Lecture 5: Which Polynomial Rings are U.F.D.s?

The story so far: Euclidean $\Rightarrow$ PID $\Rightarrow$ U.F.D.

For a field $F$, the ring $F[x]$ is Euclidean with

\[ N(p(x)) = \text{deg } p. \]

For a non-field $R$, the ring $R[x]$ is not a P.I.D.,
since $(x)$ is a prime ideal which isn't maximal

\[ (R[x]/(x) \cong R). \]

E.g., \( R = \mathbb{Z}, \mathbb{Z}[i], \mathbb{Z}[\sqrt{-5}], \ldots \)

Q: When is $R[x]$ a UFD?

Since only const polys can mult to give a const
poly, $R$ must be a UFD if $R[x]$ is. [In fact,
the converse is also true!]

Consider $p \in \mathbb{Z}[x]$. In $\mathbb{Q}[x]$, know that $p$
is a prod of irreducible $q_1 \cdots q_n$. If $q_i \in \mathbb{Z}[x]$ this
would give the needed factorization. Example:

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

Can we always do this step??
Let \( R \) be an integral domain. Recall that its field of fractions is
\[
F = \left\{ \frac{a}{b} \mid a, b \in R, b \neq 0 \right\} / \frac{a}{b} \sim \frac{c}{d} \text{ iff } ad = bc.
\]

[For any UFD \( R \) could try to use fact. in \( F[x] \).]

**Gauss' Lemma:** \( R \) a UFD w/ field of frac. \( F \).

\( \text{If } p \in R[x] \text{ is reducible in } F[x] \text{ it is red. in } R[x] \).

Specifically if \( p = A \cdot B \text{ in } F[x] \text{ with } A, B \text{ non-const.} \)

then \( \exists r, s \in R \text{ with } a = rA, b = rB \text{ in } R[x] \text{ and } p = ab. \)

\( \text{ i.e.: Factorization in } \mathbb{Z}[x] \text{ is nearly the same as in } \mathbb{Q}[x]. \)

**Note:** \( 2x \text{ factors in } \mathbb{Z}[x] \text{ into } 2, x \text{ but is irreducible in } \mathbb{Q}[x]. \)

**Idea Behind Gauss:**

\[
p(x) = x^2 + 5x + 6 = \left( \frac{1}{2}x + 1 \right) \left( 2x + 6 \right) = A(x) \cdot B(x).
\]

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

Reduce mod \( I = (2) \), i.e. look at \( \mathbb{Z}[x]/(2) = (\mathbb{Z}/2\mathbb{Z})[x] = \mathbb{F}_2[x]. \)
and get so one of the right-hand factors must be 0, i.e., every coefficient is divisible by 2.

So \( p(x) = (x+2)(x+3) \)

**Proof:** Pick \( r, s \in \mathbb{R} \) so that \( a'(x) = r a(x) \) and \( b'(x) = s b(x) \) are in \( R[x] \). Set \( d = rs \). So that \( d p(x) = a'(x) b'(x) \). If \( d \) is a unit, take \( a(x) = d^{-1} a'(x) \) and \( b(x) = b'(x) \). Otherwise consider a factorization \( d = q_1 \cdots q_n \) into irreducibles.

Consider \( R[x]/(q_i) = \overline{R}[x] \) where \( \overline{R} = R/(q_i) \) is an unit domain (reason: in a UFD, irrebs are prime). In \( \overline{R}[x] \) we have

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

Say \( \overline{a'}(x) = 0 \). Then \( a'(x) = q, a''(x) = b(x) \) and

\[
(q \cdot q_3 \cdots q_n) p(x) = a''(x) \cdot b'(x)
\]

Repeating reduces the number of factors of \( d \) until we're done.
Next time: \( R[x] \) is a U.F.D. if \( R \) is.

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

This is interesting even when \( R = \) field as \( \mathbb{Q}[x, y] \) is not a PID.

**Irreducibility Criteria:**

\[ p(x) \text{ - monic poly in } R[x], \text{ monic constant.} \]
\[ \implies p(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_0 \]

If \( p(x) \) factors, then it does so into monic factors

\[ p(x) = (a_1 x^k + \ldots) (b_2 x^l + \ldots) \quad a_k b_2 = 1 \]

So divide by \( a_k \) and \( b_2 \).

\( I \neq R \) an ideal.

**Test:** \( c \bar{I} | p(x) \) is irreducible in \( (R/I)[x] \) then \( p(x) \) is irreducible in \( R[x] \). \( [Pf \text{ is clear}] \)

Why useful? \( (R/I)[x] \) is "smaller" and it can be easier to decide irreducible there. \( \text{Ex: } x^2 + x + 1 \in \mathbb{Z}[x] \)

\[ I = 2\mathbb{Z}. \]