1. Find a monic polynomial $f(x)$ with integer coefficients such that $f(\sqrt{3} + \sqrt{5}) = 0$.

**Ans:** One could solve this as on p. 188, but computing some powers of $\sqrt{3} + \sqrt{5}$ and looking for a relationship among them is probably easier. So we compute

\[
(\sqrt{3} + \sqrt{5})^2 = 8 + 2\sqrt{15}
\]
\[
(\sqrt{3} + \sqrt{5})^4 = 124 + 32\sqrt{15}.
\]
Thus we choose the monic polynomial $x^4 - 16x^2 + 4$.

2. Suppose that $\alpha$ is an algebraic integer, and that $f(x) = x^m + a_{m-1}x^{m-1} + \cdots + a_1x + a_0$ is the monic polynomial of lowest degree satisfied by $x$. Prove that $\alpha^{-1}$ is an algebraic integer if and only if $a_0 = \pm 1$.

**Ans:** In both directions, we’ll use that $\alpha^{-1}$ is a zero of $a_0x^m + a_1x^{m-1} + \cdots + a_{m-1}x + 1$,

which follows from multiplying the equation $0 = f(\alpha) = \alpha^m + \cdots + a_1\alpha + a_0$

by $\alpha^{-m}$.

$\Leftarrow$ If $a_0 = \pm 1$, then the equation shows that $\alpha^{-1}$ is an algebraic integer.

$\Rightarrow$ ?

3. An algebraic integer $\alpha$ is said to have *degree at most* $m$ if it satisfies a monic polynomial with integer coefficients having degree $m$. Suppose that $\alpha$ has degree at most $m$, and $g$ is any polynomial with integer coefficients. Prove that $g(\alpha)$ is an algebraic integer of degree at most $m$.

**Ans:** This is shown on p. 188, where we set $\beta = 1$ and $\omega = g(\alpha)$.

4. (Denominators for algebraic numbers.) Suppose that $\beta$ is a complex number, $f$ is a non-zero polynomial with rational coefficients, and that $f(\beta) = 0$. Prove that there is a positive integer $d$ such that $d\beta$ is an algebraic integer. (That is, any algebraic number is an algebraic integer divided by a positive ordinary integer.) Explain how to find a possible $d$ by inspection of the polynomial $f$.

**Ans:** Let $f(x) = r_0x^n + r_1x^{n-1} + \cdots + r_{n-1}x + r_n$. Multiplying $f$ by the least common multiple of the denominators, we get a polynomial $g(x)$ with integer coefficients and which is satisfied by $\beta$. Let $d$ denote the new leading coefficient. Then $d\beta$ is an algebraic integer, as can be seen by multiplying $g(x)$ by $d^{n-1}$ and substituting $\beta$ for $x$. So $d$ is the product of the least common multiple of the denominators with the leading coefficient. It’s easy to see by example that no smaller $d$ in general will work, for instance, $2x - \frac{1}{3}$.
5. In the axioms for a ring given on page 182 of the text, the axiom $a \times 0 = 0$ is listed. Prove that this fact is a consequence of the other axioms (and therefore it should not be listed as an axiom).

**Ans:** We start with

\[
(1) \quad a \times 0 = a \times (1 + -1) \\
(2) \quad = a \times 1 + a \times (-1) \\
(3) \quad = a + (-a) \\
(4) \quad = 0.
\]

Equation 1 follows from the additive inverse property applied to 1.

1 ⇒ 2 follows from the distributive law.

2 ⇒ 3 follows from the identity property of 1 and the definition of $-a$. (Some people would use $-a$ to simply mean “the additive inverse of $a$”, but here he must mean $-1 \times a$, otherwise the additive inverse axiom would have no content. But by $-1$, we do mean the additive inverse of 1.)

3 ⇒ 4 follows again from the additive inverse property.

6. Give an example of a non-commutative ring having exactly eight elements. (Hint: use matrices with entries in the field $\mathbb{Z}/2\mathbb{Z}$ of two elements. I think that rings having a smaller number of elements have to be commutative, but I would be entertained to be shown wrong.)

**Ans:** Consider the ring of $2 \times 2$ matrices with entries in $\mathbb{Z}/2\mathbb{Z}$ with lower-left entry 0. We have two choices for each of the three remaining entries, so this has eight elements. It is a subset of the ring of $2 \times 2$ matrices with entries in $\mathbb{Z}/2\mathbb{Z}$, and has the operations inherited from that ring, so to show that this set is a ring it suffices to show that it is closed under addition, subtraction and multiplication. But these are all obvious from the way matrix addition and multiplication are defined. (If we had chosen instead matrices with upper-left entry 0, then it wouldn’t be closed under multiplication.)

So, it remains to see that this ring is non-commutative.

\[
\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}.
\]