Il completamento di uno spazio metrico ed i numeri p-adici

Andrea Mori
Dip.to di Matematica, Università di Torino

Versione Novembre 2002

Introduzione

La costruzione dell'insieme $\mathbf{Z}$ dei numeri interi relativi e dell'insieme $\mathbf{Q}$ dei numeri razionali a partire dall'insieme $\mathbf{N} = \{0, 1, 2, 3, \cdots\}$ dei numeri naturali[1] è motivata da esigenze di tipo puramente algebrico. In breve, $\mathbf{Z}$ e $\mathbf{Q}$ possono essere caratterizzati rispettivamente come il più piccolo anello ed il più piccolo campo contenenti $\mathbf{N}$.

L'insieme $\mathbf{R}$ dei numeri reali (la cui prima motivazione è data dalla necessità di misurare i segmenti della geometria elementare[2]) è ottenuto con tecniche di natura diversa. Delle varie costruzioni possibili isoliamo in particolare quella che rivede i numeri reali come limiti di successioni di Cauchy di numeri razionali. La definizione di successione di Cauchy fa entrare in gioco (per la prima volta) la struttura *metrica* di $\mathbf{Q}$, cioè una struttura non algebrica.

La costruzione appena ricordata può essere replicata nel caso apparentemente ben più generale di uno spazio metrico qualsiasi. Dato uno spazio metrico X costruiremo uno spazio metrico più grande X^c che gode della proprietà seguente: ogni successione di Cauchy in X^c converge in X^c. Il fatto che uno spazio metrico possieda tale proprietà è estremamente utile. Per esempio, in certe situazioni essa permette di costruire soluzioni di equazioni mediante approssimazioni successive.

Applicheremo questa costruzione generale per costruire i campi di numeri p-adici $\mathbf{Q}_p$ che hanno una notevole importanza in aritmetica. Il punto di partenza sarà la definizione, sul campo razionale $\mathbf{Q}$ di una *metrica p-adica* non equivalente alla metrica naturale definita dal valore assoluto archimedeo.

1 Successioni

Sia X uno spazio topologico. Una *successione* in X è una funzione $s\colon \mathbf{N} \to X$. Se dotiamo $\mathbf{N}$ della topologia discreta non è restrittivo assumere che la successione s sia una funzione continua.

Assegnati elementi $x_1, x_2, \ldots \in X$ in questo ordine, esiste un'unica successione s in X tale che $s(n) = x_n$. Pertanto non è ambiguo identificare la successione s con l'insieme ordinato $\{x_n\}$ dove $x_n = s(n)$. Nel seguito useremo indifferentemente l'una o l'altra notazione.

Sia $x \in X$. Diciamo che la successione $\{x_n\}$ *converge* a x (o che x è il *limite* della successione), e scriviamo $\lim x_n = x$, se è soddisfatta la condizione seguente:

[1] A volte torna comodo escludere 0 da $\mathbf{N}$. Includeremo lo zero in $\mathbf{N}$ o no a seconda delle esigenze del momento.

[2] La tradizione vuole che il primo ad accorgersi dell'inadeguatezza di $\mathbf{Q}$ per le misurazioni fu Pitagora, che dimostrò l'incommensurabilità della diagonale e del lato di un quadrato (cioè $\sqrt{2} \notin \mathbf{Q}$).

per ogni intorno U di x esiste $N = N_U \in \mathbf{N}$ tale che $x_n \in U$ per ogni $n > N$.

Diciamo che la successione $\{x_n\}$ *non converge* se per ogni $x \in X$ la successione non converge a x.

Esempio 1 In $X = \mathbf{R}$ con la topologia euclidea consideriamo la successione $\{1/n\}$. Allora $\lim(1/n) = 0$ in quanto dato un intorno U di 0 esiste un $\epsilon > 0$ tale che $(-\epsilon, \epsilon) \subseteq U$. Allora scelto $N > 1/\epsilon$ si ha che $1/n \in U$ per ogni $n > N$.

Esempio 2 In $X = \mathbf{R}$ con la topologia euclidea la successione $\{n\}$ non converge.

È interessante osservare che in generale il limite di una successione non è unico. Ad esempio, si consideri $X = \mathbf{R}$ con la topologia di Zariski e la successione $\{n\}$. Vediamo che per ogni $r \in \mathbf{R}$ si ha $\lim n = r$. Infatti ogni aperto non vuoto U è il complementare di un insieme finito di numeri reali e quindi $n \in U$ per n sufficientemente grande (v. Problemi 1 e 2).

Sotto quali condizioni vale l'unicità del limite? La proposizione seguente risponde a questa domanda.

Proposizione 3 *Sia X uno spazio di Hausdorff. Ogni successione convergente ammette un unico limite.*

Dimostrazione : Supponiamo per assurdo che si abbia $\lim x_n = x$ e $\lim x_n = y$ con $x \neq y$ per una certa successione $\{x_n\}$. Poichè X è di Hausdorff possiamo trovare aperti $x \in A$ e $y \in B$ tali che $A \cap B = \emptyset$. Questo contraddice l'ipotesi perchè dovremmo anche avere $x_n \in A$ e $x_n \in B$ per n sufficientemente grande. ∎

In particolare si ha l'unicità del limite delle successioni in spazi metrici. Da ora in poi assumiamo che X è uno spazio metrico. Per ogni $x \in X$ e per ogni numero reale $\epsilon > 0$ denotiamo $S(x, \epsilon)$ la *sfera aperta di centro x e raggio ϵ*, ovvero l'insieme dei punti di X che distano da x meno di ϵ.

2 Successioni in uno spazio metrico

In uno spazio metrico è possibile caratterizzare i sottoinsiemi chiusi in termini di successioni convergenti:

Proposizione 4 *Sia S un sottoinsieme di uno spazio metrico X e sia $x \in X$. Allora $x \in \bar{S}$ se e soltanto se esiste una successione $\{s_n\}$ in S tale che $\lim s_n = x$*

Dimostrazione : Supponiamo dapprima che $x \in \bar{S}$ e consideriamo l'aperto $U_n = S(x, 1/n)$. Si ha l'ovvia catena di inclusioni $U_1 \supseteq U_2 \supseteq \cdots$. Definiamo una successione $\{s_n\}$ scegliendo come s_n un punto arbitrario in $U_n \cap S$. Allora la successione $\{s_n\}$ è in S e converge a x perchè ogni aperto contenente x contiene anche tutti gli U_n per n sufficientemente grande.

D'altra parte, se la successione $\{s_n\}$ in S converge a x, per ogni aperto $x \in U$ deve risultare $x_n \in U$ per n sufficientemente grande. Quindi $U \cap S \neq \emptyset$ e $x \in \bar{S}$. ∎

La proposizione precedente comporta che in uno spazio metrico i chiusi (e quindi tutta la topologia) si possono ricostruire a partire dalle successioni convergenti. In altre parole, in uno spazio metrico è equivalente assegnare la topologia o l'insieme delle successioni convergenti. Allora è lecito aspettarsi che anche le funzioni continue siano caratterizzabili in termini di successioni. Questo è l'oggetto della proposizione seguente.

Proposizione 5 *Sia X uno spazio metrico e Z uno spazio topologico qualsiasi. Allora una funzione $f: X \to Z$ è continua in $x \in X$ se e soltanto se per ogni successione $\{x_n\}$ in X convergente a x la successione $\{f(x_n)\}$ converge a $f(x)$.*

Dimostrazione : Sia $f: X \to Z$ continua in x e poniamo $z = f(x)$. Sia $\{x_n\}$ una successione convergente a x e sia V un intorno di z in Z. Allora $f^{-1}(V)$ è un intorno di x in X. Dunque deve risultare $x_n \in f^{-1}(V)$ per n sufficientemente grande. Per gli stessi n, $f(x_n) \in V$, cioè $\lim f(x_n) = z$.

Per dimostrare l'implicazione opposta possiamo equivalentemente supporre f non continua in x e costruire una successione $\{x_n\}$ convergente ad x tale che $\{f(x_n)\}$ non converga a z. Poniamo ancora $U_n = S(x, 1/n)$. Poichè f non è continua in x, c'è un intorno V di z tale che per ogni n, $f(U_n) \not\subset V$. Allora scegliendo $x_n \in U_n$ in modo che $f(x_n) \notin V$ otteniamo una successione convegente a x tale che $\{f(x_n)\}$ non converge a z. ■

Poichè la topologia di uno spazio metrico è interamente definita dalla metrica, non deve sorprendere che anche le successioni convergenti possano essere descritte in termini della metrica.

Proposizione 6 *Siano $\{x_n\}$ una successione in uno spazio metrico (X, d) e $x \in X$. Allora $\lim x_n = x$ se e soltanto se $\lim d(x_n, x) = 0$.*

Dimostrazione : È noto che la funzione $d_x: X \to \mathbf{R}$ definita come $d_x(y) = d(x, y)$ è continua. Allora se $\lim x_n = x$, la proposizione 3 implica che la successione di numeri reali $\{d_x(x_n)\}$ converge a $d_x(x) = d(x, x) = 0$.

Supponiamo invece di avere $\lim d(x_n, x) = 0$. Allora per ogni $\epsilon > 0$ esiste N tale che $d(x_n, x) < \epsilon$ per ogni $n > N$. Cioè $x_n \in S(x, \epsilon)$ per ogni $n > N$. Siccome ogni intorno $x \in U$ contiene una sfera $S(x, \epsilon)$, questo dimostra che $\lim x_n = x$. ■

La proposizione appena dimostrata non caratterizza però completamente le successioni convergenti nel senso che non serve a decidere se una successione s è convergente guardando semplicemente ai punti x_n. L'esempio seguente mostra che un criterio di convergenza per una successione non può prescindere da un analisi delle proprietà generali dello spazio.

Esempio 7 Sia $X = \mathbf{R}$ con la metrica euclidea e sia $Y = (0, 1)$. La successione $\{1/n\}$ converge (a 0) in X ma non converge in Y (perchè $0 \notin Y$).

3 Successioni di Cauchy

Diciamo che una successione $\{x_n\}$ in uno spazio metrico (X, d) è una *successione di Cauchy* se per ogni $\epsilon > 0$ esiste un N tale che per ogni m ed $n > N$ si ha $d(x_m, x_n) < \epsilon$.

Le successioni convergenti sono l'esempio più immediato di successioni di Cauchy. Infatti se $\lim x_n = x$, fissato $\epsilon > 0$ esiste N tale che per ogni $n > N$ si ha $d(x_n, x) < \epsilon/2$. Allora, per ogni $m, n > N$,

$$d(x_m, x_n) \leq d(x_m, x) + d(x, x_n) < \epsilon.$$

D'altra parte **esistono successioni di Cauchy non convergenti**. Nell'esempio 3, la successione $\{1/n\}$ è di Cauchy (v. Problema 4) ma non converge in $(0, 1)$.

Definizione 8 *Diciamo che uno spazio metrico X è completo se ogni succesione di Cauchy in X converge in X.*

Esempio 9 Esempi di spazi completi sono

a) $\mathbf{R}$ con la metrica euclidea.

b) Ogni sottospazio chiuso C di uno spazio completo X. Infatti se $\{c_n\}$ è una successione in C, esiste $\lim c_n = x \in X$. Per la proposizione 1 si ha $x \in \bar{C} = C$ e quindi C è completo.

Inoltre, ogni sottospazio completo S di uno spazio completo X è chiuso. Infatti, dato $x \in \bar{S}$ possiamo costruire, per la Proposizione 2, una successione $\{x_n\}$ in S convergente a x. Siccome S è supposto completo e $\{x_n\}$ è una successione di Cauchy, $x \in S$.

L'esempio 3 sopra mostra anche che *la completezza non è una proprietà topologica.* Infatti gli spazi $(0, 1)$ e $\mathbf{R}$ sono omeomorfi ma solo il secondo è completo. Ciò dipende dal fatto che per una successione essere di Cauchy dipende dalla metrica e non dalla topologia (v. Problema 5). Come ulteriore esempio si consideri lo spazio $X = \{1/n\}_{n\in\mathbf{N}}$. Lo spazio X eredita la metrica euclidea d da $\mathbf{R}$ e siccome X è discreto, la metrica d è equivalente alla metrica discreta d'. Però (X, d') è completo e (X, d) no.

4 Completamento

L'esistenza di spazi metrici non completi porta a dare la seguente

Definizione 10 *Sia X uno spazio metrico. Uno spazio metrico Y si dice un completamento di X se:*

a) Y è completo;

b) Esiste un'isometria $i: X \to Y$ tale che $i(X)$ è denso in Y.

La richiesta b) sopra significa che il completamento Y deve essere il più piccolo possibile fra gli spazi soddisfacenti la a) (in quanto, per l'Esempio 4, se $X \subset Y$ con Y completo, lo spazio $\bar{X}$ è un completamento di X). Evidentemente se X è completo, il suo unico completamento è X stesso. Sorgono immediatamente i seguenti problemi:

1. Quali spazi metrici X possiedono un completamento?
2. Può uno stesso spazio metrico possedere più completamenti diversi, cioè non isometrici[3] fra di loro?

Dato uno spazio metrico (X, d), consideriamo l'insieme

$$\mathcal{C}(X) = \{\text{successioni } s: \mathbf{N} \longrightarrow X \text{ di Cauchy}\}$$

ed osserviamo che per ogni $\{x_n\}$, $\{y_n\} \in \mathcal{C}(X)$ la successione di numeri reali $\{d(x_n, y_n)\}$ converge. Infatti applicando ripetutamente la disuguaglianza triangolare al quadrilatero di vertici x_m, x_n, y_m, y_n, otteniamo

$$d(x_n, y_n) \leq d(x_m, x_n) + d(x_m, y_m) + d(y_m, y_n)$$

e

$$d(x_m, y_m) \leq d(x_m, x_n) + d(x_n, y_n) + d(y_m, y_n).$$

Queste due disuguaglianze possono riscriversi equivalentemente come

$$|d(x_n, y_n) - d(x_m, y_m)| \leq d(x_m, x_n) + d(y_m, y_n). \tag{1}$$

[3]Nella categoria degli spazi metrici la relazione di "isomorfismo" naturale è quella di isometria. Naturalmente ci si potrebbe chiedere se esistano completamenti non omeomorfi nelle topologie associate alle metriche. Una risposta negativa alla domanda del testo implica una risposta negativa anche alla domanda in questa nota, ma non viceversa.

Fissato $\epsilon > 0$ e ricordando che le successioni scelte sono di Cauchy, possiamo trovare N tale che per ogni $m, n > N$ si ha $d(x_m, x_n) < \epsilon/2$ e $d(y_m, y_n) < \epsilon/2$. Allora dalla formula 1 segue che per gli stessi m ed n vale la

$$|d(x_n, y_n) - d(x_m, y_m)| \leq \epsilon.$$

Dunque la successione $\{d(x_n, y_n)\}$ è di Cauchy, e quindi converge perchè $\mathbf{R}$ è completo. Questo permette di definire una funzione $\delta \colon \mathcal{C}(X) \times \mathcal{C}(X) \to \mathbf{R}$ come segue: date successioni $f, g \in \mathcal{C}(X)$ poniamo

$$\delta(f, g) = \lim_{n \to \infty} d(f(n), g(n)). \tag{2}$$

La funzione δ soddisfa le proprietà seguenti:

(P1) $\delta(f, f) = 0$ per ogni $f \in \mathcal{C}(X)$.

(P2) Per ogni $f, g \in \mathcal{C}(X)$, $\delta(f, g) = \delta(g, f)$

(P3) Per ogni $f, g, h \in \mathcal{C}(X)$, $\delta(f, g) \leq \delta(f, h) + \delta(g, h)$.

Le proprietà (P1) e (P2) seguono immediatamente dalla definizione 2. La (P3) si ottiene applicando la definizione 2 alla consueta disuguaglianza triangolare valida per d.

La funzione δ non è pero una metrica[4] in quanto è possibile avere $\delta(f, g) = 0$ con $f \neq g$. È quanto accade, ad esempio, con le successioni reali $f(n) = 1/n$ e $g(n) = 2/n$.

Nell'insieme $\mathcal{C}(X)$ introduciamo la relazione

$$f \sim g \text{ se e soltanto se } \delta(f, g) = 0. \tag{3}$$

Proposizione 11 *La relazione $\sim$ è una relazione di equivalenza.*

Dimostrazione : Riflessività e simmetria sono immediate. Supponiamo $f \sim g$ e $g \sim h$. Allora, per la (P3), $0 \leq \delta(f, h) \leq \delta(f, g) + \delta(g, h) = 0 + 0 = 0$ e dunque $\delta(f, h) = 0$. ∎

Possiamo allora definire l'insieme

$$X^c = \mathcal{C}(X)/\sim$$

(privo, per ora, di struttura). Denotiamo f^c la classe in X^c di $f \in \mathcal{C}(X)$. Definiamo una funzione $\Delta \colon X^c \times X^c \to \mathbf{R}$ come

$$\Delta(f^c, g^c) = \delta(f, g). \tag{4}$$

Naturalmente occorre verificare che la funzione Δ è ben definita, cioè bisogna controllare che se $f_1^c = f_2^c$ e $g_1^c = g_2^c$ allora $\delta(f_1, g_1) = \delta(f_2, g_2)$ (v. Problema 7). Una volta fatto questo, si osservi che le proprietà (P1)..(P3) risultano soddisfatte anche dalla funzione Δ. Inoltre supponiamo di avere $\Delta(f^c, g^c) = 0$, allora $0 = \Delta(f^c, g^c) = \delta(f, g)$ e dunque $f^c = g^c$.

Questa analisi ci permette di concludere che (X^c, Δ) è uno spazio metrico. Il seguente teorema dice che X^c è proprio lo spazio che andavamo cercando.

Teorema 12 (Esistenza del Completamento)

1) (X^c, Δ) è uno spazio metrico completo.

2) C'è un'isometria $i \colon X \to X^c$ tale che $i(X)$ è denso in X^c.

3) $X = X^c$ se e soltanto se X è completo.

[4] Una funzione soddisfacente le proprietà formali (P1)...(P3) è detta una *pseudometrica*.

Dimostrazione : Come abbiamo già notato, il terzo punto segue dai primi due.

Iniziamo dimostranto il punto 2). Definiamo una mappa $i\colon X \to X^c$ ponendo

$$i(x) = {i_x}^c$$

dove i_x è la successione costante $i_x(n) = x$ in X. Per ogni $x, y \in X$ si ha $\Delta({i_x}^c, {i_y}^c) = \delta(i_x, i_y) = \lim d(i_x(n), i_y(n)) = d(x, y)$, dunque i è un'isometria.

Per dimostrare che $i(X)$ è denso in X^c, scegliamo un elemento $f^c \in X^c$ e fissiamo $\epsilon > 0$. Possiamo allora trovare $N > 0$ tale che per ogni $m, n > N$ si ha $d(f(m), f(n)) < \epsilon/2$. Sia $M > N$ e consideriamo la successione costante $i_M = i_{f(M)}$. Allora $\Delta(f^c, {i_M}^c) = \delta(f, i_M) = \lim_{n\to\infty} d(f(n), f(M)) \leq \epsilon/2 < \epsilon$. Siamo così riusciti a trovare un elemento in $i(X)$ a distanza $< \epsilon$ da f^c per ϵ arbitrario. Per la genericità della scelta di f^c, questo vuol dire che $i(X)$ è denso in X^c.

Dimostriamo ora il punto 1). Sia $\{{f_n}^c\} \in \mathcal{C}(X^c)$. Dobbiamo mostrare che questa successione converge in X^c. Siccome, da quanto appena dimostrato, $i(X)$ è denso in X^c, possiamo scegliere per ogni $n > 0$ un elemento $z_n \in X$ tale che la successione costante $i_n = i_{z_n}$ soddisfa la disuguaglianza

$$\Delta({f_n}^c, {i_n}^c) < 1/n. \tag{5}$$

Applicando la disuguaglianza triangolare per Δ e la formula (5) otteniamo $d(z_m, z_n) = \Delta({i_m}^c, {i_n}^c) \leq \Delta({i_m}^c, {f_m}^c) + \Delta({f_m}^c, {f_n}^c) + \Delta({i_n}^c, {f_n}^c) < \Delta({f_m}^c, {f_n}^c) + (1/m) + (1/n)$. Scegliamo $\epsilon > 0$, possiamo allora trovare $N > 0$ tale che per ogni $m, n > N$ si ha $\Delta({f_m}^c, {f_n}^c) < \epsilon/2$. Se risulta essere anche $m, n > 4/\epsilon$, la stima calcolata sopra fornisce la disuguaglianza

$$d(z_m, z_n) < (\epsilon/2) + 2(\epsilon/4) = \epsilon.$$

Ciò dimostra che $\{z_n\}$ è una successione di Cauchy. Sia z^c la sua classe di equivalenza in X^c.

Per ogni n, dalla posizione (5) segue

$$\Delta(z^c, {f_n}^c) \leq \Delta(z^c, {i_n}^c) + \Delta({i_n}^c, {f_n}^c) < \lim_{m\to\infty} d(z_m, z_n) + (1/n).$$

Scelto $\epsilon > 0$ è possibile trovare $N > 0$ tale che per ogni $m, n > N$ si ha $\lim_{m\to\infty}(z_m, z_n) \leq \epsilon/2$. Se si ha anche $n > 2/\epsilon$ la stima precedente fornisce la disuguaglianza

$$\Delta(z^c, {f_n}^c) < \epsilon/2 + \epsilon/2 = \epsilon.$$

Questo significa che $\lim {f_n}^c = z^c$. Il teorema è così dimostrato. ■

Rimane ancora da rispondere alla seconda domanda che ci eravamo posti a pag. 5. La risposta è fornita dal teorema seguente.

Teorema 13 (Unicità del Completamento) *Siano (Y, i) e $(Y', i'))$ due completamenti dello spazio metrico X. Allora esiste un'isometria $\psi\colon Y \to Y'$ tale che $\psi \circ i = i'$.*

Dimostrazione : La composizione $\psi_0 = i \circ (i')^{-1}$ è certamente un isometria $i(X) \to i'(X)$ che soddisfa la richiesta dell'enunciato. Si tratta di vedere che ψ_0 può estendersi a tutto Y.

Sia $y \in Y$. Poichè $i(X)$ è denso in Y, possiamo scegliere una successione $\{y_n\}$ in $i(X)$ che convege ad y. Allora $\{y_n\} \in \mathcal{C}(i(X))$ e siccome ψ_0 è un'isometria, la successione $\{y'_n\}$, dove $y'_n = \psi_0(y_n)$, è una successione di Cauchy in $i'(X)$. Poichè Y' è completo, la successione $\{y'_n\}$ converge. Sia $y' = \lim y'_n$ e poniamo $\psi(y) = y'$.

Si dimostra (v. Problema 8) che la mappa ψ così costruita è ben definita, è definita su tutto Y, è invertibile ed infine è anche un'isometria. La seconda richiesta dell'enunciato risulta verificata in quanto $\psi|_{i(X)} = \psi_0$. ■

Dunque lo spazio metrico (X^c, Δ) è l'unico a meno di isometria che risponda ai requisiti richiesti. Esso è detto il *completamento* di X.

5 I numeri p-adici

In questa sezione applichiamo la teoria svolta nei §§ precedenti per costruire degli spazi metrici di notevolissimo interesse aritmetico a partire da certe metriche non euclidee definite sul campo $\mathbf{Q}$ dei numeri razionali.

Iniziamo ricordando il

Teorema 14 (Teorema Fondamentale dell'Aritmetica) *Ogni $n \in \mathbf{Z}$ non nullo si decompone in modo unico*[5] *come prodotto di numeri primi e ± 1.*

Fissiamo un numero primo p. In virtù del Teorema appena citato, ogni numero $q \in \mathbf{Q}$, $q \neq 0$, può scriversi in modo unico nella forma

$$q = p^{e_p(q)} \frac{a}{b}$$

dove a e b sono numeri interi relativi non divisibili per p ed $e_p(q) \in \mathbf{Z}$.

Esempio 15 Posto $p = 3$ si ha

$$\frac{1}{5} = 3^0 \frac{1}{5}, \qquad \frac{4}{99} = 3^{-2} \frac{4}{11}, \qquad \frac{54}{7} = 3^3 \frac{2}{7},$$

quindi $e_3(1/5) = 0$, $e_3(4/99) = -2$, $e_3(54/7) = 3$.

La funzione $e_p(\cdot)$ soddisfa la proprietà

$$e_p(1) = 0, \qquad e_p(q_1 q_2) = e_p(q_1) + e_p(q_2) \tag{6}$$

e quindi definisce un omomorfismo (suriettivo) tra il gruppo moltiplicativo del campo $\mathbf{Q}$ ed il gruppo additivo $\mathbf{Z}$ (v. Problema 9). Definiamo una mappa $|\cdot|_p \colon \mathbf{Q} \to \mathbf{R}$ come

$$|q|_p = \begin{cases} p^{-e_p(q)}, & \text{se } q \neq 0, \\ 0, & \text{se } q = 0. \end{cases}$$

Il valore $|q|_p$ si dice *valore assoluto p-adico* di q.

Proposizione 16 *La funzione $|\cdot|_p$ soddisfa le proprietà seguenti:*

1) $|q|_p \geq 0$, e l'uguaglianza vale se e soltanto se $q = 0$;

2) $|q_1 q_2|_p = |q_1|_p |q_2|_p$;

3) $|q_1 + q_2|_p \leq \max\{|q_1|_p, |q_2|_p\}$

Dimostrazione : Le prime due proprietà seguono immediatamente dalla definizione e dalla 6. Per ottenere la terza proprietà, poniamo $q_1 = p^{e_p(q_1)}(u/v)$ e $q_2 = p^{e_p(q_2)}(x/y)$, dove possiamo senz'altro assumere $e_p(q_2) \geq e_p(q_1)$. Allora $q_1 + q_2 = p^{e_p(q_1)}(U/V)$ dove sicuramente p non divide V (in quanto $V = vy$). Quindi $e_p(q_1 + q_2) \geq e_p(q_1)$ (in generale non vale l'uguaglianza perchè p potrebbe dividere U) da cui segue la formula cercata. ■

Definiamo ora una funzione $d_p \colon \mathbf{Q} \times \mathbf{Q} \to \mathbf{R}$ ponendo

$$d_p(q_1, q_2) = |q_1 - q_2|_p.$$

[5] La convenzione secondo cui 1 non è un numero primo è adottata per salvaguardare questa unicità. Infatti se 1 fosse considerato primo si avrebbero infinite decomposizioni distinte, ad esempio $6 = 2\times 3 = 1\times 2\times 3 = 1\times 1\times 2\times 3$, etc.

Proposizione 17 *La funzione d_p definisce una metrica in $\mathbf{Q}$.*

Dimostrazione : Dalla proprietà 1) della Proposizione 6 segue che $d_p(x,y) \geq 0$ e che l'uguaglianza vale se e soltanto se $x = y$.

Combinando la proprietà 2) della Proposizione 6 col fatto che $|-1|_p = 1$ si ottiene $d_p(x,y) = |x-y|_p = |-(y-x)|_p = |-1|_p|y-x|_p = |y-x|_p = d_p(y,x)$.

Infine, dalla proprietà 3) della Proposizione 7 possiamo far discendere che

$$d_p(x,y) \leq \max\{d_p(x,z), d_p(y,z)\} \leq d_p(x,z) + d_p(y,z),$$

ovvero la funzione d_p soddisfa la disuguaglianza triangolare[6]. ∎

Osserviamo che la metrica d_p appena costruita non è equivalente alla metrica euclidea di $\mathbf{Q}$. Per vedere questo consideriamo la successione $s(n) = p^n$. Siccome $d_p(p^n, 0) = |p^n - 0|_p = |p^n|_p = p^{-n} \to 0$ per $n \to \infty$, per la Proposizione 4 si ha che $\lim p^n = 0$ Allora, per la Proposizione 2, 0 appartiene alla chiusura dell'insieme $\{p^n\}$ nella topologia definita dalla metrica d_p. Però 0 non appartiene a quella chiusura nella topologia euclidea, e questo dimostra l'asserto.

Possiamo ora chiederci se $\mathbf{Q}$ è completo per la metrica d_p.

Esempio 18 *Consideriamo una successione x_n soddisfacente le seguenti congruenze :*

$$x_n^2 + 1 \equiv 0 \bmod 5^n, \qquad x_{n+1} \equiv x_n \bmod 5^n. \tag{7}$$

Questa può essere costruita induttivamente come segue. Sia a_1=2. Supposto di aver costruito $a_1, a_2, \ldots, a_n$, poniamo $a_n^2 + 1 = 5^n c_n$ e definiamo $a_{n+1} = a_n + b5^n$, dove b è una soluzione della congruenza $c_n + 2a_n b \equiv 0 \bmod 5$. La seconda congruenza in 7 significa che la successione $\{x_n\}$ è di Cauchy. Supponiamo che la successione converga e sia $\lim x_n = x$. Allora siccome si ha $|x_n^2 + 1|_5 \leq 5^{-n}$ dalla prima congruenza in 7, dobbiamo avere $|x^2 + 1|_5 = 0$, cioè $x^2 + 1 = 0$. Ma questo non è possibile (in $\mathbf{Q}$).

Proposizione 19 $\mathbf{Q}$ *non è completo rispetto alla metrica d_p.*

Dimostrazione : L'esempio 6 mostra una successione di Cauchy in $(\mathbf{Q}, d_5)$ che non converge. Esempi analoghi si possono costruire per d_p con p qualunque. ∎

Definizione 20 *Si dice campo dei numeri p-adici $\mathbf{Q}_p$ il completamento dello spazio metrico $(\mathbf{Q}, d_p)$.*

Il nome di campo dato al completamento $\mathbf{Q}_p$ è giustificato dalla seguente

Proposizione 21 *Il completamento $\mathbf{Q}_p$ possiede una struttura algebrica naturale di campo, rispetto alla quale l'immersione canonica $\mathbf{Q} \subset \mathbf{Q}_p$ è un omomorfismo.*

Dimostrazione : Assegnati α e $\beta \in \mathbf{Q}_p$, scegliamo succesioni di Cauchy $\{\alpha_n\}$ e $\{\beta_n\}$ in $(\mathbf{Q}_p, d_p)$ che rappresentino rispettivamente α e β.

Osserviamo che le successioni $\{\alpha_n + \beta_n\}$ e $\{\alpha_n \beta_n\}$ sono di Cauchy. Infatti abbiamo

$$|\alpha_{n+1} + \beta_{n+1} - \alpha_n - \beta_n|_p \leq \max\big\{|\alpha_{n+1} - \alpha_n|_p, |\beta_{n+1} - \beta_n|_p\big\} \leq \epsilon$$

[6] La disuguaglianza $d(x,y) \leq \max\{d_p(x,z), d_p(y,z)\}$ si dice *disuguaglianza ultrametrica*. Essa è evidentemente più forte della disuguaglianza triangolare. Uno spazio metrico (X,d) si dice *ultrametrico* se la d soddisfa la disuguaglianza ultrametrica.

per $n >> 0$. Similmente per l'altra. Possiamo allora porre

$$\alpha + \beta = \{\alpha_n + \beta_n\}^c, \qquad \alpha\beta = \{\alpha_n \beta_n\}^c.$$

Queste operazioni in $\mathbf{Q}_p$ sono ben definite in quanto, per esempio, se $\{\alpha_n\} \sim \{\alpha'_n\}$ e $\{\beta_n\} \sim \{\beta'_n\}$, allora $\lim(\alpha_n + \beta_n) = \lim \alpha_n + \lim \beta_n = \lim \alpha'_n + \lim \beta'_n = \lim(\alpha'_n + \beta'_n)$, cioè $\{\alpha_n + \beta_n\}^c = \{\alpha'_n + \beta'_n\}^c$ (considerazioni analoghe valgono per il prodotto).

Con queste operazioni, $\mathbf{Q}_p$ è un campo. Infatti:

- Gli elementi neutri di somma e prodotto sono dati, rispettivamente, da ${i_0}^c$ e ${i_1}^c$ (notazione come nella dimostrazione del Teorema di Esistenza del Completamento)
- L'opposto dell'elemento $\alpha = \{\alpha_n\}^c$ è $-\alpha = \{-\alpha_n\}^c$.
- Se $\alpha = \{\alpha_n\} \neq 0$, deve aversi $\alpha_n \neq 0$ per $n >> 0$. Sia t un numero tale che $\alpha_n \neq 0$ per ogni $n > t$, allora la successione

  $$\beta_n = \begin{cases} 0 & \text{se } n \leq t \\ \alpha_n^{-1} & \text{se } n > t \end{cases}$$

  è ben definita ed è di Cauchy. La sua classe di equivalenza β è un inverso moltiplicativo di α.

Infine osserviamo che $i_{x+y} = i_x + i_y$ e $i_{xy} = i_x i_y$ e dunque l'immersione canonica di $\mathbf{Q}$ in $\mathbf{Q}_p$ è anche un omomorfismo di campi. ∎

Abbiamo così costruito una famiglia infinita di metriche su $\mathbf{Q}$, parametrizzate dai numeri primi (v. Problema 10). Ci si può chiedere se quelle costruite sinora siano *tutte* le metriche possibili su $\mathbf{Q}$, o se non sia possibile costruirne altre. Il teorema seguente, di cui diamo solo l'enunciato[7] (dove per metrica banale intendiamo quella discreta) risponde completamente a questa domanda.

Teorema 22 (Ostrowski) *Ogni metrica non banale su $\mathbf{Q}$ è equivalente o alla metrica euclidea, oppure ad una metrica d_p con p numero primo opportuno.*

6 Problemi

Problema 1 *Si consideri la topologia di Zariski in $\mathbf{R}$.*

- *Sia $\{x_n\}$ la successione tale che $x_n = 0$ se n è pari e $x_n = 1$ se n è dispari. Per quali $r \in \mathbf{R}$ si ha $\lim x_n = r$?*
- *Si dimostri che non esistono successioni non convergenti.*

Problema 2 *Si costruisca una successione non convergente in $\mathbf{Q}$ con la topologia di Zariski.*

Problema 3 *Verificare che le successioni seguenti di numeri reali sono successioni di Cauchy:*

- $\{1/n^\alpha\}$, *dove* $\alpha > 1$.
- $\{n/n+1\}$.

[7] La dimostrazione non è breve, ma è concettualmente semplice. Il lettore interessato può—oltre che provare ad ottenerla da sè come esercizio—consultare J.W.S. Cassels, *Local Fields*, London Math. Society Student Texts, 3 (1986), pp. 16 e segg.

- $\{\int_n^{n+1} f(x)\,dx\}$ *dove* $f(x)$ *è un'arbitraria funzione positiva monotona decrescente definita in* $x \in (0, \infty)$.

Problema 4 *Siano* $X_1, \ldots, X_n$ *spazi completi. Dimostrare che il prodotto* $X_1 \times \cdots \times X_n$ *è uno spazio completo.*

Problema 5 *Siano* X *e* Y *due spazi metrici isometrici. Dimostrare che* X *è completo se e soltanto se* Y *è completo.*

Problema 6 *Dimostrare che la funzione* Δ *definita dalla formula 4 nel §5 è ben definita.*

Problema 7 *Completare i dettagli della dimostrazione del Teorema di Unicità. Precisamente, dimostrare che :*

- *Siano* A *e* B *spazi metrici e supponiamo assegnata un'isometria* $\varphi\colon A \to B$. *Allora, la successione* $\{a_n\}$ *in* A *è di Cauchy se e soltanto se la successione* $\{\varphi(a_n)\}$ *è di Cauchy in* B.
- *La mappa* ψ *è ben definita.*
- *La mappa* ψ *è invertibile.*
- *La mappa* ψ *è un'isometria.*

Problema 8 *Dimostrare in dettaglio che la funzione* $e_p(\cdot)$ *definisce un omomorfismo suriettivo tra il gruppo moltiplicativo di* $\mathbf{Q}$ *ed il gruppo additivo di* $\mathbf{Z}$. *Descriverne il nucleo in modo più esplicito possibile.*

Problema 9 *Siano* p *e* q *due primi distinti. Dimostrare che le metriche* d_p *e* d_q *non sono mai equivalenti.*

Problema 10 *Dimostrare che non esiste alcun elemento* $x \in \mathbf{Q}_p$ *tale che* $x^2 = p$.

Problema 11 *Completare i dettagli della dimostrazione della Proposizione 9.*