21-237: Math Studies Algebra I November 21, 2022

Lecture 32 : Uniquely Factorizing Polynomials

Lecturer: James Cummings

Scribe: Rajeev Godse

1 Polynomial rings over UFDs are UFDs

Theorem: If R is a UFD, then $R[x]$ is a UFD.

Proof: Recall that for a field K, $K[x]$ is a Euclidean domain, and thus a PID and UFD.

The units of $K[x]$ are exactly $K \setminus \{0\}$. In $K[x]$, all polynomials of degree one are irreducibles. Up to associates, these are linear terms of the form $x - a$ for a unique $a \in K$.

Cautionary tale: $x^2 + 1$ is irreducible in $\mathbb{R}[x]$ but can be factored into $(x + i)(x - i)$ in $\mathbb{C}[x]$.

For UFD R, let K be the field of fractions of R. Note that $R \subseteq R[x] \subseteq K[x]$ and $R, K[x]$ are UFDs.

The units of $R[x]$ are the units of R. So for $r \in R$, r irreducible in $R \iff r$ irreducible in $R[x]$, as r can only be factored into degree-0 polynomials in $R[x]$.

Cautionary tale: When $R = \mathbb{Z}$, $K = \mathbb{Q}$, $2x$ is reducible in R but not in K. The reason for this confusing behavior is that 2 is a unit in $\mathbb{Q}$, but not in $\mathbb{Z}$.

Let $f \in R[x]$, $f \neq 0$. Then, we say that the **content** of f, denoted $C(f)$, is a gcd of the coefficients of f. We say f is **primitive** if $C(f)$ is a unit, or equivalently if there is no prime p of R which divides all coefficients of f.

Gauss's Lemma: If $f, g \in R[x]$ are primitive, then fg is primitive.

Proof: Assume there is prime $p \in R$ such that $p \mid fg$ in $R[x]$. (p) is a prime ideal in R since R is ID, and then $R/(p)$ is ID.

Let $\phi_{(p)} : R \to R/(p)$ be the quotient map. $\phi_{(p)}$ induces a coefficient-wise HM $\phi'_{(p)} : R[x] \to (R/(p))[x]$.

See that $\phi'_{(p)}(f)\phi'_{(p)}(g) = \phi'_{(p)}(fg) = 0$. Since $R/(p)$ is ID, $(R/(p))[x]$ is ID, so $\phi'_{(p)}(f)$ or $\phi'_{(p)}(g)$ is 0 and thus, f or g is primitive. $\square$

For any non-zero $f \in R[x]$, we can write $f = C(f)f_0$ where f_0 is primitive.

Fact: For $f \in R[x]$, if $\deg(f) > 0$ and f is irreducible, then f is primitive.

Proof: If f is not primitive, i.e. $C(f)$ is non-unit, then we can write $f = C(f)f_0$ and $\deg(f_0) > 0$, so f_0 is non-unit. $\square$

Fact: It can be proved that if $f \in R[x]$ irreducible and $\deg(f) > 0$, f is irreducible in $K[x]$.

Proof idea: If $f = gh$ in $K(x)$, the coefficients of g and h are fractions over R. Use the irreducibility of f in R to show that g or h must be unit.

Fact: If $f \in R[x]$, f primitive, $\deg(f) > 0$ and f irreducible in $K[x]$, then f is irreducible in $R[x]$.

Fact: Let $f \in K[x]$, $f \neq 0$. Then f has an associate in $K[x]$ that is a primitive polynomial in $R[x]$.

Proof: Since each coefficient of f is a fraction a/b, $a, b \in R$, $b \neq 0$, we can find $D \in R$, $D \neq 0$, $Df \in R[x]$. Let $c = C(Df)$. Then, $(D/c)f \in R[x]$ is primitive. $\square$

To finish (to be proven next lecture), given $g \in R[x]$, a non-zero non-unit, we want to factor it uniquely. If $\deg(g) = 0$, just use "R is a UFD." If $\deg(g) > 0$, $g = C(g)g_0$. $C(g)$'s unique factorization in R is its unique factorization in $R[x]$.

So it's the primitive polynomial g_0 that poses the issue, but we can start by factoring it in $K[x]$. Up to associates, we get a unique factorization into primitive polynomials of $R[x]$.