⊗ Matricola: ..... A B$^{\leq 6}$: ... C D$^{\geq 4}$: ... 1 2 3 4$^{\geq 8}$: ... Voto: .....

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

Algebra 1 – Esame 02.02.11

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

A Sia X un insieme non vuoto. Sia $f : X \to X$ una applicazione iniettiva e $x_0 \in X$.

1. Si ha che $Y = \{x_0, f(x_0), f^2(x_0), \ldots, f^n(x_0), \ldots\}$ è infinito ? [No] | 1 | |

   Si consideri ad esempio un insieme X di cardinalità 1 (sia $X = \{x_0\}$, e si scelga $f = \mathrm{Id}_X$).

2. Se l'applicazione indotta $f : Y \to Y$ è surgettiva Y è finito ? [Sì] | 2 | |

   Se la restrizione di f a Y è surgettiva, esiste $y \in Y$ tale che $f(y) = x_0$, dunque esiste un intero $m \geq 1$ tale che $f^m(x_0) = x_0$. È quindi evidente che, per ogni $n \in \mathbb{N}$, esiste $k \in \{0, ..., m-1\}$ tale che $f^n(x_0) = f^k(x_0)$ (intendendo $f^0(x_0) = x_0$). Concludiamo che si ha $|Y| \leq m$.

B Sia $k \in \mathbb{N}$ fissato, $k \geq 1$ e $f_k(n) = n(n-1)(n-2)\cdots(n-k+1)$ per $n \in \mathbb{N}$. Notare che per $k \geq 2$ si ha $(*)$ $f_k(n+1) - f_k(n) = k f_{k-1}(n)$...

Osserviamo che, per $n \geq k$, si ha $f_k(n) = \binom{n}{k} \cdot k!$. Dunque, per $n \geq k$, l'uguaglianza equivale a $\binom{n+1}{k} \cdot k! - \binom{n}{k} \cdot k! = \binom{n}{k-1} \cdot k!$, che è vera per la ben nota proprietà dei coefficienti binomiali $\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1}$. Inoltre, per $n+1 < k$ entrambi i membri dell'uguaglianza valgono 0, mentre per $n+1 = k$ valgono entrambi $(n+1)!$.

...e mostrare che per ogni $m \in \mathbb{N}^+$ si ha:

1. $\displaystyle\sum_{n=1}^{m} f_{k-1}(n) = f_k(m+1)/k$ | 1 | |

   Procediamo per induzione su m. Per $m = 1$ diventa $f_{k-1}(1) = f_k(2)/k$, ovvero

   $$f_k(2) - f_k(1) = k f_{k-1}(1)$$

   (visto che $f_k(1) = 0$), che è vera per quanto dimostrato sopra. Supponiamo dunque che l'uguaglianza sia vera per l'intero $m \geq 1$ e proviamola vera per $m+1$. Si ha

   $$\sum_{n=1}^{m+1} f_{k-1}(n) = \sum_{n=1}^{m} f_{k-1}(n) + f_{k-1}(m+1) = (\text{ipotesi induttiva}) = f_k(m+1)/k + f_{k-1}(m+1).$$

   Quest'ultima espressione è uguale a $f_k(m+2)/k$ in virtù di $(*)$ applicata con $m+1$ nel ruolo di n.

2. $\displaystyle\sum_{n=1}^{m} n^2 = \sum_{n=1}^{m} n + m(m^2-1)/3$ | 2 | |

   Applichiamo l'uguaglianza del punto precedente con $k = 3$. Si ha $\displaystyle\sum_{n=1}^{m} f_2(n) = f_3(m+1)/3$.

   Poiché

   $$\sum_{n=1}^{m} f_2(n) = \sum_{n=1}^{m} (n^2 - n), \qquad \text{e} \qquad f_3(m+1)/3 = m(m^2-1)/3,$$

   l'uguaglianza che si voleva risulta vera.

C Sia A un dominio e siano $M \in \mathbb{M}_n(A) = \{\text{matrici } n \times n \text{ ad entrate in } A\}$ con $n \geq 2$. Per ogni $n \geq 2$ e è vero che

1. se esiste M^{-1} allora $M^2 \neq 0$? [Sì] | 1 | |

   Se fosse $M^2 = 0$, si avrebbe $M = M^2M^{-1} = 0M^{-1} = 0$, dunque M non sarebbe invertibile.

2. se $M^2 = 0$ allora $M = 0$? [No] | 1 | |

   Si consideri ad esempio $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ *in* $\mathbb{M}_2(\mathbb{Z}_2)$.

3. se $M^3 = 0$ allora $M^2 = 0$? [No] | 2 | |

   Si consideri ad esempio $\begin{pmatrix} 0 & 1 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}$ *in* $\mathbb{M}_3(\mathbb{Z}_2)$.

4. se $M = -M$ allora $M^2 = 0$? [No] | 2 | |

   Si considerni ad esempio la matrice identica in $\mathbb{M}_2(\mathbb{Z}_2)$.

D Siano $a, b \in A$ non nulli in A dominio e supponiamo che $(a) \subseteq (b)$ come ideali principali.

1. Se $(a) = (b)$ allora $a = b$? [No] | 1 | |

   Si considerino ad esempio $a = 1$ e $b = -1$ in $\mathbb{Z}$.

2. Se a è irriducibile allora $(a) = (b)$? [No] | 1 | |

   Si considerino ad esempio $a = 2$ e $b = 1$ in $\mathbb{Z}$.

3. Se per qualche $k \gg 0$ si ha $(a^k) = (b^k)$ allora $(a) = (b)$? [Sì, basta $k \geq 1$] | 2 | |

   Poiché $a \in (b)$, esiste $s \in A$ tale che $a = sb$, da cui $a^k = s^k b^k$; inoltre, poiché $b^k \in (a^k)$, esiste $t \in A$ tale che $b^k = ta^k$. Allora si ha $a^k = s^k b^k = s^k t a^k$, e visto che siamo in un dominio, deve essere $s^k t = 1$ (notare che, essendo $a \neq 0$, è anche $a^k \neq 0$). Ma allora $s(s^{k-1}t) = 1$, dunque s è invertibile, e infine $b = s^{-1}a \in (a)$.

1. Sia $f(X) = X^{p+1} - (p+1)X^p - pX^{p-1} + p \in \mathbb{Z}[X]$ e sia $\bar{f}(X) \in \mathbb{Z}_p[X]$ la riduzione modulo p di $f(X)$, con p primo.

   (a) Per ogni p il polinomio $f(X)$ è irriducibile in $\mathbb{Z}[X]$? [No] | 2 | |

   Per $p = 2$ si ha che $f(X) = X^3 - 3X^2 - 2X + 2$ ha radice -1, dunque è divisibile per $X - 1$ e non è pertanto irriducibile.

   (b) Per ogni p trovare tutte le radici non-nulle di $\bar{f}(X)$ in $\mathbb{Z}_p$. [1] | 2 | |

   Si ha $\bar{f}(X) = X^{p+1} - X^p = X^p(X - 1)$.

2. Sia $r \in \mathbb{Q}$ e si consideri la relazione di equivalenza $\equiv$ in $\mathbb{Q}$ per cui $r \equiv r'$ se $r - r' \in \mathbb{Z}$. Indichiamo $\mathbb{Q}/\equiv$ con $\mathbb{Q}/\mathbb{Z}$ ovvero l'insieme delle classi di equivalenza $[r]$ al variare di $r \in \mathbb{Q}$.

   (a) Ponendo $[r] + [r'] = [r + r']$ sulle classi di equivalenza $(\mathbb{Q}/\mathbb{Z}, +)$ è un gruppo ? [Sì] | 1 | |

   Per definizione, non è altro che il gruppo quoziente del gruppo abeliano $(\mathbb{Q}, +)$ modulo il suo sottogruppo $\mathbb{Z}$.

   (b) È vero che dato $r \in \mathbb{Q}$ esiste $n \in \mathbb{N}$ tale che $n[r] = [0]$? [Sì] | 1 | |

   Sia $r = a/b$ con a e b interi, $b \neq 0$. Osserviamo che, a meno di moltiplicare numeratore e denominatore per -1, si può supporre $b \in \mathbb{N}$. Basta dunque prendere $n = b$, e si avrà $n[r] = [a] = [0]$.

   (c) Ponendo $[r] \cdot [r'] = [rr']$ sulle classi di equivalenza $(\mathbb{Q}/\mathbb{Z}, +, \cdot)$ è un anello ? [No] | 2 | |

   Se così fosse, $\mathbb{Z}$ sarebbe un ideale di $(\mathbb{Q}, +, \cdot)$, il che evidentemente non è.

3. Sia $A = \mathbb{Z}[\sqrt{-5}]$.

   (a) Esiste un massimo comune divisore di $3 + i\sqrt{5}$ e 4 in A ? [1] | 2 | |

   Sia d un massimo comun divisore. Poiché d divide $3+i\sqrt{5}$ *e divide* 4*, la sua norma* $N(d)$ *deve dividere* $N(3 + i\sqrt{5}) = 14$ *e* $N(4) = 16$*, dunque* $N(d) \in \{1, 2\}$*. In A non ci sono elementi aventi norma* 2*, mentre gli elementi di norma* 1 *sono* 1 *e* -1*. Ciascuno di questi ultimi è quindi un massimo comun divisore dei due elementi considerati.*

   (b) Esiste un massimo comune divisore di $i\sqrt{5}$ e 5 in A ? $[i\sqrt{5}]$ | 2 | |

   Infatti $i\sqrt{5}$ *è un divisore di* 5 *in A.*

4. Sia $\mathbb{Z}_p$ il campo delle classi di resti modulo p (p primo). Sia $\phi : \mathbb{Z}_p \longrightarrow \mathbb{Z}_p$ l'applicazione definita ponendo $\phi(a) = a^3 + a$ per $a \in \mathbb{Z}_p$

   (a) Esiste p tale che $\phi(a + b) = \phi(a) + \phi(b)$? $[p = 3]$ | 2 | |

   Per il Piccolo Teorema di Fermat, ogni elemento a di $\mathbb{Z}_3$ *soddisfa* $a^3 = a$*. Dunque, per* $p = 3$*, l'applicazione* ϕ *diventa la moltiplicazione per* $2 \in \mathbb{Z}_3$ *(o l'elevamento al quadrato da un punto di vista additivo). È chiaro che in questo caso è soddisfatta la condizione richiesta.*

   (b) Esiste p tale che ϕ è suriettiva ? $[p = 3]$ | 2 | |

   Per quanto osservato al punto precedente, nel campo $\mathbb{Z}_3$ *l'applicazione* ϕ *è la moltiplicazione per un elemento non nullo -quindi invertibile- di* $\mathbb{Z}_3$*, pertanto è suriettiva.*