AL210 - Appunti integrativi - 5

Prof. Stefania Gabelli - a.a. 2016-2017

Il campo delle frazioni di un dominio

Il procedimento che permette di costruire, a partire da $\mathbb{Z}$, il campo dei numeri razionali può essere generalizzato per costruire, a partire da un qualsiasi dominio A, un "campo minimale" contenente A in cui siano risolubili tutte le equazioni lineari a coefficienti in A.

Dato un dominio A, consideriamo la relazione su $A \times A^*$ definita da:

$$(x, y) \ \rho \ (x', y') \quad \Leftrightarrow \quad xy' = x'y.$$

Si vede subito che ρ è una relazione di equivalenza. L'insieme quoziente di $A \times A^*$ rispetto a ρ si indica con $\mathcal{Q}z(A)$.

Per semplicità di notazione, si usa indicare la classe della coppia (x, y) rispetto a ρ con $\dfrac{x}{y}$, in modo da poter scrivere

$$\mathcal{Q}z(A) := \left\{ \frac{x}{y} \,;\ x, y \in A,\ y \neq 0 \right\}.$$

Le operazioni

$$\frac{x}{y} + \frac{z}{w} = \frac{xw + zy}{yw} \quad \text{e} \quad \frac{x}{y}\frac{z}{w} = \frac{xz}{yw}.$$

sono ben definite (cioè non dipendono dai rappresentanti delle classi scelti) e rispetto a queste operazioni $\mathcal{Q}z(A)$ è un campo. Se 1 è l'unità moltiplicativa di A, lo zero di $\mathcal{Q}z(A)$ è l'elemento $\dfrac{0}{1}$ e l'unità moltiplicativa di $\mathcal{Q}z(A)$ è $\dfrac{1}{1}$. Inoltre, se $x \neq 0$, l'inverso di $\dfrac{x}{y}$ è $\dfrac{y}{x}$.

Il campo $\mathcal{Q}z(A)$ si chiama il *campo delle frazioni di A*. Le seguenti proprietà si verificano facilmente e ci dicono in particolare che, a meno di isomorfismi, $\mathcal{Q}z(A)$ è il più piccolo campo contenente A.

Teorema 1 *Sia A un dominio con unità moltiplicativa* 1.

(a) *L'applicazione*

$$\iota : A \longrightarrow \mathcal{Q}z(A)\,; \quad x \mapsto \frac{x}{1}$$

è un omomorfismo iniettivo di anelli.

(b) *A è un campo se e soltanto se A è isomorfo a $\mathcal{Q}z(A)$.*

(c) *Se K è un campo e $\varphi : A \longrightarrow K$ è un omomorfismo iniettivo, l'applicazione*

$$\psi : \mathcal{Q}z(A) \longrightarrow K\,; \quad \frac{x}{y} \mapsto \varphi(x)\varphi(y)^{-1}$$

è ben definita ed è un omomorfismo (iniettivo) di campi. Inoltre ψ è l'unico omomorfismo di campi tale che $\varphi = \psi \circ \iota$.

(d) *Se A' è un dominio e $\eta : A \longrightarrow A'$ è un omomorfismo iniettivo di anelli, l'applicazione*

$$\mathcal{Q}z(A) \longrightarrow \mathcal{Q}z(A')\,; \quad \frac{x}{y} \mapsto \frac{\eta(x)}{\eta(y)}$$

è ben definita ed è un omomorfismo (iniettivo) di campi. In particolare, domini isomorfi hanno campi delle frazioni isomorfi.

Se A è contenuto in un campo K, per il Teorema 1 (c), l'applicazione

$$\psi : \mathcal{Q}z(A) \longrightarrow K\,; \quad \frac{x}{y} \mapsto xy^{-1}$$

è un omomorfismo non nullo di campi e la sua immagine

$$F := \left\{xy^{-1}\,;\, x, y \in A\,,\, y \neq 0\right\} \subseteq K$$

è il più piccolo sottocampo di K contenente A. Diremo che il campo F è il *campo delle frazioni di A in K*.

Esempio 2 **(1)** Il campo delle frazioni di $\mathbb{Z}$ in $\mathbb{C}$ è il campo $\mathbb{Q}$ dei numeri razionali. Poiché ogni campo numerico contiene $\mathbb{Z}$ (perché contiene 1 ed è un gruppo additivo), allora esso contiene $\mathbb{Q}$. Ne segue che $\mathbb{Q}$ è il più piccolo campo numerico.

(2) Se K è un campo e $\mathbf{X} := \{X_1, \ldots, X_n\}$ è un insieme di indeterminate indipendenti su K, il campo delle frazioni del dominio $K[\mathbf{X}]$ è il campo

$$K(\mathbf{X}) := \left\{ \frac{f(\mathbf{X})}{g(\mathbf{X})}\,;\, f(\mathbf{X}), g(\mathbf{X}) \in K[\mathbf{X}]\,,\, g(\mathbf{X}) \neq 0 \right\}.$$

Questo campo si chiama il *campo delle funzioni razionali nelle indeterminate* $\mathbf{X}$ su K.

(3) Se A è un dominio con campo delle frazioni K e $\mathbf{X} := \{X_1, \ldots, X_n\}$ è un insieme di indeterminate indipendenti su A, il campo delle frazioni di $A[\mathbf{X}]$ è il campo $K(\mathbf{X})$.

Infatti, a meno di isomorfismi, $\mathcal{Q}z(A[\mathbf{X}]) \subseteq \mathcal{Q}z(K[\mathbf{X}]) = K(\mathbf{X})$. D'altra parte, $K := \mathcal{Q}z(A) \subseteq \mathcal{Q}z(A[\mathbf{X}])$ e quindi $K(\mathbf{X}) \subseteq \mathcal{Q}z(A[\mathbf{X}])$.

Ad esempio, il campo delle frazioni sia di $\mathbb{Z}[\mathbf{X}]$ che di $\mathbb{Q}[\mathbf{X}]$ è il campo $\mathbb{Q}(\mathbf{X})$ delle funzioni razionali su $\mathbb{Q}$.

(4) Il campo delle frazioni in $\mathbb{C}$ dell'anello degli interi di Gauss $\mathbb{Z}[\imath]$ è

$$\begin{aligned}\mathcal{Q}z(\mathbb{Z}[\imath]) &= \left\{(a+b\imath)(c+d\imath)^{-1}\,;\, a,b,c,d\in\mathbb{Z}\,, c+d\imath\neq 0\right\}\\ &= \{x+y\imath\,;\, x,y\in\mathbb{Q}\} =: \mathbb{Q}(\imath).\end{aligned}$$

(5) Se A è un dominio e $x, y \in A$, $y \neq 0$, per definizione risulta $\dfrac{x}{y} = \dfrac{ax}{ay}$ per ogni $a \in A^*$. Quindi un numero finito di elementi $\dfrac{x_1}{y_1}, \ldots, \dfrac{x_n}{y_n} \in \mathcal{Q}z(A)$ possono sempre essere *ridotti a comune denominatore*. Infatti, se $d := y_1 y_2 \cdots y_n$ e $d_i := d y_i^{-1}$, si ha $\dfrac{x_i}{y_i} = \dfrac{d_i x_i}{d_i y_i} = \dfrac{x_i'}{d}$, con $x_i' \in A$, per $i = 1, \ldots, n$.

(6) Se A è un dominio con il massimo comune divisore, in particolare un dominio a fattorizzazione unica, ogni frazione non nulla $\dfrac{x}{y} \in \mathcal{Q}z(A)$ può essere *ridotta ai minimi termini*, cioè si può supporre che $(x, y) = 1$. Infatti, se $(x, y) = d$, scrivendo $x = dx'$ e $y = dy'$, si ha $\dfrac{x}{y} = \dfrac{dx'}{dy'} = \dfrac{x'}{y'}$ con $(x', y') = 1$. È evidente che ogni frazione non nulla ha una unica rappresentazione $\dfrac{x}{y}$ con $(x, y) = 1$.

Se $A \subseteq B$, $A' \subseteq B'$ sono anelli e $\varphi : A \longrightarrow A'$ è un omomorfismo, si dice che un omomorfismo $\psi : B \longrightarrow B'$ *estende* φ (o che φ *si può estendere a* ψ) se $\psi(x) = \varphi(x)$ per ogni $x \in A$, ovvero se la restrizione di ψ ad A coincide con φ.

Il punto (d) del Teorema 1 asserisce che se A e A' sono domini, ogni omomorfismo iniettivo $\varphi : A \longrightarrow A'$ si può estendere ad un omomorfismo (necessariamente iniettivo) tra i rispettivi campi delle frazioni.

La caratteristica di un anello

Sia A un anello. Se $a \in A$ e $m \geq 1$, definiamo per ricorsione

$$0a := 0\,; \quad ma := (m-1)a + a\,; \quad (-m)a := -(ma).$$

Se esiste un intero positivo m tale che $ma = 0$, per ogni $a \in A$, il minimo intero positivo n con questa proprietà si chiama la *caratteristica* di A e si dice che A ha *caratteristica finita*, o *positiva* (uguale a n). Altrimenti si dice che A ha *caratteristica zero*. È evidente che l'unico anello che ha caratteristica 1 è l'anello nullo.

Notiamo che, se A ha caratteristica finita uguale a n, l'ordine additivo di ogni elemento non nullo di A è finito e divide n.

Proposizione 3 *Sia A un anello unitario, con unità moltiplicativa 1. Allora A ha caratteristica finita uguale a $n \geq 2$ se e soltanto se 1 ha ordine additivo finito uguale a n.*

Dimostrazione: Sia n l'ordine additivo di 1. Poiché $ma = m(1a) = (m1)a$, per ogni $m \geq 0$ e $a \in A$, allora $na = 0$, per ogni $a \in A$. D'altra parte n divide la caratteristica di A, quindi è uguale ad essa. Il viceversa è ovvio. □

Se A è un anello unitario con unità moltiplicativa 1, l'intersezione di tutti i sottoanelli di A contenenti 1 è un anello, che si chiama il *sottoanello fondamentale* di A. Esso è chiaramente il più piccolo sottoanello di A contenente 1. Analogamente, l'intersezione di tutti i sottocampi di un campo K è un campo, che si chiama il *sottocampo fondamentale* o il *sottocampo minimo* di K.

Proposizione 4 *Se A è un anello unitario con unità moltiplicativa 1, il suo sottoanello fondamentale è l'anello $\{z1\,;\, z \in \mathbb{Z}\}$. Esso è isomorfo a $\mathbb{Z}$ se (e soltanto se) A ha caratteristica zero ed è isomorfo all'anello $\mathbb{Z}_n$ delle classi resto modulo n se (e soltanto se) A ha caratteristica finita uguale a $n \geq 2$.*

Dimostrazione: Consideriamo l'applicazione

$$f : \mathbb{Z} \longrightarrow A\,; \quad z \mapsto z1.$$

Si verifica subito che f è un omomorfismo di anelli non nullo; perciò la sua immagine $\operatorname{Im} f = \{z1\,;\, z \in \mathbb{Z}\}$ è un sottoanello di A. Inoltre, ogni sottoanello di A che contiene 1 contiene anche $\operatorname{Im} f$, perché è un gruppo additivo. Quindi $\operatorname{Im} f = \{z1\,;\, z \in \mathbb{Z}\}$ è il sottoanello fondamentale di A.

Il nucleo di f è l'ideale $\operatorname{Ker} f = \{z \in \mathbb{Z}\,;\, z1 = 0\} \subseteq \mathbb{Z}$. Allora, per definizione, A ha caratteristica zero se e soltanto se $\operatorname{Ker} f = (0)$. Altrimenti $\operatorname{Ker} f = n\mathbb{Z}$, dove $n \neq 2$ è il minimo intero positivo in $\operatorname{Ker} f$. Quindi $\operatorname{Ker} f = n\mathbb{Z}$ se e soltanto se A ha caratteristica finita uguale a n.

Per il Teorema Fondamentale di Omomorfismo, se A ha caratteristica zero, allora $\operatorname{Im} f$ è isomorfo a $\mathbb{Z}$. Altrimenti, $\operatorname{Im} f$ è isomorfo a $\mathbb{Z}_n := \mathbb{Z}/n\mathbb{Z}$, dove $n \geq 2$ è la caratteristica di A. □

Corollario 5 *Se A è unitario e non ha zero-divisori, il suo sottoanello fondamentale è isomorfo a $\mathbb{Z}$ oppure al campo $\mathbb{F}_p$, per qualche primo $p \geq 2$.*

Dimostrazione: Per la Proposizione 4, il sottoanello fondamentale di A è isomorfo a $\mathbb{Z}$ oppure a $\mathbb{Z}_n$. Nel secondo caso, poiché A non ha zero-divisori, $\mathbb{Z}_n$ deve essere integro; perciò $n = p$ deve essere un numero primo. □

Corollario 6 (E. Steinitz, 1910) *Se K è un campo, il suo sottocampo fondamentale è isomorfo a $\mathbb{Q}$ oppure a $\mathbb{F}_p$, per qualche primo $p \geq 2$.*

Dimostrazione: Per il Corollario 5, il sottoanello fondamentale di K è isomorfo a $\mathbb{Z}$ oppure a $\mathbb{F}_p$. Nel primo caso, per la Proposizione 1 (c), il sottocampo fondamentale di K è isomorfo al campo delle frazioni di $\mathbb{Z}$ in $\mathbb{C}$, cioè a $\mathbb{Q}$. □

Il risultato precedente ci assicura che un campo di caratteristica finita ha *caratteristica prima*.

Corollario 7 *Ogni sottocampo di un campo K ha la stessa caratteristica di K.*

Esempio 8 (1) Ogni campo numerico ha caratteristica zero. Un campo di caratteristica zero, contenendo isomorficamente $\mathbb{Q}$ è infinito; quindi ogni campo finito ha caratteristica finita.

(2) Per ogni anello commutativo unitario A, A e $A[\mathbf{X}]$ hanno la stessa caratteristica. Quindi il campo delle funzioni razionali $\mathbb{F}_p(\mathbf{X})$ è un campo infinito di caratteristica finita uguale a p.