

## DISCRETA: GRUPPI • GRUPPI 1

### OPERAZIONI BINARIE >

Per operazioni binarie si intende una funzione  $f$  applicata su un insieme  $A$  definita come

$$f: A \times A \rightarrow A \quad (a, a') \mapsto a * a' = *$$

PROPRIETÀ DELLE COMBINAZIONI > (vai a scrivere delle operazioni)

Alcune delle proprietà delle operazioni v

- p. associativa:  $\forall a, b, c \in A \quad (a * b) * c = a * (b * c)$

- p. commutativa:  $\forall a, b \in A \quad a * b = b * a$

- p. esistenza elemento neutro:  $\exists e \in A \quad \forall a \in A \quad a * e = a = e * a$

- p. esistenza degli inversi:  $\forall x \in A \quad \exists y \in A \quad x * y = y * x = e$

### ALCUNI ESEMPI

1. ADDIZIONE  $A = \mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$   $* = +$   $a + b$

2. MOLTIPLICAZ.  $A = \mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$   $* = *$   $a * b$

3. SOTTRAZIONE  $A = \mathbb{Z}, \mathbb{Q}, \mathbb{R}$   $* = -$   $a - b$  non  $\mathbb{N}$

4. DIVISIONE  $A = \mathbb{R} \setminus \{0\}$   $* = \frac{a}{b}$   $a/b$  non  $\mathbb{N}$

5. UNIONE FINITA  $x \neq \emptyset \quad A = \{x\}$   $* = \cup$   $a_1 \cup a_2$

6. COMPOSIZIONE  $x \neq \emptyset \quad A = \{f: x \rightarrow x\}$   $* = \circ$   $g \circ f \in A$

In base alle quantità di proprietà soddisfatte i gruppi possono essere classificati in:

- SEMIGRUPPO: Gruppi in cui vale P.1 - associativa
- MONOIDE: Gruppi in cui valgono P2, P3 associativa, elem. neutro
- GRUPPO: // in cui valgono P1, P2, P4 ass. elem. neutro, inversi

Inoltre, esso (semigruppo, monoide, gruppo) è commutativo/ se P2 commutativo abelliano

### ESEMPI ✓ ✓ ✓ ✗

-  $(\mathbb{N}, +)$ :  $P_1, P_2, P_3, P_4$  è un monoide commutativo

-  $(\mathbb{R}, \cdot)$ :  $P_1, P_2, P_3, P_4$   $\circ \cdot y = 0 \neq 1$

### ESEMPIO (FOND. INF.)

Per alfabeto si intende un insieme finito formato da lettere  $\Lambda = \{a, b, c, \dots\}$ , mentre per parola si intende una successione di lettere finita  $\in P$  e insieme parole.

Ese hanno un'operazione di concatenazione  $b * a = ba$

- P1:  $a, b \in P$   $(a * b) * c = a * (b * c) = abc$  ✓

- P2:  $a, b \in P$   $a * b \neq b * a$  ✗  $ab \neq ba$

- P3:  $a \in P$   $\exists e \in P$  ( $a * e = a = e * a$ ) ✗ ✓ solo se  $e = \epsilon$  stringa vuota

- P4:  $x \in P$   $\exists y \in P$  ( $x * y = \epsilon$ ) ✗ nessuno concat può dare  $\epsilon$  se  $x \in P$   
 $\epsilon \in P$

] La parola è un monoide non commutativo (se  $\epsilon \in P$ )

## DISCRETA: GRUPPI • GRUPPI 2

Per i gruppi valgono le seguenti proprietà:

- $G$  ammette un unico elemento neutro  $e$ :

Dati  $e, e' \in G$  allora  $e = e + e' = e'$  per cui  $e = e'$

- Ogni elemento  $g \in G$  ammette un unico inverso:

Dati  $h, h' \in G$  t.c. siano inversi di  $g$ , allora  $h = h * e = h * g * h' = e * h' = h'$  per cui  $e = e'$

- $\forall g, h \in G \quad (g * h)^{-1} = g^{-1} * h^{-1}$

Sappendo che  $(g * h)^{-1}$  è unico, per confermare la prop. basta provare che  $h^{-1} * g^{-1}$  è inverso di  $g * h$ :

$$\begin{aligned} & (g * h) * (h^{-1} * g^{-1}) = g * (h * h^{-1}) * g^{-1} = g * e * g^{-1} = g * g^{-1} = e \\ & h^{-1} * g^{-1} * g * h = h^{-1} * e * h = e * e = e \end{aligned}$$

- LEGGE DI CANCELLAZIONE: se  $g, g', h \in G$  t.c.  $gh = g'h \vee hg = hg' \vdash g = g'$

caso di  $gh = g'h$ :  $gh = g'h \Rightarrow g * \underbrace{h * h^{-1}}_e = g' * \underbrace{h * h^{-1}}_e \Rightarrow g = g'$

se si moltiplica per qualcosa da entrambe le parti il risultato non cambia

caso di  $hg = hg'$ :  $hg = hg' \Rightarrow h * g * h^{-1} = h * g' * h^{-1} \Rightarrow g = g'$

- LEGGE DELLE POTENZE:  $g^n * g^m = g^{n+m}$

Dato  $g \in G$  ed  $n \in \mathbb{N}$  si sa che  $g^n = \underbrace{g * g * \dots * g}_{n \text{ volte}}$  per cui  $(g^{-1})^n = \underbrace{g^{-1} * g^{-1} * \dots * g^{-1}}_{n \text{ volte}}$  si osserva

$$\begin{aligned} & \underbrace{g * g * \dots * g}_{n \text{ volte}} * \underbrace{(g^{-1} * g^{-1} * \dots * g^{-1}) * g * \dots * g}_{n \text{ volte}} = e \\ & (g^{-1})^n * g^n = e \end{aligned}$$

disponendo tutti gli elementi e moltiplicandoli tra di loro si ottiene la moltiplicazione degli inversi.

$$\text{Quindi } (g^{-1})^n = g^{-n}$$

SOTTOGRUPPI  $\triangleright (G, +) \wedge H \subseteq G \vdash (H, +)$

Dato un gruppo  $(G, +)$  ed  $H \subseteq G$ , esso è un sotto-gruppo se  $(H, +)$  con la stessa operazione è anch'esso un gruppo.

In ogni sotto-gruppo sono sempre presenti:

- $4\text{et}$
- $6\text{stesso}$

STEPS PER VERIFICA SEMP. SOTTO-GRUPPI  $\triangleright$

- 1)  $H + H \subseteq H$ , ossia che le operazioni sul presunto siano sempre parte del sotto-gruppo

- 2)  $e \in H$

- 3)  $h \in H \vdash h^{-1} \in H$  per ogni elemento deve esistere il suo inverso.

### ESEMPI

$\mathbb{R} \setminus \{0\} \xrightarrow{\mathbb{R}^+ \subseteq (\mathbb{R}, +)} (\mathbb{R}^+, +)$  non è sotto-gruppo perché  $+ \neq *$

$(\mathbb{Q}^+, \cdot) \xleftarrow{\text{è sotto-gruppo}} (\mathbb{R}^+, \cdot)$

## DISCRETA: GRUPPI • GRUPPI 2

OPERAZIONI corrispondenti × corrispondenti  $\Rightarrow g \in G \wedge h \in G' \models (g, g') \cdot (h, h') \stackrel{\text{def}}{=} (g \ast h, g' \circ h')$

Dati 2 gruppi distinti  $(G, \ast)$  e  $(G', \circ)$  considerando il prodotto cartesiano  $G \times G' = \{(g, g') \mid g \in G \wedge g' \in G'\}$  allora è possibile effettuare un'operazione sul prodotto cartesiano  $(g, g') \cdot (h, h')$  in cui  $g, h \in G \wedge g', h' \in G'$

- Si effettua l'operazione del primo gruppo tra i suoi elementi (in questo caso  $g \ast h$ )
- Si effettua l'operazione del secondo gruppo tra i suoi elementi (in questo caso  $g' \circ h'$ )

### SOTTOGRUPPI DA OPERAZIONI >

È anche possibile definire un sotto-gruppo e portare due un'operazione su prod. cartesiano

#### ESEMPIO

$H = \{(g, g') \in G \times G' \mid g' = e'\}$  è sotto-gruppo di  $G \times G'$  perché  $(g, e') \cdot (g_2, e') = (g \ast g_2, e' \circ e') = (g_1 \ast g_2, e') \in H$

## DISCRETA: GRUPPI • GRUPPI 3

DETERMINARE TUTTI I SOTTO-GRUPPI DATO UN GRUPPO >

È possibile determinare tutti i sotto-gruppi dato un gruppo seguendo i seguenti:

- Si identificano altri sotto-gruppi
- Ci si accerta che non ce ne siano altri.

ESEMPIO: Determinare tutti i sotto-gruppi di  $(\mathbb{Z}, +)$

1. Altri sotto-gruppi

es: con  $n=2$ ,  $H = \{-2, 0, 2, 4, \dots\}$

Dato un  $n \in \mathbb{Z}$  si definisce il sottoinsieme  $H = \{n \cdot z \mid z \in \mathbb{Z}\}$   
inoltre si nota che  $\mathbb{Z}$  stesso e  $\{0\}$  sono sottogruppi banali

Per provare che  $H \subset \mathbb{Z}$  si prova che:

- esistenza e. neutro: Si sa che per ogni  $n$   $0 \in H$  ✓
- esistenza inversa: Si sa che in  $H$   $\forall h \in H \exists k \in \mathbb{Z} (h = n \cdot k)$   
ma siccome  $h \in \mathbb{Z}$  il suo inverso in  $\mathbb{Z}$  è  $-h$   
che è descrivibile come  $-n \cdot k = n \cdot -k$  che  
per definizione di  $H$   $n \cdot -k \in H$  ✓

2. Non ce ne sono altri:

Dato  $H \subset \mathbb{Z}$  si vuole vedere che esiste  $n > 0$  t.c.  $H = \langle n \cdot \mathbb{Z} \rangle$

$H = \{0\}$  ok per def.

Siccome  $H \subset \mathbb{Z}$ ,  $0 \in H$  per cui  $\exists n \in \mathbb{N}$  t.c.  $h \neq 0 \models \exists h \in H$  t.c.  $h \neq 0$   
quindi se si intersecano  $H$  e  $\mathbb{Z}^{>0}$  non si ottiene l'insieme vuoto.  $H \cap \mathbb{Z}^{>0} \neq \emptyset$   
ma siccome esso è un insieme non-vuoto di numeri positivi  
Dove deve un minimo.

Dopo di che definisco  $x \in \mathbb{N}$ , se lo si divide per  $n$  se avrà  $x = q \cdot n + r$  o in formula inversa  $r = x - qn$  in cui si sa che

$\begin{cases} q \\ r \end{cases}$  ris. divi. resto

$qn \in H = \underbrace{n+n+\dots}_{\text{e' vuoto}}$   
 $x - qn \in H$

$0 \leq r < n$  e  $n = \min(H \cap \mathbb{Z}^{>0})$  per cui si nota che  $V$  per cui  $r \in H$   
ma se  $r \in H$  e  $0 \leq r < n$  allora  $r = 0$  per cui la  
formula cambia in  $x = q \cdot n$  ovvero  $n \cdot \mathbb{Z}$

## DISCRETA: GRUPPI • GRUPPI 3

### LATERALI DI UN GRUPPO >

Dato un gruppo  $G$  ed il suo sottogruppo  $H \subset G$ , esso può avere dei sottoinsiemi definiti dato un singolo elemento  $g \in G$

- Laterale destro di  $H$  su  $G$   $L_d = \{h \cdot g \mid h \in H\}$

In esso sono presenti gli elementi  $h \cdot g \in H$

- Laterale sinistro di  $H$  su  $G$   $L_s = \{g \cdot h \mid h \in H\}$

In esso sono presenti gli elementi  $g \cdot h \in H$

In generale per i gruppi:

$$L_d \neq L_s$$

anche se essi coincidono quando  $g = e$

### PROPRIETÀ DEI LATERALI DI UN GRUPPO >

Dato un gruppo  $G$  e il sottogruppo  $H \subset G$ , vengono le seguenti proprietà:

-  $\forall g \in G \ f: H \rightarrow gH$  è biettiva

Si dimostra la biettività tramite le dimostrazioni di iniettività e suriettività:

**INIEZIATIVITÀ:**  $f(h) = f(h') \Leftrightarrow gh = gh'$  ma se  $gh = gh'$  per la proprietà di cancellazione dei gruppi  $h = h'$  verificata

dimostrare

**SURIEZIATIVITÀ:**  $\forall g \cdot h \in gH \ (gh = f(h) \wedge f(h) \in \text{Im}(f))$  Ossia per ogni elemento di  $gH$ , il singolo elemento è il risultato dell'applicazione di  $h$  su  $f$  e esso appartiene all'immagine di  $f$  verificata

per cui  $f$  è biettiva

-  $g_1 H = g_2 H \Leftrightarrow (g_1^{-1} \cdot g_2) \in H$

cioè si dimostra in 2 passi:

•  $xH = H \Leftrightarrow x \in H$  Il lat. sinistro di un sottogruppo è uguale al sottogruppo stesso se e solo se l'elemento del gruppo appartiene al sottogruppo

1. Supponendo che  $xH = H$ , per definizione  $e \in H$ , allora  $x \cdot e \in xH$  e, per ipotesi,

$x \cdot e \in H$  e siccome  $x \cdot e = x$ , allora  $x \in H$ . ( $xH = H \models x \cdot e \in xH \wedge x \cdot e \in H \wedge x \in H$ )

2. Supponendo che  $x \in H$ , allora  $x \cdot H \subseteq H$  la loro operazione finisce dentro  $H$ .

Usando sempre questa proprietà, allora dato  $h \in H$ ,  $h = x \cdot (x^{-1} \cdot h) \in xH$  con la conseguente  $xH \subseteq H$  e la conclusione che  $xH = H$

• Semplificazione  $g_1 H = g_2 H \Rightarrow \overbrace{g_1^{-1} \cdot g_2}^e H = \overbrace{g_2^{-1} \cdot g_2}^x H \Rightarrow H = xH \Leftrightarrow x = g_1^{-1} \cdot g_2 \in H$

Usando i teoremi precedenti, si semplifica la definizione

- "I laterali sono partitioni"

Una partizione è una collezione di sottoinsiemi che se uniti danno il sottogruppo, non includono  $\emptyset$  e non hanno elementi in comune.

•  $\forall g \in G \ gH \neq \emptyset$

cioè è dimostrabile dal primo punto con la biettività di  $f: H \rightarrow gH$  oppure dal fatto che  $g \cdot e \in gH \models g \cdot e = g \wedge g \in gH \wedge gH \neq \emptyset$

•  $\forall g \in G \ (g \equiv g \cdot e \wedge g \cdot e \models g \in gH)$  Ossia ogni elemento del gruppo è rappresentato in una laterale, ricoprendo  $G$ .

## DISCRETA: GRUPPI • GRUPPI DI PT. 1

### ESEMPIO APPLICAZIONE PROPRIETÀ GRUPPI

Dato un gruppo  $G = \mathbb{Z}_{\geq 0}$ , il sottogruppo  $H \leq G$  è il l'intervallo  $gH = \{gh \mid h \in H\}$  si fissa un  $n \in \mathbb{Z}$  in cui  $n \neq 0 \wedge n \neq \pm 1 \wedge n \neq -1$ . Si definiscono  $a, b \in \mathbb{Z}$  e per le seconde proprietà  $H+a = H+b \Leftrightarrow b-a \in H$   
 Per cui  $8\mathbb{Z}+3 \neq 8\mathbb{Z}+4$  perché  $11$  non è multiplo di  $8$  ( $11-3 \not\in 8\mathbb{Z}$ )  
 analogamente  $5\mathbb{Z}+2 = 5\mathbb{Z}-8$  lo è  $-2-8 \in 5\mathbb{Z}$

INSIEMI DELLE CLASSI DI RESTO >  $\mathbb{Z}_n = \{0, \overline{1}, \overline{2}, \dots, \overline{n-1}\}$   $|Z_n| = n$

Definendo sempre  $G = \mathbb{Z}$ ,  $H = n\mathbb{Z} \cap H \leq G$   $n \neq 0, \pm 1$ , definendo un elemento  $k \in \mathbb{Z}$ ,  $H+k = n\mathbb{Z}+k$  si osserva che  $k = q \cdot n + r$  in cui  $0 \leq r < n$  ma estendo la formula di  $k$  invertibile in  $qn = r - n$  essa è multiplo di  $n$  per cui  $n\mathbb{Z}+k = n\mathbb{Z}+r$ .

Da esso è possibile concludere che i l'intervali nella forma  $n\mathbb{Z}+k$  sono insiemi delle classi di resto modulo n, ossia tutti gli elementi divisibili da n con resto  $k$ .

### ESEMPIO

$\mathbb{Z}_5 = \{0, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}$  ovvero  $5\mathbb{Z}, 5\mathbb{Z}+1, 5\mathbb{Z}+2, 5\mathbb{Z}+3, 5\mathbb{Z}+4$

ORDINE DI UN GRUPPO >  $G = \mathbb{Z}$  ordine  $G = |Z|$   $G = S_3$  ordine  $G = 3!$

Per ordine di un gruppo si intende la sua cardinalità  $|G|$

TEOREMA DI LAGRANGE >  $\forall H \leq G \quad |H| \leq |G| \wedge d \mid n \quad \text{o} \quad n = r \cdot d$

Il teorema di Lagrange dice che per ogni gruppo G di ordine n, ogni suo sottogruppo H ha un ordine minore e divisore di n

NB: Ciò NON significa che dato n esistono per forza dei sottogruppi di ordine n! cfr

### DIMOSTRAZIONE

Dati  $H \leq G$ , in cui  $|H| = d$ ,  $|G| = n$  per le proprietà dei sottogruppi esistono partizioni quindi  $G = g_1H \cup g_2H \cup \dots \cup g_rH$  e sempre per le stesse proprietà  $|G| = |g_1H| + |g_2H| + \dots + |g_rH|$  ma siccome sempre per le stesse proprietà esiste una bizione

tra  $H$  e  $g_iH$ , allora può essere riscritta come

$$|G| = \underbrace{|H| + |H| + \dots + |H|}_{r \text{ volte}} \Rightarrow |H| \cdot r = r \cdot d \Rightarrow n = r \cdot d \quad \text{ovvero} \quad d \text{ divide } n$$

$$r = \frac{n}{d} \quad \text{num. l'intervali}$$

NB2: Se l'ordine del gruppo è primo, allora gli unici sottogruppi possibili saranno  $\{e\}, G$

## DISCRETA • GRUPPI • GRUPPI DI PT. 2

COSTRUIRE SISTEMATICAMENTE ALCUNI SOTTO-GRUPPI >

Dato un gruppo qualsiasi  $G$ , considerando un suo elemento  $g \in G$ , è possibile costruire un' sottogruppo ciclico gen. $g$ :  $\langle g \rangle = g^{\mathbb{Z}} \stackrel{\text{def}}{=} \{ \dots, \bar{g}^2, \bar{g}, e, g, g^2, \dots \}$  in cui il quale sembra contenere infiniti elementi. Non è sempre così.

Dico: sono SOTTOGRUPPI

$\langle g \rangle$  è sottogruppo di  $G$  in quanto:

- $e \in \langle g \rangle$  presente elem. neutro
- $g^n + g^m \in \langle g \rangle$  per la proprietà delle potenze
- $\forall g^n \exists g^{-n} (\bar{e} = g^n + g^{-n})$  per ogni elemento del sottogruppo ciclico ne esiste l'inverso

ESEMPPIO: con  $|G| = |\mathbb{Z}|$

Dato  $G = (\mathbb{Z}, +)$  in cui  $g = n \neq 0$  allora  $\langle n \rangle = \{ \dots -2n, -n, 0, n, 2n, \dots \} = n\mathbb{Z}$  il quale contiene  $\infty$  elementi anche se con  $n=0$  allora  $\langle n \rangle = \{0\}$  inoltre  $\langle n \rangle = \langle -n \rangle$

CASO PARTICOLARE  $|G| < |\mathbb{N}|$   $|G| < |\mathbb{N}| \models |\langle g \rangle| < |\mathbb{N}| \wedge \exists n, m \in \mathbb{Z} (g^n = g^m)$

Se  $|G|$  non è  $\infty$ , allora  $\langle n \rangle$  non può contenere infiniti elementi ovvero  $\in G$  per cui dovranno esistere 2 esponenti che ritornano lo stesso risultato. Questo può accadere quando  $|\mathbb{N}| \leq |G|$  es:  $\langle -1 \rangle = \{1, -1\}$  per  $G = \mathbb{R}^\times = \mathbb{R} \setminus \{0\}$

In particolare, se esiste il caso  $\bar{g} = g^m$  allora  $g^n \cdot \bar{g}^m = g^n \cdot g^{-m} \equiv g^{n-m} \stackrel{\text{def}}{=} \bar{g}$  dimostrando che anche l'elemento neutro è ripetuto. L'esponente più piccolo per cui si verifica questa caratteristica viene detto periodo o ordine di  $g \in G = e, g, g^2, g^3, \dots, \bar{g}_1, \bar{g}_2$

Di conseguenza, le potenze successive nel sottogruppo ciclico saranno nella forma  $g^0, g^1, g^2, \dots, g^{p-1}, g^0$  risultando nella ripetizione degli elementi.

Ciò vale anche per le potenze negative di  $g$  in quanto per definizione se  $e \equiv g^p \equiv g + g \models g^{p-1} \equiv g^{-1}$  ovvero che  $g^{p-1}$  è un inverso come lo è  $g^{-1}$  e così via  $e \equiv g \circ g \models g^{p-2} \equiv g^{-2}$

INTEGRAZIONE CON LAGRANGE  $|G| = n \wedge |G| < |\mathbb{N}| \models \exists d \in \mathbb{Z} (n = rd)$

È anche possibile integrare Lagrange nel sottogruppo ciclico definendo che la cardinalità del sottogruppo ciclico divide dividere  $|G|$ . Possibili applicazioni:

- NELLE PERMUTAZIONI:  $\forall \alpha \in S_n$  ( $\text{ord}(\alpha)$  divide  $S_n = n!$ )

- POSS. DI E IN GENERALE:  $\forall g \in G (g^{|G|} = e)$

## DISCRETA: GRUPPI • GRUPPI 5

SOTTOGRUPPI CICLICI COMMUTATIVI  $\Rightarrow g^n * g^m = g^m * g^n = g^{(n+m)}$

Indipendentemente dalla commutatività del gruppo, tutti i sottogruppi ciclici sono commutativi. Questo per la legge delle potenze.

GRUPPI CICLICI  $\Rightarrow \langle g \rangle \equiv G \models G$  è gruppo ciclico

Nel caso invece in cui il sottogruppo ciclico sia uguale al gruppo, allora quest'ultimo viene detto gruppo ciclico infinito

ESEMPIO:  $G = (\mathbb{Z}, +)$  è ciclico  $\forall$  perché  $\langle 1 \rangle \equiv \langle 1 \rangle \equiv \{1, -1, 0, 1, 2, 3, 4, \dots\}$

ESEMPIO 2:  $G = (S_n, \circ)$  è ciclico finito  $\langle \pi \rangle \equiv \{\pi, \pi^2, \pi^3, \dots, \pi^{p-1}\}$  con  $p = \text{periodo di } \pi$   
per cui  $\forall l \in \mathbb{Z} \exists g \in \langle \pi \rangle$  ( $\langle g \rangle = l$ )

NB1: Siccome ogni gruppo ciclico è commutativo, allora un gruppo NON commutativo NON può essere ciclico. ES:  $S_n$  non è comm. se  $n \geq 3$

NB2: Esistono molti gruppi commutativi non ciclici.

È inoltre vero che i gruppi ciclici possono avere più generatori.

ESEMPIO: Dato  $G = \langle g \rangle = \{e, g, g^2, g^3, g^4, g^5, g^6, g^7, g^8, g^9, g^{10} = e\}$  allora  $\langle gy^3 \rangle = \{e, g^3, g^6, g^9, g^{12}, g^{15}, g^{18}, g^{21}, g^{24}\} = G = \langle g \rangle$

DIMOSTRARE CHE I GRUPPI FINITI SONO CICLICI >

Dato un gruppo ciclico con  $n$  elementi  $C_n \equiv \langle g \rangle$  in cui  $\text{periodo}(g) = n \equiv |C_n|$ .

Si definisce un nuovo gruppo formato dall'operazione su due gruppi ciclici  $G = C_m \times C_n$  in cui  $n, m \in \mathbb{Z}^+$ . In questo caso  $G$ :

- È CICLICO SE  
Esiste un elemento con periodo  $n \cdot m$  all'interno
- NON È CICLICO SE  
Ogni elemento ha periodo  $< n \cdot m$

In questo caso si procede con la dimostrazione definendo  $m = \text{m.c.m}(m, n) < m \cdot n$ .

Per due elementi  $(g, h) \in G$  la loro potenza è definita come:  $(g, h)^m \equiv (g^m, h^m)$  e siccome  $m$  è il m.c.m. sia di  $m$  che di  $n$  esso è un suo divisore per cui:  $= (e, e) \equiv e$  per qualsiasi  $g, g'$  di conseguenza anche il loro periodo  $\leq m \cdot n$  dimostrando quindi che  $G$  non è un gruppo ciclico

ESEMPIO >  $G = C_3 \times C_5$  in cui  $C_3 = \{1, g, g^2\}$   $C_5 = \{1, h, h^2, h^3, h^4\}$   
 $(g, h)^n \equiv (g^n, h^n) = (e, e) = e$

In questo caso non deve essere sia multiplo di 3 che di 5, m.c.m(3, 5) = 15.  $\forall g, h \in G$  ma essendo che  $|G| = 15$  allora tutti e 15 gli elementi vengono soddisfatti per cui si conclude che  $G$  è ciclico.

## DISCRETA: ARITMETICA MODULARE • ARITMETICA I

**UTILITY: DIVISIBILITÀ** >  $a, b \in \mathbb{Z}$ ,  $a | b \Leftrightarrow \exists k \in \mathbb{Z} (b = k \cdot a \vee k = \frac{b}{a})$

$a$  divide  $b \Leftrightarrow a$  è un divisore di  $b$

Il principio di divisibilità indica che se un numero divide un altro, allora esiste un numero  $k \in \mathbb{Z}$  usato come moltiplicatore del divisore.

**PROPRIETÀ:** dati  $a, b, c \in \mathbb{Z}$

- $c | a \wedge c | b \Leftrightarrow c | ab$  **DIM.**  $a = k \cdot c$  e  $b = h \cdot c$  perciò  $ab = k \cdot c \cdot h \cdot c \stackrel{c \neq 0}{=} c \cdot (k \cdot h)$  verificato
- $c | a \wedge c | ab \Leftrightarrow c | b$  **DIM.**  $a = k \cdot c$  e  $ab = j \cdot c$  perciò  $b = j \cdot c - k \cdot c \stackrel{c \neq 0}{=} (j-k) \cdot c$  verificato

stessa forma  
di  $c = l$

**UTILITY: CATEGORIE DI NUMERI INTERI**

- **INTERI IRREDUCIBILI**:  $n$  è irriducibile  $\Leftrightarrow a, b \in \mathbb{Z} \wedge n = a \cdot b \Leftrightarrow a = \pm 1 \vee b = \pm 1$

Un num.  $n \in \mathbb{Z}$  è irriducibile se e solo se, quando viene rappresentato nella forma  $n = a \cdot b$  in cui  $a, b \in \mathbb{Z}$ ,  $a = \pm 1 \vee b = \pm 1$ . Questo perché se è così, allora  $n$  non è più scomponibile in altri numeri e quindi al massimo è rappresentabile moltiplicando per  $\pm 1$ .

**ESEMPIO:**  $5 = 5 \cdot 1 \vee 5 = -5 \cdot -1$ ,  $7 = 7 \cdot 1 \vee 7 = -7 \cdot -1$

- **INTERI RIDUCIBILI**:  $n$  è riducibile  $\Leftrightarrow n$  non è irriducibile  $\wedge \nexists_{a, b \in \mathbb{Z}} (n = a \cdot b \wedge (a \neq \pm 1 \wedge b \neq \pm 1))$

Un num.  $n \in \mathbb{Z}$  è riducibile se non è irriducibile, ovvero se quando rapp. nella forma  $n = a \cdot b$  allora  $a \neq \pm 1 \wedge b \neq \pm 1$ . Questo perché se è riducibile allora i suoi componenti sono scomponibili.

**ESEMPIO:**  $12 = 3 \cdot 4 \vee 12 = 6 \cdot 2$ ,  $6 = 3 \cdot 2$

- **INTERI PRIMI**:  $n$  primo  $\Leftrightarrow \nexists_{a, b \in \mathbb{Z}} (n | ab \Leftrightarrow n | a \vee n | b)$

Un num.  $n \in \mathbb{Z}$  è primo se ogni volta che è divisore di  $a \cdot b$ , allora è divisore di  $a$  o  $b$ .

**ESEMPIO:** 8 non è primo  $= 8 | 16$  ma  $8 \nmid 5 \wedge 8 \nmid 2$

**UTILITY: MASSIMO COMUN DIVISORE** >  $\text{MCD}(a, b) \equiv \text{gcd}(a, b) \equiv \max \{ z \in \mathbb{Z} \mid z | a \wedge z | b \}$

Per massimo comun divisore si intende il numero massimo utilizzabile come divisore su due numeri. Esso è sempre  $\geq 0$ .

N.B.:  $\text{MCD}(0, b) = |b| \vee \text{MCD}(a, 0) = |a|$

**UTILITY: DIVISIONE EUCLIDEA O NU. CON RESTO** >  $\forall a, b \geq 0 \exists q, r \in \mathbb{Z} (a = q \cdot b + r \wedge 0 \leq r < |b|)$

Esso è un teorema utilizzato per descrivere la divisione. Dice che, per  $z$  interi dei quali il secondo  $\neq 0$ , allora il primo numero può essere rappresentato come il multiplo del secondo sommato ad un altro intero  $\geq 0 \vee < |b|$ .

**DIMOSTRAZIONE ESISTENZA**  $\exists q, r \in \mathbb{Z}$

Tesi:  $a \geq 0, b > 0$

CASE D'ASE  $a=0$ : verificato per  $q=0 \wedge r=0 \quad \forall b > 0$

Per ipotesi induttiva, si ipotizza che esistano  $q, r \quad \forall x > 0 \wedge x < a \wedge b > 0$ .

Se  $a < b$  allora  $q=0, r=a$

Se  $a \geq b$ :  $a-b = c \geq 0$  e per ip. induttiva  $\exists q', r' \in \mathbb{Z}, c = q' \cdot b + r'$  da cui

$$0 \leq r' < b \quad \text{e} \quad a = b+c = b+q' \cdot b+r' = (q'+1) \cdot b+r'$$

**DIMOSTRAZIONE UNICITÀ**

Si dimostra che  $q \cdot b + r \equiv q' \cdot b + r'$  ovvero l'unicità di  $q$  e  $r$ .

Se è vero ciò, allora  $0 \leq r, r' < b$  per il teorema. Si ipotizza che  $r \geq r'$ , ovvero che  $0 \leq r-r' < b$  di conseguenza il teorema iniziale si può riscrivere come

$(q'-q) \cdot b = r-r'$  da cui ne consegue che  $r-r'$  è divisore di  $b \Rightarrow b | r-r'$  ma se è vero e  $r, r' < b$ , questo vuol dire che  $r, r'=0$  e di conseguenza  $q, q'=0$

## DISCRETA: GRUPPI • GRUPPI 6 PT 2

FUNZIONI TRA GRUPPI >  $(G, \cdot)$ ,  $(H, \circ)$   $\vdash F: G \rightarrow H$

Per funzioni tra gruppi si intendono delle funzioni che accettano sia come dominio che co-dominio dei gruppi.

Essere dunque essere compatibili con la struttura del gruppo.

ESEMPIO:  $G = (\mathbb{Z}, +)$ ,  $H = (\mathbb{R}^*, \mathbb{R} \setminus \{0\}, \circ)$

si definisce come  $F: \mathbb{Z} \rightarrow \mathbb{R}^*$   $z \mapsto z^n$

$$- F(n, m) = z^{m+n} \quad \forall n, m \in \mathbb{Z}$$

$$- F(m) = z^m, \quad F(n) = z^n \text{ da cui } F(m) \circ F(n) = F(m+n)$$

La funzione definita con  $z^n$  "Trasforma le somme in prodotti".  $\equiv F(n+m) = F(n) \circ F(m)$

OMOAFISMO >  $F: (G, *) \rightarrow (H, \circ)$ ,  $F$  è un omoafismo  $\Leftrightarrow \forall g, g' \in G \quad F(g * g') \equiv F(g) \circ F(g')$

Dato una funzione tra gruppi  $F$ , essa è un omoafisismo se per ogni elementi diversi di  $G$ , la loro operazione all'interno della funzione è uguale all'operazione sul risultato delle funzioni.

ESEMPIO:  $F: (\mathbb{Z}, +) \rightarrow (\mathbb{Z}, +)$   $k \mapsto k \cdot z$  per un  $k \in \mathbb{Z} \wedge k \neq 0$

$$F(n+m) \equiv F(n) + F(m)$$

$$k \cdot (m+n) \equiv k \cdot m + k \cdot n$$

$$km + kn = m \cdot n + k \cdot m \quad \text{Verificato}$$

ESEMPIO 2:  $F: (\mathbb{Z} \times \mathbb{Z}, +) \rightarrow (\mathbb{Z}, +)$   $(x, y) \mapsto x - y$

$$F((x, y) + (p, q)) \equiv F(x, y) + F(p, q)$$

$$F((x+p), (y+q)) \equiv (x-y) + (p-q)$$

$$(x+p) - (y+q) \equiv x - y + p - q$$

$$x + p - y - q \quad \text{Verificato}$$

## DISCRETA: GRUPPI • GRUPPI 6 PT.2

### PROPRIETÀ DEGLI OMOMORFISMI >

Dato l'omomorfismo  $F: G \rightarrow H$ :

- $F(e_G) = e_H$  ovvero che l'applicazione delle funzioni di omomorfismi con l'elemento neutro del dominio deve essere uguale all'elemento neutro del co-dominio.

DIMOSTRAZIONE: Sapendo che  $e_G * e_G = e_G$ , allora per definizione

$$F(e_G * e_G) \equiv F(e_G) * F(e_G)$$

$$F(e_G) \equiv F(e_G) * F(e_G) \text{ per la proprietà di cancellazione.}$$

$$e_H \equiv F(e_G)$$

ESEMPIO:  $F: \mathbb{Z} \rightarrow \mathbb{Z}$   $F(n) = 3n - 1$   $F(0) = -1$  è diverso dall'elemento neutro del co-dominio. Errore.

In generale, una funzione NON è un omorfismo se l'immagine di  $F(e_G) \neq e_H$

- $\forall g \in G (F(g)^{-1} \equiv F(g^{-1}))$  Ovvero che per ogni elemento del gruppo è che l'immagine dell'inverso è equivalente all'inverso dell'immagine.

DIMOSTRAZIONE Si sa che  $g * g^{-1} = e_G$  per cui  $F(g * g^{-1}) \equiv F(e_G)$

$$\frac{1}{\cancel{F(g)}} F(g) * F(g^{-1}) \equiv e_H \circ \frac{1}{\cancel{F(g)}} \\ F(g^{-1}) \equiv F(g)^{-1}$$

- $\forall g \in G \forall n \in \mathbb{N} (F(g)^n \equiv F(g^n))$  Ovvero l'immagine di  $F$  elevata a  $n$  è log. equivalente a  $g^n$  applicato su  $F$ .

DIMOSTRAZIONE

- Se  $n > 0$ :  $g^n \equiv \overbrace{g * g * \dots}^{n \text{ volte}}$  allora  $F(g^n) \equiv F(g * g * \dots) \equiv \overbrace{F(g) * F(g) * \dots}^{n \text{ volte}}$
- Se  $n = 0$ :  $g^0 = e_G$  e quindi  $F(e_G) = e_H$
- Se  $n < 0$ :  $g^n = (g^{-1})^{-n} \equiv (g^{-1})^{-1} \text{ allora } F(g^{-1})^{\cancel{n}} \equiv F(g^{-1} * g^{-1} * \dots) \equiv \overbrace{F(g^{-1}) * F(g^{-1}) * \dots}^{n \text{ volte}}$

CASO PARTICOLARE:  $G = \langle g \rangle$   $F(g^n) \equiv F(e_H) \equiv F(g)^n \equiv e_H$

In caso si definisce l'omomorfismo con una funzione  $F$  usando un gruppo ciclico, allora per poterla definire velocemente quel è un singolo elemento di  $G$  in quanto fa da generatore.

Inoltre, se  $G$  è finito, allora se elevato al suo periodo all'interno dell'omomorfismo esso dovrà essere contemporaneamente

- essere  $e_H$  per la P2
- essere uguale  $F(g)^n$

per cui  $F(g)^n = e_H$

omomorfismo:

- $F: G \rightarrow H$ ,  $G' \subset G \models F(G') \subset H$

Ossia, dato un omomorfismo, se un altro gruppo è sotto gruppo del gruppo originale  $G$ , allora l'applicazione della funzione passando il sotto gruppo ritornerei un sottogruppo del co-dominio.

DIMOSTRAZIONE

$$e_G \in G' \models F(e_G) = e_H \in F(G')$$

$$g, g' \in G' \rightarrow g * g' \in G' \models$$

$$F(g * g') \equiv F(g) * F(g') \in F(G')$$

$e_G \in G'$  in quanto per essere un gruppo deve avere almeno l'elemento neutro. allora  $F(e_G) = e_H \in F(G')$  per proprietà 2

Inoltre, se  $g, g' \in G'$ , allora anche  $g * g' \in G'$  di conseguenza

$$F(g * g') \equiv F(g) * F(g') \in F(G')$$

$$G': R^x = (R^x \setminus \{0\}, *)$$

ESEMPIO: Dato  $F: R^x \rightarrow R^x$   $r \mapsto r^2$  è un omorfismo dati  $x, y \in R^x$

$$F(x * y) \equiv F(x) * F(y)$$

$$(xy)^2 \equiv x^2 * y^2 \Rightarrow x^2 * y^2 = x^2 * y^2$$

Prendendo come esempio  $R^x = G'$ , allora l'immagine della funzione sarà  $R^x$  ovvero un sottogruppo