14/09/18

1. F INIETTIVE DA [5] A [8]

1° → 8 OPZIONI

2° → 7 OPZIONI

3 6

4 5

5 4

⇒ IN TOTALE # : 8·7·6·5·4

IN GENERALE F INIETTIVE DA [h] A [K]

1° → K OPZIONI

2° → K-1 OPZIONI

$K \cdot (K-1) \cdot (K-2) \cdot \ldots \cdot (K-(h-1)) = \frac{K!}{(K-h)!}$

h K-(h-1) OPZIONI

QUINDI IN TOTALE # : $\begin{cases} 0 & \text{se } h > K \\ \frac{K!}{(K-h)!} & \text{se } h \leq K \end{cases}$

2.

$G \neq \{1_G\}$ e G non ha sottogruppi diversi da $\{1_G\}$ e G.

Sia $g \in G$ $g \neq 1_G$, considero $\langle g \rangle$, lui è sottogruppo di G $\Rightarrow \langle g \rangle = \{1_G\}$ o $\langle g \rangle = G$, ma la prima evidentemente non è

⇒ G è ciclico.

G è ciclico quindi se fosse infinito sarebbe isomorfo a $\mathbb{Z}$. Ma $\mathbb{Z}$ ha sottogruppi non propri, ad esempio $2\mathbb{Z}$

⇒ G è finito.

G è ciclico finito, quindi $\exists n \geq 2$ t.c. $G \cong \mathbb{Z}_n$. Se n non fosse primo $\exists d \mid n$ t.c. $n = dk$ con $k \neq 1, n$

e dato $g \in G$ generatore si avrebbe $\langle g^d \rangle \leq G$ di ordine $k \neq 1, n$ cioè $\langle g^d \rangle \neq \{1_G\}, G$ assurdo

⇒ n è primo

3.

- Sia D dominio d'integrità finito. Sia $a \in D$ $a \neq 0$ considero $A = \{a^n \mid n \in \mathbb{N}\}$, $A \subseteq D$ perché è chiuso per moltiplicazione. Ma D è finito, quindi $\exists n, m \in \mathbb{N}$ t.c. $a^n = a^m$ $n \neq m$, diciamo $n > m$.
Sono in un dominio d'integrità, per cui è lecita la cancellazione, ottengo $a^{n-m} = 1$.
Definisco $b = a^{n-m-1}$ (si osserva che $n-(m+1) \geq 0$ per cui la definizione ha senso).
⇒ b è l'inverso di a, quindi D è un campo
- Consideriamo $\mathbb{Z}_n$, vogliamo mostrare che $\mathbb{Z}_n$ è campo $\Leftrightarrow$ n è primo.
$\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ e un quoziente è un campo $\Leftrightarrow$ l'ideale rispetto cui si quoziente è massimale.
Cioè $\mathbb{Z}_n$ campo $\Leftrightarrow$ $n\mathbb{Z}$ ideale massimale di $\mathbb{Z}$, ma in $\mathbb{Z}$ gli ideali massimali e primi coincidono e coincidono a loro volta con gli ideali generati nella forma $p\mathbb{Z}$ con p primo. Quindi $n\mathbb{Z}$ ideale massimale di $\mathbb{Z}$ $\Leftrightarrow$ n primo, che è la tesi.

OSSERVAZIONE:

Se vogliamo, una dimostrazione del fatto che in $\mathbb{Z}$ ideali primi e massimali coincidono può essere fatta usando il primo punto dell'esercizio: sia $n\mathbb{Z}$ ideale primo di $\mathbb{Z}$, allora $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n$ è un dominio d'integrità, ma è finito, allora, usando il primo punto risulta essere un campo, quindi $n\mathbb{Z}$ è massimale (massimale $\Rightarrow$ primo vale sempre).

• Come osservato se $\mathbb{Z}_n$ è un campo $n\mathbb{Z}$ è ideale primo e massimale di $\mathbb{Z}$.

4. Vista varie volte.

24/09/18

1. $F: A \longrightarrow B$

a) Th: F SURIETTIVA $\iff \forall B' \subseteq B \quad B' = F(F^{-1}(B'))$

($\Rightarrow$)

Sia F SURIETTIVA e $B' \subseteq B$ la tesi diventa $B' = F(F^{-1}(B'))$

"$\subseteq$"

Sia $y \in B'$, per suriettività $\exists x \in A$ t.c. $F(x) = y$ e, per definizione $x \in F^{-1}(B')$, dunque $y = F(x) \in F(F^{-1}(B'))$.

"$\supseteq$"

Sia $y \in F(F^{-1}(B'))$, quindi $\exists x \in F^{-1}(B')$ t.c. $y = F(x)$, ma allora per definizione di $F^{-1}(B')$ $y \in B'$. (vale anche per F non suriett)

($\Leftarrow$)

Supponiamo che $\forall B' \subseteq B \quad B' = F(F^{-1}(B'))$

Sia $b \in B$, considero $B' = \{b\} \Rightarrow \{b\} = F(F^{-1}(\{b\}))$, se $F^{-1}(\{b\})$ fosse vuoto avrei $\{b\} = F(\emptyset)$ che non è ammissibile, quindi $F^{-1}(\{b\})$ è non vuoto ossia b ha almeno una preimmagine.

b)

$F^*: \mathcal{P}(B) \longrightarrow \mathcal{P}(A)$

$B' \longmapsto F^{-1}(B')$

Th: F SURIETTIVA $\iff$ F^* INIETTIVA

($\Rightarrow$)

Sia F SURIETTIVA, siano $B_1', B_2' \in \mathcal{P}(B)$ t.c. $F^*(B_1') = F^*(B_2')$ ossia $F^{-1}(B_1') = F^{-1}(B_2')$

Per quanto visto al punto a) essendo F suriettiva $B_1' = F(F^{-1}(B_1'))$ e $B_2' = F(F^{-1}(B_2'))$, ma coincidendo gli argomenti devono farlo anche le immagini $\Rightarrow B_1' = B_2'$, ossia F^* è iniettiva.

($\Leftarrow$)

Sia F^* INIETTIVA, la tesi diventa (usando il punto a)) ~~e sul fatto che l'inclusione "$\supseteq$" è sempre valida~~

Th: $\forall B' \subseteq B \quad B' = F(F^{-1}(B'))$

Denoto con $B_1' := B'$ e $B_2' = F(F^{-1}(B'))$., considero $F^*(B_2')$, voglio mostrare che $F^*(B_2') = F^*(B_1')$,

~~$F(B_2') = F^*(F(F^{-1}(B')))$~~

cioè $F^*(F(F^{-1}(B'))) = F^*(B')$ cioè $F^{-1}(F(F^{-1}(B'))) = F^{-1}(B')$

"$\subseteq$"

Sia $x \in F^{-1}(F(F^{-1}(B'))) \Rightarrow F(x) \in F(F^{-1}(B')) \Rightarrow \exists x' \in F^{-1}(B')$ t.c. $F(x') = F(x)$, ma per def di $F^{-1}(B')$ $x' \in F^{-1}(B')$

~~questo~~ implica $F(x') \in B'$ e quindi $F(x) \in B'$ e quindi $x \in F^{-1}(B')$

"$\supseteq$"

Sia $x \in F^{-1}(B') \Rightarrow F(x) \in F(F^{-1}(B'))$ ma per def $F^{-1}(F(F^{-1}(B')))$ allora $x \in F^{-1}(F(F^{-1}(B')))$.

Quindi ho dimostrato che $F^*(B_1') = F^*(B_2')$, ma F^* è iniettiva quindi $B_1' = B_2'$ ossia $B' = F(F^{-1}(B'))$

2.

a) $G \cong \mathbb{Z}_n$, $H \cong \mathbb{Z}_m$

$|G \times H| = n \cdot m$ perciò $G \times H$ è ciclico $\iff$ è isomorfo a $\mathbb{Z}_{n \cdot m}$.

Per il teorema cinese dei resti $\mathbb{Z}_n \times \mathbb{Z}_m \cong \mathbb{Z}_{nm} \iff (n,m) = 1$. Dunque

$\Rightarrow$ $G \times H$ è ciclico $\iff$ $(n,m) = 1$

b) $\mathbb{Z} \times \mathbb{Z}$ non è ciclico, infatti: supponiamo per assurdo lo sia, $\exists (a,b) \in \mathbb{Z} \times \mathbb{Z}$ t.c. $\forall (x,y) \in \mathbb{Z} \times \mathbb{Z}$ $\exists \kappa \in \mathbb{Z}$ t.c. $\kappa(a,b) = (x,y)$. In particolare $\exists \kappa_1, \kappa_2 \in \mathbb{Z}$ t.c.

$$\begin{cases} \kappa_1(a,b) = (1,0) \\ \kappa_2(a,b) = (0,1) \end{cases} \Rightarrow \begin{cases} \kappa_1 a = 1 \\ \kappa_1 b = 0 \\ \kappa_2 a = 0 \\ \kappa_2 b = 1 \end{cases}$$

Per non contraddire la $(\kappa_1 a = 1)$ $\kappa_1 \neq 0$ ma allora per la $(\kappa_1 b = 0)$ $b = 0$.
Analogamente dalle altre due otteniamo $a = 0$. Quindi il generatore di $\mathbb{Z} \times \mathbb{Z}$ è $(0,0)$, assurdo.

ALTERNATIVA:
Se $\mathbb{Z} \times \mathbb{Z}$ fosse ciclico, essendo infinito, dovrebbe essere isomorfo a $\mathbb{Z}$. $\mathbb{Z}$ è un dominio di integrità, infatti $\mathbb{Z} \times \mathbb{Z}$ non lo è, ad esempio $(1,0)$ e $(0,1)$ sono divisori dello zero.

3.

Introduco una notazione: $\forall$ se I è ideale di A $\mathrm{Int}(A, I) = \{J \text{ ideale di } A \mid I \subseteq J\}$.

Con questa notazione $\mathcal{J}(A/I) = \{J/I \mid J \in \mathrm{Int}(A, I)\}$. Si ottiene

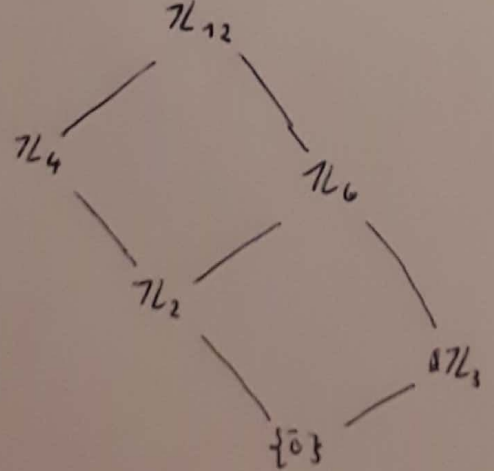
I massimale $\iff \mathrm{Int}(A, I) = \{A, I\} \iff \mathcal{J}(A/I) = \{A/I, I/I\} \iff A/I$ è un campo

4.

a) I sottogruppi di $\mathbb{Z}_{12} = \langle \bar{1} \rangle$ sono i generati da $d \cdot \bar{1}$ al variare di $d \mid 12$, quindi

$\langle \bar{1} \rangle = \mathbb{Z}_{12}$ $\langle \bar{2} \rangle \cong \mathbb{Z}_6$ $\langle \bar{3} \rangle \cong \mathbb{Z}_4$ $\langle \bar{4} \rangle \cong \mathbb{Z}_3$ $\langle \bar{6} \rangle \cong \mathbb{Z}_2$ $\langle \bar{0} \rangle = \{\bar{0}\}$ nel gruppo

Nel grafo opero un leggero abuso e $\mathbb{Z}_n$ denoto con gli $\mathbb{Z}_n$.



b) $7L_{12}$ è il massimo di H e $\{\bar{0}\}$ il minimo.

Ovviamente l'unico complemento di $7L_{12}$ è $\{\bar{0}\}$ e l'unico di $\{\bar{0}\}$ è $7L_{12}$.

$7L_4$ ha come unico complemento $7L_3$

$7L_3$ ha come unico complemento $7L_4$

$7L_2$ e $7L_6$ non hanno complementi

d) Il reticolo non è di Boole perché non tutti gli elementi hanno un complemento

c) Il reticolo è distributivo perché non contiene nessun sottoreticolo isomorfo a M_3 o N_5