

Euclid's Lemma and Algorithm, and Then Some!

Let's start off with a proposition that likely looks familiar (trading the word "irreducible" for another 'p' word):

Proposition (3.66). Let k be a field. Then every nonconstant $f(x) \in k[x]$ has a factorization

$$f(x) = ap_1(x) \cdots p_t(x)$$

where each $p_i(x)$ is a monic irreducible polynomial and $a \in k$, $a \neq 0_k$.

Proof. Let's prove this by induction on $\deg(f)$. (This is really just a "follow your nose" proof.)

Now what's the only thing separating the above proposition from the Fundamental Theorem of Arithmetic, which dealt with integers instead of polynomials?

We can remedy this difference once we're armed with a couple of easy lemmas:

Lemma (3.67). If k is a field, $p, f \in k[x]$, and $d = \gcd(p, f)$, then if $p(x)$ is a monic irreducible polynomial then

$$d(x) = \begin{cases} 1 & \text{if } p \nmid f \text{ and} \\ p(x) & \text{if } p \mid f. \end{cases}$$

Proof. What are the only monic divisors of p ? What does this say about our possibilities for d ?

Theorem (Euclid's Lemma, 3.68). Let k be a field and let $f, g \in k[x]$. If p is a monic irreducible polynomial and $p \mid fg$, then either $p \mid f$ or $p \mid g$. More generally, if $p \mid f_1 f_2 \cdots f_n$, then $p \mid f_i$ for some i .

Proof. For the case in which $n = 2$, use the above lemma: when $p \nmid f$, what's that say about $\gcd(p, f)$?

Thus if $p \nmid f$, we can write 1 as a linear combination of p and f . Use this fact to show that $p|g$:

For the general case, induct! Here's some room to finish it off:

At last, we're in a position to obtain

Theorem (Euclid's Algorithm, 3.71). There is an algorithm which, given a field k and polynomials $f, g \in k[x]$, computes $d(x) = \gcd(f, g)$ and finds $s, t \in k[s]$ such that $d = sf + tg$.

Proof. This is identical to the proof of Euclid's algorithm for integers, using our updated Division Algorithm instead of the "classical" one. \diamond

Example. Apply the algorithm to find $(3x^2 - 12, 5x^3 + 6x^2 - 9x - 2)$ in $\mathbb{Q}[x]$.