Math 5320

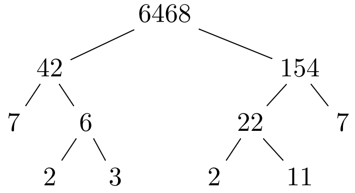
The “factoring terminates” property of UFD’s

Factoring terminates in the integers Suppose I want to factor the number 6468 into prime factors (the irreducible elements of $\mathbb{Z}$), and I go about it by finding two factors (neither of them a unit) that multiply to 6468, and then finding two factors of each of those factors, and so on, stopping when I find primes, for instance:

$$6468 = 42 * 154 = (7 * 6) * (22 * 7) = (7 * (2 * 3)) * ((2 * 11) * 7)$$

Even though I’m not going about finding factors in any “organized” way (like first factoring out powers of 2, then 3, etc), I still get to a prime factorization after finitely many steps. This is what it means for $\mathbb{Z}$ to have the property that “factorization terminates”.

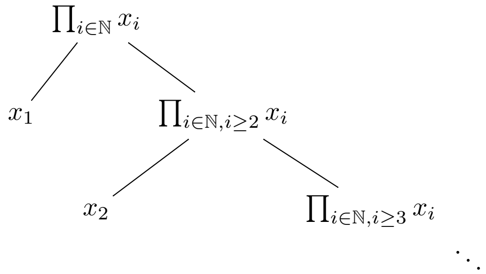
We can envision this factorization process more graphically in a way that looks like roots stretching out under a tree. Every time we find a proper factorization into a product of two elements, the roots bifurcate and goes down another level.



What the “factoring terminates” property says in general is that no matter how I choose the factors at each stage, each part of the root system will go down only finitely many levels before it arrives at irreducible factors.

A hand-wavy discussion of a non-example This would be a good point to introduce an example of a ring in which factoring doesn’t necessarily terminate. But examples of such rings are pretty out of the ordinary – factorization not terminating is a stronger condition than being non-Noetherian (you don’t need to know what this is now, but I’ll just say that a lot of algebraists don’t deal regularly with rings that aren’t Noetherian, so by the time we’re dealing with a non-Noetherian ring, we’re generally considered to be already pretty far out into badly-behaved-example-land, and factorization not terminating is even further out).

However, I’ll try to give a very hand-wavy discussion: Suppose we’re in a ring with polynomials in infinitely many variables: $x_1, x_2, x_3, \ldots$ AND that it contains the product of all of them: $\prod_{i \in \mathbb{N}} x_i$. If I try to factor $\prod_{i \in \mathbb{N}} x_i$ by successively breaking it into products of two things, I’ll never be done. Put another way, it’s possible to make a diagram with the factorizations like the one above that goes down infinitely many levels:


$\prod_{i \in \mathbb{N}} x_i$
x_1
$\prod_{i \in \mathbb{N}, i \geq 2} x_i$
x_2
$\prod_{i \in \mathbb{N}, i \geq 3} x_i$
$\ddots$

NOTA BENE: This discussion is totally informal and there are several aspects of it that might be misleading that I’ll try to point out here. First, it’s possible to form the polynomial ring $R[x_1, x_2, \ldots]$ with coefficients in a ring R and containing variables indexed by $\mathbb{N}$, but this ring doesn’t contain the product $\prod_{i \in \mathbb{N}} x_i$ because rings are closed under finite products, but not infinite ones, so constructing an example of a ring where factorization doesn’t terminate isn’t as easy as that. Second, I don’t want to lead you into thinking that rings where factorization doesn’t terminate are rings that necessarily contain infinite products of irreducibles. The key property here is that it’s possible to produce a factorization tree that goes down infinitely many levels. This could happen in an example where we’re factoring a product of finitely many irreducibles, but it's possible to produce a sequence of proper factorizations that gets somehow closer and closer to the irreducibles but doesn't ever arrive at them.

Factorization terminating in $\mathbb{Z}[x]$ We know that factorization terminates in $\mathbb{Q}[x]$. We also know that the irreducibles of $\mathbb{Z}[x]$ consist of prime integers and primitive polynomials that are irreducible in $\mathbb{Q}[x]$.

Suppose (with the aim of finding a contradiction) that factorization doesn't terminate in $\mathbb{Z}[x]$. That means there is some element $p(x) \in \mathbb{Z}[x]$ and a factorization of it like described above that doesn't terminate after finitely many steps. These factorizations in $\mathbb{Z}[x]$ are also factorizations in $\mathbb{Q}[x]$, but we haven't found our contradiction yet because proper factorizations in $\mathbb{Z}[x]$ aren't necessarily proper in $\mathbb{Q}[x]$. However, a proper factorization $f(x) = g(x)h(x)$ in $\mathbb{Z}[x]$ is not proper in $\mathbb{Q}[x]$ if and only if one of the factors is an integer other than 1. Our factoriztion of $p(x)$ can only have finitely many such proper factorizations because otherwise an infinite product of integers would divide $p(x)$, which is impossible because an integer divides $p(x)$ if and only if it divides the gcd of the coefficients of $p(x)$ and factorization terminates in $\mathbb{Z}$. So, our factorization of $p(x)$ with infinitely many steps is only not proper in $\mathbb{Q}[x]$ at finitely many steps, which still leaves a factorization with infinitely many steps in $\mathbb{Q}[x]$, giving us the contradiction we want.