

Consideriamo gli insiemi

$$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$$

$$\mathbb{Q}(i) = \{a + bi \mid a, b \in \mathbb{Q}\}$$

**Esercizio:** Provare che  $\mathbb{Q}(\sqrt{2})$  e  $\mathbb{Q}(i)$  sono sottocampi di  $\mathbb{R}$  e di  $\mathbb{C}$ , rispettivamente.

Svolgimento: Proviamo solo la prima affermazione. Anzitutto osserviamo che, come è facile verificare,  $\mathbb{Q}(\sqrt{2})$  è un sottoanello di  $\mathbb{R}$ , quindi, in particolare, è commutativo. Inoltre è unitario, avendo come elemento neutro del prodotto il numero 1. Resta da verificare che ogni elemento non nullo di  $\mathbb{Q}(\sqrt{2})$  è invertibile in  $\mathbb{Q}(\sqrt{2})$ . In effetti, se  $(a, b) \neq (0, 0)$  è una coppia di numeri razionali, allora

$$(a + b\sqrt{2})^{-1} = \frac{a - b\sqrt{2}}{a^2 - 2b^2} = \frac{a}{a^2 - 2b^2} + \frac{-b}{a^2 - 2b^2}\sqrt{2} \in \mathbb{Q}(\sqrt{2}).$$

La seconda affermazione si prova in modo del tutto analogo.

**Esercizio:** Dire se i campi  $\mathbb{Q}(\sqrt{2})$  e  $\mathbb{Q}(i)$  sono anelli isomorfi.

Svolgimento: Se esiste un isomorfismo di anelli  $\varphi: \mathbb{Q}(\sqrt{2}) \rightarrow \mathbb{Q}(i)$ , allora  $\varphi(1) = 1$ , e quindi, applicando la conservazione della somma, si ricava che  $\varphi(2) = 2$ . Ma, d'altra parte, la conservazione del prodotto fornisce  $2 = \varphi(\sqrt{2} \cdot \sqrt{2}) = \varphi(\sqrt{2})^2$ , il che è assurdo, dato che in  $\mathbb{Q}(i)$  non esistono radici quadrate di 2. Ciò prova che i due campi non sono anelli isomorfi.

Osservazioni aggiuntive:

1.) Allo stesso modo si prova che  $\mathbb{Q}(\sqrt{2})$  non è isomorfo al seguente sottocampo di  $\mathbb{R}$ :

$$\mathbb{Q}(\sqrt{3}) = \{a + b\sqrt{3} \mid a, b \in \mathbb{Q}\}.$$

2.) Lo stesso ragionamento dimostrativo consente anche di concludere che i campi  $\mathbb{Q}(\sqrt{2})$  e  $\mathbb{C}$  non sono isomorfi. A tale conclusione si può giungere per altro anche più direttamente, su basi insiemistiche, considerando che diverse sono le cardinalità, rispettivamente numerabile e più che numerabile.

Domanda supplementare: Sono isomorfi gli anelli  $2\mathbb{Z}$  e  $3\mathbb{Z}$ ? Sono isomorfi gli anelli  $n\mathbb{Z}$  e  $m\mathbb{Z}$ , ove  $n$  e  $m$  sono numeri naturali distinti?

Siano  $n, m$  numeri naturali e sia  $f : n\mathbb{Z} \rightarrow m\mathbb{Z}$  un omomorfismo di anelli. Sia  $a \in \mathbb{Z}$  tale che  $f(n) = ma$ . Allora, per la conservazione della somma, si avrà che

$$f(n^2) = f(\underbrace{n + \cdots + n}_{n \text{ volte}}) = \underbrace{f(n) + \cdots + f(n)}_{n \text{ volte}} = nf(n) = n(ma)$$

D'altra parte, dato che  $f$  conserva anche il prodotto, si avrà anche:

$$f(n^2) = f(n \cdot n) = f(n)f(n) = f(n)^2 = (ma)^2.$$

Sarà dunque  $n(ma) = (ma)(ma)$ . Se fosse  $a = 0$ , allora sarebbe  $f(n) = 0$  e quindi per ogni  $b$  intero positivo si avrebbe, per la conservazione della somma, analogamente a quanto visto sopra,

$$f(bn) = bf(n) = 0.$$

Inoltre, per ogni  $b$  intero negativo, si avrebbe, per la conservazione degli opposti e della somma,

$$-f(bn) = f(-bn) = f((-b)n) = (-b)f(n) = 0.$$

Ciò prova che, per ogni intero  $b$ ,  $f(bn) = 0$ , ossia  $f$  sarebbe l'omomorfismo nullo. In caso contrario,  $ma \neq 0$ , e pertanto, cancellando  $ma$  dall'uguaglianza qui sopra si ottiene  $n = ma$ . Ne consegue che  $m$  divide  $n$ . Questa è dunque condizione necessaria all'esistenza di un omomorfismo di anelli non nullo  $f : n\mathbb{Z} \rightarrow m\mathbb{Z}$ . In particolare, se esiste un isomorfismo di anelli  $f$ , allora  $m|n$  e, per simmetria,  $n|m$ . Quindi gli anelli  $n\mathbb{Z}$  e  $m\mathbb{Z}$  sono isomorfi solo se  $n = m$ , ossia solo se sono uguali.