Clearly, the minimal polynomial is quite a powerful concept. Let's just look at a few more properties it has.

**Proposition 20.** Suppose $L/K$ is a field extension, and that $\omega \in L$ is algebraic over $K$. Suppose $p(X)$ is a polynomial with coefficients in $K$. Then $p(\omega) = 0$ iff $m(X)|p(X)$, where $m(X)$ is the minimal polynomial of $\omega$.

**Proof.** Let's first show that if $m(X)|p(X)$, then $p(\omega) = 0$. By the assumption that $m(X)|p(X)$, we have $p(X) = q(X)m(X)$ for some $q(X)$. Then, if we plug in $X = \omega$, we see $p(\omega) = q(\omega) \cdot 0$ (remembering $m(\omega) = 0$). Thus we are done in this direction.

Now, let's imagine that $p(\omega) = 0$. We know that $m(X)$ and $p(X)$ must have an hcf; and as before, the fact that $m(X)$ is irreducible tells us that we can take either $h(X) = m(X)$ or $h(X) = 1$ as an hcf.

If $h(X) = 1$, then we can write $1 = a(X)m(X) + b(X)p(X)$ for some polynomials $a(X)$ and $b(X)$; plugging in $X = \omega$, we see $1 = 0$, a contradiction. (Remember $p(\omega) = m(\omega) = 0$)

So we are forced to conclude that $h(X) = m(X)$. But then, since $h(X)|m(X)$ since its a highest common factor of $m(X)$ and $p(X)$, we have shown what we were asked to show. □

**Corollary 21.** Suppose $L/K$ is a field extension, and that $\omega \in L$ is algebraic over $K$. Suppose that $m(X)$ and $m'(X)$ are two different minimal polynomials for $\omega$. Then they are associates.

**Proof.** Since $m(\omega) = 0$, we see that $m'(X)|m(X)$. The same argument gives that $m(X)|m'(X)$. Thus they are associates. □

**Corollary 22.** Suppose $L/K$ is a field extension, and that $\omega \in L$ is algebraic over $K$. Any irreducible polynomial $p(X) \in K[X]$ which $\omega$ satisfies must be a minimal polynomial.

**Proof.** Suppose $p(X) \in K[X]$ is such a polynomial, and let $m(X)$ be a minimal polynomial for $\omega$. Then $m(X)|p(X)$. But $p(X)$ is irreducible, so $m(X)$ is a constant polynomial or an associate of $p(X)$. But it can't be a unit (otherwise $\omega$ wouldn't satisfy it), so $m(X)$ and $p(X)$ are associates, and so have the same degree. So $p(X)$ is a polynomial which $\omega$ satisfies, which has the same degree as $m(X)$, which is the minimal degree. Thus we are done. □

**Corollary 23.** Suppose $L/K$ is a field extension, and that $\omega \in L$ is algebraic over $K$. There is only one monic minimal polynomial for $\omega$. (A polynomial is called monic if the coefficient of the biggest power of $X$ is 1.)

**Proof.** If $m(X)$ and $m'(X)$ are both monic minimal polynomials for $\omega$, then (by the previous-but-one corollary) they are associates, i.e. $m'(X) = km(X)$ for some constant $k$. Comparing leading terms, we see that $k = 1$. □

Sometimes, we call the unique monic minimal polynomial for $\omega$ just 'the minimal polynomial' for $\omega$. We shall close out this section of the course with a few examples, using Prop 19 to quickly figure out the degrees of a few extensions.

**Example 24.** Let's figure out the degree $[\mathbb{Q}(\sqrt{11})_{\mathbb{R}} : \mathbb{Q}]$. First, we can easily see that $\omega = \sqrt{11}$ is irrational the same way we see $\sqrt{2}$ is—technically, this is called ‘Theatetus’ theorem’. Thus it does not satisfy any linear polynomial (otherwise it would be rational). But it does satisfy a quadratic polynomial. Thus the minimal polynomial of $\sqrt{2}$ is quadratic, and $[\mathbb{Q}(\sqrt{11})_{\mathbb{R}} : \mathbb{Q}] = 2$.

**Example 25.** Let’s figure out the degree $[\mathbb{Q}(\sqrt[3]{2})_{\mathbb{R}} : \mathbb{Q}]$. First, $\omega = \sqrt[3]{2}$ satisfies the cubic polynomial $X^3 + 2 = 0$. If we can show this polynomial is irreducible, then it must be the minimal polynomial for $\omega$, and so $[\mathbb{Q}(\sqrt[3]{2})_{\mathbb{R}} : \mathbb{Q}] = \deg X^3 + 2 = 3$. If it were not irreducible, it would factorize, and at least one of the factors would be linear. That means that the polynomial $X^3 + 2 = 0$ would have a rational solution. But then $a^3 = 2b^3$ for some integers $a, b$, a contradiction.