$\boxed{\star}$ MATRICOLA: .... A ... B ... C ... D ... VOTO$^{\geq 10}$: ......

NOME: .... COGNOME: ....

Algebra 1 – Esame 17.09.14

Rispondere alle domande su questo foglio usando gli appositi spazi e giustificando brevemente ma esaurientemente tutte le risposte.

A Sia S un insieme e sia $\mathcal{P}(S)$ l'insieme delle parti di S. Per ogni $X \subseteq S$ definiamo una funzione $f_X : \mathcal{P}(S) \to \mathcal{P}(S)$ con $A \mapsto X \setminus A$. Consideriamo anche la funzione $g : \mathcal{P}(S) \to \mathcal{P}(S)^{\mathcal{P}(S)}$ definita da $X \mapsto f_X$.

1. Per quali X la funzione f_X è bigettiva? [S] $\boxed{2}$

Sia $X \subsetneq S$, e sia $a \in S \setminus X$. Si ha $f_X(X) = \emptyset = f_X(X \cup \{a\})$, pertanto f_X non e' iniettiva. Invece f_S associa ad ogni $A \in \mathcal{P}(S)$ il suo complementare in S, ed e' quindi biettiva.

2. Esistono degli S finiti tali che la funzione g è bigettiva? Se sì, quali? [$\emptyset$] $\boxed{2}$

Sia $A \subseteq S$ con $A \neq \emptyset$. Per ogni $X \in \mathcal{P}(S)$ si ha ovviamente $f_X(A) \neq A$, dunque $f_X \neq id_{\mathcal{P}(S)}$. Segue che, se $S \neq \emptyset$, la funzione g non e' suriettiva, poiché $id_{\mathcal{P}(S)} \notin g(\mathcal{P}(S))$. Se invece $S = \emptyset$, si ha che g e' ovviamente biettiva.

3. Esistono degli S infiniti tali che la funzione g è bigettiva? Se sì, quali? [No] $\boxed{2}$

L'argomento di sopra mostra che g non e' mai suriettiva se $S \neq \emptyset$, dunque in particolare se S e' infinito.

B Sia G un gruppo e siano $x, y \in G$ tali che $xy = yx$.

1. Dimostrare che per ogni n intero (non solo naturale) abbiamo $x^n y = y x^n$. $\boxed{1}$

Induzione su $n \in \mathbb{N}$: per $n = 0$, si ha $x^n y = y = y x^n$. Supponiamo dunque che sia vero per $n-1$ ($n \geq 1$): si ha $x^n y = x^{n-1}(xy) = (x^{n-1} y) x = y(x^{n-1} x) = y x^n$. Nel caso $n < 0$: $x^n y = (x^{-1})^{-n} y = y (x^{-1})^{-n} = y x^n$ (oss: $x^{-1} y \cancel{x} = x^{-1} x y = y = y x^{-1} \cancel{x}$, dunque x^{-1} commuta con y)

2. Dimostrare che per ogni n e per ogni m interi abbiamo $x^n y^m = y^m x^n$. $\boxed{2}$

Per il punto precedente, si ha $y^m x = x y^m$, dunque x commuta con y^m. Ancora per il punto precedente si ha allora $x^n y^m = y^m x^n$.

C Nell'anello $\mathbb{Z}[i]$ degli interi di Gauss, si consideri l'ideale $H = (2i, 6 + 4i)$.

1. H è principale? Se sì indicarne un generatore. [2] 2

$\mathbb{Z}[i]$ è un dominio euclideo, dunque un PID, dunque H è senz'altro principale. Si vede infatti che $6+4i = 2i(2-3i)$, dunque $2i \mid 6+4i$ e $H = (2i) = (2)$

2. H è massimale? [No] 2

H è generato da un elemento non irriducibile: $2 = (1+i)(1-i)$, pertanto si ha $H \subsetneq (1+i) \subsetneq \mathbb{Z}[i]$.

3. H è primo? [No] 2

In un PID, ogni ideale primo è massimale...

D Fattorizzare in $\mathbb{Z}_7[x]$ il polinomio $x^4 + x^2 + 1$. 3

Si vede che $2, 3$ sono radici di x^4+x^2+1 in $\mathbb{Z}_7$ (dunque lo sono anche $-2, -3$). Pertanto $x^4+x^2+1 = (x-2)(x+2)(x-3)(x+3)$.