November 11, hour 25: Prime ideals, primes

November-04-10
12:47 PM

Local goal. Prime ideals & primes

Euclidean $\Rightarrow$ PID $\Rightarrow$ UFD

Read Aluffi. Slide 2.2, 2.7, (2.8, 2.9)

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

IT2C4W: M f.g. over a PID $R \Rightarrow$ 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 $\Rightarrow$

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

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

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

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

Theorem. A maximal ideal is prime.

Primes. 1. $a|b$ $\quad (a|b \wedge b|a \Rightarrow a = ub)$

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

3. Primes: $p \neq 0$ non-unit $\quad p|ab \Rightarrow p|a$ 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 $\Rightarrow$ 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 $\Leftrightarrow$ irreducible.

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

Thm. In a UFD gcd's always exist.

Sketch: Euc domain: $d : R - \{0\} \to \mathbb{N}$ s.t.

1. $d(a) \leq d(ab)$
2. $\forall a, b \ \exists q, r$ s.t. $a = qb + r$, with $r = 0$ or $d(r) < d(b)$

Thm Euc $\Rightarrow$ PID.

Thm PID $\Rightarrow$ UFD

Pf Take x; $x \in M_1$ where M_1 is a maximal ideal containing $\langle x \rangle$. $M_1 = \langle p_1 \rangle$, p_1 prime. So $x = p_1 x_2 \ldots$