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

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

Algebra 1 – Esame 14.01.11

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

A Sia $X \neq \emptyset$ e sia $\Omega = \{\emptyset, \{\emptyset\}\}$. Sia Ω^X l'insieme delle applicazioni $f : X \to \Omega$.

1. Esistono sempre $f : X \to \Omega$ applicazioni surgettive ma non iniettive ? [No] | 1 |

   Se consideriamo un insieme X di cardinalità 1, evidentemente non esisteranno applicazioni suriettive di X in Ω.

2. L'applicazione $f \in \Omega^X \rightsquigarrow f^{-1}(\emptyset) \in \mathcal{P}(X)$ è bigettiva ? [Sì] | 2 |

   Proviamo l'iniettività della funzione. Siano f e g elementi di Ω^X tali che $f^{-1}(\emptyset) = g^{-1}(\emptyset)$, e sia $x \in X$; se $x \in f^{-1}(\emptyset)$ si ha $f(x) = \emptyset = g(x)$, mentre se $x \notin f^{-1}(\emptyset)$ (e dunque $x \notin g^{-1}(\emptyset)$) deve essere $f(x) = \{\emptyset\} = g(x)$. Ciò vale per ogni $x \in X$, dunque $f = g$.
   proviamo ora la suriettività della funzione. Sia $Y \subseteq X$; definiamo $f : X \to \Omega$ come la funzione che assume il valore $\emptyset$ su tutti e soli gli elementi di Y. È evidente che la preimmagine di $\emptyset$ tramite f è Y.
   N.B.: l'insieme Ω^X può essere identificato con l'insieme delle funzioni caratteristiche definite su X, ed è un fatto noto che tale insieme sia in biiezione con $\mathcal{P}(X)$ proprio mediante la funzione che stiamo considerando.

B Sia $A = \{(x, y) \mid x, y \in \mathbb{Z}_5\}$. Definiamo: $(x, y) \oplus (z, t) = (x + z, y + t)$ e inoltre $(x, y) \odot (z, t) = (xz, xt + yz)$ per ogni (x, y) e (z, t) in A.

1. $(A, \oplus)$ è un gruppo abeliano ? [Sì] | 1 |

   Associatività e commutatività di $\oplus$ seguono immediatamente da associatività e commutatività di $+$ in $\mathbb{Z}_5$. È inoltre evidente che $(0, 0)$ funziiona da elemento neutro per $\oplus$, e che ogni elemento $(x, y) \in A$ ha inverso $(-x, -y) \in A$.

2. $(A, \odot)$ è un monoide ? [Sì] | 2 |

   Verifichiamo l'associatività di $\odot$. Si ha

   $$[(x, y) \odot (z, t)] \odot (h, k) = (xz, xt + yz) \odot (h, k) = ((xz)h, (xz)k + (xt + yz)h),$$

   e

   $$(x, y) \odot [(z, t) \odot (h, k)] = (x, y) \odot (zh, zk + th) = (x(zh), x(zk + th) + y(zh)).$$

   L'uguaglianza delle due espressioni segue dalla proprietà associativa della moltiplicazione in $\mathbb{Z}_5$, e dalla proprietà distributiva di somma e moltiplicazione in $\mathbb{Z}_5$.
   Inoltre, si verifica facilmente che $(1, 0)$ funziona da elemento neutro per $\odot$ in A.

C Sia $A[t]$ l'anello dei polinomi nella variabile t a coefficienti in A anello commutativo con 1.

1. Se $A = \mathbb{Z}_{31}$ è vero che $\mathbb{Z}_{31}[t]$ è P.I.D. ? [Sì] | 1 | |

   Infatti è ben noto che, dato un dominio D, l'anello di polinomi $D[t]$ è un dominio euclideo se e solo se D è un campo. Nel caso in esame, 31 è un numero primo, dunque $\mathbb{Z}_{31}$ è un campo.

2. Se $A = \mathbb{Z}_8$, è vero che l'insieme $K = \{2f(t) + tg(t) \mid f(t), g(t) \in A[t]\}$ è tutto $\mathbb{Z}_8[t]$? [No] | 2 | |

   Gli elementi di K valutati in 0 danno $2f(0)$, dunque $1 \notin K$ (altrimenti 1 sarebbe divisibile per 2, ovvero, 2 sarebbe invertibile in $\mathbb{Z}_8$, il che non è).

3. È vero che, per ogni $f(t)$ e $g(t)$ in $A[t] \setminus \{0\}$, vale $\deg(f(t)g(t)) = \deg(f(t)) + \deg(g(t))$? [No] | 2 | |

   È senz'altro vero se A è un dominio. Ma si considerino ad esempio $2t$ e $2t+1$ in $\mathbb{Z}_4[t]$: si ha $2t \cdot (2t+1) = 4t^2 + 2t = 2t$, dunque evidentemente la formula sui gradi che stiamo considerando non vale.

D Sia A un dominio.

1. Se $a \in A$ è irriducibile è primo ? [No] | 2 | |

   In un dominio che non sia a fattorizzazione unica, in generale gli elementi irriducibili non sono primi (sufficiente questa risposta). Un esempio è dato dall'elemento $2 \in \mathbb{Z}[\sqrt{-5}]$.

2. È vero che $\mathbb{Z}$ è un sottoanello di A ? [No] | 2 | |

   Si consideri $A = \mathbb{Z}_2$.

3. Esiste sempre almeno un $a \in A$ irriducibile in A ? [No] | 1 | |

   Se A è un campo, tutti i suoi elementi non nulli sono invertibili. Nessun elemento è quindi irriducibile.

1. Sia $\mathbb{Z}_p[x]$ l'anello dei polinomi sul campo $\mathbb{Z}_p$ delle classi di resti modulo p (p primo) e siano $f(x) = x^3 + x + 1$ e $g(x) = x^p - x + 1 \in \mathbb{Z}_p[x]$

   (a) Posto $p = 3$ si determinino le radici di $f(x)$ in $\mathbb{Z}_3$? [1] | 1 | |

   Basta inserire i tre elementi di $\mathbb{Z}_3$ al posto dell'indeterminata, e verificare che solo 1 *annulla il polinomio $f(x)$.*

   (b) Per ogni p si ha che $g(x) \in \mathbb{Z}_p[x]$ ha radici $\in \mathbb{Z}_p$? [No] | 2 | |

   In effetti, ciò è falso per ogni p. Per ogni $\alpha \in \mathbb{Z}_p$ vale infatti $\alpha^p - \alpha = 0$, dunque $g(\alpha) = 1$.

   (c) Per $p = 3$ i polinomi $f(x)$ e $g(x) \in \mathbb{Z}_p[x]$ sono coprimi ? [Sì] | 1 | |

   Il polinomio $g(x)$ non ha radici, dunque (avendo grado 3*) è irriducibile. Se non fosse coprimo con $f(x)$ dovrebbe dunque esserne un divisore, il che evidentemente non è.*

2. Sia $\mathbb{Q}$ il campo dei numeri razionali e siano $x, y \in \mathbb{Z}$ fissati, non entrambi nulli. Si consideri in $\mathbb{Q}$ la seguente operazione

$$a * b = ax + by$$

   (a) $(0 * 1) * 1 = 0 * (1 * 1)$ per i seguenti valori di x e y [$y \in \{0, 1\}, \forall x \in \mathbb{Z}$] | 1 | |

   Valutiamo le due espressioni:

$$(0 * 1) * 1 = y * 1 = xy + y;$$

$$0 * (1 * 1) = 0 * (x + y) = (x + y)y = xy + y^2.$$

   Si ha dunque l'uguaglianza se e solo se $y \in \{0, 1\}$ (mentre non c'è nessuna condizione su x).

   (b) $(\mathbb{Q}, *)$ è un semigruppo ? [No] | 1 | |

   Non vale l'associatività se si sceglie $y \notin \{0, 1\}$.

   (c) Se $x = 1$ allora $(\mathbb{Q}, *)$ è un gruppo per i seguenti valori di y [1] | 2 | |

   Per il punto (a)*, ci sono speranze solo per $y \in \{0, 1\}$. Per $y = 0$ si ha $a * b = a$ per ogni $a, b \in \mathbb{Q}$; Se $(\mathbb{Q}, *)$ fosse un gruppo, la legge di cancellazione darebbe $b = e$ per ogni $b \in \mathbb{Q}$ (dove con e denotiamo l'elemento neutro del presunto gruppo $(\mathbb{Q}, *)$), assurdo.*
   Per $y = 1$, si ha $a * b = a + b$ per ogni $a, b \in \mathbb{Q}$. Dunque $(\mathbb{Q}, *)$ non è altro che il gruppo additivo dei razionali.

3. Sia A un dominio. Siano p e q due elementi primi di A non associati fra loro.

   (a) Se p e q dividono un elemento $a \in A$ allora pq divide a in A ? [Sì] | 2 | |

   Scriviamo $a = rp$ e $a = sq$, per opportuni r, s in A. Si ha quindi $p \mid sq$, da cui $p \mid s$ oppure $p \mid q$; analogamente vale $q \mid r$ oppure $q \mid p$. Poiché p e q non sono associati, non valgono contemporaneamente $p \mid q$ e $q \mid p$, dunque vale una tra $p \mid s$ e $q \mid r$. Segue la tesi.

   (b) Sia $A = \mathbb{Z}[\sqrt{-3}] = \{a + ib\sqrt{3} \quad a, b \in Z\}$. Siano $p = 2$ e $q = 1 + i\sqrt{3}$. È vero che p e q sono primi ? [No] | 2 | |

   Si ha che 2 divide $4 = (1 + i\sqrt{3})(1 - i\sqrt{3})$, ma evidentemente 2 non divide alcuno dei fattori (non ne divide la parte reale).

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

   (a) Per quali $z \in A$ esiste $z^{-1} \in A$? [1, -1, i, $-i$] | 2 | |

   Se $z = a + ib$ è invertibile, allora divide 1. In particolare, la sua norma (quadrato del modulo complesso) $a^2 + b^2$ divide la norma di 1, che è 1. Si vede facilmente che deve dunque essere $a^2 = 1$ e $b^2 = 0$, oppure $a^2 = 0$ e $b^2 = 1$, da cui la conclusione (è evidente che tutti gli elementi elencati nella risposta siano effettivamente invertibili).

   (b) Per $z = 1 + i$ e $z' = 2 - 2i$ in A determinare, se esiste, un massimo comun divisore.

   M.C.D.$(z, z') = [z]$ | 2 | |

   Si ha che 2 divide z', ma $2 = (1 + i)(1 - i)$. Dunque $z \mid 2$, da cui $z \mid z'$. Segue immediatamente che M.C.D.$(z, z') = z$.