Lezione 2 Algebra 1

Federico De Sisti

2024-10-03

1 Nelle lezioni precedenti...

Definizione 1
$(G, \cdot)$ gruppo $H \leq G$ $f, g \in G$ si dicono congruenti modulo H se
$f^{-1} \cdot g \in H$

2 Classi di equivalenza

Notazione 1
classi di equivalenza:

$$G/H.$$

Esempi importanti
$(G, \cdot) = (\mathbb{Z}, +)$ $H = (m) = \{am | a \in \mathbb{Z}\}$ con m fissato
$G/H = \mathbb{Z}/(m)$
Attenzione
potete definire $f = g \bmod H$ tramite la condizione $f \cdot g^{-1}$
Le due definizioni non sono equivalenti [La chiameremo congruenza destra]

Notazione 2
L'insieme delle classi di equivalenza destra si indica con

$$H \backslash G.$$

Definizione 2
Gli elementi di G/H si chiamano laterali sinistri, quelli di $H \backslash G$ si chiamano laterali destri

Esercizio:
$(G, \cdot)$ gruppo
$H \leq G$ $g \in G$ fissato
Allora il laterale sinistro a cui appartiene g è

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

Soluzione
fisso $f \in G$ e osserviamo che

$$g \equiv f \bmod H.$$

Se e solo se $g^{-1} \cdot f \in H$.
Questo è equivalente a

$$\exists h \in H \text{ tale che } g^{-1} \cdot f = h.$$

ovvero

$$\exists h \in H \text{ tale che } f = g \cdot h.$$

Esercizio
$H \leq G$
Allora $|G/H| = |H \backslash G|$
Soluzione
Basta eseguire un'applicazione biunivoca tra i due insiemi

Definizione 3
$(G, \cdot)$ gruppo $H \leq G$ si dice sottogruppo normale se $gH = Hg \quad \forall g \in G$

Esempio
$G = S_3$ ricordo che S_3 è il gruppo di permutazioni dell'insimee $\{1, 2, 3\}$
Quali sono gli elementi di S_3?

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = (2, 3)$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (3, 2, 1)$$

scambio il 3 con l'uno , il 2 con il 2
(2,3,1)
(1,3)
(1,2)
Id

$$H_1 =< (1, 2) >= \{id, (1, 2)\}.$$

$$H_2 =< (3, 2, 1) >= \{id, (3, 2, 1), (2, 3, 1)\}.$$

Esercizio— Dimostrare che $H_1 \leq S_3$ <u>non</u> è normale, mentre $H_2 \leq S_3$ è normale

Notazione 3
Se $H \leq G$ è normale scriveremo

$$H \trianglelefteq G.$$

Esercizio
$H \leq G$ sottogruppo dimostrare che l'applicazione $\phi : H \to gH$
$g \to g \cdot h$
Soluzione
ϕ è suriettiva per definizione di gH
è anche iniettiva infatti se $h_1, h_1 \in H$ soddisfano

$$gh_1 = gh_2 \quad .$$

allora $h_1 = h_2$ (per la legge di cancellazione)
Ossercazione
$(G, \cdot)$ gruppo
$H \leq G$ Allora

$$|gH| = |Hg| \quad \forall g \in G.$$

anche se $gH \neq Hg$ poiché hanno entrambi la stessa cardinalità di H
Inoltre tutti i laterali sinistri (e destri) hanno la stessa cardinalità

Definizione 4
$(G, \cdot)$ gruppo, $H \leq G$ l'indice di H in G è

$$[G : H] = |G/H|.$$

dove $|G/H|$ è il numero di classi laterali sinistre

Osservazione
$H \leq G$ sottogruppo
Se G è abeliano allora $H \trianglelefteq G$
Il viceversa è falso! Possono esistere sottogruppi normali in gruppi non abeliani

Proposizione 1
$(G, \cdot)$ gruppo $H \leq G$ allora

$$|G| = [G : H]|H|.$$

Dimostrazione
Basta ricordare che la cardinalità di ciascun laterale sinistro è pari a $|H|$ $\square$
Osservazione
$H \subseteq G => [G : H] = \dfrac{|G|}{|H|}$

Teorema 1 (Lagrange)
$(G, \cdot)$ gruppo $H \leq G$ Allora l'ordine di H divide l'ordine di G

Dimostrazione
Dall'osservazione segue $\dfrac{|G|}{|H|} = [G : H] \in \mathbb{N}$ $\square$

Corollario 1
$(G, \cdot)$ gruppo di ordine primo (ovvero $|G| = p$ con p primo)
Allora G non contiene sottogruppi non banali (tutto il gruppo o il gruppo minimale)

Dimostrazione
Sia $H \leq G$ *allora per Lagrange abbiamo*

$$|H| \text{ divide } p.$$

$\Rightarrow |H| = 1$ *quindi* $H = \{e\}$
oppure $\Rightarrow |H| = p$ *quindi* $H = H$

$\square$

Corollario 2
$(G, \cdot)$ *gruppo (finito)*
Dato $g \in G$ *si ha* $ord(g)$ *divide l'ordine di* G

Dimostrazione
Dato $g \in G$ *considero*

$$< g >= \{e, g, g^2, \ldots, g^{n-1}\}$$
$$| < g > | = ord(g).$$

La tesi segue ora da Lagrange $\square$

3 Operazioni fra sottogruppi

Proposizione 2
$(G, \cdot)$ *gruppo* $H, K \leq G$
Allora $H \cap K \leq G$

Dimostrazione
$H \cap K$ *è chiuso rispetto all'operazione e agli inversi poiché sia* H *che* K *che lo sono* $\square$

Esercizio
Esibire due sottogruppi $H, J \leq G$ tali che $H \cup K$ non è un gruppo

Definizione 5
Dati $H, K \leq G$ *definiamo il* *sottoinsieme*

$$HK = \{h \cdot k | h \in H, k \in K\}.$$

Attenzione *non è necessariamente un sottogruppo*

Esercizio
Dimostrare che HK è un sottogruppo, di G se e solo se

$$HK = KH.$$

Soluzione
Supponiamo che HK sia un sottogruppo

$$HK = (HK)^{-1} = \{(h \cdot k)^{-1} | h \in H, k \in K\} = K^{-1}H^{-1} = KH.$$

Viceversa supponiamo che $HK = KH$
1) Dimostro che KH è chiuso rispetto all'operazione.
$h_1 k_1 \in HK$ e $h_2 \cdot k_2 \in HK$

$$(h_1 \cdot k_1) \cdot (h_2 \cdot k_2) = h_1 \cdot (k_1 \cdot h_2) \cdot k_2 = h_1 \cdot h_3 \cdot k_3 \cdot k_2 = (h_1 \cdot h_3) \cdot (k_3 \cdot k_1).$$

2) HK è chiuso rispetto agli inversi

$$h \cdot k \in HK \rightsquigarrow (h \cdot k)^{-1} = k^{-1} \cdot h^{-1} = h_4 \cdot k_4 \in HK.$$

Definizione 6 (Sottogruppo generato da un sottoinsieme)
$(G, \cdot)$ gruppo $X \subseteq G$ sottoinsieme
Il sottogruppo generato da X è

$$< X >= \bigcap_{H \leq G, X \subseteq H} H.$$

Notazione 4
$\cdot H, K \leq G$

$$< H, K >:=< H \cup K > .$$

$\cdot g_1, , g_n \in G$

$$< g_1, \ldots, g_n >:=< \{g_1, \ldots, g_n\} > .$$

Caso Speciale
$(G, \cdot) = (\mathbb{Z}, +) \quad m \in \mathbb{Z}$
$(m) :=< m >$

4 Sottogruppi di Z

Ricordo
dato $a \in \mathbb{Z}$ si ha $(a) \leq \mathbb{Z}$
Obbiettivo
non esisotno altri sottogruppi

Teorema 2
$H \leq \mathbb{Z}$ allora esiste $m \in \mathbb{Z}$ tale che $H = (m)$

Dimostrazione
Distinguiamo due casi:
1) $H = (0)$ finito
2) $H \neq (0)$ allora H contiene (almeno) un intero positivo, Definiamo

$$m := \min\{n \in \mathbb{Z} | n \geq 1, n \in H\}.$$

Vogliamo verificare che $H = (m)$ Sicureamente $(m) \subseteq H$ poich$H \leq \mathbb{Z}$
$Viceversasupponiamoche \exists n \in H x(n)$.
Allora

$$n = qm - r \textit{ per qualche } q \in \mathbb{Z} \quad 0 < r < m.$$

$\rightarrow r = n - qm \in H$
Ma $r > 0, r < m$ quindi otteniamo l'assurdo per minimalità di m

$\square$

Proposizione 3
$a, b \in \mathbb{Z}$, Allora:
$1)(a) \cap (b) = (n)$ *dove* $m := mcm\{a, b\}$
$2)(a) + (b) = (d)$ *dove* $d := MCD\{a, b\}$

Osservazione
$(a) + (b)$ è della forma HK con $H = (a)$ e $K = (b)$
inoltre $(a) + (b) \leq \mathbb{Z}$ poich$(\mathbb{Z}, +)$ è abeliano
Dimostrazione
$1)(a) \cap (b)$ *è il sottogruppo dei multipli di a e di b*
Dunque $(a) \cap (b) = (m)$
$2)a + b \leq \mathbb{Z} \Rightarrow (a) + (b) = (d')$ *per teorema*
Dobbiamo verificare che $d' = d$

$$(d) = (a) + (b) \supseteq (a) \Rightarrow d' | a (d' \textit{ divide } a).$$

$$\Rightarrow \begin{cases} d' | a \\ d' | b \end{cases} \Rightarrow d' \leq d$$

$d' \in (a) + (b) \Rightarrow \exists h, k \in \mathbb{Z}$ *tale che* $d' = ha + kb$
Dunque:

$$\begin{cases} d | a \\ d | b \end{cases} \Rightarrow d | d' => d \leq d'$$

Allora $d = d'$ $\square$

5 Gruppi D_n e C_n

Ricordo
$n \geq 3$
Fissiamo un $n - agono$
$D_n = \{$isometrie che preservano l'n-agono$\}$
$C_n = \{$isometrie che preserrvano l'n-agono e l'orientazione$\}$

Teorema 3
$n \geq 3$ *Allora*

$$|D_n| = 2n$$

$$|C_n| = n$$

Dimostrazione
Fissiamo un lato l dell'n-agono. Un'isometria $\varphi \in D_n$ è univocamente determinata dall'immagine di $\varphi(l)$
Ho n scelte per il lato e per ogniuna di queste ho 2 scelte per le orientazione (mando il lato in se stesso? in quello dopo? in quello dopo ancora?, posso anche invertire la sua orientazione, i successivi lati vengono definiti da dove viene mandato il primo)
se non scegliamo l'orientazione, ci rimane il gruppo ciclico, e ciò conclude la dimostrazione □

Osservazione
La dimostrazione prova che

$$C_n =< \rho > .$$

dove ρ è la rotazione di angolo $\frac{2\pi}{n}$ attorno al centro dell'n-agono
Infatti $\rho \in C_n \Rightarrow < \rho > \subseteq C_n$ ma l'ordine di questa rotazione è n

$$| < \rho > | = ord(\rho) = n = |C_n| => C_n =< \rho > .$$

Osservazione
Dalla dimostrazione segue che D_n è costituito da n rotazioni
(della forma $\rho^i \quad i \in \{1, \ldots, n\}$
e n riflessioni

Proposizione 4
$n \geq 3$ *Allora:*
1)$D_n =< \rho, \sigma >$
Dove σ è una rotazione qualsiasi ($\sigma \in D_n \setminus C_n$)
2)$\rho^i \sigma = \sigma \rho^{n-i}$

Dimostrazione
1)Sicuramente $< \rho, \sigma > \subseteq D_n$
$H =< \rho >= \{Id, \rho, \rho^2, \ldots, \rho^{n-1}\}$
$K =< \sigma >= \{Id, \sigma\}$
$H \cap K = \{Id\}$

$$|KH| = \frac{|H||K|}{|H \cap K|} = 2n.$$

$\Rightarrow HK \subseteq D_n$ *(In particolare HK è sottogruppo)* $\Rightarrow D_n = HK =< \rho, \sigma >$
$\rho\sigma$ *<u>non</u> preserva l'orientazione*
$\Rightarrow \rho^i\sigma$ *è riflessione*
$\Rightarrow ord(\rho^i\sigma) = 2$
$\Rightarrow \rho^i\sigma\rho^i\sigma = Id$
$\Rightarrow \rho^i\sigma\rho^i = \sigma$
$\Rightarrow \sigma\rho^i = \rho^{n-1}\sigma$ $\square$