

CIOÈ SE E SOLO SE $\det(A) \in \{-1, 1\}$, E QUINDI SE E SOLO SE LA FUNZIONE ASSOCIAVA $f: \{1, \dots, n\} \rightarrow \{1, \dots, n\}$ È BIUNIVOCO. DA CIÒ SEGUE IL TEOREMA DI CAYLEY: UN GRUPPO FINITO G DI CARDINALITÀ $|G|=n$ È ISOMORFO AD UN GRUPPO DI MATEMATICHE, DELL'ELEMENTO DI PERMUTAZIONI, LE CUI COMPONENTI SONO "0" ED "1" E CHE HANNO UN UNICO "1" IN OGNI RIGA E OGNI COLONNA. INOLTRE, IL GRUPPO G È ISOMORFO AD UN SOTTOGRUPPO DEL GRUPPO DELLE FUNZIONI BIUNIVOCHE DA $\{1, \dots, n\}$ IN $\{1, \dots, n\}$ CHE ABBIAMO INDICATO COME GRUPPO SIMMETRICO S_n . GLI ELEMENTI DI S_n IN NOTAZIONE AD UNA LINEA SONO INDICATI COME SEGU:

SIA $\alpha \in S_n$ UNA FUNZIONE BIUNIVOCO DA $\{1, \dots, n\}$ IN $\{1, \dots, n\}$.
ALLORA, LA STRINGA $\alpha(1)\alpha(2)\dots\alpha(n)$ INDICA UNIVOCAMENTE L'ELEMENTO

ESEMPI:

a) $S_2 = \{12, 21\}$

b) $S_3 = \{123, 213, 132, 231, 312, 321\}$

c) VEDIAMO $(\mathbb{Z}_2, +)$ COME GRUPPO DI MATEMATICHE E GRUPPO DI PERMUTAZIONI. $(\mathbb{Z}_2, +) \cong \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\} \stackrel{\text{ISOMORFISMO DI GRUPPI}}{\cong} \{12, 21\} = S_2$

RELAZIONI SU UN INSIEME

SIA A UN INSIEME. UNA RELAZIONE SU A È DEFINITA DA UN SOTTOINSIEME $R \subseteq A \times A$. UN PARTICOLARE TIPO DI RELAZIONE È LA RELAZIONE DI EQUIVALENZA, CHE SI HA QUANDO SONO SODDISFAITE LE PROPRIETÀ:

• RIFLESSIVA $(a, a) \in R \quad \forall a \in A$

• SIMMETRICA $(a_1, a_2) \in R \Rightarrow (a_2, a_1) \in R \quad \forall a_1, a_2 \in A$

• TRANSITIVA $(a_1, a_2) \in R \wedge (a_2, a_3) \in R \Rightarrow (a_1, a_3) \in R \quad \forall a_1, a_2, a_3 \in R$

SE R È UNA RELAZIONE DI EQUIVALENZA SU A E $(a_1, a_2) \in R$,

SCRIVIAMO $a_1 \sim a_2$ "a₁ È EQUIVALENTE AD a₂".

SIA $a_1 \in A$ UN ELEMENTO DI A ED R UNA RELAZIONE DI EQUIVALENZA.

L' INSIEME $[a_1] := \{a_2 \in A | a_1 \sim a_2\}$ È DETTO CLASSE DI EQUIVALENZA DI a₁.

L' INSIEME $\frac{A}{\sim} := \{[a] | a \in A\}$ È DETTO INSIEME QUOTIENTE.

LA FUNZIONE $\pi: A \xrightarrow{\sim} \frac{A}{\sim}$ È DETTA PROIEZIONE CANONICA.
 $a \mapsto [a]$

SIANO $a_1, a_2 \in A$. $a_1 \sim a_2 \Rightarrow [a_1] = [a_2]; a_1 \not\sim a_2 \Rightarrow [a_1] \cap$

$\pi[a_2] = \emptyset$. QUINDI $A = \bigcup_{[a] \in \frac{A}{\sim}} [a]$, OSSIA $\frac{A}{\sim}$ È UNA

PARTIZIONE DI A.

ESEMPI:

a) L'UGUAGLIANZA = È UNA RELAZIONE DI EQUIVALENZA SU Ogni INSIEME A

b) SIA $A = \{1, 2, \dots, n\}$. DEFINIAMO SU (PCA) LA RELAZIONE $X \sim Y \Leftrightarrow |X| = |Y|$

$\forall X, Y \subseteq A$. QUESTA È UNA RELAZIONE DI EQUIVALENZA E $\frac{\text{PCA}}{|A|} \sim$

$\sim \{0, 1, \dots, n\}$. SE $X \subseteq A$ ($|X| = k \leq n \Rightarrow |[X]| = \binom{n}{k} = \frac{n!}{k!(n-k)!}$)

$\binom{n}{k}$ È DETTO COEFFICIENTE BINOMIALE, POICHÉ $(x+y)^n = \sum_{k=0}^n \binom{n}{k} x^n y^{n-k} \forall x, y \in$

c) SIA G UN GRUPPO E $H \subseteq G$ UN SOTOGRUPPO. LA RELAZIONE \sim SU G

DEFINITA DA $g_1 \sim g_2 \Leftrightarrow \exists h \in H \mid g_1 = g_2 h$ È DI EQUIVALENZA

- $g \sim g : g = g_i, g \in G \wedge i \in H$
- $g_1 \sim g_2 \Rightarrow g_2 \sim g_1 : \exists h \in H \mid g_1 = g_2 h \Rightarrow \exists h^{-1} \in H \mid g_2 = g_1 h^{-1}$
- $g_1 \sim g_2 \wedge g_2 \sim g_3 \Rightarrow g_1 \sim g_3 : \exists h, h' \mid g_1 = g_2 h \wedge g_2 = g_3 h'$
 $\Rightarrow \exists h'' = hh' \in H \mid g_1 = g_3 h'' \quad \forall g_1, g_2, g_3 \in G.$

IN QUESTO CASO, INDICHEREMO CON $\frac{G}{H}$ L'INSIEME QUOTIENTE. SE G È UN

GRUPPO ABELIANO LA CUI OPERAZIONE COMMUTATIVA È INDICATA CON "+",

POSSIAMO DEFINIRE, SU $\frac{G}{H}$, L'OPERAZIONE $[g_1] + [g_2] = [g_1 + g_2]$ COME segue:

$$g'_1 = g_1 + h_1 \wedge g'_2 = g_2 + h_2 \Rightarrow [g'_1] = [g_1] \wedge [g'_2] = [g_2] \wedge g'_1 + g'_2 =$$

$$= g_1 + h_1 + g_2 + h_2 = g_1 + g_2 + h, \text{ con } h_1, h_2, h \in H \Rightarrow [g'_1 + g'_2] = [g_1 + g_2] \Rightarrow$$

\Rightarrow L'OPERAZIONE È COMMUTATIVA E ASSOCIAUTIVA, ESSENDO ANCHE QUELLA SU G .

INOLTRE, $\forall [g] \in \frac{G}{H}$ $[g] + [0] = [g] \Rightarrow$ LA CLASSE $[0]$ DELL'IDENTITÀ DI G È L'IDENTITÀ DI $(\frac{G}{H}, +)$. INFINE, DATO $-g \in G$ L'INVERSO DI g ,

$$[g] + [-g] = [g - g] = 0 \Rightarrow -[g] = [-g] \quad \forall [g] \in \frac{G}{H}$$

$\Rightarrow (\frac{G}{H}, +)$ È UN GRUPPO ABELIANO

ESEMPI:

a) $H = \{\overline{0}\} \subseteq G \Rightarrow G/H \cong G$

GRUPPO BANALE \downarrow GRUPPO ABELIANO \curvearrowright ISOMORFISMO DI GRUPPI

b) SIA $G = (\mathbb{Z}, +)$ E $n \in \mathbb{N}$. I SOTTOINSIEMI $n\mathbb{Z} := \{\sum kn \mid k \in \mathbb{Z}\}$

È UN SOTOGRUPPO DI \mathbb{Z} . DEFINIAMO IL GRUPPO ABELIANO $\mathbb{Z}_n := \frac{\mathbb{Z}}{n\mathbb{Z}}$

$$\mathbb{Z}_0 = \frac{\mathbb{Z}}{0\mathbb{Z}} = \frac{\mathbb{Z}}{\{\overline{0}\}} \cong \mathbb{Z}$$

In GENERALE, SIA $n > 0$ E $x, y \in \mathbb{Z}$

$$\Rightarrow x \sim y \Leftrightarrow \exists h \in \mathbb{Z} \mid x = y + h \Leftrightarrow \exists k \in \mathbb{Z} \mid x - y = kn$$

\Leftrightarrow IL RESTO DELLA DIVISIONE DI x PER n È UGUALE AL RESTO DELLA

DIVISIONE DI y PER n . I POSSIBILI RESTI DELLA DIVISIONE PER n SONO

$$\{\overline{0}, \overline{1}, \dots, \overline{n-1}\} \Rightarrow \mathbb{Z}_n = \{\overline{0}, \overline{1}, \dots, \overline{n-1}\} = \{\overline{0}, \overline{1}, \dots, \overline{n-1}\}.$$

$$\mathbb{Z}_2 = \{\overline{0}, \overline{1}\}$$

ESEMPIO

$$\overline{1} + \overline{1} = [\overline{1} + \overline{1}] = [\overline{2}] = [\overline{0}]$$

+	$\overline{0}$	$\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{1}$
$\overline{1}$	$\overline{1}$	$\overline{0}$

$$\mathbb{Z}_3 = \{\bar{0}, \bar{1}, \bar{2}\}$$

$$\bar{1} + \bar{1} = [1+1] = [2] = \bar{2}$$

$$\bar{1} + \bar{2} = [1+2] = [3] = [0] = \bar{0}$$

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{0}$	$\bar{1}$

SIA G UN GRUPPO ABELIANO E $H \subseteq G$ UN SOTTOGRUPPO. LA PROIEZIONE

CANONICA $\pi_G: G \rightarrow \frac{G}{H}$ È UN MORFISMO SURGETTIVO DI GRUPPI.

SE G È UN GRUPPO FINITO E $H \subseteq G$ È UN SOTTOGRUPPO $\Rightarrow \frac{G}{H} \exists [g]$

$\Rightarrow |[g]| = |H|$. INFATTI, $[g] = \{gh \mid h \in H\} \wedge gh_1 = gh_2 \Rightarrow h_1 = h_2$. POICHÉ LE CLASSI DI EQUIVALENZA SONO UNA PARTIZIONE DI G , ABBIAMO $|G| = |\frac{G}{H}| \cdot |H|$.

In particolare, LA CARDINALITÀ/ORDINE DI UN SOTTOGRUPPO DI UN GRUPPO

FINITO DIVIDE LA CARDINALITÀ DEL GRUPPO.

PROPOSIZIONE: SIA $f: G_1 \rightarrow G_2$ UN MORFISMO DI GRUPPI. ALLORA f È

INIETTIVO SE E SOLO SE $\text{Ker}(f) = \{i_1\}$

DIM

$\Rightarrow)$ SIA f UNA FUNZIONE INIETTIVA E SI CONSIDERI $x \in \text{Ker}(f)$. ALLORA

$f(x) = i_2$ E, POICHÉ ANCHE $f(i_1) = i_2 \Rightarrow x = i_1$ PER INIETTIVITÀ ✓

$\Leftarrow)$ SIA $\text{Ker}(f) = \{i_2\}$ E $x, y \in G_1 \mid f(x) = f(y)$. ALLORA $f(x) = f(y)$

$= i_2 \Rightarrow f(x^{-1}) = i_2 \Rightarrow x^{-1} \in \text{Ker}(f) \Rightarrow x^{-1} = i_1 \Rightarrow x = y$

$\Rightarrow f$ INIETTIVA ✓



IL TEOREMA PRECEDENTE NON È VERO PER I MORFISMI DI MONOIDI, AD ESEMPIO

$$f_N: (\mathbb{N}, \cdot) \rightarrow (\mathbb{N}, \cdot) \text{ E } f(n) = \begin{cases} 1 & n=1 \\ 0 & n \neq 1 \end{cases}$$

ESEMPI:

a) $G = \mathbb{Z}_4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$

$$\langle \bar{0} \rangle = \{\bar{0}\} \text{ SOTTOGRUPPO BANALE } \simeq \mathbb{Z}_1$$

$$\langle \bar{1} \rangle = \mathbb{Z}_4 \quad \langle \bar{2} \rangle = \{\bar{0}, \bar{2}\} = \mathbb{Z}_2 \quad \langle \bar{3} \rangle = \mathbb{Z}_4$$

I SOTTOGRUPPI DI \mathbb{Z}_4 POSSONO AVERE CARDINALITÀ 1, 2, 4. L'INSIEME

DEI SOTTOGRUPPI DI \mathbb{Z}_4 È $\{\{ \bar{0} \}, \{\bar{0}, \bar{2}\}, \mathbb{Z}_4\}$

b) $G = \mathbb{Z}_6 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$

$$\langle \bar{0} \rangle = \{\bar{0}\} \quad \langle \bar{1} \rangle = \langle \bar{5} \rangle = \mathbb{Z}_6 \quad \langle \bar{2} \rangle = \{\bar{0}, \bar{2}, \bar{4}\} = \langle \bar{4} \rangle = \mathbb{Z}_3$$

$$\langle \bar{3} \rangle = \{\bar{0}, \bar{3}\} = \mathbb{Z}_2$$

In GENERALE consideriamo il GRUPPO $\mathbb{Z}_n = (\{\bar{0}, \bar{1}, \dots, \bar{n-1}\}, +)$ E SIA

$m \in \mathbb{N}$ $|m| < n$.

• $m=0 \Rightarrow \langle \bar{0} \rangle = \{\bar{0}\}$

• $m > 0$, $\bar{z} = \frac{m \cdot m \{m, n\}}{m} = \sum_{i=1}^m \bar{m}_{i,i} = \overline{\bar{m}} = \overline{m \cdot m \{m, n\}} = 0$

$$i \not\mid z \Rightarrow i \mid m \wedge z \mid m = m \cdot m \{m, n\} \Rightarrow n \text{ NON DIVIDE } im$$

• $1 \leq i \leq z \Rightarrow \sum_{k=1}^i \bar{m}_{k,k} = \overline{im} \neq \bar{0}$ PERCHÉ im È MULTIPLO DI m E
 $im \not\mid m \cdot m \{m, n\}$

$\Rightarrow im \in \mathbb{Z} \text{ È DIVISO DA } n \text{ PER LA MINIMALITÀ DI MCM} \Rightarrow |Lm| = \mathbb{Z} \subset \frac{\mathbb{Z}_{m,n}}{m}$

IN PARTICOLARE, $\langle \bar{m} \rangle = \mathbb{Z}_m \Leftrightarrow z = n \Leftrightarrow \text{MCD}\{\bar{m}, \bar{n}\} = 1$, OSSIA L'INSIEME

$\{\bar{m}\}$ GENERA IL GRUPPO $\mathbb{Z}_n \Leftrightarrow m \text{ ED } n \text{ SONO COPRIMI.}$

DEFINIZIONE) LA FUNZIONE DEFINITA DA $\varphi: \mathbb{N}_{\geq 0} \rightarrow \mathbb{N}_{\geq 0}$ COME

$\varphi(n) = |\{m \leq n \mid \text{MCD}\{m, n\} = 1\}|$ È LA FUNZIONE DI EULER, QUINDI

CI SONO $\varphi(n)$ ELEMENTI $\bar{m} \mid \langle \bar{m} \rangle = \mathbb{Z}_n$

PROPOSIZIONE 4a: L'INSIEME DEI SOTOGRUPPI DI $(\mathbb{Z}, +)$ È $\{n\mathbb{Z} \mid n \in \mathbb{N}\}$

DIM

SIA $H \subseteq \mathbb{Z}$ UN SOTOGRUPPO NON BANALE E $K := \min H > 0$, DOVE

$H_{>0} := \{h \in H \mid h > 0\}$. SIA $h \in H_{>0} \neq K$. ALLORA, SICURAMENTE

$h > K$ E, IN PARTICOLARE, $h = hK + r$ CON $n \in \mathbb{N}$ E $0 \leq r < K$. DUNQUE,

$r = h - hK \in H \Rightarrow r = 0$ PER LA MINIMALITÀ DI K

DEFINIZIONE) UN GRUPPO G È CIClico SE $\exists g \in G \mid G = \langle g \rangle$

NOTA: UN GRUPPO CIClico È ABELIANO

ESEMPI:

a) $\mathbb{Z} = \langle 1 \rangle$ È CIClico

b) $\mathbb{Z}_n = \langle \bar{1} \rangle$ È CIClico

c) $\mathbb{Z} \times \mathbb{Z} = \langle (1,0), (0,1) \rangle$ NON È CIClico

INFATI, IN $\mathbb{Z} \times \mathbb{Z}$, SE $(a, b) \in \mathbb{Z} \times \mathbb{Z} \Rightarrow L(a, b) = \{(ka, kb)\}$

$| k \in \mathbb{Z} \} = \{(x, y) | x \text{ DIVIDE } x \wedge b \text{ DIVIDE } y\} \notin \mathbb{Z} \times \mathbb{Z}$

d) $\mathbb{Z}_2 \times \mathbb{Z}_2$ NON È CICLO

INFATI, IN $\mathbb{Z}_2 \times \mathbb{Z}_2$, SI HA:

- $L(\bar{0}, \bar{0}) = \{\bar{0}, \bar{0}\}$
- $L(\bar{0}, \bar{1}) = \{\bar{0}\} \times \mathbb{Z}_2$
- $L(\bar{1}, \bar{0}) = \mathbb{Z}_2 \times \{\bar{0}\}$
- $L(\bar{1}, \bar{1}) = \{\bar{0}, \bar{0}\}, (\bar{1}, \bar{1})\}$

QUINDI NESSUN ELEMENTO DI $\mathbb{Z}_2 \times \mathbb{Z}_2$ GENERA $\mathbb{Z}_2 \times \mathbb{Z}_2$

TEOREMA 3a: SIA $f: G_1 \rightarrow G_2$ UN MORFISMO DI GRUPPI ABELIANI. ALLORA

ESISTE UN MORFISMO INIETTOVO $\varphi: \frac{G_1}{\ker(f)} \rightarrow G_2$ TALE CHE $\frac{G_1}{\ker(f)} \cong \text{Im}(f)$

$$\begin{array}{ccc} G_1 & \xrightarrow{f} & G_2 \\ \downarrow \pi & \nearrow \varphi & \\ \frac{G_1}{\ker(f)} & & \end{array}$$

E IL SEGUENTE DIAGRAMMA È COMMUTATIVO

DIM

L'ASSEGNAZIONE $[g] \mapsto f(g)$ $\forall g \in G$ DEFINISCE UNA FUNZIONE $\varphi: \frac{G_1}{\ker(f)} \rightarrow G_2$.

INFATI, SE $g' \sim g$ (OSSIA $[g] = [g']$) $\Rightarrow \exists h \in \ker(f) \mid g = g' + h \Rightarrow$

$f(g) = f(g' + h) = f(g') + f(h) = f(g')$. POICHÉ f È MORFISMO DI GRUPPI,

ANCHE φ LO È. INOLTRE, $\text{Ker}(\varphi) = \{[g] \in \frac{G}{\text{Ker}(\varphi)} \mid \varphi([g]) = 0_2\} =$

$= \{[g] \in \frac{G}{\text{Ker}(\varphi)} \mid R(g) = 0_2\} = \{[0_2]\} \Rightarrow \varphi$ È INIEITIVO.

INFINE, $\varphi: \frac{G}{\text{Ker}(\varphi)} \rightarrow \text{Im}(\varphi)$ È UN MORFISMO DI GRUPPI INIEITIVO E SURIENTIVO
E QUINDI UN ISOMORFISMO

TEOREMA 1: SIA G UN GRUPPO CIClico. ALLORA OGNI SOTOGRUPO DI G È CICLICO

DIM

SIA $g \in G | G = \langle g \rangle$. LA FUNZIONE $\varphi: (\mathbb{Z}, +) \rightarrow G$ DEFINITA DA $\varphi(n) = g^n$

$\forall n \in \mathbb{Z}$ È UN MORFISMO SURIENTIVO DI GRUPPI. SI DISTINGUONO DUE CASI:

- G È INFINITO $\Rightarrow \text{Ker}(\varphi) = \{0\} \Rightarrow \varphi$ INIEITIVO $\Rightarrow \varphi$ È UN ISOMORFISMO

DI GRUPPI. TUTTI I SOTOGRUSSI DI \mathbb{Z} SONO CICLICI

- G È FINITO \Rightarrow SIA $H \subseteq G$ UN SOTOGRUPO. ALLORA

$\varphi^{-1}(H) := \{n \in \mathbb{Z} \mid \varphi(n) \in H\} \subseteq \mathbb{Z}$ È UN SOTOGRUPO DI $\mathbb{Z} \Rightarrow \exists k \in \mathbb{N} \mid$

$\varphi^{-1}(H) = \langle k \rangle$. LA RESTRIZIONE $\varphi: k\mathbb{Z} \rightarrow H$ È UN MORFISMO SURIENTIVO

DI GRUPPI E $\varphi(hk) = \varphi\left(\sum_{i=1}^h k_i\right) = \prod_{i=1}^h \varphi(k)_i = [\varphi(k)]^h$ $\forall h \in \mathbb{Z} \Rightarrow H = \langle \varphi(k) \rangle$

COROLARIO 4C: L'INSIEME DEI SOTOGRUSSI DI \mathbb{Z}_n , $n \in \mathbb{N}$, È

$\{\bar{m} \mid \bar{m} \in \mathbb{Z}_n\}$

PROPOSIZIONE: SIA $n \in \mathbb{N}$ E d/n (d DIVIDE n). ALLORA ESISTE AL PIÙ UN UNICO SOTOGRUPO DI \mathbb{Z}_n DI CARDINALITÀ d .

DIM

SIA $H \subseteq \mathbb{Z}_n$ UN SOTOGRUPO $|H|=d$. SI CONSIDERINO LE PROIEZIONI

CANONICHE $\mathbb{Z} \xrightarrow{\pi_1} \mathbb{Z}_n \xrightarrow{\pi_2} \frac{\mathbb{Z}_n}{H}$. POICHÉ $\pi_1^{-1}(H) = \{m \in \mathbb{Z} \mid \pi_1(m) \in H\}$

È UN SOTOGRUPO DI \mathbb{Z} , $\exists k \in \mathbb{N} \mid \pi_1^{-1}(H) = k\mathbb{Z}$. INOLTRE, $\text{Ker}(\pi_2 \circ \pi_1) =$

$= \pi_1^{-1}(H)$ E QUINDI, ESSENDO $(\pi_2 \circ \pi_1)$ MORFISMO SURIEBITIVO DI GRUPPI,

$\frac{\mathbb{Z}_n}{H} \cong \frac{\mathbb{Z}}{\pi_1^{-1}(H)} = \frac{\mathbb{Z}}{k\mathbb{Z}} = \mathbb{Z}_k \Rightarrow |\mathbb{Z}_k| = k = \left| \frac{\mathbb{Z}_n}{H} \right| = \frac{|\mathbb{Z}_n|}{|H|} = \frac{n}{d} \Rightarrow k \text{ È UM VOLAMENTE DETERMINATO}$

DETERMINATO E $H = \pi_1(k\mathbb{Z})$ È UNIVOCAMENTE DETERMINATO

ESEMPIO: \mathbb{Z}_{899} $899 = 31 \cdot 29 \Rightarrow$ QUANTO SOTOGRUPPI:

$\{ \{0\}, \{ \overline{29} \}, \{ \overline{31} \}, \mathbb{Z}_{899} \}$

ANELLI

SIA A UN INSIEME SU CUI SONO DEFINITE LE OPERAZIONI "+" E ":" A È UN

ANELLO CON UNITÀ 1_A SE:

- $(A, +)$ È UN GRUPPO ABELIANO
- (A, \cdot) È UN MONOIDE CON IDENTITÀ 1_A
- VALGONO LE PROPRIETÀ DISTRIBUTIVE: $\forall a_1, a_2, a_3 \in A$
 $(a_1 + a_2)a_3 = a_1a_3 + a_2a_3; a_3(a_1 + a_2) = a_3a_1 + a_3a_2$

DICIAMO CHE A È COMMUTATIVO SE IL MONOIDE (A, \circ) È COMMUTATIVO.

INDICHIAMO CON " θ " L'IDENTITÀ DEL GRUPPO $(X, +)$.

ESEMPI:

a) GLI INSIEMI $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ CON LE OPERAZIONI DI ADDIZIONE E

MOLTIPLICAZIONE SONO ANELLI COMMUTATIVI CON UNITÀ 1.

b) L'INSIEME DEUE MATERI $n \times n, n > 1$. A VALORI SU $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ O \mathbb{C} CON

L'OPERAZIONE DI SOMMA E PRODOTTO RIGHE PER COLONNE È UN ANELLO

NON COMMUTATIVO CON UNITÀ I_n . IN GENERALE, SE A È UN

ANELLO COMMUTATIVO CON UNITÀ, L'INSIEME $M_{n \times n}(A)$ DELLE MATERI

A VALORI IN \mathbb{R} CON LE OPERAZIONI DI SOMMA E PRODOTTO RIGHE PER

COLONNE, È UN ANELLO NON COMMUTATIVO CON UNITÀ.

c) $\emptyset \times \emptyset$ È L'ANELLO NULLO. LE DUE OPERAZIONI SONO LA STESSA E

$$0 = 1_{\emptyset \times \emptyset} = x.$$

CONSIDEREREMO SEMPRE CHE $0 \neq 1_A$ E I SOLI ANELLI COMMUTATIVI CON

DEFINIZIONE) SIA A UN ANELLO COMMUTATIVO. UN ELEMENTO $x \in A$ È

• ZERO-DIVISIONE SE $\exists y \in A \setminus \{0\} | xy = 0$

• INVERTIBILE SE È UN ELEMENTO INVERTIBILE DEL MONOIDE (A, \circ)

PROPOSIZIONE: SIA A UN ANELLO COMMUTATIVO. ALLORA L'INSIEME
DEGLI ELEMENTI INVERTIBILI È DISGIUNTO DAI INSIEME DEGLI ZERO-DIVISORI
DIM $\Rightarrow X$ NON È UNO ZERO-DIVISORE
SIANO $X, Y \in A$ | $X \neq 0$. X INVERTIBILE $\Rightarrow X^{-1} \cdot X = 1 \Rightarrow X^{-1} \cdot Y = Y$

DI A



LEGGE DI CANCELLAZIONE: SIA A UN ANELLO COMMUTATIVO E $x \in A$ UN
ELEMENTO CHE NON È UNO ZERO-DIVISORE. ALLORA $X \cdot Y = X \cdot Z \Rightarrow Y = Z$

$\forall Y, Z \in A$



DIM $X \cdot Y = X \cdot Z \Rightarrow X(Y - Z) = 0$. X NON È ZERO-DIVISORE $\Rightarrow Y - Z = 0 \Rightarrow Y = Z$

DEFINIZIONE) UN ANELLO COMMUTATIVO PRIVO DI ZERO-DIVISORI NON NULLI

È DETTO DOMINIO DI IDENTITÀ. INOLTRE, QUANDO GLI ELEMENTI NON NULLI
SONO INVERTIBILI SI PARLA DI CAMPO.

ESEMPI:

- L'ANELLO \mathbb{Z} È UN DOMINIO DI IDENTITÀ MA NON UN CAMPO
- GLI ANELLI $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ SONO CAMPI

IDEALI

SIA A UN ANELLO COMMUTATIVO. UN SOTTOINSIEME $I \subseteq A$ È

DETTO IDEALE SE:

- I È SOTTOGRUPPO DI $(A, +)$

- $\alpha x \in I \forall \alpha \in A, x \in I$

ESEMPIO 4b: ABBIAMO GIÀ VISTO CHE OGNI SOTOGRUPPO DI

$(\mathbb{Z}, +)$ È DEL TIPO $n\mathbb{Z} = \{kn \mid k \in \mathbb{Z}\}$ DOVE $n \in \mathbb{N}$. INOLTRE,

$$\alpha \in \mathbb{Z} \wedge x \in \mathbb{Z} \text{ (ossia } \exists k \in \mathbb{Z} \mid x = kn) \Rightarrow \alpha x = \alpha kn$$

$\Rightarrow n\mathbb{Z}$ È UN IDEALE DI \mathbb{Z} $\forall n \in \mathbb{N}$ E TUTTI GLI IDEALI DI \mathbb{Z} SONO DI

OSSERVAZIONI: SIANO $I, J \subseteq A$ IDEALI DI UN ANELLO COMMUTATIVO:

- $I \cap J$ È UN IDEALE DI A
- $I + J := \{x + y \mid x \in I \wedge y \in J\}$ È UN IDEALE DI A
- $IJ := \{x \cdot y \mid x \in I \wedge y \in J\}$ È UN IDEALE DI A

DEFINIZIONE) SIA $S \subseteq A$ UN SOTTOINSIEME DI UN ANELLO COMMUTATIVO. L'

IDEALE GENERATO DA S È L'INTERSEZIONE DI TUTTI GLI IDEALI DI A

CONTENENTI S ED È INDICATO CON $\langle S \rangle$. IN PARTICOLARE, $S = \{x\}$

$\Rightarrow \langle S \rangle$ È L'IDEALE PRINCIPALE GENERATO DA x DI A .

ESEMPIO: ABBIAMO VISTO CHE GLI IDEALI DI \mathbb{Z} SONO TUTTI E SOLI I

SOTTOINSIEMI $n\mathbb{Z} = \langle n \rangle$, $n \in \mathbb{N} \Rightarrow$ GLI IDEALI DI \mathbb{Z} SONO TUTTI PRINCIPALI

DEFINIZIONE) UN ANELLO I WI GLI IDEALI SONO TUTTI PRINCIPALI SI DICE

ANELLO AD IDEALI PRINCIPALI