Lezione 4 Algebra 1

Federico De Sisti

2025-03-13

0.1 Divisibilità

Notazione 1 (Divisibilità)
R dominio d'integrità $a, b \in R$
Diremo che:

- *a divide b se esiste $q \in R$ tale che $a \cdot q = b$ (scriviamo $a|b$)*
- *se $a|b$ allora a è <u>divisore</u> di b e b è <u>multiplo</u> di a*

Esercizio
R dominio d'integrità $a, b, c \in R$

1. se $a|b$ e $b|c \quad \Rightarrow \quad a|c$
2. se $a|b$ e $a|c \quad \Rightarrow \quad a|(b \pm c)$
3. se $a|b$ allora $a|b$
4. se $a|b$ e $b|a$
5. se $a|b$ e $b|a \ \Rightarrow \ \exists u, v \in R \ : \ \begin{cases} a = ab \\ b = va \\ uv = 1 \end{cases}$

Soluzione 4
per definizione esistono $u, v \in R$ tali che $\begin{cases} a = ub \\ b = va \end{cases}$
se $b = 0$
allora $a = 0 \ \Rightarrow$ avremmo potuto scegliere $u = v = 1$
se $b \neq 0$
Allora $b = va = vub \Rightarrow b(10vu) = 0$
$\Rightarrow 1 - vu = 0$ perché R dominio
$\Rightarrow u \cdot v = 1$

Definizione 1
R dominio d'integrità:

1. *$a \in R$ si dice unità se $a|1$.*
2. *$a, b \in R$ si dicono associati se $a|b$ e $b|a$*

Osservazione

1. $a \in R$ è unità se e solo se ammette inverso moltiplicativo.
2. dall'esercizio segue che a, b sono associati se si ottengono l'uno dall'altro moltiplicando per un invertibile.

Esercizio
R dominio d'integrità, dimostrare che:

1. $a, b \in \mathbb{Z}$ sono associati se e solo se $a = \pm b$
2. $\mathbb{K}$ campo. $f, g \in \mathbb{K}[x]$ sono associati se e solo se $f = \lambda g$ con $\lambda \in \mathbb{K} \setminus \{0\}$

Definizione 2
R dominio d'integrità. $a \in \mathbb{R} \setminus \{0\}$

1. *diremo che a è irriducibile se $a = b \cdot c \Rightarrow$ a, b associati oppure a, c associati*
2. *diremo che a è primo $a|b \cdot x \Rightarrow a|b$ oppure $a|c$*

Esercizio
determinare tutti gli irriducibile e i primi in $\mathbb{Z}$
Osservazione
R dominio d'integrità $a \in R$ primo
$\Rightarrow (a) \subseteq R$ è un ideale primo
Se $b, c \in R$ tali che $b \cdot c \in (a)$ allora $b \in (a)$ oppure $c \in (a)$
Ma $b \cdot c \in (a)$ se e solo se $a|b \cdot c$
L'ipotesi chi primalità implica che $a|b$ oppure $a|c \Rightarrow b \in (a)$ oppure $c \in (a)$
Esercizio:
R dominio ad ideali principali. Allora $a \in R$ irriducibile $\Rightarrow (a) \subseteq R$ massimale.
Soluzione
Sia $J \subseteq R$ ideale tale che $(a) \in J$. Per ipotesi $J = (b)$ pewr qualche $b \in R$
$(a) \subseteq (b) \Rightarrow b|a \Rightarrow \exists p \in R : a = b \cdot q$
Abbiamo due casi:
primo caso: a, b associati
Allora $\exists q \in R$ invertibile tale che $b = ua \Rightarrow (b) \subseteq (a)$
$J = (b) = (a)$
secondo caso: a, q associati
$\Rightarrow$ esiste $v \in R$ invertibile tale che $q = v \cdot a$
$\Rightarrow a = bq = bva$
$\Rightarrow a(1 - bv) = 0$
$\Rightarrow 1 - bv = 0$
$\Rightarrow b$ invertibile
$\Rightarrow J = (b) = R$
Quindi $(a) \subseteq R$ è massimale
Esercizio:
R dominio a ideali principali, allora se a è primo, a è irriducibile
Soluzione
$a \in \mathbb{R} \setminus \{0\}$ a primo verifichiamo che a irriducibile se $a = bc$ allora : $\begin{cases} b|a \\ c|a \\ a|b \cdot c \end{cases}$

Deduciamo che a, b associati oppure a, c associati $=>$ a irriducibile

Corollario 1
In $\mathbb{Z}$ a è primo se e solo se a è irriducibile

Dimostrazione
($\Rightarrow$) $(\mathbb{Z}, +, \cdot)$ *è dominio a ideali principali quindi per l'esercizio a primo* $\Rightarrow$ *a irriducibile*
($\Leftarrow$) *a irriducibile* $\Rightarrow (a) \subseteq \mathbb{Z}$ *massimale* $\Rightarrow (a) \subseteq \mathbb{Z}$ *è ideale primo* $\Rightarrow$ *a è primo in* $\mathbb{Z}$ $\square$
esercizio:
$R = \mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} | a, b \in \mathbb{Z}\}$
1) dimostrare che R è un dominio d'integrità
2) $3 \in R$ non è primo
3) $3 \in R$ è irriducibile **Soluzione**
1) $\mathbb{Z}[\sqrt{-5}]$ è un sottoanello di $\mathbb{C}$ ma $\mathbb{C}$ è un campo $\Rightarrow \mathbb{C}$ dominio d'integrità,
Quindi anche $\mathbb{Z}[\sqrt{-5}]$ è un dominio d'integrità.
2) $3 \cdot 7 = (4 + \sqrt{-5})(4 - \sqrt{-5})$.
Allora
3 divide $(4 + \sqrt{-5})(4 - \sqrt{-5})$
D'altra parte $\nmid (4 \pm \sqrt{-5})$
Infatti.
$3(a + b\sqrt{-5}) = 3a + 3b\sqrt{-5}$ Ma $3 \nmid 4$ in $\mathbb{Z}$
3) Verifichiamo che $3 \in R$ è irriducibile
Supponiamo che $3 = (a + b\sqrt{-5})(c + d\sqrt{-5})$
Vogliamo verificare che 3 e il primo termine oppure 3 e il secondo termine sono associati.
Considero $|| \cdot ||$ norma in $\mathbb{C}$

$$\begin{aligned} \Rightarrow 9 &= ||a + b\sqrt{-5}||^2 + ||c + d\sqrt{-5}||^2 \\ &= (a^2 + 5b^2) \cdot (c^2 + 5a^2) \end{aligned}$$

Quindi $a^2 + 5b^2 = \begin{cases} 1 \\ 3 \\ 9 \end{cases}$
$a^2 + 5b^2 = 3 \rightsquigarrow$ impossibile.
se $a^2 + 5b^2 = 9$
$\Rightarrow c^2 + 5d^2 = 1 \Rightarrow \begin{cases} c = \pm 1 \\ d = 0 \end{cases}$
Quindi
$3 = \alpha + \beta$ allora $\alpha = \pm 1 \rightsquigarrow 3, \beta$ associati
oppure $\beta = \pm 1 \rightsquigarrow 3, \alpha$ associati

0.2 UFD

Definizione 3
R dominio d'integrità, R si dice dominio a fattorizzazione unica se:

1. *per ogni $R \setminus \{0\}$ esiste una "fattorizzazione" $a = u \cdot b_1 \cdot \ldots \cdot b_h$ tale che*
   - *u unità in R*
   - *b_i irriducibile per ogni $i \in \{1, \ldots, h\}$*
2. *Se $a \cdot b_1 \cdot \ldots \cdot b_h = v \cdot c_1 \cdot \ldots \cdot c_k$ con*
   - *$h = k$*
   - *$\exists \omega \in S_h$ tale che $b_i, c_{\sigma(i)}$ associati per ogni $i \in \{1, \ldots, h\}$*

Teorema 1
R dominio d'integrità,
Allora R è UFD se e solo se valgono le seguenti condizioni:

1. *Ogni elemento irriducibile è primo*
2. *Data una successione in R di elementi $a_1, \ldots, a_2, \ldots, a_r, \ldots$ tali che $a_{i+1} \mid a_i \quad \forall i$ si ha che esiste $i \in \mathbb{Z}_{>1}$ tale che a_j, a_h siano associati $\forall h, k > 1$*

Dimostrazione
Supponiamo che R sia UFD
Verifichiamo (1):
Sia $a \in R \setminus \{0\}$ irriducibile.
Considero $b, c \in R$ tali che $a \mid bc$
Allora $\exists q \in R$ tale che.
$a \cdot q = b \cdot c$
Sfrutto l'ipotesi UFD

$$q = \varepsilon \cdot t_1, \ldots, t_m.$$
$$b = \eta \cdot r_1, \ldots, r_n.$$
$$c = \delta \cdot s_1, \ldots, s_h.$$

dove $\varepsilon, \eta, \delta$ unità in R
t_i, s_i, r_i irriducibili in R
$\Rightarrow \varepsilon \cdot a \cdot t_1 \ldots t_m = (\delta\eta) r_1, \ldots, r_n \cdot s_1, \ldots, s_h$
Per unicità della fattorizzazione a è associato a un qualche r_i (se $a \mid b$) oppure s_i (se $a \mid c$)
quindi a è primo

Verifichiamo che $UFD \Rightarrow 2$
Sia $a_1, \dots, a_i, \dots$
una successione in R *tale che* $a_{i+1} \mid a_i \quad \forall i$
Denotiamo: $n_i =$ *numero di irriducibili in una (qualsiasi) fattorizzazione di* a_i
$\Rightarrow n_{i+1} \leq n_i$
Ho una successione $n_1, n_2, \dots, n_i, \dots$ *monotona decrescente*
$\Rightarrow$ *definitivamente costante*
$\Rightarrow \exists \underline{i} \in \mathbb{Z}_{\geq 1}$ *tale che* $n_j = n_{\underline{i}} \quad \forall j \geq i$
Allora l'ipotesi
$a_k \mid a_{\underline{i}} \quad$ *per* $k \geq \underline{i}$
$\Rightarrow a_k \cdot q_k = a_{\underline{i}}$
e $UFD \Rightarrow q_k$ *invertibile.*
Quindi $a_k, a_{\underline{i}}$ *associati*
$\forall k \geq i \Rightarrow (2)$
Supponiamo ora che esistano valgano (1) *e* (2) *verifichiamo che* R *è* UFD
Esistenza: sia $a_1 \in R$ *non invertibile e non irriducibile*
$\Rightarrow a_1 = a_2 \cdot b_2$ *tale che*
a_1, a_2 *non associati*
a_1, b_2 *non associati*
Se per assurdo a_1 *non ammette fattorizzazione lo stesso vale per* a_2 *oppure* b_2
abbiamo costruito a_2 *che*

- $a_2 \mid a_1$
- a_2 *non ammette fattorizzazione e non è invertibile e non è associato ad* a_1

□