⊕ Matricola: ..... A B C D$^{\geq 7}$: .....1 2 3 4$^{\geq 8}$: ..... Voto: .....

Nome: ..... Cognome: .....

Algebra 1 – Esame 19.04.12

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

A Sia U un insieme non vuoto. Siano S, T e V sottoinsiemi di U.

1. È vero che $(S \setminus T) \setminus V = S \setminus (T \setminus V)$? [No] | 1 |

   Vedi punto 3...

2. È vero che $(S \setminus T) \setminus V = S \setminus (T \setminus V)$ se S e V sono disgiunti ? [Sì] | 2 |

   Si ha $(S \setminus T) \setminus V = (S \cap \complement(T)) \cap \complement(V) = (S \cap \complement(V)) \cap \complement(T) = S \cap \complement(T)$, visto che $S \subseteq \complement(V)$. D'altra parte, $S \setminus (T \setminus V) = S \cap \complement(T \cap \complement(V)) = S \cap (\complement(T) \cup V) = (S \cap \complement(T)) \cup (S \cap V) = S \cap \complement(T)$, visto che $S \cap V = \emptyset$. Dunque, i due membri sono uguali.

3. È vero che $(S \setminus T) \setminus V = S \setminus (T \setminus V)$ se S e T sono disgiunti ? [No] | 2 |

   Si prendano S e V uguali e non vuoti...

B Sia $\mathbb{Q}^+$ l'insieme dei numeri razionali non negativi e $f : \mathbb{N} \to \mathbb{Q}^+$ la funzione $f(n) = \dfrac{n}{n+1}$

1. f iniettiva ? [Sì] | 2 |

   Siano $n, m \in \mathbb{N}$ tali che $f(n) = f(m)$, ovvero $\dfrac{n}{n+1} = \dfrac{m}{m+1}$. Se $0 \in \{n, m\}$ è evidente che si ha $n = m = 0$, dunque possiamo supporre n, m entrambi positivi. Si ha $n(m+1) = (n+1)m$, da cui $n \mid m$ (visto che n ed $n+1$ sono coprimi) e $m \mid n$ (visto che m e $m+1$ sono coprimi); concludiamo che è $m = \pm n$, ma essendo n ed m entrambi positivi, deve essere $n = m$. (Il punto è che ogni numero razionale ha un'unica rappresentazione come frazione ridotta ai minimi termini...)

2. f invertibile ? [No] | 1 |

   È evidente che per nessun $n \in \mathbb{N}$ si ha $f(n) = 1$, dunque f non è suriettiva.

C Provare per induzione.

1. Se $n \geq 1$ si ha che | 2 | |

$$(1 \cdot 2 \cdot 3) + (2 \cdot 3 \cdot 4) + (3 \cdot 4 \cdot 5) + ... + [n(n+1)(n+2)] = 6 \begin{pmatrix} n+3 \\ 4 \end{pmatrix}$$

L'uguaglianza è ovviamente vera per $n = 1$. Supponendola vera per n, la proviamo per $n+1$. Si ha

$$\sum_{i=1}^{n+1} i(i+1)(i+2) = \left(\sum_{i=1}^{n} i(i+1)(i+2) \right) + (n+1)(n+2)(n+3) =$$

$$= 6 \begin{pmatrix} n+3 \\ 4 \end{pmatrix} + (n+1)(n+2)(n+3) = 6 \begin{pmatrix} n+4 \\ 4 \end{pmatrix},$$

come si voleva.

2. Sia $f : \mathbb{Z} \to \mathbb{Z}$ $f(x) = 2 + 5x$. Sia $f^1 = f$ e $f^{n+1} = f^n f$. Se $n \geq 1$ si ha che | 2 | |

$$f^n(x) = \frac{5^n - 1}{2} + 5^n x$$

L'uguaglianza è ovviamente vera per $n = 1$. Supponendola vera per n, la proviamo per $n+1$. Si ha

$$f^{n+1}(x) = f(f^n(x)) = f\left(\frac{5^n - 1}{2} + 5^n x \right) = 2 + 5\left(\frac{5^n - 1}{2} + 5^n x \right) = \frac{5^{n+1} - 1}{2} + 5^{n+1} x,$$

come si voleva.

D Supponiamo di avere una struttura di monoide $(M, \circ, 1)$ su un insieme <u>infinito</u> M.

1. Un esempio di tale $(M, \circ, 1)$ che sia un gruppo **non** commutativo è M=$[(\mathrm{GL}_2(\mathbb{R}), \cdot)]$ | 2 | |

(Ovvero, il gruppo delle matrici 2×2 invertibili a coefficienti reali, con l'ordinario prodotto riga per colonna.)

2. Un esempio di tale $(M, \circ, 1)$ che **non** sia un gruppo è M=$[(\mathrm{Mat}_2(\mathbb{R}), \cdot)]$ | 1 | |

(Ovvero, il monoide delle matrici 2×2 a coefficienti reali, con l'ordinario prodotto riga per colonna)

1. Si consideri in $\mathbb{Q}[x]$ il polinomio $f(x) = 2x^3 - 9x + 6$.

   (a) Mostrare che le eventuali radici in $\mathbb{Q}$ della forma $\alpha = r/s$ (con r e s coprimi) sono tali che $r \mid 6$ e $s \mid 2$. | 2 | |

   Siano r ed s interi coprimi, con $s \neq 0$, tali che valga $2\left(\frac{r}{s}\right)^3 - 9\left(\frac{r}{s}\right) + 6 = 0$. Allora si ha $2r^3 - 9rs^2 + 6s^3 = 0$, da cui

   $$r(9s^2 - 2r^2) = 6s^3, \text{ ovvero } s(9rs - 6s^2) = 2r^3.$$

   Tenendo conto della coprimità di r ed s, dalla prima delle due equazioni precedenti otteniamo $r \mid 6$, e dalla seconda $s \mid 2$.

   (b) f è irriducibile in $\mathbb{Q}[x]$? [Sì] | 2 | |

   Essendo $f(x)$ un polinomio di grado 3, esso è irriducibile in $\mathbb{Q}[x]$ se e solo se non ha radici in $\mathbb{Q}$. Per il punto precedente, le possibili radici in $\mathbb{Q}$ sono gli elementi dell'insieme $\{\pm 1, \pm 2, \pm 3, \pm 6, \pm\frac{1}{2}, \pm\frac{3}{2}\}$. Basta verificare che nessuno di questi numeri è in effetti una radice di $f(x)$.

2. Si consideri la legge $\perp : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ così definita $a \perp b = a + b + ab$ per ogni $a, b \in \mathbb{N}$

   (a) $\perp$ è un'operazione in $\mathbb{N}$? [Sì] | 1 | |

   Per ogni coppia $(a, b) \in \mathbb{N} \times \mathbb{N}$, ovviamente $a \perp b \in \mathbb{N}$.

   (b) $(\mathbb{N}, \perp)$ è un semigruppo ? [Sì] | 1 | |

   Si tratta di verificare l'associatività di $\perp$. Ebbene,

   $$(a \perp b) \perp c = (a + b + ab) \perp c = (a + b + ab) + c + (a + b + ab)c,$$

   mentre

   $$a \perp (b \perp c) = a \perp (b + c + bc) = a + (b + c + bc) + a(b + c + bc).$$

   Per le proprietà di somma e prodotto in $\mathbb{N}$, le due espressioni coincidono per ogni scelta di $a, b, c \in \mathbb{N}$.

   (c) $(\mathbb{N}, \perp)$ è commutativo ? [Sì] | 1 | |

   Per la commutatività di somma e prodotto in $\mathbb{N}$, l'operazione $\perp$ è commutativa.

   (d) $(\mathbb{N}, \perp)$ è un gruppo ? [No] | 1 | |

   Si vede facilmente che 0 funziona da elemento neutro per $\perp$. Tuttavia, ad esempio, se x fosse l'inverso di 1 avremmo $1 \perp x = 1 + 2x = 0$, ma nessun numero naturale x soddisfa questa equazione.

3. Sia $A = \mathbb{Z}[i]$ l'anello degli interi di Gauss.

   (a) Il massimo comune divisore di $a = 2 + i$ e $b = -1 + 2i$ in A è $(a, b) = [a]$ | 2 | |

   I due elementi sono associati ($-1 + 2i = i \cdot (2 + i)$).

   (b) È vero che $2 + i$ è primo in A ? [Sì] | 2 | |

   Infatti, la sua norma è 5. Un elemento z di A che divide $2 + i$ ha norma un divisore (positivo) di 5, dunque 1 o 5: nel primo caso z è invertibile, nel secondo è associato a $2 + i$. Concludiamo che $2 + i$ è un elemento irriducibile di $\mathbb{Z}[i]$, il che equivale al fatto che sia primo (poiché $\mathbb{Z}[i]$ è un UFD).

4. Sia $\phi : \mathbb{Z}_p \longrightarrow \mathbb{Z}_p$ l'applicazione definita ponendo

$$\phi(x) = (x + 2)^p + 4x + 1$$

   per $x \in \mathbb{Z}_p$ dove $\mathbb{Z}_p$ è il campo delle classi di resti modulo p primo dispari.

   (a) È vero che per $p = 3$ ϕ è invertibile ? [Sì] | 2 | |

   Per ogni $x \in \mathbb{Z}_p$ si ha $\phi(x) = x^p + 2^p + 4x + 1 = x + 2 + 4x + 1 = 5x + 3$. (Abbiamo utilizzato il fatto che l'elevamento alla p è un omomorfismo di $(\mathbb{Z}_p, +)$, ed il Piccolo Teorema di Fermat.). Dunque, se $p = 3$, diventa $\phi(x) = 2x = -x$, che è l'inversione di $(\mathbb{Z}_p, +)$ e dunque è biettiva.

   (b) È vero che ϕ è sempre invertibile ? [No] | 2 | |

   Se $p = 5$, si ha $\phi(x) = 3$ per ogni x...