

$\Phi$  MATRICOLA: ..... A  $B^{\leq 5}$ : ... C  $D^{\geq 5}$ : ... 1 2 3 4  $\geq 8$ : ... VOTO: .....

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

### Algebra 1 – Esame 22.12.11

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

**A** Siano  $A$  e  $B$  due insiemi tali che  $A \cap B$  sia non vuoto e sia  $\mathbf{2} = \{0, 1\}$ .

1. Esiste un'applicazione bigettiva tra  $\mathbf{2}^{(A \cup B)}$  e  $\mathbf{2}^A \cup \mathbf{2}^B$ ? [No]

1

*Consideriamo ad esempio  $A = \{0, 1\}$  e  $B = \{0\}$ . Si ha  $|\mathbf{2}^{(A \cup B)}| = |\mathbf{2}^A| = 4$ , mentre  $|\mathbf{2}^B| = 2$ . D'altra parte,  $\mathbf{2}^A$  e  $\mathbf{2}^B$  sono insiemi disgiunti (il dominio delle funzioni in  $\mathbf{2}^A$  è diverso dal dominio delle funzioni in  $\mathbf{2}^B$ ), pertanto  $|\mathbf{2}^A \cup \mathbf{2}^B| = 6$ .*

2. Se  $B \subset A$  l'insieme  $\{f : A \rightarrow \mathbf{2} \mid f(B) = 0\}$  ha cardinalità strettamente maggiore di quella di  $A \setminus B$ ? [Sì]

*Ricordiamo che, dato un insieme non vuoto  $X$ , l'insieme  $\mathbf{2}^X$  è in biiezione con l'insieme delle parti  $\mathcal{P}(X)$ . Nella biiezione standard tra questi due insiemi,  $\mathcal{P}(A \setminus B)$  (visto come sottoinsieme di  $\mathcal{P}(A)$ ) resta identificato esattamente con  $\{f : A \rightarrow \mathbf{2} \mid f(B) = 0\}$ . Pertanto quest'ultimo insieme ha sempre cardinalità strettamente maggiore di  $A \setminus B$ .*

2

**B** Sia  $S$  non vuoto e  $f : S \rightarrow S$  surgettiva ma non iniettiva.

1. L'insieme  $S$  è un insieme infinito? [Sì]

1

*È ben noto che, se  $S$  è un insieme finito (e non vuoto), ogni applicazione surgettiva di  $S$  in sé è anche iniettiva.*

2. Se  $S = \mathbb{N}$  esiste una tale  $f$ ? [Sì]

1

*Si consideri ad esempio l'applicazione che manda 0 in 0 e  $n$  in  $n - 1$  per ogni  $n \in \mathbb{N} \setminus \{0\}$ .*

C Sia  $A$  un dominio tale che  $1 + 1 = 0$  ovvero  $\mathbb{Z}_2 \subset A$  è un sottoanello.

1. È vero che  $(a + b)^4 = a^4 + b^4$  per ogni  $a, b \in A$  ? [Sì]

2

*Espandendo il binomio con la formula dei coefficienti binomiali (cosa che è lecita in un qualsiasi anello commutativo), si osserva che tutti i termini misti hanno un coefficiente divisibile per 2, vale a dire hanno coefficiente 0.*

2. Esiste un tale anello  $A$  infinito ? [Sì]

2

*Ad esempio, l'anello di polinomi  $\mathbb{Z}_2[x]$ .*

3. Esiste un tale anello  $A$  P.I.D. ? [Sì]

2

*L'esempio precedente è buono anche in questo caso, visto che  $\mathbb{Z}_2$  è un campo e dunque  $\mathbb{Z}_2[x]$  è un dominio euclideo.*

4. È vero che se  $A$  è finito allora è un campo ? [Sì]

1

*Si prova facilmente che, fissato  $a \in A \setminus \{0\}$ , la mappa  $x \mapsto ax$  di  $A$  in sé è iniettiva. Se  $A$  è finito, tale applicazione è dunque anche suriettiva, pertanto esiste  $y \in A$  tale che  $ay = 1$ , i.e.,  $a$  è invertibile.*

D Sia  $(A, \delta)$  dominio euclideo con norma  $\delta : A \setminus \{0\} \rightarrow \mathbb{N}$

1. È vero che se  $a \mid b$  allora  $\delta(a) \mid \delta(b)$  ? [No]

2

*Si consideri ancora  $\mathbb{Z}_2[x]$ , che è un dominio euclideo se si pone che la norma di un polinomio (non nullo) sia il suo grado. Ebbene,  $x^2$  divide  $x^3$ , ma 2 non divide 3.*

2. È vero che se  $\delta(a) = 0$  allora  $a \in A^*$  è invertibile ? [Sì]

2

*È noto che gli elementi invertibili di un dominio euclideo sono gli elementi che hanno norma minima tra gli elementi non nulli. È allora chiaro che se un elemento non nullo ha norma 0, esso ha norma minima possibile ed è quindi invertibile.*

1. Sia  $\mathbb{Z}_p[X]$  l'anello dei polinomi a coefficienti in  $\mathbb{Z}_p$  con  $p$  primo. Siano  $f(X), g(X) \in \mathbb{Z}_p[X]$  i polinomi  $f(X) = X^6 - X^4 + 2X + 2$  e  $g(X) = X^6 + 9X^4 + 10X^3 - X^2 + 1$ .

(a)  $f(X)$  è riducibile solo per  $p = 2$ ? [No]

1

*Si ha  $f(-1) = 0$ , dunque un'applicazione del Teorema di Ruffini garantisce che  $f(X)$  sia divisibile per  $X + 1$ . Ciò indipendentemente dal primo  $p$ .*

(b)  $g(X)$  è divisibile per  $X + 1$ ? [Sì]

1

*Infatti  $-1$  è radice anche di  $g(X)$ .*

(c) Sono  $f(X)$  e  $g(X)$  coprimi? [No]

1

*Hanno una radice in comune...*

(d) Se  $p = 2$  allora  $f(X) \mid g(X)$ ? [No]

1

*Per  $p = 2$  il polinomio  $f(X)$  diventa  $X^6 - X^4$ , che ha radice 0. Invece, 0 non è radice di  $g(X)$ , e questo evidentemente esclude la divisibilità di  $g(X)$  per  $f(X)$ .*

2. Sia  $G = \mathbb{Q} \setminus \{-1/2\}$  e sia  $\star$  l'operazione così definita:  $x \star y = x + y + 2xy$  per  $x, y \in G$ .

(a)  $(G, \star)$  è un semigruppato? [Sì]

1

*Verifichiamo innanzi tutto che l'operazione sia interna. Siano  $x, y \in G$ : se fosse  $x \star y = -1/2$ , avremmo  $x + y + 2xy = -1/2$ , da cui  $(1 + 2x)y = -(1/2 + x)$ , da cui  $y = -1/2$ , una contraddizione. Inoltre, proviamo l'associatività di  $\star$ :*

$$(x \star y) \star z = (x + y + 2xy) \star z = (x + y + 2xy) + z + 2(x + y + 2xy)z;$$

*d'altra parte,*

$$x \star (y \star z) = x \star (y + z + 2yz) = x + (y + z + 2yz) + 2x(y + z + 2yz).$$

*Come si vede facilmente utilizzando le proprietà delle operazioni in  $\mathbb{Q}$ , le due espressioni coincidono per ogni scelta di  $x, y, z \in G$ .*

(b)  $(G, \star)$  è commutativo? [Sì]

1

*Si ha  $x \star y = x + y + 2xy = y + x + 2yx = y \star x$ , per ogni scelta di  $x, y \in G$ .*

(c)  $(G, \star)$  è un gruppo? [Sì]

1

*Verifichiamo l'esistenza dell'elemento neutro. Imponiamo  $x \star e = x$ ; otteniamo  $x + e + 2xe = x$ , da cui  $(1 + 2x)e = 0$ . Ciò deve valere per ogni scelta di  $x \in G$ , ad esempio per  $x = 0$ , da cui  $e = 0$ . In effetti, 0 funziona da elemento neutro per  $\star$ . Inoltre, sia  $x \in G$ , e imponiamo  $x \star y = 0$ : si ha  $x + y + 2xy = 0$ , da cui  $y = -\frac{x}{1 + 2x}$ . Poiché questa espressione non assume il valore  $-1/2$  per alcun valore di  $x$  (come si può facilmente verificare), concludiamo che ogni  $x \in G$  ha inverso.*

3. Sia  $A = \mathbb{Z}[i]$  l'anello degli interi di Gauss e sia  $S = \{z = a + ib \mid a \equiv_2 0 \equiv_3 b\}$ .

(a) Mostrare che  $S$  non è un ideale di  $A$ .

2

*Si ha  $2 \in S$ , ma  $2i \notin S$ . Dunque  $S$  non "assorbe" i prodotti mediante generici elementi di  $A$ .*

(b) Sia  $I$  l'ideale generato da  $S$ . È vero che  $I$  è un ideale proprio di  $A$ ? [No]

2

*Osserviamo che  $1 = (3i) \cdot (-i) - 2 \in I$ : infatti  $3i \in S \subseteq I$  implica  $(3i) \cdot (-i) \in I$ , inoltre  $2 \in S \subseteq I$ , dunque  $1$  è differenza di due elementi di  $I$ . Concludiamo che  $I = A$ .*

4. Sia  $A$  l'anello costituito dalle classi di equivalenza  $[z]$  per  $z \in \mathbb{Z}[i]$  dove  $[z] = [z']$  se  $z - z'$  è un multiplo di  $1 + 3i$  ovvero  $A = \mathbb{Z}[i]/(1 + 3i)$  con somma e prodotto indotte da quelle di  $\mathbb{Z}[i]$ .

(a) È vero che  $[10] = [0]$  in  $A$ ? [Sì]

2

*Chiaramente  $10$  è divisibile per  $1 + 3i$  in  $\mathbb{Z}[i]$ ; infatti si ha  $10 = (1 + 3i)(1 - 3i)$ . Dunque  $10 - 0 = 10 \in (1 + 3i)$ , da cui  $[10] = [0]$  in  $A$ .*

(b) È vero che  $A$  è finito? [Sì]

2

*Infatti, data la struttura di dominio euclideo di  $\mathbb{Z}[i]$ , sappiamo che ogni  $z \in \mathbb{Z}[i]$  si lascia scrivere come  $q(1 + 3i) + r$ , dove  $q, r \in \mathbb{Z}[i]$  e la norma di  $r$  è strettamente minore della norma di  $1 + 3i$ , ovvero di  $10$ . Osserviamo che  $z - r \in (1 + 3i)$ , dunque  $[z] = [r]$  in  $A$ . Concludiamo che ogni elemento di  $\mathbb{Z}[i]$  è equivalente ad un elemento di norma inferiore a  $10$ . La conclusione segue dal fatto che gli elementi di norma inferiore a  $10$  in  $\mathbb{Z}[i]$  sono ovviamente un numero finito.*