November 10, hour 25: Primes, UFDs, One Theorem Two Corollaries Four Weeks

November-04-11 9:22 AM

Local goal. Prime ideals & primes

Euclidean ⇒ PID ⇒ UFD

Read Alon. slides 2.2, 2.7, (2.8, 2.9)

~~Publish~~ link or perish

Global goal "v.s." "f.d." "$\mathbb{Z}, F[x]$"

IT2C4W: M f.g. over a PID R ⇒ Uniquely

$$M \cong R^k \oplus \bigoplus R/(p_i^{s_i}) \quad p_i \text{ prime},\ s_i \geq 1$$

Cor 1. A f.g. Abelian ⇒

$$A \cong \mathbb{Z}^k \oplus \bigoplus \mathbb{Z}/p_i^{s_i}$$

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

(Comment on linking at http://katlas.math.toronto.edu/drorbn/index.php?title=User:Lp.thibault)

Did: Maximal & prime ideals, Fields & domains.

R is a commutative integral domain.

Primes. 1. $a|b$ "a,b are associates" $(a|b \wedge b|a \Rightarrow a = ub)$

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

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

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

4. Irreducible $x = ab \Rightarrow a \in R^* \vee b \in R^*$

Claim. prime ⇒ irreducible

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

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

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.

done line.

Thm. In a UFD, Prime ⇔ irreducible.

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

Thm. UFD ⇔ every $x \neq 0$ has a unique decomposition

pf need irred ⇒ prime. If x is irred & $x|ab$, then 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.