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 $a_0, \ldots, a_n \in A$

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

   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 $a_0, \ldots, a_n \in A$

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

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 Euclidean with respect to this norm.

Proof. Let $x, y \in R$ and write $x = x_a + x_b\sqrt{3}$ and $y = y_a + y_b\sqrt{3}$. We have

$$\begin{aligned}
\frac{x}{y} &= \frac{x_a + x_b\sqrt{3}}{y_a + y_b\sqrt{3}} \\
&= \frac{x_a + x_b\sqrt{3}}{y_a + y_b\sqrt{3}} \cdot \frac{y_a - y_b\sqrt{3}}{y_a - y_b\sqrt{3}} \\
&= \frac{x_a y_a - 3x_b y_b + (x_b y_a - x_a y_b)\sqrt{3}}{y_a^2 - 3y_b^2} \\
&= \underbrace{\frac{x_a y_a - 3x_b y_b}{y_a^2 - 3y_b^2}}_{=:\alpha} + \underbrace{\frac{x_b y_a - x_a y_b}{y_a^2 - 3y_b^2}}_{=:\beta}\sqrt{3}.
\end{aligned}$$

Set $z_\alpha \in \mathbb{Z}$ to be the closest integer to α and $z_\beta \in \mathbb{Z}$ to be the closest integer to β.

To show that R is Euclidean, we want to find $p, r \in \mathbb{Z}[\sqrt{3}]$ such that $x = py + r$. Set $\theta := (\alpha - z_\alpha) + (\beta - z_\beta)\sqrt{3}$. We claim that

$$p = (z_\alpha + z_\beta\sqrt{3}) \qquad \text{and} \qquad r = y\theta.$$

We have

$$\begin{aligned}
r &= y\theta \\
&= y((\alpha - z_\alpha) + (\beta - z_\beta)\sqrt{3}) \\
&= y(\alpha - z_\alpha + \beta\sqrt{3} - z_\beta\sqrt{3}) \\
&= y((\alpha + \beta\sqrt{3}) - (z_\alpha + z_\beta\sqrt{3})) \\
&= y(\alpha + \beta\sqrt{3}) - y(z_\alpha + z_\beta\sqrt{3}) \\
&= y\frac{x}{y} - py \\
&= x - py
\end{aligned}$$

Addint py on both ends yields the representation $x = py + r$ as desired.

We show $N(r) < N(y)$. Because $|\alpha - z_\alpha| < 2$ and $|\beta - z_\beta| < 2$, we have

$$\begin{aligned}
N(r) &= N(y\theta) \\
&= N(y)N(\theta) \\
&= N(y) \cdot |(\alpha - z_\alpha)^2 - 3(\beta - z_\beta)^2| \\
&\leq N(y) \cdot \max\{(\alpha - z_\alpha)^2, 3(\beta - z_\beta)^2\} \\
&\leq N(y) \cdot \frac{3}{4} \\
&\leq N(y)
\end{aligned}$$

□

Exercise 1.4

Let $R = \mathbb{Z}[\sqrt{-5}]$. Show that R is not a unique factorization domain by taking the following steps.

1. Compute the group of units $R^\times$.

   Proof. Define a norm $N : R \longrightarrow \mathbb{N}_0$ as $N(a + b\sqrt{5}) = a^2 + 5b^2$ and let $x + y\sqrt{5} \in \mathbb{Z}[\sqrt{5}]$. If $x + y\sqrt{5}$ is a unit, then $N(x + y\sqrt{5}) = 1$, and the only integers that satisfy $a^2 + 5b^2 = 1$ is $a = \pm 1$ and $b = 0$. Therefore, the only units in R is ± 1. $\square$

2. Find two different factorizations of $6 \in R$ into irreducible factors.

   Proof. Trivially, $2 \cdot 3 = 6$. Also, it is not hard to find $(1 + \sqrt{-5})(1 - \sqrt{-5}) = 6$. $\square$

3. Show that the factors appearing are pairwise non-associated.

   Proof. This is clear. Conclude that there are distinct factorizations in $\mathbb{Z}[\sqrt{-5}]$, hence it is not a unique factorization domain. $\square$

Exercise 1.4+

Let $R = \mathbb{Z}[\sqrt{5}]$. Show that R is not a unique factorization domain by taking the following steps.

1. Compute the group of units $R^\times$.

   Proof. Let $a + b\sqrt{5} \in \mathbb{Z}[\sqrt{5}]$. We want to find another element $x + y\sqrt{5} \in \mathbb{Z}[\sqrt{5}]$ such that their product is 1. We have

   $$\begin{aligned} 1 &= (a + b\sqrt{5})(x + y\sqrt{5}) \\ &= ax + ay\sqrt{5} + bx\sqrt{5} + 5by \\ &= (ax + 5by) + (bx + ay)\sqrt{5} \end{aligned}$$

   So we have a system of linear equations

   $$\begin{aligned} ax + 5by &= 1 \\ bx + ay &= 0 \end{aligned}$$

   where x and y are the variables.

   If $b = 0$, then

   $$\begin{aligned} ax &= 1 \\ ay &= 0. \end{aligned}$$

   Because $a \neq 0$, we have $y = 0$, and since $x \in \mathbb{Z}$, the only units in $\mathbb{Z}[\sqrt{5}]$ with $b = 0$ is ± 1.

   If $b \neq 0$, then multiplying the second equation yields

   $$\left.\begin{aligned} ax + 5by &\quad= 1 \\ ax + \tfrac{a^2}{b}y &\quad= 0 \end{aligned}\right\} \Rightarrow \frac{b}{5b^2 - a^2} = y$$

   so $(5b - a^2b^{-1})^{-1} = y$. But y can $\square$