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 $X = \{1, \dots, n\}$
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

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

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 all' inverso ovvero*

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

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

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

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

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

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 $H \to gH \quad \forall g \in G$

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 $f = g \mod H$ 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

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

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 $H_1 \leq S_3$ non 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 $H \leq G$
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 $|H|$ □
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 $\dfrac{|G|}{|H|} = [G : H] \in \mathbb{N}$ □

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* $H = H$

□

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 □

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* □

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.
$h_1k_1 \in HK$ 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$\exists n \in Hx(n)$.
Allora

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

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

□

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 $d' = d$

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

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

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

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

Allora $d = d'$ □

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*
$\Rightarrow ord(\rho^i\sigma) = 2$
$\Rightarrow \rho^i\sigma\rho^i\sigma = Id$
$\Rightarrow \rho^i\sigma\rho^i = \sigma$
$\Rightarrow \sigma\rho^i = \rho^{n-1}\sigma$ □

Lezione 3 Algebra I

Federico De Sisti

2024-10-08

1 Altra roba sui gruppi

Proposizione 1 (Caratterizzazione dei sottogruppi normali)
$(G,\cdot)$ *gruppo,* $N \leq G$
Le seguenti sono equivalenti:
1)$gNg^{-1} \subseteq N \quad \forall g \in G$
2)$gNg^{-1} = N \quad \forall g \in G$
3)$N \trianglelefteq G$
4) *L'operazione* $G/N \times G/N \to G/N$
è ben posta $\quad (fN, gN) \to fgN$
o equivalentemente $N\backslash G \times n\backslash G \to n\backslash G$
$(Nf, Ng) \to Nfg$

Dimostrazione
$1 \to 2$
Verifichiamo che $N \subseteq gNg^{-1}$
Dato che $n \in N \Rightarrow n = g(g^{-1}ng)g^{-1}$ *basta dimostrare che* $g^{-1}ng \in N$
D'altra parte $g^{-1}ng \in g^{-1}Ng \subseteq N$ *(per ipotesi 1)*
$2 \to 3$
$\forall g \in G \quad \forall n \in N$
$gng^{-1} \in N$ *(per ipotesi 2)*

$$\begin{cases} gn \in Ng \\ ng^{-1} \in g^{-1}N \end{cases} \Rightarrow \begin{cases} gN \subseteq Ng (1) \\ Ng^{-1} \subseteq g^{-1}N (2) \end{cases} .$$

Il che è equivalente a dire che $gN = Ng$ *la prima condizione mi dice* $G/N \subseteq G/N$ *e la seconda dell'arbitrarietà di* g
$G/N \subseteq G/N$
$3 \to 4$
Datife$g \in G$ *abbiamo*

$$(Nf)(Ng) = (fN)(Ng) = fNg = (fN)g = (Nf)g = Nfg.$$

$4 \to 1$
Per ipotesi 4 $(Nf)(Ng) = Nfg \quad \forall f, g \in G$ *quindi*

$$nfn'g \in Nfg \quad \forall n, n' \in N.$$

dall'arbitrarietà di g*, scelgo* $g = f^{-1}$*, quindi*

$$nfn'f^{-1} \in N \quad \forall f \in G.$$

Moltiplico (a sinistra) per n^{-1} *e ottengo*

$$fn'f^{-1} \in N \quad \forall f \in G.$$

Dall'arbitrarietà di n' *otteniamo* $fNf^{-1} \subseteq N \quad \forall f \in G$ *che è la condizione (1)*
□

Osservazione
$(G, \cdot)$ gruppo, la proposizione ci dice che un sottogruppo H è normale se e solo se l'operazione indotta su G/H è ben definita

Teorema 1
$(G, \cdot)$ gruppo $N \trianglelefteq G$
Allora $(G/N, \cdot)$ è un gruppo (detto gruppo quoziente)

Dimostrazione
Associatività, ovvia
elemento neutro : $N = Ne$
elemento inverso di Ng è Ng^{-1} $\quad \forall g \in G$ □

Osservazione
$(G, \cdot)$ gruppo e $H \leq G$ t.c. $[G : H] = 2$ Allora $H \trianglelefteq G$
Infatti esistono solo due laterali sinistri o destri: H, G/H

Osservazione
$(G, \cdot)$ gruppo abeliano $\Rightarrow$ ogni sottogruppo è normale
Non vale sempre il viceversa

Esempio
Dimostrare che $Q = \{\pm 1, \pm i, \pm j, \pm k\}$
è un gruppo (rispetto al prodotto) non abeliano in cui però tutti i sottogruppi sono normali

Prodotti:
$i^2 = k^2 = j^2 = -1$
$ij = k \;\; jk = i \;\; ki = j$
$ji = -k \;\; kh = -i \;\; ik = -j$

Definizione 1
Siano $(G_1, \cdot)$ e $(G_2, *)$ gruppi
Sia φ un'applicazione
$\varphi : G_1 \to G_2$ si dice omomorfismo se:

$$\varphi(g \cdot f) = \varphi(g) * \varphi(f) \quad \forall g, f \in G_1.$$

Osservazione
Graficamente φ è un omomorfismo se

$$\begin{array}{ccc} (g,f) & G_1 \times G_1 \xrightarrow{\cdot} G_1 & (g,f) \longrightarrow g \cdot f \\ \downarrow & \downarrow{\scriptstyle \varphi\times\varphi} \quad \downarrow{\scriptstyle \varphi} & \downarrow \\ (\varphi(g), \varphi(f)) & G_2 \times G_2 \xrightarrow{*} G_2 & \varphi(g \cdot f) \end{array}$$

Esempi:
$(\mathbb{R}, +)$ gruppo additivo reali
$(\mathbb{R}_{>0}, \cdot)$ gruppo moltiplicativo reali positivi
Allora
$exp : \mathbb{R} \to \mathbb{R}_{>0}$
$x \to e^x$
è un omomorfismo infatti: $\forall x, y \in \mathbb{R}$

$$e^{x+y} = e^x \cdot e^y.$$

Esempio
$ln : \mathbb{R}_{>0} \to \mathbb{R}$
$x \to ln(x)$
è un omomorfismo, infatti $\ln(x \cdot y) = \ln(x) + \ln(y) \quad \forall x, y \in \mathbb{R}_{>0}$
Osservazione:
$l^0 = 1 \;\; ln(1) = 0$
0 è l'elemento neutro in $(\mathbb{R}, +)$
1 è l'elemento neutro in $(\mathbb{R}_{>0}, \cdot)$
Osservazione:
$e^{-x} = \frac{1}{e^x}$
Inverso di x in $(\mathbb{R}, +)$
è invero di e^x in $(\mathbb{R}_{>0}, \cdot)$
$\ln(\frac{1}{x}) = -\ln(x)$
Esercizio
$\varphi : G_1 \to G_2$ omomorfismo. Dimostrare
1)$\varphi(e_1) = e_2$
2)$\varphi(g^{-1}) = \varphi(g)^{-1} \;\; \forall g \in G_1$
Soluzione:
$\varphi(e_1) = \varphi(e_1 \cdot e_2) = \varphi(e_1) * \varphi(e_1)$
moltiplico per $\varphi(e_1)^{-1}$
$\Rightarrow e_2 = \varphi(e_1)^{-1} * \varphi(e_1) = \varphi(e_1)^{-1} * (\varphi(e_1) * \varphi(e_1)) = \varphi(e_1)$
Esempio: $(G, \cdot)$ gruppo, $N \trianglelefteq G$
Allora
$\pi : G \to G/N$
$g \to gN$
è un omomorfismo
Esempio
$det : GL_n(\mathbb{K}) \to \mathbb{K}^*$
dove $\mathbb{K}$ campo
$\mathbb{K}^* = \mathbb{K} \setminus \{0\}$ è un gruppo rispetto l prodotto
allora det è un omomorfismo
infatti:

$$\forall A, B \in GL_n(\mathbb{K}) \quad det(AB) = det(A)det(B).$$

in particoalre:
$det(Id) = 1$
$det(A^{-1}) = \frac{1}{det(A)} \quad \forall A \in GL_n(\mathbb{K})$

Definizione 2
$\varphi : G_1 \to G_2$ *omomorfismo*
il nucleo di φ *è* $ker(\varphi) := \{g \in G_1 | \varphi(g) = e\}$
L'immagine di ϕ *è*
$Im(\varphi) = \{h \in H_2 | \exists g \in G_1 : \varphi(g) = h\}$

Esercizio:
$\varphi : G_1 \to G_2$ omomorfismo
Allora $ker(\varphi) \trianglelefteq G_1$)
Soluzione
Chiamo $H : ker(\varphi)$
vorrei verificare che $gHg^{-1} \subseteq H \quad \forall g \in G_1$
scegliamo $h \in H$ (ovvero $\varphi(g) = e_2$)
$\Rightarrow \varphi(ghg^{-1}) = \varphi(g)\varphi(h)\varphi(g^{-1}) =$ per esercizio $= \varphi(g)\varphi(h)\varphi(g)^{-1} = e_2$
$\Rightarrow ghg^{-1} \in H \forall h \in H, \forall g \in G \Rightarrow gHg^{-1} \subseteq H$
Osservazione
$(G, \cdot)$ gruppo, $H \leq G$. Allora HG se e solo se esiste $\varphi : G_1 \to G_2$ omomorfismo tale che $H = ker(\varphi)$

Dimostrazione
Resta solo l'implicazione $\Rightarrow$
Sia $H \trianglelefteq G$. *considero l'omomorfismo*
$\pi : G \to G/H$
$\quad g \to gH$
chi è $ker(\pi)$
$ker(\pi) = \{g \in G | gH = H\} = \{g \in G | g \in H\} = H$ □

Esempio
$det : GL_n(\mathbb{K}) \to K^*$
$ker(det) := \{A \in GL_n(\mathbb{K}) | det(A) = 1\} = SL_n(\mathbb{K})$
quindi
$\mathrm{SL}_n(\mathbb{K}) \trianglelefteq GL_n(\mathbb{K})$
Esercizio
$(G, \cdot)$ gruppo $g \in G$ fissato
$\varphi : \mathbb{Z} \to G$
$\quad n \to g^n$
è un omomorfismo
determinare $ker\varphi$ e $Im\varphi$
Esercizio
Sia $\varphi : G_1 \to G_2$ omomorfismo
1) Se $H_1 \leq G_1 \Rightarrow \varphi(H_1) \leq G_2$
se $H_1 \trianglelefteq G_1 \Rightarrow \varphi(H_1) \trianglelefteq \varphi(G_1)$
1) Se $H_2 \leq G_2 \Rightarrow \varphi^{-1}(H_2) \leq G_1$
se $H_1 \trianglelefteq G_2 \Rightarrow \varphi^{-1}(H_2) \trianglelefteq \varphi(G_1)$

Lezione 4 Algebra I

Federico De Sisti

2024-10-10

1 Altre informazioni sugli omomorfismi

Esercizio
Sia $\varphi : G_1 \to G_2$ omomorfismo dei gruppi
$ker\varphi = \{g \in G_1 | \varphi(g) = e_2\}$
Dimostrare che
φ è iniettivo $\Leftrightarrow ker(\varphi) = \{e_1\}$
soluzione:
supponiamo che $ker(\varphi) = \{e_1\}$
Allora dati $g, h \in G_1$ t.c $\varphi(g) = \varphi(h)$
dobbiamo mostrare che $g = h$
moltiplico per $\varphi(h)^{-1}$

$$\begin{aligned} &\Rightarrow \varphi(h)^{-1} * \varphi(g) = e_2 \\ &\Rightarrow \varphi(h^{-1}) * \varphi(g) = e_2 \\ &\Rightarrow \varphi(h^{-1} \cdot g) = e_2 \\ &\Rightarrow h^{-1} \cdot g \in ker\varphi \\ &\Rightarrow h^{-1} \cdot g = e_1 \\ &\Rightarrow g = h \end{aligned}$$

Il viceversa è lasciato al lettore come esercizio
Soluzione di un esercizio passato
1)Se $H_1 \subseteq G_1$ dimostriamo che $\varphi(H_1) \trianglelefteq \varphi(G_1)$
Verifichiamo che

$$f\varphi(H_1)f^{-1} \subseteq \varphi(H_1) \quad \forall f \in (G_1).$$

Quindi basta dimostrare che
$\forall h \in H_1 \quad \forall g \in G_1$ abbiamo
$\varphi(g)\varphi(h)\varphi(g)^{-1} \in \varphi(H_1)$
Questo è equivalente a richiedere che

$$\varphi(g \cdot h \cdot g^{-1})\varphi(H_1).$$

Ma $ghg^{-1} \in gH_1g^{-1} = H_1$ dato che $H_1 \trianglelefteq G_1$

$$\begin{aligned} &\exists \tilde{h} \in H_1 \text{ t.c } g \cdot h \cdot g^{-1} = \tilde{h} \\ &\varphi(ghg^{-1}) = \varphi(\tilde{h}) \in \varphi(H_1) \end{aligned}$$

2) Se $H_2 \trianglelefteq G_2$ dimostriamo che $\varphi^{-1}(H_2) \trianglelefteq G_1$
Ho due omomorfismi,
li compongo:

$$\psi : G_1 \underset{\varphi}{\to} G_2 \underset{\pi}{\to} G_2/H_2.$$

Studia il $\ker(\psi)$
$\ker(\psi) := \{g \in G_1 | \psi(g) = H_2\} = \{g \in G_1 | \varphi(g)H_2 = H_2\}$
$ker(\psi) = \{g \in G | \varphi(g) \in H_2\} = \varphi^{-1}(H_2)$
Quindi $\varphi^{-1}(H_2)$ è il nucleo di un omomorfismo $\psi : G_1 \to G_2/H_2$ e dunque $\varphi^{-1}(H_2) \trianglelefteq G_1$
Osservazione:
Se $\varphi : G_1 \to G_2$
omomorfismo di gruppi
$H_2 = \{e_2\} \trianglelefteq G_2$
l'esercizio (2) ci dice che $\ker(\varphi) = \varphi^{-1}(\{e_2\}) \trianglelefteq G_1$
Osservazione
Dalla parte (1) segue che
$H_1 \leq G_1 \Rightarrow \varphi(H_1) \leq G_2$
Quindi se scelgo $H_1 = G_1 \leq G_1$
$\Rightarrow Im(\varphi) = \varphi(G_1) \leq G_2$

2 Parte figa della lezione

Lemma 1
$(G, \cdot)$ gruppo
$N \trianglelefteq G, H \trianglelefteq G$ sottogruppi normali
$\pi : G \to G/N$
Allora $\pi(H) = \pi(HN)$

Dimostrazione
$H \subseteq HN$ poiché $e \in N$ ogni elemento di H lo scrivo come lui stesso $e \Rightarrow$ $\pi(H) \subseteq \pi(HN)$
Viceversa dimostriamo che $\pi(HN) \subseteq \pi(H)$
infatti:
$\forall h \in H \quad \forall n \in N$
$\pi(hn) = \pi(h)\pi(n)$ *(omomorfismo)*
$n \in N$
$\Rightarrow \pi(n) = N \to \pi(h)\pi(e) = \pi(ne)$
$\pi(e) = N \qquad = \pi(n) \in \pi H$ □

Lemma 2
$(G, \cdot)$ *gruppo*
$\cdot H \trianglelefteq G$
$\cdot N \trianglelefteq G$
$\cdot \pi \to G/N$
Allora:
1)$\pi^{-1}(\pi(H)) = HN$
2) *se* $N \subseteq H \to \pi^{-1}(\pi(H)) = N$
3)$\bar{H} \leq G/N \to \pi(\pi^{-1}(\bar{H})) = \bar{H}$

Dimostrazione (1)
$\pi^{-1}(\pi(H)) =?$
osserviamo che dal lemma 1
$\pi(H) = \pi(HN) = HN$
dato che $\pi(hn) = \pi(h)\pi(n) = hn$
$\Rightarrow \pi^{-1}(\pi(H)) = \pi^{-1}(\pi(HN)) = \pi^{-1}(HN) \supseteq HN$
Resta da verificare che $\pi^{-1}(\pi(H)) \subseteq HN$

$$\begin{aligned}
\pi^{-1}(\pi(H)) &:= \{g \in G | \pi(g) \in \pi(H)\} \\
&= \{g \in G | \exists g \in H : \pi(g) = \pi(h)\} \\
&= \{g \in G | \exists h \in H : \pi(h)^{-1}\pi(g) = N\} \ N = \text{elemento neutro in } G \\
&= \{g \in G | \exists h \in H : \pi(hg) = N\} \\
&= \{g \in G | \exists h \in H : h^{-1}g \in N\} \\
&= \{g \in G | \exists h \in H : g \in hN \acute{r} brace \subseteq HN
\end{aligned}$$

segue (1) □

Dimostrazione (2)
È un caso particolare del punto 1, infatti se

$$N \subset H \Rightarrow HN = H.$$

□

Dimostrazione (3)
Segue dal fatto che π*è un omomorfismo suriettivo*

$$\pi(\pi^{-1}(\bar{H})) = \pi(G) \cap \bar{H} = \bar{H}.$$

□

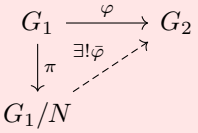
Teorema 1
$(G,\cdot)$, $n \trianglelefteq G$
Allora esistono due corrispondenze biunivoche

$$\{\textit{sottogruppi } H \leq G \;\; t.c. \;\; N \supseteq H\} \to \{\textit{sottogruppi di } G/N\}$$
$$H \to \pi(H)$$
$$\pi^{-1} \leftarrow \bar{H}$$
$$\{ \textit{ sottogruppi normali } H \trianglelefteq G \; t.c \; N \subseteq H\} \to \{ \textit{ sottogruppi normali } G/N\}$$
$$H \to \pi(H)$$
$$\pi^{-1}(\bar{H}) \to \bar{H}$$

Dimostrazione
Il lemma 2 (punti 2 e 3) garantisce che le due applicazioni $H \to \pi(H)$ $\pi^{-1}(H) \to \bar{H}$
sono una l'inversa dell'altra □
Osservazione:
Per la seconda corrispondenza osserviamo che per la suriettività di π e l'esercizio di oggi

$$H \trianglelefteq G \to \pi(H) \trianglelefteq G/N.$$

Teorema 2 (Teorema di omomorfismo)
$\varphi : G_1 \to G_2$ *omomorfismo*
$\cdot N \trianglelefteq G_1$
$\pi : G_1 \to G/N$
Allora:
1) esiste unico omomorfismo
$\bar{\varphi} G/N \to G_2$
t.c. $\bar{\varphi} \circ \pi = \varphi$



2) $Im(\bar{\varphi}) = Im(\varphi)$
3) $\bar{\varphi}$ *è iniettivo* $\Leftrightarrow ker\varphi = N$

Dimostrazione
La condizione $\bar{\varphi} \cdot \pi = \varphi$
Significa
$\forall g \in G_1$ *si ha*
$\bar{\varphi} \cdot \pi(g) = \varphi(g)$
ovvero
$\bar{\varphi}(gN) = \varphi(g)$
Dobbiamo verificare:
$\cdot$ *Unicità (segue da* $\bar{\varphi} \cdot \pi = \varphi$*)*
$\cdot \bar{\varphi}$ *è ben definita*

$\cdot\bar{\varphi}$ *è un omomorfismo*
significa che se $gN = fN$ *per qualche* $g, f \in G_1$, *allora* $\varphi(g) = \varphi(f)$
Verifichiamo:
$gN = fN \to g \equiv f mod N$
$\Rightarrow \exists n \in N$ *t.c.* $g^{-1}f = n$
$\Rightarrow f = gn \Rightarrow \varphi(f) = \varphi(gn)$
$\Rightarrow \varphi(f) = \varphi(g)\varphi(n) = \varphi(g)$
dato che $\varphi(n) = e_2$ *ovvero* $N \subseteq \ker\varphi$
Mostriamo adesso che $\bar{\varphi}$ ***è un omomorfismo***
Significa che $\forall f, g \in G$

$$\bar{\varphi}((fN)\cdot(gN)) = \bar{\varphi}(fN)\cdot\bar{\varphi}(gN).$$

Per definizione

$$\bar{\varphi}((fN)(gN)) = \bar{\varphi}(fgN) = \varphi(fg) = \varphi(f)\varphi(g).$$

2)$\bar{\varphi}\circ\pi = \varphi$
dalla suriettività del π *segue che* $Im(\bar{\varphi}) = Im(\varphi)$
3)$\bar{\varphi}$ *è iniettivo* $\Leftrightarrow ker\bar{\varphi} = \{N\}$
$ker\bar{\varphi} = \{gN \in G_1/N | \bar{\varphi}(gN) = e_2\}$
$= \{gN \in G_1/N | \varphi(g) = e_2\}$
$= \{gN \in G_1/N | g \in ker(\varphi)\}$ □

Corollario 1
$(G, \cdot)$, $N \trianglelefteq G$
Allora esiste una corrispondenza biunivoca

$$\{omomorfismi\ \varphi : G \to G'\ t.c.\ N \subseteq ker(\varphi)\} \to \{omomorfismi\ G/N \to G'\}$$
$$\varphi \to \bar{\varphi}$$
$$\pi \leftarrow \bar{\varphi}$$

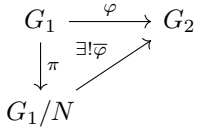
Dimostrazione
basta osservare che
dato $\bar{\varphi} : G/N \to G'$ *la composizione*
$\bar{\varphi}\circ\pi : G \to G'$ *è un omomorfismo*
tale che $ker(\bar{\varphi}\circ\pi) \supseteq N$
segue $\pi(N) = N$ *che è l'elemento neutro di* G/N
$\Rightarrow \bar{\varphi}\circ\pi(N) = e'$ *che è l'elemento neutro di* G'

□

Definizione 1
$\varphi : G_1 \to G_2$
omomorfismo si dice isomorfismo se è invertibile

Teorema 3 (Primo teorema di isomorfismo)
$\varphi : G_1 \to G_2$
Allora:
$Im(\varphi) \cong G_1/ker(\varphi)$
Dove $\cong$ *(isomorfo) significa che esiste un isomorfismo tra i due gruppi*

Dimostrazione



scelgo $N - ker\varphi$
il teorema di isomorfismo fornisce un omomorfismo iniettivo

$$\bar{\varphi} : G_1/\ker\varphi \to G_2.$$

Allora mi restringo all'immagine di $\bar{\varphi}$ *così diventa suriettiva*

$$G/ker\varphi \cong Im(\bar{\varphi}) \cong Im(\varphi).$$

la prima tramite $\bar{\varphi}$ *la seconda per il teorema di isomorfismo*
Applicazione:
det: $GL_n(\mathbb{K}) \to (\mathbb{K}^*, \cdot) = (\mathbb{K} \setminus \{0\}, \cdot)$
$\ker(det) = SL_n(\mathbb{K})$ *matrici con det 1*
$\Rightarrow GL_n(\mathbb{K})/SL_n(\mathbb{K}) \cong (\mathbb{K}^*, \cdot)$ □

Lezione 5 Algebra I

Federico De Sisti

2024-10-15

1 Teoremi di isomorfismo

Teorema 1 (Secondo teorema di isomorfismo)
$(G,\cdot)$ *gruppo*
$H, N \trianglelefteq G$ *tali che* $N \subseteq H$ *Allora*

1. $H/M \trianglelefteq G/N$
2. $G/N/H/N \cong G/H$

Dimostrazione

$$\begin{array}{ccc} G & \xrightarrow{\varphi=\pi_H} & G/H \\ \downarrow{\scriptstyle \pi} & \nearrow{\scriptstyle \exists!\overline{\varphi}} & \\ G/N & & \end{array}$$

π_H *proiezione sul quoziente* H

$N \subseteq H = ker(\varphi)$
Inoltre $Im(\bar{\varphi}) = Im(\varphi) = G/H$
Idea: *applicare il primo teorema di isomorfismo*
suriettiva $\bar{\varphi} : G/N \to G/H$
basta quindi dimostrare che $ker(\bar{\varphi}) = H/N$
Studiamo

$$ker(\bar{\varphi}) = \{gN \in G/N | \bar{\varphi}(gN) = H\}.$$
$$\{gN \in G/N | gH = H\}.$$
$$\{gN \in G/N | g \in H\} = H/N.$$

□

Corollario 1
In $(\mathbb{Z},+)$ *gruppo abeliano*
$a, n \in \mathbb{Z}$ *interi non nulli*
Denotiamo con

$$[a] = a + (n) \in \mathbb{Z}/(n) = \{[0],[1],[2],\ldots,[n-1]\}.$$

Allora $ord_{\mathbb{Z}/(n)}([a]) = \frac{n}{MCD(a,n)}$

Nota:
se $MCD(n,a) = 1$ allora a genera il gruppo ciclico $\mathbb{Z}/(n)$
Dimostrazione
Consideriamo $G = \mathbb{Z}$ $H = (a) + (n)$ $N = (n)$
Dal II Teorema di isomorfismo

$$\mathbb{Z}/(n) \Big/ ([a]) \cong \mathbb{Z}/(n) \Big/ (a) + (n)/(n) \cong G/N \Big/ H/N \cong G/N \cong \mathbb{Z}/(MCD(a,n)).$$

□

Confrontiamo le cardinalità

$$MCD(a,n) = |\mathbb{Z}/(MCD(a,n))|.$$
$$= |\mathbb{Z}/(n) \Big/ ([a])|$$

.

$$\frac{|Z/(n)|}{([a])} = \frac{n}{ord([a])}.$$
$$ord([a]) = \frac{n}{MCD(a,n)}.$$

Lemma 1
$a, bg \in Z$ non nulli
tali che $a|b$ (allora $(b) \subseteq (a)$
Allora

$$|(a)/(b)| = \frac{b}{a}.$$

Dimostrazione
Studiamo $(a)/(b)$
Per definizione è l'insieme dei laterali

$$(a)/(b) = \{ta + (b) | t \in \mathbb{Z}\}.$$

dobbiamo capire quanti laterali distinti esistono
Dati $t, s \in \mathbb{Z}$ tali che

$$ta + (b) = sa + (b).$$
$$\Leftrightarrow ta \equiv sa \ mod(b).$$
$$\Leftrightarrow -ta + sa \in (b).$$

Allora

$$(a)/(b) = \{ta + (b) | tt \in \{1, \dots, \frac{b}{a}\}\}.$$

□

Teorema 2 (III teorema di isomorfismo)
$(G, \cdot)$ *gruppo*

- $N \trianglelefteq G$

- $H \leq G$

Allora

1. $H \cap N \trianglelefteq H$
2. $H/H \cap N \cong HN/N$

Dimostrazione
$\pi_N : G \to G/N$
$g \to gN$
consideriamo la restrizione

$$\pi_N|_H : H \to G/H$$
$$h \to hN$$
$$ker(\pi_N|_H) = \{h \in H | \pi_N|_H(h) = N\}$$
$$= \{h \in H | hN = N\}$$
$$= \{h \in H | h \in N\}$$
$$= H \cap N$$

Deduciamo che $H \cap N \trianglelefteq N$
Idea: Applicare il I teorema di isomorfismo all'omomorfismo

$$\varphi = \pi_N|_H : H \to G/N.$$

Avremo $Im(\varphi) \cong H/ker(\varphi) = H/H \cap N$
Studiamo $Im(\varphi)$

$$Im(\varphi) = Im(\pi_N|_H) = \pi_N(H) = \pi_N(HN) = HN/N.$$

Il penultimo passaggio deriva da un lemma già visto a lezione □

Corollario 2
$a, b \in \mathbb{Z}$ *non nullli*
Allora $mcm(a, b) = \frac{ab}{MCD(a,b)}$

Dimostrazione
$G = \mathbb{Z}$
$H = (a)$
$N = (b)$
$H + N = (MCD(a, b))$

$H \cap N = (mcm(a,b))$
Dal III teorema di isomorfismo

$$(a)\Big/_{(mcm(a,b))} \cong H\Big/_{H\cap N} \cong HN\Big/_{N} \cong (MCD(a,b))\Big/_{(b)}.$$

Confrontiamo la cardinalità
Per il lemma

$$\frac{mcm(a,b)}{a} = |(a)(mcm(a,b))| = |(MCD(a,b))\Big/_{(b)} = \frac{b}{MCD(a,b)}.$$

Quindi

$$mcm(a,b) = \frac{ab}{MCD(a,b)}.$$

□

2 Classificazione di gruppi di ordine "piccolo" a meno di isomorfismo

Ordine 1
Se $|G| = 1 \quad \Rightarrow \quad G = \{e\}$
Ordine p primo:
Abbiamo mostrato che se $|G| = p$ allora G non ammette sottogruppi non banali
Sia $g \in G$ tale che $g \neq e \Rightarrow ord(g) = p \ \Rightarrow G =< g >$

$$\varphi : G \to G_p =< p >$$
$$g \to p$$

Obiettivo: classificare a meno di isomorfismo i gruppi di ordine 4 e di ordine 6

Definizione 1 (Klein,1884)
Il gruppo di Klein, K_4 è il gruppo delle isometrie del piano che preservano un rettangolo fissato.

Esercizio
Verificare che $K_4 = \{id, \rho, \sigma, \rho\sigma\}$
dove ρ = rotazione di angolo π
e dove σ = riflessione rispetto ad un lato **Osservazione**
tutti gli elementi in K_4 hanno ordine ≤ 2 Quindi $K_4 \neq C_4$
Dato che $K_4 =< \rho, \sigma >$
denoteremo anche

$$K_4 = D_2 \text{ (gruppo diedrale).}$$

Esercizio
$(G, \cdot)$ gruppo in cui ogni elemento ha ordine ≤ 2 (equivalentemente ogni elemento è inverso di se stesso)
1) Dimostrare che G è abeliano
2) Se $|G| = 4$ dimostrare che $G \cong K_4$ **Svolgimento** 1) Dati $f, g \in G$
$fg = (fg)^{-1} = g^{-1}f^{-1} = gf$
2) Sia $|G| = 4$
Scelgo $g, f \in G$ distinti tali che $\begin{cases} g \neq e \\ f \neq e \end{cases}$
Considero $H =< g, h >$
Per Lagrange
$H \geq 3$
$\Rightarrow H = H$
$\Rightarrow G = \{e, f, g, fg\}$
abeliano
Costruisco l'isomorfismo esplicito con K_4

$$\varphi : G \to K_4 =< \rho, \sigma >$$
$$e \to e$$
$$f \to \rho$$
$$g \to \sigma$$
$$fg \to \rho\sigma$$

che è chiaramente biunivoca ed è un omomorfismo $\Rightarrow \varphi$ è un isomorfismo

Lezione 6 Algebra I

Federico De Sisti

2024-10-21

1 Teoremi sulla cardinalità dei gruppi

Teorema 1
$(G, \cdot)$ gruppo. Se $|G| = 6$ allora
$G \cong C_6$ (abeliano) oppure $G \cong D_3$ (non abeliano)

Dimostrazione
Se G contiene un elemento di ordine 6 allora $G \cong C_6$
Se invece G non contiene elementi di ordine 6, per l'esercizio (2) esistono elementi $r, s \in G$ t.c. $ord(r) = 3$ e $ord(s) = 2$
Definisco:

$$G :=< r >= \{e, r, r^2\} \qquad k :=< s >= \{e, s\}.$$

$$H \cap K = \{e\}.$$

$$|HK| = \frac{|H||K|}{|H \cap K|} = 6 = |KH|.$$

$\Rightarrow HK = G = KH$
Esplicitamente:
$HK = \{e, r, r^2, s, rs, r^2s\}$
$KH = \{e, r, r^2, s, sr, sr^2\}$
Dobbiamo considerare 2 casi:
I caso: $rs = sr$
studiamo $ord(rs)$
$(rs)^2 = r^2s^2 = r^2 \neq e \Rightarrow ord(rs) \neq 2$
$(rs)^3 = r^3s^3 = s^3 = s \neq e$
Per Lagrange
necessariamente $ord(rs) = 6$
$\Rightarrow G$ *è ciclico* $\Rightarrow$ *Assurdo*
II caso: $\begin{cases} rs = sr^2 \\ r^2s = sr \end{cases}$
Costruiamo l'isomorfismo

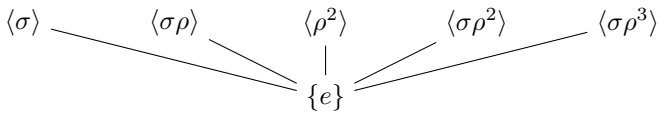
$$G \to D_3 :=< \rho, \sigma >$$
$$e \to Id$$
$$r \to \rho$$
$$r^2 \to \rho^2$$
$$s \to \sigma$$
$$sr \to \sigma\rho$$

□

Definizione 1
Dato un gruppo $(G, \cdot)$ il reticolo dei sottogruppi T_G è un grafo definito come

- *esiste un vertice in T_G per ogni sottogruppo $H \leq G$*
- *esiste un lato H_1 — H_2 se e solo se $H_1 \subseteq H_2$ e $\nexists K \leq G$ t.c. $H_1 \subset K \subset H_2$*

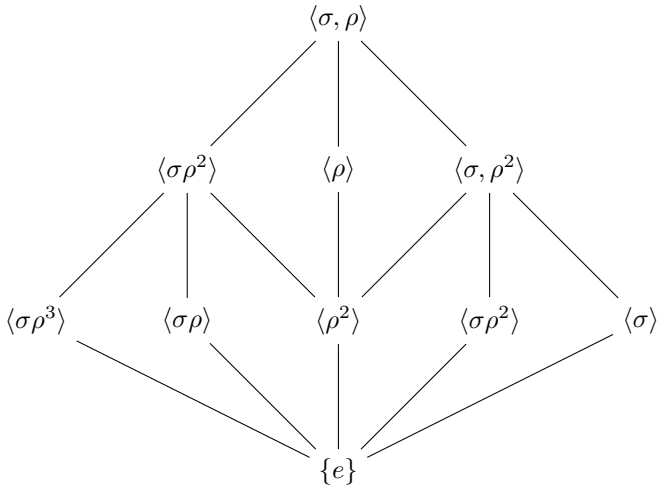
Esempio:
T_{D_4}
Ricordiamo che $D_4 =< \sigma, \rho >$ $\quad |D_4| = 8$
studiamo i sottogruppi di D_4
ordine 1: L'unico sottogruppo è $H = \{e\}$
ordine 2: Sono tutti e soli quelli generati da un elemento di ordine 2 in D_4



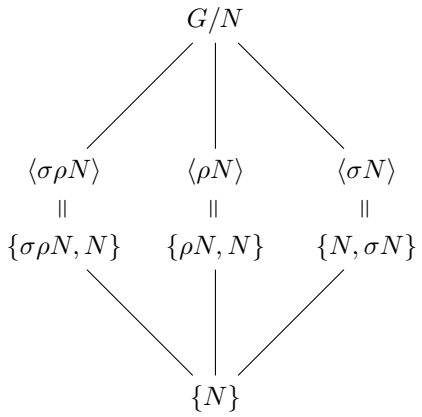
ordine 4: per la classificazione sono ciclici (C_4) oppure di Klein (K_4) altre al ciclico $< p >$ esistono altri sottogruppi

$$\langle \rho^2, \sigma \rangle = \{e, \sigma, \rho^2, \sigma\rho^2\}.$$
$$\rangle \rho^2, \sigma\rho \rangle = \{e, \sigma\rho, \rho^2, \sigma\rho^3\}.$$

Ordine 8: D_4



Esempio:
$G = D_4$
$N =< \rho^2 > \trianglelefteq G$
Vogliamo $T_{G/N}$
studiamo $G/N = D_4/ < rho^2 >$
$|G/N| = [G : N] = \dfrac{|G|}{|N|} = \dfrac{8}{2} = 4$
chi sono i laterali?
$IdN = N < \rho^2 >= \{Id, \rho^2\}$
$\rho N = \{\rho, \rho^3\}$
$\sigma N = \{\sigma, \sigma\rho^2\}$
$\sigma\rho N = \{\sigma\rho, \sigma\rho^3\}$
Ricordo:
Abbiamo una corrispondenza biunivoca tr ai sottogruppi di G/N e i sottogruppi di G contenenti N.



Obiettivo: studiare S_n
Ricordo:
$X := \{1, \ldots, n\}$
$S_n := S_X = \{$ applicazioni biunivoche $X \to X\}$
S_n gruppo di permutazioni
Osservazione:
$|S_n| = n!$
Osservazione:
se $n = 3 \to |S_3| = 6$
$\Rightarrow S_3 \cong D_3$
Osservazione
$S_n \cong D_n \quad \forall n \geq 4$
Infatti $n! > 2n \quad \forall n \geq 4$

2 Notazioni in S_n

$\sigma = (123)(47)$
$\tau = (23456)$
$\sigma\tau = \sigma \circ \tau = (123)(46)(23456)(12)(36)(45)$
$\tau \circ \sigma = (23456)(123)(46) = (13)(24)(56)$

Lemma 1
Data $\sigma \in S_n$ allora σ partizione $X = \{1, \dots, n\}$ in sottoinsiemi permutati ciclicamente e disgiunti tra loro

Dimostrazione
Definiamo la relazione d'equivalenza $i \sim j \Leftrightarrow \exists k \in \mathbb{Z}$ t.c. $\sigma^k(i) = j$
È una relazione d'equivalenza!
studiamo le classi di equivalenza
fissato $i \in X$
la sua clase

$$X_i = \{\sigma^k(i) | k \in \mathbb{Z}\} \subseteq X.$$

quindi $\exists \;\; k_1, k_2 \in \mathbb{Z}$ distinti t.c. $\sigma^{k_1}(i) = \sigma^{k_2}(i)$
$\Rightarrow i = \sigma^{k_2 - k_1}(i)$
$\Rightarrow m := min\{k \in \mathbb{Z}_{>0} | \sigma^k(i) = i\}$
$\Rightarrow X_i = \{i, \sigma(i), \sigma^2(i), \dots, \sigma^{n-1}(i)\}$ □

Proposizione 1
Data $\sigma \in S_n$, allora σ può essere rappresentata come composizione di cicli disgiunti

Obiettivo: Definire un omomorfismo

$$sgn : S_n \to (\{\pm 1\}, \cdot).$$

Questo ci permetterà di definire il sottogruppo alterno $A_n \trianglelefteq S_n$
$A_n := ker(sgn)$

Notazione 1
Dato un polinomio
$f \in \mathbb{Q}[x_1, \dots, x_n]$
e data $\sigma \in S_n$
Definiamo

$$f^\sigma(x_1, \dots, x_n) := f(x_{\sigma(1),\dots,x_{\sigma(n)}\}}.$$

Ci sta un polinomio speciale:

- $\Delta(x_1, \dots, x_n) = \prod_{1 \le i < j \le n}(x_i - x_j)$
- $\Delta^\sigma(x_1, \dots, x_n) = \prod_{1 \le i < j \le n}(x_{\sigma(i)} - x_{\sigma(j)})$

Definizione 2
$\sigma \in S_n$
$sgn(\sigma) := \frac{\Delta^\sigma}{\Delta} \in \{\pm 1\}$

Osservazione
$sgn : S_n \to \{\pm 1\}$
è un omomorfismo

Dimostrazione
In generale
$(f^\sigma)^\tau = f^{\sigma\tau}$
$(fg)^\sigma = f^\sigma g^\sigma$

$$sgn(\sigma\tau) = \frac{\Delta^{\delta\tau}}{\Delta} = \frac{(\Delta^\sigma)^\tau)}{\Delta} = \frac{\Delta^\sigma}{\Delta}\frac{(\Delta^\sigma)^\tau}{\Delta^\sigma} = sgn(\sigma)\frac{\Delta^\tau}{\Delta} = sgn(\delta)sgn(\tau) \qquad \square$$

Lezione 7 Algebra I

Federico De Sisti

2024-10-22

1 parte da recuperare

2 Seconda ora