SOTTOGRUPPI, OMOMORFISMI, ANELLI & CAMPI

Def: Sia G un gruppo e considero $H \subseteq G$.
Diciamo che H è **SOTTOGRUPPO** di G se:

0. $H \neq \emptyset$
1. $\forall x, y \in H \Rightarrow x \star y \in H$ ($\star$ é operazione su H)
2. $e \in H$
3. $\forall x \in H \Rightarrow x^{-1} \in H$

P.S. $\star$ associativa su $H \rightarrow$ associativa anche su G

Oss: Con queste condizioni H è gruppo

Def: Sia $(G, \star)$ e $(H, \square)$, due gruppi
Una funzione $f: G \rightarrow H$ è detta **OMOMORFISMO DI GRUPPI**
se $\forall a, b \in G$ $\underbrace{f(a \star b)}_{\in H} = \underbrace{f(a) \square f(b)}_{\in H}$

Def: Sono $(G, \star)$ e $(H, \square)$, 2 gruppi

Dico che $f: G \rightarrow H$ omomorfismo, è
ISOMORFISMO se f è <u>biiettiva</u>

In questo caso dico che $(G, \star)$ e $(H, \square)$
sono **ISOMORFI**.

→ Nei gruppi si possono definire le potenze

$a \in A$ $\quad a^{-1}$ é inverso di a

$a^0 := e$ $\quad$ (a^0 é neutro)

$$a^n := \underbrace{((a \star a) \star a) \star a \dots \star a}_{n \text{ volte}} \quad (\text{cioè } a^n = a^{n-1} \star a)$$

$$a^1 = a$$

$$a^{-n} := ((a^{-1} \star a^{-1}) \star a^{-1} \dots \star a^{-1}$$

Oss: Siano $n, m \in \mathbb{Z}$

- $a^n \star a^m = a^{n+m}$
- $(a^n)^m = a^{n \cdot m}$

Considero insieme A con 2 operazioni $+, \cdot$

$+ , A \times A \to A$, $\cdot , A \times A \to A$ sono funzioni

Def: Dico che $(A, +, \cdot)$ è ANELLO (unitario) se:

1. $(A, +)$ è gruppo abeliano
2. $(A, \cdot)$ è monoide
3. vale proprietà distributiva,

$\forall a, b, c \in A$

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c)$$
$$(a + b) \cdot c = (a \cdot c) + (b \cdot c)$$

es $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$ sono anelli

$(\mathbb{R}[x], +, \cdot)$ è anello

$\hookrightarrow$ {polinomi in x con coefficienti in $\mathbb{R}$} =

$= \{a_0 + a_1 x^1 + a_2 x^2 + a_d x^d, \ a_i \in \mathbb{R}\}$

$$(\mathbb{Q}, +, \cdot) \leadsto \begin{array}{l} (\mathbb{Q}, +) \text{ è gruppo} \\ (\mathbb{Q}/\{0\}, \cdot) \text{ è gruppo} \end{array}$$

<u>Notazione</u>: Se $(A, +, \cdot)$ è anello, indico:

- → con 0, e neutro di $+$
- → con 1, e neutro di $\cdot$
- → con $-a$, l'inverso di a rispetto $+$

Def: $(K, +, \cdot)$ è **CAMPO** se:

1. è anello
2. $(K - \{0\}, \cdot)$ è gruppo
3. $\cdot$ è commutativo

<u>Es</u> Sono campi $(\mathbb{Q}, +, \cdot)$ $(\mathbb{R}, +, \cdot)$ $(\mathbb{C}, +, \cdot)$
anelli ma no campi $(\mathbb{Z}, +, \cdot)$, $(\mathbb{R}[x], +, \cdot)$

Insieme Quoziente

sia A un insieme
sia R una relazione di equivalenza
(da adesso in poi $R = \sim$)

- riflessiva
- simm.
- transitiva

Def: Chiamo **CLASSE DI EQUIVALENZA** di $a \in A$
l'insieme $[a]_\sim := \{ b \in A \text{ t.c. } a \sim b \}$
$:= \{$ gli elementi in relazione con $a \}$

Teorema: Sia X un insieme, $\sim$ una relazione di equivalenza in X:

i) $\forall a \in X \quad a \in [a]_\sim$

ii) $a \sim b \iff [a]_\sim = [b]_\sim$

iii) $a \not\sim b \iff [a]_\sim \cap [b]_\sim = \emptyset$

dim i) $[a] = \{x \in X \mid a \sim x\}$

poiché $\sim$ è a di equivalenza

$\forall a \in X \quad a \sim a \Rightarrow a \in [a]$

dim ii) Mostro che $a \sim b \Rightarrow [a] = [b]$

cioè $[a] \subseteq [b]$ e $[b] \subseteq [a]$

so che $a \sim b$ mostro che $\forall x \in [a]$

si ha $x \in [b]$

$x \in [a] \Rightarrow a \sim x$ inoltre so che $a \sim b$

$\Rightarrow a \sim x$ e $b \sim a$

$b \sim a, \; a \sim x \underset{\text{TRANSITIVA}}{\Rightarrow} b \sim x \Rightarrow x \in [b]$

Si mostra analogamente $[b] \subseteq [a] \Rightarrow [a] = [b]$

dim ii) $\Leftarrow$ Mostro che $[a] = [b] \Rightarrow a \sim b$

$\underset{\text{punto i)}}{b \in [b]} = [a] \Rightarrow b \in [a] \Rightarrow a \sim b$

dim iii) $\Rightarrow a \not\sim b \Rightarrow [a] \cap [b] = \emptyset$

per assurdo $x \in [a] \cap [b] \Rightarrow$

$a \sim x, \; b \sim x \Rightarrow a \sim x, \; x \sim b \Rightarrow a \sim b$

dim iii) $\Leftarrow$ $[a] \cap [b] = \emptyset \Rightarrow a \nsim b$

per assurdo $a \sim b \Rightarrow b \in [a]$

$b \in [b]$

$\Rightarrow b \in [a] \cap [b]$

ASSURDO!!!

Dim: Sia X un insieme, una partizione di X è una collezione di sottoinsiemi di X, $\{A_i\}_i$

1. $A_i \cap A_j = \emptyset$ se $i \neq j$
2. $\bigcup A_i = X$
3. ($A_i \neq \emptyset$)

Teorema: Se X è insieme e $\sim$ è relazione di equivalenza

$\{[a], a \in X\} := \{[a]\}_{a \in X}$ → insieme delle classi di equivalenza di elem. in X

è partizione

infatti $[a] = A_i$ $A_j = [b]$ $i \neq j$ significa → $[a] \neq [b]$

$A_i = [a] \neq \emptyset$ (infatti $a \in [a]$ per i)

$A_i \cap A_j = \emptyset$ se $i \neq j$ diventa →

$[a] \cap [b] = \emptyset$ se $[a] \neq [b]$ cioè

se $a \nsim b$ (per ii)

$\Rightarrow$ per (iii) dice che $[a] \cap [b] = \emptyset$

$X = \bigcup A_i \quad A_i \subseteq X$ è ovvio che $\bigcup_i A_i = X$

Voglio dimostrare che $X \subseteq \bigcup A_i$:

- cioè $X \subseteq \bigcup [a]$

$\forall x \in X \quad x \in [x] \Rightarrow x \in$ all'unione delle classi di equivalenza

Def: Sia X un insieme, $\sim$ una relazione di equivalenza l'INSIEME QUOZIENTE di X rispetto a $\sim \rightarrow$

$$X/_\sim := \{ [a], \text{ al variare di } a \in X \}$$

è l'insieme delle classi di equivalenza di X rispetto a $\sim$

$$X = \mathbb{Z} \times \mathbb{Z} - \{0\}$$

$$(h, k) \sim (m, n) \iff hn = km$$

$\rightarrow$ è riflessiva $(h,k) \sim (h,k) \rightarrow hk = kh$

$\rightarrow$ è simmetrica $(h,k) \sim (m,n) \rightarrow hn = km \rightarrow mk = nh$

$\Rightarrow (m,n) \sim (h,k)$

$\rightarrow$ è transitiva $(h,k) \sim (m,n), (m,n) \sim (a,b)$

$\Rightarrow hn = km, \quad mb = na \Rightarrow m = \frac{hn}{k} \quad (k \neq 0)$

$\Rightarrow \frac{hnb}{k} = na \Rightarrow hb = ka$

$\Rightarrow (h,k) \sim (a,b)$

$$[(h,k)] = \{(n,d) \mid (h,k) \sim (n,d)\}$$
$$= \{(n,d) \mid hd = kn\}$$
$$= \{(n,d) \mid \frac{h}{k} = \frac{n}{d}\}$$

$\rightarrow \frac{n}{d}$ é FRAZIONE EQUIVALENTE a $\frac{h}{k}$

es $\frac{1}{2} = \frac{4}{8}$

$\Rightarrow X/_{\sim} = \mathbb{Q}$ l'insieme delle frazioni

L'INSIEME $\mathbb{Z}_n$ DELLE CLASSI DI RESTO DI MODULO n

Def: Considero l'insieme $\mathbb{Z}$, scelgo $n \in \mathbb{N}$ $n > 0$.
Definisco la relazione $\sim_n$:

$$x \sim_n y \iff \exists k \in \mathbb{Z} \mid x - y = kn$$

es $n = 3$

$1 \sim_3 -2$ (infatti $1-(-2) = 3$ $(k\ 1)$)

$1 \not\sim_3 2$ (infatti $1-2 = -1 \rightarrow$ non é multiplo di 3)

$27 \sim_3 81$ (infatti $27-81 = 3\cdot(-18)$)

Teorema: $\sim_n$ é relazione di equivalenza

dimostrazione: $\sim_n$ é riflessiva $x \sim_n x$
perché $x - x = 0 \cdot n$

$\sim_n$ é simmetrica infatti se
$x \sim_n y \Rightarrow x - y = kn \Rightarrow y - x = (-k)n \Rightarrow y \sim_n x$

$\sim_n$ é transitiva infatti $x \sim_n y$ $y \sim_n z$

$\Rightarrow x-y = kn$ e $y-z = hn$

$\Rightarrow x-z = x-y+y-z = kn+hn = (k+h)n$

$\Rightarrow x \sim_n z$