm 8$, giving $3u^2 = 3$ or 19.
  We must have $u = \pm 1$, $v = -1$.
- $v = \pm 2$. Then $3u^2 - 44 = \pm 4$, giving $3u^2 = 40$ or 48.
  We must have $u = \pm 4$, $v = +2$.
- $v = \pm 4$. Then $3u^2 - 176 = \pm 2$, giving $3u^2 = 174$ or 178.
  Neither of these has an integer solution.
- $v = \pm 8$. Then $3u^2 - 704 = \pm 1$, giving $3u^2 = 703$ or 705.
  Neither of these has an integer solution.

From $u = \pm 1, v = -1$, we get

$$8y = \pm(1 - 33) = \pm 32$$

so $y = \pm 4$. Then $x^3 = 16 + 1127$ so $x = 3$ **or**

$$x = \Big(\frac{u+v\sqrt{-11}}{2}\Big)\Big(\frac{u-v\sqrt{-11}}{2}\Big) = \frac{u^2+11v^2}{4} = \frac{12}{4} = 3.$$

From $u = \pm 4, v = 2$, we get

$$8y = \pm 4(16 - 132) = \pm 4 \times 116$$

so $y = \pm 58$. Then $x^3 = 3364 + 11 = 3375$ so $x = 15$ **or**

$$x = \Big(\frac{u+v\sqrt{-11}}{2}\Big)\Big(\frac{u-v\sqrt{-11}}{2}\Big) = \frac{u^2+11v^2}{4} = \frac{16+44}{4} = 15.$$

9. Let $K = \mathbb{Q}(\sqrt{10})$.
   (i) Determine the fundamental unit of K.
   (ii) Prove that K contains a unique prime ideal $\mathfrak{p}_2$ of norm 2, and that $\mathfrak{p}_2$ is not principal. (For the second part, you may find it helpful to work mod 5.)
   (iii) Show that $\mathrm{Cl}(K) \cong \mathbb{Z}/2\mathbb{Z}$. (You may find it useful to consider the factorisation of the ideal $\langle 2 + \sqrt{10} \rangle$, which has norm 6.)

Answer:
(i) Since $10 \equiv 2 \bmod 4$, we look for the solution to $x^2 - 10y^2 = \pm 1$ in positive integers x, y with the smallest value of x.

If $x = 1$, we get $10y^2 = 1 \pm 1 = 0$ or 2. So the only solution is $y = 0$, which is not positive.

If $x = 2$, we get $10y^2 = 4 \pm 1 = 3$ or 5. There are no integer solutions.

If $x = 3$, we get $10y^2 = 9 \pm 1 = 8$ or 10. Thus $y = 1$ is a solution, so the fundamental unit is $3 + \sqrt{10}$.

(ii) $\mathcal{O}_K = \mathbb{Z}[\alpha]$ where $\alpha = \sqrt{10}$ has minimal polynomial $f(X) = X^2 - 10$.

$f(X) \equiv X^2 \bmod 2$ so by the Dedekind–Kummer theorem, $\langle 2 \rangle = \mathfrak{p}_2^2$ for a prime ideal $\mathfrak{p}_2$ of norm 2.

The equation $x^2 - 10y^2 = \pm 2$ has no integer solutions because $x^2 \equiv 0, 1$ or $4 \bmod 5$. Hence $\mathfrak{p}_2$ is not principal.

(iii) The Minkowski bound for K is

$$\left(\frac{4}{\pi}\right)^0 \frac{2!}{2^2}\sqrt{40} = \frac{1}{2}\sqrt{40} = \sqrt{10} < 4$$

so $\mathrm{Cl}(K)$ is generated by prime ideals dividing 2 or 3.

$f(X) \equiv (X - 1)(X + 1) \bmod 3$, so by Dedekind–Kummer, $\langle 3 \rangle = \mathfrak{p}_3\mathfrak{q}_3$ for prime ideals $\mathfrak{p}_3$ and $\mathfrak{q}_3$ of norm 3.

$\mathrm{Nm}_{K/\mathbb{Q}}(2 + \sqrt{10}) = 4 - 10 = -6 = -2 \times 3$ so the factorisation of the ideal $\langle 2 + \sqrt{10} \rangle$ into prime ideals must consist of one prime ideal of norm 2 (which must be $\mathfrak{p}_2$) and one prime ideal of norm 3 (we may choose the labelling so that this is $[\mathfrak{p}_3]$).

In $\mathrm{Cl}(K)$, we have $[\mathfrak{p}_2][\mathfrak{p}_3] = [1]$. Since $[\mathfrak{p}_2]^2 = [1]$, this implies that $[\mathfrak{p}_3] = [\mathfrak{p}_2]^{-1} = [\mathfrak{p}_2]$.

Similarly, in $\mathrm{Cl}(K)$ we have $[\mathfrak{p}_3][\mathfrak{q}_3] = [1]$ so $[\mathfrak{q}_3] = [\mathfrak{p}_3]^{-1} = [\mathfrak{p}_3]$.

Hence $\mathrm{Cl}(K)$ is generated by the class $[\mathfrak{p}_2]$, which has order 2, so $\mathrm{Cl}(K) \cong \mathbb{Z}/2\mathbb{Z}$.