November 16, hours 26-27: UFDs, Euc->PID->UFD

November-11-10
11:18 AM

HW. HW3 due today, HW4 on web by midnight.

Reminders. prime: $p \neq R^* \cup \{0\}$ $p|ab \Rightarrow p|a \vee p|b \iff \langle p \rangle$ is prime.

irreducible: $0 \neq x = ab \Rightarrow a \in R^* \vee b \in R^*$

Prime $\Rightarrow$ irreducible $\not\Leftarrow$ Prime

UFD: $\forall x \neq 0$, $x = a p_1 \cdots p_n$, $a \in R^*$ p_i primes.

Thm. This decomposition is unique up to units & permutation.

IT 2C 4W: [M f.g. / R PID $\Rightarrow M \cong R^k \oplus \bigoplus R/\langle p_i^{s_i} \rangle$]

$\Rightarrow$ structure of f.g. Abelian groups, J.C.F.

Today. PIDs, modules(?).

Thm. In a UFD, Prime $\iff$ irreducible.

PF If an irred. is decomposed, the decomposition must have length 1.

Thm. [skip] UFD $\iff$ every $x \neq 0$ has a unique decomposition into irreducibles.

PF need irred $\Rightarrow$ prime. If x is irred & $x|ab$, then $xz = a_1 \cdots a_n b_1 \cdots b_m$ (a_i, b_j irreds) $\Rightarrow x \sim a_i$ or $x \sim b_j$ $\Rightarrow x|a \vee x|b$.

Thm. In a UFD gcd's always exist.

How show UFD? Norm $\Rightarrow$ "PID" $\Rightarrow$ UFD.

Def. Euclidean domain: has a "norm" $\ell: R - \{0\} \to \mathbb{N}$ s.t.

1. $\ell(ab) \geq \ell(a)$
2. $\forall a, b$ $\exists q, r$ s.t. $a = qb + r$ & $r = 0$ or $\ell(r) < \ell(b)$

Examples. 1. $\mathbb{Z}$

Example $\dfrac{a = x^3 - 2x^2 - 5x + 12}{b = x^2 + 1}$

2. $F[x]$ ... $r = -6x + 14$, $a(i) = 14 - 6i$ } why?

theorem. A Euclidean domain is a "PID" (def).
(Thm: a PID is a UFD, later)

Proposition. In a PID, every prime ideal is maximal.

Pf. $I = \langle p \rangle$ prime, $I \subset J = \langle x \rangle \subset R \Rightarrow p = ax \Rightarrow$

$p \mid x \Rightarrow J \subset I \Rightarrow I = J$.

or

$p \mid a \Rightarrow a = bp \Rightarrow p = bpx \Rightarrow 1 = bx \Rightarrow x \in R^* \Rightarrow J = R$.

theorem. PID $\Rightarrow$ UFD.

Pf Take x_1; $x_1 \in M_1$, where M_1 is a maximal ideal containing $\langle x_1 \rangle$. $M_1 = \langle p_1 \rangle$, p_1 prime. So $x_1 = p_1 x_2$; $x_2 \in \langle x_2 \rangle \subset M_2$ maximal, $M_2 = \langle p_2 \rangle$, $x_2 = p_2 x_3$, ...

$\langle x_1 \rangle \subset \langle x_2 \rangle \subset \langle x_3 \rangle \subset \dots \subset \langle x_n \rangle = \langle x_{n+1} \rangle$

"Noetherian"

theorem. In a PID $\langle a, b \rangle = \langle \gcd(a,b) \rangle$. (so $\gcd(a,b) = sa + tb$)

The Euclidean Algorithm. In a Euc. Domain, a practical algorithm for finding $s(a,b)$ & $t(a,b)$ as above: WLOG, $\ell(a) \geq \ell(b)$

If $\langle a, b \rangle = \langle b \rangle$, take $(s,t) = (0,1)$. Otherwise

$a = bq + r$, $\ell(r) < \ell(b)$,

$\langle a, b \rangle = \langle b, r \rangle$ so if $g = s'b + t'r$, then

$g = s'b + t'(a - bq) = t'a + (s' - t'q)b$

theorem. R is a PID iff it has a "Dedekind-Hasse" norm: $d: R-\{0\} \to \mathbb{N}_{\geq 0}$ [or add $d(0)=0$] s.t. if $a, b \neq 0$ either $a \in \langle b \rangle$ or $\exists\, 0 \neq x \in \langle a, b \rangle$ w/ $d(x) < d(b)$.

pf. $\Leftarrow$ as before. $\Rightarrow$ Replace every prime by 2, get even a "multiplicative" D-H norm.

If time: Modules, $\mathbb{Z}$, V, $T: V \to V$. done line.