Exercise Sheet 7

Exercise 3
Solution 1.
Let $D \in \mathbb{Z}$ be square-free integer with $D \equiv 1 \mod 4$ and denote $L := \mathbb{Q}(\sqrt{D})$. Then, according to example 3.2.5. (script) we have

$$\mathcal{O}_L = \mathbb{Z}\left[\frac{1+\sqrt{D}}{2}\right] =: \mathbb{Z}[\alpha]. \tag{1}$$

We want to apply the theorem from the lecture. First, we find the minimal polynomial of α. It is

$$\left(\frac{1+\sqrt{D}}{2}\right)^2 = \left(\frac{D-1}{4}\right) + \left(\frac{1+\sqrt{D}}{2}\right). \tag{2}$$

Thus the minimal polynomial is

$$f_\alpha(X) = X^2 - X - \frac{D-1}{4} \in \mathbb{Z}[X] \tag{3}$$

as $D \equiv 1 \mod 4$. Now, we will aplly the theorem.

Let $p \in \mathbb{Z}$ be an odd prime.
<u>Case 1:</u> Let $p \mid D$. Then,

$$\begin{aligned} f(X) &= X^2 - X - \frac{D-1}{4} && (4)\\ &\equiv X^2 + (p-1)X + \frac{1}{4} \mod p && (5)\\ &\equiv \left(X + \frac{p-1}{2}\right)^2 \mod p && (6)\end{aligned}$$

So we have $p\mathcal{O}_L = (p, \frac{p+\sqrt{D}}{2})^2$. Finally, we want to show $(p, \frac{p+\sqrt{D}}{2}) = (p, \sqrt{D})$. Clearly, it is $(p, \frac{p+\sqrt{D}}{2}) \subseteq (p, \sqrt{D})$. For the other side, we have

$$p \cdot \alpha - \sqrt{D} \cdot \frac{p-1}{2} = \frac{p+\sqrt{D}}{2}. \tag{7}$$

We conclude $p\mathcal{O}_L = (p, \sqrt{D})^2$.

<u>Case 2:</u> Let $p \nmid D$ but $D \equiv m^2 \mod p$. We have $D = m^2 + pn \equiv m^2 \mod p$ and hence

$$\begin{aligned} f(X) &= X^2 - X - \frac{D-1}{2} && (8)\\ &\equiv X^2 - X - \frac{\cdot m^2 + 1}{4} \mod p && (9)\\ &\equiv (X + \frac{m-1}{2})(X - \frac{m+1}{2}) \mod p. && (10)\end{aligned}$$

So we have $\mathcal{O}_L = (p, \frac{\sqrt{D}+m}{2})(p, \frac{\sqrt{D}-m}{2})$. Similary as above, we can rewrite the ideals and get $p\mathcal{O}_L = (p, \sqrt{D}+m)(p, \sqrt{D}-m)$.

<u>Case 3:</u> Otherwise, we have $D \not\equiv m^2 \mod p$ for any $m \in \mathbb{Z}$. We have

$$f(X) = X^2 - X - \frac{D-1}{4} \tag{11}$$

and since this polynomial mod p is irreducible, we have $p\mathcal{O}_L = (p)$.

Solution 2.
Now let $p = 2$. We apply the same theorem used above. If $D \equiv 1 \mod 8$, then we have for some $n \in \mathbb{Z}$

$$\begin{aligned} f_\alpha(X) &= X^2 - X - \frac{8n+1-1}{4} && (12) \\ &= X^2 - X - 2n && (13) \\ &\equiv \overline{X(X+1)} \mod 2 && (14) \end{aligned}$$

hence $2\mathcal{O}_L = (2, \alpha)(2, 1+\alpha)$. On the other hand, if $D \equiv 5 \mod 8$, then we have for some $n \in \mathbb{Z}$

$$\begin{aligned} f_\alpha(X) &= X^2 - X - \frac{8n+5-1}{4} && (15) \\ &= X^2 - X - 2n - 1 && (16) \\ &\equiv \overline{X^2 + X + 1} \mod 2. && (17) \end{aligned}$$

As f_α here is irreducible, we have $2\mathcal{O}_L = (2, \alpha^2 + \alpha + 1)$.