Algebra I: UFDs, poly. rings

- Exam is soon!
- I'm gone on Tues.
- Office Hours on Wed.

8.3 9.1-9.2

In $\mathbb{Z}$, there is another way to compute gcds: prime factorizations!

Def: R int. domain.

1). $r \in R$ not 0 or a unit. r is irreducible in R if $r = ab \Rightarrow a$ or b a unit.

2). $p \in R \setminus \{0\}$ is prime if (p) is a prime ideal; i.e., $p \mid ab \Rightarrow p \mid a$ or $p \mid b$.

3). a, b are associates if $a = ub$, u a unit

Prop: primes are always irred

Pf: If (p) prime, $p = ab$, then $ab = p \in (p)$
$\Rightarrow$ a or b is in (p). WLOG, $a \in (p)$, say
$a = pr \Rightarrow p = ab = prb \Rightarrow rb = 1 \Rightarrow b \in R^\times$
(domain) $\Rightarrow p$ irred.

Converse true in $\mathbb{Z}$: Bezout's Lemma! (irred. = usual def^n of prime).

~~False in $\mathbb{Z}[\sqrt{-5}]$.~~

Prop: In a PID, a non-zero elt. is prime $\Leftrightarrow$ irred.

Pf: WNTS irred $\Rightarrow$ prime.

If p is irred, Let $M \supseteq (p)$ be an ideal. $M = (m)$, as R = PID.
$\Rightarrow p \in (m) \Rightarrow p = rm$ some r. p irred $\Rightarrow r$ or m a unit
$\Rightarrow (p) = (m)$ or $(m) = R$
(associates) (contains unit).
$\Rightarrow (p)$ is max^l $\Rightarrow (p)$ is prime
$\Rightarrow p$ is prime.

Def^n: A UFD is an int. domain R s.t. (for) every non-zero non-unit r:

1). $r = p_1 \cdots p_n$, some irred. $p_1, \ldots, p_n$

2). This factorization is unique up to associates.

Ex: • We'll show: PID $\Rightarrow$ UFD.
R UFD $\Rightarrow R[x]$ UFD.

• $\mathbb{Z}[\sqrt{-5}]$ not a PID:

$$6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5}) \quad (*)$$

$N(a+b\sqrt{-5}) = a^2+5b^2$, $N(\alpha)N(\beta) = N(\alpha\beta)$, $N(\alpha) = 1 \iff \alpha$ a unit
$\iff a^2+5b^2 = 1 \iff \alpha = \pm 1$.

So if $N(\alpha)$ is prime, α is irred. Factor of $N(\alpha)$

More generally, α reducible $\Rightarrow \exists$ proper ~~factor~~ of

s.t. $\exists$ elt. of norm d.

~~$N(\alpha) =$~~ $\Rightarrow$ all of these elts are irred. Note FLT would be easy if all these are UFDs!

But in reals, $(*) \Rightarrow (2)$ is not prime.

factor $(6) = (2, 1+\sqrt{-5})^2 \cdot (3, 1+\sqrt{-5})(3, 1-\sqrt{-5})$.

Alg # theory: products of prime ideals is unique (reason for name ideal)

Prop: In a UFD, prime $\iff$ irred.

Pf: R a UFD. WNTS irred $\Rightarrow$ prime

Let $p \in R$ be irred, & $\nmid$ $p|ab$. Want $p|a$ or $p|b$.

$p|ab \Rightarrow ab = pc$, some c. Write a, b = prod. of irred.

By uniqueness of prime fact., $ab = pc \Rightarrow p$ is assoc. to an irred. in a or b (possibly empty)

say p assoc. to irred. factor of a: $a = (up)p_2 \cdots p_n$,

$\Rightarrow p|a$ ⊠

(R)

Prop: R UFD $a = u p_1^{e_1} \cdots p_n^{e_n}$, $b = v p_1^{f_1} \cdots p_n^{f_n}$ (u, v units)

$\Rightarrow d = p_1^{\min(e_1, f_1)} \cdots p_n^{\min(e_n, f_n)}$ = a gcd of a, b.

Th PID $\Rightarrow$ UFD

Pf: R a PID, $r \in R$ non-zero, non-unit. Find a prime factor.

r irred. $\Rightarrow$ done.

otherwise, $r = r_1 r_2$, neither a unit $(r) \subsetneq (r_1) \subseteq R$.

If both irred, done. If not, keep going... $r_1 = r_{11} r_{12} = \cdots$

If this doesn't terminate, get infinite chain (axiom of choice)

$$(r) \subsetneq (r_1) \subsetneq (r_{11}) \subsetneq \cdots \subsetneq R.$$

Claim: this can't happen in a PID.

If $I_1 \subseteq I_2 \subseteq \cdots \subseteq R$, then the chain stabilizes.

Let $I = \bigcup_{n \geq 1} I_n$ an ideal. $\Rightarrow I = (a)$

$\Rightarrow a \in I$, and so $a \in I_n$, some I_n. $\Rightarrow (a) = I \subseteq I_n$

$\Rightarrow I = I_n$.

$\Rightarrow$ every non-zero elt. factorizes as irred.

Uniqueness: If $r = p_1 \cdots p_n = q_1 \cdots q_m$, $m \geq n$

p_1 (RHS $\Rightarrow$ (prop. irred=prime) p_1 divides a q_j, say q_1 by reordering

$\Rightarrow q_1 = p_1 u$, u a unit as q_1 is irred.

$\Rightarrow p_1 p_2 \cdots p_n = u p_1 q_2 \cdots q_m \Rightarrow p_2 \cdots p_n = q_2' \cdots q_m$ (π assoc.)

Done by induction all factors matching up!

Cor: Fund. Thm of arithmetic in $\mathbb{Z}$! ED $\Rightarrow$ PID $\Rightarrow$ UFD.

For fun: In book: Arithmetic in $\mathbb{Z}[i]$ => $p = x^2+y^2$ iff $p \equiv 1 \bmod 4$ (Fermat!)
$p = x^2+y^2$? x^2+ny^2 ? a whole book!

Poly rings. $R[x]$, R an int. domain

Recall: Degree: $\deg(f \cdot g) = \deg f + \deg g$, $f, g \neq 0$.

$(R[x])^\times = R^\times$.

$R[x]$ is an int. domain

Quotient field: set of $\frac{f}{g}$, $f, g \in R[x]$, $g \neq 0$. $R(x)$. rational fns.

Prop: I ideal of R, $(I) = I[x]$ ideal of $R[x]$ gen. by I. (polys w/ coeffs. in I).

Then $R[x]/(I) \cong (R/I)[x]$.

In part, I prime => (I) prime in $R[x]$.

Pf: Nat. map $\varphi: R[x] \to (R/I)[x]$: reduce coeffs. mod I! (reduction hom)

hom is easy to check.

$\ker$ = {polys with all coeffs. $\in I$} $= (I)$.

Rest E-Z ≠ (Input...)

Def: $R[x_1, \dots, x_n] = R[x_1, \dots, x_{n-1}][x_n]$ (recursive) (what it seems like)

terms $x_1^{d_1} \cdots x_n^{d_n}$ = monomials. (monic)

$d_1 + \cdots + d_n$ = deg of monomial.

deg of poly = ... max deg of monomials parts.

homogeneous (form): all monomials same degree.

Poly rings / Fields.

After F field. Norm in $F[x]$: $N(p(x)) = \deg(p)$.
$+ (N(0) = 0)$.

Thm $F[x]$ is a ~~LFD~~ ED under this norm.

Pf: Let $a, b \in F[x]$, $b \neq 0$.

Want $q, r \in F[x]$, $a = bq + r$, $r = 0$ or $\deg(r) < \deg(b)$.

If $a = 0$, Let $b = r = 0$.

If $a \neq 0$. Induct on $\deg(a) = n$. Let $\deg(b) = m$.

If $n < m$, Let $q = 0$, $r = a$. Else, $n \geq m$.

Write $a(x) = a_n x^n + \dots + a_1 x + a_0$, $b(x) = b_m x^m + b_{m-1} x^{m-1} + \dots + b_0$.
$a_n, b_m \neq 0$.

Subtract away top term from $a(x)$

$a'(x) = a(x) - \frac{a_n}{b_m} x^{n-m} b(x)$ has $\deg < n$.

Here i used $b_m \neq 0$ is in a field.

By induction, $\exists\, q', r$ s.t.

$a' = q'b + r$, $r = 0$ or $\deg(r) < \deg(b)$

Let $q = q' + \frac{a_n}{b_m} x^{n-m} \Rightarrow a = qb + r$,

$r = 0$ or $\deg r < \deg b$

These q, r are actually unique. $\leftarrow$

Then $a - qb$, $a - q_1 b$ both have $\deg < m = \deg(b)$.

Difference $= b(q - q_1)$ has $\deg < m$, but $\deg$ is additive $\Rightarrow q - q_1 = 0$
has deg 0 $\Rightarrow q = q_1$

also $\Rightarrow r = r_1$

Cor: $F[x]$ is a PID, UFD.

Ex: p prime $\Rightarrow \mathbb{Z}/p\mathbb{Z}[x]$
obtained by reducing $\mathbb{Z}[x]$ mod (p)
is a PID, since coeffs lie in the field $\mathbb{Z}/p\mathbb{Z}$.

In particular, a quotient of something that's not a PID may be a PID. ($\mathbb{Z}[x]$, $(2,x)$ not prime.)

Ex: $\mathbb{Q}[x,y]$ is not a PID, as
$\mathbb{Q}[x,y] = \mathbb{Q}[x][y]$, $\mathbb{Q}[x]$ not a field
(can't find elt. of pos. deg. non-invertible)

We'll see: $\mathbb{Q}[x,y]$ is a PID. UFD?

Start next lecture.