GRUPPI

VERIFICARE VALIDITÀ OPERAZIONI NEI GRUPPI

IN: • G • $g, g' \in G$, $g * g'$

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

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

NB: SE l'operazione contiene sistemi verificare ogni casistica.

ES: "Dato $G = [0,1) = \{ k \in \mathbb{R} \mid 0 \le k \wedge k < 1 \}$ e l'operazione $* : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ definita come:

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

Verificare che $*$ sia in G"

1. Definisco $g \in G$

$t \in G \leftrightarrow t \ge 0 \wedge t < 1 \rightarrow$

2. Estendo il ragionamento

$t_1 * t_2 \in G$ sse

Verifico per i casi del sistema

(CASO 1): $t_1 + t_2 < 1$

$t_1 + t_2 \in G$ sse

$$\underbrace{t_1 + t_2 \ge 0}_{\text{Vero per definizione}} \wedge \underbrace{t_1 + t_2 < 1}_{\text{Vero in questo caso del sistema}}$$

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

sse $t_1 + t_2 - 1 \ge 0$ ✓

sse $t_1 + t_2 \ge 1$) altro modo

sse $t_1 + t_2 < 2$

sse $t_1 + t_2 - 1 < 2 - 1$

sse $t_1 + t_2 - 1 < 1$ ✓

CALCOLARE PERIODO DI $x \in G$ IN OPERAZIONE

IN: • G • $g, g' \in G$, $g * g'$

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

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

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

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

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

1. 2. $\frac{2}{7} * \frac{2}{7} = \frac{4}{7}$ | 3. $\frac{4}{7} * \frac{2}{7} = \frac{6}{7}$ | 4. $\frac{6}{7} * \frac{2}{7} = \frac{1}{7}$ |
5. $\frac{1}{7} * \frac{2}{7} = \frac{3}{7}$ | 6. $\frac{3}{7} * \frac{2}{7} = \frac{5}{7}$ | 7. $\frac{5}{7} * \frac{2}{7} = \frac{7}{7} = e_G$

Il periodo è 7

GRUPPI 6

CASO DIOSO >

"Dato $U = \mathbb{Z}_{10}^*$, gruppo di classi di resto invertibili in $\mathbb{Z}_{10}$,
Provare che $a = [3^{303}]_{10}$ appartiene a U e che $\langle a \rangle$ coincide con U"

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

Ovvero provare che $[3^{303}]_{10}$ è invertibile.
Siccome n^x è invertibile $\leftrightarrow$ n è invertibile si può semplificare trovando l'inverso di 3

in $\mathbb{Z}_{10}$:
$MCD(3,10)$: $10 = 3 \cdot 3 + \underline{1}$
$3 = 3 \cdot 1 + 0$

$MCD(3,10) = 1 \leftrightarrow$ 3 è invertibile in $\mathbb{Z}_{10}$
quindi 3^x è invertibile in $\mathbb{Z}_{10}$
ovvero $[3^{303}]_{10}$ appartiene a U

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

Sapendo che $MCD(3,10) = 1$ e $10 = 3 \cdot 3 + 1$
bisogna semplificare $[3^{303}]_{10}$:

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

$303 = 75 \cdot 4 + 3$
$3^{75 \cdot 4 + 3} \Rightarrow \cancel{3}^{\cancel{4} \cdot 75} \cdot 3^3 = 3^3 \mod 10$
$3^{\varphi(n)} = 1$

Ciò vuol dire che si può
$27 \mod 10$ $27 - 10 = 7$
$7 \mod 10$

Per definire $\langle a \rangle = a^0, a^1, a^2, \dots$
con $\langle 7 \rangle$ $= 1, 7^1, 7^2, 7^3, 7^4, 7^5$
$= 1, 7, 49, 343, 2401$ 49 in mod 10 = 9
$1, 7, 9, 3, 1$
si ripete, va omesso

$\langle 7 \rangle = \{1, 7, 9, 3\}$

Per verificare che coincida con U dobbiamo elencare tutti gli elementi da 1 a n in $\mathbb{Z}_n$ che siano invertibili, ovvero $MCD(x,n) = 1$

in $\mathbb{Z}_{10}$
$MCD(1,10) = 1$
$MCD(2,10) = 2$ $10 = 5 \cdot 2 + 0$ $U = \{1, 3, 7, 9\} = \langle a \rangle$
$MCD(3,10) = 1$
$MCD(4,10) = 2$ $10 = 4 \cdot 2 + \underline{2}$
$MCD(5,10) = 5$ $10 = 2 \cdot 5 + 0$
$MCD(6,10) = 2$ $10 = 1 \cdot 6 + 4 \rightarrow 6 = 1 \cdot 4 + \underline{2} \rightarrow 4 = 2 \cdot 2 + 0$
$MCD(7,10) = 1$ $10 = 1 \cdot 7 + 3 \rightarrow 7 = 2 \cdot 3 + \underline{1} \rightarrow 3 = 3 \cdot 1 + 0$
$MCD(8,10) = 2$ $10 = 1 \cdot 8 + \underline{2} \rightarrow 8 = 4 \cdot 2 + 0$
$MCD(9,10) = 1$ $10 = 1 \cdot 9 + \underline{1} \rightarrow 9 = 9 \cdot 1 + 0$

GRUPPI 7

ELENCARE ELEMENTI INVERTIBILI $\mathbb{Z}_n^\times$

1. Usare la funzione di Eulero per ottenere la quantità di invertibili
   [vedere Gruppi 1: Funz. Eulero]
2. 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]
   - La seconda metà saranno gli elementi della prima negati (poi sommare n quanto basta per averli ≥ 0)

ALTERNATIVA A
[GRUPPI 4 - ELENCARE ELEMENTI INVERTIBILI]

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

$\mathbb{Z}^\times = \{\pm 1\}$

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

$12 = 3 \cdot 2^2$

Trovo la prima metà: 1, 5

$\underline{1}\ \cancel{2}\ \cancel{3}\ \cancel{4}\ \underline{5}\ 6\ 7\ 8\ 9\ 10\ 11$

La seconda metà sarà negata: $-1, -5$

$= -1 + 12 = 11$

$= -5 + 12 = 7$

Totale$_{\mathbb{Z}_{12}}$ = 1, 5, 11, 7

GENERATORI ($\mathbb{Z}_n^\times$)

! RICHIEDE UNO TRA
[GRP-4: ELENCARE ELEMENTI INVERTIBILI]
[GRP-7: ELENCARE ELEMENTI INVERTIBILI]

1. Calcolare gli elementi invertibili !
2. PER OGNI elemento invertibile g
   1.1 Determinare il minimo $k \in \mathbb{N}$ per il quale $g^k \equiv 1 \bmod n$
3. I generatori saranno tutti gli elementi che hanno $k = \varphi(n)$
   [GRP 1 - EULERO]

NB Basta trovare il k per la prima metà

ES: "Dato $\mathbb{Z}_{20}$ determinare i generatori"

(1) Elenco gli invertibili

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

$1\ \cancel{2}\ 3\ \cancel{4}\ \cancel{5}\ \cancel{6}\ 7\ \cancel{8}\ 9$

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

$= \{1, 3, 7, 9, 19, 17, 13, 11\}$

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

$(\pm 1)^1 \equiv 1 \bmod 20$

$(\pm 3)^4 \equiv 1 \bmod 20$

$(\pm 7)^4 \equiv 1 \bmod 20$

$(\pm 9)^2 \equiv 1 \bmod 20$

Nessuno ha $k = 8$
NON CI SONO GENERATORI

CICLICITÀ $(\mathbb{Z}_n^\times)$ => 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 $\mathbb{Z}_{20}$:
- Quanti modi si hanno di scegliere 3 classi invertibili
- Dire se il gruppo moltiplicativo $\mathbb{Z}_{20}^\times$ è ciclico o no
- Determinare tutti gli n tale che $\bar{3}^n = \bar{9}$"

(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: ✗ ripetizioni, ✗ ordine

$= \binom{8}{3} = \frac{8!}{3! \cdot 5!} = 56$ modi

(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: $12 = 2^2 \cdot 5$
1° metà 1 ~~2~~ 3 ~~4~~ ~~5~~ ~~6~~ 7 ~~8~~ 9
su 8 = 1, 3, 7, 8, 9 → $\{\pm 1, \pm 3, \pm 7, \pm 9\}$

2.2) Determino min k t.c. $g^k = 1 \bmod n$

$(\pm 1)^1 \equiv 1 \bmod 20$, $(\pm 3)^4 \equiv 1 \bmod 20$, $(\pm 7)^4 \equiv 1 \bmod 20$
$(\pm 9)^2 \equiv 1 \bmod 20$

Non ha generatori <-> Non è ciclico

3) Sapendo che il periodo di $\bar{3}^n$ è 4 e $\bar{3}^2 = 9$
allora

$\{n \in \mathbb{Z} \mid n \equiv 2 \bmod 4\} = \{\ldots, -6, -2, 2, 6, 10 \ldots\}$

(sopra: $-2\ \ -1\ \ 0\ \ 1\ \ 2$)

FUNZIONI • 1 [VERIFICA BEN DEFINITA]

PER $\mathbb{Z}_n \to S_m$

1. Partire definendo due elementi uguali $a, b \in \mathbb{Z}_m$.
2. Proseguire definendo che se sono uguali, anche le applicazioni delle funzioni dovranno esserlo.
   NB: Sfruttare la proprietà $\sigma^a = \sigma^b$ sse $a-b=0$
3. Sfruttare la proprietà precedente, definendo che la n di $\mathbb{Z}_n$ divide a-b : $n \mid a-b$ giungendo che sse $\exists t$ t.c. $a = b + tn$
4. Applicare la funzione con a e sostituirla con quanto detto
   NB: Calcolare il periodo di σ [vedere sezione] per semplificare
5. SE si ottiene f(b), allora è ben definita.

ES: "Data la funzione $f: \mathbb{Z}_{10} \to S_m$, $\bar{a} \mapsto \sigma^{3a}$. Stabilire se è ben definita."

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

Dati $\bar{a}, \bar{b} \in \mathbb{Z}_{10}$, se $\bar{a} = \bar{b} \to f(\bar{a}) = f(\bar{b})$

(2) sfrutto prop. $\to$ sse $\sigma^a = \sigma^b$

sse $\sigma^{a-b} = id$

$\to$ sse $a - b = 0$

(3) n di $\mathbb{Z}_n \mid a-b \to$ sse $10 \mid a-b$ in $\mathbb{Z}_{10}$

(3) definisco 'a' sse $\exists t$ t.c. $a = b + 10t$

(4) applico f(a)

con $f(\bar{a}) = \sigma^{3a} \Rightarrow \sigma^{3(b+10t)} \Rightarrow \sigma^{3b+30t} = \sigma^{3b} = f(\bar{b}) \leftarrow (5)$

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

quindi Periodo(σ) $\mid 30t \to \sigma^{30t} = id$

FUNZIONI • 2 [VERIFICA BEN DEFINITA]

Per $S_n \to \mathbb{Z}_n$ >

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 $\sigma^a = \sigma^B$ sse $\sigma^{a-b} = id$
3. Calcolare il Periodo. Partendo dalla formula precedente:
   Periodo$(\sigma) \mid a-b$ [vedere sezione Periodo Perm]
4. Adattare l'espressione applicando la funzione.
5. SE Quando applicata la funzione ho l'uguaglianza tra a,b allora è ben definita.

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

$\forall a,b \in \mathbb{Z}$

(1): Definisco le Permutazioni — Dati $\sigma^a, \sigma^B \in S_n$ allora

(2): Definisco l'uguaglianza: — se $\sigma^a = \sigma^B \to f(\sigma^a) = f(\sigma^B)$

se $\sigma^{a-b} = id$

(3): Calcolo Periodo e definisco uguaglianza. — sse Periodo$(\sigma) = a-b$

[Periodo] $= 6 \mid a-b$

(4): Applico la f — sse $3 \cdot 6 \mid 3(a-b)$

sse $18 \mid 3a-3b$

sse $3a = 3b$ ✓ ok

FUNZIONI • 3 [VERIFICA BEN DEFINITA]

Per $\mathbb{Z}_n \to \mathbb{Z}_a \times \mathbb{Z}_b$ >

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 $[c]_n = [c']_n$ sse $([c]_a, [c]_b) = ([c']_a, [c']_b)$
3. Ciò sarà possibile solo se, quando i due numeri sono congruenti nel modulo di partenza, lo sono nei moduli del co-dominio

   SE $c \equiv c' \mod n \to c \equiv c' \mod a \wedge c \equiv c' \mod b$
4. Questo sarà possibile solo se i moduli del co-dominio dividono il mod del dominio.

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

(1) Dati $g, g' \in \mathbb{Z}_{30}$ se $g \equiv g' \mod 30$ allora $g \equiv g' \mod 6$ $\wedge\ g \equiv g' \mod 15$

(2) sse $6 | 30$ e $15 | 30$
verificata

FUNZIONI 3

VERIFICA OMOMORFISMO [RICHIEDE CHE SIA BEN DEFINITA]

1. Definire il gruppo come:
   $$f(g * g') = f(g) * f(g') \quad \text{per } g, g' \in G$$

2. Svolgere le operazioni su entrambi i lati dell'uguaglianza.
3. **SE** convergono allo stesso elemento, allora è un omomorfismo.

KERNEL OMOMORFISMO (DEF)

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

Se $\ker(f) = \{e_G\} \iff f$ è iniettiva

KERNEL OMOMORFISMO ($\mathbb{Z}_n \to S_m$)

1. Sono tutti gli elementi $\in \mathbb{Z}_n$ che se usati come potenza della permutazione danno l'identità:
   $$\ker(f) = \{ [n] \in \mathbb{Z}_n \mid f(\bar{n}) = id \}$$

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

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

Ovvero l'applicazione della funzione.

ES: "Data $f: \mathbb{Z}_7 \to S_n \quad \bar{z} \mapsto \sigma^{2z}$ omomorfismo, calcolare il Kernel."

(0) Calcolo periodo $\text{Periodo}(\sigma) = [\text{periodo}] = 6$

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

$6 \mid 2k \qquad 6 \mid 2 \cdot 0$ ✓

$6 \mid 2 \cdot 1 \quad k=1$ ✗, $6 \mid 2 \cdot 2 \quad k=2$ ✗, $6 \mid 2 \cdot 3 \quad k=3$ ✓

$6 \mid 2 \cdot 4 \quad k=4$ ✗, $6 \mid 2 \cdot 5 \quad k=5$ ✗, $6 \mid 2 \cdot 6 \quad k=6$ ✓

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

Immagine(f) (Co-Dominio)

Sono tutti gli elementi che vengono raggiunti dalla funzione.

Im(f) = Codominio $\iff$ Suriettiva

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

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

ES: "Data $f: \mathbb{Z}_7 \to S_n$ $z \mapsto \sigma^{2z}$ omomorfismo, calcolarne il immagine."

(0) Calcolo periodo Periodo(σ) = [periodo] = 6

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

$6 \mid 24$ $\quad 6 \nmid 2 \cdot 0$

$6 \mid 2 \cdot 1 \quad k=1$, $6 \mid 2 \cdot 2 \quad k=2$, $6 \mid 2 \cdot 3 \quad k=3$

$6 \mid 2 \cdot 4 \quad k=4$, $6 \mid 2 \cdot 5 \quad k=5$, $6 \mid 2 \cdot 6 \quad k=6$

$Im(f) = \{ id, \sigma^2, \sigma^4, \sigma^6, \sigma^8, \sigma^{10}, \sigma^{12} \}$

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

1. Elencare gli elementi partendo dai valori del dominio

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

1. Oltre a controllare che $Im(f) = \mathbb{Z}_a \times \mathbb{Z}_b$, si può controllare per cardinalità.
2. SE $|\mathbb{Z}_n| \neq |\mathbb{Z}_a \times \mathbb{Z}_b|$ non è suriettiva.
   - $|\mathbb{Z}_n|$ = Num. di elementi = n
   - $|\mathbb{Z}_a \times \mathbb{Z}_b| = a \cdot b$

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

$|\mathbb{Z}_{30}| = 30$ $\quad |\mathbb{Z}_6 \times \mathbb{Z}_{15}| = 90$ $\quad |\mathbb{Z}_{30}| < |\mathbb{Z}_6 \times \mathbb{Z}_{15}|$

Non è suriettiva.

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

1. Sono gli elementi di $\mathbb{Z}_n$ che sono divisibili dai moduli del co-dominio.

ES: "Data la funzione $f: \mathbb{Z}_{30} \to \mathbb{Z}_6 \times \mathbb{Z}_5$, $[a]_{30} \mapsto ([a]_6, [a]_5)$
Determina Kernel(f)"

$$\ker(f) = \{ z \in \mathbb{Z} \mid z \equiv \bar{0} \bmod 6 \wedge z \equiv \bar{0} \bmod 5 \}$$
$$= \{ z \in \mathbb{Z} \mid 6 \mid z \wedge 5 \mid z \} \qquad mcm(6,5) = 30$$
$$= \{ z \in \mathbb{Z} \mid 30 \mid z \} = \{ \bar{0} \} \text{ in } \mathbb{Z}_{30} \iff \text{iniettiva}$$