

Simply irreducible!

We've now seen that irreducibles are quite interesting: they play the same role in polynomial rings what primes play in \mathbb{Z} .

Therefore it's an interesting question to ask how we might find irreducible elements easily. One way in which a polynomial can fail to be irreducible is if it has a root; in this case, we saw that the Division Algorithm allows us to factor the polynomial nontrivially in this case.

But when are we guaranteed to have roots? Here's a simple first result:

Theorem (Corollary 3.65). If k is a field and $f \in k[x]$ has degree at most 3, then f is irreducible if and only if f has no roots in k .

Proof. This is a follow-your-nose proof if I ever saw one!:

Example. Find an example of a polynomial in $\mathbb{Z}[x]$ with degree 4 which is not irreducible but still has no root.

From here on we'll focus on $\mathbb{Z}[x]$ and $\mathbb{Q}[x]$, for reasons which will become more obvious as we continue. A slightly more sophisticated means of finding roots might remind you of something you did back in Precalc:

Theorem (Rational Root Theorem; 3.90). Let

$$f(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{Z}[x] \subseteq \mathbb{Q}[x].$$

Every rational root of f has the form $\frac{p}{q}$ where $p|a_0$ and $q|a_n$.

Example. Use the RRT to find all roots of the polynomial $f(x) = 6x^3 - 11x^2 - 3x + 2$.

Here's something you didn't do in Precalc!:

Proof. Take a root $\frac{p}{q}$, assumed to be reduced so that $(p, q) = 1$. Plug it in and clear denominators in the resulting expression.

What results if we solve for the term involving a_0 ?

What if we solve for the term involving a_n ?

Your textbook distinguishes what it calls _____ *integers*: $\alpha \in \mathbb{C}$ is such a number if it is the root of a monic polynomial in $f \in \mathbb{Z}[x]$.

Corollary (3.91). If an _____ integer α is rational, then $\alpha \in \mathbb{Z}$.

Proof. The proof is so short that it'll likely be shorter than this here sentence!:

Before we move on to our next substantial root finding techniques, we need to build up a few lemmas based on the following

Definition. Given $f \in \mathbb{Z}[x]$, f is called _____ if the greatest common divisor of its coefficients is 1.

Examples. Obviously, every _____ polynomial is _____. More generally, how can you modify a given polynomial $f \in \mathbb{Z}[x]$ so that the result is _____?

Gauss's Lemma (3.92). The product of two _____ polynomials is _____.

Proof. Let $f(x) = \sum a_i x^i$, $g(x) = \sum b_j x^j$, and $f(x)g(x) = \sum c_k x^k$. Then BWOC suppose that some prime p divides into all of the c_k s. What if a_i and b_j are the smallest of their respective terms into which p does *not* divide?

Lemma (3.93). Every $f \in \mathbb{Q}[x]$, $f(x) \neq 0$, has a unique factorization $f(x) = c(f)f^\#(x)$, where $c(f) \in \mathbb{Q}^+$ and $f^\#(x) \in \mathbb{Z}[x]$ is primitive.

We call $c(f)$ the _____ of the polynomial f .

Proof. First clear the denominators in f 's coefficients, and then divide by the right number to make sure the result is primitive. Let $f(x) = \sum \left(\frac{a_i}{b_i}\right) x^i$ and show how this can be done!

What, then, is $c(f)$? And what is $f^\#(x)$?

That's all well and good, but why are these guys *unique*? Well, let's say we've got $c(f)f^\#(x) = eh(x)$ where $e \in \mathbb{Q}^+$ and $h \in \mathbb{Z}[x]$ is primitive. If we let $\frac{e}{c(f)}$ have lowest-terms representation $\frac{u}{v}$, can you figure out how to show that $u = v = 1$, and thus that $e = c(f)$ and $h(x) = f^\#(x)$ both hold?

It's not too hard to show that both the "content operation" c and the "primitivizing operation" $\#$ are both "homomorphic":

Corollary (3.95). For $f, g \in \mathbb{Q}[x]$, $c(fg) = c(f)c(g)$ and $(fg)^\# = f^\#g^\#$.

On the next handout we'll look at two more sophisticated means of testing irreducibility based on the coefficients of the given polynomial.