Exercise 2.1.

(a) Show that every number field of degree 2 over $\mathbb{Q}$ is one of the quadratic fields $\mathbb{Q}[\sqrt{m}], m \in \mathbb{Z}$.

Proof. Suppose K is a degree 2 number field. Every such field is of the form $\mathbb{Q}[\alpha]$ for an algebraic number $\alpha \in \mathbb{C}$. Since K is degree 2, α must be the root of a degree 2 irreducible polynomial $f = ax^2 + bx + c$. When considering the irreducibility of f over $\mathbb{Q}$, we might as well consider a monic polynomial ($a = 1$) after rescaling. Hence, f is irreducible if and only if

$$\frac{-b \pm \sqrt{b^2 - 4c}}{2} \notin \mathbb{Q},$$

which happens if and only if $b^2 - 4c$ is squarefree. It's clear then that $\mathbb{Q}[\sqrt{b^2 - 4c}] = \mathbb{Q}[\alpha]$, since we have $\alpha = -\frac{b}{2} \pm \frac{1}{2}\sqrt{b^2 - 4c} \in \mathbb{Q}[\sqrt{b^2 - 4c}]$ and $\sqrt{b^2 - 4c} = \pm\frac{b}{2} \pm \alpha \in \mathbb{Q}[\alpha]$. □

(b) Show that the fields $\mathbb{Q}[\sqrt{m}]$, m squarefree, are pairwise distinct. (Hint: Consider the equation $\sqrt{m} = a + b\sqrt{n}$); use this to show that they are in fact pairwise non-isomorphic.

Proof. Suppose m and n are squarefree with $m \neq n$. We want to show that $\mathbb{Q}[\sqrt{m}]$ and $\mathbb{Q}[\sqrt{n}]$ are pairwise distinct. Suppose they are equal, then $\sqrt{m} = a + b\sqrt{n}$ for some $a, b \in \mathbb{Q}$. Then, $m = a^2 + b^2 n + 2ab\sqrt{n}$. That is, $2ab = 0$ and $m = a^2 + b^2 n$. Then we must have $a = 0$ or $b = 0$, but if $b = 0$, then $m = a^2$, contradicting the fact that m is not a square of an integer, let alone a rational number. On the other hand, writing $b = \frac{x}{y}$ for $x, y \in \mathbb{Z}$, we obtain $y^2 m = x^2 n$. Since m and n are squarefree, this only happens if $y = x$ and $m = n$. □

Exercise 2.2. Let I be the ideal generated by 2 and $1+\sqrt{-3}$ in the ring $\mathbb{Z}[\sqrt{-3}] = \{a+b\sqrt{-3} : a,b \in \mathbb{Z}\}$. Show that $I \neq (2)$ but $I^2 = 2I$. Conclude that ideals in $\mathbb{Z}[\sqrt{-3}]$ do not factor uniquely into prime ideals. Show moreover that I is the unique prime ideal containing (2) and conclude that (2) is not a product of prime ideals.

Proof. Note that $I = (2)$ if and only if $1+\sqrt{-3} \in (2)$, but we clearly cannot have

$$1+\sqrt{-3} = 2(a+b\sqrt{-3}) = 2a+2b\sqrt{-3}$$

for $a,b \in \mathbb{Z}$. Now, $I^2 = (4, 2+2\sqrt{-3}, -2+2\sqrt{-3})$ while $2I = (4, 2+2\sqrt{-3})$. Since $2+2\sqrt{-3} = 4+(-2+2\sqrt{-3})$, a sum of the other two generators of I^2, we can conclude that $I^2 = 2I$. For the next claim, we want to show that I and (2) are prime ideals. We claim that 2 is prime. Suppose $2 \mid (a+b\sqrt{-3})(c+d\sqrt{-3}) = ac-3bd+(ad+bc)\sqrt{-3}$. □

Exercise 2.3. Complete the proof of Corollary 2, Theorem 1.

Proof. We'll start with finishing the proof of Corollary 2. We have that for $\alpha = r + s\sqrt{m}$, $r, s \in \mathbb{Q}$, for $s \neq 0$, the monic irreducible polynomial over $\mathbb{Q}$ having α as a root is

$$x^2 - 2rx + r^2 - ms^2.$$

Hence, α is an algebraic integer if and only if $2r$ and $r^2 - ms^2$ are integers. Now if m is squarefree, then we must have $m \equiv 1, 2, 3 \pmod 4$. □

Exercise 2.4.

Exercise 2.5. Show that if f is any polynomial over $\mathbb{Z}_p$ (p a prime) then $f(x^p) = (f(x))^p$. (Suggestion: Use induction on the number of terms.)

Proof. Recall that the binomial formula gives us for $f, g \in \mathbb{Z}_p[x]$, $(f+g)^p = f^p + g^p$. Induction gives us the result. □

Exercise 2.6. Show that if f and g are polynomials over a field K and $f^2 \mid g$ in $K[x]$, then $f \mid g'$. (Hint: Write $g = f^2 h$ and differentiate)

Proof. If $f^2 \mid g$ in $K[x]$, then we can write $g = f^2 h$. By the product rule and chain rule, we get $g' = 2ff'h + f^2 h'$ so that $g' = f(2f'h + fh')$. Hence, $f \mid g'$. □