Lezione 11 - 10/05/19

martedì 30 aprile 2019 15:10

Def: Definiamo il MASSIMO COMUN DIVISORE tra a e b $d = MCD(a,b)$ un elemento tale che
- $d \mid a$ e $d \mid b$
- Se $x \mid a$ e $x \mid b \Rightarrow x \mid d$.

Oss: Il massimo comun divisore esiste negli anelli speciali:
Infatti
1. Euclideo: Si usa la divisione e la funzione grado
2. PID: Si usa il generatore dell'ideale (a,b)
3. UFD: Si usa la fattorizzazione unica prendendo i fattori comuni.

Lemma di Zorn: Sia $\mathcal{F}$ un insieme parzialmente ordinato. Chiamiamo CATENA una sequenza di $A \in \mathcal{F}$ ordinata secondo l'ordine parziale. Se ogni catena C di $\mathcal{F}$ ammette maggiorante $\overline{A} \in \mathcal{F}$ e $\mathcal{F} \neq \emptyset$, allora $\exists M$ elemento massimale in $\mathcal{F}$.

Oss: L'elemento massimale potrebbe non essere unico

Esempio: Sia $\mathcal{F}$ l'insieme degli ideali propri di un anello A. Consideriamo una qualsiasi catena $I_0 \subseteq I_1 \subseteq \_\_ \subseteq I_n \subseteq \_$ in $\mathcal{F}$. Consideriamo $\bigcup I_i = I$. Allora I è un ideale in quanto le relazioni si possono ricondurre al finito. Inoltre $\mathcal{F} \neq \emptyset$ in quanto (0) è ideale $\forall A$ anello. Dunque $\exists m$ massimale in $\mathcal{F}$. Questo dimostra che in ogni anello c'è un ideale massimale.

Teorema: Se A è UFD $\Rightarrow A[x]$ è UFD
Dim: Non la riportiamo (svolta a lezione; si trova nelle dispense)

Corollario: Se A è UFD $\Rightarrow A[x_1, \_\_, x_n]$ è UFD $\forall n \in \mathbb{N}$.
Dim: Ovvia per teo precedente.

FATTI SU UN ESEMPIO IMPORTANTE: $\mathbb{Z}[i]$

Def: Definiamo l'ANELLO DEGLI INTERI DI GAUSS

$$\mathbb{Z}[i] \cong \frac{\mathbb{Z}[x]}{(x^2+1)} = \{a+bi \mid a,b \in \mathbb{Z}\}.$$

Fatti su $\mathbb{Z}[i]$:

(1) $\mathbb{Z}[i]$ è un anello EUCLIDEO ($\Rightarrow$PID $\Rightarrow$UFD). La funzione grado è data da

$$N: \mathbb{Z}[i] \longrightarrow \mathbb{Z}, \quad (a+bi) \longmapsto a^2+b^2$$

(2) $\mathbb{Z}[i]^* = \{\pm 1, \pm i\}$

(3) Sia $p \in \mathbb{Z}$ un numero primo; allora
- $p=2$: $2 = -i(1+i)^2$ e $(1+i)$ è primo in $\mathbb{Z}[i]$
- $p \equiv 1 \pmod 4$: Esistono $a,b \in \mathbb{Z}$ tali che

(3) Sia $p \in \mathbb{Z}$ un numero primo; ovvero

- $p=2$: $2 = -i(1+i)$ e $(1+i)$ è primo in $\mathbb{Z}[i]$
- $p \equiv 1 \ (4)$: Esistono $a, b \in \mathbb{Z}$ tali che

$$p = (a+bi)(a-bi) = a^2+b^2$$

con $(a+bi)$ e $(a-bi)$ primi in $\mathbb{Z}[i]$

Inoltre p si scrive in modo unico come somma di quadrati

- $p \equiv 3 \ (4)$: p è primo in $\mathbb{Z}[i]$

(4) I primi di $\mathbb{Z}[i]$ sono:

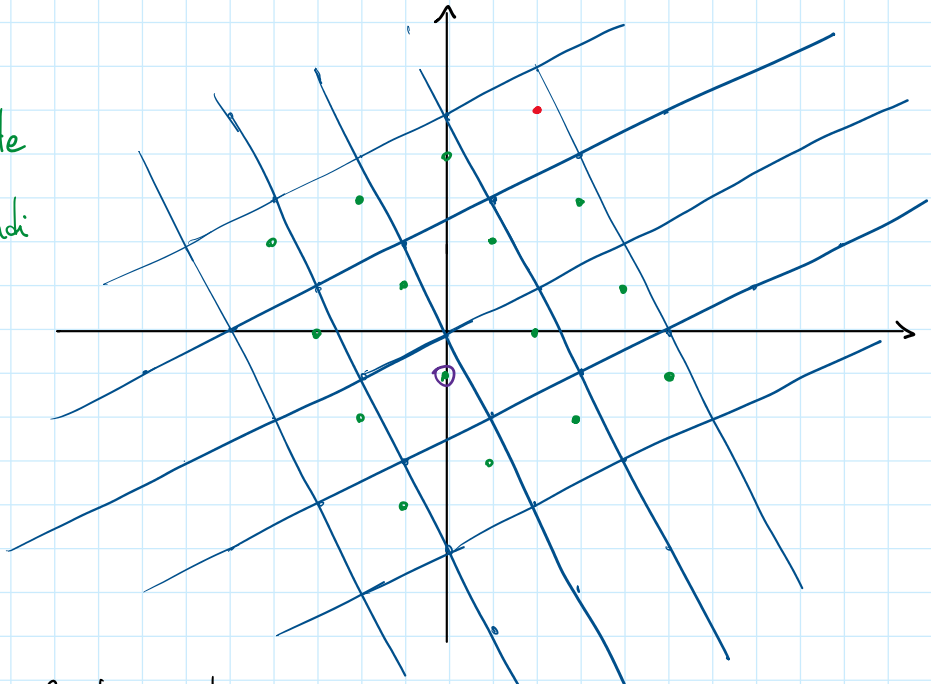
- $(a+bi)$ con $a^2+b^2=2$ o $a^2+b^2 = p$ primo $p \equiv 1 \ (4)$
- $p \equiv 3 \ (4)$ in $\mathbb{Z}$

(5) Sia $(a+bi)$ ideale di $\mathbb{Z}[i]$. Allora

$$\left| \frac{\mathbb{Z}[i]}{(a+bi)} \right| = N(a+bi) = a^2+b^2$$

Oss: La divisione in $\mathbb{Z}[i]$ si può immaginare come una tassellatura del piano data dal divisore e l'idea è quella di vedere il dividendo dentro il "quadrato di riferimento" dell'origine:

Esempio: Dividiamo per $(2+i)$



Il quoziente identifica tutti i verdi

Tassellazione $(2+i)$

- $2+5i$
- Punti corrisp. cioè quelli che hanno lo stesso resto divisi per $(2+i)$. Il punto più vicino all'origine è il resto 0. La divisione va svolta

Leggere la tassellatura è anche un modo diverso (Via TEOREMA DI PICK) di dimostrare che $\left| \frac{\mathbb{Z}[i]}{(a+bi)} \right| = a^2+b^2$.