

Uniqueness of Factorization

Well, we can now do it: we can prove a full generalization of the Fundamental Theorem of Arithmetic for polynomial rings over fields:

Theorem (3.84). If k is a field, then every $f \in k[x]$ of degree at least 1 is a product of a nonzero constant and monic irreducible polynomials. Moreover, any such a product representations is unique up to a permutation of the monic irreducible terms. That is,

$$ap_1(x)p_2(x)\cdots p_m(x) = bq_1(x)q_2(x)\cdots q_n(x) \Rightarrow a = b, m = n, \text{ and for all } i, p_i = q_{\pi(i)}$$

for some permutation π of the set $\{1, 2, \dots, m\}$.

Proof. This is really just a coupling of facts we already know (for existence) and an easy induction (for uniqueness):

Of course, as soon as we replace k by a more general ring, things go haywire:

Example. Find two different monic polynomials in $\mathbb{Z}_8[x]$, each of which can be factored in two utterly different ways.

Those rings in which uniqueness of factorization *does* hold are known (perhaps not too surprisingly!) as UFDs *domains*. Your textbook has a nice “aside” on such domains on pages 276–277.

Just as is the case in \mathbb{Z} , unique factorizations are useful beasts:

Proposition (3.86). Let k be a field and let $f(x) = ap_1^{s_1}(x) \cdots p_n^{s_n}(x)$, $g(x) = ap_1^{t_1} \cdots p_n^{t_n} \in k[x]$. Let $m_i = \min\{s_i, t_i\}$ and $M_i = \max\{s_i, t_i\}$ for all $i = 1, \dots, n$. Then

$$\gcd(f, g) = p_1^{m_1}(x) \cdots p_n^{m_n}(x) \quad \text{and} \quad p_1^{M_1}(x) \cdots p_n^{M_n}(x).$$

Proof. Let’s show the first formula is true; it’s really just a matter of checking the definition of (f, g) :

Sometimes decomposition as a product of monic irreducibles isn’t *exactly* what’s wanted. Perhaps instead we’d like to write a given polynomial g in terms of “digits” relative to some “base”:

Theorem (Lemma 3.87). Let k be a field, and let $b(x) \in k[x]$ have degree at least 1. Then for any $g \in k[x]$, there exist polynomials $d_0, d_1, \dots, d_m \in k[x]$ such that for every i either $d_i = 0$ or $\deg(d_i) < \deg(b)$, and

$$g(x) = d_0(x) + d_1(x)b(x) + d_2(x)(b(x))^2 + \cdots + d_m(x)(b(x))^m.$$

Proof. This is just a repeated application of the Division Algorithm, to first obtain d_0 , and then the others by induction: