Lecture 5: Which polynomial rings are UFDs?

Previously on Math 418: Euclidean \( \Rightarrow \) PID \( \Rightarrow \) UFD.

For a field \( F \), the ring \( F[x] \) is Euclidean with norm \( N(p(x)) = \deg p \).

For a non-field \( R \), the ring \( R[x] \) is not a PID, since \( (x) \) is prime but not maximal. \( (R[x]/(x) \cong R) \)

Today: When is \( R[x] \) a UFD?

Note \( R \subseteq R[x] \) as the constant polynomials, and if \( p(x), q(x) \in R \) then \( p, q \in R \). So \( R[x] \) a UFD \( \Rightarrow \) \( R \) a UFD. [Turns out this sufficient!]

Consider \( p \in \mathbb{Z}[x] \). In \( \mathbb{Q}[x] \), \( p \) factors into irreducibles; would like those to be in \( \mathbb{Z}[x] \).

Ex:
\[
X^2 + 5x + 6 = (\frac{1}{2}x + 1)(2x + 6) = (x + 2)(x + 3)
\]

Can we always do this? Yes!

[Want to try this approach for a general \( R \).]
For an integral domain $R$, its field of fractions is

$$F = \left\{ \frac{a}{b} \mid a, b \in R, \ b \neq 0 \right\} / \frac{a}{b} \sim \frac{c}{d} \text{ iff } ad = bc.$$  

Can often think concretely: $\mathbb{Z}[i] \subseteq \mathbb{Q}(i) = \{a + bi \mid a, b \in \mathbb{Q}\}$

**Gauss' Lemma:** If $p \in R[x]$ is reducible in $F[x]$, then it is reducible in $R[x]$. Specifically, if $p = AB$ with $A, B \in F[x]$ non-constant, then $\exists f \in F$ with $a = f \cdot A$ and $b = \frac{1}{f} B$ in $R[x]$; thus $p = ab$.

**Cor.** Factorization in $\mathbb{Z}[x]$ is nearly the same as in $\mathbb{Q}[x]$.

**Note:** $2x$ factors in $\mathbb{Z}[x]$ as $2 \cdot x$ but is inert in $\mathbb{Q}[x]$.

**Key idea:** $p(x) = x^2 + 5x + 6 = (\frac{1}{2}x + 1) (2x + 6) = A \cdot B$

So $2p = (x + 2)(2x + 6)$ in $\mathbb{Z}[x]$

Reduce modulo $I = (2)$, i.e. look in $\mathbb{Z}[x]/(2) = \left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)[x]$ and see $0 = x \cdot 0$ and

and see $0 = x \cdot 0$ and

so at least one of $A, B$ is $0$ in $\mathbb{F}_2[x]$. 
Hence, all coefficients of the factor \((B)\) are divisible by 2. So \(p(x) = (x+2)(x+3)\). \(\uparrow\) just notation. \(\nabla\) not a derivative.

Proof: Pick \(r, s \in \mathbb{R}\) so that \(a'(x) = r A(x)\) and \(b'(x) = s B(x)\) are in \(\mathbb{R}[x]\). Set \(d = rs\) so that

\[ dp(x) = a'(x) b'(x) \]

If \(d\) is a unit in \(\mathbb{R}\), take \(a(x) = d^{-1} A(x)\) and \(b(x) = B(x)\). Otherwise, consider a factorization \(d = q_1 \cdots q_n\) into indeps.

Consider \(\mathbb{R}[x] / (q_1) = \overline{\mathbb{R}[x]}\) where \(\overline{\mathbb{R}} = \mathbb{R} / (q_1)\) is an integral domain (indeps are prime in a UFD).

In \(\overline{\mathbb{R}}[x]\) we have

\[ 0 = \overline{d} \overline{p}(x) = \overline{a}'(x) \overline{b}'(x) \Rightarrow \overline{a}'(x) = 0 \text{ or } \overline{b}'(x) = 0 \]

Say \(\overline{a}'(x) = 0\). Then \(a'(x) = q_1 a''(x)\) and

\[(q_2 q_3 \cdots q_n) p(x) = a''(x) b'(x)\]
Repeating reduces the number of factors of \( d \) until we’re done.

Next time: \( R[x] \) is UFD iff \( R \) is.

Cor: \( R \) is a UFD. Then \( R[x_1, x_2, \ldots, x_n] \) is a UFD.

Interestingly even when \( R = \text{field} \) as applies to \( \mathbb{Q}[x,y] \) which is not a P.I.D.

Irreducibility Criteria: [Probably won’t get to.]

\( \underbrace{p(x) - \text{monic poly in } R[x]}_{\rightarrow} - \text{non-const.} \Rightarrow p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \)

If \( p \) factors, can take the factors to be monic too

\[
p(x) = (a_kx^k + \cdots)(b_lx^l + \cdots) \Rightarrow a_k b_l = 1
\]

so divide though by \( a_k \) and \( b_l \).

\( I \neq R \) an ideal.

Test: If \( \overline{p}(x) \) is irreducible in \( (R/I)[x] \) then \( p(x) \) is irreducible in \( R[x] \).

Ex: \( x^2 + x + 1 \in \mathbb{Z}[x] \quad I = 2\mathbb{Z} \).