Aritmetica - Simulazione Secondo Compitino

scritto da Alessandro Fenu, Alessio Sgubin

12 dicembre 2024

Motivare adeguatamente le vostre risposte, sia nella parte dei quiz che nella parte dimostrativa.

Avete a disposizione in totale 2 ore di tempo per la prova.

Esercizio 1 - Quiz
Consideriamo l'anello quoziente $\mathbb{Z}[x]/I$ dove $I = (x^3 - 3x^2 + 3x - 2)$.
Calcolare l'inverso dell'elemento $x^5 - 5x^4 + 10x^3 - 10x^2 + 5x - 1 + I$.

Esercizio 2 - Quiz
Scrivere l'ideale $I = (9 + i, 5i + 3)$ di $\mathbb{Z}[i]$ come ideale principale.

Esercizio 3 - Dimostrativo
Dire e motivare in modo dettagliato se i seguenti anelli sono isomorfi:

$$\mathbb{Z}_3[x]\big/(x^2+1) \quad \text{e} \quad \mathbb{Z}_3[x]\big/(x^2+x+1).$$

Esercizio 4 - Dimostrativo
Consideriamo l'anello $A = \mathbb{Z}[x] \times \mathbb{Z}[x]$ e presi due numeri $m, n \in \mathbb{Z} \setminus \{0\}$ definiamo

$$I_{m,n} := \Big\{(f(x), g(x)) \in A \text{ tali che } m \mid f(0) \text{ e } n \mid g(0)\Big\} \subseteq A.$$

Dimostrare:

a) che $I_{m,n}$ è un ideale di A.

b) per quali $m, n \in \mathbb{Z}$ il quoziente $A/I_{m,n}$ è un anello ciclico. [Ricordiamo che un anello si dice *ciclico* se è ciclico visto rispetto alla sua struttura additiva].

Soluzioni

Esercizio 1

Prima soluzione.
Notiamo preliminarmente che $x^3 - 3x^2 + 3x - 2$ si può scrivere come $(x-1)^3 - 1$ e dunque che $(x-1)^3 + I$ (come elemento del quoziente) è uguale a $1 + I$ (hanno differenza che appartiene all'ideale I).
Possiamo riscrivere $x^5 - 5x^4 + 10x^3 - 10x^2 + 5x - 1 + I$ come $(x-1)^5 + I$ e dunque, usando $(x-1)^3 + I = 1 + I$, otteniamo che è equivalente invertire $(x-1)^2 + I$.
Moltiplicando per $(x-1) + I$ si ha

$$(x - 1 + I)((x-1)^2 + I) = (x-1)^3 + I = 1 + I$$

dunque l'inverso cercato è proprio $(x-1) + I$.

Seconda soluzione.
Ricordiamo che in generale nell'anello quoziente $R[x]/(p(x))$ ogni elemento ammette un unico rappresentante di grado minore stretto di $\deg(p(x))$.
Possiamo ridurre il polinomio $x^5 - 5x^4 + 10x^3 - 10x^2 + 5x - 1$ eseguendo la divisione con resto:

$$x^5 - 5x^4 + 10x^3 - 10x^2 + 5x - 1 = (x^3 - 3x^2 + 3x - 2) \cdot (x^2 - 2x + 1) + \overbrace{x^2 - 2x + 1}^{\text{resto}}$$

e concentrarci dunque sul suo unico rappresentante nel quoziente di grado minore di 3, $x^2 - 2x + 1 + I$.
Per le stesse considerazioni fatte, possiamo supporre senza perdita di generalità che il suo inverso sia della forma $(ax^2 + bx + c) + I$, pertanto basterà risolvere

$$(x^2 - 2x + 1 + I) \cdot (ax^2 + bx + c + I) = 1 + I,$$

e svolgendo i conti, $a = 0, b = 1, c = -1$ va bene.
L'inverso cercato è dunque $(x-1) + I$. □

Esercizio 2

Vogliamo trovare un elemento $x \in \mathbb{Z}[x]$ (chiaramente non nullo) tale che $(x) = (9 + i, 5i + 3)$ in $\mathbb{Z}[i]$.
Dato che le condizioni di divisibilità in $\mathbb{Z}[i]$ implicano divisibilità tra le norme, sicuramente $|x|$ divide $\mathrm{MCD}(|9+i|, |5i+3|) = \mathrm{MCD}(82, 34) = 2$. Pertanto $|x| = 1$ (e dunque x è una unità) oppure $|x| = 2$, da cui $x = 1 + i$ a meno di associati.

Effettivamente $1 + i$ divide entrambi i generatori:

$$9 + i = (1 + i) \cdot (5 - 4i) \quad \text{e} \quad 5i + 3 = (1 + i) \cdot (i + 4)$$

Abbiamo appena dimostrato che x è un multiplo di $(1 + i)$ con norma al più 2.
Ma $1 + i$ ha già norma 2 quindi $(x) = (1 + i)$ e abbiamo concluso. □

Esercizio 3

Gli anelli del testo **non** sono isomorfi.
Un isomorfismo (in realtà basta morfismo iniettivo) di anelli f rispetta la seguente proprietà: se a, b sono elementi non nulli con prodotto 0 allora anche $f(a)$ ed $f(b)$ sono elementi non nulli (data l'iniettività) con prodotto 0 in arrivo.
Nel nostro caso, notiamo che:

- l'anello $\mathbb{Z}_3[x]/(x^2 + 1)$ è un dominio (è proprio un campo!) dato che $x^2 + 1$ è irriducibile in $\mathbb{Z}_3[x]$. Infatti, per polinomi di grado ≤ 3 la riducibilità è equivalente all'esistenza di radici nell'anello dei coefficienti, ma $x^2 + 1 = 0$ non ha soluzioni modulo 3.

- l'anello $\mathbb{Z}_3[x]/(x^2+x+1)$ **non** è un dominio: $x^2+x+1=(x-1)^2$ in $\mathbb{Z}_3[x]$ pertanto $(x-1)$ ed $(x-1)$ sono elementi che non appartengono alla classe di 0 ma con prodotto 0.

Per la considerazione di prima, un isomorfismo tra anelli stabilisce una bigezione tra i divisori di zero che però abbiamo dimostrato esistere in uno dei due anelli e non nell'altro: abbiamo concluso che gli anelli del testo non sono isomorfi (in particolare, abbiamo in realtà dimostrato che non esistono mappe iniettive non nulle $\mathbb{Z}_3[x]/(x^2+x+1) \hookrightarrow \mathbb{Z}_3[x]/(x^2+1)$). □

Esercizio 4

a) Dobbiamo verificare la chiusura per somma e per prodotto esterno.

- Dati $(f(x),g(x)),(f'(x),g'(x)) \in I_{m,n}$ anche la somma $(f(x)+f'(x),g(x)+g'(x)) \in I_{m,n}$: la valutazione in 0 della prima coordinata corrisponde alla somma delle valutazioni in 0 di $f(x)$ ed $f'(x)$, ambedue multipli di m. Analogamente per la seconda coordinata $\Rightarrow$ la somma rispetta la condizione di appartenenza ad $I_{m,n}$.

- Per il prodotto esterno procediamo similmente: dati $(f(x),g(x)) \in I_{m,n}$ e $(f'(x),g'(x)) \in \mathbb{Z}[x]\times\mathbb{Z}[x]$ il loro prodotto si scrive come $(f(x)\cdot f'(x), g(x)\cdot g'(x))$. La valutazione in 0 della prima coordinata è il prodotto $f(0)\cdot f'(0)$ che è multiplo di m visto che lo è $f(0)$. Analogamente per la seconda coordinata. Ne concludiamo la chiusura per prodotto esterno.

b) Dimostriamo anzitutto che $A/I_{m,n} \cong \mathbb{Z}_m \times \mathbb{Z}_m$.
Consideriamo l'omorfismo di anelli

$$A \xrightarrow{\Phi} \mathbb{Z}_m \times \mathbb{Z}_n$$

dato da $(f(x),g(x)) \mapsto (f(0),g(0))$. Questo omorfismo è chiaramente surgettivo, dato che ogni elemento $([a]_m,[b]_n) \in \mathbb{Z}_m\times\mathbb{Z}_n$ è, ad esempio, immagine della coppia (a,b) data da due polinomi costanti.
Per il primo teorema di isomorfismo otteniamo allora $A/\ker\Phi \cong \mathbb{Z}_m\times\mathbb{Z}_n$.

Studiamo $\ker\Phi$. Questo è composto da tutte le coppie di polinomi $(f(x),g(x)) \in A$ tali che $([f(0)]_m,[g(0)]_n) = ([0]_m,[0]_n)$, ossia dai polinomi $f(x)$ e $g(x)$ con termine noto divisibile rispettivamente per m ed n. Questa però è proprio la definizione di $I_{m,n}$. Segue che $A/I_{m,n} \cong \mathbb{Z}_m\times\mathbb{Z}_n$.

Per rispondere alla domanda del testo basta allora usare il teorema cinese del resto (o delle considerazioni sugli ordini additivi):

- Per m,n coprimi vale $\mathbb{Z}_m\times\mathbb{Z}_n \cong \mathbb{Z}_{m\cdot n}$, che è ciclico.

- Se invece $\mathrm{MCD}(m,n)=k\neq 1$ allora l'ordine (additivo) di qualsiasi elemento di $\mathbb{Z}_m\times\mathbb{Z}_n$ è minore o uguale di $\frac{m\cdot n}{k} < m\cdot n$ e pertanto l'anello non è ciclico (un anello ciclico avrebbe un elemento che ha ordine additivo pari alla cardinalità dell'anello).

Riassumendo, l'anello $A/I_{m,n}$ è ciclico se e solo se m,n sono coprimi. □