Algebra 1

Prof. A. D'Andrea, A. De Sole, G. Mondello

Prova scritta del 31-1-2022

Nome e Cognome: _____

Numero di Matricola: _____

Docente: **D'Andrea \ De Sole - Mondello** (cerchiare il/i docente/i).

Esercizio	Punti totali	Punteggio
1	6	
2	6	
3	6	
4	6	
5	6	
Totale	30	

Esercizio 1. Trovare tutti gli x interi soluzioni del seguente sistema alle congruenze:

$$\begin{cases} 4x & \equiv & 2 & \mod 6 \\ 2^x & \equiv & 3 & \mod 5 \end{cases}$$

Soluzione:

Si vede facilmente che 2 è invertibile modulo 5 e ha ordine (moltiplicativo) 4 nel gruppo $\mathbb{Z}/(5)^\times$. Le potenze di 2 si ripetono quindi periodicamente nell'esponente, con periodo 4. Poiché $2^3 = 8 \equiv 3 \mod 5$, la seconda congruenza è equivalente a $x \equiv 3 \mod 4$.

D'altro canto, la prima congruenza è equivalente a $2x \equiv 1 \mod 3$ e quindi a $x \equiv 2 \mod 3$. Dobbiamo quindi risolvere il sistema

$$\begin{cases} x \equiv 2 & \mod 3 \\ x \equiv 3 & \mod 4, \end{cases}$$

che ha soluzione unica modulo 12 per il Teorema Cinese dei Resti. Potete trovarne una soluzione intera nel modo che preferite, per concludere che la soluzione è $x \equiv 11 \mod 12$. Ricordate però che x deve essere positivo, altrimenti la seconda congruenza del sistema iniziale non ha senso!

Le soluzioni sono quindi $x = 11 + 12k$ con $k \geq 0$ intero.

Risposta: $x =$

Esercizio 2. Il gruppo G ha ordine 36 e i suoi 3-Sylow non sono normali.

(a) Spiegare perché i 3-Sylow di G siano abeliani.

(b) Mostrare che l'intersezione di due 3-Sylow contiene esattamente tre elementi.

(c) Mostrare che G ha centro non banale.

Soluzione:

(a) I 3-Sylow di G hanno ordine 9, e sappiamo che i gruppi di ordine p^2, con p primo, sono tutti abeliani.

(b) Se $P \neq Q$ sono due 3-Sylow, allora PQ possiede $|P||Q|/|P \cap Q|$ elementi. Poiché $|P| = |Q| = 9$ e $|PQ| \leq 36$, si vede che $|P \cap Q| \geq 81/36 = 9/4$. Poiché $|P \cap Q|$ deve dividere 9 per il Teorema di Lagrange ed essere inferiore a 9 poiché $P \neq Q$, si ottiene $|P \cap Q| = 3$.

(c) Se $P \neq Q$ sono due 3-Sylow, ogni elemento di $P \cap Q$ commuta sia con gli elementi di P che con quelli di Q, poiché P, Q sono entrambi abeliani. Ma allora commuta con i $9 \cdot 9/3 = 27$ elementi contenuti in PQ. Ad ogni modo, il centralizzatore di un elemento è un sottogruppo, e un sottogruppo di G che contenga almeno 27 elementi è tutto G. Ogni elemento di $P \cap Q$ è quindi centrale.

Volendo anche mostrare che il centro di G non è tutto il gruppo, basta osservare che i 3-Sylow non sono normali, mentre in un gruppo abeliano ogni sottogruppo è normale.

Esercizio 3. Si consideri, nell'anello $\mathbb{Z}[i]$ degli interi di Gauss, l'ideale $I = (3+4i, 7+6i)$.

(a) Dire se $\mathbb{Z}[i]/I$ sia un dominio d'integrità .

(b) Dire se $\mathbb{Z}[i]/I$ sia un campo.

(c) Quanti elementi possiede $\mathbb{Z}[i]/I$?

Soluzione: L'ideale I è generato dal MCD di $3+4i$ e $7+6i$, che possiamo calcolare per mezzo dell'algoritmo euclideo. Eseguendolo, si ottiene

$$\begin{aligned} 7+6i &= 2\cdot(3+4i)+(1-2i) \\ 3+4i &= (-1+2i)\cdot(1-2i)+0. \end{aligned}$$

e il MCD è quindi $1-2i$, che avendo norma prima è irriducibile in $\mathbb{Z}[i]$. L'ideale $I=(1-2i)$ è quindi sia primo che massimale, e il quoziente $\mathbb{Z}[i]/I$ è sia un dominio d'integrità che un campo.

Per quanto riguarda la cardinalità del quoziente $\mathbb{Z}[i]/I$ si può procedere in vari modi. Tre possibilità sono le seguenti:

- Si può osservare che nell'isomorfismo di gruppi abeliani

  $$\mathbb{Z}^2 \ni (a,b) \mapsto a+bi \in \mathbb{Z}[i]$$

  all'ideale $(1-2i) = I \subset \mathbb{Z}[i]$ corrisponde il sottogruppo $\langle (1,-2),(2,1)\rangle$. La forma canonica di Smith della matrice

  $$\begin{pmatrix} 1 & 2 \\ -2 & 1 \end{pmatrix}$$

  si ottiene con la solita procedura, che fornisce

  $$\begin{pmatrix} 1 & 0 \\ 0 & 5 \end{pmatrix},$$

  e pertanto $\mathbb{Z}[i]/I$ è isomorfo, come gruppo abeliano, a $\mathbb{Z}/(5)$ e contiene quindi 5 elementi.

- Si può mostrare che l'applicazione $\phi : \mathbb{Z}[i] \to \mathbb{Z}/(5)$ data da $\phi(a+bi) = [a-2b]_5$ è un ben definito omomorfismo di anelli il cui nucleo contiene $I=(1-2i)$ ma non è tutto $\mathbb{Z}[i]$. Per massimalità di I, il nucleo di ϕ coincide allora con I e pertanto $\mathbb{Z}[i]/I$ è isomorfo, come anello, all'immagine di ϕ, che è $\mathbb{Z}/(5)$.

- Si può ricordare che nel quoziente $\mathbb{Z}[i]/I$ ogni elemento è della forma $[r]$, dove r è (un) resto della divisione euclidea per $1-2i$ ed è 0 oppure un elemento di norma euclidea strettamente inferiore a 5. Gli elementi di questo tipo si scrivono tutti:

  $$0, \qquad \pm 1, \qquad \pm i, \qquad \pm(1+i), \qquad \pm(1-i), \qquad \pm 2, \qquad \pm 2i.$$

  Tali elementi, però, possono individuare la stessa classe di equivalenza. Ad esempio, $[1] = [2i]$ poiché $1-2i \in I$. Eliminando le ridondanze, si ottiene

  $$\mathbb{Z}[i] = \{[0],[1],[2],[i],[1+i]\}.$$

Risposta:

(a) $\mathbb{Z}[i]/I$ è un dominio? **SI** / **NO**. (b) $\mathbb{Z}[i]/I$ è un campo? **SI** / **NO**. (c) $\#(\mathbb{Z}[i]/I) =$ $\boxed{}$

Esercizio 4. Sia M il gruppo abeliano generato da quattro elementi x, y, z, w soggetti alle relazioni

$$\begin{aligned} x - y + 2z + 5w &= 0 \\ 2x + y + 4z + 10w &= 0 \end{aligned}$$

Identificare M (a meno di isomorfismo) come prodotto diretto di gruppi ciclici.

Soluzione:

M è isomorfo a $\mathbb{Z}^4/U$ dove U è il sottogruppo do $\mathbb{Z}^4$ generato da $(1, -1, 2, 5), (2, 1, 4, 10)$. Possiamo *diagonalizzare* il sottogruppo U come fatto a lezione:

$$\begin{pmatrix} 1 & 2 \\ -1 & 1 \\ 2 & 4 \\ 5 & 10 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 2 \\ 0 & 3 \\ 0 & 0 \\ 0 & 0 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 0 \\ 0 & 3 \\ 0 & 0 \\ 0 & 0 \end{pmatrix},$$

e ricavare che M è quindi isomorfo a $\mathbb{Z}/(1) \oplus \mathbb{Z}/(3) \oplus \mathbb{Z}/(0) \oplus \mathbb{Z}/(0) \simeq \mathbb{Z}^2 \oplus \mathbb{Z}/(3)$. Si può ovviamente sostituire il simbolo $\oplus$ di somma diretta di $\mathbb{Z}$-moduli con quello $\times$ di prodotto diretto di gruppi abeliani.

Risposta: $M \simeq$ $\boxed{}$

Esercizio 5. Mostrare che l'anello $A = \mathbb{Z}[x]/(3, x^3 + x^2 - 1)$ è un campo finito e determinarne il numero di elementi.

Soluzione:

Possiamo utilizzare i soliti teoremi di omomorfismo e isomorfismo per mostrare che A è isomorfo al quoziente $\mathbb{F}_3[x]/(x^3+x^2-1)$. Ad ogni modo, il polinomio $x^3+x^2-1 \in \mathbb{F}_3[x]$ è irriducibile poiché ha grado 3 e non possiede radici in $\mathbb{F}_3$. Ma allora l'ideale $(x^3 + x^2 - 1) \subset \mathbb{F}_3[x]$ è massimale e il corrispondente quoziente è un campo, i cui elementi sono univocamente rappresentati come classi di congruenza di polinomi di grado ≤ 2 a coefficienti in $\mathbb{F}_3$. Per individuare un elemento di $\mathbb{F}_3[x]/(x^3+x^2-1)$ vanno scelti i tre coefficienti di un tale polinomio in $\mathbb{F}_3$, e questo si può fare in $3^3 = 27$ modi. Il campo A possiede quindi 27 elementi.

Attenzione: mostrare che 3 è primo e $x^3 + x^2 - 1$ è irriducibile in $\mathbb{Z}[x]$ non conduce a molto. Ad esempio, 5 è primo e $x^2 + 1$ è irriducibile in $\mathbb{Z}[x]$; tuttavia, l'ideale $J = (5, x^2 + 1)$ non è massimale in $\mathbb{Z}[x]$ poiché è contenuto, ad esempio, in $(5, x - 2)$ come segue facilmente da

$$x^2 + 1 = (x^2 - 4) + 5 = (x + 2)(x - 2) + 5 \in (x - 2)\mathbb{Z}[i] + 5\mathbb{Z}[i] = (5, x - 2).$$

Risposta: $\#(A) =$ $\boxed{}$

Foglio per la brutta copia

Foglio per la brutta copia

Foglio per la brutta copia