Esercitazione 10-10-18

2.3.19

1) Per induzione su n, stabilire che se X e Y sono insiemi finiti con lo stesso numero n di elementi, e $f: X \to Y$ è una funzione iniettiva, allora f è surgettiva.

Passo base $n=1$ $\#X = \#Y = 1$ $X = \{x\}$, $Y = \{y\}$

$f: X \to Y$

$f(x) = y$ - l'unica funzione da X in Y. f è surgettiva e iniettiva ok.

Passo induttivo: Supponiamo che $\# X = \# Y = n+1$.

$f : X \to Y$ iniettiva.

Scegliamo $x \in X$, $f(x) \overset{"}{\in} Y$. $\quad y$

Consideriamo $f|_{X \setminus \{x\}} : X \setminus \{x\} \to Y$ $\rightsquigarrow$ restrizione di f a $X \setminus \{x\}$.

$\# (X \setminus \{x\}) = n$

- Notiamo che, per iniettività di f, che $\mathrm{Im}(f|_{X \setminus \{x\}}) \subseteq$
$= Y \setminus \{f(x)\} = Y \setminus \{y\}$.

Notiamo che $\underset{\in Y}{f(x)} \notin \mathrm{Im}\left(f|_{X\setminus\{x\}}\right)$

Supponiamo per assurdo che $\exists\ x' \in X\setminus\{x\}$ tale che $f(x') = y$. Allora $f(x) = f(x') = y$. Assurdo poiché f è iniettiva.

Consideriamo $f|_{X\setminus\{x\}} : X\setminus\{x\} \longrightarrow Y\setminus\{f(x)\}$

$\#(X\setminus\{x\}) = n$, $\#(Y\setminus\{f(x)\}) = n$ + $f|_{X\setminus\{x\}}$ è iniettiva

Applichiamo l'ipotesi induttiva e otteniamo che $f|_{X \setminus \{x\}} : X \setminus \{x\} \to Y \setminus \{f(x)\}$ è surgettiva

$\mathrm{Im}(f|_{X \setminus \{x\}}) = Y \setminus \{f(x)\}$. Da ciò segue

che $\mathrm{Im}(f) = (Y \setminus \{f(x)\}) \cup \{f(x)\} = Y \Rightarrow f$ surgettiva

2) Usando il fatto precedente, stabilire che se X e Y hanno lo stesso numero finito di elementi e $f: X \to Y$

è surgettiva, allora f è anche iniettiva.

- $\# X = \# Y = n$,

$f : X \to Y$ surgettiva.

$\forall\, y \in Y \;\exists\, x \in X$ t.c. $f(x) = y$.

Definiamo $g : Y \to X$ → possiamo farlo per surgettività di $f : X \to Y$

$y \mapsto x$ tale che $f(x) = y$.

Osserviamo che g così definita è un'inversa destra di f, ossia $f \circ g : Y \to Y$ è l'identità.

$$Y \ni y \xrightarrow{g} x \xrightarrow{f} y.$$
$$\qquad\qquad x \in f^{-1}(\{y\})$$

Inoltre verifichiamo che g così definita è iniettiva.

Siano $y_1, y_2 \in Y$ tali che $g(y_1) = g(y_2) = x \in X$.

$$\underset{\substack{\parallel \\ f(x)}}{f \circ g(y_1)} = \underset{\substack{\parallel \\ f(x)}}{f \circ g(y_2)} = y \Rightarrow y_1 = y_2 \Rightarrow g \text{ è iniettiva}$$

Applicando 1) verifichiamo che g è surgettiva.

Concludiamo che f è una funzione iniettiva, nel modo seguente:

Supponiamo $x_1, x_2 \in X$ tali che $f(x_1) = f(x_2) = y \in Y$.

Poiché g è surgettiva, $\exists\, y_1, y_2 \in Y$ tali che $g(y_1) = x_1$, $g(y_2) = x_2$.

Poiché $f \circ g = id_Y$ $\Rightarrow$

$$y_1 = f \circ g(y_1) = y$$
$$y_2 = f \circ g(y_2) = y$$

Concludiamo che $x_1 = g(y) = x_2$, quindi f è iniettiva

3) Dedurre che se X è finito e $f: X \to X$ è una funzione, allora f è iniettiva $\Leftrightarrow$ f è surgettiva.
(Applicare i punti 1) e 2) con $Y = X$.

Es: 2.3.20: Dato $n \in \mathbb{N}$, $n \geq 3$, sia $F_n = \{0, 1, \dots, n-1\}$. Considerare le operazioni $\oplus$ e $\odot$ definite come segue:

$a \oplus b$ è il resto della divisione euclidea $a + b : n$

$a \odot b$ è il resto della divisione euclidea $(a \cdot b) : n$

↳ operazioni nuove ↳ operazioni "vecchie"

Dimostrare che F_n con tali operazioni e' un campo $\Leftrightarrow$ n e' primo.

Dimostrazione: Verificare che valgono tutte le proprietà di campo tranne la (6) (esistenza dell'inverso moltiplicativo per elementi non nulli).

- n non e' primo $\Rightarrow$ non vale (6)

n non primo $\Rightarrow \exists\, a, b \in F_n,\ a, b \neq 0$ tali che $a \cdot b = n$

Osserviamo che a e' non nullo ma non ammette inverso

Se per assurdo $\exists\, c \in F_n$ tale che $a \odot c = 1$, avremmo:

$$b = b \odot 1 = b \odot (a \odot c) = (b \odot a) \cdot c = (\underbrace{a \odot b}_{= 0 \text{ in } F_n}) \odot c = \underset{\substack{\shortparallel \\ 0}}{0 \odot c}$$

Poichè $a \cdot b = n$ Assurdo poichè $b \neq 0$ in F_n.

- n primo $\Rightarrow \forall a \in F_n$ non nullo ammette inverso $\odot$

Sia $\underset{\substack{\shortparallel \\ 0}}{a} \in F_n$, definiamo $\varphi_a : F_n \to F_n$, come

$\varphi_a(b) \overset{\circ}{=} a \odot b$

- 1) Dimostrare che φ_a è iniettiva (segue dalla definizione di φ_a e dell'operazione $\odot$).

2) Applichiamo l'esercizio precedente

concludiamo che $\forall a \in F_n$, $\varphi_a : F_n \to F_n$ è surgettiva

(poiché $\# F_n = n \in \mathbb{N}$)

Concludiamo infine che, poiché φ_a è surgettiva,

$1 \in \operatorname{Im} \varphi_a$, cioè $\exists\, b \in F_n$ tale che $\varphi_a(b) = 1$

$$\varphi_a(b) = a \odot b$$

$\Rightarrow$ concludiamo che b

è l'inverso moltiplicativo di a.