Lezione del 18 marzo; Registro dettagliato

1. Nel seguito mettiamo in relazione la costruzione del campo $\mathbb{Q}$ a partire dal dominio d'integrita' $\mathbb{Z}$ come caso particolare della costruzione del campo dei quozienti di un domnio d'integrita' (come sinteticamente data nella lezione precedente) con una presentazione del campo $\mathbb{Q}$ per una scuola media (per una trattazione piu' ampia cfr: EAV1415, Par. 3.4 pp. 69-79).

2. **Relazione d'equivalenza**. Abbiamo considerato l'insieme delle frazioni di interi con denominatore non nullo; abbiamo definito una relazione d'equivalenza dicendo che una prima frazione e' equivalente ad una seconda frazione se e solo se il numeratore della prima per il denominatore della seconda e' uguale al denominatore della prima per il numeratore della seconda; abbiamo definito l'insieme $\mathbb{Q}$ dei numeri razionali come l'insieme quoziente dell'insieme delle frazioni rispetto a questa relazione d'equivalenza.

   Ci sono altri modi di definire la stessa relazione d'equivalenza, due esempi:

   (1) dicendo che una prima frazione e' equivalente ad una seconda frazione se e solo se la prima si puo' trasformare nella seconda mediante un passo del tipo "moltiplicare numeratore e denominatore per uno stesso intero" e/o un passo del tipo "dividere (quando possibile) numeratore e denominatore per uno stesso intero";

   (2) dicendo che due frazioni sono equivalenti se e solo se si possono trasformare in una stessa frazione mediante un passo del tipo "moltiplicare numeratore e denominatore per uno stesso intero".

   L'operazione di "dividere (quando possibile) numeratore e denominatore per uno stesso intero" si dice "semplificazione".

   Un insieme di rappresentanti canonici per le classi d'equivalenza e' costituito dalle "frazioni ridotte ai minimi termini". cioe' dalle frazioni del tipo $\frac{a}{b}$ con $b > 0$ e $\mathrm{MCD}(a, b) = 1$, compreso il caso limite $\frac{0}{1}$.

   Per abuso di notazione, ciascun numero razionale viene identificato con una qualsiasi frazione che lo rappresenta (ridotta o meno), e dunque l'uguaglianza di numeri razionali viene ad essere identificata con l'equivalenza di frazioni.

3. **Operazioni**. Abbiamo definito operazioni di addizione e moltiplicazione di frazioni ponendo

   $$\frac{a_1}{b_1} + \frac{a_2}{b_2} = \frac{a_1 b_2 + b_1 a_2}{b_1 b_2}, \qquad \frac{a_1}{b_1}\frac{a_2}{b_2} = \frac{a_1 a_2}{b_1 b_2};$$

   queste operazioni sono compatibili con la relazione d'equivalenza data fra frazioni, e dunque inducono operazioni di addizione e moltiplicazione sui numeri razionali.

   L'abuso di notazione di identificare numeri razionali e frazioni e' compatibile con le operazioni.

L'operazione di addizione di numeri razionali puo' esere definita anche come segue:

si definisce un'operazione parziale di addizione di frazioni ponendo

$$\frac{a_1}{b} + \frac{a_2}{b} = \frac{a_1 + a_2}{b};$$

questa operazione parziale e' compatibile con la relazione d'equivalenza data fra frazioni, e induce un'operazione di addizione sui numeri razionali.

Esplicitamente, per ogni due numeri razionali $\frac{a_1}{b_1}$ e $\frac{a_2}{b_2}$, se $b = b_1c_1 = b_2c_2$ e' un multiplo comune di b_1 e b_2 allora

$$\frac{a_1}{b_1} + \frac{a_2}{b_2} = \frac{a_1c_1}{b_1c_1} + \frac{a_2c_2}{b_2c_2} = \frac{a_1c_1 + a_2c_2}{b}.$$

Normalmente si prende $b = \mathrm{mcm}(b_1, b_2)$.

Per quanto riguarda la moltiplicazione

$$\frac{a_1}{b_1}\frac{a_2}{b_2} = \frac{a_1a_2}{b_1b_2},$$

si nota che l'operazione di semplificazione sulla frazione prodotto si puo' anticipare, semplificando un numeratore di una frazione fattore con un denominatore, della stessa frazione fattore o dell'altra.

4. **Struttura di campo**. Essendo $\mathbb{Q}$ un campo, in esso:

   (1) ciascuna equazione $x + b = c$ $(b, c \in \mathbb{Q})$ nell'incognita x ha una ed una sola soluzione, data da $x = c + (-b)$ che si abbrevia in $c - b$ e si dice "sottrazione" di c meno b;

   (2) ciascuna equazione $ax = c$ $(a, c \in \mathbb{Q};\ a \neq 0)$ nell'incognita x ha una ed una sola soluzione, data da $x = a^{-1}c$ che si scrive spesso $\frac{c}{a}$ (una frazione di frazioni) e si dice "divisione" di c su a;

   (3) ciascuna "equazione di I grado" $ax + b = c$ $(a, b, c \in \mathbb{Q};\ a \neq 0)$ nell'incognita x ha una ed una sola soluzione ...

   Chiaramente, $\mathbb{Q}$ e' un campo di caratteristica 0.

5. **Immersione di $\mathbb{Z}$ in $\mathbb{Q}$**. La funzione $\mathbb{Z} \to \mathbb{Q}$ $a \mapsto \frac{a}{1}$ (abuso di notazione) e' un monomorfismo di anelli, ed e' dunque ammissibile identificare $\mathbb{Z}$ con un sottinsieme (sottoanello) di $\mathbb{Q}$, e scrivere in breve a al posto di $\frac{a}{1}$.

   Per ogni $\frac{a}{b} \in \mathbb{Q}$, (con $b > 0$), applicando la divisione con resto di a su b nella forma $a = qb + r$ con $0 \leq r < b$ (con $q, r \in \mathbb{Z}$) si ha

$$\frac{a}{b} = \frac{qb + r}{b} = q + \frac{r}{b}, \qquad \text{con } 0 \leq \frac{r}{b} < 1;$$

   si dice che q e' la parte intera di $\frac{a}{b}$.

6. **Ordinamento**. Indicati con $\mathbb{Q}^+$ e $\mathbb{Q}^-$ gli insiemi costituiti da 0 e dai numeri razionali rappresentati da frazioni con numeratore e denominatore rispettivamente concordi e discordi, si ha che $\mathbb{Q}^+$ e $\mathbb{Q}^-$ sono l'uno l'insieme degli elementi opposti degli elementi dell'altro e $\mathbb{Q}^+$ e' chiuso rispetto ad addizione e moltiplicazione. Cio' basta per garantire che relazione

$$x \leq y \quad \text{sse} \quad \exists z \in \mathbb{Q}^+ : \quad x + z = y$$

sia una relazione d'ordine totale su $\mathbb{Q}$, compatibile con le operazioni, cioe' tale che

$$x \leq y \quad \text{implichi} \quad x + z \leq y + z \quad \text{e} \quad \begin{cases} xz \leq yz & \text{per } z > 0 \\ xz \geq yz & \text{per } z < 0. \end{cases}$$

In breve, $\mathbb{Q}$ e' un campo ordinato.

Lo stesso ordine su $\mathbb{Q}$ si ottiene definendo

$$x \leq y \quad \text{sse} \quad \text{si puo' scrivere} \quad x = \frac{\xi}{b},\ y = \frac{\eta}{b} \quad \text{con } b > 0,\ \xi \leq \eta$$

$(\xi, \eta, b \in \mathbb{Z})$.

L'ordine su $\mathbb{Q}$ e' denso: per ogni $x, y \in \mathbb{Q}$ con $x < y$ esiste qualche $z \in \mathbb{Q}$ tale che $x < z < y$; cio' si puo' provare usando solo le proprieta' di campo ordinato mostrando che $x < \frac{x+y}{2} < y$, oppure si puo' provare rappresentando x e y con frazioni aventi lo stesso denominatore e differenza fra i numeratori maggiore di 1 ...

$\mathbb{Q}$ e' un campo archimedeo: per ogni $0x, y \in \mathbb{Q}$ con $0 < x < y$ esiste un intero naturale $m \in \mathbb{N}$ tale che $m \cdot x > y$; cio' si puo' provare in vari modi, ad esempio rappresendo x ed y con frazioni aventi lo stesso denominatore positivo, si riconduce questa proprieta' ad una proprieta' degli interi.

L'ordine su $\mathbb{Q}$ non e' completo: ad esempio, $\{x \in \mathbb{Q} : \ x^2 \leq 2\}$ e' superiormente limitato ma non ha estremo superiore; cio' si puo' provare a posteriori dopo avere costruito il campo dei reali; per esercizio se ne dia una dimostrazione diretta.

$\mathbb{Q}$ e gli altri campi

1. Ciascun anello A ha almeno due congruenze (se A non e' banale, distinte): quella in cui tutti gli elementi di A sono congruenti fra loro e quella in cui ciascun elemento di A e' congruente solo a se' stesso, i cui nuclei sono rispettivamente gli ideali di A dati da A stesso e dall'insieme $\{0\}$ ridotto al solo zero di A. Queste si dicono congruenze e ideali "banali," le altre eventuali si dicono congruenze e ideali "propri". I campi sono caratterizzati dal seguente

   Theorem 1. *Un anello commutativo A e' un campo se e solo se non possiede ideali propri.*

Dim.

Se A e' un campo e se I e' un ideale di A non ridotto a $\{0\}$ allora $I = A$. Infatti: esiste un $i \in I$ con $i \neq 0$, per ciascun $a \in A$ esiste un $s \in A$ tale che $is = a$ (essendo A un campo), dunque $a \in I$ (essendo I un ideale).

Se A e' un anello privo di ideali propri e se $a \in A$ con $a \neq 0$ allora a posside inverso in A. Infatti: a genera un ideale $(a) = \{ax;\ x \in A\}$ di A, e si ha $(a) = A$ (essendo A privo di ideali propri), in particolare esiste un $x \in A$ tale che $ax = 1$.

Questo teorema ha una conseguenza diretta sugli omomorfismi tra campi:

Proposition 1. *Ciascun omomorfismo fra campi e' iniettivo.*

Dim. Se $f : K_1 \to K_2$ e' un omomorfismo fra campi, allora f e' iniettivo. Infatti $\mathrm{Ker}(f)$ e' un ideale di K_1 e $1 \notin \mathrm{Ker}(f)$ (essendo $f(1) = 1 \neq 0$), dunque $\mathrm{Ker}(f) = \{0\}$ (essendo A privo di ideali propri), cioe' f e' iniettivo.

Per quel che riguarda il campo $\mathbb{Q}$, si ha

Proposition 2. *Per ogni campo K di caratteristica 0, esiste uno ed un solo monomorfismo $\mathbb{Q} \to K$.*

L'immagine di $\mathbb{Q}$ in K e' il piu' piccolo sottocampo di K, il "sottocampo fondamentale" di K.