Relative primality of polynomials over a UFD is preserved over the fraction field

written by rapha on Functor Network
original link: https://functor.network/user/2593/entry/1047

First attempt and proof

Let A be a UFD and write K for its fraction field; write $\phi : A[x] \to K[x]$ for the canonical inclusion of rings. My goal is to show that any polynomials that are relatively prime in $A[x]$ continue to be relatively prime polynomials as elements of $K[x]$.

Take two non-zero, non-unit polynomials f and g in $A[x]$. Because we are working in a UFD, they both admit a unique prime factorization:

$$f = f_1 f_2 \cdots f_n, \qquad g = g_1 g_2 \cdots g_m,$$

where each f_i and g_i are irreducible polynomials. Suppose that $\phi(f)$ and $\phi(g)$ are *not* relatively prime in $K[x]$; we will show that in this case f and g are also *not* relatively prime in $A[x]$.

Notice that if all f_i's were constants, then $\phi(f)$ would be invertible, contrary to our hypothesis that $\phi(f)$ and $\phi(g)$ are not relatively prime; the same argument shows that at least one of the g_i's is not a constant. Since for our purposes it suffices to exhibit a common irreducible factor, we can, without loss of generality, suppose that *none* of the f_i's and g_i's are constant polynomials.

By Gauss' Lemma on polynomials, all of the $\phi(f_i)$'s and $\phi(g_i)$'s are irreducible polynomials in $K[x]$. Let h be an irreducible factor of $\phi(f)$ and $\phi(g)$. We must have $h = \phi(f_i)$ and $h = \phi(g_j)$ for some indices i and j. Because ϕ is an injective function, this yields $f_i = g_j$. Hence f and g share an irreducible factor, so they are not relatively prime. ■

EDIT In fact, this does not yield $f_i = g_j$, but only that f_i divides g_j. This is still sufficient for the proof to conclude.

Second attempt and proof

The resultant gives a better result and proof, in my opinion. As before, let A be a UFD and write K for its fraction field. Let f and g be two polynomials in $A[x]$, with respective degrees n and m, both degrees ≥ 1. Recall that their

resultant is

$$R(f,g) = \det \begin{pmatrix} a_0 & a_1 & \dots & a_{n-1} & a_n & & & \\ & a_0 & a_1 & \dots & a_{n-1} & a_n & & \\ & & \ddots & & & & & \\ & & & a_0 & \dots & a_{n-1} & a_n \\ b_0 & b_1 & \dots & b_{m-1} & b_m & & \\ & b_0 & b_1 & \dots & b_{m-1} & b_m & \\ & & \ddots & & & & \\ & & & b_0 & \dots & b_{m-1} & b_m \end{pmatrix}$$

where each a-line is repeated m times and each b-line repeated n times in order to get a square matrix. Now it is a nice and simple fact (see for instance *Algebraic Curves*, Walker 1991, p.24) that $R(f,g)$ is zero if and only if f and g have a common non-constant factor, i.e. if and only if f and g are not relatively prime in $A[x]$. But the vanishing of $R(f,g)$ is independant of wether we consider its matrix as a matrix with coefficients in A, or with coefficients in K. In other words, the resultant of f and g seen as polynomials in $A[x]$ vanishes if and only if the resultant of f and g seen as polynomials in $K[x]$ vanishes. ■

Let me be a bit more precise. Let f and g be two generic polynomials of positive degrees n and m, respectively. Write $f = a_0 + a_1 x + \cdots + a_n x^n$ and $g = b_0 + b_1 x + \cdots + b_n x^n$. Now their resultant is a polynomial in the $n + m$ variables a_0, b_0, a_1, b_1, etc. Let $\phi : A[x] \to K[x]$ be the injective canonical map of rings. Because ϕ is injective, we must have that $R(f,g)$ vanishes at some point (f_0, g_0) if and only if the image of the polynomial $R(f,g)$ in $K[x]$ vanishes at $(\phi(f_0), \phi(g_0))$.

To conclude: two *non-constant* polynomials in $A[x]$ are relatively prime in $A[x]$ if and only if their images are relatively prime in $K[x]$; and if two *arbitrary* polynomials in $A[x]$ are relatively prime in $A[x]$, then their images are also relatively prime in $K[x]$ (for instance, 2 and 4 are relatively prime in $\mathbb{Q}[x]$ but not in $\mathbb{Z}[x]$, so for the converse implication to work we really need both polynomials to be non-constant).

EDIT This is Theorem 9.5, p.25 in Walker's *Algebraic Curves* (1991).