14-1100 Nov 3, hours 23-24: "better rings", Euc -> PID -> UFD

October-10-14 1:09 PM

(141102) Assaf's riddle: ~~k~~ 5 kids share a loot of ~~n~~ 50 in-wrapping halloween candies. The first kid proposes a way to split the loot; if it is not accepted by a strict majority (her included), she's ~~left out~~ goes home and the second proposes a split, etc. How is the loot split?

Global goal: ITBCSW: 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.

Reminders R/I a field $\Leftrightarrow I$ is maximal.

R/I a domain $(ab=0 \Rightarrow (a=0)\vee(b=0))$ $\Leftrightarrow I$ is prime. start line

Prime Ideals. 1. Definition $P \subset R$ is prime if $ab \in P \Rightarrow a \in P$ or $b \in P$.

2. Theorem. R/P is a domain iff P is prime.

Proof $\Rightarrow$ $ab \in P \Rightarrow [ab]=0 \Rightarrow [a][b]=0 \Rightarrow$ either $[a]=0 \Rightarrow a \in P$ or $[b]=0 \Rightarrow b \in P$.

$\Leftarrow$ $[a][b]=0 \Rightarrow [ab]=0 \Rightarrow ab \in P \Rightarrow$ either $a \in P \Rightarrow [a]=0$ or $b \in P \Rightarrow [b]=0$

Theorem. A maximal ideal is prime.

From this point on, R is a commutative integral domain.

Divisibility & Primes. 1. $a|b$ $[a\neq 0, \exists q$ s.t. $aq=b]$ $(a|b \wedge b|a \Rightarrow a=ub)$ "a,b are associates"

2. $\gcd(a,b)=q$ if $\gcd=q$ & $\gcd=q' \Rightarrow q'=uq$.

3. Irreducible $c=ab \Rightarrow a \in R^* \vee b \in R^*$

4. Primes: $p \neq 0$ non-unit $p|ab \Rightarrow p|a$ or $p|b$

p is prime iff $\langle p \rangle$ is prime ideal.

Claim. prime $\Rightarrow$ irreducible

$p = ab \Rightarrow p \mid a \Rightarrow a = pc$

$\Rightarrow p = pcb \Rightarrow cb = 1 \Rightarrow b \in R^*$

counterexample: in $\mathbb{Z}[\sqrt{-5}]$, 2 is irred (for norm reasons) but not prime, as $2 \mid (1-\sqrt{-5})(1+\sqrt{-5}) = 6$

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 & $x \mid ab$, then $zx = a_1 \cdots a_n b_1 \cdots b_m$ (a_i, b_j irreds) $\Rightarrow x \sim a_i$ or $x \sim b_j \Rightarrow x \mid a \vee x \mid b$

Thm. In a UFD gcd's always exist.

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

Def. Euclidean domain: has a "norm" $\ell : R - \{0\} \to \mathbb{W}$ 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. $\mathbb{Z}$

2. $F[x]$

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

$\cdots r = -6x + 14$

$a(i) = 14 - 6i$ } 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, $I \subset J = \langle x \rangle \subset R \Rightarrow p = ax \Rightarrow$

$(a \in R^* \Rightarrow I = J) \vee (x \in R^* \Rightarrow J = R)$

done line

---

theorem. PID $\Rightarrow$ UFD.

Weak proof. Take $x = x_1 \cdot$ 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 $x_1 = p_1 x_2 \cdot$ unless $x_2 \in R^*$ $x_2 \in \langle x_3 \rangle \subset M_2$ maximal $M_2 = \langle p_2 \rangle$, $x_2 = p_2 x_3$, ... if process was infinite,

$M_2 = \langle p_2 \rangle$, $x_2 = p_2 x_3$, ... if process was infinite,

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

But a PID is "Noetherian",

So the process must terminate.

$\langle x_n \rangle \subset \langle x_{n+1} \rangle$ 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.

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

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

target line

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: $d : R - \{0\} \to \mathbb{N}_{\geq 0}$ [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.