Lecture 5: Which Polynomial Rings are U.F.Ds?

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

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 P.I.D., since (x) is a prime ideal which isn't maximal $\left(R[x]/_{(x)} \cong R\right)$.

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 irred $q_1 \cdots q_n$. If $q_i \in \mathbb{Z}[x]$ this would give the needed factorization. Example:

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

Can we always do this step?

Let R be an integral domain. Recall that its field of fractions is

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

[For any UFD R could try to use fact. in $F[x]$.]

<u>Gauss' Lemma:</u> R a UFD w/ field of fracs F.
If $p \in R[x]$ is reducible in $F[x]$ it is red. in $R[x]$.

Specifically if $p = A \cdot B$ in $F[x]$ with A, B non const then $\exists\, r, s \in R$ with $a = rA$, $b = rB$ in $R[x]$ and $p = ab$.

<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 $\mathbb{Z}[x]$ into $2 \cdot x$ but is irred in $\mathbb{Q}[x]$.

<u>Idea Behind Gauss:</u>

$$p(x) = x^2 + 5x + 6 = \left(\tfrac{1}{2}x + 1\right)(2x + 6) = A(x)\,B(x)$$

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

Reduce mod $I = (2)$, i.e. look at $\mathbb{Z}[x]/(2) = (\mathbb{Z}/2\mathbb{Z})[x] = \mathbb{F}_2[x]$.

and get

$$0 = x \cdot 0$$

so one of the right-hand factors must be 0, i.e. every coeff is divisible by 2.

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

<u>Proof</u>: Pick $r, s \in R$ 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 $a(x) = d^{-1} \cdot a'(x)$ and $b(x) = b'(x)$. Otherwise consider a factorization $d = q_1 \cdots q_n$ into irreducibles.

Consider $R[x]/(q_1) = \bar{R}[x]$ where $\bar{R} = R/(q_1)$ is an int. domain (Reason: in a UFD, irreds are prime). In $\bar{R}[x]$ we have

$$0 = \bar{d}\,\bar{p}(x) = \bar{a}'(x)\,\bar{b}'(x) \implies \bar{a}'(x) = 0 \text{ or } \bar{b}'(x) = 0$$

Say $\bar{a}'(x) = 0$. Then $a'(x) = q_1\, a''(x)$ and

$$(q_2 \cdot q_3 \cdots q_n)\, p(x) = a''(x) \cdot b'(x)$$

Repeating reduces the number of factors of d until we're done. ∎

Next time: $R[x]$ is a U.F.D. iff R is.

Cor: R a UFD. Then $R[x_1, x_2, \dots, x_n]$ is a UFD.

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

Irreducibility Criteria:

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

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

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

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

So divide 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 $R[x]$. [Pf is clear.]

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

$I = 2\mathbb{Z}$.