Algebra I: Polynomial rings that are UFDs, Gauss' Lemma, irreducibility.

We saw: R int. domain $\Rightarrow$ $R[x]$ int. domain.

embeds in $F[x]$, F = field of fractions of R, $F[x]$ is a Euclidean domain.

Q: What can we learn about $R[x]$ by computing in $F[x]$?

Prop: (Gauss' Lemma):

R a UFD, Field of fracs F, $p(x) \in R[x]$.

Then p reducible in $F[x] \Rightarrow p$ reducible in $R[x]$.

More precisely, if

$p = AB$, A, B non const. polys $/F$,

$\exists$ non-zero $r, s \in F$: $rA = a$, $sB = b$. are in $R[x]$,

$p = a \cdot b$.

Pf: Consider the poly $A(x) \cdot B(x)$. Its coeffs. are in $F \Rightarrow$ quotients of elts of the UFD R.

Multiply by a common denominator of these coeffs to get

$d p(x) = a'(x) \cdot b'(x)$, where $a'(x), b'(x) \in R[x]$, $d \in R \setminus \{0\}$.

d unit $\Rightarrow$ prop. true with $a = d^{-1}a'$, $b = b'$.

If d isn't a unit, write it as a product of irreducibles in R,

$d = p_1 \cdots p_n$.

p_1 irred. $\Rightarrow (p_1)$ is a prime ideal $\Rightarrow$ (earlier prop) $p_1 R[x]$ prime in $R[x]$,

$(R/p_1R)[x]$ is an int. domain

Reduce: (*) $p = f(x) = a'(x)b'(x) \mod p_1$

$\rightsquigarrow 0 = \overline{a'(x)} \cdot \overline{b'(x)}$, in this int. domain (bar means image in the quotient ring)

$\Rightarrow$ one factor, say $\overline{a'(x)}$, is 0.

$\Rightarrow$ all coeffs of $a'(x)$ divis. by p_1, so $\frac{1}{p_1} a'(x) \in R[x]$.

ie, we can cancel a p_1 from both sides of (*) and still have an eq^n in $R[x]$.

Keep reducing in this way $\rightsquigarrow$ eq^n $p(x) = a(x) \cdot b(x)$, $a(x), b(x) \in R[x]$, $a(x), b(x)$ F-mult. of $A(x), B(x)$. ☐

Cor: R a UFD, F field of Frac., $p(x) \in R[x]$.

If the gcd of coeffs. of $p(x) = 1$, then

$p(x)$ irred. in $R[x] \iff p(x)$ irred. in $F[x]$.

In particular, $p(x)$ a monic poly irred. in $R[x]$

$\Rightarrow p$ irred. in $F[x]$.

Pf: By Gauss' Lemma: $p(x)$ red. in $F[x] \Rightarrow$ red. in $R[x]$.

Conversely, if gcd of coeffs $= 1$, and p is red, then

$p(x) = a(x)\,b(x)$ where neither a nor b is constant.

(as if $p = a \cdot b$, with $\deg(a) = 0$, say, then $a \in R$, a unit $\Rightarrow \exists\, q \in R$ irred. @ $q \mid a$ $\Rightarrow q \mid p(x)$ $\Rightarrow q \mid$ all coeffs of $p(x)$ $\Rightarrow$ gcd(coeffs) $\neq 1$ too. ☐)

This factorization $\Rightarrow p$ is red. in $F[x]$.

Th^m: R UFD $\iff R[x]$ UFD

($R[x]$ UFD $\Rightarrow$ coeffs are $\Rightarrow R$ UFD. Converse: R UFD, F = f.o.f rac.)

Pf (Sketch): Suppose R is a UFD, F = f.o.f rac.

Let $p(x) \in R[x] \neq 0$, unit. Want to show: $p(x)$ has a unique factorization into irred.

WLOG, $p \neq$ const. (otherwise use R UFD) $\Rightarrow \deg(p) > 0$.
WLOG, gcd of coeffs $= 1$ (else factor out gcd) and can factor that.
Factor $p(x) = p_1(x) \cdots p_r(x)$ in $R[x]$. Clearly each p_i ($F[x]$ is a UFD) ↖ Gauß' Lemma.
is ~~irred.~~ primitive, as p is. Gauß' Lemma $\Rightarrow$ p_i's are irred. in $R[x]$ ☒
(gcd=1) [See book for full pf (don't give full details).
uniqueness follows from uniqueness in $F[x]$. (tell class: see book).

Cor: R UFD $\Rightarrow R[x_1, \dots, x_n]$ UFD.
Pf: Induct on n.

Irred. criteria:

Prop: F field, $p(x) \in F[x]$. p has a factor of deg. $1 \Leftrightarrow p$ has a root in F.
Pf: p has factor deg. $1 \Rightarrow$ can write (as F is a field)
$p = (x-a) \cdot q(x) \Rightarrow p(a) = 0$.
$\Rightarrow a \in F$ a root.
Conversely, if $p(a) = 0$, Division alg in $F[x]$:
$p(x) = q(x) \cdot (x-a) + r$, $\deg r < 1 \Rightarrow \deg r =$ const.
plug in a: $p(a) = 0 = q(a) \cdot 0 + r = r \Rightarrow r = 0$
$\Rightarrow p = q(x) \cdot (x-a)$ ☒

Lemma: Poly of deg. 2 or 3 in a field is red. $\Leftrightarrow$ has a root in F.
Pf: From the prop, as reducible poly of deg 2,3 $\Leftrightarrow$ has a linear factor.

Rat'l roots Theorem: R UFD, F = f. of frac.
Let $p(x) = a_n x^n + \dots + a_1 x + a_0$, $a_i \in R$.
If $\frac{r}{s} \in F$ is in lowest terms, $p(\frac{r}{s}) = 0$, then
$r | a_0$, $s | a_n$. (If $p(x)$ is monic, any root of F must lie in R, divide a_0).

Pf: By hyp., $a_n(\frac{r}{s})^n + \cdots + a_1(\frac{r}{s}) + a_0 = 0$.

Multiply by $s^n \rightsquigarrow a_n r^n + a_{n-1} r^{n-1} s + \cdots + a_0 s^n = 0$.

$\Rightarrow a_n r^n = s(-a_{n-1} r^{n-1} - \cdots - a_0 s^{n-1}) \Rightarrow s \mid a_n r^n$

As $(s,r)=1$, $s \mid a_n$. Similarly, solving for $a_0 s^n$ shows $r \mid a_0$.

Ex: $x^3 + 3x + 3$ is irred. / $\mathbb{Q}$ (and hence / $\mathbb{Z}$ (Gauss' Lemma))

For only possible roots are $\pm 1, \pm 3$, none of these are roots

$x^4 + x^2 + 1$ has no rat'l roots, but is reducible;

it is $(x^2 + x + 1)(x^2 - x + 1)$.

Prop: Let I a proper ideal of int. dom. R, $p(x) \in R[x]$ non-constant & monic (usually consider maximal ideal) — irred. by rat'l roots Th $\neq$.

If the image of $p(x)$ in $R/I[x]$ can't be factored in $(R/I)[x]$ into two polys of smaller degree, then p is irred in $R[x]$.

Pf: Suppose p can't be factored in $(R/I)[x]$, but p is reducible in $R[x]$.

Then $p(x)$ has a factorization $p = a(x) \cdot b(x)$, $a, b \in R[x]$ monic and non-constant

(as prod of leading factors a leading factor $\Rightarrow$ leading factors of a decomp. are units, so can arrange to be 1).

By earlier prop, reducing coeffs. mod I gives a factorization in $(R/I)[x]$ with non-constant factors $\Rightarrow$ contradiction

(i.e. $\bar{p}(x) = \bar{a}(x) \cdot \bar{b}(x)$ and $\bar{a}, \bar{b}$ have deg ≥ 1 $\Rightarrow \bar{p}$ red. in $\bar{I}[x]$).

Ex: • x^2+x+1 is irred. $/\mathbb{F}_2$, hence $/\mathbb{Q}$.
Same for x^3+x+1

• x^3+2 factors mod 2, 3, 5 but is irred. mod 7.
$\Rightarrow$ irred. $/\mathbb{Q}$.

• x^4-72x^2+4 is irred. $/\mathbb{Z}[x]$ but is reducible mod every integer!!

Start here!

Eisenstein Criterion: R int. domain, P prime ideal.
$f = x^n + c_{n-1}x^{n-1} + \dots + c_0 \in R[x]$ monic poly of deg. $n \geq 1$.
If $c_0, \dots, c_{n-1} \in P$, $c_0 \notin P^2$, then $f(x)$ is irred. in $R[x]$
(hence in $F[x]$ by Gauss' Lemma).

Pf: ☹ Pf in book not quite right.
Suppose to the contrary that $f(x) = a(x)\,b(x)$,
$a = a_\ell x^\ell + \dots + a_0 \in R[x]$, $b = b_m x^m + \dots + b_0 \in R[x]$,
$1 \leq \ell \leq n-1$.
Since $a_0 b_0 = c_0 \in P$, we have either $a_0 \in P$ or $b_0 \in P$.
WLOG, $a_0 \in P$. Since $c_0 \notin P^2$, we have $b_0 \notin P$.
As $a_\ell b_m = 1 \notin P$, we have $a_\ell \notin P$.
Let j be the smallest int. $1 \leq j \leq \ell$ such that
$a_j \notin P$, so that $a_j \notin P$, but $a_0, a_1, \dots, a_{j-1} \in P$.
Since $c_j = a_j b_0 + a_{j-1} b_1 + \dots + a_0 b_j$, $a_j b_0 \notin P$,
(a_j, b_0 both not in P)
and $a_{j-1} b_1 + \dots + a_1 b_{j-1} + a_0 b_j \in P$, it follows
that $c_j \notin P$. But $j \leq \ell \leq n-1$ so this contradicts
our assumption that $c_0, c_1, \dots, c_{n-1} \in P$ ▨

Ex: $x^3 + 25x + 10x - 15$ irred $/\mathbb{Q}$ by Eisenstein @ $p = 5$.

- $f(x) = x^4+1$. Eisenstein doesn't apply directly, but.
  $g(x) = f(x+1) = x^4 + 4x^3 + 6x^3 + 4x + 2$
  is irred. by Eisenstein @ 2 $\Rightarrow$ f is irred.

- $\Phi_p(x) = \frac{x^p - 1}{x-1} = x^{p-1} + x^{p-2} + \cdots + x + 1$

  $\Phi_p(x+1) = \frac{(x+1)^p - 1}{x}$. Eisenstein applies by binomial theorem!

Prop: max ideals in $F[x]$ are exactly $(f(x))$ with $f(x)$ irred. $/F$. Thus, $F[x]/(f(x))$ is a field $\Leftrightarrow$ $f(x)$ is irred $/F$.

Pf: $F[x]$ PID $\Rightarrow$ every non-zero prime ideal is max ideal.
If f factors, then clearly it isn't prime (irred $\Leftrightarrow$ prime in PID)
If not, then f irred. $\Rightarrow$ f prime (PID) $\rightarrow (f)$ prime $\Rightarrow (f)$ max ideal $\Rightarrow$ quotient is a field.

Prop: $g(x)$ non-const poly in $F[x]$,
$g(x) = f_1(x)^{n_1} \cdots f_k(x)^{n_k}$ fact. into irreducibles, f_i distinct.

Then
$$F[x]/(g(x)) \cong F[x]/(f_1(x)^{n_1}) \times \cdots \times F[x]/(f_k(x)^{n_k})$$

Pf: Follows by Chinese Remainder Theorem + $F[x]$ is a Euclidean Domain.

Prop: A poly. of deg. n in $F[x]$ has $\leq n$ roots (counting multiplicities).

Pf: $F[x]$ is a UFD + linear polys are irred. + induction on earlier prop.

Prop: Finite subgp of mult. subgp. of a field is cyclic.

Pf + Corollary next time.