Lezione 1 Algebra

Federico De Sisti

2024-10-01

1 Cosa c'è su e-leaning di Francesco Mazzini

Date appelli
Esercizi settimanali
All'esame ti chiedono due esercizi delle schede scelti a caso
Ci sono 2 esoneri (primo 17 dicembre) (secondo ?? maggio)
Libri
M. Artin Algebra
IN. Hernstein: Algebra (difficile)

2 Gruppi

Definizione 1 (Gruppo)
Un gruppo è un dato di un insieme G con un'operazione $\cdot$ tali che:
1) L'operazione è associativa

$$f \cdot (gh) = (f \cdot g) \cdot h \qquad \forall f, g, h \in G$$

2) Esistenza elemento neutro

$$\exists e \in G \text{ tale che } g \cdot e = e \cdot g = g \quad \forall g \in G.$$

3) esistenza degli inversi

$$\forall g \in G \qquad \exists \qquad g^{-1} \in G \quad \text{tale che } g^{-1} \cdot g = g \cdot g^{-1} = e.$$

Nomenclatura 1 (notazione)
$(G, \cdot)$ *dato* $g \in G$ *denotiamo con:*
1) $g^0 = e$
2)$g^1 = g$
3)$g^n = g \cdot \ldots \cdot g 4) g^{-n} = (g^{-1})^n$

Osservazione:
Con questa notazione:

$$(g^n)^m = g^{nm}$$
$$g^n \cdot g^m = g^{n+m}$$

Esempi
1) $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +)$
2) $GL_n(\mathbb{K}) = \{A \in Mat_{n \times n}(\mathbb{K}) | det(A) \neq 0\}$ con prodotto
3) $SL_n(\mathbb{K}) = \{A \in Mat_{nn}(\mathbb{K}) | det(A) = 1\}$
4) X insieme

$$S_X = \{ \text{ funzioni } X \to X \text{ invertibili}\}$$

Speciale Se $X = \{1, \ldots, n\}$
Allora chiamiamo

$$S_n = S_X.$$

(è i lgruppo di permutazioni su n elementi)
Si chiama gruppo simmetrico

Definizione 2 (Gruppo diedrale)
$n \geq 3$ Consideriamo l'n-agono regoalre nel piano (3-agono, triangolo)
D_n è l'insieme delle simmetrie del piano che preservano l' n-agono
Si chiama gruppo diedrale, l'operazione è la composizione

Esempio:
Per $n = 3$ abbiamo D_3
TODO INSERISCI DISEGNO gruppo diedrale
Esercizio
Determina gli inversi e tutti i possibili prodotti degli elementi di D_3

Definizione 3 (Gruppo Abeliano)
$(G,)$ gruppo si dice Abeliano se l'operazione è commutativa

$$f \cdot g = g \cdot f)$$

Definizione 4 (Gruppo finito)
$(G, \cdot)$ gruppo si dice finito se la sua cardinalità è finita

$$|G| < +\infty$$

Definizione 5 (Ordine del gruppo)
$L(G, \cdot)$ gruppo, l'ordine di G è $|G|$

Definizione 6 (Ordine di un elemento)
$ord(g) = \min\{n \in \mathbb{N} | g^n = e\}$
se $\nexists n \in \mathbb{N}$ tale che $g^n = e \quad$ poniamo $\quad ord(g) = +\infty$

Definizione 7 (Gruppo ciclico)
$n \geq 3$ consideriamo C_n l'insieme delle isometrie del piano che preservano l' n-agono e preservano l'orientazione, questo si chiama gruppo cicliclo

Esempio
Nel caso di $n = 3$ abbiamo solamente 3 elementi: identità, e le due rotazioni (ordine dispari) **Esercizi**
1) si dimostri che l'elemento neutro in un gruppo è unico

2) si dimostri che ogni elemento in un gruppo ammette un unico elemento inverso
per casa
1) Trvoare un'applicazione biunivoca $S_3 \to D_3$
2) Dimostrare che non esiste un'applicazione biunivoca $S_4 \to D_4$
3) Dimostrare che i seguenti nkn sono gruppi
$\cdot Mat_{n\times n}(\mathbb{K})$ con prodotto riche per colonne
$GL(\mathbb{K})$ con somma tra matrici
$\mathbb{Z}\mathbb{Q}\mathbb{R}conilprodotto$

Proposizione 1
$(G, \cdot)$ gruppi finito, Allora ogni elemento ah ordine finito

Dimostrazione
$g \in G$ Considero il sottoinsieme

$$A = \{g, g^2, g^3, \dots\} \subseteq G.$$

quindi $|A| < +\infty \Rightarrow \exists s, t \in \mathbb{N}, s > t$ tali che

$$g^s = g^t.$$

Moltiplico per g^{-t} a destra

$$g^s = g^t \quad \Rightarrow \quad g^s \cdot g^{-t} = g^t \cdot g^{-t} \quad \Rightarrow \quad g^{s-t} = e.$$

Quindi $n = s - t \geq 1$ e $g^n = e \Rightarrow ord(g) \leq n < +\infty$ □

Definizione 8 (Sottogruppo)
$(G, \cdot)$ gruppo $H \subseteq G$ sottosinsieme, si dice che H è un sottogruppo se $(H, \cdot)$ è un gruppo.
In tal caso scriveremo $H \leq G$

Osservazione
$(G, \cdot)$ gruppo, $G \subseteq G$ sottoinsieme allora $H \leq G$se H è chiuso rispettto a $\cdot$
e H è chiuso rispetto agli inversi
(se $g, h \in G \Rightarrow g \cdot h \in H$ e se $h \in H \Rightarrow h^{-1} \in H$)

Proposizione 2
$(G, \cdot)$ gruppo $H \subseteq G$ sottoinsieme con $|H| < +\infty$ Allora:
1) $H \leq G$ se e solo se H è chiuso rispetto a $\cdot$

Dimostrazione
($\Rightarrow$) *ovvia*
($\Leftarrow$) *basta dimostrare che H è chiuso rispetto alĺ inverso ovvero*

se $|H| < +\infty$
e H *chiuso rispetto a* $\cdot$
Allora H *è chiuso rispetto agli inversi*
Sia $h \in H$
$A = \{h, h^2, h^3, \dots\} \subseteq H$
Allora $|A| < \infty$
Ragionando come prima deduciamo $ord(h) < +\infty$

$$h \cdot h^{ord(h)-1} = h^{ord(h)-1} \cdot h = e.$$

Quindi $h^{-1} = h^{ord(h)-1} = h \cdot \ldots \cdot h \in H \Rightarrow h^{-1} \in H$ $\square$

Esempi
1)$C_n \leq D_n$
2) $SL_n(\mathbb{K}) \leq GL_n(\mathbb{K})$
3) $(G, \cdot)$ gruppo $g \in G$

$$< g >= \{g^n \in G | n \in \mathbb{Z}\}.$$

Allora $< g > \leq G$
Congruenze
$(G, \cdot)$ gruppo $H \leq G$

Definizione 9
$f, g \in G$ si dicono congruenti modulo H se

$$f^{-1}g \in H.$$

In tal caso scriveremo

$$f \equiv g \quad mod \quad H.$$

Esercizio
Dimostrare che al congruenza modulo H definisce una relazione di equivalenza su G
Suggerimento
$(f^{-1} \cdot g)^{-1} = g^{-1} \cdot (f^{-1})^{-1} = g^{-1} \cdot f$
e H è chiuso rispetto agli inversi
Esercizi:
$(G, \cdot)$ è un gruppo $H \leq G$ Allora la classe di equivalenza di $g \in G$ modulo H è il sottoinsieme

$$gH = \{g \cdot h | h \in H\}.$$

C'è una classe di equivalenza speciale in G data da

$$e \cdot H = H.$$

l'unica ad essere un sottogruppo

Dimostrare che esiste un'applicazione biunivoca tra $H \to gH \quad \forall g \in G$