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

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

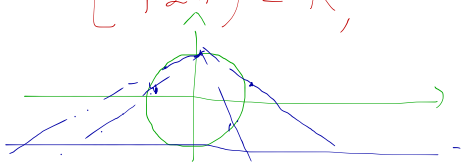
Algebra 1 – Esame 17.06.14

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

A Consideriamo $C = \{z \in \mathbb{C} \mid |z| = 1\}$ l'insieme dei numeri complessi di modulo 1.

1. L'insieme C è numerabile? [NO] | 1 |

E' ben noto che C è in biezione con $[0, 2\pi) \subseteq \mathbb{R}$, che non è numerabile. Oppure: $C \setminus \{i\}$ è in biezione con $\mathbb{R}$ →



2. Poniamo zRw se esiste un $n \geq 1$ tale che $z^n = w^n$. Dimostrare che è una relazione di equivalenza. | 2 |

La relazione è ovviamente riflessiva e simmetrica. E' inoltre transitiva: sia $z^n = w^n$ e $w^t = y^t$, allora $z^{nt} = w^{nt} = y^{nt}$ (dove $n, t \geq 1$)

3. L'insieme quoziente C/R è numerabile? [No] | 2 |

Per $n \geq 1$, sia $X_n = \{z \in \mathbb{C} : z^n = 1\}$; sia poi $X = \bigcup_{n \geq 1} X_n$ (X è l'insieme delle radici di 1 in $\mathbb{C}$). Tale X è numerabile e, per $z, w \in C$, si ha $zRw \Leftrightarrow \exists x \in X$ con $w = xz$. Allora $|[z]_R| = |Xz| = |X|$. Concludiamo che le classi di R sono numerabili. Se lo fosse C/R, lo sarebbe C.

B Risolvere se possibile il seguente sistema di congruenze lineari:

$$\begin{cases} x \equiv 2 \pmod 9 \\ x \equiv 3 \pmod 7 \end{cases}$$

| 2 |

Poiché 9 e 7 sono coprimi, esiste una e una sola soluzione mod. 9×7 (Teorema Cinese del resto). Questa è $[38]_{63}$. L'insieme delle soluzioni è dunque $\{38 + 63t : t \in \mathbb{Z}\}$

C Provare per induzione che

Se $k \geq 1$ si ha

$$\sum_{k=1}^{n}(k^2+1)k! = n((n+1)!)$$

2	

Per $n=1$ entrambi i membri dell'uguaglianza valgono 2.
Supponiamo dunque l'uguaglianza vera per $n \geq 1$, e proviamola per $n+1$: si ha

$$\sum_{k=1}^{n+1}(k^2+1)k! = \sum_{k=1}^{n}(k^2+1)k! + ((n+1)^2+1)((n+1)!) = n((n+1)!) +$$

$$+ ((n+1)^2+1)((n+1)!) = ((n+1)!)[n^2+3n+2] = ((n+1)!)(n+2)(n+1) =$$

$$= (n+1)((n+2)!).$$

D Si consideri l'applicazione $\phi : \mathbb{C}^* \to \mathbb{C}^*$ definita da $\phi(z) = z^n$.

1. ϕ è un omomorfismo di gruppi?

4	

Sì. Infatti, per $z, w \in \mathbb{C}^*$, si ha $\varphi(zw) = (zw)^n =$

$$= z^n w^n = \varphi(z)\cdot\varphi(w)$$

(Perché $(\mathbb{C}^*, \cdot)$ è abeliano)

2. Determinare nucleo e immagine di ϕ.

2	

$\ker\varphi = X_n$ (come definito in A3), mentre

$\operatorname{Im}\varphi = \{z^n : z \in \mathbb{C}^*\} = \mathbb{C}^*$

1. Nell'anello degli interi di Gauss $\mathbb{Z}[i]$ si consideri l'ideale $I = (2i, 6+4i)$.

(a) Dire se I è principale, e, in caso affermativo, trovare un generatore. | 2 |

$\mathbb{Z}[i]$ è un PID, dunque I è senz'altro principale. Un suo generatore è un mcd tra $2i$ e $6+4i$:
$2i = (1+i)\cdot(1-i)\cdot i$; $6+4i = (1+i)(1-i)(3+2i)$
(oss: $3+2i$ ha norma 13, dunque è primo in $\mathbb{Z}[i]$).
Concludiamo che $I = ((1+i)\cdot(1-i)) = (2)$.
Si può anche argomentare: 2 divide $2i$ e $6+4i$, dunque $I \subseteq (2)$;
d'altra parte $2 = 2i\cdot(-i) \in I$.

(b) L'ideale I è massimale? | 4 |

No. Non è neppure un ideale primo, poiché $2 = (1+i)(1-i)$.

2. Sia $S = \mathbb{Z}_m$ e si consideri la legge $\perp : S \times S \to S$ così definita $x \perp y = ax + by$ per ogni $x, y \in S$.

(a) Esistono $a, b \neq 0, 1 \in \mathbb{Z}_m$ tali che $(S, \perp)$ è un semigruppo per qualche $m > 0$? [ ] | 2 |

Se $(S, \perp)$ è semigruppo, allora $(1 \perp 0) \perp 0 = 1 \perp (0 \perp 0)$
(da cui $a^2 = a$), e $(0 \perp 0) \perp 1 = 0 \perp (0 \perp 1)$, (da cui $b = b^2$)
Dunque, condizione necessaria affinché S sia un semigruppo è che a, b siano idempotenti. Ad esempio, si scelga $a = 3 = b$ con $m = 6$. La condizione è in effetti anche sufficiente.

(b) Inoltre, in modo che m sia un numero primo ? [No] | 1 |

Se m è primo, $(\mathbb{Z}_m, +, \cdot)$ è un campo, dunque non ha elementi idempotenti eccetto 0 e 1.

3. Consideriamo l'anello dei polinomi $\mathbb{Z}_4[X]$.

(a) Il polinomio $2X+1$ è invertibile in $\mathbb{Z}_4[X]$? [Sì] | 2 |

$(2X+1)^2 = 4X^2 + 4X + 1 = 1$

(b) È vero che $\mathbb{Z}_4$ è un sottoanello di $\mathbb{Z}_4[X]/(2X+1)$? [No] | 2 |

Poiché $2X+1$ è invertibile, si ha $(2X+1) = \mathbb{Z}_4[X]$, dunque $\frac{\mathbb{Z}_4[X]}{(2X+1)}$ è un anello ridotto al solo 0.

(c) È vero che $\mathbb{Z}_4[X]/(2, X)$ è un anello finito ? [Sì] | 2 |

Si ha $(X) \subseteq (2, X)$, e l'anello $\frac{\mathbb{Z}_4[X]}{(X)}$ è finito. Infatti, avendo X coefficiente principale invertibile, ogni polinomio $p(X)$ può essere diviso per X dando un resto costante. Se $p(X) = X \cdot q(X) + r$, si ha dunque $[p(X)]_{(X)} = [r]_{(X)}$ (in altre parole, $\mathbb{Z}_4[X]/(X) \simeq \mathbb{Z}_4$).

(d) È vero che l'ideale (2) è primo in $\mathbb{Z}_4[X]$? [Sì] | 2 |

L'anello quoziente $\frac{\mathbb{Z}_4[X]}{(2)}$ è isomorfo a $\mathbb{Z}_2[X]$, che è un dominio.