Lezione 3

Classi di equivalenza

sia $\sim$ una relazione di equivalenza in A, una classe di equivalenza sono tutti gli elem. in relazione con $a \in A$, ovvero:

$$[a]_{\sim} = [a] = \{b \in A : b \sim a\}$$

Partizioni

dato un insieme X, si definisce partizione una collezione di insiemi $X_i \subseteq X$ t.c.:

- $X_i \neq \emptyset$
- X_i partizione di X, $X_i \neq X_j \Rightarrow X_i \cap X_j = \emptyset$ ovvero le partizioni sono disgiunte
- $\bigcup_{i=0}^{\infty} X_i = X$

Insieme quoziente modulo $\sim$

l'insieme delle cl. di eq. $A/_{\sim} = \{[a]_{\sim} : a \in A\}$ è detto insieme quoziente di A modulo $\sim$

Congruenza modulo n

sia $A=\mathbb{Z}$ e $n \in \mathbb{Z}, n>0$

$a, b \in A$ si dicono congrui modulo n se $\exists h \in \mathbb{Z} : a-b = hn$

si scrive $a \sim b \pmod{n}$ o $a \underset{n}{\sim} b$ ($a-b$ è multiplo di n)

Teorema $\underset{n}{\sim}$ è rel. d'eq.

ipotesi: sia $\underset{n}{\sim}$ una congruenza modulo n

tesi: $\underset{n}{\sim}$ è una rel. d'equivalenza

Insieme classi di resto di modulo n

l'insieme quoziente di $\mathbb{Z}$ modulo $\underset{n}{\sim}$ viene chiamato insieme delle classi di resto di modulo n e denotato con $\mathbb{Z}_n$ o $\mathbb{Z}/n$

Teorema: addizione e moltiplicazione in $\mathbb{Z}$ sono compatibili con $\underset{n}{\sim}$

enunciato: $a \underset{n}{\sim} b, \; c \underset{n}{\sim} d \Rightarrow a+c \underset{n}{\sim} b+d, \; ac \underset{n}{\sim} bd$

Teorema: $\mathbb{Z}_n$ campo solo se n è primo

enunciato: $(\mathbb{Z}_n, +_n, \cdot_n)$ è un campo solo se n è primo

Teorema di partizione di un'insieme nelle classi di equivalenza

ipotesi: sia $\sim$ una rel. d'eq. in un insieme A

tesi

1) $[a] \neq \emptyset \quad \forall a \in A$

2) $[a] \neq [b] \Rightarrow [a] \cap [b] = \emptyset$

3) $A = \bigcup_{a \in A} [a]$

ovvero le classi di equivalenza di $\sim$ formano una partizione su A

dimostrazione

si devono quindi dimostrare queste tre:

1) $a \in [a]_\sim$

$\sim$ è riflessiva quindi $a \sim a$ quindi $a \in [a]$

2) $a \sim b \Leftrightarrow [a]_\sim = [b]_\sim$

$\Leftarrow$

se $[a] = [b]$, per la (1) $a \in [a] \Rightarrow a \in [b] \Rightarrow a \sim b$

$\Longrightarrow$

$a \sim b$, $\forall x \in [a]$ $x \sim a$ $\Rightarrow$ per transitività $x \sim b \Rightarrow x \in [b]$, $b \sim a \Rightarrow [a] \subseteq [b]$

3) $a \not\sim b \Leftrightarrow [a]_\sim \cap [b]_\sim = \emptyset$

$\Longrightarrow$

per assurdo $\exists x \in [a] \cap [b] \Rightarrow x \sim a$, $x \sim b \Rightarrow$ per simmetria $a \sim x$, $b \sim x$

$\Rightarrow$ per transitività $a \sim b \Rightarrow \perp$

$\Longleftarrow$

per assurdo $a \sim b \Rightarrow [a] = [b]$ da (2) e $[a] \neq \emptyset$ da (1) $\Rightarrow \perp$