MATH7421 Coursework 4 Solutions

1. Let $\alpha = \sqrt{2} + \sqrt{5}$. Then $(\alpha - \sqrt{2})^2 = 5$, so that $\alpha^2 - 2\alpha\sqrt{2} + 2 = 5$. Rearranging gives $2\alpha\sqrt{2} = \alpha^2 - 3$, so that $(\alpha^2 - 3)^2 = 8\alpha^2$. It follows that $\alpha^4 - 6\alpha^2 + 9 = 8\alpha^2$, so that α is a root of the polynomial $x^4 - 14x^2 + 9 \in \mathbb{Q}[x]$. We show that this is the minimal polynomial of α by showing that it is irreducible over $\mathbb{Q}$, which can be done using Gauss' Lemma (i.e. show that it doesn't admit a non-trivial factorisation over $\mathbb{Z}$).

   First note that the rational root test tells us that if this polynomial has a rational root then it must be $x = \pm 1, \pm 3$. Neither of these values is a root and so there can be no linear factors.

   The only other possibility for a non-trivial factorisation over $\mathbb{Z}$ is into two quadratics:

$$x^4 - 14x^2 + 9 = (ax^2 + bx + c)(dx^2 + ex + f).$$

   Comparing x^4 coefficients gives $ad = 1$ and we may scale the factorisation by ± 1 so that $a = d = 1$. Comparing x^3 coefficients gives that $e + b = 0$, so that $e = -b$. Comparing constant coefficients gives that $cf = 9$. We can reorder the factors in the factorisation so that either $c = f \pm 3$ or $c = \pm 1$ and $f = \pm 9$.

   Our possible factorisations are now:

$$x^4 - 14x^2 + 9 = (x^2 + bx \pm 1)(x^2 - bx \pm 9)$$
$$x^4 - 14x^2 + 9 = (x^2 + bx \pm 3)(x^2 - bx \pm 3)$$

   Comparing x^2 coefficients in the second equation gives $\pm 6 - b^2 = -14$, so that $b^2 = 8$ or $b^2 = 20$. There are no integer solutions to this equation and so such a factorisation must not exists. Comparing x^2 coefficients in the first equation gives either $\pm 10 - b^2 = -14$, so that $b^2 = 24$ or $b^2 = 4$. Only the second of these has an integer solution $b = \pm 2$, leading to the potential factorisation:

$$x^4 - 14x^2 + 9 = (x^2 + 2x - 1)(x^2 - 2x - 9).$$

   However, this is not a valid factorisation, since the x coefficient on the RHS is $-16 \neq 0$.

   We therefore have that:

$$\mathbb{Q}(\sqrt{2} + \sqrt{5}) = \{a + b(\sqrt{2} + \sqrt{5}) + c(\sqrt{2} + \sqrt{5})^2 + d(\sqrt{2} + \sqrt{5})^3 \mid a, b, c, d \in \mathbb{Q}\}$$

   and $[\mathbb{Q}(\sqrt{2} + \sqrt{5}) : \mathbb{Q}] = 4$.

2. If $\beta = a + b\sqrt{d} \in \mathbb{Q}(\sqrt{d})$ then $m_\beta(x) = x^2 - 2ax + (a^2 - db^2)$. For this to be in $\mathbb{Z}[x]$ we would require:

$$2a \in \mathbb{Z} \qquad \text{and} \qquad (a^2 - db^2) \in \mathbb{Z}.$$

The first inclusion tells us that $a \in \frac{1}{2}\mathbb{Z}$ and the second then tells us that $db^2 \in \frac{1}{4}\mathbb{Z}$, so that $b^2 \in \frac{1}{4d}\mathbb{Z}$, hence $b \in \frac{1}{2}\mathbb{Z}$ (we cannot have any odd prime $p|d$ dividing the denominator since otherwise p^2 would divide the denominator of b^2, which is too big (since d is square-free).

Let $a = \frac{c_1}{2}$ and $b = \frac{c_2}{2}$ with $c_1, c_2 \in \mathbb{Z}$. Then the second inclusion gives $c_1^2 - dc_2^2 \in 4\mathbb{Z}$, so that $c_1^2 - dc_2^2 \equiv 0 \bmod 4$.

Case 1: If $d \equiv 2, 3 \bmod 4$ then the congruences $c_1^2 - 2c_2^2 \equiv 0 \bmod 4$ and $c_1^2 - 3c_2^2 \equiv 0 \bmod 4$ only have the trivial solution $(c_1, c_2) \equiv (0, 0) \bmod 4$, hence that c_1, c_2 are even. This implies that $a, b \in \mathbb{Z}$, so that $\mathcal{O}_K \subseteq \mathbb{Z}[\sqrt{d}]$.

It's clear that every element of $\mathbb{Z}[\sqrt{d}]$ satisfies the two includions, so that $\mathcal{O}_K \subseteq \mathbb{Z}[\sqrt{d}]$.

Case 2: If $d \equiv 1 \bmod 4$ then the congruence $c_1^2 - c_2^2 \equiv 0 \bmod 4$ has more solutions. In fact, it implies that either c_1, c_2 are both even or both odd, so that $a, b \in \mathbb{Z}$ or $a, b \in \frac{1}{2}\mathbb{Z}\backslash\mathbb{Z}$.

It follows that $\mathcal{O}_K \subseteq \mathbb{Z}[\sqrt{d}] \cup \left\{ \frac{a+b\sqrt{d}}{2} \mid a, b \text{ odd} \right\}$. Note that if a, b are odd then $\frac{a+b\sqrt{d}}{2} = \frac{(a-b)+b+b\sqrt{d}}{2} = \frac{(a-b)}{2} + b\left(\frac{1+\sqrt{d}}{2}\right) \in \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$. Also $\mathbb{Z}[\sqrt{d}] \subset \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$, since if $a, b \in \mathbb{Z}$ then $a + b\sqrt{d} = (a-b) + 2b\left(\frac{1+\sqrt{d}}{2}\right)$. Conversely, if $a + b\left(\frac{1+\sqrt{d}}{2}\right) \in \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$ then either b is even (in which case the element lies in $\mathbb{Z}[\sqrt{d}]$) or b is odd (in which case the element lies in $\left\{ \frac{a+b\sqrt{d}}{2} \mid a, b \text{ odd} \right\}$. This now implies that $\mathcal{O}_K \subseteq \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$.

To show the reverse inclusion, let $a + b\left(\frac{1+\sqrt{d}}{2}\right) \in \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$. Then this element can be shown to be a root of the monic integer polynomial $x^2 - (2a+b)x + \left(a^2 + ab + \left(\frac{1-d}{4}\right)b^2\right) \in \mathbb{Z}[x]$, hence $\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$.