November 15, hours 26-27: Euclidean is PID is UFD

November-14-11 4:53 PM

HW3 due, HW4 on Web soon.

Global goal: IT2C4W: M f.g. module over a PID $R \Rightarrow$ uniquely
$M \cong R^k \oplus \bigoplus R/(p_i^{s_i})$ p_i prime, $s_i \geq 1$

Cor 1. A f.g. Abelian $\Rightarrow A \cong \mathbb{Z}^k \oplus \bigoplus \mathbb{Z}/p_i^{s_i}$

Cor 2. $A \in M_{n\times n}(\mathbb{C})$ has a "Jordan form"

No Joy Agenda. Euc $\Rightarrow$ PID $\Rightarrow$ UFD.

UFDs. Def. Every non-zero element can be factored into primes.

Thm. Uniqueness up to units & a permutation.

Thm. In a UFD, prime $\Leftrightarrow$ irreducible.

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

Thm. UFD $\Leftrightarrow$ every $x \neq 0$ has a unique decomposition into irreducibles.

PF need irred $\Rightarrow$ prime. If x is irred & $x | ab$, then $zx = \underbrace{a_1 \dots a_n b_1 \dots b_m}_{\text{irreds}} \Rightarrow x \sim a_i$ 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" $e: R - \{0\} \to \mathbb{N}$ s.t.

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

Example. 1. $\mathbb{Z}$

2. $F[x]$

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

$\dots\ r = -6x + 14$
$a(i) = 14 - 6i$ } 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, $I \subset J = \langle x \rangle \subset R \Rightarrow p = ax \Rightarrow$
$(a \in R^* \Rightarrow I = J) \vee (x \in R^* \Rightarrow J = R)$

theorem. PID $\Rightarrow$ UFD.

Weak proof. Take $x = x_1$; unless $x_1 \in R^*$, $x_1 \in M_1$ where M_1 is a maximal ideal containing $\langle x_1 \rangle$. $M_1 = \langle p_1 \rangle$, p_1 prime. So $x_1 = p_1 x_2$; unless $x_2 \in R^*$ $x_2 \in \langle x_3 \rangle \subset M_2$ maximal $M_2 = \langle p_2 \rangle$, $x_2 = p_2 x_3, \ldots$ if process was infinite,

$\langle x_1 \rangle \subsetneq \langle x_2 \rangle \subsetneq \langle x_3 \rangle \subsetneq \ldots$

$\langle x_n \rangle \subset \langle x_{n+1} \rangle$ as $x_n = p_n x_{n+1}$
if $x_{n+1} \in \langle x_n \rangle$, $x_{n+1} = a x_n$ so
$x_n = p_n a x_n$ & p's not prime.

But a PID is "Noetherian",
so the process must terminate.

So $x = x_1 = p_1 x_2 = p_1 p_2 x_3 = \ldots = p_1 p_2 \ldots p_n u$

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

$$g = s'b + t'(a - bq) = \underbrace{t'}_{s} a + \underbrace{(s' - t'q)}_{t} b$$

---

theorem. R is a PID iff it has a "Dedekind-Hasse" norm: $d : R - \{0\} \to \mathbb{N}_{>0}$ [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.

---

done line

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