Compendio Lezioni del Corso: Algebra$_1$/

Federico De Sisti

March 12, 2025

0.1 Ideali primi e massimali

Sia $(R, +, \cdot)$ un anello. Un ideale $I \subseteq R$ si dice primo se

- $I \neq R$
- $\forall a, b \in R$ se $a \cdot b \in I \Rightarrow a \in I \vee b \in I$

$(R, +,)$ anello $I \subseteq R$ ideale (bilatero). Allora l'anello quoziente R/I è dominio d'integrità $\Leftrightarrow I$ è ideale primo   Per ogni $a, b \in I$, la proprietà :

$$[a] \cdot [b] = [a \cdot b] = [0] \text{ in } R/I \Rightarrow [a] = [0] \vee [b] = [0] \text{ in } R/I.$$

è equivalente a richiedere $a \cdot b \in I \Rightarrow a \in B \vee b \in I$ **Esempio**
$R = [x]/(x^2)$
Osserviamo che spazio vettoriale $[x]/(x^2) = \oplus[x]$
Ricorda
Gli ideali di $[x]/(x^2)$ sono in corrispondenza biunivoca con gli ideali di $[x]$ che contengono (x^2)
L'ideale $(x) \in [x]$ contiene (x^2) e $(x)/(x^2)$ in $[x]/(x^2)$ è un ideale primo
Infatti:
$C[x]/(x^2)/x/(x^2) \Rightarrow$ è un corpo $\Rightarrow$ è un dominio d'integrità
Osserviamo che l'ideale banalae in $C[x]/(x^2)$ è $(x^2)/(x^2)$
il quale non è primo infatti $x \cdot x = x^2$
$\Rightarrow [x] \cdot [x] = [x^2] = [0]$ in $C[x]/(x^2)$
Osservazione
$[x]/(x^2)$ si chiama

- "algebra dei numeri duali"
- "fat point" (Geometricamente è un punto)

$(R, +, \cdot)$ anello, $I \subseteq R$ si dice ideale massimale se:

- $I \neq R$
- Dato un ideale $J \subseteq R$ tale che $I \subseteq J$, si ha
  $I = J \quad \vee \quad J = R$

$(R, +, \cdot)$ anello commutativo, $I \subseteq R$ ideale
I è massimale se e solo se R/I è un campo   Ricordo che esiste una corrispondenza biunivoca tra { Ideali di R che contengono I} $\leftrightarrow$ { ideali di R/I}
$J- > J/I$
$\Rightarrow I$ massimale se e solo se R/I contiene solo ideali banali
$\Rightarrow$ Sappiamo inoltre che (data la commutatività per ipotesi), R/I contiene solo ideali banali $\Leftrightarrow R/I$ è banale **Esercizio**
$n \geq 1$ intero, $(n) \subseteq$ ideale in $(, +, \cdot)$
dimostra che sono equivalenti

- (n) è ideale primo
- n è numero primo

0.2 Polinomi

In questa sezione lavoriamo con anelli commutativi.
Problema S anello commutativo, $R \subseteq S$ sottoanello, $t \in S$
Vogliamo costruire il più piccolo sottoanello B di S che contenga R e t
Osservazione
Ogni sottoanello è chiuso rispetto alle operazioni.

- $t \in B \Rightarrow t^n = t \cdot \ldots \cdot t \in B$ (n volte) $\quad \forall n \geq 1$ intero
- $r \in R \Rightarrow r \cdot t^n \in B$
- $r_1, \ldots, r_k \in R \subseteq B \Rightarrow r_0 + r_1 t + \ldots r_k t^k \in B$

Deduciamo che $R[t] \subseteq B$ dove $R[i] = \{r_0, +r_1 t + \ldots + r_k t^k \mid k \in, r_0, \ldots, r_l \in R\}$
$R[t] = B$ La dimostrazione è lasciata al lettore (basta verificare che $R[t]$ è sottoanello di S **Esempi**
1) $R =, S =, t = i$

$$R[t] = R[i] = \{r_0 + r_1 i + r_2 i^2 + \ldots + r_k i^k \, | r_1, \ldots, r_k \in\}$$

$$= \{c_0 + c_1 i \mid c_0, c_1 \in\} = .$$

Qual'è il problema? La scrittura $r_0 + r_1 t + \ldots + r_k t^k$ non è unica. $R \subseteq S$ sottoanello (commutativo), $t \in S$, allora t è trascendente su R se la scrittura $r_0 + \ldots + r_k t^k$ è unica t è trascendente su R se e solo se $r_0 + r_1 t + \ldots + r_k t^k = 0 \Leftrightarrow r_0 = r_1 = \ldots = r_k = 0$ $(\Rightarrow)$ Se t è trascendente $\Rightarrow 0 \in R$ ammette scrittura unica $\Rightarrow$ vale la proprietà
$(\Leftarrow)$ Se vale tale proprietà
P.A.
$a_0 + a_1 t + \ldots + a_k t^k = b_0 + b_1 t + \ldots + b_h t^h$
Assumo $k \geq h$ senza perdita di generalità
Porto tutto a sinistra
$(a_0 - b_0) + (a_1 - b_1)t + +(a_h - b_h)t^h + \ldots a_k t^k = 0$
Dove tutti i termini sono gli r_i nella struttura precedente
Per ipotesi $\Rightarrow a_i = b_i \quad \forall i \leq h, a_j = 0 \; \forall h < j \leq k$
$\Rightarrow$ la scrittura è unica

0.3 Ricordo

S anello commutativo $R \subseteq S$ sottoanello $t \in S$
Abbiamo dimostrato che $R[t] = \{\sum_{i=0}^{k} r_i t_i \mid k \in_{>0}, \quad t_i \in\}$
è il più piccolo sottoanello si S contenente e t
$t \in S$ si dice trascendente su se per ogni $a \in [t]$ la scrittura

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

è unica **Esercizio:**
Dimostrare che $i \in S$ è trascendente su 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 $0 \in$ 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

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

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 $[x]$ è definita la funzione grado

$$\begin{aligned} deg : [\text{x}] &\rightarrow_{\geq 0} \\ p &\rightarrow deg(p) \end{aligned}$$

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 $k = deg(p)$
[Divisione Euclidea] R anello commutativo
$f, g \in R[x], g$ monico
Allora esistono $q, r \in [x]$ tali che

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

con $deg(r) < def(g)$
Tali q e r sono unici   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
$\hat{f} = \hat{q} \cdot g + \hat{r} \quad$ 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
$\Rightarrow q_1 = q_2 \quad \Rightarrow r_2 = r_1 \quad R$ 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. $\bar{\phi}|_R = 0$

Le richieste danno ϕ :

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

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

$$R[r,"\phi"][d,"\mathrm{i}"]SR[x][ru,"\exists\bar{\phi}",dashed]$$

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

(R) at (0,4) R; (Ryx) at (2,4) $R[y][x]$; (Rx) at (0,2) $R[x]$; (Rxy) at (0,0) $R[x][y]$;
[-¿] (R) – (Rx) node[midway, left] ; [-¿] (R) – (Ryx); [down hook, -¿] (Rx) – (Rxy); [dotted,thick, ¡-] (Ryx) to [hook] (Rxy); [red, dotted,thick, -¿] (Rx) to (Ryx);

esiste un omomorfismo ψ con le proprietà cercate.
Per dimostrare che ψ è un <u>iso</u>morfismo basta costruire l'inverso in modo analogo.
R anello commutativo R dominio d'integrità se e solo se $R[x]$ dominio d'integrità
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 $\Rightarrow f \cdot g \neq 0$

1 Domini Euclidei

R anello commutativo

$$\nu : R \rightarrow_{>0} \text{ funzione tale che.}$$

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

2. dati $a, b, c \in$ 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 $\nu(0) = 0$
$(, \nu)$ 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 $([i], \nu)$ è domino euclideo dove $\nu[a + ib] = a^2 + b^2$
Esempio
$f = 4+3i,\ \ g = 3+2i \neq 0$ Cerco $q, r \in [i]$ tale che $f = q \cdot g + r$ e $\nu(e) < \nu(g) = 13$
Idea generale
$$\frac{a + ib}{c = id} = \alpha + i\beta \quad \alpha, \beta \in .$$
R anello commutativo.
Definiamo gli insiemi U_i iterativamente

$$U_0 = \{0\} \subseteq$$
$$U_{i+1} = \{p \in |U_i \rightarrow /(p) \text{ è suriettivo}\} \cup \{0\}$$

Osservazione 1
L'omomorfismo $U_i \rightarrow R/(p)$ è la composizione
$$U_i \xrightarrow{inc} R \xrightarrow{\pi} R/(p).$$

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

$U_i \subseteq U_{i+1} \quad \forall i \geq 0$
Osservazione 4
Chi è U_1?
$U_1 = \{p \in R | \{0\} \to R/(p)$ è suriettiva$\}$
$\{q \in R \mid (p) = R\}$
$\{p \in R \mid p$ invertibile$\}$
R dominio d'integrità, Allora R è un dominio euclideo se e solo se

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

Supponiamo che (R, ν) sia un dominio Euclideo.
$Im(\nu) = \{0, a_0, a_1, \ldots, a_n, \ldots\} \subseteq_{\geq 0}$
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 $V_i = U_i \quad \forall i \geq 0$ (esercizio)
Viceversa: Se $R = \bigcup_{i=0}^{+\infty} U_i$
vogliamo definire $\nu : R \to_{>0}$
tale che (R, ν) dominio Euclideo, Dato $r \in \exists i \geq 0$ 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

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

1.1 Seconda parte della lezione

Domanda:
Cosa cambia in [2] quando è un campo?
$u_1 =$
Chi è u_2?
$p \in u_2$ se e solo se

$$\to [x]/(p) \quad \text{è suriettiva.}$$

se e solo se $deg(p) = 1 \vee deg(p) = 0$
In generale
$\forall i \geq 1 \quad u_{i+1} \setminus u_i$ è l'insieme dei polinomi di grado i **Attenzione** $[x, y]$ non è domino euclideo.
$u_1 =$
$u_2 =?$
R anello commutativo, Dati $r_1, \ldots, r_k \in R$ chiamiamo

$$(r_1, \ldots, r_k) = \{\sum_{i=1}^{k} a_i r_i \mid k \in Z_{\geq 1} \quad a_i \in R\}.$$

Ideale generato da $r_1, \ldots, r_k$ in R
Osservazione
$(r_1, \ldots, r_k)$ è il più piccolo ideale di R contenente $r_1, \ldots, r_k$ [Ideale principale] R anello commutativo $I \subseteq R$ ideale, si dice principale se $\exists\ r \in R$ tale che $I = (r)$
R anello commutativo.

- R si dice Anello a ideali principali se tutti i suoi ideali sono principali.
- R si dice dominio a ideali principali se è un dominio d'integrità e un anello a ideali principali.

Esempio
$R = (, +, \cdot)$ è un dominio a ideali principali.
Esercizio
Trovare un anello a ideali principali che non sia un dominio
$n \in$, n composto
$\Rightarrow /(n)$ è un anello a ideali principali che non è un dominio   campo. $R = [x]$ è un dominio a ideali principali $[x]$ è dominio d'integrità poiché lo è.
Sia $I \subseteq R[x]$ ideale , $I \neq \{0\}$
Sia $f \in I \setminus \{0\}$ di grado minimo in I
Vogliamo dimostrare che $I = (f)$

- $(f) \subseteq I$, infatti se $f \in I$ allora $q \cdot f \in I \quad \forall q \in [x]$
- $I \subseteq (f)$, infatti $g \in I$ usiamo la divisione per f
  $\Rightarrow g = q \cdot f + r$ con $deg(r) < deg(f) \Rightarrow r = g - q \cdot f \in I$
  $\Rightarrow r = 0 \Rightarrow g = q \cdot f \in (f)$

Esercizio
Dimostrare che se

- R dominio d'integrità
- $R[x]$ dominio a ideali principali

Allora R è un campo
Soluzione
Dobbiamo verificare che dato $a \in R \setminus \{0\}$ esiste l'inverso moltiplicativo.
Consideriamo l'ideale $(a, x) \subseteq R[x]$
$R[x]$ a ideali principali $\Rightarrow \exists p \in R[x]$ tale che $(p) = (a, x)$
Quindi:

$$\Rightarrow a = q_1 \cdot p$$
$$\Rightarrow x = q_2 \cdot p \;\to\; ax = \tilde{q}_2 \cdot p$$

Deduciamo che q_1 e p sono entrambi costanti.
Infatti il termine di grado più alto del prodotto $q_1 \cdot p$ è il prodotto dei termini direttivi di p e di q_1 (Stiamo usando il fatto che R sia dominio d'integrità)
Se p costante

$$\Rightarrow q_2 = hx \text{ con } h \cdot p = 1$$

p invertibile $\Rightarrow (p) = R[x]$
$1 \in (a, x) \Rightarrow$ esistono $s, t \in R[x]$:

$$1 = a \cdot s + t \cdot x \Rightarrow s = \sum_{i \geq 0} s_i x^i \Rightarrow a s_0 = 1.$$

Esercizio/Proposizione
R dominio a ideali principali. I ideale, Se I è primo, allora I è massimale.
Soluzione
$I = (p) \subseteq R$
I primo. Supponiamo che esista un ideale $J = (q) \subseteq R$ tale che $I \subseteq J$
$I \subseteq J \Rightarrow (p) \subseteq (q) \Rightarrow p = a \cdot q$ per qualche $a \in R$
I primo $\Rightarrow a \in I$ oppure $q \in I$

$$\begin{aligned} \text{q} \in I &\Rightarrow q \in (p) \\ &\Rightarrow (q) \subseteq (p) \\ &\Rightarrow J = I \end{aligned}$$

$$\begin{gathered} a \in I \Rightarrow a \in (p) \\ \Rightarrow a = k \cdot p \text{ per qualche } k \in R \\ \Rightarrow p = a \cdot q = p \cdot k \cdot q \\ \Rightarrow p \cdot (1 - k \cdot q) = 0 \\ \Rightarrow 1 + k \cdot q = 0 \Rightarrow q \text{ invertibile} \\ J = R \end{gathered}$$

R dominio a ideali principali (PID) allora un ideale è primo se e solo se è massimale Resta da verificare che I massimale $\Rightarrow I$ primo
I massimale $\Rightarrow R/I$ campo $\Rightarrow R/I$ dominio integrità $\Rightarrow I$ primo