

## Lecture 21 Which polynomial rings are UFDs?

①

Previously on Math 500: 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 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:

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

[Want to try this approach for a general  $R$ .] Can we always do this? Yes!

For an integral domain  $R$ , its field of fractions is ②

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

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

Gauss' Lemma:  $R$  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  $p = a \cdot b$ .

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 irred 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  $\mathbb{Z}[x] / (2) = (\mathbb{Z}/2\mathbb{Z})[x]$

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  $p(x) = (x+2)(x+3)$ . 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, so are  $r$  and  $s$ . Then  $A(x) = r^{-1} a'(x)$  and  $B(x) = s^{-1} b'(x)$  were in  $R[x]$  already. Otherwise, consider a factorization  $d = q_1 \cdots q_n$  into ined.

Consider  $R[x] / (q_1) = \bar{R}[x]$  where  $\bar{R} = R / (q_1)$

is an integral domain (ined are prime in a UFD).

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

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

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. ④  
□

Next time:  $R[x]$  is UFD iff  $R$  is.

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

Interesting 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.]

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

$$\hookrightarrow p(x) = x^n + a_{n-1}x + \dots + a_1x + a_0$$

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

$$p(x) = (a_k x^k + \dots)(b_l x^l + \dots) \Rightarrow \underbrace{a_k b_l}_{\text{units}} = 1$$

so divide through by  $a_k$  and  $b_l$ .

$I \neq R$  an ideal.

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

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