MATH7421 Problems Week 5

Dirichlet's Unit Theorem

1. Let $d > 1$ be square-free and $K = \mathbb{Q}(\sqrt{d})$. Assume that there exists a unit $u \in \mathcal{O}_K^\times$ satisfying $u > 1$. Show that there must exist a smallest such unit. (Hint: If $1 < w < u$ is another such unit then consider $N(w)$ and $T(w)$).

2. In this question we will find a full description of the unit group of $\mathbb{Z}[\sqrt{3}]$.

   (a) Find a unit $u \in \mathbb{Z}[\sqrt{3}]$ satisfying $u > 1$.

   (b) Either prove that your unit is the smallest such unit, or find the smallest one.

   (c) Hence give a full description of the unit group $\mathbb{Z}[\sqrt{3}]^\times$.

   (d) Use part (c) to find three positive integer solutions to the Pell equation $x^2 - 3y^2 = \pm 1$.

3. For each of the following number fields K, use results from the notes to give a description of the unit group $\mathcal{O}_K^\times$ (it is not necessary to give explicit fundamental units):

   (a) $K = \mathbb{Q}(\sqrt{199})$

   (b) $K = \mathbb{Q}(\sqrt[3]{-10})$

   (c) $K = \mathbb{Q}(\sqrt{2} + \sqrt{3})$

   (d) $K = \mathbb{Q}(\zeta)$ with $\zeta = e^{\frac{2\pi i}{5}}$ a primitive 5th root of unity. You may assume that the only roots of unity in K are $\pm\zeta^i$ for $i = 0, 1, 2, 3, 4$.

4. Show that the only number fields K having finite unit group $\mathcal{O}_K^\times$ are $K = \mathbb{Q}$ and $K = \mathbb{Q}(\sqrt{d})$ with $d < 0$ square-free.

5. In this exercise we will generalise the recursion used to find solutions to Pell's equation seen in the introduction (e.g. Exercise 7 of Week 1).

   (a) Let $d > 1$ not be a square and $\alpha + \beta\sqrt{d}$ be a fundamental unit for $\mathbb{Z}[\sqrt{d}]^\times$. Show that the solutions to $x^2 - dy^2 = \pm 1$ are of the form $(\pm a, \pm b)$ where (a, b) is a term in the recursion

   $$(a_{n+1}, b_{n+1}) \mapsto (\alpha a_n + d\beta b_n, \beta a_n + \alpha b_n)$$

   with starting value $(a_0, b_0) = (1, 0)$.

   (b) Given that $8 + 3\sqrt{7} \in \mathbb{Z}[\sqrt{7}]^\times$ is a fundamental unit, use the recursion in (a) to find 3 positive integer solutions to the equation $x^2 - 7y^2 = \pm 1$.

6. (a) Let $d > 1$ not be a square. Show that if $n \in \mathbb{Z}$ can be written as $n = x^2 - dy^2$ for some $x, y \in \mathbb{Z}$ then there are infinitely many solutions.
   (b) Use your solution to find three positive integer solutions to the equation $x^2 - 2y^2 = 7$.

7. We've been considering integer solutions of equations of the form $x^2 - dy^2 = \pm 1$ for various integer values of d. To summarise our progress:

   - When $d = -1$, there are exactly four integer solutions i.e. $(x, y) = (\pm 1, 0), (0, \pm 1)$ (equivalently $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$).
   - When $d < -1$, there are exactly two integer solutions i.e. $(x, y) = (\pm 1, 0)$ (equivalently $\mathbb{Z}[\sqrt{d}]^\times = \{\pm 1\}$ in this case).

   When $d > 1$ is not a square we've seen that there are infinitely many solutions, since they correspond to units in $\mathbb{Z}[\sqrt{d}]^\times$, which in this case is an infinite group (i.e. all solutions can be described using the fundamental unit).

   What happens in the one remaining case, i.e. when d is a square?

8. Let $d > 0$ not be a square. We've been studying the equation $x^2 - dy^2 = \pm 1$ and linking integer solutions with the units of the ring $\mathbb{Z}[\sqrt{d}]$. However, there is another family of quadratic rings generated by algebraic integers, namely $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$ when $d \equiv 1 \bmod 4$. Naturally, we wonder what analogue of Pell's equation these units provide solutions for?

   (a) Show that the integer solutions to $x^2 + xy + \left(\frac{1-d}{4}\right) y^2 = \pm 1$ are in bijection with units $x + y\left(\frac{1+\sqrt{d}}{2}\right) \in \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]^\times$.

   (b) The analogue of Dirichlet's Unit Theorem still holds for these rings, i.e. $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]^\times = \{\pm v^m \mid m \in \mathbb{Z}\}$ for some fundamental unit $v = \alpha + \beta\left(\frac{1+\sqrt{d}}{2}\right)$.
   Show that the solutions to $x^2 + xy + \left(\frac{1-d}{4}\right) y^2 = \pm 1$ are of the form $\pm(a, b)$ or $\pm(a+b, -b)$ where (a, b) is a term in the recursion
   $$(a_{n+1}, b_{n+1}) \mapsto \left(\alpha a_n + \left(\frac{d-1}{4}\right)\beta b_n, \beta a_n + (\alpha + \beta) b_n\right)$$
   with starting value $(a_0, b_0) = (1, 0)$.

   (c) Let $d = 5$. In this case the fundamental unit is the golden ratio $\frac{1+\sqrt{5}}{2}$. Use this to find three positive integer solutions to the equation $x^2 + xy - y^2 = \pm 1$.

   (d) (Bonus) Show that in this case the recursion has solution $(a_n, b_n) = (F_{n-1}, F_n)$ for $n \geq 1$ where F_n is the nth Fibonacci number (i.e. the famous sequence defined by $F_0 = 0, F_1 = 1$ and $F_n = F_{n-1} + F_{n-2}$ for each $n \geq 2$).
   (This proves that the integer solutions of the equation $x^2 + xy - y^2 = \pm 1$ are precisely
   $$(\pm 1, 0), \qquad \pm(F_{n-1}, F_n), \qquad \text{and} \qquad \pm\left(F_{n+1}, -F_n\right)$$
   for some $n \geq 1$. Alternatively, this proves that the units of the ring $\mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$ are precisely the elements (for $n \geq 1$) :
   $$\pm 1, \qquad \pm\left(F_{n-1} + F_n\left(\frac{1+\sqrt{5}}{2}\right)\right), \text{ and } \qquad \pm\left(F_{n+1} - F_n\left(\frac{1+\sqrt{d}}{2}\right)\right).$$

9. We saw in Exercise 3 of Week 3 that the ring of integers of $\mathbb{Q}(\sqrt[3]{2})$ is $\mathbb{Z}[\sqrt[3]{2}]$. We know by Dirichlet's Unit Theorem that the unit group $\mathbb{Z}[\sqrt[3]{2}]^\times$ has exactly one fundamental unit (since there is only one real conjugate of $\sqrt[3]{2}$ and two complex conjugate conjugates). In the notes we claimed that:

$$\mathbb{Z}[\sqrt[3]{2}]^\times = \{\pm(1 + \sqrt[3]{2} + \sqrt[3]{2}^2)^m \,|\, m \in \mathbb{Z}\},$$

i.e. that $v = 1 + \sqrt[3]{2} + \sqrt[3]{2}^2$ is a fundamental unit.

(a) Show that $v \in \mathbb{Z}[\sqrt[3]{2}]^\times$.

(b) Prove that there is no unit $w \in \mathbb{Z}[\sqrt[3]{2}]^\times$ satisfying $1 < w < v$. (Hint: Try to adapt the method used in the notes and in Exercise 1. At some point it might be helpful to recall that $e^{\frac{2\pi i}{3}} = \frac{-1+\sqrt{-3}}{2}$).

(c) Hence prove the claim.

The content in Chapter 6 of the notes (Fermat's Last Theorem) is non-examinable. However, if you are interested in learning more about this, see Chapter 9 of the book by Jarvis.