

GRUPPI

S

• G

VERIFICARE VALIDITÀ OPERAZIONI NEI GRUPPI \rightarrow IN8 • $g, g' \in G, g * g'$

Sta tutto nel verificare che $g * g' \in G$

1. Definire il comportamento di $g \in G$
2. Estendere il ragionamento a $g * g' \in G$

NR: SE l'operazione contiene sistemi
verificare ogni costitutiva.

ES: Dato $G = [0, 1] = \{k \in \mathbb{R} \mid 0 \leq k \wedge k < 1\}$ e l'operazione

$* : \mathbb{R} \times \mathbb{R} \rightarrow \mathbb{R}$ definita come:

$$\forall t_1, t_2 \in \mathbb{R} \quad t_1 * t_2 = \begin{cases} t_2 + t_1 & \text{se } t_1 + t_2 < 1 \\ t_1 + t_2 - 1 & \text{se } t_1 + t_2 \geq 1 \end{cases}$$

Verificare che $*$ sia in G

1. Definisco $g \in G$

$$t \in G \Leftrightarrow t \geq 0 \wedge t < 1 \rightarrow t_1 * t_2 \in G \text{ se}$$

Verifico per i casi del sistema

$$(\text{CASO 1}): t_1 + t_2 < 1$$

$$t_1 + t_2 \in G \text{ se}$$

$$t_1 + t_2 \geq 0 \wedge t_1 + t_2 < 1$$

Vero per
definizione

Vero in
questo caso
del sistema

2. Estendo il ragionamento

$$(\text{CASO 2}): t_1 + t_2 - 1 \in G$$

$$\text{sse } t_1 + t_2 - 1 \geq 0 \quad \checkmark$$

$$\text{sse } t_1 + t_2 \geq 1 \quad (\text{altro modo})$$

$$\text{sse } t_1 + t_2 < 2$$

$$\text{sse } t_1 + t_2 - 1 < 1$$

$$\text{sse } t_1 + t_2 - 1 < 1 \quad \checkmark$$

CALCOLARE PERIODO DI $x \in G$ W OPERAZIONE \rightarrow

2. Partendo dall'operazione
nel gruppo, seguire formula:

$$x \in G \models \text{Periodo}(x, (G, *)) = \min\{n \in \mathbb{N} \mid x + x * \dots * x = e_G \text{ } n \text{ volte}\}$$

Ovvero il numero minimo di
operazioni per ottenere l'elemento
neutro e_G .

• G

ES: Dato G del IN8 • $g, g' \in G$,
caso su, calcolare
il periodo di $\frac{2}{7} \in G$

Applico l'operazione fin quando non
ottengo l'elemento neutro:

$$\begin{array}{ccccccccc} 1 & 2 & 3 & 4 \\ \frac{2}{7} * \frac{2}{7} = \frac{4}{7} & | \frac{4}{7} * \frac{2}{7} = \frac{6}{7} & | \frac{6}{7} * \frac{2}{7} = \frac{1}{7} & | \\ \frac{1}{7} * \frac{2}{7} = \frac{3}{7} & | \frac{3}{7} * \frac{2}{7} = \frac{5}{7} & | \frac{5}{7} * \frac{2}{7} = \frac{7}{7} = e_G & | \\ 5 & 6 & 7 & \end{array}$$

Il periodo è $\textcircled{7}$

CASO D'OSO >

"Dato $U = \mathbb{Z}_{10}^*$, gruppo di classi di resto invertibili in \mathbb{Z}_{10} ,

Provare che $a = [3]_{10}^{303}$ appartiene a U e che $\langle a \rangle$ coincide con U "

1. Provare che $[3]_{10}^{303}$ appartiene a U

Ovvero provare che $[3]_{10}^{303}$ è invertibile.

Siccome n^x è invertibile $\Leftrightarrow n$ è invertibile si può semplificare trovando l'inverso di 3

in \mathbb{Z}_{10} :

$$\text{MCD}(3, 10) : 10 = 3 \cdot 3 + 1 \\ 3 = 3 \cdot 1 + 0$$

$\text{MCD}(3, 10) = 1 \Leftrightarrow 3$ è invertibile in \mathbb{Z}_{10}

quindi
ovvero

3^{303} è invertibile in \mathbb{Z}_{10}
 $[3]_{10}^{303}$ appartiene a U

2. " $\langle a \rangle$ coincide con U "

Sapendo che $\text{MCD}(3, 10) = 1$ e $10 = 3 \cdot 3 + 1$

bisogna semplificare $[3]_{10}^{303}$:

$$\varphi(10) = \varphi(5 \cdot 2) = 4 \\ \text{rappresentare } 3^{303} \text{ come}$$

$$3^{303} = 3^{75 \cdot 4+3} = 3^{75 \cdot 4+3} = 3^{75 \cdot 3} = 3^7 \pmod{10} \\ 3 = 1 \quad 27 \pmod{10} \quad 27 - 10 = 7$$

$$\begin{aligned} \text{Per definire } \langle a \rangle &= \langle 1, 3, 9, 27, 81, 243, 729, 2187, 6561, 19683, 59049, 177147, 531441, 1594323, 4782969, 14348907, 43046721, 129140163, 387420489, 1162261467, 3486784401, 10459353203, 31378059609, 94134179027, 282392537081, 847177611243, 2541532833729, 7624608501187, 22873825503561, 70621476510683, 211864429532049, 635593288596147, 1906779865788441, 5719339597365323, 1715801879209597, 5147405637628791, 15442216912886373, 46326650738659119, 138979952215977357, 416939856647932071, 1250819570043796213, 3752458710131388639, 11257376130394165817, 33772128390182507451, 101316385170547522333, 303949155511642567001, 911847466534927699993, 2735542399604783099979, 8206627198814359299937, 24619881596433077999011, 73859645789299233999033, 221578937367897703999099, 664736812103693103999297, 2004210436311079303999891, 6012631208933237903999673, 18037893626799713703999229, 54113670880399101303999087, 16234101264119730399902661, 48702303792359190399901393, 146106911377177590399900471, 4383207341315327903999001433, 131496220299559839039990001299, 4004886608986795190399900003879, 120146598269573855903999000011637, 3604457948087215679039990000035111, 10813373844261646990399900000105333, 32437121532784939990399900000031601, 973113645983547199903999000000105333, 2919340917950641599903999000000031601, 87578227538519241999039990000000105333, 262734682615577721999039990000000031601, 7882639478467331619990399900000000105333, 23647918435391994819990399900000000031601, 709537553061759844199903999000000000105333, 2128612659182279532199903999000000000031601, 63858376775468385961999039990000000000105333, 191575129326405657882199903999000000000031601, 5747253880792169736461999039990000000000105333, 17241761642375509113382199903999000000000031601, 517252849271265273401641999039990000000000105333, 1551758547813795820204921999039990000000000031601, 46552756434313874606147641999039990000000000105333, 139658269132911623828442921999039990000000000031601, 4189747973987354714853287641999039990000000000105333, 125692439219620641455698631241999039990000000000031601, 3770773176588619243670958937241999039990000000000105333, 11312319529765857330998976877241999039990000000000031601, 33936958589307572092996932632419990399900000000000105333, 101810875767922716278992798892419990399900000000000031601, 305432627303748158836973396672419990399900000000000105333, 916307882111244576459910190012419990399900000000000031601, 2749033643333733739369733966724199903999000000000000105333, 82471019300012445764599101900124199903999000000000000031601, 24741305790003733739369733966724199903999000000000000105333, 742239173700012445764599101900124199903999000000000000031601, 22267175210003733739369733966724199903999000000000000105333, 667515856300012445764599101900124199903999000000000000031601, 20025475690003733739369733966724199903999000000000000105333, 600764270700012445764599101900124199903999000000000000031601, 18022928120003733739369733966724199903999000000000000105333, 540687843600012445764599101900124199903999000000000000031601, 16218635210003733739369733966724199903999000000000000105333, 486559056300012445764599101900124199903999000000000000031601, 14596775580003733739369733966724199903999000000000000105333, 437893267400012445764599101900124199903999000000000000031601, 13136897920003733739369733966724199903999000000000000105333, 400106937600012445764599101900124199903999000000000000031601, 12003208120003733739369733966724199903999000000000000105333, 360106937600012445764599101900124199903999000000000000031601, 10801069376000373373936973396672419990399900000000000105333, 324032081200012445764599101900124199903999000000000000031601, 9720962436000373373936973396672419990399900000000000105333, 291628872800012445764599101900124199903999000000000000031601, 8748866184000373373936973396672419990399900000000000105333, 262465985520001244576459910190012419990399900000000000031601, 7873979565600037337393697339667241999039990000000000105333, 236219386688001244576459910190012419990399900000000000031601, 7086581595680037337393697339667241999039990000000000105333, 212597457870400124457645991019001241999039990000000000031601, 6377923736128003733739369733966724199903999000000000105333, 191337612038400124457645991019001241999039990000000000031601, 5743128361152003733739369733966724199903999000000000105333, 172393847834560124457645991019001241999039990000000000031601, 5171815435036800373373936973396672419990399900000000105333, 155154463651104001244576459910190012419990399900000000031601, 4654633909533120037337393697339667241999039990000000105333, 13964801728599600124457645991019001241999039990000000031601, 4189440518579880037337393697339667241999039990000000105333, 125633215557962400124457645991019001241999039990000000031601, 3770106366738848003733739369733966724199903999000000105333, 11310319519236480012445764599101900124199903999000000031601, 3493695858930757209299693263241999039990000000000000031601, 1048108757679227162789910190012419990399900000000000105333, 3144326273037481588369733966724199903999000000000000031601, 94320519300012445764599101900124199903999000000000000031601, 2829617569000373373936973396672419990399900000000000105333, 84887548580001244576459910190012419990399900000000000031601, 2544646478000373373936973396672419990399900000000000105333, 76368555360001244576459910190012419990399900000000000031601, 2291056668000373373936973396672419990399900000000000105333, 71775695040001244576459910190012419990399900000000000031601, 2153260824000373373936973396672419990399900000000000105333, 64698924720001244576459910190012419990399900000000000031601, 1935967741600037337393697339667241999039990000000000105333, 5903906324800012445764599101900124199903999000000000031601, 1771371897440003733739369733966724199903999000000000105333, 5214115692320012445764599101900124199903999000000000031601, 1564234677696003733739369733966724199903999000000000105333, 4692703932088001244576459910190012419990399900000000031601, 1407811176264003733739369733966724199903999000000000105333, 4223433428792001244576459910190012419990399900000000031601, 1261739942637600373373936973396672419990399900000000105333, 3785219827912800124457645991019001241999039990000000031601, 11312319529765857330998976877241999039990000000000000031601, 34936958589307572092996932632419990399900000000000000031601, 104810875767922716278991019001241999039990000000000000031601, 31443262730374815883697339667241999039990000000000000031601, 94320519300012445764599101900124199903999000000000000031601, 28296175690003733739369733966724199903999000000000000105333, 84887548580001244576459910190012419990399900000000000031601, 2544646478000373373936973396672419990399900000000000105333, 76368555360001244576459910190012419990399900000000000031601, 2291056668000373373936973396672419990399900000000000105333, 64698924720001244576459910190012419990399900000000000031601, 1935967741600037337393697339667241999039990000000000105333, 5214115692320012445764599101900124199903999000000000031601, 1564234677696003733739369733966724199903999000000000105333, 4692703932088001244576459910190012419990399900000000031601, 14078111762637600373373936973396672419990399900000000105333, 42234334287912800124457645991019001241999039990000000031601, 1261739942637600373373936973396672419990399900000000031601, 37852198279128001244576459910190012419990399900000000031601, 11312319529765857330998976877241999039990000000000000031601, 34936958589307572092996932632419990399900000000000000031601, 104810875767922716278991019001241999039990000000000000031601, 28296175690003733739369733966724199903999000000000000031601, 84887548580001244576459910190012419990399900000000000031601, 2544646478000373373936973396672419990399900000000000105333, 76368555360001244576459910190012419990399900000000000031601, 2291056668000373373936973396672419990399900000000000105333, 64698924720001244576459910190012419990399900000000000031601, 1935967741600037337393697339667241999039990000000000105333, 5214115692320012445764599101900124199903999000000000031601, 1564234677696003733739369733966724199903999000000000105333, 4692703932088001244576459910190012419990399900000000031601, 14078111762637600373373936973396672419990399900000000105333, 42234334287912800124457645991019001241999039990000000031601, 1261739942637600373373936973396672419990399900000000031601, 37852198279128001244576459910190012419990399900000000031601, 11312319529765857330998976877241999039990000000000000031601, 34936958589307572092996932632419990399900000000000000031601, 104810875767922716278991019001241999039990000000000000031601, 28296175690003733739369733966724199903999000000000000031601, 84887548580001244576459910190012419990399900000000000031601, 2544646478000373373936973396672419990399900000000000105333, 76368555360001244576459910190012419990399900000000000031601, 2291056668000373373936973396672419990399900000000000105333, 64698924720001244576459910190012419990399900000000000031601, 1935967741600037337393697339667241999039990000000000105333, 5214115692320012445764599101900124199903999000000000031601, 1564234677696003733739369733966724199903999000000000105333, 4692703932088001244576459910190012419990399900000000031601, 14078111762637600373373936973396672419990399900000000105333, 42234334287912800124457645991019001241999039990000000031601, 1261739942637600373373936973396672419990399900000000031601, 37852198279128001244576459910190012419990399900000000031601, 11312319529765857330998976877241999039990000000000000031601, 34936958589307572092996932632419990399900000000000000031601, 104810875767922716278991019001241999039990000000000000031601, 28296175690003733739369733966724199903999000000000000031601, 84887548580001244576459910190012419990399900000000000031601, 2544646478000373373936973396672419990399900000000000105333, 76368555360001244576459910190012419990399900000000000031601, 2291056668000373373936973396672419990399900000000000105333, 64698924720001244576459910190012419990399900000000000031601, 1935967741600037337393697339667241999039990000000000105333, 5214115692320012445764599101900124199903999000000000031601, 1564234677696003733739369733966724199903999000000000105333, 4692703932088001244576459910190012419990399900000000031601, 14078111762637600373373936973396672419990399900000000105333, 42234334287912800124457645991019001241999039990000000031601, 1261739942637600373373936973396672419990399900000000031601, 37852198279128001244576459910190012419990399900000000031601, 11312319529765857330998976877241999039990000000000000031601, 34936958589307572092996932632419990399900000000000000031601, 104810875767922716278991019001241999039990000000000000031601, 28296175690003733739369733966724199903999000000000000031601, 84887548580001244576459910190012419990399900000000000031601, 2544646478000373373936973396672419990399900000000000105333, 76368555360001244576459910190012419990399900000000000031601, 2291056668000373373936973396672419990399900000000000105333, 64698924720001244576459910190012419990399900000000000031601, 1935967741600037337393697339667241999039990000000000105333, 5214115692320012445764599101900124199903999000000000031601, 1564234677696003733739369733966724199903999000000000105333, 4692703932088001244576$$

ELENCARE ELEMENTI INVERTIBILI

- Usare la funzione di Euler per ottenere la quantità di invertibili
- Vedere Gruppi 1: funz. Euler

- La funzione restituirà un num. pari, di questi elementi

- Elencare la prima metà come i numeri da 1 a $n-1$ NON divisibili dai coefficienti della scomposizione in fattori primi di n . [Vedere alternativa]
- Le seconde metà saranno gli elementi della prima negati (per sommare n quanto basta per averli > 0)

GENERATORI (Z_n^*)

- Calcolare gli elementi invertibili!

- PER OGNI elemento invertibile g
- Determinate il minimo $k \in \mathbb{N}$ per il quale $g^k \equiv 1 \pmod{n}$

- I generatori saranno tutti gli elementi che hanno $k = \varphi(n)$

[GRP1 - ESEMPIO]

NB Basta trovare il k per la prima metà

ALTERNATIVA A

[GRUPPI 4 - ELENCARE ELEMENTI INVERTIBILI]

 Z_n^*

ES: "Dato $Z \times Z_{12}$, calcolare gli invertibili rispetto al prodotto componente per componente"

$$Z^* = \{\pm 1\}$$

$$\varphi(12) = \varphi(3) \cdot \varphi(2^2) = 2 \cdot 2 = 4$$

$$12 = 3 \cdot 2^2$$

Trovò la prima metà: 1, 5

$$\underline{1 \neq 5 \neq 6 \neq 8 \neq 10 \neq}$$

Le seconde metà saranno negate: $-1, -5$

$$= -1 + 12 = 11$$

$$= -5 + 12 = 7$$

$$\text{Totale} = 1, 5, 7, 11, 12$$

RICUADERE OVO TRA

[GRP-4: ELENCARE ELEMENTI INVERTIBILI]

[GRP-7: ELENCARE ELEMENTI INVERTIBILI]

ES: "Dato Z_{20} determinare i generatori"

(1) Elenco gli invertibili

$$20 = 2^2 \cdot 5 \quad \varphi(20) = \varphi(2^2) \cdot \varphi(5) = 2 \cdot 4 = 8$$

$$1 \neq 3, 4, 8, 16 \neq 7, 9$$

$$= \{\pm 1, \pm 3, \pm 7, \pm 9\}$$

$$= \{\pm 1, \pm 3, \pm 7, \pm 9, \pm 16, \pm 13, \pm 11\}$$

(2) Trovo il minimo k per cui $g^k \equiv 1$

$$(\pm 1)^2 \equiv 1 \pmod{20} \quad \text{nessuno}$$

$$(\pm 3)^4 \equiv 1 \pmod{20} \quad \text{ha } k=8$$

$$(\pm 7)^4 \equiv 1 \pmod{20} \quad \text{non ci sono GENERATORI}$$

$$(\pm 9)^2 \equiv 1 \pmod{20}$$

CICLICITÀ (\mathbb{Z}_n^\times) \Rightarrow È ciclico se ha almeno 1 generatore
 [GRP-7: Generatori \mathbb{Z}_n^\times]

CASO D'USO (\mathbb{Z}_n^\times)

Considerando le classi di resto \mathbb{Z}_n :

- Quanti modi ci hanno di scegliere 3 classi invertibili
- Dire se il gruppo moltiplicativo \mathbb{Z}_{20}^\times è ciclico o no
- Determinare tutti gli n tali che $\bar{3}^n = \bar{q}$

(1) Classi invertibili (con [GRP-7: elementi invertibili])

$$\varphi(20) = \varphi(2^2) \cdot \varphi(5) = 2 \cdot 4 = 8$$

Dovendo scegliere 3 elementi su 8 in cui: X ripetizioni

$$= \binom{8}{3} = \frac{8!}{3! \cdot 5!} = 56 \text{ modi} \quad \times \text{ordine}$$

(2) Determino se è ciclico [GRP-8: Ciclicità \mathbb{Z}_n^\times]

Ovvero se ha 1 generatore [GRP-7: Generatori \mathbb{Z}_n^\times]

2.1) SCOMPOSIZIONE: $12 = 2^2 \cdot 3$

1° metà $\pm 1, \pm 3, \pm 9$

su 8 = $\pm 1, \pm 3, \pm 7, \pm 9$

2.2) Determino min k t.c. $g^k \equiv 1 \pmod{n}$

$$(\pm 1)^1 \equiv 1 \pmod{20}, (\pm 3)^4 \equiv 1 \pmod{20}, (\pm 7)^4 \equiv 1 \pmod{20}$$

$$(\pm 9)^2 \equiv 1 \pmod{20}$$

Non ha generatori \leftrightarrow Non è ciclico

3) Sapendo che il periodo di $\bar{3}^n$ è 4 e $\bar{3}^2 = q$
 allora

$$\{ n \in \mathbb{Z} \mid n \equiv z \pmod{4} \} = \{-6, -2, 2, 6, 10, \dots\}$$

PER $Z_n \rightarrow S_m$

1. Partire definendo due elementi uguali $a, b \in Z_n$.
2. Proseguire definendo che se sono uguali, anche le applicazioni delle funzioni dovranno esserlo.
NB: Sfruttare la proprietà $\sigma^a = \sigma^b \Leftrightarrow a = b$
3. Sfruttare la proprietà precedente, definendo che se n di Z_n divide $a - b$: $n \mid a - b$ giungendo che $\Leftrightarrow \exists t \text{ t.c. } a = b + tn$
4. Applicare la funzione con a e sostituirlo con quanto detto
NB: Calcolare il periodo di σ [vedere sezione I] per semplificare
5. SE si ottiene $f(b)$, allora è ben definita.

ES: "Data la funzione $f: Z_{10} \rightarrow S_3$, $\bar{a} \mapsto \sigma^{\frac{3a}{10}}$. Stabilire se è ben definita."

Definisco 2 elementi uguali + Definisco che se sono uguali anche le applicazioni delle funzioni devono esserlo: (1,2)

Dati $\bar{a}, \bar{b} \in Z_{10}$, se $\bar{a} = \bar{b} \rightarrow f(\bar{a}) = f(\bar{b})$

(2) Sfrutto prop. \Leftrightarrow se $\sigma^a = \sigma^b$

$$\begin{cases} \Leftrightarrow \\ \Leftrightarrow \\ \Leftrightarrow \end{cases} \begin{array}{l} \sigma^a = \sigma^b \\ a = b \\ a - b = 0 \end{array}$$

(3) n di $Z_n \mid a - b \rightarrow$ se $\exists t \mid a - b$ in Z_{10}

(3) definisco ' t ' $\Leftrightarrow \exists t \text{ t.c. } a = b + 10t$

(4) applico $f(a)$

$$\text{con } f(\bar{a}) = \sigma^{\frac{3a}{10}} \Rightarrow \sigma^{\frac{3(b+10t)}{10}} \Rightarrow \sigma^{3b+30t} = \sigma^{3b} = f(\bar{b}) \text{ d'(5)}$$

(4) calcolo Periodo(σ) Periodo(σ) = [vedere sezione I] = 30

quindi Periodo(σ) | 30t $\Rightarrow \sigma^{30t} = id$

Per $S_n \rightarrow \mathbb{Z}_n$

1. Definire due permutazioni con esponente $a, b \in \mathbb{Z}$
 $\sigma^a = \sigma^b$

2. Esse dovranno essere uguali alle applicazioni delle funzioni.
 NB: Sfruttare che $\sigma^a = \sigma^b \Leftrightarrow \sigma^{a-b} = id$

3. Calcolare il Periodo. Partendo dalla formula precedente:
 $\text{Periodo}(\sigma) | a-b$ [vedere sezione Periodo Perm]

4. Adattare l'espressione applicando la funzione.

5. SE Quando applicata la funzione ho l'ugualanza
 tra a, b allora è ben definita.

ES: "Data la funzione $f: S_m \rightarrow \mathbb{Z}_n$ $\sigma^k \mapsto \bar{3k}$ verificare che sia ben definita".

(1): Definisco le Permutazioni

(2): Definisco l'ugualanza:

(3): Calcolo Periodo e
 definisco uguaglianza.

(4): Applico la f

Dati $\sigma^a, \sigma^b \in S_n$ allora
 se $\sigma^a = \sigma^b \rightarrow f(\sigma^a) = f(\sigma^b)$
 se $\sigma^{a-b} = id$

se Periodo(σ) = $a-b$

[Periodo] = 6 | a-b

se $3 \cdot 6 | 3(a-b)$

se $18 | 3a - 3b$

se $3a = 3b \checkmark$ ou

Per $\mathbb{Z}_n \rightarrow \mathbb{Z}_a \times \mathbb{Z}_b$

1. Definire 2 elementi di \mathbb{Z}_n : c, c' uguali $c=c'$ in \mathbb{Z}_n
2. Se è ben definita allora l'applicazione della funzione è equivalente: se $[c]_n = [c']_n$ se $([c]_a, [c]_b) = ([c']_a, [c']_b)$
3. Ciò sarà possibile solo se, quando i due numeri sono congruenti nel modulo di partenza, lo sono nei moduli del codominio.
Se $c \equiv c' \pmod{n} \rightarrow c \equiv c' \pmod{a} \wedge c \equiv c' \pmod{b}$
4. Questo sarà possibile solo se i moduli del codominio dividono il mod del dominio.

ES: "Data la funzione $f: \mathbb{Z}_{30} \rightarrow \mathbb{Z}_6 \times \mathbb{Z}_{15}$, $[a]_{30} \mapsto ([a]_6, [a]_{15})$
Determinare se è ben definita"

- (1) Dati $g, g' \in \mathbb{Z}_{30}$ se $g \equiv g' \pmod{30}$ allora
 $\begin{aligned} &g \equiv g' \pmod{6} \\ &\wedge g \equiv g' \pmod{15} \end{aligned}$
- (2) se $6|30$ e $15|30$
verificata

VERIFICA OMOMORFISMO \rightarrow C'RICHIENE CHE SIA BEN DEFINITA I

1. Definire il gruppo come:

$$f(g * g') = f(g) * f(g') \text{ per } g, g' \in G$$

2. Svolgere le operazioni su entrambi i lati dell'ugualanza.

3. SE convergono allo stesso elemento, allora è un omomorfismo.

KERNEL OMOMORFISMO \rightarrow (DEF)

Sono tutti gli elementi del Dominio dell'omomorfismo che puntano all'elemento neutro della funzione.

$$\text{Se } \text{Ker}(f) = \{e_0\} \Leftrightarrow f \text{ è iniettiva}$$

KERNEL OMONOMIA $(\mathbb{Z}_n \rightarrow S_m)$

1. Sono tutti gli elementi $\in \mathbb{Z}_n$ che se usati come potenza della permutazione danno l'identità:

$$\text{Ker}(f) = \{[n] \in \mathbb{Z}_n \mid f([n]) = id\}$$

Ovvio tutti i $\bar{z} \in \mathbb{Z}_n$ per i quali

$$\text{Periodo}(\sigma) \mid f(\bar{z})$$

Ovvio l'applicazione della funzione.

ES: "Data $f: \mathbb{Z}_7 \rightarrow S_6$ $\bar{z} \mapsto \bar{\sigma}^z$ omomorfismo, calcolare il Kernel."

(al calcolo periodo $\text{Periodo}(\sigma) = |\text{Periodo}| = 6$

(1) elenco gli elementi di \mathbb{Z}_7 che sono divisibili dal periodo:

$$6|2^0 \quad 6|2^1 \checkmark$$

$$6|2^2 \quad n=1 \times, 6|2^3 \quad n=2 \times, 6|2^4 \quad n=3 \checkmark$$

$$6|2^5 \quad n=4 \times, 6|2^6 \quad n=5 \times, 6|2^7 \quad n=6 \checkmark$$

$$\text{Kernel}(f) = \{ \bar{0}, \bar{3}, \bar{6} \}$$

Immagine(f) (co-dominio) \rightarrow

Sono tutti gli elementi che vengono raggiunti dalla funzione.

$$\text{Im}(f) = \text{Codominio} \Leftrightarrow \text{Suriettiva}$$

Immagine(f) : $\mathbb{Z}_m \rightarrow S_n$ \rightarrow

1. Partendo da 0 fino al periodo \mathbb{Z}_m applicare la funzione ed elencare gli elementi

ES: "Data $f: \mathbb{Z}_7 \rightarrow S_6$ $z \mapsto z^2$ omomorfismo, calcolare il immagine."

(1) Calcolo periodo Periodo(ω) = [Periodo] = 6

(2) elenco gli elementi di \mathbb{Z}_7

$$6|2|4 \quad 6|2|0$$

$$6|2|1 \quad n=1, \quad 6|2|2 \quad k=2, \quad , \quad 6|2|3 \quad k=3$$

$$6|2|4 \quad n=4, \quad 6|2|5 \quad n=5, \quad , \quad 6|2|6 \quad k=6$$

$$\text{Im}(f) = \{ \text{id}, 0^2, 1^2, 2^2, 3^2, 4^2, 5^2 \}$$

Immagine(f) : $\mathbb{Z}_n \rightarrow \mathbb{Z}_a \times \mathbb{Z}_b$ \rightarrow

1. Elencare gli elementi partendo dai valori del dominio

SURIETTIVITÀ : $\mathbb{Z}_n \rightarrow \mathbb{Z}_a \times \mathbb{Z}_b$ \rightarrow

1. Oltre a controllare che $\text{Im}(f) = \mathbb{Z}_a \times \mathbb{Z}_b$, si può controllare per cardinalità.

2. SE $|\mathbb{Z}_n| \neq |\mathbb{Z}_a \times \mathbb{Z}_b|$ non è suriettiva.

$$- |\mathbb{Z}_n| = \text{Num. di elementi} = n$$

$$- |\mathbb{Z}_a \times \mathbb{Z}_b| = a \cdot b$$

ES: "Data la funzione $f: \mathbb{Z}_{30} \rightarrow \mathbb{Z}_6 \times \mathbb{Z}_{15}$, $[a]_{30} \mapsto ([a]_6, [a]_{15})$

Determinare se è suriettiva

$$|\mathbb{Z}_{30}| = 30$$

$$|\mathbb{Z}_6 \times \mathbb{Z}_{15}| = 90$$

$$|\mathbb{Z}_{30}| < |\mathbb{Z}_6 \times \mathbb{Z}_{15}|$$

Non è suriettiva.

KERNEL OMOMORFISMO $\mathbb{Z}_n \rightarrow \mathbb{Z}_a \times \mathbb{Z}_b$

1. Sono gli elementi di \mathbb{Z}_n che sono divisibili dai moduli del codominio.

ES: "Data la funzione $f: \mathbb{Z}_{30} \rightarrow \mathbb{Z}_6 \times \mathbb{Z}_5$, $[z]_{30} \mapsto ([z]_6, [z]_5)$
Determinare $\text{Kernel}(f)$

$$\begin{aligned}\text{Ker}(f) &= \{z \in \mathbb{Z} \mid z \equiv 0 \pmod{6} \wedge z \equiv 0 \pmod{5}\} \\ &= \{z \in \mathbb{Z} \mid 6|z \wedge 5|z\} \quad \text{mcm}(6, 5) = 30 \\ &= \{z \in \mathbb{Z} \mid 30|z\} = \{0\} \text{ in } \mathbb{Z}_{30} \hookrightarrow \text{iniettiva}\end{aligned}$$