Algebra III M3P8, M4P8

Exercise Sheet 2

1. Show that $\mathbb{Q}$ contains infinitely many integral domains.

2. Let d be an integer not divisible by a square of an integer. (Such integers are called *square-free*.) Recall that $K = \mathbb{Q}(\sqrt{d}) \subset \mathbb{C}$ is the field whose elements are $z = x + y\sqrt{d}$ with $x, y \in \mathbb{Q}$. We define the conjugate element $\overline{z} = x - y\sqrt{d}$, the trace $\mathrm{Tr}(z) = z + \overline{z} = 2x$ and the norm $\mathrm{N}(z) = z\overline{z} = x^2 - dy^2$. It is clear that $\mathrm{Tr}(z_1 + z_2) = \mathrm{Tr}(z_1) + \mathrm{Tr}(z_2)$, and $\mathrm{N}(z_1 z_2) = \mathrm{N}(z_1)\mathrm{N}(z_2)$. Define O_K as the set of those elements $z \in K$ for which $\mathrm{Tr}(z) \in \mathbb{Z}$ and $\mathrm{N}(z) \in \mathbb{Z}$.

(a) Determine all the elements $x + y\sqrt{d} \in O_K$ arguing as follows. Show that if $x \in \mathbb{Z}$, then $y \in \mathbb{Z}$ (Hint: d is square-free). Hence $\mathbb{Z}[\sqrt{d}] \subset O_K$. If $x \notin \mathbb{Z}$, then $x = (2n+1)/2$ for some $n \in \mathbb{Z}$. Show that this implies that $y = (2m+1)/2$ for some $m \in \mathbb{Z}$. Prove that this occurs only if d is 1 modulo 4. Conclude that

$$O_K = \{a + b(\frac{1}{2} + \frac{\sqrt{d}}{2})|a, b \in \mathbb{Z}\}$$

if d is congruent to 1 modulo 4, and that $O_K = \mathbb{Z}[\sqrt{d}]$ otherwise.

(b) Use the above description to prove that O_K is a subring of K.

(c) Let $z \in K$. Prove that $z \in O_K$ if and only if there exists a *monic* quadratic polynomial $f(t)$ with integral coefficients such that $f(z) = 0$.

(d) Let $z \in O_K$. Prove that $z \in O_K^*$ if and only if $\mathrm{N}(z) = \pm 1$. Hence determine O_K^* for all square-free integers $d < 0$.

(e) Let $d = \sqrt{-3}$. In lectures we used the equality $2 \times 2 = (1 + \sqrt{-3})(1 - \sqrt{-3})$ to prove that $\mathbb{Z}[\sqrt{-3}]$ is not a UFD. Will the same proof work in O_K where $K = \mathbb{Q}(\sqrt{-3})$?

(f) (harder) Prove that O_K from (e) is a Euclidean domain with $\phi(z) = \mathrm{N}(z)$. Hence O_K is a UFD by a theorem from lectures.

3. Let R be an integral domain. An element $a \in R$ is called a *greatest common divisor* of b and c if $a|b$, $a|c$, and $r|b$ and $r|c$ imply $r|a$ for any $r \in R$. (In general, a gcd is not necessarily unique. If $R = \mathbb{Z}$, then the positive gcd is also called the highest common factor.) In a Euclidean domain a gcd can be found using Euclid's algorithm.

(a) Let $R = \mathbb{Q}[x]$. Find a gcd of $x^3 - 1$ and $x^5 + x^4 + x^3 + x^2 + x + 1$.

(b) Let $R = \mathbb{Z}[\sqrt{-1}]$. Find a gcd of $9 - 2i$ and $7 - i$.

(c) Let $R = O_K$ where $K = \mathbb{Q}(\sqrt{-3})$. Find a gcd of $2 + 2\sqrt{-3}$ and $3 - 3\sqrt{-3}$. (Hint: you can use the result of 2 (f), or try to apply Euclid's algorithm directly.)