Lezione 20 Algebra I

Federico De Sisti

2024-12-05

1 Argomenti dell'esonero

Al massimo ci sta qualcosa sugli anelli

2 Gli anelli

Definizione 1
Un anello $(R, +, \cdot)$ *è un insieme* R *dotato di due operazioni,* $+, \cdot$ *che soddisfano le seguenti:*

1. $(R, +)$ *è un gruppo abeliano*
2. *L'operazione* $\cdot$ *è associativa* $(a \cdot b \cdot c = (a \cdot b) \cdot c = a \cdot (b \cdot c) \quad \forall a, b, c \in R)$
3. $\exists 1 \in R$ *tale che* $1 \cdot a = a \cdot 1 = a \ \ \forall a \in R$ (R *è unitario*)
4. *Vale la legge distributiva*
   $(a + b) \cdot c = a \cdot c + b \cdot c$
   $c \cdot (a + b) = c \cdot a + c \cdot b \ \ \forall a, b, c \in R$

Nota
Artin richiede anche la commutatività

Definizione 2
Un anello $(\mathbb{R}, +, \cdot)$ *si dice commutativo se*

$$a \cdot b = b \cdot a \ \ \forall a, b \in R.$$

Esempi
1)$(\mathbb{Z}, +, \cdot)$ è un anello commutativo
2)$Mat_{2\times 2}(\mathbb{Q})$ è un anello non commutativo

Definizione 3 (Dominiio d'integrità)
Un dominio d'integrità è un anello commutativo tale che

1. $0 \neq 1$
2. $\forall a, b \in R$ *tale che* $a \cdot b = 0$ *si ha* $a = 0$ *oppure* $b = 0$

0 *denota l'elemento neutro del gruppo* $(R, +)$
Si dice che R *non ha divisori dello* 0

Esempio:
$R = \{e\}$
$e + e = e$
$e \cdot e = e$
$(R, +, \cdot)$ è un anello che soddisfa $0 = 1$

Si chiama Anello Banale (Zero Ring)
Esercizio
$(R, +, \cdot)$ anello
1) dimostrare che

$$a \cdot 0 = 0 \cdot a = 0 \quad \forall a \in R$$

2) dimostrare che

$$(-a) \cdot b = a \cdot (-b) = -(a \cdot b)$$

3) se $0 = 1$ allora R è l'anello banale (ovvero $|R| = 1$)

Definizione 4
$(R, +, \cdot)$ anello.
Un sottoanello di R è un sottoinsieme $A \subseteq R$ tale che:

1. $(A, +) \leq (R, +)$
2. $1 \in A$
3. *A è chiuso rispetto all'operazione $\cdot$*

Esempi
$M \geq 2$ intero
$(\mathbb{Z}/(m), +)$ gruppo abeliano
$(\mathbb{Z}/(m), +, \cdot)$ è un anello commutativo
IN generale non è un dominio d'integrità.
Ad esempio se $m = 6$
$[2][3] = [6] = [0]$
quindi $[2]$ e $[3]$ sono divisori di $[0]$ in $\mathbb{Z}/(6)$

Proposizione 1
$m \geq 2$ è intero allora $\mathbb{Z}/(m)$ è un dominio d'integrità se e solo se m è primo

Dimostrazione
Se m non è primo allora esistono $1 < a, b < m$ tali che $m = ab$
Allora $[a] \cdot [b] = [m] = [0]$ e $[a]$ è un divisore dello zero
Viceversa se m è primo dobbiamo dimostrare che non esistono zero divisori
Considero $[a] \in \mathbb{Z}/(m)$ con $[a] \neq [0]$
Assumo che $0 < a < m$
Allora $MCD(a, m) = 1$
$\Rightarrow (a) + (m) = (1) = \mathbb{Z}$
$\Rightarrow \exists k, h \in \mathbb{Z}$ *tali che* $ka + hm = 1$
$\Rightarrow [k] \cdot [a] = [1] \in \mathbb{Z}/(m)$
Ora se esiste $[b] \in \mathbb{Z}/(m)$ tale che

$[a] \cdot [b] = [0]$
$\Rightarrow [k] \cdot [a] \cdot [b] = [k] \cdot [0]$
$\Rightarrow [b] = [0]$
$\Rightarrow [a]$ *non è zero divisore* $\square$

Osservazione
Abbiamo dimostrato che se $a \in R$ ammette un inverso moltiplicativo allora R è un dominio d'integrità (assumendo "solo" che R sia anello commutativo)

Definizione 5
Un anello $(R, +, \cdot)$ *si dice corpo se*
$0 \neq 1$
$\forall a \in R,\ \exists a^{-1} \in R$ *t.c.*
$a^{-1} \cdot a = a \cdot a^{-1} = 1$ a^{-1} *si dice inverso moltiplicativo*

Definizione 6
Un campo è un corpo commutativo

Osservazione
Se $(R, +, \cdot)$ anello $a \in R$ che ammette inverso moltiplicativo $a^{-1} \in R$ Allora a non è zero divisore
Infatti se $\exists b \in R$ t.c. $a \cdot b = 0$
$0 = a^{-1} \cdot (a \cdot b) = a^{-1} \cdot a \cdot b = (a^{-1} \cdot a) \cdot b = b$
$1 \cdot b = 0 \Rightarrow b = 0$
$\Rightarrow a$ non è divisore di 0

Corollario 1
Ogni campo è un dominio d'integrità

Dimostrazione
$\forall a \in R$ *esiste* $a^{-1} \Rightarrow R$ *dominio d'integrità* $\square$

Osservazione

$$\begin{tikzcd}
& \text{CAMPO} \arrow[dl, Rightarrow] \arrow[dr] & \\
\text{CORPO} \arrow[d, Rrightarrow] & & \text{DOMINIO D'INTEGRITÀ} \arrow[d] \\
\text{ANELLO} \arrow[rr] & & \text{ANELLO COMMUTATIVO}
\end{tikzcd}$$

Esempio: 1) $\mathbb{H}$ quaternioni è un corpo
infatti $i^2 = j^2 = k^2 = ijk = -1$ $q \in \mathbb{H}$
$\rightsquigarrow q = x + yi + zj + wk \in \mathbb{H}, \quad x, y, z, w \in \mathbb{R}$
$\rightsquigarrow \overline{q} := x - yi - zj - wk$ (coniugato)
$\rightsquigarrow |q|^2 = q\overline{q} = x^2 + y^2 + z^2 + w^2$
$\rightsquigarrow q \cdot \frac{\overline{q}}{|q|^2} = 1$ quindi tutti invertibili (tranne 0) $\Rightarrow \mathbb{H}$ è un corpo

Proposizione 2
Ogni dominio d'integrità finito è un campo

Dimostrazione
$(R, +, \cdot)$ dominio finito. Dato $a \in R \setminus \{0\}$ vogliamo dimostrare che esiste a^{-1}
Idea:
considero la funzione $\begin{aligned} \varphi_a :& R \to R \\ & b \to a \cdot b \end{aligned}$ *φ_a è iniettiva. Infatti φ_a è un omomorfismo di gruppi*
$(R, +) \to (R, +)$ per la distributività
Inoltre
$ker(\varphi_a) = \{b \in R | \varphi_a(b) = 0\} = \{b \in R | a \cdot b = 0\} = \{0\}$ (dato che R è dominio)
$\Rightarrow \varphi_a$ è iniettiva
Ora dato che $|R| < +\infty$ φ_a è biunivoca
Quindi nell'immagine di ϕ_a abbiamo 1
$\Rightarrow b \in R$ tale che $\varphi_a(b) = 1$ ovvero $a \cdot b = 1$
$\Rightarrow b$ è l'inverso moltiplicativo di a $\square$

Definizione 7
Dati $(R_1, +, \cdot)$ e $(R_2, \oplus, \odot)$ anelli, un omomorfismo di anelli è una funzione $f : R_1 \to R_2$ tale che

1. $f(a + b) = f(a) \oplus f(b)$
2. $f(a \cdot b) = f(a) \odot f(b)$
3. $f(1_{R_1}) = 1_{R_2} \quad \forall a, b \in R_1$

2.1 Idee per gli esercizi

1)$(R, +,)$ anello $a \in R$
$0 \cdot a = (0 + 0) \cdot a = 0 \cdot a + 0 \cdot a$
$\Rightarrow -(0 \cdot a) + (0 \cdot a) = -(0 \cdot a) + (0 \cdot a) + (0 \cdot a)$
$\Rightarrow 0 = 0 \cdot a$
2) $a, b \in R$
$0 = 0 \cdot b = (a + (-a)) \cdot b = a \cdot b + (-a) \cdot b$
Sommando $-(a \cdot b)$ ad entrambi i membri ottengo:
$-(ab) = -(a)b$