Exercise 1.1

Let $A \subset B$ be an integral extension of rings and assume that B is an integral domain. Suppose $\mathfrak{q} \subset B$ is a prime ideal and let $\mathfrak{p} := \mathfrak{q} \cap A \subset A$.

1. Prove that A is a field if and only if B is a field.

   Proof. Assume A is a field. Let $\mathfrak{m}$ be a maximal ideal in B and fix a nonzero element $b \in \mathfrak{m}$. Because b is integral over A, we have an expression with some $a_0, \dots, a_n \in A$

   $$0 = a_0 + a_1 b + a_2 b^2 + \cdots + a_n b^n \iff -a_0 = a_1 b + a_2 b^2 + \cdots + a_n b^n.$$

   On the right side, for each $1 \leq i \leq n$, we have that $a_i b^i$ is in $\mathfrak{m}$, so the whole sum $\sum_{i=1}^n a_i b^i$ is in $\mathfrak{m}$.

   For the other direction of the implication, let B be a field and fix an $x \in A$. x is a unit in B, so there is a $y \in B$ with $xy = 1$. Again, for y we have the expression

   $$0 = a_0 + a_1 y + a_2 y^2 + \cdots + a_n y^n$$

   and if we multiply x^{n-1} on both sides, we yield

   $$\begin{aligned} 0 &= a_0 x^{n-1} + a_1 x^{n-2} + a_2 x^{n-3} + \cdots + a_n y \\ \iff & - a_0 x^{n-1} - a_1 x^{n-2} - a_2 x^{n-3} - \cdots - a_{n-1} = a_n y \\ \iff & a_n^{-1}(-a_0 x^{n-1} - a_1 x^{n-2} - a_2 x^{n-3} - \cdots - a_{n-1}) = y \end{aligned}$$

   In other words, y is in A or in different words, A is a field. $\square$

2. Show that $\mathfrak{p}$ is a prime ideal of A and that $A/\mathfrak{p}$ can be viewed as a subring of $B/\mathfrak{q}$.

   Proof. Consider $A+\mathfrak{q}$. This is a subring of B and $\mathfrak{q}$ is also prime in $A+\mathfrak{q}$. With the second isomorphism theorem we have

$$A \big/ \mathfrak{p} = A \Big/ (A \cap \mathfrak{q}) \simeq (A+\mathfrak{q}) \big/ \mathfrak{q},$$

   and since the last expression is a integral domain, $A/\mathfrak{p}$ is an integral domain. The last expression also shows that $A/\mathfrak{p}$ can be viewed as a subring of $B/\mathfrak{q}$. $\square$

3. Show that $B/\mathfrak{q}$ is integral over $A/\mathfrak{p}$.

Proof. Fix a $(b + \mathfrak{q}) \in B/\mathfrak{q}$. Because B is an integral extension, we have an equation for b with some $a_0, \dots, a_n \in A$

$$b^n + a_{n-1}b^{n-1} + \cdots + a_0 = 0.$$

If $b \in B$ and $a \in A$, then $(a + \mathfrak{p})(b + \mathfrak{q})^n = (ab^n + \mathfrak{q})$. Now we have

$$\begin{aligned}
&(b + \mathfrak{q})^n + (a_{n-1} + \mathfrak{q})(b + \mathfrak{q})^{n-1} + \cdots + (a_0 + \mathfrak{q}) \\
=&(b^n + \mathfrak{q}) + (a_{n-1}b^{n-1} + \mathfrak{q}) + \cdots + (a_0 + \mathfrak{q}) \\
=&b^n + a_{n-1}b^{n-1} + \cdots + a_0 + \mathfrak{q} \\
=&0 + \mathfrak{q},
\end{aligned}$$

so $B/\mathfrak{q}$ is integral over $A/\mathfrak{p}$. $\square$

4. Deduce that $\mathfrak{q}$ is maximal in B if and only if $\mathfrak{p}$ is maximal A.

   Proof. $\mathfrak{q}$ is maximal in B if and only if $B/\mathfrak{q}$ is a field. We know from 2. that $A/\mathfrak{p}$ is a subring of $B/\mathfrak{q}$ and from 3. that $B/\mathfrak{q}$ is an integral extension of $A/\mathfrak{p}$. Applying 1. yields that $A/\mathfrak{p}$ is a field if and only if $B/\mathfrak{q}$ is a field. Hence $\mathfrak{p}$ is maximal in A. $\square$

Exercise 1.2

Let K be a number field with $[K : \mathbb{Q}] = 2$.

1. Show that $K = \mathbb{Q}(\sqrt{d})$ where d is square-free.

   Proof. Since every extension of a field of characteristic 0 is separable, K is separable, and by the primitive element thoerem, we know that K is simple. Now the algebraic closure of $\mathbb{Q}$ is $\mathbb{C}$, there is an element in $x \in \mathbb{C}$ such that $K = \mathbb{Q}(x)$. If x^2 is not rational, then $[K : \mathbb{Q}] > 2$. Now assume that x^2 is not square-free, i.e. there is a prime $p \in \mathbb{N}$ such that $n \cdot p^2 = x^2$ for some $n \in \mathbb{Z}$. Then, $K = \mathbb{Q}(p\sqrt{n}) = \mathbb{Q}(\sqrt{n})$. Moreover, if x^2 is not an integer, another primitive element that is an integer can be found. All in all, there is a square-free integer d such that $K = \mathbb{Q}(\sqrt{d})$. □

2. In this setting, show that $\mathcal{O}_K = \mathbb{Z}[\alpha]$ where

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

   Proof. Use minimal polynomials □

3. No.

Exercise 1.3

Consider $R = \mathbb{Z}[\sqrt{3}]$ with the norm $N : R \longrightarrow \mathbb{N}_0$,

$$N(a + b\sqrt{3}) = |a^2 - 3b^2|.$$

Show that R is euclidian with respect to this norm.

Proof.

$$\begin{aligned}
x_a + x_b\sqrt{3} &= q(y_a + y_b\sqrt{3}) + r \\
&= (q_a + q_b\sqrt{3})(y_a + y_b\sqrt{3}) + r \\
&= q_a y_a + q_a y_b\sqrt{3} + q_b y_a\sqrt{3} + 3q_b y_b + r \\
&= q_a y_a + 3q_b y_b + (q_a y_b + q_b y_a)\sqrt{3} + r \\
&= q_a y_a + 3q_b y_b + r_a + (q_a y_b + q_b y_a + r_b)\sqrt{3}
\end{aligned}$$

So

$$\begin{aligned}
x_a &= q_a y_a + 3q_b y_b + r_a \\
x_b &= q_a y_b + q_b y_a + r_b
\end{aligned}$$

Say $r \neq 0$. We want to show $|r_a^2 - 3r_b^2| < |y_a^2 - 3y_b^2|$.

$$\begin{aligned}
|r_a^2 - 3r_b^2| &= |(x_a - q_a y_a - 3q_b y_b)^2 - 3(x_b - q_a y_b - q_b y_a)^2| \\
&= |x_a^2 - 2x_a q_a y_a - 6x_a q_b y_b + q_a^2 y_a^2 + 6q_a y_a q_b y_a + 9q_b^2 y_b^2|
\end{aligned}$$

It is

$$\begin{aligned}
r_a^2 &= (x_a - q_a y_a - 3q_b y_b)^2 \\
&= x_a^2 - 2x_a q_a y_a - 6x_a q_b y_b + q_a^2 y_a^2 + 6q_a q_b y_a y_b + 9q_b^2 y_b^2 \\
-3r_b^2 &= -3(x_b - q_a y_b - q_b y_a)^2 \\
&= -3(x_b^2 - 2x_b q_a y_b - 2x_b q_b y_a + q_a^2 y_b^2 + 2q_a q_b y_a q_b + q_b^2 y_a^2) \\
&= -3x_b^2 + 6x_b q_a y_b + 6x_b q_b y_a - 3q_a^2 y_b^2 - 6q_a q_b y_a q_b - 3q_b^2 y_a^2 \\
r_a^2 - 3r_b^2 &= x_a^2 - 2x_a q_a y_a - 6x_a q_b y_b - 3x_b^2 + 6x_b q_a y_b + 6x_b q_b y_a + q_a^2 y_a^2 + 9q_b^2 y_b^2 - 3q_a^2 y_b^2 - 3q_b^2 y_a^2
\end{aligned}$$

It is enough to show

$$x_a^2 - 2x_a q_a y_a - 6x_a q_b y_b + q_a^2 y_a^2 + 6q_a q_b y_a y_b + 9q_b^2 y_b^2 < |y_a^2 - 3y_b^2|$$

$\square$