

Exercise Sheet 7

Exercise 3

Solution 1.

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

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

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

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

Thus the minimal polynomial is

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

as $D \equiv 1 \pmod{4}$. Now, we will apply the theorem.

Let $p \in \mathbb{Z}$ be an odd prime.

Case 1: Let $p \mid D$. Then,

$$X^2 - X - \frac{D-1}{4} \equiv X^2 + (p-1)X + \frac{1}{4} \pmod{p} \quad (4)$$

$$\equiv \left(X + \frac{p-1}{2} \right)^2 \pmod{p} \quad (5)$$

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

$$p \cdot \alpha - \sqrt{D} \cdot \frac{p-1}{2} = \frac{p + \sqrt{D}}{2}. \quad (6)$$

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

Case 2: Let $p \nmid D$ but $D \equiv m^2 \pmod{p}$. We have $D = m^2 + pn \equiv m^2 \pmod{p}$ and hence $\overline{f(X)} = X^2 - m^2 = (X+m)(X-m)$. With the theorem, we have $p\mathcal{O}_L = (p, \sqrt{D} + m)(p, \sqrt{D} - m)$.

Case 3: Otherwise, we have $D \not\equiv m^2 \pmod{p}$ for any $m \in \mathbb{Z}$. We have $\overline{f(X)} = X^2 - D$

Solution 2.

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

$$f_\alpha(X) = X^2 - X - \frac{8n+1-1}{4} \quad (7)$$

$$= X^2 - X - 2n \quad (8)$$

$$\equiv \overline{X(X+1)} \pmod{2} \quad (9)$$

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

$$f_\alpha(X) = X^2 - X - \frac{8n+5-1}{4} \quad (10)$$

$$= X^2 - X - 2n - 1 \quad (11)$$

$$\equiv \overline{X^2 + X + 1} \pmod{2}. \quad (12)$$

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