© 88–08–24312–5

32. Un tale deposita in banca un capitale di Lit. C_0 (per fissare le idee, $C_0 =$ Lit. 10 000 000). La banca gli corrisponde annualmente l'interesse composto j (per fissare le idee, $j = 10\% = 0,10$). Supponiamo che il cliente non prelevi né versi nulla nel periodo di cui si parla e che l'interesse resti costante. Dopo un anno, egli ha un capitale $C_1 = C_0 + C_0 j = C_0(1+j)$.

Qual è il capitale dopo m anni ($m = 1, 2, 3, \dots$)?

Quanti anni occorrono perché il suo capitale diventi maggiore o uguale ad un fissato capitale C (per fissare le idee, $C =$ Lit. 11 000 000)?

Se la banca gli corrispondesse invece ogni 6 mesi l'interesse (sempre composto) $j/2$ sarebbe più conveniente per il cliente? La risposta dipende da j o no?

33. In un lago dell'area di $1\,\mathrm{km}^2$ appare un'alga che galleggia alla superficie, ed ogni giorno raddoppia la sua estensione. Dopo 50 giorni dalla sua comparsa l'alga occupa 1/4 dell'intera superficie. Quanto tempo occorre perché l'alga copra l'intero lago? Si calcoli poi, in μ^2, l'area che l'alga occupa quando giunge nel lago ($1\,\mu = 1$ micrometro o micron $= 10^{-6}$ metri).

34. Siano $a, b, c \in \mathbb{R}$ con $a < c < b$. Sia $f : [a,b] \to \mathbb{R}$ funzione tale che $f_{|[a,c]}$ ed $f_{|[c,b]}$ sono entrambe crescenti (rispettivamente: strettamente crescenti). Provare che in tal caso f è crescente (rispettivamente: strettamente crescente). Provare, con esempi, che la conclusione non vale più se si suppone soltanto che $f_{|[a,c[}$, $f_{|]c,b]}$ siano crescenti (vedi anche (ii), (iii) dell'esercizio 16).

35. Per ciascuna delle seguenti funzioni $f : X \to \mathbb{R}$ si richiede di:
(i) tracciare il grafico;
(ii) dire se f è o no monotòna, strettamente o no;
(iii) provare che f è iniettiva;
(iv) trovare $f(\mathbb{R})$;
(v) detta φ l'inversa della biiezione che f induce su $f(\mathbb{R})$, trovare φ.

(a) $f(x) = \begin{cases} x & \text{se } x \in]-\infty, 1[; \\ x^2 & \text{se } x \in [1,4[; \\ 2^x & \text{se } x \in [4,+\infty[; \end{cases}$ dominio: $X = \mathbb{R}$;

(b) $f(x) = \begin{cases} -4-x & \text{se } x \in [-2,-1[; \\ x & \text{se } x \in [-1,1]; \\ 4-x & \text{se } x \in]1,2]; \end{cases}$ dominio: $X = [-2,2]$;

(c) $f(x) = \exp_3(\exp_2(x))$ $(= 3^{(2^x)})$; dominio: $x = \mathbb{R}$;
(d) $f(x) = \exp_{1/2}(\exp_2(x))$ $(= (1/2)^{(2^x)})$; dominio: $x = \mathbb{R}$;
(e) $f(x) = \dfrac{x-a}{x-b}$ $a, b \in \mathbb{R}$ fissati; dominio: $X = \mathbb{R} \setminus \{b\}$;
(f) $f(x) = \log_2(5 \cdot 3^x + 1)$; dominio: $X = \mathbb{R}$;
(g) $f(x) = (\operatorname{sgn} x) \cdot 2^{|x|}$; dominio: $X = \mathbb{R}$;
(h) $f(x) = (\operatorname{sgn} x) \cdot 3^{-|x|}$; dominio: $X = \mathbb{R}$.

36. Sia $\vartheta \in \mathbb{R} \setminus \{0\}$. Definiamo $f_\vartheta : \mathbb{Z} \to [0,1[$ ponendo $f_\vartheta(m) = \operatorname{frac}(m\vartheta)$ per ogni $m \in \mathbb{Z}$. Provare che se ϑ è *irrazionale*, allora f_ϑ è iniettiva. Se invece ϑ è razionale, si scriva $\vartheta = \pm a/b$, con a, b interi positivi primi fra loro. Provare che f_ϑ non è iniettiva, e trovare $f_\vartheta(\mathbb{Z})$.

© 88–08–24312–5

37. Provare che per ogni $x, y \in \mathbb{R}$ vale la disuguaglianza

$$xy \le \frac{x^2+y^2}{2}$$

e che si ha uguaglianza se e solo se $x = y$.

0.4. Descrizione assiomatica di $\mathbb{R}$. Assioma di completezza. Nella sezione 2 abbiamo ricordato cosa sono i numeri reali e abbiamo riepilogato le regole di calcolo, algebriche e ordinali, che valgono in $\mathbb{R}$. Nel successivo numero 0.4.1 daremo un sistema di assiomi che descrivono ed individuano univocamente $\mathbb{R}$. Essi contengono tutto quanto ci serve sui reali, e da essi ricaveremo i risultati che useremo: non diciamo per ora ciò che i singoli numeri reali effettivamente sono, ci interessiamo soltanto alle proprietà a cui i numeri reali soddisfano globalmente. Resta naturalmente da dimostrare che esiste un insieme $\mathbb{R}$ munito delle operazioni e relazioni che descriveremo, e resta altresì da dimostrare che quanto diremo in 0.4.1 individua unicamente $\mathbb{R}$ stesso. Ma lasciamo questo al futuro: continuiamo a basarci sulla familiarità con il concetto di numero reale acquisita alle scuole medie: d'ora in poi però ogni affermazione, anche la più banale, che si fa sui numeri reali dovrà essere ricavata dagli assiomi di 0.4.1 (e dagli altri assiomi della teoria degli insiemi, ad esempio, il *principio del buon ordinamento* di $\mathbb{N}$).

0.4.1. Il corpo ordinato $\mathbb{R}$. *Il corpo ordinato* dei numeri reali è un insieme $\mathbb{R}$ (i cui elementi sono detti numeri reali) su cui sono definite:

(i) Un'operazione di *addizione* (cioè un'applicazione di $\mathbb{R} \times \mathbb{R}$ in $\mathbb{R}$, $(x,y) \mapsto x+y$).
(ii) Un'operazione di *moltiplicazione* (cioè un'applicazione di $\mathbb{R} \times \mathbb{R}$ in $\mathbb{R}$, $(x,y) \mapsto x \cdot y$).
(iii) Una relazione di ordine, $\le$, in modo tale che i seguenti assiomi siano soddisfatti:
  A1 $x + (y+z) = (x+y) + z$ per ogni $x, y, z \in \mathbb{R}$ (associatività dell'addizione);
  A2 esiste un elemento $0 \in \mathbb{R}$ tale che $0 + x = x + 0 = x$ per ogni $x \in \mathbb{R}$ (esistenza dell'elemento neutro rispetto all'addizione);
  A3 per ogni $x \in \mathbb{R}$ esiste un elemento $-x \in \mathbb{R}$ tale che sia $x + (-x) = (-x) + x = 0$ (esistenza dell'opposto);
  A4 $x + y = y + x$ per ogni $x, y \in \mathbb{R}$ (commutatività dell'addizione).

Questi quattro assiomi si riassumono dicendo che $\mathbb{R}$ è *gruppo commutativo* rispetto all'addizione.

M1 $x(yz) = (xy)z$ per ogni $x, y, z \in \mathbb{R}$ (associatività della moltiplicazione);

M2 esiste un elemento $1 \in \mathbb{R}$, con $1 \neq 0$, tale che sia $1 \cdot x = x \cdot 1 = x$ per ogni $x \in \mathbb{R}$ (esistenza dell'elemento neutro rispetto alla moltiplicazione);

M3 per ogni $x \in \mathbb{R}$, $x \neq 0$ esiste un elemento $1/x \in \mathbb{R}$ tale che sia $(1/x)x = x(1/x) = 1$ (esistenza dell'inverso, o reciproco, di ogni elemento non nullo);

M4 $xy = yx$ per ogni $x, y \in \mathbb{R}$ (commutatività della moltiplicazione);

DM per ogni $x, y, z \in \mathbb{R}$ si ha $x(y + z) = xy + xz$ (distributività della moltiplicazione rispetto all'addizione).

La totalità degli assiomi A, M, DM si riassume dicendo che $\mathbb{R}$ è un *corpo commutativo*: gli assiomi dicono che possiamo addizionare, sottrarre, moltiplicare, dividere i numeri reali con le solite regole di calcolo (stando attenti a non dividere per 0). Queste regole di calcolo sono state riepilogate (e in buona parte dedotte dagli assiomi stessi) nella sezione 1. Diamo ora gli assiomi per l'ordine. Come ogni relazione di ordine essa gode delle proprietà riflessiva, antisimmetrica e transitiva:

O1 *per ogni* $x \in \mathbb{R}$ *si ha* $x \leq x$;

O2 *siano* $x, y \in \mathbb{R}$. *Se* $x \leq y$, *ed* $y \leq x$ *allora* $x = y$;

O3 *siano* $x, y, z \in \mathbb{R}$. *Se* $x \leq y$ *ed* $y \leq z$, *allora* $x \leq z$; ma l'ordinamento di $\mathbb{R}$ è anche totale:

O4 *siano* $x, y \in \mathbb{R}$. *Allora è* $x \leq y$, *oppure* $y \leq x$.

Questi assiomi sono già stati dati in 0.1.13. Di più, l'ordine di $\mathbb{R}$ è compatibile con l'addizione e moltiplicazione:

AO *siano* $x, y, z \in \mathbb{R}$. *Se* $x \leq y$, *allora* $x + z \leq y + z$;

MO *siano* $x, y \in \mathbb{R}$, $z > 0$. *Se* $x \leq y$, *allora* $xz \leq yz$.

Questi assiomi sono già stati dati in 0.1.14. La totalità degli assiomi fin qui dati si può riassumere dicendo che $\mathbb{R}$ è *corpo totalmente ordinato commutativo*. Come visto nella sezione 1, da questi assiomi segue che le disuguaglianze possono essere sommate membro a membro, che i quadrati sono positivi, ecc., in breve si hanno le *regole di calcolo con le disuguaglianze*. Ma gli assiomi dati fin qui non bastano a caratterizzare $\mathbb{R}$; è evidente che, ad esempio, anche il corpo razionale $\mathbb{Q}$ è corpo commutativo totalmente ordinato. L'assioma che distingue $\mathbb{R}$ dagli altri corpi ordinati è quello di *completezza*. Per enunciarlo efficacemente, introduciamo prima alcuni simboli. Se A, B sono sottoinsiemi non vuoti di $\mathbb{R}$, scriveremo $A \leq B$ per indicare che presi comunque $a \in A$ e $b \in B$ risulta $a \leq b$ (si avrà cura di non confondere la nozione $A \leq B$ con l'inclusione $A \subseteq B$, che evidentemente indica una cosa del tutto diversa). È ovvio che significato hanno simboli come $A < B$, $A \geq B$, ecc. Se A contiene un solo elemento a si scrive anche $a \leq B$ in luogo di $\{a\} \leq B$, analogamente se $B = \{b\}$; e così $a < B$, $b \geq A$, ecc. Ciò detto, enunciamo:

CO ASSIOMA DI COMPLETEZZA ORDINALE $\mathbb{R}$. *Se A, B sono sottoinsiemi di $\mathbb{R}$ entrambi non vuoti, e se è $A \leq B$, allora esiste $\xi \in \mathbb{R}$ tale che $A \leq \xi \leq B$.*

Un tale elemento ξ è detto un elemento separatore di A e B; in generale ξ non è unico (ad esempio se $A =]-\infty, 0[$, $B =]1, +\infty[$ ogni $\xi \in [0, 1]$ è elemento separatore di A e B); se ξ è unico si dice che (A, B) è una coppia di *classi contigue* di $\mathbb{R}$. Osserviamo che l'assioma di completezza non vale nell'insieme $\mathbb{Q}$ dei razionali. Se si prende $A = \{x \in \mathbb{Q} : x^2 \leq 2\}$ e $B = \{x \in \mathbb{Q} : x > 0, x^2 \geq 2\}$ si vede facilmente che A, B sono entrambi non vuoti ($1 \in A, 2 \in B$) e che è $A \leq B$; si dimostra (con un po' di lavoro, vedi 0.4.7) che se ξ è elemento separatore di A e B (cioè se è $A \leq \xi \leq B$) allora deve essere $\xi^2 = 2$. Ma è noto che non esiste un numero razionale il cui quadrato sia 2, vedi esercizio 1; quindi, A, B non hanno elemento separatore in $\mathbb{Q}$. Ce l'hanno invece, unico, in $\mathbb{R}$: il numero $\sqrt{2} \in \mathbb{R} \setminus \mathbb{Q}$.

0.4.2. ESTREMO INFERIORE ED ESTREMO SUPERIORE PER UN INSIEME DI NUMERI REALI. Dato un insieme S di numeri reali, superiormente limitato, l'insieme S^* dei suoi maggioranti contiene sempre infiniti elementi: se $b \in S^*$, tutti i numeri reali maggiori di b sono evidentemente ancora maggioranti di S. Conoscendo una maggiorazione b di S, è interessante conoscere eventuali maggiorazioni b' di S che siano "migliori" di b, cioè i $b' < b$ che siano ancora maggioranti di S (b' è "migliore" di b come maggiorazione di S perché "restringe meglio" l'insieme S). In particolare, ci si può chiedere se ci sia una maggiorazione migliore di tutte le altre: ciò equivale a chiedersi se l'insieme S^* dei maggioranti di S ha un *minimo*.

DEFINIZIONE. Sia S un sottoinsieme non vuoto di $\mathbb{R}$. Si chiama *estremo superiore* di S in $\mathbb{R}$ il minimo dei maggioranti di S (in $\mathbb{R}$), se questo esiste.

Le stesse cose, dualmente, si possono ripetere per le minorazioni, e portano alla:

DEFINIZIONE. Sia S sottoinsieme non vuoto di $\mathbb{R}$. Si chiama *estremo inferiore* di S (in $\mathbb{R}$) il massimo dei minoranti di S (in $\mathbb{R}$), se questo esiste.

L'estremo superiore di S (se esiste) si indica con $\sup S$; quello inferiore (se esiste) con $\inf S$. Per loro definizione $\sup S$, $\inf S$, se esistono, sono unici. È bene ricordare che $\sup S$, $\inf S$, anche se esistono, possono *non appartenere* ad S. Si ha anzi: $\sup S \in S$ se e solo se S ha massimo (nel qual caso è $\sup S = \max S$) e dualmente $\inf S \in S$ se e solo se S ha minimo (nel qual caso è $\inf S = \min S$). Ciò è di verifica immediata; $\sup S$, se esiste è un maggiorante di S, e se appartiene ad S è dunque massimo in S; e viceversa, se $\max S$ esiste, è un maggiorante di S, e necessariamente il minimo dei maggioranti (dato un maggiorante b di S, è $b \geq s$ per ogni $s \in S$, in particolare $b \geq \max S$); in modo analogo si prova l'affermazione per inf e min.

ESEMPI. (1) $S = [0, 1[$ ha 0 come estremo inferiore (perché 0 è anche il minimo di S); ha 1 come estremo superiore, che però non è massimo (è $S^* = [1, +\infty[$, e $\min S^* = 1$, chiaramente).

(2) $S =]0,1]$ ha 0 come estremo inferiore, che però non è minimo (l'insieme S_* dei minoranti di S è $S_* =]-\infty, 0]$, che ha 0 come massimo), ha 1 come massimo, quindi anche come estremo superiore (è $S^* = [1, +\infty[$).

(3) $S =]0,1[$ non ha né massimo né minimo, però ha 0 come estremo inferiore ($S_* =]-\infty, 0]$) e 1 come estremo superiore ($S^* = [1, +\infty[$).

(4) $S = \{ n/n+1 : n \in \mathbb{N} \}$ ha minimo 0 (e quindi ha 0 anche come estremo inferiore), ha 1 come estremo superiore, ma non ha massimo; verificare che è $S^* = [1, +\infty[$.

Un insieme $S \subseteq \mathbb{R}$ superiormente non limitato non ha estremo superiore in $\mathbb{R}$: infatti $S^* = \emptyset$ e, come osservato in 0.2.5, l'insieme vuoto non ha minimo. Analogamente, un sottoinsieme inferiormente non limitato di $\mathbb{R}$ non ha estremo inferiore in $\mathbb{R}$. Vediamo ora che questi sono i soli casi, per sottoinsiemi di $\mathbb{R}$, in cui sup e inf non esistono.

0.4.3. Teorema. *Per l'insieme ordinato $\mathbb{R}$ dei reali, le asserzioni che seguono sono equivalenti*:

(i) (Assioma di completezza) *Dati $A, B \subseteq \mathbb{R}$, A, B entrambi non vuoti, con $A \leq B$, esiste $\xi \in \mathbb{R}$ tale che $A \leq \xi \leq B$.*

(ii) (Esistenza dell'estremo superiore) *Se $S \subseteq \mathbb{R}$ è non vuoto e superiormente limitato, allora* $\sup S$ *esiste in* $\mathbb{R}$.

(iii) (Esistenza dell'estremo inferiore) *Se $S \subseteq \mathbb{R}$ è non vuoto ed inferiormente limitato, allora* $\inf S$ *esiste in* $\mathbb{R}$.

Dimostrazione. Proviamo che (i) implica (ii). Sia $S \subseteq \mathbb{R}$, S non vuoto ed S^* (insieme dei maggioranti di S) pure non vuoto. È $S \leq S^*$; essendo $S \neq \emptyset$ ed $S^* \neq \emptyset$ per (i) esiste $\xi \in \mathbb{R}$ tale che sia $S \leq \xi \leq S^*$. Proviamo che $\xi = \sup S$, cioè che $\xi = \min S^*$. Essendo $\xi \geq S$, si ha $\xi \in S^*$; ed essendo anche $\xi \leq S^*$, $\xi = \min S^*$. In modo esattamente analogo si prova che (i) implica (iii).

Proviamo che (ii) implica (i). Siano $A, B \subseteq \mathbb{R}$, $A, B \neq \emptyset$, $A \leq B$, e proviamo che hanno un elemento separatore in $\mathbb{R}$; A è non vuoto e superiormente limitato, perché è $\emptyset \neq B \subseteq A^*$; pertanto ha estremo superiore ξ, $\xi = \sup A$. Poiché, come osservato, è $B \subseteq A^*$, si ha $\xi = \min A^* \leq B$; e poiché $\xi \in A^*$, si ha $A \leq \xi$. La dimostrazione del fatto che (iii) implica (i) è analoga ($\eta = \inf B$ è elemento separatore per A, B). □

Dalla dimostrazione precedente segue che (ii), oppure (iii) sono in tutto equivalenti all'assioma di completezza, e ciascuno di essi potrebbe in sua voce essere usato come assioma per definire i numeri reali. La forma (i) è però più simmetrica e non privilegia (privilegio solo apparente, naturalmente, visto che (ii), (iii) sono equivalenti fra loro) l'estremo inferiore su quello superiore, o viceversa. Altre forme per esprimere l'assioma di completezza possono essere viste negli esercizi 11, 12.

0.4.4. Soltanto gli insiemi non vuoti e superiormente limitati hanno estremo superiore in $\mathbb{R}$. Se $S \subseteq \mathbb{R}$ è non vuoto e superiormente non limitato in $\mathbb{R}$, si usa dire che l'estremo superiore di S in $\widetilde{\mathbb{R}}$ è $+\infty$, e si scrive $\sup_{\widetilde{\mathbb{R}}} S = +\infty$;

dualmente, se $S \subseteq \mathbb{R}$ è non vuoto, ed inferiormente non limitato in $\mathbb{R}$, si dice che l'estremo inferiore di S in $\widetilde{\mathbb{R}}$ è $-\infty$ e si scrive $\inf_{\widetilde{\mathbb{R}}} S = -\infty$. Ricordiamo che l'insieme esteso dei reali $\widetilde{\mathbb{R}} = \mathbb{R} \cup \{ -\infty, +\infty \}$ è stato introdotto in 0.2.2, ed è stato munito di un ordinamento; in $\widetilde{\mathbb{R}}$, un sottoinsieme S di $\mathbb{R}$ ha $+\infty$ come estremo superiore se e solo se è non vuoto e superiormente non limitato in $\mathbb{R}$ ($+\infty$ è l'unico maggiorante, in $\widetilde{\mathbb{R}}$, di un tale S); analogamente per $-\infty$ ed insiemi inferiormente non limitati.

Possiamo ora vedere facilmente che ogni intervallo I di $\mathbb{R}$ è di uno dei tipi descritti in 0.2.2; escluso il caso $I = \emptyset$, $\sup I$ ed $\inf I$ esistono comunque in $\widetilde{\mathbb{R}}$. Dalla convessità segue che in ogni caso $I \supseteq]\inf I, \sup I[$; e si può concludere discutendo separatamente i casi $\inf I \in I$, $\sup I \in I$, $\inf I \notin I$, $\sup I \notin I$.

Osservazione. Parlando di maggioranti, minoranti, estremo inferiore, estremo superiore di un sottoinsieme $S \subseteq \mathbb{R}$ abbiamo insistito su S non vuoto. Per $S = \emptyset$, l'insieme dei suoi maggioranti in $\mathbb{R}$ viene assunto uguale ad $\mathbb{R}$, e così l'insieme dei suoi minoranti. Pertanto $\emptyset$ non ha estremo superiore, né estremo inferiore in $\mathbb{R}$; sarebbe invece $\inf_{\widetilde{\mathbb{R}}}(\emptyset) = +\infty$, $\sup_{\widetilde{\mathbb{R}}}(\emptyset) = -\infty$. Una spiegazione di ciò è data in 0.6. Nel cercare di dimostrare l'esistenza di sup ed inf di un insieme, è bene assicurarsi che esso non sia vuoto; talvolta è questa la parte più difficile di quanto si deve provare.

0.4.5. Proprietà caratteristiche di sup ed inf. La totalità dell'ordine di $\mathbb{R}$ permette di caratterizzare estremo inferiore e superiore dei sottoinsiemi di $\mathbb{R}$ come segue:

Proposizione. *Sia S sottoinsieme di $\mathbb{R}$; $S \neq \emptyset$. Allora:*

(Proprietà caratteristiche dell'estremo superiore) *Il numero $\beta \in \mathbb{R}$ è estremo superiore di S in $\mathbb{R}$ se e solo se le seguenti condizioni si verificano:*

(1) *Per ogni $s \in S$ si ha $s \leq \beta$* (cioè β è maggiorante di S);

(2) *Per ogni $x \in \mathbb{R}$, con $x < \beta$, esiste $s \in S$ tale che sia $x < s$.*

(Proprietà caratteristiche dell'estremo inferiore). *Il numero $\alpha \in \mathbb{R}$ è estremo inferiore di S in $\mathbb{R}$ se e solo se le seguenti condizioni si verificano:*

(1) *Per ogni $s \in S$ si ha $\alpha \leq s$* (cioè α è minorante di S);

(2) *Per ogni $x \in \mathbb{R}$, con $\alpha < x$, esiste $s \in S$ tale che sia $s < x$.*

Dimostrazione. Supponiamo che sia $\beta = \sup S$, e vediamo che β soddisfa alle proprietà (1), (2): la (1) è evidente; quanto alla (2), sia $x < \beta$; per definizione, β è il minimo dei maggioranti di S, quindi x non è maggiorante di S; ciò significa che per almeno un $s \in S$ si ha $s \not\leq x$ (s non minore od uguale ad x). Poiché l'ordinamento di $\mathbb{R}$ è totale, $s \not\leq x$ equivale ad $x < s$.

Viceversa, supponiamo che β soddisfi alle proprietà (1), (2) e vediamo che è $\beta = \sup S$; per (1) β è maggiorante di S; vediamo che (2) (assieme con la totalità dell'ordine), dice che β è il minimo dei maggioranti. Se così non fosse, ci sarebbe un maggiorante x di S tale che $\beta \not\leq x$; la totalità dell'ordine dice

allora che è $x < \beta$; per (2), esiste $s \in S$ tale che $x < s$; ma allora x non è maggiorante di S. La dimostrazione per l'estremo inferiore si fa allo stesso modo, cambiando tutti i versi delle disuguaglianze. □

OSSERVAZIONE. Abbiamo insistito sulla totalità dell'ordine di $\mathbb{R}$ nella precedente proposizione, per questo motivo: la nozione di estremo superiore ed inferiore si può dare anche per sottoinsiemi di insiemi solo parzialmente ordinati esattamente come la si è data qui per i sottoinsiemi di $\mathbb{R}$; cessano però di essere vere negli insiemi non totalmente ordinati le proprietà caratteristiche qui descritte.

0.4.6. CLASSI CONTIGUE. Attesa la sua importanza, esplicitiamo la definizione di *coppia di classi contigue* in $\mathbb{R}$. Chiamiamo così ogni coppia ordinata (A, B) di sottoinsiemi non vuoti di $\mathbb{R}$ tali che sia $A \leq B$, e che A e B abbiano un unico separatore. Si lascia al lettore al cura di mostrare che se A, B sono sottoinsiemi non vuoti di $\mathbb{R}$, con $A \leq B$, allora (A, B) è coppia di classi contigue se e solo se si ha $\inf(B - A) = 0$; si pone $B - A = \{b - a : b \in B,\ a \in A\}$ (se $\xi \leq \eta$ sono entrambi separatori di A e B, si ha $b - a \geq \eta - \xi$ per ogni $a \in A$ e $b \in B \ldots$). Similmente, se $A \leq B$ ed A contiene almeno un elemento strettamente positivo, A e B sono classi contigue se e solo se $\inf\{b/a : b \in B,\ a \in A, a > 0\} = 1$.

0.4.7. ESISTENZA DELLE RADICI. Dimostriamo ora che ogni reale strettamente positivo x ha una radice n-esima, per ogni intero $n \geq 2$ come si era detto in 0.3.17. Cominciamo con un esercizio.

ESERCIZIO. Sia $n \geq 2$ intero, e sia $x > 0$ reale. Mostrare che l'insieme

$$P = \{u^n : u \in \mathbb{Q},\ u > 1\}$$

non ha minimo, ed ha 1 come estremo inferiore.

Risoluzione: L'insieme non ha minimo per la stretta crescenza della potenza ad esponente n: se $\bar{u}^n \in P$, con $\bar{u} > 1$ razionale, essendo $1 < (1 + \bar{u})/2 < \bar{u}$ si ha $((1 + \bar{u})/2)^n < \bar{u}^n$, e $((1 + \bar{u})/2)^n \in P$, quindi $\bar{u}^n$ non è il minimo di P. Sia poi $b = \inf P$; essendo $1 \leq P$, si ha $1 \leq b$. Se fosse $1 < b$ si avrebbe $b < b^2$; per la seconda proprietà caratteristica dell'estremo inferiore esisterebbe un razionale $u > 1$ tale che $b \leq u^n < b^2$; e poiché b non è minimo di P si ha in realtà $b < u^n$; applicando ancora la proprietà caratteristica si trova $v > 1$ razionale e tale che sia $b < v^n < u^n$. Dalle disuguaglianze $b < v^n < u^n < b^2$ si trae $u^n/v^n < b^2/b = b$, che si scrive anche $(u/v)^n < b$; ma $u/v > 1$ (se così non fosse, sarebbe $u \leq v$ e quindi $u^n \leq v^n$, contraddizione); quindi $(u/v)^n \in P$, ma $(u/v)^n < b = \inf P$, assurdo. □

PROPOSIZIONE. *Sia $x > 0$ fissato. Posto*

$$A_x = \{a \in \mathbb{R} : a > 0,\ a^n \leq x\}; \qquad B_x = \{b \in \mathbb{R} : b > 0,\ b^n \geq x\}\,.$$

Allora: A_x e B_x sono entrambe non vuote, si ha $A_x \leq B_x$, e se ξ è un separatore si ha $\xi > 0$ e $\xi^n = x$ (quindi $\xi = \sqrt[n]{x}$: la radice n-esima esiste).

Dimostrazione. Mostriamo anzitutto che A_x e B_x sono entrambi non vuoti. Se $x \geq 1$, si ha $x^n \geq x \geq 1 = 1^n$, per cui $1 \in A_x$ ed $x \in B_x$; se invece $x \leq 1$ si ha $x^n \leq x \leq 1 = 1^n$, per cui $x \in A_x$ e $1 \in B_x$. Chiaramente si ha poi $a \leq b$ per ogni $a \in A_x$ e $b \in B_x$ (per la crescenza della funzione potenza ad esponente n: se fosse $a > b$ sarebbe $a^n > b^n$, ma $a^n \leq x \leq b^n$). L'assioma di completezza mostra che esiste un separatore ξ, $A_x \leq \xi \leq B_x$; si noti che $\xi > 0$, dato che A_x non è vuoto e consta di strettamente positivi. Proviamo che è $\xi^n = x$. Se fosse $\xi^n < x$ si avrebbe $\xi \in A_x$, e quindi $\xi = \max A_x$; sia $u > 1$ razionale tale che sia $u^n < x/\xi^n$; u esiste per l'esercizio precedente. Si ha allora $u^n\xi^n = (u\xi)^n < x$, e quindi $u\xi \in A_x$; ma $u\xi > \xi$, perché $u > 1$, contraddicendo $\xi = \max A_x$. Similmente si esclude che possa essere $\xi^n > x$ (se così fosse ξ sarebbe il minimo di B_x; preso $u > 1$ tale che sia $u^n < \xi^n/x$, si avrebbe $\xi/u \in B_x$, essendo $(\xi/u)^n > x$, e $\xi/u < \xi$, assurdo). Resta quindi solo l'alternativa $\xi^n = x$. Per l'unicità della radice n-esima il separatore è unico, e quindi le classi sono contigue. □

0.4.8. LA COMPLETEZZA IMPLICA L'ARCHIMEDEITÀ. Vediamo come dall'assioma di completezza discende l'archimedeità di $\mathbb{R}$, già enunciata in 0.2.5. *Se $x \in \mathbb{R}$, $x > 0$, ed $y \in \mathbb{R}$, allora esiste $n_0 \in \mathbb{N}$ tale che $n_0 x > y$.*

Dimostrazione. Se così non fosse, per ogni $n \in \mathbb{N}$ sarebbe $nx \not> y$, cioè, per la totalità dell'ordine di $\mathbb{R}$, sarebbe $nx \leq y$ *per ogni* $n \in \mathbb{N}$. Quindi $\mathbb{N}x = \{\, nx : n \in \mathbb{N} \,\}$ è superiormente limitato (ha y come maggiorante); quindi ha un estremo superiore x^* (0.4.3 Teorema). Essendo $x > 0$, è $x^* - x < x^*$; per la seconda proprietà caratteristica dell'estremo superiore 0.4.5, esiste un $nx \in \mathbb{N}x$ tale che $x^* - x < nx$; ma allora $x^* < (n + 1) \cdot x \in \mathbb{N}x$, e quindi $x^* = \sup(\mathbb{N}x)$ non è maggiorante di $\mathbb{N}x$, assurdo. □

OSSERVAZIONE. Anche il corpo ordinato $\mathbb{Q}$ dei razionali, pur essendo non completo, è archimedeo (come è evidente: nella proposizione precedente x, y possono essere presi entro $\mathbb{Q} \subseteq \mathbb{R}$). L'archimedeità è una proprietà più debole della completezza.

0.4.9. L'analogo moltiplicativo dell'archimedeità è il seguente:

PROPOSIZIONE. *Sia $b \in \mathbb{R}$, $b > 1$. Per ogni reale $c > 0$ esiste un numero naturale n tale che sia $b^n > c$.*

Dimostrazione. Ripetere passo passo quella data in 0.4.8, sostituendo all'addizione la moltiplicazione, all'opposto il reciproco, ai multipli le potenze, allo 0 l'1, ecc. □

COROLLARIO. *Se è $0 < a < 1$, per ogni $c > 0$ esiste un numero naturale n tale che sia $(<)$ $a^n < c$.*

Dimostrazione. Esercizio. □

0.4.10. Dall'archimedeità si è tratto, in 0.2.6, il risultato seguente: se $\delta > 0$ è un numero reale, per ogni $x \in \mathbb{R}$ esiste un unico intero $m \in \mathbb{Z}$ tale che sia $m\delta \le x < (m+1)\delta$. L'analogo moltiplicativo (la cui dimostrazione si fa sostituendo all'addizione la moltiplicazione, all'opposto il reciproco, a $|x|$ il valore $\max\{x, 1/x\}$, allo 0 l'1, ecc.) è il seguente:

PROPOSIZIONE. *Sia $b > 1$ numero reale. Per ogni reale $x > 0$ esiste un unico $m \in \mathbb{Z}$ tale che sia $b^m \le x < b^{m+1}$.*

Dimostrazione. Esercizio (vedi sopra). □

L'insieme $\{b^m : m \in \mathbb{Z}\}$ si rappresenta sulla retta press'a poco come in figura 0.34.

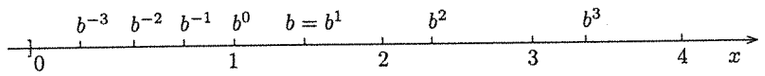

FIGURA 0.34

I suoi elementi sono in *progressione geometrica di ragione b* mentre quelli di $\mathbb{Z}\delta = \{m\delta : m \in \mathbb{Z}\}$ sono in *progressione aritmetica di ragione δ*. L'intero m è talvolta detto *caratteristica in base b del numero $x > 0$*. Servendosi dei logaritmi, si ha subito $m = [\log_b x]$ (parte intera del logaritmo a base b di x).

0.4.11. Sia I intervallo di $\mathbb{R}$ (vedi 0.2.2):

DEFINIZIONE. Un sottoinsieme $S \subseteq I$ si dice *denso* in I se dati $x, y \in I$, con $x < y$ esiste $s \in S$ tale che sia $x < s < y$.

Naturalmente, I stesso è denso in I (se $x, y \in I$, $x < y$, si ha $x < ((x+y)/2) < y$, e $((x+y)/2) \in I$, per definizione stessa di intervallo). Ricordiamo che anche $\mathbb{R}$ è un intervallo di $\mathbb{R}$; $\mathbb{Z}$ non è denso in $\mathbb{R}$ (fra $x = 1/3$ e $y = 1/2$ non ci sono numeri interi); $\mathbb{Q}$ invece è denso in $\mathbb{R}$, come fra poco vedremo. Dimostriamo ora il:

LEMMA. *Sia $\delta > 0$, $x, y \in \mathbb{R}$, $x < y$. Se è $\delta < y - x$ allora esiste un intero $n \in \mathbb{Z}$ tale che sia $x < n\delta < y$.*

Dimostrazione. Sia m l'intero tale che $m\delta \le x < (m+1)\delta$ (0.2.5, Proposizione); $n = m + 1$ è uno degli interi cercati. Infatti, se fosse $(m+1)\delta > y$ essendo $-m\delta \ge -x$ si avrebbe, sommando queste disuguaglianze membro a membro, che è $\delta > y - x$, contro l'ipotesi. □

OSSERVAZIONE. Intuitivamente (e sempre figurandosi i numeri reali sulla retta) il lemma è chiaro: i numeri $m\delta$, $m \in \mathbb{Z}$, sono in progressione aritmetica, e "saltano di δ in δ". Se un intervallo $]x, y[$ ha ampiezza maggiore di δ, essi non possono saltarlo, uno almeno deve cascarci dentro.

Il lemma ha evidentemente un analogo moltiplicativo, che è: *sia $b > 1$, $x, y > 0$. Se $b < y/x$, esiste un intero $n \in \mathbb{Z}$ tale che sia $x < b^n < y$.*

Dimostrazione. Esercizio (solito metodo: sostituire moltiplicazione all'addizione, ecc.). □

COROLLARIO. *$\mathbb{Q}$ è denso in $\mathbb{R}$.*

Dimostrazione. Dati $a, b \in \mathbb{R}$ con $a < b$ si prenda $n \in \mathbb{N}$ tale che sia $1/n < b - a$; esiste allora un intero m tale che sia $a < m/n < b$. □

Si osservi che anche l'insieme $\mathbb{R} \setminus \mathbb{Q}$ degli irrazionali è denso in $\mathbb{R}$. Per dimostrarlo, basta prendere un qualsiasi irrazionale $\vartheta > 0$ (se si vuole, $\vartheta = \sqrt{2}$) e dati $a, b \in \mathbb{R}$ con $a < b$ prendere $n \in \mathbb{N}$ tale che $\vartheta/n < b - a$ (al solito, n esiste per l'archimedeità di $\mathbb{R}$); esiste un intero m tale che sia $a < (m/n)\vartheta < b$; ed $(m/n)\vartheta$ è irrazionale, essendo multiplo razionale dell'irrazionale ϑ, a meno che non sia $m = 0$; in tal caso è $a < 0 < b$, e basta prendere $n \in \mathbb{N}$ in modo che sia $(0 <)\vartheta/n < b$.

0.4.12. ESPONENZIALE. L'esistenza delle radici permette di definire le potenze ad esponente razionale. Fissato $a > 1$, la funzione $e_a : \mathbb{Q} \to \mathbb{R}$ definita da $e_a(\varrho) = a^\varrho$ è strettamente crescente, come visto nell'esercizio 0.3.18.1.

ESERCIZIO. L'insieme

$$E = \{a^\varrho : \varrho \in \mathbb{Q},\ \varrho > 0\}$$

ha 1 come estremo inferiore.

Risoluzione: Sia $b = \inf E$; si ha $1 \le b$, essendo ovviamente $a^\varrho > 1$ se $\varrho > 0$ (vedi esercizio 0.3.18.1). Se fosse $1 < b$, sarebbe $b < b^2$; esiste allora $\varrho > 0$, $\varrho \in \mathbb{Q}$, tale che sia $a^\varrho < b^2$. Estraendo le radici quadrate si ha $a^{\varrho/2} < b$; ma poiché anche $\varrho/2 > 0$ si ha $b \le a^{\varrho/2}$, contraddizione. □

Vediamo ora l'esistenza della funzione esponenziale, annunciata in 0.3.20.

PROPOSIZIONE. *Sia $a \in \mathbb{R}$, $a > 1$. Per ogni $x \in \mathbb{R}$ si ponga*

$$U_x = \{a^p : p \in \mathbb{Q},\ p < x\}; \qquad V_x = \{a^q : q \in \mathbb{Q},\ q > x\}.$$

Allora: U_x e V_x sono una coppia di classi contigue in $\mathbb{R}$. Se $e_a(x)$ denota il loro unico separatore in $\mathbb{R}$ si ha $e_a(x) = a^x$ se x è razionale, ed inoltre $e_a(x+y) = e_a(x)e_a(y)$ per ogni $x, y \in \mathbb{R}$.

Dimostrazione. Si ha $U_x < V_x$ per la stretta crescenza di $\varrho \mapsto a^\varrho$. Se $\xi < \eta$ fossero due separatori di U_x e V_x si avrebbe $a^p \le \xi < \eta \le a^q$ per ogni $p < x < q$, con $p, q \in \mathbb{Q}$; sarebbe allora $a^q/a^p \ge \eta/\xi > 1$, e cioè $a^{q-p} > \eta/\xi > 1$ per ogni $p < x < q$, con $p, q \in \mathbb{Q}$; ma ogni numero razionale strettamente positivo ϱ si scrive $\varrho = q - p$, con $p < x < q$ (densità di $\mathbb{Q}$ in $\mathbb{R}$, vedi 0.4.11), qualunque sia x reale. Ciò contraddice quindi quanto visto nell'esercizio precedente; (U_x, V_x) è una coppia di classi contigue. Se $x \in \mathbb{Q}$ si ha $a^p < a^x < a^q$ per

$p < x < q$, $p, q \in \mathbb{Q}$, e quindi a^x è il separatore di U_x e V_x. Dati poi $x, y \in \mathbb{R}$, siano ξ, η, ζ i separatori di (U_x, V_x), di (U_y, V_y) e di (U_{x+y}, V_{x+y}) rispettivamente. Se $p_1 < x < q_1$ e $p_2 < y < q_2$ si ha $p_1 + p_2 < x + y < q_1 + q_2$ da cui $a^{p_1+p_2} \leq \zeta \leq a^{q_1+q_2}$, e simultaneamente, moltiplicando membro a membro $a^{p_1} \leq \xi \leq a^{q_1}$, $a^{p_2} \leq \eta \leq a^{q_2}$ si ottiene $a^{p_1+p_2} \leq \xi\eta \leq a^{q_1+q_2}$. Inoltre, se p, q in $\mathbb{Q}$ sono tali che sia $p < x + y < q$ esistono $p_1, p_2, q_1, q_2 \in \mathbb{Q}$ con $p_1 < x < q_1$ e $p_2 < y < q_2$ tali che sia $p = p_1 + p_2$ e $q = q_1 + q_2$. Infatti, da $p < x + y < q$ si trae $p - y < x < q - y$; per la densità di $\mathbb{Q}$ in $\mathbb{R}$ esistono $p_1, q_1 \in \mathbb{Q}$ tali che sia $p - y < p_1 < x < q_1 < q - y$; da $p - y < p_1$ si trae $p - p_1 < y$, e da $q_1 < q - y$ si trae $y < q - q_1$; posto $p_2 = p - p_1$ e $q_2 = q - q_1$ si conclude come si voleva. Si ha quindi $\xi\eta = \zeta$, essendo i due numeri ζ e $\xi\eta$ separatori delle stesse classi. □

DEFINIZIONE. Se $a > 1$ è reale, ed x è reale, si definisce la *potenza ad esponente reale* a^x come il separatore della coppia di classi contigue sopra considerate

$$U_x = \{a^p : p \in \mathbb{Q},\ p < x\}; \qquad V_x = \{a^q : q \in \mathbb{Q},\ q > x\}.$$

Se $0 < a < 1$ ed $x \in \mathbb{R}$, si pone per definizione $a^x = 1/(1/a)^x$; infine si pone $1^x = 1$ per ogni $x \in \mathbb{R}$, e $0^x = 0$ per $x > 0$.

È immediato vedere che se si pone $\exp_a(x) = a^x$, $\exp_a$ ha le proprietà annunciate in 0.3.20: infatti (1), (2) di 0.3.20 valgono; come dimostrato in 0.3.20, se una funzione soddisfa a (1), (2), necessariamente è $\exp_a(\varrho) = a^\varrho$ se ϱ è razionale e la monotonia costringe a *definire* $\exp_a(x)$ per x reale coma sopra fatto.

0.4.13. SOTTOGRUPPI ADDITIVI DI $\mathbb{R}$. Chiamiamo *sottogruppo additivo di* $\mathbb{R}$ un sottoinsieme $H \subseteq \mathbb{R}$ tale che

(1) $0 \in H$;
(2) se $x, y \in H$ allora $x + y$, $x - y$, $-x$, $-y \in H$.

Questa definizione è sovrabbondante; ma qui ci interessa soltanto dire che un sottogruppo additivo di $\mathbb{R}$ è un sottoinsieme non vuoto di $\mathbb{R}$ (contiene almeno 0 come elemento) i cui elementi possono essere sommati e sottratti, restando in H; in particolare, se H è sottogruppo additivo di $\mathbb{R}$, ed $a \in H$, allora $2a = a + a \in H$, $3a = 2a + a \in H$, $-a \in H$, $(-2)a = (-a) + (-a) \in H$, e in generale $ma \in H$, per ogni $m \in \mathbb{Z}$, cioè $\mathbb{Z}a = \{ma : m \in \mathbb{Z}\} \subseteq H$. Esempi di sottogruppi additivi di $\mathbb{R}$ sono $H = \{0\}$, sottogruppo banale e $H = \mathbb{R}$, sottogruppo improprio.

Per ogni $a \in \mathbb{R}$, $\mathbb{Z}a$, insieme dei multipli interi di a, è evidentemente un sottogruppo additivo di $\mathbb{R}$, detto *gruppo additivo generato da* a (si verifica che, rispetto all'inclusione, è il minimo sottogruppo additivo di $\mathbb{R}$ contenente a). In particolare $\mathbb{Z} = \mathbb{Z} \cdot 1$ è sottogruppo additivo di $\mathbb{R}$. I sottogruppi della forma $\mathbb{Z}a$ sono detti sottogruppi (additivi) *discreti* di $\mathbb{R}$ (il sottogruppo banale $\{0\}$ si scrive $\mathbb{Z} \cdot 0$ ed è anch'esso discreto). Anche $\mathbb{Q}$ è sottogruppo additivo di $\mathbb{R}$, ma non è discreto, come si vede facilmente.

PROPOSIZIONE. *Sia H sottogruppo additivo di $\mathbb{R}$. Sono possibili tre casi (ciascuno dei quali esclude gli altri due):*

(1) *$H = \{0\}$ è il sottogruppo banale;*
(2) *$H \cap]0, +\infty[$ ha un minimo a_0; in tal caso è $H = \mathbb{Z}a_0$, ed H è discreto;*

(3) *$H \cap]0, +\infty[$ non ha minimo; in tal caso H è denso in $\mathbb{R}$*, cioè (0.4.11): dati $x, y \in \mathbb{R}$, con $x < y$, esiste $h \in H$ tale che $x < h < y$.

Dimostrazione. Escluso il caso (1), H contiene almeno un $x \neq 0$. Poiché x, $-x \in H$, certamente H contiene un numero reale strettamente positivo, in altre parole $H \cap]0, +\infty[\neq \emptyset$; poiché $H \cap]0, +\infty[$ ha 0 come minorante, esso ha un estremo inferiore $\alpha \geq 0$. Se, caso (2), α è il minimo di $H \cap]0, +\infty[$, allora è $H = \mathbb{Z}\alpha$; infatti è $\mathbb{Z}\alpha \subseteq H$ (perché $\alpha \in H$ ed H è sottogruppo); inoltre, se $x \in H$, esiste un unico intero m tale che $m\alpha \leq x < (m+1)\alpha$; se è $x \neq m\alpha$, si ha $m\alpha < x < (m+1)\alpha$; sottraendo $m\alpha$ a tutti i membri di questa disuguaglianza, si ha $0 < x - m\alpha < \alpha$: ma poiché $x - m\alpha \in H$, questo contraddice il fatto che α è minimo di $H \cap]0, +\infty[$. Se invece, caso (3), α non è minimo di $H \cap]0, +\infty[$, proviamo che H è denso in $\mathbb{R}$; vediamo anzitutto che in tal caso è $\alpha = \inf(H \cap]0, +\infty[) = 0$. Se fosse $\alpha > 0$, si avrebbe $\alpha < 2\alpha$; per la seconda proprietà caratteristica dell'estremo inferiore esiste $x_1 \in H \cap]0, +\infty[$ tale che $x_1 < 2\alpha$; non essendo α minimo, si ha $\alpha < x_1$; sempre per la seconda proprietà caratteristica dell'estremo inferiore esiste $x_2 \in H \cap]0, +\infty[$ tale che sia $x_2 < x_1$; si ha quindi $\alpha < x_1 < x_2 < 2\alpha$, da cui si trae $0 < x_1 - x_2 < \alpha$. Poiché H è sottogruppo, $x_1 - x_2 \in H$; ma allora $x_1 - x_2 \in H \cap]0, +\infty[$, e $x_1 - x_2 < \alpha = \inf(H \cap]0, +\infty[)$, assurdo. Dopo di ciò, siano $x, y \in \mathbb{R}$, $x < y$. Si prenda $\delta \in H$ tale che sia $0 < \delta < y - x$ (questo si può fare perché è $\inf(H \cap]0, +\infty[) = 0$). Per il lemma 0.4.11 esiste $m \in \mathbb{Z}$ tale che sia $x < m\delta < y$; ma $m\delta \in H$, e la conclusione è raggiunta. □

Il precedente teorema permette di riottenere quanto visto in 0.4.11: $\mathbb{Q}$ è denso in $\mathbb{R}$, essendo sottogruppo additivo, con $\mathbb{Q}^> = \mathbb{Q} \cap]0, +\infty[$ chiaramente privo di minimo.

0.4.14. SOTTOGRUPPI MOLTIPLICATIVI DI $\mathbb{R}^*_+$. Esponiamo qui l'analogo moltiplicativo di 0.4.13. Come detto in 0.1.14, indichiamo con $\mathbb{R}^*_+$ l'intervallo $]0, +\infty[$ dei reali strettamente positivi; $\mathbb{R}^*_+$ è detto anche *gruppo moltiplicativo* dei reali (strettamente) positivi. Ciò esprime il fatto che $1 \in \mathbb{R}^*_+$ e che se $x, y \in \mathbb{R}^*_+$ allora xy, x/y, $1/x$, $1/y \in \mathbb{R}^*_+$. Chiamiamo *sottogruppo moltiplicativo di* $\mathbb{R}^*_+$ un sottoinsieme $G \subseteq \mathbb{R}^*_+$ tale che:

(1) $1 \in G$
(2) se $x, y \in G$ allora xy, x/y, $1/x$, $1/y \in G$.

Esempi di sottogruppi moltiplicativi di $\mathbb{R}^*_+$ sono $G = \{1\}$, sottogruppo banale e $G = \mathbb{R}^*_+$, sottogruppo improprio. Per ogni $a \in \mathbb{R}^*_+$ l'insieme $\langle a \rangle = \{a^m : m \in \mathbb{Z}\}$ è sottogruppo moltiplicativo di $\mathbb{R}^*_+$ come subito si verifica. È il sottogruppo moltiplicativo generato da a (è l'analogo moltiplicativo di $\mathbb{Z}a$ ed è anch'esso chiamato discreto). Se G è sottogruppo moltiplicativo di $\mathbb{R}^*_+$ ed $a \in G$, allora $\langle a \rangle \subseteq G$ come è facile vedere.

PROPOSIZIONE. *Sia G sottogruppo moltiplicativo di $\mathbb{R}^*_+$. Sono possibili tre casi (ciascuno dei quali esclude gli altri due):*

(1) *$G = \{1\}$ è sottogruppo banale;*
(2) *$G \cap]1, +\infty[$ ha un minimo a_0; in tal caso è $G = \langle a_0 \rangle$ $(= \{a_0^m : m \in \mathbb{Z}\})$;*
(3) *$G \cap]1, +\infty[$ non ha minimo; in tal caso G è denso nell'intervallo $\mathbb{R}^*_+ =]0, +\infty[$.*

Dimostrazione. Ripetere quella fatta in 0.4.13 sostituendo moltiplicazione con addizione, quozienti con differenze, reciproci con opposti, 0 con 1, multipli con potenze, eccetera. □

ESERCIZIO. Sia I intervallo di $\mathbb{R}$ e siano $U, V \subseteq I$ entrambi non vuoti, con $U \leq V$. Mostrare che se $U \cup V$ è denso in I, allora U e V son classi contigue, ed il loro separatore appartiene ad I.

ESERCIZIO (TEOREMA DEI VALORI INTERMEDI PER FUNZIONI MONOTONE). Sia X intervallo di $\mathbb{R}$, e sia $f : X \to \mathbb{R}$ monotona. Sia I intervallo aperto di $\mathbb{R}$. Si ha $I \subseteq f(X)$ se e solo se $f(X) \cap I$ è denso in I.

Risoluzione: Ovviamente, se $I \subseteq f(X)$, $I = I \cap f(X)$ è denso in I. Supponiamo $f(X) \cap I$ denso in I, f monotona crescente, e mostriamo che $I \subseteq f(X)$. Sia $y \in I$; essendo I aperto, y non è il minimo, né il massimo, di I; esistono cioè $c, d \in I$ con $c < y < d$. Per la densità di $f(X) \cap I$ in I esistono $a, b \in X$ tali che sia $c < f(a) < y < f(b) < d$. Sia ora $A = \{x \in X : f(x) \leq y\}$, $B = \{x \in X : f(x) \geq y\}$; A e B sono non vuoti ($a \in A$, $b \in B$) ed inoltre $A \leq B$ (immediato, per la crescenza di f). Se ξ è un separatore per A, B, si ha $\xi \in X$, perché X è intervallo. Vogliamo provare che è $f(\xi) = y$. Se fosse $f(\xi) < y$ esisterebbe, per densità, $f(u) \in f(X) \cap I$ con $f(\xi) < f(u) < y < f(b)$; essendo $f(u) < y$ si ha $u \in A$; ma la monotonia di f implica che è $\xi < u < b$, e quindi u è maggiore del separatore ξ, pur stando nella classe inferiore, assurdo. Similmente si esclude che sia $f(\xi) > y$; ed il ragionamento per f decrescente è analogo. □

ESERCIZIO. Usando il teorema di densità dei sottogruppi moltiplicativi di $\mathbb{R}^>$ provare che $p_m(\mathbb{R}^>)$ è denso in $\mathbb{R}^>$, per ogni intero $m \geq 1$, e dedurne che $p_m(\mathbb{R}^>) = \mathbb{R}^>$, usando il precedente risultato; $p_m : \mathbb{R} \to \mathbb{R}$ è la funzione potenza m-esima, $p_m(x) = x^m$. Similmente, si provi che $\exp_a(\mathbb{R}) = \mathbb{R}^>$. □

Esercizi alla sezione 4.

1. *Il numero 2 non è un quadrato in $\mathbb{Q}$;* cioè *non esiste un numero razionale x tale che $x^2 = 2$.*

Risoluzione: Ragioniamo per assurdo: supponiamo che esista un razionale $x = a/b$ tale che $a^2/b^2 = 2$; possiamo supporre, riducendo la frazione a/b, che a e b siano interi positivi e primi fra loro. Si ha dunque $a^2 = 2b^2$. Quindi a^2 è pari. Poiché il quadrato di un intero dispari è dispari (infatti $(2m+1)^2 = 4m^2 + 4m + 1$), a deve essere pari, cioè è $a = 2u$. Da $a^2 = 2b^2$ segue $4u^2 = 2b^2$ e quindi $b^2 = 2u^2$. Ma allora b^2 è pari, e quindi b è pari. Pertanto sia a che b sono pari, e quindi non sono primi fra loro, contro l'ipotesi.

OSSERVAZIONE. Quanto sopra dimostra evidentemente che $\sqrt{2}$ è irrazionale, e quindi che la diagonale ed il lato di un quadrato sono *incommensurabili.* È un risultato assai antico, che risale alla scuola di Pitagora (circa 500 A.C.). Ammette numerose generalizzazioni: per esempio, dato un intero $a > 0$, ed un altro intero $n \geq 2$, $\sqrt[n]{a}$ è razionale se e solo se è intero: in altre parole le eventuali soluzioni razionali dell'equazione $x^n = a$ sono intere; in questa direzione, c'è l'ulteriore generalizzazione seguente: ogni soluzione dell'equazione

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0$$

dove $a_0, a_1, \ldots, a_{n-1} \in \mathbb{Z}$, è intera, oppure irrazionale. Tutto ciò si dimostra facilmente grazie alla fattorizzazione di un intero in numeri primi.

2. Siano $A, B \subseteq \mathbb{R}$; supponiamo $A, B \neq \emptyset$; si pone:

$$A + B = \{\, a + b : a \in A, b \in B \,\}$$

(quindi $A + B$ è l'immagine di $A \times B \subseteq \mathbb{R}^2$ tramite la funzione addizione $+ : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$);

$$A \cdot B = \{\, a \cdot b : a \in A, b \in B \,\}$$

(quindi $A \cdot B$ è l'immagine di $A \times B \subseteq \mathbb{R}^2$ tramite la funzione moltiplicazione $\cdot : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$);

$$-B = \{\, -b : b \in B \,\}$$

(quindi $-B$ è l'immagine di B tramite la funzione opposta $x \mapsto -x$, di $\mathbb{R}$ in $\mathbb{R}$).

Si pone poi $A - B = A + (-B)$ (N.B. attenzione a non confondere $A - B$ con $A \smallsetminus B$, differenza insiemistica di A e B, che è definita in 0.0.4). Se A si riduce ad un solo elemento, $A = \{\, a \,\}$, si scrive $a + B$, aB in luogo di $A + B$, AB, ecc.; analogamente per B.

(i) Provare che $A + B$ è superiormente (rispettivamente: inferiormente) limitato se e solo se tali sono sia A che B, e che in tal caso si ha $\sup(A + B) = \sup A + \sup B$ (rispettivamente $\inf(A + B) = \inf A + \inf B$).

(ii) Si supponga $A, B \subseteq \mathbb{R}_+$: provare che è sempre $\inf(A \cdot B) = \inf A \cdot \inf B$; provare che se A e B sono superiormente limitati, allora $A \cdot B$ è superiormente limitato e si ha $\sup(A \cdot B) = \sup A \cdot \sup B$. Se A non è superiormente limitato, è vero che $A \cdot B$ non è superiormente limitato? Cosa si può dire se si toglie l'ipotesi $A, B \subseteq \mathbb{R}_+$?

(iii) Provare che è $\inf_{\tilde{\mathbb{R}}}(-A) = -\inf_{\tilde{\mathbb{R}}} A$ (si intende che è $-(+\infty) = -\infty$ e $-(-\infty) = +\infty$).

3. Sia $\emptyset \neq A \subseteq B \subseteq \mathbb{R}$. Provare che è $\inf_{\tilde{\mathbb{R}}} B \leq \inf_{\tilde{\mathbb{R}}} A \leq \sup_{\tilde{\mathbb{R}}} A \leq \sup_{\tilde{\mathbb{R}}} B$.

4. Siano $A, B \neq \emptyset$, $A, B \subseteq \mathbb{R}$. Provare che è

$$\sup_{\tilde{\mathbb{R}}}(A \cup B) = \max\{\sup_{\tilde{\mathbb{R}}} A, \sup_{\tilde{\mathbb{R}}} B\};$$
$$\inf_{\tilde{\mathbb{R}}}(A \cup B) = \min\{\inf_{\tilde{\mathbb{R}}} A, \inf_{\tilde{\mathbb{R}}} B\}$$

Supposto $A \cap B \neq \emptyset$, si può dire qualcosa su $\sup_{\tilde{\mathbb{R}}}(A \cap B)$, $\inf_{\tilde{\mathbb{R}}}(A \cap B)$ (si intende, in termini di $\sup_{\tilde{\mathbb{R}}} A$, $\sup_{\tilde{\mathbb{R}}} B$, ecc.)?

5. Sia $E = \left\{ \dfrac{xy}{x+y} : x, y \in]0, 1[\right\}$.
Provare che è $\inf E = 0$, $\sup E = 1/2$.

6. Sia $a > 0$. Posto $E_1 = \{\, a^\varrho : \varrho \in \mathbb{Q}, \varrho > 0 \,\}$ ed $E_2 = \{\, a^n : n \in \mathbb{N} \smallsetminus \{0\} \,\}$, trovare $\sup_{\tilde{\mathbb{R}}}$, $\inf_{\tilde{\mathbb{R}}}$ di E_1 ed E_2.

7. Sia $E = \{\, x \in \mathbb{R}_+ : \cos(1/x) = 0 \,\}$. Trovare $\sup E$, $\inf E$.

8. Provare che $H \subseteq \mathbb{R}$ è sottogruppo additivo di $\mathbb{R}$ se e solo se H non è vuoto, e $H - H \subseteq H$.

9. Quando accade che un sottogruppo additivo di $\mathbb{R}$ è superiormente, o inferiormente, limitato? E un sottogruppo moltiplicativo di $\mathbb{R}_+^*$?

10 ◑◑. Sia $\varrho \in \mathbb{R}$, con $0 < \varrho < 1$, e sia c_n una successione di numeri appartenenti all'intervallo $[0, c]$, $c \geq 0$ (cioè, per ogni $n \in \mathbb{N}$ è $c_n \in [0, c]$, ovvero $0 \leq c_n \leq c$).

Per ogni $n \in \mathbb{N}$ sia $s_n = c_0\varrho^0 + c_1\varrho^1 + \cdots + c_n\varrho^n$. Sia $S = \{ s_n : n \in \mathbb{N} \}$.

(i) Provare che S è superiormente limitato e che $c/(1-\varrho)$ è un maggiorante di S.

(ii) Provare che $\sup S = 1/(c-\varrho)$ se e solo se è $c = c_0 = c_1 = \cdots = c_n = c_{n+1} = \ldots$, per ogni $n \in \mathbb{N}$.

Suggerimento: Ricordare che per ogni $x \in \mathbb{R}$ è $1 - x^{n+1} = (1-x)(1 + x + \cdots + x^n)$, quindi se $x \neq 1$ si ha $1 + x + \cdots + x^n = (1 - x^{n+1})/(1-x)$.

11. Una *sezione* (o *taglio di Dedekind*) di $\mathbb{R}$ è una coppia ordinata (H, K) di sottoinsiemi di $\mathbb{R}$, entrambi non vuoti, e tali che $H \cup K = \mathbb{R}$, e $H < K$ (cioè è $h < k$ per ogni $h \in H$ e ogni $k \in K$, vedi 0.4.1). Provare che l'assioma di completezza ordinale di $\mathbb{R}$ equivale al fatto che ogni sezione di $\mathbb{R}$ ammette un unico elemento separatore. Provare che tale elemento separatore è il massimo di H, oppure il minimo di K, le due cose escludendosi a vicenda.

12. Sia $\mathcal{I}$ un insieme non vuoto di intervalli chiusi e limitati di $\mathbb{R}$; si supponga che $\mathcal{I}$ soddisfi alla seguente condizione: se $I, J \in \mathcal{I}$, allora $I \cap J \neq \emptyset$. Provare che l'assioma di completezza implica allora

$$\bigcap_{I \in \mathcal{I}} I \neq \emptyset,$$

cioè che esiste ξ tale che $\xi \in I$, per ogni $I \in \mathcal{I}$.

Suggerimento: Dati due intervalli $[a, b]$, $[c, d]$ chiusi e limitati, osservate che $[a, b] \cap [c, d] \neq \emptyset$ se e solo se $c \leq b$ e $a \leq d$. Sia A l'insieme degli estremi inferiori degli intervalli di $\mathcal{I}$, B l'insieme dei loro estremi superiori; dall'ipotesi $I \cap J \neq \emptyset$ per ogni $I, J \in J$ segue allora $A \leq B$. Provare che questa proprietà implica a sua volta l'assioma di completezza (quindi, gli è equivalente).

13. Sia $\mathcal{I} = \{ I_n : n \in \mathbb{N} \}$ dove è $I_n = [n/(n+1), 1[$ per ogni $n \in \mathbb{N}$. Dati $I, J \in \mathcal{I}$ si ha $I \cap J \neq \emptyset$; ma non esiste nessun $\xi \in \mathbb{R}$ che appartenga a tutti gli $I_n \in \mathcal{I}$. Quindi, l'ipotesi fatta nell'esercizio 12 che gli intervalli siano chiusi è essenziale. La considerazione di $\mathcal{I} = \{ I_n : n \in \mathbb{N} \}$, dove è $I_n = [n, +\infty[$, mostra che anche l'ipotesi di limitatezza degli intervalli è essenziale nell'esercizio 12.

14. Sia S denso in $\mathbb{R}$, vedi 0.4.11, e sia $a \in \mathbb{R}$. È vero che $a + S$ è denso in $\mathbb{R}$? ed aS?

15. Siano S_1, S_2 densi in $\mathbb{R}$. È vero che $S_1 \cup S_2$ è denso in $\mathbb{R}$? ed $S_1 \cap S_2$?

16. Un sottoinsieme di un insieme non denso in $\mathbb{R}$ chiaramente non è denso in $\mathbb{R}$. Pertanto, i sottogruppi additivi dei sottogruppi additivi discreti di $\mathbb{R}$ sono ancora discreti. In particolare, ogni sottogruppo additivo di $\mathbb{Z}$ è della forma $m_0\mathbb{Z}$, con $m_0 \in \mathbb{Z}$.

17. Dati $\alpha, \beta \in \mathbb{R}$, consideriamo $\mathbb{Z}\alpha + \mathbb{Z}\beta = \{ m\alpha + n\beta : m \in \mathbb{Z}, n \in \mathbb{Z} \}$:

(i) Verificare che $\mathbb{Z}\alpha + \mathbb{Z}\beta$ è sottogruppo additivo di $\mathbb{R}$.

(ii) Supposti α, β entrambi non nulli, verificare che $\mathbb{Z}\alpha + \mathbb{Z}\beta$ è discreto se e solo se α/β è razionale.

18. Provare il *teorema di Bezout*: dati due interi $\alpha, \beta \neq 0$, e detto d un loro massimo comun divisore, provare che esistono interi u, v tali che sia $u\alpha + v\beta = d$; (provare che d è massimo comun divisore di α e β se e solo se è $\mathbb{Z}\alpha + \mathbb{Z}\beta = \mathbb{Z}d$: ricordiamo che un massimo comun divisore di α, β è un divisore di α e β che è diviso da ogni divisore comune ad α e β).

19 ⦿⦿. Sia $\vartheta \in \mathbb{R} \setminus \mathbb{Q}$ un irrazionale. Provare che l'insieme $\{ \mathrm{frac}(m\vartheta) : m = 1, 2, 3 \ldots \}$ è denso in $[0, 1[$.

20. Sia $f : \mathbb{R} \to \mathbb{R}$ monotòna e tale che $f(x + y) = f(x) + f(y)$ per ogni $x, y \in \mathbb{R}$. Provare che esiste un unico $c \in \mathbb{R}$ tale che $f(x) = cx$, per ogni $x \in \mathbb{R}$.

Suggerimento: Posto $c = f(1)$, provare anzitutto che è $f(\varrho) = c\varrho$ per ogni $\varrho \in \mathbb{Q}$; considerare poi $H = f(\mathbb{Q})$ ...

21. Sia $f : \mathbb{R}_+^* \to \mathbb{R}_+^*$ monotòna e tale che $f(xy) = f(x)f(y)$ per ogni $x, y \in \mathbb{R}_+^*$. Provare che esiste un unico $c \in \mathbb{R}$ tale che $f(x) = x^c$, per ogni $x \in \mathbb{R}$.

Suggerimento: Si può ragionare in analogia all'esercizio 20; oppure si può considerare $g = \log_2 \circ f \circ \exp_2$, ed applicare a questa il risultato dell'esercizio 20.

0.5. Funzioni circolari. Funzioni periodiche. Nella sezione 3, oltre a definire il concetto di funzione, abbiamo passato in rassegna le funzioni elementari più comunemente usate nella pratica matematica quotidiana. Questa rassegna non è completa senza le funzioni circolari (seno, coseno, tangente, arco seno, arco coseno, arco tangente, ecc.).

Mentre una trattazione abbastanza "pulita" e naturale di potenze, esponenziali, logaritmi è possibile restando nell'ambito reale, per introdurre elementarmente le funzioni circolari occorre fare ricorso a concetti facili da intuire, ma non facili da giustificare rigorosamente: parleremo di versi di percorrenza di un circolo, di *archi di cerchio* e di lunghezza dei medesimi, cose che potranno venire economicamente spiegate solo in futuro. Le funzioni circolari sono in realtà strettamente legate alle funzioni esponenziali, ma questo legame può essere riconosciuto solo nel campo complesso $\mathbb{C}$. È però utile acquistare fin d'ora familiarità con queste funzioni, la cui interpretazione geometrica deve comunque essere conosciuta. Nel prossimo numero diremo quali sono i *postulati* intuitivamente accettati, e non dimostrati, che stanno alla base della nostra trattazione *ingenua* delle funzioni circolari. Anche i grafici di queste vanno per ora presi come articoli di fede (geometricamente ci si può rendere conto del fatto che sono davvero come li faremo).