Exercise 2.1

Let $d \in \mathbb{Z}$ be a square-free integer and consider $K = \mathbb{Q}(\sqrt{d})$.

1. Find an integral basis for K.

   Proof. From exercise 1.2.2. we have that $\mathcal{O}_K = \mathbb{Z}[\alpha]$ where

   $$\alpha = \begin{cases} \frac{1+\sqrt{d}}{2} & d \equiv 1 \mod 4 \\ \sqrt{d} & d \not\equiv 1 \mod 4. \end{cases}$$

   so the integral basis is $\mathcal{B} = \{1, \alpha\}$. $\square$

2. Using the basis, compute the discriminant of $K/\mathbb{Q}$.

   Proof. We have

   $$\Delta_K = \det \begin{pmatrix} \sigma_1(b_1) & \sigma_1(b_2) \\ \sigma_2(b_1) & \sigma_2(b_2) \end{pmatrix}^2$$

   where σ_1 and σ_2 are the set of embeddings of K onto the complex numbers, and b_1 and b_2 are the integral basis of $\mathcal{O}_K$. If $d \equiv 1 \mod 4$, we have

   $$\Delta_K = \det \begin{pmatrix} \sigma_1(b_1) & \sigma_1(b_2) \\ \sigma_2(b_1) & \sigma_2(b_2) \end{pmatrix}^2 = \det \begin{pmatrix} 1 & \frac{1+\sqrt{d}}{2} \\ 1 & \frac{1-\sqrt{d}}{2} \end{pmatrix}^2 = (-\sqrt{d})^2 = d.$$

   If $d \not\equiv 1 \mod 4$, we have

   $$\Delta_K = \det \begin{pmatrix} \sigma_1(b_1) & \sigma_1(b_2) \\ \sigma_2(b_1) & \sigma_2(b_2) \end{pmatrix}^2 = \det \begin{pmatrix} 1 & \sqrt{d} \\ 1 & -\sqrt{d} \end{pmatrix}^2 = (-2\sqrt{d})^2 = 4d.$$

   So the discriminant is

   $$\Delta_K = \begin{cases} d & d \equiv 1 \mod 4 \\ 4d & d \not\equiv 1 \mod 4 \end{cases} \tag{1}$$

   $\square$

Exercise 2.2

Let $K = \mathbb{Q}(\sqrt{-5})$, so $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$. Consider the ideals $\mathfrak{p} := (2, 1+\sqrt{-5})$ and $\mathfrak{q} = (3, 1+\sqrt{-5})$ in $\mathcal{O}_K$ and let $\overline{\mathfrak{p}}$ and $\overline{\mathfrak{q}}$ denote the ideals obtained by elementwise complex conjugation.

1. Show that $\mathfrak{p}$ and $\mathfrak{q}$ are prime but not principal. Prove $\mathfrak{p} = \overline{\mathfrak{p}}$.

   Proof. Consider $\mathbb{Z}[\sqrt{-5}]/(2, 1+\sqrt{-5})$. We want to show that this is an integral domain. We have

   $$\begin{aligned} \mathbb{Z}[\sqrt{-5}]/(2, 1+\sqrt{-5}) &\simeq (\mathbb{Z}[X]/(2, 1+X))/(X^2+5) \\ &\simeq (\mathbb{Z}/(2))[X]/(X+1, X^2+5) \\ &\simeq (\mathbb{Z}/(2))[X]/(X+1, X^2+1) \\ &\simeq (\mathbb{Z}/(2))[X]/(X+1) \\ &\simeq (\mathbb{Z}/(2))[X]/(X) \\ &\simeq (\mathbb{Z}/(2)) \end{aligned}$$

   And the last expression is an integral domain.

Similary, we have

$$\begin{aligned}
\mathbb{Z}[\sqrt{-5}] \Big/ (3, 1+\sqrt{-5}) &\simeq \mathbb{Z}[X] \Big/ (X^2+5, 3, X+1) \\
&\simeq \mathbb{Z} \Big/ (3) \, [X] \Big/ (X^2+5, X+1) \\
&\simeq \mathbb{Z}/(3)[X] \Big/ (X^2+2, X+1) \\
&\simeq \mathbb{Z}/(3)[X]/(X) \\
&\simeq \mathbb{Z}/(3)
\end{aligned}$$

which again is an integral domain.

To show □

2. Verify that $\mathfrak{p}\mathfrak{q} = (1+\sqrt{-5})$ and $\mathfrak{p}\overline{\mathfrak{q}} = 1-\sqrt{-5}$.
3. Show that $\mathfrak{p}^2\mathfrak{q}\overline{\mathfrak{q}} = (6)$.

Excersie 2.3

Let K be a field suppose $L = K(\alpha)$ is a separable extension such that the minimal polynomial of α has the form $f = T^3 + aT + b$ for some $a, b \in K$. Compute $D(1, \alpha, \alpha^2)$ in terms of a and b.

Proof. We have

$$D(1, \alpha, \alpha^2) = (1-\alpha)^2(1-\alpha^2)^2(\alpha-\alpha^2)^2$$

□