Lezione 7 Algebra I

Federico De Sisti

2025-03-24

0.1 Varie cose su polinomi e UFD

Definizione 1
R UFD, $f \in R[x]$ il contenuto di f è

$$c(f) = MCD(a_0, \dots, a_n) \in R.$$

dove $f = \sum_{i=0}^{n} a_i x^i$

Osservazione
$c(f)$ è ben definito a meno di moltiplicazioni per unità di R.

Definizione 2
R UFD, $f \in R[x]$ si dice primitivo se $c(f) = 1$

Lemma 1 (Gauss)
R è UFD $f, g \in R[x]$
Allora

$$c(f \cdot g) = c(f) \cdot c(g).$$

Dimostrazione
$f, g \in R[x]$ possiamo scriverli come

$$\begin{cases} f = c(f) \cdot f' \\ g = c(g) \cdot g' \end{cases}.$$

con $f', g' \in R[x]$ primitivi
Inoltre $c(r \cdot h) = r \cdot c(h) \quad \forall r \in R$ e $\forall h \in R[x]$
Allora

$$c(f \cdot g) = c(c(f) \cdot f' \cdot c(g) \cdot g') = c(f)c(g) \cdot c(f' \cdot g').$$

dato che $c(f), c(g) \in R$
Quindi è sufficiente dimostrare che $c(f' \cdot g') = 1$
Equivalentemente verifichiamo che non esiste alcun primo in $q \in R$ tale che $a|c(f' \cdot g')$
Supponiamo per assurdo che esista $q \in R$ tale che $q|c(f' \cdot g')$ primo in R.
$q \in R$ primo $\Rightarrow (q) \subseteq R$ ideale primo
$\Rightarrow \overline{R} = R/(q)$ è un dominio d'integrità.
$\Rightarrow \overline{R}[x]$ dominio d'integrità.
Considero $\bar{f}', \bar{g}' \in \bar{R}[x]$ i polinomi indotti in $\bar{R}[x]$
riducendo il coefficiente di f' e g' mod(q)
Allora $q|c(f' \cdot g') \Rightarrow \bar{f}' \cdot \bar{g}' = 0$ in $\bar{R}[x]$
Quindi (dato che $\bar{R}[x]$ dominio d'integrità)
$\bar{f}' = 0$ in $\bar{R}[x]$ oppure $\bar{g}' = 0$ in $\bar{R}[x]$
$\Rightarrow q|c(f')$ in R oppure $q|c(g')$ in R

Ma f', g' sono primitivi in $R[x] \Rightarrow c(f'), c(g')$ unità in $R \Rightarrow$ assurdo

$\square$

Ricordo
R dominio d'integrità
$X = \{(a,b) \mid a \in R, b \in R \setminus \{0\}\}$
$(a,b) \sim (c,d) \Leftrightarrow ad = cb$
$Frac(R) = X/\sim$ è il campo delle frazioni di R
Osservazione

$$\begin{aligned} \text{R} &\rightarrow Frac(R) \\ \text{r} &\rightarrow (r,1) \end{aligned}$$

omomorfismo di anelli.

Notazione 1
denoteremo (a,b) in $Frac(R)$ come $a \cdot b^{-1}$

Lemma 2
R UFD. $f \in R[x]$ primitivo $g \in R[x]$
Allora $f|g$ in $R[x]$ se e solo se $f|g$ in $\mathbb{K}[x]$ dove $\mathbb{K} = Frac(R)$

Dimostrazione
$f|g$ in $R[x]$ significa $f \cdot q = g$ per qualche $q \in R[x]$
$f|g$ in $\mathbb{K}[x]$ significa $f \cdot q = g$ per qualche $q \in \mathbb{K}[x]$
Nota che $\mathbb{K}[x]$ potrebbe avere molti più elementi di R quindi è un'informazione più generale.
Basta mostrare che la seconda implica la prima
Se $q \in \mathbb{K}[x] \Rightarrow q = a \cdot b^{-1}$ dove $a \in R[x]$ e $b \in R \setminus \{0\}$
Allora
$b \cdot g = b \cdot f \cdot q = \cancel{b} \cdot f \cdot a \cdot \cancel{b^{-1}}$
Per il lemma di Gauss

$$c(b) \cdot c(g) = c(b \cdot g) = c(f \cdot a) = c(f) \cdot c(a).$$

Notando che $c(f) = 1$ deduciamo che $c(a) = b \cdot c(g)$
Allora:

$$q = a \cdot b^{-1} = c(a) \cdot a' \cdot b^{-1} = \cancel{b} \cdot c(g) \cdot a' \cdot \cancel{b^{-1}} \in R[x].$$

$\square$

Proposizione 1
R UFD. Allora $f \in R[x]$ è irriducibile se e solo se una delle seguenti condizioni è verificata

1. *$f \in R$ e f irriducibile in R*
2. *$f \in R[x]$ primitivo e f irriducibile in $\mathbb{K}[x]$*

Dimostrazione

- *Le unità di $R[x]$ sono le stesse di R.*
  Infatti se $fg = 1$ allora $deg(f) + deg(g) = deg(f \cdot g) = deg(1) = 0$
- *Se $f \in R$ allora le uniche fattorizzazioni in $R[x]$ sono quelle in R.*
  Quindi f irriducibile in R se e solo se f irriducibile in $R[x]$
- *Resta da studiare il caso in cui $f \in R[x]$ con $deg(f) \geq 1$*
  Supponiamo che f sia irriducibile in $R[x]$ e sia $f = u \cdot v$ una fattorizzazione in $\mathbb{K}[x]$ con u, v non invertibili.
  Abbiamo
  $$v = a \cdot b^{-1} \text{ con } a \in R[x], b \in R \setminus \{0\}.$$
  $\Rightarrow f = u \cdot b^{-1} \cdot b \cdot v$ in $\mathbb{K}[x]$
  ma $b \cdot v \in R[x]$
  Allora basta verificare che f sia primitivo, poiché la fattorizzazione precedente fornirebbe una fattorizzazione di f in $R[x]$ per il lemma.
  Dimostriamo che f è irriducibile in $R[x] \Rightarrow f$ primitiva
  Consideriamo f
  $$f = c(f) \cdot f'.$$
  con f' primitivo in $R[x]$
  f irriducibile in $R[x]$
  $\Rightarrow c(f)$ invertibile in $R[x]$ oppure f' invertibile in $R[x]$
  Ma $deg(f') > 0$
  $\Rightarrow f'$ non invertibile in $R[x]$
  $\Rightarrow c(f)$ è invertibile
  $\Rightarrow f$ primitivo

$\square$

Corollario 1
R è UFD $f \in R[x]$ è primo se e solo se è irriducibile.

Dimostrazione
primo $\Rightarrow$ *irriducibile (sempre vero per domini d'integrità)*
Dobbiamo verificare che irriducibile $\Rightarrow$ *primo*
Abbiamo due casi:

1. $f \in R$ *irriducibile in* $R \Rightarrow f$ *primo in* R *(usiamo R UFD)*
   Se $f|u \cdot v$ *con* $u, v \in R[x]$
   $\Rightarrow c(f) = f \mid c(u) \cdot c(v)$ *in* R *(Per il lemma di Gauss)*
   $\Rightarrow f|c(u)$ *oppure* $f|c(v)$
   $\Rightarrow f|u$ *oppure* $f|v$
   $\Rightarrow$ *primo in* $R[x]$

2. f *primitivo e* f *è irriducibile in* $\mathbb{K}[x]$
   Se $f|u \cdot v$ *in* $R[x]$
   $\Rightarrow f \mid u \cdot v$ *in* $\mathbb{K}[x]$
   $\Rightarrow f|u$ *in* $\mathbb{K}[x]$ *oppure* $f|v$ *in* $\mathbb{K}[x]$
   Dato che $u, v \in R[x]$ *e* f *primitivo, questo significa* $f|u$ *in* $R[x]$ *oppure* $f|v$ *in* $R[x]$

$\square$

Teorema 1
R UFD, Allora $R[x]$ *UFD*

Dimostrazione
$f \in R[x]$. *Dimostriamo ceh esiste una fattorizzazione in irriducibili*
$f = c(f) \cdot f'$

- $c(f) \in R$ *si fattorizza come prodotto di irriducibili in* R *(che sono anche irriducibili in* $R[x]$ *)*

- $f' \in R[x]$ *è primitivo.*
  se f' *è irriducibile allora* f *si fattorizza in irriducibili in* $R[x]$
  se invece f' *non è irriducibile in* $R[x]$ *allora* $f' = u \cdot v$ *con* $c, v \in R[x]$ *non invertibili e primitivi (per il lemma di Gauss)*
  La tesi segue per induzione su $deg(f')$ *fattorizzando* u *e* v

Verifichiamo che la fattorizzazione è unica
Supponiamo che $f = \varepsilon \cdot b_1 \cdot b_2 \cdot \ldots \cdot b_k = \eta \cdot c_1 \cdot c_2 \cdot c_h$ *con* $\varepsilon\eta$ *invertibili,*
b_i, c_j *irriducibili in* $R[x]$
b_1 *irriducibile in* $R[x] \Rightarrow b_1$ *primo in* $R[x]$ *(Per il corollario)*
$\Rightarrow b_1 \mid c_1$ *(a meno di permutare* $c_1, \ldots, c_h$*)*
$\Rightarrow b_1, c_1$ *associati poiché* c_1 *irriducibile*
$\Rightarrow c_1 = \lambda b_1$ *con* λ *invertibile*
$\Rightarrow \varepsilon \cdot b_1 \cdot \ldots \cdot b_k = (\eta \cdot \lambda) \cdot b_1 \cdot c_2 \cdot \ldots \cdot c_h$
$\Rightarrow b_1 \cdot (\varepsilon b_2 \cdot \ldots \cdot b_k - \eta \cdot c_2 \cdot \ldots \cdot c_h) = 0$

$\varepsilon b_2 \cdot \ldots \cdot b_k = \eta\lambda c_2 \cdot \ldots \cdot c_h$
Si conclude per induzione su k

$\square$