Algebra 1

Proff. A. De Sole, P. Piazza e E. Spinelli

Primo Esonero

23 Aprile 2012

Nome e Cognome: ____________________

Numero di Matricola: ____________________

Esercizio	Punti totali	Punteggio
1	6	
2	6	
3	6	
4	6	
5	6	
Totale	30	

Giustificate le risposte!

Esercizio 1. Si determini la cardinalità dei seguenti insiemi:

(i) $A = \{(x, y) \in \mathbb{R}^2 \mid x - y \in \mathbb{Q}\}$

(ii) $S = (\mathbb{N} \setminus \{0\})/\sim$, dove $\sim$ è la seguente relazione d'equivalenza: $a \sim b$ se e solo se a e b hanno lo stesso resto quando divisi per 17.

(iii) $B = \{(x, y) \in \mathbb{R} \times \mathbb{Q}|$ esistono a, b razionali e non entrambi nulli tali che $ax + by \in \mathbb{Q}\}$.

(iv) $C = \{(x, y) \in \mathbb{C} \times \mathbb{Q}|$ esistono a, b razionali con $a \neq 0$ tali che $ax + by \in \mathbb{Q}\}$.

(v) $M =$ insieme delle matrici quadrate a coefficienti interi di ordine (finito) qualunque.

Soluzione: (i) $A \subseteq \mathbb{R}^2$, quindi $\text{Card}(A) \leq \text{Card}(\mathbb{R}^2) = \text{Card}(\mathbb{R})$. Ora, per ogni $a \in \mathbb{R}$, $(a, a) \in A$, quindi ha senso considerare la funzione $f : \mathbb{R} \to A$, $a \mapsto (a, a)$. Essa è iniettiva e pertanto $\text{card}(\mathbb{R}) \leq \text{Card}(A)$. Concludiamo allora che A ha la potenza del continuo.

(ii) Osserviamo che $a \sim b$ se, e solo se, $a \equiv_{17} b$. Quindi $\text{Card}(S) = 17$.

(iii) Verifichiamo che $B = \mathbb{R} \times \mathbb{Q}$. Ovviamente $B \subseteq \mathbb{R} \times \mathbb{Q}$. Sia ora $(r, q) \in \mathbb{R} \times \mathbb{Q}$. Poniamo $a := 0$ e $b := 1$. Allora $ar + bq = q \in \mathbb{Q}$ e quindi $(r, q) \in B$.
Pertanto B ha la potenza del continuo.

(iv) Verifichiamo che $C = \mathbb{Q} \times \mathbb{Q}$. Ovviamente $\mathbb{Q} \times \mathbb{Q} \subseteq C$. Supponiamo, se possibile, che $C \nsubseteq \mathbb{Q} \times \mathbb{Q}$. Allora esistono $r \in \mathbb{C} \setminus \mathbb{Q}$ e $q \in \mathbb{Q}$ e $a, b \in \mathbb{Q}$ con $a \neq 0$ tali che $ar + bq \in \mathbb{Q}$. Da questo segue che $r \in \mathbb{Q}$, il che è falso.
Pertanto C ha la potenza del numerabile.

(v) $M = \cup_{n \in \mathbb{N}_+} M_n(\mathbb{Z})$. Ora, per ogni intero n, $M_n(\mathbb{Z})$ è equipotente a $\mathbb{Z}^{n^2}$, che è numerabile. Poichè l'unione di una infinità numerabile di insiemi numerabili è numerabile, ne segue che M è numerabile.

Risposta:

(i) $\text{Card}(A) = \boxed{}$ (ii) $\text{Card}(S) = \boxed{}$ (iii) $\text{Card}(B) = \boxed{}$

(iv) $\text{Card}(C) = \boxed{}$ (v) $\text{Card}(M) = \boxed{}$

Esercizio 2. (a) Enunciare il Piccolo Teorema di Fermat.

(b) Dimostrare che per ogni $n \in \mathbb{N}$ il numero $n^{55} + 2n^{50} + 3n^{45} + 4n^3 + 5n^2 + 6n$ è divisibile per 7.

Soluzione: (b) Sia $n \in \mathbb{N}$. Se $7 \mid n$ il risultato è ovvio.
Assumiamo pertanto che $7 \not| n$. Poichè $\mathrm{mcd}(7, n) = 1$, per il Piccolo Teorema di Fermat $n^6 \equiv_7 1$. Questo implica che, per ogni $k \in \mathbb{N}$, $n^{6k} \equiv_7 1$. Allora

$$n^{55} + 2n^{50} + 3n^{45} + 4n^3 + 5n^2 + 6n \equiv_7 n + 2n^2 + 3n^3 + 4n^3 + 5n^2 + 6n \equiv_7 7(n^3 + n^2 + n) \equiv_7 0.$$

Risposta:

(a)	Piccolo Teorema di Fermat:	
(b)	Dimostrazione (in breve):	

Esercizio 3. Si determini per quali valori del parametro $k \in \mathbb{Z}$ il seguente sistema di equazioni alle congruenze ammette soluzioni (NON è necessario determinare le soluzioni):

$$\begin{cases} 6x \equiv 8 \mod (10)\,, \\ 9x \equiv 15 \mod (21)\,, \\ 2x \equiv k \mod (6)\,. \end{cases}$$

Soluzione: Il sistema dato è equivalente a

$$\begin{cases} 3x \equiv 4 \mod (5)\,, \\ 3x \equiv 5 \mod (7)\,, \\ 2x \equiv k \mod (6)\,. \end{cases}$$

Poichè $5, 7$ e 6 sono a due a due coprimi, il sistema ha soluzione se tutte le equazioni che lo compongono hanno soluzione. Le prime due hanno soluzione (essendo $\mathrm{mcd}(3, 5) = \mathrm{mcd}(3, 5) = 1$). L'ultima equazione ha soluzione se, e solo se, $\mathrm{mcd}(6, 2) \mid k$. Concludiamo allora che il sistema ha soluzione per k pari.

Risposta:

$k =$ $\boxed{}$

Esercizio 4. Si considerino i seguenti insiemi $X = \{1, 2, 3, 4\}$ e $Y = \{3, 4\} \subset X$. Sia $\mathbb{Z}^X$ l'insieme di tutte le funzioni $f : X \to \mathbb{Z}$, e si consideri la seguente relazione su di esso:

$$f \rho g \text{ se e solo se } f(y) = g(y) \, \forall y \in Y \, .$$

(a) Verificare che ρ è una relazione d'equivalenza.

(b) Determinare una biezione fra l'insieme quoziente $(\mathbb{Z}^X)/\rho$ e l'insieme $\mathbb{Z}^Y$.

Soluzione: Consideriamo la funzione

$$F : \mathbb{Z}^X \longrightarrow \mathbb{Z}^Y, \qquad g \longmapsto F(g) := g|_Y \, .$$

Verifichiamo che F è suriettiva: Data $g \in \mathbb{Z}^Y$, sia $h_g \in \mathbb{Z}^X$ (cioè $h_g : X \to \mathbb{Z}$) tale che $h_g(y) := g(y)$ per ogni $y \in Y$ e $h_g(y) := 0$ altrimenti. Allora $F(h_g) = g$.

Detta σ_F la relazione di equivalenza canonicamente associata a F, dimostriamo che $\rho = \sigma_F$: questo è sufficiente per dimostrare (a) (essendo uguale a σ_F la relazione ρ è di equivalenza) e (per il teorema fondamentale delle applicazioni) quasi sufficiente per determinare una biezione fra $(\mathbb{Z}^X)/\rho$ e $\mathbb{Z}^Y$, come richiesto in (b).
Si ha

$$f \sigma_F g \text{ se e solo se } F(f) = F(g) \text{ se e solo se } f|_Y = g|_Y \text{ se e solo se } f(y) = g(y) \, \forall y \in Y \text{ se e solo se } f \rho g \, .$$

Una biezione come richiesto in (b) è allora l'applicazione

$$\tilde{F} : (\mathbb{Z}^X)/\rho = (\mathbb{Z}^X)/\sigma_F \xrightarrow{\sim} \mathbb{Z}^Y$$

che a $[g]_\rho = [g]_{\sigma_F}$ associa $\tilde{F}([g]_\rho) = \tilde{F}([g]_{\sigma_F}) := F(g) = g|_Y$.

Risposta:

(a)	Dimostrazione (in breve):	
(b)	Dimostrazione (in breve):	

Esercizio 5. Consideriamo l'insieme

$$A := \{a + bi \mid a, b \in \mathbb{Z}\} \subset \mathbb{C}\,.$$

Tale sottoinsieme è un sottoanello unitario di $\mathbb{C}$ (non dovete dimostrarlo). Dato un intero fissato $t \in \mathbb{Z}$, sia $f_t : A \to \mathbb{Z}_5$ la funzione così definita:

$$f_t(a + bi) = [a + bt]_5\,.$$

(i) verificare che f_2 è un omomorfismo di anelli.

(ii) determinare i valori di $t \in \mathbb{Z}$ per i quali f_t è un omomorfismo di anelli.

Soluzione: (i) Siano $a + ib, c + id \in A$.

$$f_2(a + ib + c + id) = f_2((a + c) + i(b + d)) = [a + c + 2(b + d)]_5 = \\ [a + 2b]_5 \widehat{+} [c + 2d]_5 = f_2(a + ib) \widehat{+} f_2(c + id).$$

$$f_2((a + ib)(c + id)) = f_2((ac - bd) + i(bc + ad)) = [ac - bd + 2(bc + ad)]_5 = \\ [a + 2b]_5 \widehat{\cdot} [c + 2d]_5 = f_2(a + ib) \widehat{\cdot} f_2(c + id).$$

(ii) Siano $a + ib, c + id \in A$ e $t \in \mathbb{Z}$. Poichè f_t è sempre un omomorfismo rispetto alle operazioni di somma, bisogna guardare all'aspetto moltiplicativo degli anelli. Ora

$$f_t((a + ib)(c + id)) = [ac - bd + t(bc + ad)]_5,$$

mentre

$$[a + tb]_5 \widehat{\cdot} [c + td]_5 = [ac + t^2 bd + t(bc + ad)]_5.$$

Affinchè f_t sia un omomorfismo deve accadere che $[ac - bd + t(bc + ad)]_5 = [ac + t^2 bd + t(bc + ad)]_5$, ovvero che $t^2 bd \equiv_5 -bd$, cioè $t^2 + 1 \equiv_5 0$. Questo avviene quando $t \in [2]_5 \cup [3]_5$.

Risposta:

(ii) f_t è omomorfismo se e solo se $t =$ $\boxed{}$