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 and let's do this a little different. 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

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

   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 is in $\mathfrak{m}$. This implies the absurdity that $-a_0$, an unit, is contained in $\mathfrak{m}$. So there is no such thing as nonzero b in $\mathfrak{m}$ and B is a field.

   For the other direction of the implication, we will do it traditionally. 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

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

   In other words, y is in A or in different words, A is a field. □

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. (a) We simply have $A/(\mathfrak{q} \cap A) \cong (A + \mathfrak{q})/\mathfrak{q}$ and since $\mathfrak{q}$ is prime in $A + \mathfrak{q}$, $A/\mathfrak{p}$ is an integral domain.

   (b) That $A/\mathfrak{p}$ is a subring of $B/\mathfrak{q}$ follows from above.

   □

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

   Proof. Should be clear. $\square$

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

   Proof. This is clear. $\square$

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