HW8 Sample Solution.

1. (13.7.) Note that if $a, b > 0$, then $(\sqrt{a} + sqrtb)^2 = a + b + 2\sqrt{ab}$, and taking square roots yields $\sqrt{a} + \sqrt{b} = \sqrt{a + b + 2\sqrt{ab}}$. Similarly $\sqrt{a} - \sqrt{b} = \sqrt{a + b - 2\sqrt{ab}}$.

Using this with $a = 9, b = 2$ yields $\sqrt{9} + \sqrt{2} = \sqrt{11 + 6\sqrt{2}}$. Using this with $a = 5, b = 2$ yields $\sqrt{5} - \sqrt{2} = \sqrt{7 - 2\sqrt{10}}$. Using this with $a = 9, b = 5$ yields $\sqrt{9} - \sqrt{5} = \sqrt{14 - 6\sqrt{5}}$.

Thus the numbers in parts (a) and (c) simplify to $3 + \sqrt{2} - \sqrt{5}$, while the number in (b) simplifies to $3 - \sqrt{2} + \sqrt{5}$. Since it is given that two answers are correct, it follows that (a) and (c) are correct. The simpler form is $3 + \sqrt{2} - \sqrt{5}$,

2. (15.2.) Suppose that $a > 0$ has a square root b in $\mathbb{F}$. If $b = 0$, then $a = b^2 = 0$, which is false, so b is positive or negative. The number $-b$ is the opposite, and $(-b)^2 = b^2 = a$, showing that a has both a positive and a negative square root, namely b and $-b$. This shows that a has at least two square roots.

Could there be another square root, c? If so, then $c^2 = a = b^2$, so $0 = c^2 - b^2 = (c-b)(c+b)$, from which it follows that $c = \pm b$. This shows that a has exactly two square roots, one positive and one negative.

3. We are asked to show that $x = \sqrt{1 + \sqrt{2}}$ satisfies a nonzero integer polynomial of degree four, but does not satisfy a nonzero integer polynomial of degree less than four.

To find a polynomial of degree 4 with x as a root, we simplify $x = \sqrt{1 + \sqrt{2}}$:

$$\begin{aligned} x &= \sqrt{1 + \sqrt{2}} \\ x^2 &= 1 + \sqrt{2} \\ x^2 - 1 &= \sqrt{2} \\ (x^2 - 1)^2 &= 2 \\ (x^2 - 1)^2 - 2 &= 0 \\ x^4 - 2x^2 - 1 &= 0. \end{aligned}$$

To show that there is no rational polynomial of smaller degree that has $\sqrt{1 + \sqrt{2}}$ as a root it suffices to show that the integer polynomial $x^4 - 2x^2 - 1$ cannot be factored into **integer** polynomials of smaller degree. It cannot be factored into (integer linear)(integer cubic), since it has no rational root (use the Rational Root Theorem). To see that it cannot be factored into (integer quadratic)(integer quadratic) note that any such factorization can be adjusted to $(x^2 - ax + 1)(x^2 + ax - 1)$. But if $a \neq 0$ the product will have a nonzero linear term, while if $a = 0$ the quadratic term will be 0. Neither case works, so there is no factorization.