☐ Matricola: ..... **A+B**$^{\geq 3}$:... **C**$^{\geq 3}$:... **D**$^{\geq 3}$:... **E+F**$^{\geq 3}$:... Voto: .....

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

Algebra 1 – Esame 26.02.14

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

A Sia $f : \mathbb{Z} \to \mathbb{Z}$ la funzione definita ponendo $f(x) = \begin{cases} 3x \text{ se } x \text{ è pari} \\ 2x \text{ se } x \text{ è dispari.} \end{cases}$

1. f iniettiva ? [No] f surgettiva ? [No] | 2 |

   Si ha $f(2) = 6 = f(3)$, dunque la funzione non è iniettiva. Inoltre, nessun intero dispari appartiene all'immagine della funzione, che non è pertanto suriettiva.

2. È vero che $2\mathbb{Z} = \{x \in \mathbb{Z} \mid f(x) \in 6\mathbb{Z}\}$? [No] | 1 |

   Come osservato sopra, $f(3) = 6 \in 6\mathbb{Z}$, ma ovviamente $3 \notin 2\mathbb{Z}$.

B Sia $A = \mathbb{Z}[i]$ l'anello degli interi di Gauss. Sia $B = \{(a-b) + i(a+b) \mid a, b \in \mathbb{Z}\} \subseteq A$.

1. È vero che B è un sottogruppo di A ? Considerata in A la relazione $\alpha \sim \beta$ se $\alpha - \beta \in B$ mostrare che $\sim$ è una relazione di equivalenza. È vero che $B = [0]_\sim$? [Sì] | 2 |

   Per $a, b, c, d \in \mathbb{Z}$, si ha $[(a-b)+i(a+b)] - [(c-d)+i(c+d)] = [(a-c)-(b-d)] + i[(a-c)+(b-d)]$; essendo inoltre B chiaramente non vuoto, si ha che B è un sottogruppo di $(A, +)$. La relazione considerata non è altro che la relazione indotta dal sottogruppo B; è dunque noto che si tratta di una equivalenza, e che vale $B = [0]_\sim$.

2. È vero che B è un semigruppo rispetto alla moltiplicazione ? È un monoide ? [Risp. sì, no] | 2 |

   Per provare che B sia un semigruppo rispetto alla moltiplicazione, è sufficiente provare che rispetto a tale operazione B risulti chiuso. Ebbene, per $a, b, c, d \in \mathbb{Z}$ si ha $[(a-b) + i(a+b)] \cdot [(c-d) + i(c+d)] = (x-y) + i(x+y)$, se si pone $x = ac - bd - ad - bc$ e $y = ac - bd + ad + bc$. D'altra parte, se per qualche $a, b \in \mathbb{Z}$ fosse $1 = (a-b) + i(a+b)$, avremmo $a - b = 1$ e $a + b = 0$, da cui $2a = 1$, che non ha soluzioni in $\mathbb{Z}$, dunque $1 \notin B$; questo è sufficiente per garantire che B non sia un monoide, poiché una eventuale unità di B sarebbe un elemento idempotente in A, ma A è un dominio, dunque i suoi soli idempotenti sono 0 e 1 (e chiaramente 0 non funziona da unità per B).

C Si considerino i polinomi $a(X) = X^2 - X - 2$ e $b(X) = X^4 + 2X^3 - X^2 + 2X + 1$.

1. La classe di $b(X)$ è invertibile nel quoziente $\mathbb{Q}[X]/(a(X))$? [Sì] | 2 | |

   Il polinomio $a(X)$ si spezza come $(X+1)(X-2)$ in $\mathbb{Q}[X]$. D'altra parte, né -1 né 2 sono radici di $b(X)$, dunque (per il Teorema di Ruffini, e tenendo conto del fatto che $\mathbb{Q}[X]$ è un UFD) i due polinomi sono coprimi. Come è ben noto, ciò è equivalente ad affermare che la classe di $b(X)$ sia invertibile in $\mathbb{Q}[X]/(a(X))$ (infatti $\mathbb{Q}[X]$ è un PID, etc...).

2. In $\mathbb{Q}[X]$ i polinomi $a(X)$ e $b(X)$ sono coprimi ? [Sì] | 3 | |

   Vedi sopra.

3. Per quali valori del primo p i polinomi $a(X)$ e $b(X)$ sono coprimi in $\mathbb{Z}_p[X]$? $[\forall p \notin \{3, 11\}]$ | 3 | |

   Essendo $\mathbb{Z}_p[X]$ un UFD per ogni primo p, la coprimità dei due polinomi equivale al fatto che né -1 né 2 siano radici di $b(X)$ in $\mathbb{Z}_p$, ovvero che né $b(-1) = -3$ né $b(2) = 33$ siano congrui a 0 modulo p. È chiaro che ciò avviene se e solo se $p \notin \{3, 11\}$.

D Sia $A = \mathbb{Z}[\sqrt{-7}]$.

1. Esiste un massimo comune divisore di $2 + 2i\sqrt{7}$ e 8 in A ? [No] | 2 | |

   Osserviamo prima di tutto che in A gli elementi di norma 1 *sono* 1 *e* -1 *(e quindi, se* $x, y \in A$ *sono tali che* $N(x) = N(y)$ *e* $x \mid y$*, allora è* $x = \pm y$*), quelli di norma* 4 *sono* 2 *e* -2*, mentre non ci sono elementi di norma* 2*. Supponiamo per assurdo che esista un massimo comune divisore* d *per* $2 + 2i\sqrt{7}$ *e* 8 *in A. Poiché* $1 + i\sqrt{7}$ *è ovviamente un divisore comune, deve essere* $1 + i\sqrt{7} \mid d$ *(osserviamo anche che lo stesso vale per* 2*) e dunque, in particolare,* $8 \mid N(d)$*; d'altra parte* $d \mid 2 + 2i\sqrt{7}$*, da cui* $N(d) \mid 32$*. Concludiamo che* $N(d) \in \{8, 16, 32\}$*. Se* $N(d) = 8$*, allora* $d = \pm(1 + i\sqrt{7})$ *e quindi* $2 \nmid d$*, una contraddizione. Se* $N(d) = 32$*, allora* $d = \pm(2 + 2i\sqrt{7})$*, ma allora* $d \nmid 8$ *(altrimenti* 8 *dovrebbe avere un divisore di norma* 2*), ancora una contraddizione. Infine, se* $N(d) = 16$*, poiché* d *è divisibile per* 2*,* d *deve essere prodotto di due elementi di norma* 4*, dunque* $d = \pm 4$ *e si ottiene ancora la contraddizione* $d \nmid 2 + 2i\sqrt{7}$*.*

2. Esiste un massimo comune divisore di $i\sqrt{7}$ e 21 in A ? [Sì] | 2 | |

   Chiaramente $i\sqrt{7}$ *è un divisore di* 21*.*

3. Esiste un massimo comune divisore di 8 e 21 in A ? [Sì] | 3 | |

   I due elementi hanno norme coprime (in $\mathbb{Z}$*), e sono dunque coprimi (in A).*

E Mostrare per induzione che per ogni $n \geq 1$ si ha

$$(-1) \cdot 1^2 + (-1)^2 \cdot 2^2 + \cdots (-1)^n \cdot n^2 = (-1)^n \cdot \frac{n(n+1)}{2}$$

3	

Per $n = 1$ si ottiene -1 ad entrambi i membri. Supponiamo dunque che la proposizione sia vera per l'intero $n \geq 1$, e proviamola per $n + 1$: si ha

$$(-1)\cdot 1^2 + (-1)^2 \cdot 2^2 + \cdots + (-1)^n \cdot n^2 + (-1)^{n+1} \cdot (n+1)^2 = (-1)^n \cdot \frac{n(n+1)}{2} + (-1)^{n+1} \cdot (n+1)^2 =$$

$$= (-1)^{n+1} \cdot (n+1) \cdot \frac{-n + 2(n+1)}{2} = (-1)^{n+1} \cdot \frac{(n+1)((n+1)+1)}{2},$$

ed il passo induttivo è completo.

F Sia A anello commutativo unitario e sia $M = A[X]$ considerato come A-modulo. Sia $f : M \to M$ l'omomorfismo A-lineare unicamente determinato da $f(1) = 0$ e $f(X^n) = X^{n-1}$ per $n \geq 1$.

1. È vero che $\mathrm{Ker} f = A$? [Sì]

3	

Per $p(X) = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0$, si ha $f(p(X)) = a_n X^{n-1} + a_{n-1} X^{n-2} + \cdots + a_2 X + a_1$, dunque $f(p(X)) = 0$ se e solo se $a_i = 0$ per ogni $i \geq 1$.

2. È vero che $M \cong M/A$? [Sì]

2	

Infatti il morfismo di moduli definito sopra è ovviamente suriettivo, ed il Teorema di Isomorfismo prova che quanto affermato è vero.