Lezione 5 Algebra 1

Federico De Sisti

2025-03-17

0.1 PID $\Rightarrow$ UFD

Esercizio
Dimostrare che Euclideo $\Rightarrow$ PID
Suggerimento
R dominio d'integrità
Per l'esistenza è lo stessa usata per verificare che $\mathbb{K}[x]$ è un PID.
Ricordo

Definizione 1
$a \in R \setminus \{0\}$ non invertibile

- *a primo se $a|bc \Rightarrow a|b$ oppure $a|c$*
- *irriducibile se $a = bc$ allora a associato a c oppure a associato a c*

Osservazione 1
$a \in R$ primo $\Rightarrow$ a irriducibile
Osservazione 2
$a \in R$ primo $\Leftrightarrow (a) \subseteq R$ primo se R domino d'integrità
Osservazione 3
R dominio PID, $a \in R$ irriducibile $\Rightarrow (a) \subseteq R$ ideale massimale.
Osservazione 4
$R = \mathbb{K}[x, y]$ PID $a = x \in R$
$(a) = (x) \subseteq \mathbb{K}[x, y]$
$J = (x, y) \neq K[x, y]$ $(x) \subsetneq J$
(x) non è massimale nonostante il suo generatore sia irriducibile.

Definizione 2 (Dominio a fattorizzazione unica)
R dominio a fattorizzazione unica se:

1. *ogni elemento si fattorizza in irriducibili.*
2. *tale fattorizzazione è unica a meno di permutazioni e irriducibili associati.*

Teorema 1
R UFD se e solo se:

1. *ogni irriducibile in R è primo in R.*
2. *Data una successione in R $a_1, a_2, \ldots a_n, \ldots$ tale che $a_{i+1}|a_i \quad \forall a_i \in \mathbb{Z}_{>0}$ allora $\exists \underline{i} \in \mathbb{Z}_{>0}$ tale che a_h, a_k associati $\forall h, k \geq \underline{i}$*

Teorema 2
R dominio a ideali principali.
Allora R è dominio a fattorizzazione unica

Dimostrazione
L'idea è sfruttare il teorema precedente.

1. *Sia $a \in R$ irriducibile*
   $\Rightarrow (a) \subseteq R$ *ideale massimale*
   $\Rightarrow (a) \subseteq R$ *ideale primo*
   $\Rightarrow a \in R$ *primo.*

2. *Consideriamo una successione in R:*
   $a_1, \dots, a_n, \dots$ *tale che* $a_{i+1} | a_i \quad \forall i \in \mathbb{Z}_{>0}$
   Voglio vedere che questa stabilizza (diventa una catena stazionaria)
   Considero gli ideali (a_i), abbiamo $(a_i) \subseteq (a_{i+1}) \quad \forall i \geq 1$
   Definiamo $I := \bigcup_{i=1}^{+\infty} (a_i)$ *che è un ideale in R*
   Infatti:
   dati $r \in R$ e $b \in I$ avremmo $b \in (a_i)$ per qualche indice i
   $\Rightarrow r, b \in (a_i) \subseteq I$

   dati $b_1, b_2 \in I$
   $\Rightarrow b_1 \in (a_{i_1}), \; b_2 \in (a_{i_2})$
   assumendo $i_1 \leq i_2$
   $\Rightarrow (a_{i_1}) \subseteq (a_{i_2})$
   $\Rightarrow b_i \in (a_{i_2})$
   $\Rightarrow b_1 + b_2 \in (a_{i_2}) \subseteq I$

   Allora $I \subseteq R$ è un ideale principale:
   $\exists a \in R$ *tale che* $(a) \in I$

   - *Quindi* $(a) = \bigcup_{i=1}^{\infty} (a_i)$
     da cui $(a_i) \subseteq (a) \Rightarrow a | a_i \quad \forall i \in \mathbb{Z}_{>0}$.
   - *D'altra parte*
     $a \in (a) = \bigcup_{i=1}^{+\infty} (a_i) \;\Rightarrow\; \exists \underline{i} \in \mathbb{Z}_{>0}$ *tale che* $a \in (a_{\underline{i}}) \subseteq (a_h) \quad \forall h \geq \underline{i}$
     da cui $a_h \mid a \quad \forall h \geq \underline{i}$

   Deduciamo a, a_h associati $\forall h \geq \underline{i}$
   Quindi $\forall h, k \geq \underline{i}$
   $$\begin{cases} a, a_h & \textit{assocaiti} \\ a, a_k & \textit{assocaiti} \end{cases} \Rightarrow a_h, a_k \textit{ associati}$$

Dal teorema segue che R è UFD. $\square$

Corollario 1
$\mathbb{Z}[i]$ è UFD

Dimostrazione
$\mathbb{Z}[i]$ è Euclideo $\Rightarrow Z[i]$ è $PID \Rightarrow \mathbb{Z}[i]$ è UFD $\square$

Problema:
Quali primi di $\mathbb{Z}$ sono primi in $\mathbb{Z}[i]$?

Esercizio (standard)
$R = \mathbb{Q}[x]$
$I = (x^3 + x^2 - x - 1, x^4 - 2x^2 + 1, x^5 - x^3)$
Determinare un generatore dell'ideale I
Cerco un polinomio $p \in \mathbb{Q}[x]$ che divida i 3 generatori

Definizione 3
R dominio d'integrità $a, b \in R \setminus \{0\}$
diremo che $c \in R$ è massimo comun divisore $c = MCD(a, b)$ se:

- $c|a$ *e* $c|b$
- $\forall d \in R : \begin{cases} d|a \\ d|b \end{cases}$ *si ha* $d|c$

$c \in R$ si dice minimo comune multiplo, $c = mcm(a, b)$ se:

- $a|c$ *e* $b|c$
- $\forall d \in R : \begin{cases} a|d \\ b|d \end{cases}$ *si ah* $c|d$

Esercizio
dimostriamo che se R è UFD allora esiste MCD e mcm

Soluzione
dati $a, b \in R \setminus \{0\}$
consideriamo $a = \varepsilon \cdot r_1 \cdot \ldots \cdot r_h$
$b = \eta \cdot s_1 \cdot \ldots \cdot s_k$
con $\varepsilon, \eta \in R$ invertibili, $r_i, s_i \in R$ irriducibili

Idea
raggruppare gli irriducibili associati fra loro e costruire $c = MCD(a, b)$ come segue
$c = r_{i_1}^{t_1} \cdot r_{i_2}^{t_2} \cdot \ldots {}_{i_m}^{t_m}$
Chi sono t_i e gli r_{i_j}?
r_{i_j} sono gli irriducibili associati ad almeno uno degli irrazionali di b
t_i è il minimo tra gli esponenti con cui il corrispondente irriducibile compare nelle fattorizzazioni di a e di b

Osservazione
MCD e mcm non sono unici in generale.

Osservazione
$(\mathbb{Z}[i], \nu)$
$\nu(a+ib) = a^2 + b^2 \quad \forall a, b \in \mathbb{Z}$
$v(a+i0) = a^2$
Osservazione
$z = a + ib \in \mathbb{Z}[i]$ tale che $v(z) \in \mathbb{Z}$ è primo in $\mathbb{Z}$
Allora z è primo in $\mathbb{Z}[i]$
Infatti se $z = \alpha \cdot \beta$
$\Rightarrow \nu(z) = \nu(\alpha) \cdot \nu(\beta)$
Allora se $\nu(z)$ primo in $\mathbb{Z} \to v(\alpha) = 1$
$\Rightarrow \alpha$ invertibile in $\mathbb{Z}[i]$
$\Rightarrow z$ irriducibile in $\mathbb{Z}[i]$
$\Rightarrow z$ primo in $\mathbb{Z}[i]$
Problema
$p \in \mathbb{Z}$ primo $\Rightarrow p \in \mathbb{Z}[i]$ è primo?
Idea
$p \in \mathbb{Z}$ primo $\Rightarrow \nu(p) = p^2$
Se p è irriducibile in $\mathbb{Z}[i]$
$\Rightarrow p = (a_1 + ib_1)(a_2 + ib_2)$
$\Rightarrow p^2 = (a_1^2 + b_1^2)(a_2^2 + b_2^2)$
Osservazione
Modulo (4) gli unici quadrati sono 0 e 1 Mentre se $p \equiv_4 3$ allora non può essere somma di quadrati $\Rightarrow$ non può essere irriducibile.