# NOTE DI ALGEBRA LINEARE 2010-11

M.M. 1 NOVEMBRE 2010

## 1. Esercizi sui campi di numeri

Nel seguito indicheremo con $\mathbb{Q}, \mathbb{R}$ e $\mathbb{C}$ gli insiemi dei numeri razionali, reali e complessi rispettivamente. Un asterisco denota gli esercizi non banali.

**Esercizio 1.1.** Siano $p, q$ interi positivi senza fattori comuni. Provare che $\sqrt{\frac{p}{q}} = \frac{\sqrt{p}}{\sqrt{q}}$ è un numero razionale se e solo se $p, q$ sono due quadrati.

**Esercizio 1.2** $(*)$**.** Dato un numero razionale $b \in \mathbb{Q}$ denotiamo $L(b) = \{r \in \mathbb{Q} \mid r < b\}$.

Diremo che un sottoinsieme $A \subset \mathbb{Q}$ è un *aperto iniziale* se per ogni $a \in A$ esiste $b \in \mathbb{Q}$ tale che $a \in L(b) \subset A$. Dimostrare:

(1) Se $\alpha$ è un numero reale, allora l'insieme $A = \{a \in \mathbb{Q} \mid a < \alpha\}$ è un aperto iniziale.
(2) Intersezione di due aperti iniziali è ancora un aperto iniziale.
(3) Unione di aperti iniziali è ancora un aperto iniziale.
(4) Dati due aperti iniziali $A, B$, l'insieme
$$A + B = \{a + b \mid a \in A, b \in B\}$$
è ancora un aperto iniziale.
(5) Dato un aperto iniziale $A$, l'insieme $-A$ definito come
$$-A = \{x \in \mathbb{Q} \mid \text{esiste } n > 0 \text{ tale che } x + a + \frac{1}{n} < 0 \text{ per ogni } a \in A\},$$
è ancora un aperto iniziale.
(6) Nelle notazioni precedenti, se $A, B$ sono aperti iniziali allora
$$B + (-A) = \{x \in \mathbb{Q} \mid \text{esiste } n > 0 \text{ tale che } x + a + \frac{1}{n} \in B \text{ per ogni } a \in A\}.$$

**Esercizio 1.3.** Siano $z, w$ due numeri complessi tali che $z^2 = w^2$. Mostrare che $z = \pm w$.

**Esercizio 1.4** $(*)$**.** Siano $\xi_k = \cos(2k\pi/n) + i\sin(2k\pi/n)$, $k = 0, \ldots, n-1$, le radici $n$-esime di 1, ossia le soluzioni dell'equazione $z^n = 1$. Dimostrare che vale
$$z^n - 1 = (z - \xi_0)(z - \xi_1)\cdots(z - \xi_{n-1})$$
e determinare il valore dei prodotti
$$(z + \xi_0)(z + \xi_1)\cdots(z + \xi_{n-1}), \qquad (z - \xi_0^2)(z - \xi_1^2)\cdots(z - \xi_{n-1}^2).$$

**Definizione 1.5.** Un **campo di numeri** $\mathbb{K}$ è un **sottocampo** di $\mathbb{C}$, ossia un sottoinsieme che contiene $0, 1$ e che è chiuso per le operazioni di somma, prodotto, opposto ed inverso di numeri diversi da 0.

In altri termini, un campo di numeri è un sottoinsieme $\mathbb{K} \subset \mathbb{C}$ che soddisfa le seguenti proprietà:

(1) $0, 1 \in \mathbb{K}$.
(2) Se $z, w \in \mathbb{K}$, allora $z + w, zw \in \mathbb{K}$.
(3) Se $z \in \mathbb{K}$ allora $-z \in \mathbb{K}$ e se $z \neq 0$, allora $z^{-1} \in \mathbb{K}$.

**Esercizio 1.6.** Dimostrare che un sottoinsieme $\mathbb{K}$ di $\mathbb{C}$ è un campo di numeri se e solo se soddisfa le seguenti condizioni:

(1) $1 \in \mathbb{K}$;
(2) se $z, w \in \mathbb{K}$ e $w \neq 0$ allora $z - w, \dfrac{z}{w} \in \mathbb{K}$.

Ad esempio $\mathbb{Q}, \mathbb{R}$ e $\mathbb{C}$ sono campi di numeri. Se $p$ è un numero primo, allora l'insieme

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

è un campo di numeri. Si dimostra immediatamente che $\mathbb{Q}(\sqrt{p})$ contiene $0, 1$ ed è chiuso per somma, prodotto ed opposto. L'unica verifica non banale riguarda l'esistenza dell'inverso. Si consideri un numero $x = a + b\sqrt{p}$ con $a, b$ non entranbi nulli; il prodotto

$$(a + b\sqrt{p})(a - b\sqrt{p}) = a^2 - b^2 p$$

è diverso da 0, altrimenti si avrebbe $a^2 = b^2 p$ e quindi $p = (a/b)^2$ che abbiamo visto non essere possibile. In particolare $x \neq 0$ e

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

**Esercizio 1.7.** Scrivere i seguenti numeri nella forma $a + b\sqrt{2}$:

$$(1 + \sqrt{2})^3, \quad \frac{2 - \sqrt{2}}{3 + 2\sqrt{2}}, \quad \frac{1 + \sqrt{2}}{1 - \sqrt{2}}.$$

**Esercizio 1.8.** Risolvere il seguente sistema lineare a coefficienti nel campo $\mathbb{Q}(\sqrt{3})$.

$$\begin{cases} x + y + z = 1 \\ x + \sqrt{3}\, y + 2z = 0 \\ x + 3y + 4z = -1 \end{cases}$$

**Esercizio 1.9.** Un numero intero $m \neq 0$ si dice ridotto se non è divisibile per quadrati di numeri primi. Sono ridotti i numeri $2, 3, 5, 6, 7, 10, 11, 13, 14 \ldots$, mentre non sono ridotti i numeri $4, 8, 9, 12, \ldots$. Dimostrare che se $m$ è ridotto, allora

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

è un campo di numeri.

**Esercizio 1.10.** Mostrare che ogni sottocampo di $\mathbb{C}$ contiene tutti i numeri razionali.

**Esercizio 1.11.** Mostrare che l'intersezione di sottocampi di $\mathbb{C}$ è ancora un sottocampo di $\mathbb{C}$.

**Esercizio 1.12.** Verificare che l'insieme

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

è un campo di numeri. Più in generale se $\xi \in \mathbb{C}$ è un numero complesso tale che $\xi^2 \in \mathbb{Q}$ e $\xi \notin \mathbb{Q}$, allora

$$\mathbb{Q}(\xi) = \{a + b\xi \in \mathbb{C} \mid a, b \in \mathbb{Q}\}$$

è un campo di numeri.

Possiamo generalizzare la precedente costruzione nel modo seguente. Sia $\mathbb{K} \subset \mathbb{C}$ un campo di numeri e sia $\alpha$ un numero complesso tale che $\alpha^2 \in \mathbb{K}$. Allora l'insieme $\mathbb{K}(\alpha) = \{a + b\alpha \mid a, b \in \mathbb{K}\}$ è ancora un campo; per dimostrarlo occorre trattare separatemante i due casi $\alpha \in \mathbb{K}$ e $\alpha \notin \mathbb{K}$.

Se $\alpha \in \mathbb{K}$ allora, siccome $\mathbb{K}$ è un campo, ne segue che ogni elemento del tipo $a + b\alpha$ appartiene ancora a $\mathbb{K}$, ossia $\mathbb{K}(\alpha) = \mathbb{K}$. Se $\alpha \notin \mathbb{K}$ allora, per ogni $a + b\alpha$ con $a, b \in \mathbb{K}$ non entrambi nulli il prodotto

$$(a + b\alpha)(a - b\alpha) = a^2 - b^2\alpha^2 \in \mathbb{K}$$

non è nullo poiché $\alpha \neq \pm a/b$. Ne consegue

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

**Esempio 1.13.** Vale $\mathbb{Q}(\sqrt{2}) \cap \mathbb{Q}(\sqrt{3}) = \mathbb{Q}$ ed in particolare $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$. Infatti, per ogni elemento $x$ dell'intersezione possiamo scrivere

$$x = a + b\sqrt{2} = c + d\sqrt{3}, \qquad a, b, c, d \in \mathbb{Q},$$

e vogliamo dimostrare che $x$ è razionale: a tal fine basta dimostrare che $b = 0$ oppure $d = 0$. Si ha $d\sqrt{3} = (a - c) + b\sqrt{2}$, ed elevando al quadrato

$$3d^2 = (a - c)^2 + 2b^2 + 2b(a - c)\sqrt{2}$$

e, siccome $\sqrt{2}$ non è razionale, deve essere $b(a - c) = 0$. Se $b = 0$ abbiamo $x = a \in \mathbb{Q}$, mentre se $a = c$ allora $3d^2 = 2b^2$ e questo è possibile solo se $d = b = 0$, non essendo $3/2$ il quadrato di un numero razionale.

**Esercizio 1.14.** Usare il risultato dell'Esempio 1.13 per dimostrare che se vale

$$a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} = 0$$

con $a, b, c, d \in \mathbb{Q}$, allora $a = b = c = d = 0$.

**Esercizio 1.15** $(*)$**.** Quali sono i numeri del tipo

$$a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}, \qquad a, b, c, d \in \mathbb{Q},$$

che sono radici di un'equazione di secondo grado a coefficienti razionali?

**Esercizio 1.16.** Sia $\xi \in \mathbb{C}$ tale che $\xi^2 + \xi + 1 = 0$. Provare che

$$\mathbb{Q}(\xi) = \{a + b\xi \in \mathbb{C} \mid a, b \in \mathbb{Q}\}$$

è un campo. Scrivere l'inverso di $1 + \xi$ nella forma $a + b\xi$.

**Esercizio 1.17.** Siano date per ogni intero $n > 0$ due proposizioni $P_n$ e $Q_n$. Si supponga inoltre che:

(1) $P_1$ è vera.
(2) Se $P_n$ è vera, allora anche $Q_n$ è vera.
(3) Se $Q_s$ è vera per ogni $s < n$, allora anche $P_n$ è vera.

Dimostrare che $P_n, Q_n$ sono vere per ogni $n$.

**Esercizio 1.18** $(*)$**.** Si consideri la successione $p_1 = 2$, $p_2 = 3$, $p_3 = 5, \ldots$ di tutti i numeri primi in ordine crescente e si consideri la successione di sottocampi:

$$F_0 = \mathbb{Q}, \quad F_1 = \mathbb{Q}(\sqrt{p_1}) = \mathbb{Q}(\sqrt{2}), \quad F_2 = F_1(\sqrt{p_2}) = \mathbb{Q}(\sqrt{2}, \sqrt{3}), \ \ldots\ ,$$
$$F_n = F_{n-1}(\sqrt{p_n}) \qquad \forall n > 0.$$

Dimostrare che per ogni $n > 0$ vale:

(1) $\sqrt{p_n} \notin F_{n-1}$.
(2) Se $x \in F_n$ e $x^2 \in \mathbb{Q}$, allora $x = a\sqrt{m}$ con $a \in \mathbb{Q}$ e $m$ intero positivo che divide il prodotto $p_1 p_2 \cdots p_n$ dei primi $n$ numeri primi.