Polynomials over UFD's

Let R be a UFD and let K be the field of fractions of R. Our goal is to compare arithmetic in the rings $R[x]$ and $K[x]$. We introduce the following notion.

Definition 1. *A non-constant polynomial $p \in R[x]$ is called* **primitive** *if any common divisor of all the coefficients of p is invertible in R. Equivalently, $p = p_0 + p_1x + ... + p_nx^n$ is primitive iff $\gcd(p_0, p_1, ..., p_n) = 1$.*

Example: The polynomial $6x^5 - 12x^3 + 5x$ is primitive in $\mathbb{Z}[x]$, but the polynomial $6x^5 - 12x^3 + 4x$ is not primitive.

The following simple observation will be very useful.

Lemma 1. *Let $f \in K[x]$ be a non-constant polynomial. There exists $k \in K$, $k \neq 0$ such $kf \in R[x]$ is primitive.*

Proof: Let $f = f_0 + f_1x + ... + f_nx^n$. There exists $a \in R$, $a \neq 0$ such that $af \in R[x]$ (if $f_i = b_i/a_i$, where $a_i, b_i \in R$, then $a = a_0a_1...a_n$ works). Let $d = \gcd(af_0, af_1, ..., af_n)$. Then $\gcd(af_0/d, af_1/d, ..., af_n/d) = 1$. In other words, af/d is primitive, i.e. $k = a/d$ works. $\square$

The key observation is the following result.

Theorem 1. *Let $\pi \in R$ be an irreducible element. Then π is a prime element in the ring $R[x]$.*

Proof: Since R is a UFD, π is a prime element of R. In order to prove that π is prime in $R[x]$ we need to prove that $\pi R[x]$ is a prime ideal. Note that a polynomial $h \in R[x]$ belongs to $\pi R[x]$ iff every coefficient of h is divisible by π.

Consider the canonical homomorphism $\phi : R \longrightarrow R/\pi R$. As we know, it extends to the homomorphism $\phi : R[x] \longrightarrow (R/\pi R)[x]$ defined by $\phi(f_0 + f_1x + ... + f_nx^n) = \phi(f_0) + \phi(f_1)x + ... + \phi(f_n)x^n$. By the very definition of ϕ, a polynomial f is in the kernel of ϕ iff $\phi(f_0) = ... = \phi(f_n) = 0$, i.e. iff all coefficients of f are divisible by π. Thus $\ker \phi = \pi R[x]$. Since πR is a prime ideal of R, the ring $R/\pi R$ is an integral domain and therefore so is the ring $(R/\pi R)[x]$. Thus the kernel of ϕ is a prime ideal. In other words, $\pi R[x]$ is a prime ideal of $R[x]$, so π is a prime element in $R[x]$. $\square$

As a corollary we get the following important result.

Gauss Lemma. *Let $f, g \in R[x]$ be primitive polynomials. Then fg is also primitive.*

Proof: Suppose that fg is not primitive. Thus there is a non-invertible $a \in R$ which divides all coefficients of fg. Let π be an irreducible divisor of a. Then $\pi | fg$. By Theorem 1, π is a prime element of $R[x]$, so $\pi | f$ or $\pi | g$. Neither case is possible since both f and g are primitive. The contradiction shows that fg is primitive. $\square$

As a corollary we get the following fundamental result:

Theorem 2. *Let $f, g \in R[x]$. Suppose that f is primitive and $g = fh$ for some $h \in K[x]$. Then $h \in R[x]$. In other words, if $f|g$ in $K[x]$ then $f|g$ in $R[x]$.*

Proof: Let $k \in K$, $k \neq 0$ be such that $kh \in R[x]$ is primitive. Since $kg = f \cdot (kh)$, we get by Gauss' Lemma that $kg \in R[x]$ is primitive. Let $g = g_0 + g_1 x + ... + g_m x^m$ so $kg_i \in R$ for $i = 0, ..., m$. We may write $k = a/b$ for some $a, b \in R$ such that $\gcd(a, b) = 1$. We see that $b | ag_i$ for $i = 0, 1, ..., m$. Since $\gcd(a, b) = 1$, we conclude that $b | g_i$ for $i = 0, 1, ..., m$. But then $kg_i = a(g_i/b)$ is divisible by a for $i = 0, 1, ..., m$. On the other hand , kg is primitive so a must be invertible in R. It follows that $h = ba^{-1}(kh) \in R[x]$. $\square$

Corollary 1. *Let $g = g_0 + g_1 x + ... + g_m x^m \in R[x]$. Suppoce that $a, b \in R$ are relatively prime and $g(a/b) = 0$ (i.e. a/b is a root of g in K). Then $a | g_0$ and $b | g_m$.*

Proof: Let $f(x) = bx - a$. Then $f \in R[x]$ is primitive, since a, b are relatively prime. Since $g(a/b) = 0$, we have $f(x) | g(x)$ in $K[x]$. By Theorem 2, $g(x) = h(x)f(x)$ for some $h = h_0 + h_1 x + ... + g_{m-1} x^{m-1} \in R[x]$. It follows that $g_0 = -h_0 a$ and $g_m = h_{m-1} b$, so $b | g_m$ and $a | g_0$. $\square$

In particular, if $R = \mathbb{Z}$ then we get a very efficient way to check if a given polynomial with integer coefficients has a rational root.

Another useful corollary is the following result.

Proposition 1. *Let $f \in R[x]$ be monic. Suppose that $g, h \in K[x]$ are monic and $f = gh$. Then $f, g \in R[x]$.*

Proof: Let $k, t \in K$ be non-zero elements such that kg, th are primitive. Since g, h are monic, both k and t are in R. By Gauss Lemma, the polynomial $(kg)(th) = (kt)f$ is primitive so kt, being a divisor of all coefficients of $(kt)f$, is a unit in R. Thus both k and t are invertible in R and therefore both g and h are in $R[x]$. $\square$

Remark. Proposition 1 is true for any R which is integrally closed, but the proof is a bit more involved.

We are able now to compare irreducible elements in $R[x]$ and $K[x]$.

Theorem 3. *An element $f \in R[x]$ is irreducible iff either f is an irreducible (in R) constant or f is primitive and irreducible in $K[x]$.*

Proof: Suppose first that f is irreducible in $R[x]$. If f is a constant, then clearly it must be irreducible in R (R and $R[x]$ have the same invertible elements). Suppose $\deg f > 0$. Then f is primitive since it is irreducible (recall that primitive simply means that f does not have any constant divisors which are not invertible). If $f = gh$ in $K[x]$, let $k \in K$ be such that $kg \in R[x]$ is primitive. We have $f = (kg)(k^{-1}h)$. Since kg is primitive, we have $k^{-1}h \in R[x]$ by Theorem 2. Thus we factored f as a product $(kg)(k^{-1}h)$ of two elements in $R[x]$. Since f is irreducible in $R[x]$, one of these two factors is constant. It follows that either g or h is constant so f is irreducible in $K[x]$.

Conversely suppose that either f is an irreducible in R constant or f is primitive and irreducible in $K[x]$. In the latter case f is irreducible in $R[x]$ by Theorem 1. In the former case, if $f = gh$ for some $g, h \in R[x]$ then one of g, h is constant since f is irreducible in $K[x]$. We may assume that g is constant. But then g divides all the coefficients of $gh = f$. Since f is primitive, g must be invertible constant in R. This shows that either g or h is invertible in $R[x]$, so f is irreducible in $R[x]$. $\square$

We prove now the following very important result.

Theorem 4. *Let R be a UFD. Then $R[x]$ is also a UFD.*

Proof: Let K be the field of fractions of R. Note that, by Lemma 1, every polynomial in $K[x]$ is associated with a primitive polynomial in $R[x]$. Since $K[x]$ is a UFD, every non-zero, non constant polynomial f in $K[x]$ can be factored as

$kp_1...p_m$, where $k \in K$ and $p_1, ..., p_m \in R[x]$ are primitive and irreducible in $K[x]$. By Theorem 3, each p_i is irreducible in $R[x]$. Suppose now that $f \in R[x]$. Since $p_1...p_m$ is primitive by Gauss' Lemma, the constant k belongs to R by Theorem 2. Thus k factors as a product of elements irreducible in R (since R is a UFD), which remain irreducible in $R[x]$ by Theorem 1. This shows that f factors in $R[x]$ into a product of irreducible elements. That any two such factorizations are equivalent is a rather easy consequence of unique factorization in $K[x]$. Alternatively, it suffices now to show that every irreducible element $p \in R[x]$ is prime. If p is constant, this follows from Theorem 1. If it is not constant, p is primitive and irreducible in $K[x]$, hence prime in $K[x]$. Suppose that $p|fg$ for some $f, g \in R[x]$. Then in $K[x]$, either $p|f$ or $p|g$. By Theorem 2, this means that $p|f$ are $p|g$ in $R[x]$, so p is indeed a prime element in $R[x]$. $\square$

Application. As an application of the ideas developed above, we will describe all rational numbers q such that $\cos(q\pi)$ is rational. Since cos has period 2π and satisfies $\cos(2\pi - x) = \cos x$, it suffices to describe such q in the interval $[0, 1]$.

Let $q = m/n$. Consider the complex number $z = \cos(q\pi) + i\sin(q\pi)$. By De Moivre's Theorem, $z^{2n} = \cos(2m\pi) + i\sin(2m\pi) = 1$. Similarly, $\overline{z}^{2n} = 1$, where $\overline{z} = \cos(q\pi) - i\sin(q\pi)$. In other words, z and $\overline{z}$ are roots of the polynomial $x^{2n} - 1$. It follows that the polynomial $f(x) = (x-z)(x-\overline{z}) = x^2 - 2\cos(q\pi) + 1$ divides $x^{2n} - 1$ in $\mathbb{C}[x]$. By our assumption, $f \in \mathbb{Q}[x]$. We want to show that $f|x^{2n} - 1$ in $\mathbb{Q}[x]$. By division algorithm, $x^{2n} - 1 = gf + r$ for some $g, r \in \mathbb{Q}[x]$ and $\deg r \leq 1$ It follows that in $\mathbb{C}[z]$ we have $f|r$ which is possible only if $r = 0$. Thus $x^{2n} - 1 = gf$ and $g \in \mathbb{Q}[x]$. Let $0 < k \in \mathbb{Q}$ be such that $kf \in \mathbb{Z}[x]$ is primitive. Then by Theorem 2, $k^{-1}g \in \mathbb{Z}[x]$. Since $x^{2n} - 1$ is monic, both kf and $k^{-1}g$ must be monic. But the leading coefficient of kf is k, so $k = 1$. This proves that $f \in \mathbb{Z}[x]$. We proved that if $\cos(q\pi)$ is rational then $2\cos(q\pi)$ is an integer. It follows that $2\cos(q\pi) \in \{-2, -1, 0, 1, 2\}$, i.e. $\cos(q\pi) \in \{-1, -1/2, 0, 1/2, 1\}$. This corresponds to $q\pi \in \{\pi, 2\pi/3, \pi/2, \pi/3, 0\}$ (recall that we have assumed $q \in [0, 1]$), i.e. $q \in \{1, 2/3, 1/2, 1/3, 0\}$. We see that $\cos(q\pi)$ is a rational number iff $q = 2m \pm r$, where $m \in \mathbb{Z}$ and $r \in \{1, 2/3, 1/2, 1/3, 0\}$.

Final remark: We proved above that if R is a UFD then so is $R[x]$. In particular, $\mathbb{Z}[x]$ is a UFD. We have seen some time ago that $\mathbb{Z}[x]$ is not a PID (for example, the

ideal $< 2, x >$ in $\mathbb{Z}[x]$ is not principal - prove it). The class of UFD's is therefore larger than the class of PID's. In fact it is substantially larger. There is a a notion of dimension for rings, analogous to the notion of dimension for topological spaces. In this theory fields have dimension 0 and PID's have dimension 1 (but not all one-dimensional rings are PID's). On the other hand, there are UFD's of arbitrary large dimension. In fact, a polynomial ring in n variables over a field has dimension n and is a UFD by Theorem 4. One should think of UFD's as very regular objects among all the rings, as smooth manifolds are among topological spaces. But there is a wealth of important rings which are not UFD's and it is the subject of commutative algebra and algebraic geometry to investigate these rings. And beyond the world of commutative ring there is a vast universe (or universes) of non-commutative rings about which our knowledge is not as extensive, but huge progress has been made in recent years in conquering important classes of non-commutative rings.