Lecture 22 R[x] is a UFD when R is.

Gauss's Lemma: R a UFD with field of fractions F. If $p(x)$ in $R[x]$ factors in $F[x]$ into nonconst polys as $p(x) = A(x)B(x)$, then $\exists f \in F$ such that $a(x) = fA(x)$ and $b(x) = f^{-1}B(x)$ are in $R[x]$. Hence $p = a \cdot b$ and is reducible in $R[x]$.

Today: **Thm:** $R[x]$ is a UFD if and only if R is a UFD.

Cor: If R is a UFD, so is $R[x_1, x_2, \ldots, x_n]$.

Caveat: $2x+2$ is reducible ($= 2(x+2)$) in $\mathbb{Z}[x]$ (← const poly)
but irreducible in $\mathbb{Q}[x]$

Cor of Gauss: R a UFD with field of fractions F. If the gcd of the coeffs of $p \in R[x]$ is 1, then p factors in $R[x]$ iff it does in $F[x]$.

Pf: [Assume p is non-const.] By gcd condition any factorization of p in $R[x]$ has non-const factors, and hence is also a factorization in $F[x]$.

<u>Proof of Thm:</u> ($\Rightarrow$) Discussed last time

($\Leftarrow$) Suppose R is a UFD, and let $p \in R[x]$ be nonconst. Can assume gcd(coeffs) = 1. By Gauss and the fact that $F[x]$ is a UFD, get

$$p(x) = q_1(x) \cdots q_n(x) \quad \text{where } q_i(x) \in R[x] \text{ are non-const and irreducible over } F[x].$$

Each q_i must have gcd(coeffs) = 1 since p does, and hence is irred in $R[x]$. So p has a factorization into irreducibles.

<u>Uniqueness:</u> Suppose $p = q_1' \cdots q_m'$ is some other fact. in $R[x]$ into irreducibles. As it is <u>also</u> a factorization in the UFD $F[x]$, have $n = m$ and can reorder so that q_i and q_i' are associates, i.e. $\exists\, a_i, b_i \in R$ with $q_i = \frac{a_i}{b_i} q_i'$. Then $b_i q_i = a_i q_i' \in R[x]$ and gcd(coeffs of $b_i q_i$) = b_i and gcd(coeffs of $a_i q_i'$) = a_i. Now gcd's are defined up to units, and so $a_i = u_i b_i$. Thus $q_i = u_i q_i'$ and so q_i and q_i' are associates in $R[x]$ as well. ▨

Irreducibility Criteria:

Q: How do we test whether $p \in F[x]$ is reducible? (F: field)

Prop: If $\deg p \le 3$ then p is red. $\Longleftrightarrow$ p has a root in F.

Pf: ($\Rightarrow$) If p is red, then one factor must be linear $= (ax+b)$ and so $c = -b/a$ is a root.

($\Leftarrow$) If $c \in F$ is a root, divide (Euclidean domain!) to get $p(x) = q(x)(x-c)+r$ where $r \in F$. Plugging in $x=c$ gives $r=0$, and so p factors. ▨

This is more useful for $F = \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ than for $F = \mathbb{Q}$.

Prop: Suppose $p(x) \in \mathbb{Z}[x]$ is monic, i.e. $p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$. Then p has a root in $\mathbb{Q}$ iff it has one in $\mathbb{Z}$.

Proof: If p has a root in $\mathbb{Q}$, it has a linear factor $\underset{\text{Gauss}}{\Longrightarrow}$ has a linear factor over $\mathbb{Z}[x]$

$\Rightarrow$ Has a monic linear factor $\Rightarrow$ has a root in $\mathbb{Z}$. ▨

see (A) on next page.

(☆) If a monic poly factors in $R[x]$ it does so into monic factors:

$$x^n + a_{n-1}x^{n-1} + \cdots = (b_k x^k + b_{k-1}x^{k-1} + \cdots)(c_\ell x^\ell + \cdots)$$

$$\Rightarrow b_k c_\ell = 1 \Rightarrow \quad = (x^k + c_\ell b_{k-1} x^{k-1} + \cdots)(x^\ell + b_k c_{\ell-1} x^{\ell-1} + \cdots)$$

<u>Ex</u>: $x^3 - 3x - 1$ is irred in $\mathbb{Q}[x]$ since the only poss roots in $\mathbb{Z}$ are ± 1 and neither works.

<u>Prop</u>: R a ring, $I \subsetneq R$ an ideal. Suppose $p \in R[x]$ is a nonconst <u>monic</u> poly. If $\bar{p}(x)$ is irred in $(R/I)[x]$ then $p(x)$ is irred in $R[x]$.

Reasons we restrict to monic:

ⓐ $3x^2 + 3$ factors in $\mathbb{Z}[x]$ but is irreducible in $(\mathbb{Z}/7\mathbb{Z})[x]$.

ⓑ $2x^2 + 3x + 2$ factor in $\mathbb{Z}[x]$ as $(2x+2)(x+1)$ but is irred. in $(\mathbb{Z}/2\mathbb{Z})[x]$ as $\bar{p} = x$.

Could also require gcd(coeff) = 1 and $\deg \bar{p} = \deg p$.

Ex: $x^3 - 3x - 1$ is irred in $\mathbb{Z}[x]$ as in $(\mathbb{Z}/2\mathbb{Z})[x]$ it is $x^3 + x + 1$ which has no roots.

Not foolproof: $x^4 - 72x^2 + 4$ is irred in $\mathbb{Z}[x]$ but factors in $(\mathbb{Z}/n\mathbb{Z})[x]$ for any n.

Eisenstein's Crit: $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$. If $p \in \mathbb{Z}$ is a prime dividing all a_i and $p^2 \nmid a_0$ then f is irred in $\mathbb{Z}[x]$.

Pf. If $f = a \cdot b$ then have $x^n = \bar{a} \cdot \bar{b}$ in $\mathbb{F}_p[x]$. Thus both a and b have const term divisible by $p \Rightarrow p^2 | a_0$ a contradiction. $\square$