Lezione 2 Secondo semestre Algebra I

Federico De Sisti

2025-03-06

0.1 Ricordo

S anello commutativo $R \subseteq S$ sottoanello $t \in S$
Abbiamo dimostrato che $R[t] = \{\sum_{i=0}^{k} r_i t_i \mid k \in \mathbb{Z}_{>0}, \quad t_i \in \mathbb{R}\}$
è il più piccolo sottoanello si S contenente $\mathbb{R}$ e t

Definizione 1
$t \in S$ si dice trascendente su $\mathbb{R}$ se per ogni $a \in \mathbb{R}[t]$ la scrittura

$$s = \sum_{i=0}^{k} r_i t^i.$$

è unica

Esercizio:
Dimostrare che $i \in S$ è trascendente su $\mathbb{R}$ se e solo se vale la seguente condizione

$$(*) \quad r_0 + r_1 t + \ldots + r_k t^k = 0 \Rightarrow r_0 = r_1 = \ldots = r_k = 0.$$

Soluzione
Se t è trascendente allora $0 \in \mathbb{R}$ ammette struttura polinomiale unica $\Rightarrow$ vale la proprietà.
Viceversa suppongo che valga $(*)$. Se

$$a_0 + a_1 t + \ldots + a_k t^k = b_0 + b_1 t + \ldots + b_h t^h.$$

Assumo $k \geq k$

$$(a_0 - b_0) + (a_1 - b_1)t + \ldots + (a_h - b_h)t^h + \ldots a_k t^k = 0.$$

$(*) \Rightarrow a_0 = b_0, \ldots, a_i = b_i \quad \forall i \leq h, \; a_j = 0 \quad \forall h < j \leq k$
Idea
R anello commutativo
x simbolo

$$R[x] = \{\sum_{i=0}^{k} r_i a^i \mid k \in \mathbb{Z}_{>0}, \; r_i \in \mathbb{R}\}.$$

Operazioni:
$\left(\sum_{i=1}^{k} a_i x^i\right) + \left(\sum_{i=0}^{h} b_i x^i\right) = \sum_{i=0}^{max(h,k)} (a_i + b_i) x^i$
$\left(\sum_{i=0}^{h} a_i x^i\right) \cdot \left(\sum_{i=0}^{k} b_i x^i\right) = \sum_{j=0}^{h+k} \left(\sum_{p+q=j} (a_p \cdot b_q)\right)$
Osservazion
Su $\mathbb{R}[x]$ è definita la funzione grado

$$deg : \text{R[x]} \to \mathbb{Z}_{\geq 0}$$
$$p \to deg(p)$$

Se $p = \sum_{i=0}^{k} a_i x^i \quad a_k \neq 0$
allora $deg(p) = k$ e p si dice **monico** se $a_k = 1$ dove $k = deg(p)$

Teorema 1 (Divisione Euclidea)
R anello commutativo
$f, g \in R[x], g$ *monico*
Allora esistono $q, r \in \mathbb{R}[x]$ *tali che*

$$f = q \cdot g + r.$$

con $deg(r) < def(g)$
Tali q *e* r *sono unici*

Dimostrazione
Procediamo per induzione su $deg(f)$
Se $deg(f) < deg(g)$
scelgo $q = 0$ *e* $f = r$
Altrimenti
$deg(f) \geq deg(g)$
scriviamo $f = \sum_{i=0}^{h} a_i x^i$
$g = \left(\sum_{i=0}^{k-1} b_i x^i \right) + x^k$
Considero

$$\hat{f} := f - a_k x^{h+k} \cdot g.$$

$\Rightarrow deg(\hat{f}) < deg(f)$
Per ipotesi induttiva
$\exists \hat{q}, \hat{r} \in R[x]$ *tali che*
$\hat{f} = \hat{q} \cdot g + \hat{r} \qquad$ *con* $deg(\hat{r}) < deg(g)$
Allora

$$f - a_k x^{h-k} \cdot g = \hat{q} \cdot g + \hat{r} \Rightarrow g = (a_h x^{h-k} + \hat{q}) \cdot g + \hat{r}.$$

con $deg(r) = deg(\hat{r}) < deg(g)$
Supponiamo

$$f = q_1 \cdot g + r_1 = q_2 \cdot g + r_2.$$

$$\Rightarrow (q_1 - q_2) \cdot g = (r_2 - r_1).$$

$deg(q_1 - q_2) \cdot g) \geq deg(g) > deg(r_2 r_1)$
$\Rightarrow$ *Assurdo*
$\Rightarrow q_1 = q_2 \quad \Rightarrow r_2 = r_1$ $\square$

Teorema 2
R anello commutativo
$\phi : R \to S$ omomorfismo di anelli $r \in S$
Allora esiste un unico omomorfismo di anelli $\bar{\phi} : R[x] \to S$ tale che

1. $\bar{\phi}(x) = t$

2. $\bar{\phi}|_R = 0$

Dimostrazione
Le richieste danno ϕ :

$$\bar{\phi}\left(\sum_{i=0}^{k} r_i x^i\right) = \sum_{i=0}^{k} \phi(r^i) t^i.$$

$\square$

Osservazione
Stiamo dicendo che esiste l'omomorfismo $R \to R[x]$ dato dall'inclusione

$$\begin{tikzcd} R \arrow[r, "\phi"] \arrow[d, "\mathrm{i}"] & S \\ R[x] \arrow[ur, dashed, "\exists\bar{\phi}"] & \end{tikzcd}$$

Esercizio
R anello commutativo
$R[x]$ anello commutativo
$R[x][y]$ anello commutativo

$$\sum_{j=0}^{k}\left(\sum_{i=0}^{m_i} a_{ij} x^i\right) y^j.$$

E se procediamo al contrario?
$R[y][x]$ è uguale a quello precedente?

$$\sum_{j=0}^{k}\left(\sum_{i=0}^{m_i} a_{ij} y^i\right) x^j.$$

Dimostrare che esiste un isomorfismo di anelli

$$\psi : R[x][y] \to R[y][x].$$

che soddisfa

1. $\psi(r) = r_1$
2. $\psi(x) = x$
3. $\psi(y) = y$

Soluzione

$$\begin{tikzcd}
R \arrow[r] \arrow[d] & R[y][x] \\
R[x] \arrow[d] \arrow[ur, dotted] & \\
R[x][y] \arrow[uur, dotted] &
\end{tikzcd}$$

esiste un omomorfismo ψ con le proprietà cercate.
Per dimostrare che ψ è un isomorfismo basta costruire l'inverso in modo analogo.

Proposizione 1
R anello commutativo R dominio d'integrità se e solo se $R[x]$ dominio d'integrità

Dimostrazione
Chiaramente se $R[x]$ è dominio d'integrità allora lo è anche R
Viceversa siano $f, g \in R[x] \setminus \{0\}$ allora il coefficiente di grado massimo di fg è il prodotto dei coefficienti di grado massimo di f e di g. Quindi se R dominio $\Rightarrow f \cdot g \neq 0$

$\square$

1 Domini Euclidei

Definizione 2
R anello commutativo

$$\nu : R \to \mathbb{Z}_{>0} \text{ funzione tale che.}$$

1. $P(r) = 0 \Leftrightarrow r = 0$

2. *dati* $a, b, c \in \mathbb{R}$ *tali che* $b \neq 0$ *e* $c = a \cdot b$ *allora*

$$\nu(c) \geq \nu(a).$$

3. $\forall f, g \in R$ *con* $g \neq 0$ *esistono* $q, r \in R$ *tali che*

$$g = q \cdot g + r.$$

   dove $\nu(r) < \nu(q)$

Tale ν *si chiama si valutazione e* (R, ν) *si chiama dominio Euclideo*

Esempio
$\mathbb{K}$ campo $(\mathbb{K}[x], \nu)$ è un dominio euclideo dove $\nu(p) = deg(p) + 1$ e $\nu(0) = 0$
$(\mathbb{Z}, \nu)$ è un domino euclideo dove $\nu(n) = |n|$
$\mathbb{K}$ campo $(\mathbb{K}, \nu)$ dominio euclideo dove $\nu(0) = 0$ e $\nu(r) = 1$ $\forall r \in \mathbb{K} \setminus \{0\}$
Esercizio
Dimostrare che $(\mathbb{Z}[i], \nu)$ è domino euclideo dove $\nu[a + ib] = a^2 + b^2$
Esempio
$f = 4+3i,\ \ g = 3+2i \neq 0$ Cerco $q, r \in \mathbb{Z}[i]$ tale che $f = q \cdot g + r$ e $\nu(e) < \nu(g) = 13$
Idea generale

$$\frac{a + ib}{c = id} = \alpha + i\beta \quad \alpha, \beta \in \mathbb{Q}.$$

Definizione 3
R anello commutativo.
Definiamo gli insiemi U_i *iterativamente*

$$U_0 = \{0\} \subseteq \mathbb{R}$$
$$U_{i+1} = \{p \in \mathbb{R} | U_i \to \mathbb{R}/(p) \quad \textit{è suriettivo}\} \cup \{0\}$$

Osservazione 1
L'omomorfismo $U_i \to R/(p)$ è la composizione

$$U_i \xrightarrow{inc} R \xrightarrow{\pi} R/(p).$$

Osservazione 2
La suriettività di $U_i \to R/(p)$ significa

$$\forall f \in R \ \exists q \in R,\ r \in U_i \quad \text{tali che } f - q \cdot p = r.$$

ovvero $f = q \cdot p + r$
Osservazione 3/esercizio
$U_i \subseteq U_{i+1} \ \ \forall i \geq 0$
Osservazione 4
Chi è U_1?
$U_1 = \{p \in R | \{0\} \to R/(p) \text{ è suriettiva}\}$
$\{q \in R \mid (p) = R\}$
$\{p \in R \mid p \text{ invertibile}\}$

Teorema 3
R dominio d'integrità, Allora R è un dominio euclideo se e solo se

$$R = \bigcup_{i=0}^{+\infty} U_i.$$

Dimostrazione
Supponiamo che (R, ν) sia un dominio Euclideo.
$Im(\nu) = \{0, a_0, a_1, \ldots, a_n, \ldots\} \subseteq \mathbb{Z}_{\geq 0}$
con $\{a_k\}$ successione strettamente crescente.
Definiamo

$$V_i = \{p \in R \mid \nu(p) \leq a\}.$$

In particolare $V_0 = \{0\}$

$$R = \bigcup_{i=0}^{+\infty} V_i.$$

La tesi segue verificando che $V_i = U_i \ \ \forall i \geq 0$ (esercizio)
Viceversa: Se $R = \bigcup_{i=0}^{+\infty} U_i$
vogliamo definire $\nu : R \to \mathbb{Z}_{>0}$
tale che (R, ν) dominio Euclideo, Dato $r \in \mathbb{R}$ $\exists i \geq 0$ tale che $r \in U_{i+1} \setminus U_o$
Definiamo $\nu(t) = i + 1$
Si possono verificare le 3 proprietà di ν.
Vediamo (2): dati $a, b, c \in R$ con $b \neq 0$ tali che $c = a + b$
vogliamo misurare $\nu(c) \geq \nu(a)$
$(c) \subseteq (a)$
$\Rightarrow R/(a) \Rightarrow R/(a)/(a)/(c) \cong R/(a)$
Se $U_i \to R/(c)$ è suriettiva
allora $U_i \to R/(c) \to R/(a)$ è suriettiva
Ovvero

$$c \in U_{i+1} \Rightarrow a \in U_{i+1}.$$

quindi

$$\nu(c) = i + 1 \Rightarrow c \in U_{i+1} \Rightarrow a \in U_{i+1} \Rightarrow \nu(a) \leq i + 1 = \nu(c).$$

□