Lecture 6: $R[x]$ is a UFD if R is.

Last time:

Gauss' Lemma: R a UFD with field of fractions F. If $p(x) \in R[x]$ factors in $F[x]$ into non-const polys $p(x) = A(x)B(x)$, then $\exists f \in F$ s.t. $a(x) = fA(x)$ and $b(x) = f^{-1}b(x)$ are in $R[x]$. Hence $p(x) = a(x)b(x)$ and is reducible.

Today:

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

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

[Remember, even if R is a field, then $\uparrow$ is not a PID if $n \geq 2$]

Factorization in $\mathbb{Z}[x]$ vs. $\mathbb{Q}[x]$: $2x+2$ is irred over $\mathbb{Q}[x]$
$2(x+1)$ over $\mathbb{Z}[x]$.

Cor [of Gauss' Lemma]

R a UFD, F its field of fractions.

If the gcd of the coeffs of $p(x) \in R[x]$ is 1, then $p(x)$ factors in $R[x]$ iff it does in $F[x]$.

Proof of Thm: ($\Rightarrow$) Discussed last time.

($\Leftarrow$) Suppose R is a U.F.D. Let $p(x) \in R[x]$ be nonconst. Can assume $\gcd(\text{coeffs}) = 1$. By Gauss' Lemma and the fact that $F[x]$ is a U.F.D.,

$$p(x) = g_1(x) \cdots g_n(x) \text{ where } g_i(x) \in R[x] \text{ are nonconst and irreducible over } F[x].$$

Each g_i must have $\gcd(\text{coeffs}) = 1$ since p does, hence is irred in $R[x]$. So $p(x)$ has a fact. into irreducibles

Uniqueness: Suppose $p(x) = g_1'(x) \cdots g_m'(x)$ is some (nonconst, $\gcd(\text{coeffs}) = 1$) other factorization in $R[x]$, hence also one over $F[x]$.

As $F[x]$ is a U.F.D., have $n = m$ an can assume g_i and g_i' are associates, i.e. $\exists a_i, b_i \in R$ with $g_i = \frac{a_i}{b_i} g_i'$.

Then $b_i g_i = a_i g_i' \in R[x]$ and so $\gcd(\text{coeff LHS}) = b_i$, $\gcd(\text{coeff RHS}) = a_i$

Thus as gcds are def. up to units, have $a_i = u_i b_i$ for $u_i \in R$ a unit. Thus $g_i = u_i g_i'$ and so g_i and g_i' are assoc. in $R[x]$ as well.

Irreducibility Criteria:

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

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

Pf: If p is red, one factor must be linear $= (ax+b)$

$\Rightarrow$ $c = -b/a$ is a root.

If $c \in F$ is a root divide to get

$$p(x) = g(x)(x-c) + r \quad \text{where } r \in F.$$

Plugging in c on both sides gives $r = 0$, and so p factors. ▨

For $F = (\mathbb{Z}/p\mathbb{Z})$ this is more useful than $F = \mathbb{Q}$.

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

Proof: If $p(x)$ has a root in $\mathbb{Q}$ $\Rightarrow$ Over $\mathbb{Q}[x]$ has a linear factor $\Rightarrow$ Over $\mathbb{Z}[x]$ has a linear factor

(Gauss)

$\Rightarrow$ Has a monic linear factor over $\mathbb{Z}[x]$ $\Rightarrow$ has a root in $\mathbb{Z}$.

▨

See next page: ⊛

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

$$x^n + a_{n-1}x^{n-1} + \cdots + a_0 = (b_k x^k + b_{k-1}x^{k-1} + \cdots)(c_\ell x^\ell + \cdots)$$

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

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

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

Why restrict to monic? Two reasons:

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

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

Could also just worry about const term factors indep and insist that $\deg \bar{p}(x) = \deg p(x)$.

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.

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

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

Pf: If $p(x) = a(x)\,b(x)$, then in $(\mathbb{Z}/p\mathbb{Z})[x]$ have $x^n = \bar{a}(x)\,\bar{b}(x)$. Thus both a and b must have const terms divisible by p, contradicting $p^2 \nmid a_0$. ▨

Next time: Chap. 13.