Ideal-theoretic characterization of irreducibility

written by rapha on Functor Network
original link: https://functor.network/user/2593/entry/1043

Recall that in an **irreducible element** in an integral domain A is a non-zero, non-unit element that admits no decomposition as the product of two non-unit elements. In particular, irreducible elements in polynomial rings are called **irreducible polynomials**; examples include $x^2 + y^2$ in $\mathbb{R}[x, y]$, and $x + iy$ or $y^2 - x$ in $\mathbb{C}[x, y]$.

Ideal-theoretic characterization of irreducibility. Let A be an integral domain. An element $f \in A$ is irreducible if, and only if, the ideal (f) is non-zero, and is maximal among the principal ideals of A. More precisely, we have $(0) < (f) < A$, and if $a \in A$ is any element such that $(f) \leq (a)$, then either $(f) = (a)$ or $(a) = A$.

(Proof is a good exercise, easy & omitted.)

Recall that in any integral domain, two elements are **relatively prime** if, whenever d divides both elements (i.e. is a common divisor), then d is a unit. It's not too hard to show the following "ideal-theoretic" characterization of this concept: in an integral domain A, the elements f and g are relatively prime if, and only if, $(f, g) \leq (d)$ implies $(d) = A$.

Proposition. Let A be an integral domain, and let f and g be two irreducible elements in A. Either $(f) = (g)$, or f and g are relatively prime.

Proof. Let d be a common divisor of f and g. Then f and g are both elements of (d), hence $(f) \leq (d)$ and $(g) \leq (d)$. Because f and g are irreducible, either $(f) = (d)$ and $(g) = (d)$, or $(d) = A$. In the first case, we obtain $(f) = (g)$. In the second case, we obtain that d is a unit, whence f and g are relatively prime. ■

Corollary. Let A be a unique factorization domain with fraction field K. Suppose f and g are two relatively prime polynomials in $A[x]$, and that g is non-constant and irreducible. Then the inclusions of f and g in the larger ring $K[x]$ are relatively prime polynomials.

Proof. By the previous proposition, it suffices to show that $(f) \neq (g)$ as ideals in $K[x]$. Suppose on the contrary that the ideals are equal, so that $f = pg$ for some $p \in K[x]$. We may put all monomials in $p(x)$ over the same denominator and write $p = (1/\alpha)q$ for some non-zero $\alpha \in A$ and some $q \in A[x]$. Hence we have the equation $\alpha f = gq$ in $A[x]$. In particular, this means $\alpha f \in (g)$. Because $A[x]$ is a UFD, the ideal (g) generated by an irreducible element is prime, so either $\alpha \in (g)$ or $f \in (g)$. Since the latter is impossible by relative primality, we must have that g divides α in $A[x]$. But α is a non-zero constant, so g is a constant polynomial as well. This contradicts our hypothesis that g was non-constant. ■

Notice that by Gauss' Lemma on polynomials, the polynomial g of the previous corollary is irreducible in $K[x]$ as well.

EDIT A way better proof is made in a more recent post.