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 <u>not</u> a PID, since (x) is prime but not maximal.

$\left(R[x]/(x) \cong R \right)$

<u>Today</u>: When is $R[x]$ a UFD?

Note $R \subseteq R[x]$ as the const polynomials, and if $p(x) \cdot q(x) \in R$ 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:

$$x^2 + 5x + 6 = \left(\tfrac{1}{2}x + 1\right)(2x+6) = (x+2)(x+3)$$

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

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

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

<u>Gauss' Lemma</u>: R a UFD with field of fractions F.
If $p \in R[x]$ is reducible in $F[x]$, then it is reducible in $R[x]$. Specifically, if $p = A \cdot B$ with $A, B \in F[x]$ nonconst, then $\exists f \in F$ with $a = f \cdot A$ and $b = \frac{1}{f} B$ in $R[x]$; thus $p = ab$.

<u>Cor.</u> Factorization in $\mathbb{Z}[x]$ is <u>nearly</u> the same as in $\mathbb{Q}[x]$.

<u>Note</u>: $2x$ factors in $\mathbb{Z}[x]$ as $2 \cdot x$ but is irred in $\mathbb{Q}[x]$.

<u>Key idea</u>: $p(x) = x^2 + 5x + 6 = \left(\frac{1}{2}x + 1\right)(2x+6) = A\,B$

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

Reduce modulo $I = (2)$, i.e. look in $\mathbb{Z}[x]/(2) = (\mathbb{Z}/2\mathbb{Z})[x]$

and see $0 = x \cdot 0$ and $= \mathbb{F}_2[x]$.

so at least one of A, B is 0 in $\mathbb{F}_2[x]$.

Hence, all coeff of that factor (B) are divisible by 2. So $p(x) = (x+2)(x+3)$.

just notation, not a derivative

Proof: Pick $r, s \in R$ so that $a'(x) = rA(x)$ and $b'(x) = sB(x)$ are in $R[x]$. Set $d = rs$ so that

$$d\,p(x) = a'(x)\,b'(x)$$

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

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

In $\bar{R}[x]$ we have

$$0 = \bar{d}\,\bar{p}(x) = \bar{a}'(x)\,\bar{b}'(x) \Rightarrow \begin{array}{c} \bar{a}'(x) = 0 \\ \text{or} \\ \bar{b}'(x) = 0 \end{array}$$

Say $\bar{a}'(x) = 0$. 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. $\square$

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.

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

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

$p(x)$ - monic poly in $R[x]$, non-const.

$\hookrightarrow p(x) = x^n + a_{n-1}x + \cdots + a_1 x + a_0$

If p factors, can take the factors to be monic too

$$p(x) = (a_k x^k + \ldots)(b_\ell x^\ell + \ldots) \Rightarrow \underbrace{a_k b_\ell}_{\text{units}} = 1$$

so divide though by a_k and b_ℓ.

$I \subsetneq R$ an ideal.

Test: If $\bar{p}(x)$ is irred in $(R/I)[x]$ then $p(x)$ is irred in $R[x]$.

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