5.50

a) L'applicazione f è bigettiva, in quanto inversa di sé stessa. Infatti, per ogni $z \in \mathbb{C}$, si ha che $\overline{\overline{z}} = z$. Inoltre, per ogni $z, w \in \mathbb{C}$, si ha che (vedi le proprietà 1.9 f e g):

$$f(z+w) = \overline{z+w} = \overline{z} + \overline{w} = f(z) + f(w).$$
$$f(z \cdot w) = \overline{z \cdot w} = \overline{z} \cdot \overline{w} = f(z) \cdot f(w).$$

Ciò prova la proprietà di omomorfismo.

b) L'insieme $H = \{a + b\sqrt{2} | a, b \in \mathbb{Q}\}$ è non vuoto, in quanto vi appartiene $0 = 0 + 0 \cdot \sqrt{2}$. Siano ora $a, b, c, d \in \mathbb{Q}$. Allora

$$(a + b\sqrt{2}) - (c + d\sqrt{2}) = (a - c) + (b - d)\sqrt{2} \in H.$$
$$(a + b\sqrt{2}) \cdot (c + d\sqrt{2}) = (ac + 2bd) + (ad + bc)\sqrt{2} \in H.$$

Infatti, nei secondi membri, i numeri fra parentesi sono razionali. In base alla seconda caratterizzazione dei sottoanelli, se ne deduce che H è un sottoanello di $\mathbb{R}$.

Per quanto concerne f, osserviamo anzitutto che è un'applicazione ben definita. Infatti, per ogni elemento z di H, sono univocamente determinati i numeri razionali a e b tali che $z = a + b\sqrt{2}$. Se l'univocità venisse meno, e dunque esistesse una coppia $(c, d) \neq (a, b)$ di numeri razionali tali che $z = c + d\sqrt{2}$, allora si avrebbe $a - c = (d - b)\sqrt{2}$, da cui, non potendo essere $b = d$ (dato che, altrimenti, si avrebbe anche $a = c$), si ricava, dividendo entrambi i membri per $d - b$, che $\frac{a-c}{d-b} = \sqrt{2}$, impossibile, a fronte dell'irrazionalità di $\sqrt{2}$. La conservazione della somma si verifica facilmente. Proviamo la conservazione del prodotto. Siano ora $a, b, c, d \in \mathbb{Q}$. Allora

$$f((a + b\sqrt{2})(c + d\sqrt{2})) = f((ac + 2bd) + (ad + bc)\sqrt{2}) = (ac + 2bd) + (ad + bc)i,$$
$$f(a + b\sqrt{2}) f(c + d\sqrt{2}) = (a + bi)(c + di) = (ac - bd) + (ad + bc)i.$$

Notiamo che le due espressioni non hanno la stessa forma. Per confutare la proprietà di omomorfismo occorre però esibire un controesempio, ossia individuare particolari valori di a, b, c, d per i quali l'uguaglianza non è verificata. Basta determinarli in modo tale da rendere $2bd$ distinto da bd. Ciò si ottiene, ad esempio, prendendo $b = d = 1$ e $a = c = 0$. In effetti in tal caso si producono due elementi di H uguali a $\sqrt{2}$, e si constata che, da un lato, $f\left(\sqrt{2} \cdot \sqrt{2}\right) = f(2) = 2$, dall'altro, $f\left(\sqrt{2}\right) f\left(\sqrt{2}\right) = i \cdot i = -1$. Ciò ci consente di

concludere che f, pur essendo un omomorfismo di gruppi additivi, non è un omomorfismo di anelli. A parte, si può osservare che f è iniettivo ed ha come immagine l'insieme dei numeri complessi aventi parte reale e parte immaginaria razionale.

Domande supplementari: Gli anelli H e $\mathbb{C}$ sono isomorfi? L'anello H è un campo?

c) La verifica che $\mathbb{Z}[i]$ è un sottoanello unitario di $\mathbb{C}$ può essere facilmente effettuata sulla base della seconda caratterizzazione dei sottoanelli, insieme alla constatazione che $1 = 1 + 0 \cdot i \in \mathbb{Z}[i]$.
L'anello $\mathbb{Z}[i]$ non è un campo, ossia non è vero che tutti i suoi elementi non nulli siano invertibili. Ad esempio, non lo è 2: se esistesse un $\alpha \in \mathbb{Z}[i]$ tale che $2\alpha = 1$, allora, leggendo questa uguaglianza in $\mathbb{C}$, si dedurrebbe che necessariamente α coincide con $\frac{1}{2}$, un numero non appartenente a $\mathbb{Z}[i]$.
L'anello $\mathbb{Z}[i]$ non è isomorfo all'anello $\mathbb{Z}$: se lo fosse, allora, in base a quanto stabilito nell'Esercizio 5.49, sarebbero isomorfi i gruppi delle unità $\mathcal{U}(\mathbb{Z}[i])$ e $\mathcal{U}(\mathbb{Z})$. Ciò, tuttavia, non è possibile per motivi puramente insiemistici: i due gruppi, entrambi finiti, hanno ordini diversi. Infatti:

- $\mathcal{U}(\mathbb{Z}) = \{1, -1\}$ ha ordine 2;
- $\mathcal{U}(\mathbb{Z}[i])$ comprende almeno 4 elementi, ossia $1, -1, i, -i$: i primi due sono inversi di sé stessi, gli altri due sono uno l'inverso dell'altro. Ciò basterebbe per concludere. Possiamo però proseguire l'indagine, e chiederci se esistano altri elementi inveritibili nell'anello $\mathbb{Z}[i]$. Sia dunque $z = a + bi$, con $a, b \in \mathbb{Z}$. Se z è invertibile, allora esiste $w \in \mathbb{Z}[i]$ tale che $zw = 1$. Passando alle norme (ossia moltiplicando ciascun membro per il suo complesso coniugato), si ottiene $||z|| \cdot ||w|| = 1$ (infatti il primo membro, da $(zw)(\overline{zw})$, diverrebbe $(z\overline{z})(w\overline{w})$ in virtù della moltiplicatività del complesso coniugato). Ora $||z|| = a^2 + b^2$ è un intero positivo, e così è naturalmente anche $||w||$. Ne consegue che $||z|| = 1$. Ma allora uno tra a e b è 0, l' altro è 1 oppure -1. I possibili valori di z sono dunque i quattro suelencati. Abbiamo così provato che $\mathcal{U}(\mathbb{Z}[i]) = \{1, -1, i, -i\} = R_4$.