

Capitolo 2

Seconda Lezione - Esercizi

Osservazione 2.1. [CCY37] *Siano*

$$\begin{array}{ccc} F: & \mathbb{R} & \rightarrow \mathbb{R} \\ & a & \mapsto a^2 \end{array} \quad \begin{array}{ccc} G: & \mathbb{R} & \rightarrow \mathbb{R} \\ & t & \mapsto 3t - 2 \end{array}$$

due funzioni di $\mathcal{F} = \{f: \mathbb{R} \rightarrow \mathbb{R}\}$ Allora

$$(F \circ G)(5) = F(G(5)) = F(3 \cdot 5 - 2) = F(13) = 169$$

$$(F \circ G)(x) = F(G(x)) = F(3x - 2) = (3x - 2)^2 = 9x^2 - 12x + 4$$

$$(F \circ G)(x - 5) = F(G(x - 5)) = F(3(x - 5) - 2) = (3x - 17)^2 = 9x^2 - 102x + 289$$

$$(F \circ G)(\spadesuit) = F(G(\spadesuit)) = F(3\spadesuit - 2) = (3\spadesuit - 2)^2 = 9\spadesuit^2 - 12\spadesuit + 4$$

2.1 Esercizi svolti

Esercizio 2.2. [AAX04] *Dire per quali $a \in \mathbb{R}$, i polinomi $x^2 + 4x - 1$, $ax^2 + (3a - 1)x + 5a \in \mathbb{R}[x]$ sono uguali.*

I polinomi hanno lo stesso grado. Per avere $x^2 + 4x - 1 \stackrel{\mathbb{R}[x]}{=} ax^2 + (3a - 1)x + 5a$ dobbiamo avere che i coefficienti dei termini dello stesso grado sono uguali uno a uno, ovvero

$$\begin{cases} 1 = a & \text{grado } 2 \\ 4 = 3a - 1 & \text{grado } 1 \\ -1 = 5a & \text{grado } 0 \end{cases}$$

Dato che dalla prima equazione si ottiene $a = 1$ e dalla terza $a = -\frac{1}{5}$, il sistema è impossibile e i polinomi sono diversi per ogni $a \in \mathbb{R}$ ($\forall a \in \mathbb{R}$).

Proposizione 2.3. [BBB08] *Sia A un anello, allora se $a \in A$ è uno zero divisore, a non è invertibile. Quindi un campo non ha zero divisori, dato che ricordiamo che logicamente $P \Rightarrow Q$ implica $\neg Q \Rightarrow \neg P$, dove P, Q sono proposizioni logiche e $\neg$ la negazione logica*

Dimostrazione. Sia $a \in A$ zero divisore. Allora esiste $b \in A$, $b \neq 0$ tale che $a \cdot b = 0$. Supponiamo per assurdo che a sia invertibile. Allora esiste $a^{-1} \in A$ tale che $a^{-1} \cdot a = 1$. Quindi

$$\begin{aligned} a \cdot b &= 0 \\ a^{-1} \cdot a \cdot b &= a^{-1} \cdot 0 \\ 1 \cdot b &= 0 \\ b &= 0 \end{aligned}$$

Ed abbiamo ottenuto $b = 0$ contro l'ipotesi. Questa è una contraddizione (un assurdo) e quindi è assurdo supporre che a sia invertibile. Quindi a non è invertibile. $\square$

Proposizione 2.4 (Legge di cancellazione per campi). [BBX08] *Sia $\mathbb{K}$ un campo, e $a, b, c \in \mathbb{K}$, $a \neq 0$. Allora $ab = ac \Leftrightarrow b = c$.*

Dimostrazione. Dato che $a \neq 0$, $\exists a^{-1}$, quindi

$$ab = ac \Leftrightarrow a^{-1}ab = a^{-1}ac \Leftrightarrow b = c$$

$\square$

Se indeboliamo l'ipotesi, prendendo un anello, la legge di cancellazione continua a valere per i non zero divisori.

Proposizione 2.5 (Legge di cancellazione per anelli). [BBX77] *Sia A un anello, e $a, b, c \in A$, $a \neq 0$, e a non zero divisore. Allora $ab = ac \Leftrightarrow b = c$.*

Dimostrazione.

$$ab = ac \Leftrightarrow ab - ac = 0 \Leftrightarrow a(b - c) = 0. \text{ Quindi } b - c = 0 \text{ o } b - c \text{ zero-divisore}$$

Da cui

- Se $b - c \neq 0$, allora $b - c$ è zero-divisore e quindi lo è anche a , contro l'ipotesi. Quindi $b - c = 0$.
- Se $b - c = 0$ abbiamo $b = c$, tesi.

$\square$

Proposizione 2.6 (Unicità dell'inverso). [BBX88] *Sia A un anello, e $a \in A$ invertibile e $b, c \in A$ tali che*

$$ab = ba = 1 \quad ac = ca = 1$$

Allora $b = c$.

Dimostrazione. Per semplicità supponiamo che A sia commutativo. Per A non commutativo la dimostrazione è lasciata per esercizio.

$$ab = 1 \text{ AND } ac = 1 \Rightarrow ab = ac \Rightarrow ab - ac = 0 \Rightarrow a(b - c) = 0$$

Dato che a è invertibile, a non è zero divisore, e quindi non lo è neppure $b - c$. Quindi $a = 0$ o $b - c = 0$. MA dato che a è invertibile, $a \neq 0$ e quindi

$$b - c = 0 \Rightarrow b = c$$

$\square$

N.B. Potevamo semplificare l'ultima parte del ragionamento usando la legge di cancellazione.

Esercizio 2.7. [AAV89]

Dire per quali $a, b \in \mathbb{Q}$ i polinomi $f(x) = ax^3 + (a+b)x^2 + 3$, $g(x) = 3x^3 + (a-b)x^2 + a$ in $\mathbb{Q}[x]$ sono uguali.

Soluzione. Usiamo il principio di identità dei polinomi

$$ax^3 + (a+b)x^2 + 3 \equiv_{\mathbb{Q}[x]} 3x^3 + (a-b)x^2 + a$$

$$\begin{cases} a = 3 \\ a + b = a - b \\ 0 = 0 \\ 3 = a \end{cases} \Leftrightarrow \begin{cases} a = 3 \\ b = 0 \end{cases}$$

□

Esercizio 2.8. [AAA94] Risolvere l'equazione

$$F(x)^2 \equiv_{\mathbb{R}[x]} x^2 + 3x + 2$$

con incognita il polinomo $F(x)$. Stiamo cercando le soluzioni tra i polinomi, ovvero vogliamo determinare l'insieme

$$\{F(x) \in \mathbb{R}[x] \mid F(x)^2 \equiv_{\mathbb{R}[x]} x^2 + 3x + 2\}$$

Dato che il quadrato di $F(x)$ ha grado 2, necessariamente $F(x)$ ha grado 1. Quindi $F(x) = ax + b$ per opportuni (ed incogniti) $a, b \in \mathbb{R}$. Possiamo quindi riscrivere l'equazione

$$\begin{aligned} F(x)^2 &\equiv_{\mathbb{R}[x]} x^2 + 3x + 2 \\ (ax + b)^2 &\equiv_{\mathbb{R}[x]} x^2 + 3x + 2 \\ a^2x^2 + 2abx + b^2 &\equiv_{\mathbb{R}[x]} x^2 + 3x + 2 \end{aligned}$$

che per il principio di identità dei polinomi si trasforma in

$$\begin{cases} a^2 = 1 \Rightarrow a = \pm 1 \\ 2ab = 3 \\ b^2 = 2 \Rightarrow b = \pm\sqrt{2} \end{cases}$$

e si vede facilmente che in tutti e quattro i casi $(a = 1, b = \sqrt{2}), \dots, (a = -1, b = -\sqrt{2})$ la seconda equazione è impossibile. Quindi

$$F(x)^2 \equiv_{\mathbb{R}[x]} x^2 + 3x + 2$$

non ha soluzioni.

Esercizio 2.9. [AAP94] Data $\alpha \in \mathbb{K}$, campo, risolvere l'equazione

$$3xF(x+2) \equiv_{\mathbb{K}[x]} 3x^2 + 3x + \alpha$$

con incognita il polinomio $F(x)$. Ricordiamo che α è dato, quindi parametro. Stiamo cercando le soluzioni tra i polinomi, ovvero vogliamo determinare l'insieme

$$\{F(x) \in \mathbb{K}[x] \mid 3xF(x+2) \equiv_{\mathbb{K}[x]} 3x^2 + 3x + \alpha\}$$

Il grado di $F(x+2)$ è uguale al grado di $F(x)$, e per le regole sul grado del prodotto di polinomi $xF(x+2)$ deve avere grado 2 perché l'equazione abbia soluzione. Quindi $F(x)$ ha grado 1 e $F(x) \equiv_{\mathbb{K}[x]} ax + b$ per opportuni (ed incogniti) $a, b \in \mathbb{K}$. Possiamo, ricordando che

$$F(x+2) \equiv_{\mathbb{K}[x]} a(x+2) + b \equiv_{\mathbb{K}[x]} ax + 2a + b$$

Usando il principio di identità dei polinomi, l'equazione su polinomi diviene il seguente sistema su $\mathbb{K}$

$$\begin{aligned} 3xF(x+2) &\equiv_{\mathbb{K}[x]} 3x^2 + 3x + \alpha \\ 3x(ax + 2a + b) &\equiv_{\mathbb{K}[x]} 3x^2 + 3x + \alpha \\ 3ax^2 + 6ax + 3bx &\equiv_{\mathbb{K}[x]} 3x^2 + 3x + \alpha \\ 3ax^2 + (6a + 3b)x &\equiv_{\mathbb{K}[x]} 3x^2 + 3x + \alpha \end{aligned}$$

che per il principio di identità dei polinomi si trasforma in

$$\begin{cases} 3a = 3 \Rightarrow a = 1 \\ 6a + 3b = 3 \\ 0 = \alpha \end{cases} \Leftrightarrow \begin{cases} a = 1 \\ 6 + 3b = 3 \Rightarrow b = -1 \\ 0 = \alpha \end{cases}$$

e quindi

- Se $\alpha \neq 0$ non esiste soluzione ($\nexists$ soluzione).
- Se $\alpha = 0$ allora la soluzione è $F(x) \equiv_{\mathbb{K}[x]} x - 1$

Verifichiamo per scrupolo nel caso $\alpha = 0$

$$3xF(x+2) \equiv_{\mathbb{K}[x]} 3x((x+2) - 1) = 3x(x+1) \equiv_{\mathbb{K}[x]} 3x^2 + 3x + \alpha \text{ con } \alpha = 0$$

Proposizione 2.10. [BBB01] Dato un'entità i tale che $i^2 = -1$, definiamo l'insieme $\mathbb{R}[i] = \{a + ib \mid a, b \in \mathbb{R}\}$. Questo è un campo con le ovvie operazioni:

$$a + ib \equiv_{\mathbb{R}[i]} 0 \Leftrightarrow a = b = 0 \Leftrightarrow (a, b) = (0, 0)$$

$0 \equiv_{\mathbb{R}[i]} 0 + 0i$ è il neutro additivo, $1 \equiv_{\mathbb{R}[i]} 1 + 0i$ è il neutro moltiplicativo,

$$\begin{aligned} +: \quad \mathbb{R}[i] \times \mathbb{R}[i] &\rightarrow \mathbb{R}[i] \\ a + ib, c + id &\mapsto a + c + i(b + d) \end{aligned}$$

e

$$\begin{aligned} \cdot: \quad \mathbb{R}[i] \times \mathbb{R}[i] &\rightarrow \mathbb{R}[i] \\ (a + ib, c + id) &\mapsto (a + ib) \cdot (c + id) \equiv_{\mathbb{R}[i]} ac - bd + i(ad + bc) \end{aligned}$$

Ricordiamo che $i^2 = -1$.

Dimostrazione. Verifichiamo che $(\mathbb{R}[i], +, \cdot)$ sia un anello controllando le proprietà una per una:

1. Dimostriamo che se $a, b \in \mathbb{R}$, $a + ib \equiv_{\mathbb{R}[i]} 0 \Leftrightarrow a = b = 0$. Infatti, se $b \neq 0$

$$a + ib \equiv_{\mathbb{R}[i]} 0 \Rightarrow i = -\frac{a}{b} \in \mathbb{R} \text{ assurdo}$$

Se invece $b = 0$

$$a + ib \equiv_{\mathbb{R}[i]} 0 \Rightarrow a = 0$$

ed abbiamo $a = b = 0$. Notiamo che due numeri complessi $a + ib$, $c + id$ sono uguali se e solo se $a = c$ e $b = d$.

2. Verifichiamo che $(\mathbb{R}[i], +)$ sia un gruppo abeliano

- (a) L'insieme $\mathbb{R}[i]$ è chiuso rispetto all'operazione $+$, dato che per ogni due elementi $(a + ib), (c + id) \in \mathbb{R}[i]$ abbiamo che

$$(a + ib) + (c + id) \equiv_{\mathbb{R}[i]} (a + c) + i(b + d) \in \mathbb{R}[i]$$

con $a + c, b + d \in \mathbb{R}$. Notiamo che l'operazione $+$ è commutativa, ovvero che per ogni due elementi $(a + ib), (c + id) \in \mathbb{R}[i]$ ($a, b, c, d \in \mathbb{R}$) abbiamo che

$$(a + ib) + (c + id) \equiv_{\mathbb{R}[i]} (a + c) + i(b + d) \equiv_{\mathbb{R}[i]} (c + a) + i(d + b) = (c + id) + (a + ib)$$

sfruttando la commutatività della somma sui reali.

- (b) Esiste il neutro additivo $0 + i0 = 0$, tale che

$$\forall a + ib \in \mathbb{R}[i] \quad (a + ib) + 0 \equiv_{\mathbb{R}[i]} a + ib$$

- (c) Ogni elemento di $\mathbb{R}[i]$ ha inverso additivo (che chiamiamo opposto). Infatti

$$\forall a + ib \in \mathbb{R}[i] \quad \exists x + iy \in \mathbb{R}[i] \text{ tale che } (a + ib) + (x + iy) \equiv_{\mathbb{R}[i]} 0$$

basta prendere come $x + iy$ l'elemento $-a + i(-b) \equiv_{\mathbb{R}[i]} -a - ib$, sfruttando gli opposti in $\mathbb{R}$.

Quindi $(\mathbb{R}[i], +)$ è un gruppo abeliano.

3. L'insieme $\mathbb{R}[i]$ è chiuso rispetto all'operazione $\cdot$, dato che per ogni due elementi $(a + ib), (c + id) \in \mathbb{R}[i]$ ($a, b, c, d \in \mathbb{R}$) abbiamo che

$$(a + ib) \cdot (c + id) \equiv_{\mathbb{R}[i]} ac + iad + ibc + i^2bd \equiv_{\mathbb{R}[i]} (ac - bd) + i(ad + bc) \in \mathbb{R}[i]$$

con $ac - bd, ad + bc \in \mathbb{R}$. Notiamo che l'operazione $\cdot$ è commutativa, ovvero che per ogni due elementi $(a + ib), (c + id) \in \mathbb{R}[i]$ abbiamo che

$$(a + ib) \cdot (c + id) \equiv_{\mathbb{R}[i]} (ac - bd) + i(ad + bc) \equiv_{\mathbb{R}[i]} (c + id) \cdot (a + ib)$$

sfruttando la commutatività del prodotto sui reali.

4. Esiste il neutro moltiplicativo $1 + i0 \equiv_{\mathbb{R}[i]} 1$, tale che

$$\forall a + ib \in \mathbb{R}[i] \quad (a + ib) \cdot 1 \equiv_{\mathbb{R}[i]} a \cdot 1 + ib \cdot 1 \equiv_{\mathbb{R}[i]} a + ib$$

5. Verifichiamo la commutatività del prodotto

$$\forall a + ib, c + id \in \mathbb{R}[i] \quad (a + ib) \cdot (c + id) \underset{\mathbb{R}[i]}{\equiv} (c + id) \cdot (a + ib)$$

Infatti

$$(a + ib) \cdot (c + id) \underset{\mathbb{R}[i]}{\equiv} ac - bd + i(ad + bc)$$

e

$$(c + id) \cdot (a + ib) \underset{\mathbb{R}[i]}{\equiv} ca + icb + ida + i^2db \underset{\mathbb{R}[i]}{\equiv} ca - db + i(cb + da) \underset{\mathbb{R}[i]}{\equiv} ac - bd + i(ad + bc)$$

dato che $\mathbb{R}$ è commutativo.

6. Verifichiamo la distributività:

$$\begin{aligned} (a + bi) \cdot ((c + id) + (e + if)) &\underset{\mathbb{R}[i]}{\equiv} (a + ib)(c + e + (d + f)i) \\ &\underset{\mathbb{R}[i]}{\equiv} ac - bd + ae - bf + (bc + ad + be + af)i \\ (a + bi) \cdot (c + id) + (a + bi) \cdot (e + if) &\underset{\mathbb{R}[i]}{\equiv} ac - bd + (bc + ad)i + ae - bf + (be + af)i \\ &\underset{\mathbb{R}[i]}{\equiv} ac - bd + ae - bf + (bc + ad + be + af)i \end{aligned}$$

Rimane da verificare che $\mathbb{R}[i]$ sia un campo, ovvero che tutti gli elementi non nulli abbiano inverso. Vediamo che dato $a + ib \in \mathbb{R}[i]$, non nullo ($(a, b) \neq (0, 0)$) esiste $x + iy \in \mathbb{R}[i]$ tale che $(a + ib)(x + iy) \underset{\mathbb{R}[i]}{\equiv} 1$. Proviamo facilmente che se $a + ib \underset{\mathbb{R}[i]}{\neq} 0 \Leftrightarrow (a, b) \neq (0, 0) \Leftrightarrow a^2 + b^2 \neq 0$, ponendo

$$x + iy \underset{\mathbb{R}[i]}{\equiv} \frac{a - ib}{a^2 + b^2} \underset{\mathbb{R}[i]}{\equiv} \frac{a}{a^2 + b^2} - i \frac{b}{a^2 + b^2}$$

abbiamo che

$$(a + ib) \cdot \frac{a - ib}{a^2 + b^2} \underset{\mathbb{R}[i]}{\equiv} \frac{a^2 + aib - iba - i^2b^2}{a^2 + b^2} \underset{\mathbb{R}[i]}{\equiv} \frac{a^2 + b^2}{a^2 + b^2} = 1$$

Quindi $\frac{a - ib}{a^2 + b^2}$ è l'inverso moltiplicativo di $a + ib$. Indichiamo l'inverso moltiplicativo di $a + ib$ come

$$(a + ib)^{-1} \underset{\mathbb{R}[i]}{\equiv} \frac{1}{a + ib} \underset{\mathbb{R}[i]}{\equiv} \frac{a - ib}{a^2 + b^2}$$

□

Esempio 2.11. [AAP66] Calcoliamo l'inverso di $2 - 3i$

$$(2 - 3i)^{-1} \underset{\mathbb{R}[i]}{\equiv} \frac{2 + 3i}{2^2 + 3^2} \underset{\mathbb{R}[i]}{\equiv} \frac{2 + 3i}{13} \underset{\mathbb{R}[i]}{\equiv} \frac{2}{13} + \frac{3}{13}i$$

Esempio 2.12. [AAQ66] Nel piano cartesiano $\mathbb{R}^2$, i vettori $\underline{v}$ dall'origine sono un gruppo commutativo con la somma secondo la regola del parallelogramma e elemento neutro $\underline{0}$. L'inverso (additivo) di $\underline{v}$ è $-\underline{v}$.

In futuro, quando non sia necessario specificare l'anello od il campo che stiamo usando, con lieve abuso di notazione, scriveremo spesso $\equiv$ o anche $=$ per anelli e campi.

2.2 Esercizi proposti

Esercizio 2.13. [AAU66] Nel piano cartesiano $\mathbb{R}^2$, i vettori $\underline{v}$ dall'origine sono un gruppo commutativo con la somma secondo la regola del parallelogramma ed elemento neutro $\underline{0}$. L'inverso (additivo) di $\underline{v}$ è $-\underline{v}$.

Esercizio 2.14. [AAQ10] Dire, al variare di $a, b, c, d \in \mathbb{R}$, quando sono uguali i polinomi

$$3(a - b + 2c)x^2 - (a + b)x - a + b - c, \quad (a + b + c - d)x^3 + 2x^2 - (2a + b - c)x + 3$$

Esercizio 2.15. [NN02] Risolvere la seguente equazione a variable polinomio $F(x)$

$$F(x) \cdot F(x+1) \underset{\mathbb{Q}[x]}{\equiv} x^4 + 6x^3 + 15x^2 + 18x + 10$$

Hint: il grado del polinomio $F(x)$ è uguale al grado del polinomio $F(x+1)$. Dato che il prodotto di questi due polinomi ha grado 4, $\deg F(x) = 2$ e quindi $F(x) \underset{\mathbb{Q}[x]}{\equiv} ax^2 + bx + c$ per incogniti $a, b, c \in \mathbb{Q}$.

Soluzione: $F(x) \underset{\mathbb{Q}[x]}{\equiv} \pm(x^2 + 2x + 2)$.

Esercizio 2.16. [AAX94] Trovare un polinomio $F(y) \in \mathbb{R}[y]$ tale che $F(y)(3y^2 + 1) \equiv 3y^4 + 4y^2 + 1$

Esercizio 2.17. [NNT02] Risolvere le seguenti equazioni a variable polinomi in $F(x)$

- $F(x) \underset{\mathbb{Q}[x]}{\equiv} F(x+3)$
- $F(x^2) \underset{\mathbb{Q}[x]}{\equiv} F(x)$
- $F(x^2) \underset{\mathbb{Q}[x]}{\equiv} F(x)^2$
- $3F(x^2 + 2) \underset{\mathbb{Q}[x]}{\equiv} F(3x^2 - 1)$

Esercizio 2.18. [AAX96] Trovare un polinomio $F(t) \in \mathbb{R}[t]$ tale che $3F(t) + t^2 \equiv 3t^4 - 2t^2 + 3t$

Esercizio 2.19 (Astratto). [AAY23] Esiste un campo $\mathbb{K}$ con un numero finito di elementi?

Esercizio 2.20 (Astratto). [AAX33] Trovare, se possibile, un campo finito con 5 elementi.

Esercizio 2.21 (Astratto). [AAX22] Trovare, se possibile, un campo finito con 4 elementi.

Osservazione 2.22. [AAP23] Dato $(\mathbb{K}, +, \cdot)$ campo, un insieme $A \subseteq \mathbb{K}$ si dice sottocampo di $\mathbb{K}$ se è chiuso rispetto alle operazioni $+, \cdot$. Per esempio, $\mathbb{Q}$ è un sottocampo di $\mathbb{R}$ che è un sottocampo di $\mathbb{C}$.

Esercizio 2.23. [AAG23] Trovare, se esistono, due sottocampi non banali di $\mathbb{R}$ diversi da $\mathbb{Q}$ e contenuti l'uno dentro l'altro.

Esercizio 2.24. [AAG22] Trovare, se esiste, un sottocampo non banale di $\mathbb{Q}$.

Esercizio 2.25. [AAT23] Trovare, se esiste, un campo B tale che $\mathbb{Q} \subsetneq B \subsetneq \mathbb{R}$.

Esercizio 2.26 (Difficile). [AAA23] L'insieme

$$\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\} \subset \mathbb{R}$$

è un sottocampo di $(\mathbb{R}, +, \cdot)$ che contiene $\mathbb{Q}$? Determinare se del caso il principio di identità e la formula dell'inverso.