

0.1 Localizzazione

Introduciamo un metodo per aumentare la struttura di un dominio di integrità.

Definizione

Sia R un dominio di integrità. Diciamo che $S \subseteq R$ è un sistema moltiplicativo se:

- (i) $1_R \in S$ e $0_R \notin S$;
- (ii) per ogni $a, b \in S$ anche $ab \in S$.

Osserviamo che S è un monoide commutativo rispetto all'operazione binaria di prodotto. Infatti, esso eredita l'associatività e la commutatività da R , la (ii) garantisce che S è chiuso rispetto al prodotto e per la (i) sappiamo che S contiene l'elemento neutro 1_R . Tuttavia, S non è sempre un gruppo, in quanto non richiediamo l'esistenza degli inversi moltiplicativi.

Esempio. L'insieme $S = \{2^n : n \in \mathbb{N}\} \subseteq \mathbb{Q}$ è un sistema moltiplicativo. Infatti, $2^0 = 1 \in S$, $0 \notin S$ per le proprietà dell'esponenziale, e presi $2^a, 2^b \in S$ anche $2^a \cdot 2^b = 2^{a+b} \in S$. Tuttavia, tale S non è un sottogruppo di \mathbb{Q} poiché ad esempio $2^{-1} = \frac{1}{2} \notin S$. \square

Sull'insieme delle coppie $(r, s) \in R \times S$ definiamo la relazione $(r, s) \sim (t, u) \Leftrightarrow ru = st$.

Proposizione 1.7.1

La relazione $\sim: (R \times S) \times (R \times S) \rightarrow \{\text{v}, \text{f}\}$ è una relazione di equivalenza.¹

Dimostrazione. Chiaramente $(r, s) \sim (r, s)$ perché $rs = sr$, dunque \sim è riflessiva. Inoltre, se $(r, s) \sim (t, u)$, allora $ru = st$, cioè $ts = ur$, da cui $(t, u) \sim (r, s)$ e \sim è simmetrica. Siano $(r, s) \sim (t, u)$ e $(t, u) \sim (v, w)$. Allora, $ru = st$ e $tw = uv$, cioè, moltiplicando per w entrambi i membri della prima uguaglianza, $ruw = s(tw) = s(uv) \Rightarrow ruw - suv = (rw - sv)u = 0_R$. Poiché R è un dominio di integrità e $u \neq 0_R$ essendo $u \in S$, si ha che $rw - sv = 0_R$, cioè $rw = sv$, da cui $(r, s) \sim (v, w)$ e dunque \sim è transitiva. \blacksquare

Denotiamo con $\frac{r}{s} = [(r, s)]_\sim$ la classe di equivalenza dell'elemento (r, s) rispetto a \sim , e sia $S^{-1}R = \{\frac{r}{s} : r \in R, s \in S\} = (R \times S)/\sim$ il quoziente di $R \times S$ rispetto a \sim .

Definizione

Sia R un dominio di integrità e sia S un sistema moltiplicativo di R . Allora, l'insieme $S^{-1}R = \{\frac{r}{s} : r \in R, s \in S\}$ è detto localizzazione di R a S .

Il termine “localizzazione” deve il suo nome alla geometria algebrica.² Dal punto di vista dell'algebra astratta, l'idea della localizzazione è quella di aggiungere ad un anello gli inversi moltiplicativi di alcuni suoi elementi introducendo delle “frazioni”, in modo simile a quanto si fa nel passare dai numeri interi ai numeri razionali.

¹La relazione \sim restituisce vero (v) o falso (f) a seconda che le due coppie siano o meno in relazione. Ricordiamo che una relazione di equivalenza è R-S-T, cioè riflessiva, simmetrica e transitiva.

²Se R è un anello di funzioni definito su un oggetto geometrico (come una varietà algebrica, cioè l'insieme delle soluzioni di un sistema di equazioni polinomiali) e vogliamo studiare tale varietà in un certo punto x_0 , definiamo S come l'insieme delle funzioni che non si annullano in x_0 e localizziamo R a S . Allora, $S^{-1}R$ è un anello generalmente più semplice di R che contiene informazioni solo sul comportamento della varietà in un intorno di x_0 , da cui l'origine del termine “locale”.

Vogliamo ora dotare tale insieme $S^{-1}R$ delle operazioni binarie di somma e prodotto affinché sia un anello. Siano $\oplus: S^{-1}R \times S^{-1}R \rightarrow S^{-1}R$ e $\odot: S^{-1}R \times S^{-1}R \rightarrow S^{-1}R$ definite come

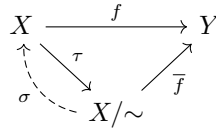
$$\frac{r}{s} \oplus \frac{t}{u} = \frac{ru + st}{su} \quad \text{e} \quad \frac{r}{s} \odot \frac{t}{u} = \frac{rt}{su}.$$

Poiché $S^{-1}R$ è un insieme quoziente, per dimostrare che tali operazioni sono ben poste è necessario mostrare che il loro risultato non dipende dai rappresentanti delle classi di equivalenza. Per fare ciò, dimostriamo prima il seguente lemma.

Lemma 1.7.2: Lemma della forbice

Siano X e Y insiemi non vuoti e sia $f: X \rightarrow Y$ una mappa. Sia \sim una relazione di equivalenza su X e $\tau: X \rightarrow X/\sim$ la proiezione canonica.³ Allora, esiste una mappa $\bar{f}: X/\sim \rightarrow Y$ tale che $f = \bar{f} \circ \tau$ se e solo se $f(x) = f(y)$ per ogni $x, y \in X$ con $x \sim y$.

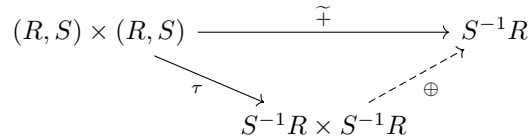
Dimostrazione. Supponiamo che $f(x) = f(y)$ per ogni $x, y \in X$ con $x \sim y$. Per l'assioma della scelta,⁴ esiste $\sigma: X/\sim \rightarrow X$ tale che $\sigma([x]) \sim x$ per ogni $x \in X$ e $\tau \circ \sigma = \text{id}_{X/\sim}$. Si consideri ora la funzione $\bar{f} = f \circ \sigma: X/\sim \rightarrow Y$.



Osserviamo innanzitutto che \bar{f} è ben definita, poiché se $[x] = [y]$, allora $\bar{f}([x]) = \bar{f}([y])$ perché $\sigma([x]) \sim x \sim y \sim \sigma([y])$ e $f(\sigma([x])) = f(\sigma([y]))$ essendo per ipotesi f costante sulle classi di equivalenza. Inoltre, $(\bar{f} \circ \tau)(x) = f(\sigma(\tau(x))) = f(\sigma([x])) = f(x)$ per ogni $x \in X$ poiché $\sigma([x]) \sim x$, dunque è effettivamente vero che $f = \bar{f} \circ \tau$.

Viceversa, sia $\bar{f}: X/\sim \rightarrow Y$ tale che $f = \bar{f} \circ \tau$. Allora, per ogni $x, y \in X$ con $x \sim y$, cioè $[x] = [y]$, si ha che $f(x) = \bar{f}(\tau(x)) = \bar{f}([x]) = \bar{f}([y]) = \bar{f}(\tau(y)) = f(y)$ come desiderato. ■

Sia $\widetilde{+}: (R, S) \times (R, S) \rightarrow S^{-1}R$ l'operazione binaria definita come $(r, s) \widetilde{+} (t, u) = \frac{ru + st}{su}$.



Per verificare che l'operazione \oplus esiste ed è ben posta, per il *Lemma della forbice* è sufficiente mostrare che se $(r, s) \sim (r', s')$ e $(t, u) \sim (t', u')$, allora $(r, s) \widetilde{+} (t, u) = (r', s') \widetilde{+} (t', u')$, cioè $\frac{ru + st}{su} = \frac{r'u' + s't'}{s'u'}$. Poiché per definizione di \sim si ha che $rs' = sr'$ e $tu' = ut'$, osserviamo che $(ru + st)s'u' = (rs')uu' + (tu')ss' = (sr')uu' + (ut')ss' = (r'u' + s't')su$. Dunque, vale $(ru + st, su) \sim (r'u' + s't', s'u')$, da cui $\frac{ru + st}{su} = \frac{r'u' + s't'}{s'u'}$.

³Cioè la mappa che manda ogni elemento $x \in X$ nella sua classe di equivalenza $[x]_{\sim}$, che per comodità di notazione denoteremo di qui in seguito semplicemente con $[x]$.

⁴L'assioma della scelta afferma che data una famiglia non vuota di insiemi non vuoti, esiste una funzione che ad ogni insieme della famiglia fa corrispondere un suo elemento. Per poter dimostrare questo lemma è necessario assumere tale assioma, di cui si fa uso nel definire la funzione σ , che altrimenti a priori non esisterebbe. Infatti, X/\sim è la famiglia delle classi di equivalenza di X , ognuna delle quali è non vuota poiché $x \in [x]$, e σ è la funzione che ad ogni classe $[x] \in X/\sim$ fa corrispondere un suo rappresentante $\sigma([x]) \in X$.

Analogamente, sia $\sim: (R, S) \times (R, S) \rightarrow S^{-1}R$ l'operazione definita come $(r, s) \sim (t, u) = \frac{rt}{su}$.

$$\begin{array}{ccc} (R, S) \times (R, S) & \xrightarrow{\sim} & S^{-1}R \\ & \searrow \tau & \nearrow \odot \\ & S^{-1}R \times S^{-1}R & \end{array}$$

Se $(r, s) \sim (r', s')$ e $(t, u) \sim (t', u')$, osserviamo che $rts'u' = (rs')(tu') = (s'r')(ut') = sur't'$, dunque $(rt, su) \sim (r't', s'u')$. Allora, $(r, s) \sim (t, u) = \frac{rt}{su} = \frac{r't'}{s'u'} = (r', s') \sim (t', u')$, da cui per il *Lemma della forbice* l'operazione \odot esiste ed è ben posta.

Per comodità di notazione, denoteremo di qui in seguito le due operazioni \oplus e \odot di $S^{-1}R$ semplicemente con $+$ e \cdot , rispettivamente.⁵

Proposizione 1.7.3

Sia R un dominio di integrità e sia S un sistema moltiplicativo di R . Allora, $S^{-1}R$ dotato di tali operazioni di somma e prodotto è un dominio di integrità.

Dimostrazione. Siano $\frac{r}{s}, \frac{t}{u}$ e $\frac{v}{w}$ elementi di $S^{-1}R$. Osserviamo innanzitutto che

$$\left(\frac{r}{s} + \frac{t}{u}\right) + \frac{v}{w} = \frac{ru + st}{su} + \frac{v}{w} = \frac{ruw + stw + suv}{suw} = \frac{r}{s} + \frac{tw + uv}{uw} = \frac{r}{s} + \left(\frac{t}{u} + \frac{v}{w}\right)$$

da cui la somma è associativa. Inoltre, $\frac{r}{s} + \frac{t}{u} = \frac{ru + st}{su} = \frac{ts + ur}{us} = \frac{t}{u} + \frac{r}{s}$, dunque $(S^{-1}R, +)$ è un gruppo abeliano con elemento neutro $0_{S^{-1}R} = \frac{0_R}{1_R}$ e opposto $-\frac{r}{s} = \frac{-r}{s}$. Essendo

$$\left(\frac{r}{s} \cdot \frac{t}{u}\right) \cdot \frac{v}{w} = \frac{rt}{su} \cdot \frac{v}{w} = \frac{rtv}{suw} = \frac{r}{s} \cdot \frac{tv}{uw} = \frac{r}{s} \cdot \left(\frac{t}{u} \cdot \frac{v}{w}\right)$$

e $\frac{r}{s} \cdot \frac{t}{u} = \frac{rt}{su} = \frac{tr}{us} = \frac{t}{u} \cdot \frac{r}{s}$, il prodotto è associativo e commutativo. Infine,

$$\left(\frac{r}{s} + \frac{t}{u}\right) \cdot \frac{v}{w} = \frac{ru + st}{su} \cdot \frac{v}{w} = \frac{ruv + stv}{suw} = \frac{rv}{sw} + \frac{tv}{uw} = \frac{r}{s} \cdot \frac{v}{w} + \frac{t}{u} \cdot \frac{v}{w}$$

perché $\frac{rv}{sw} + \frac{tv}{uw} = \frac{ruv + stv}{suw} = \frac{ruv + stv}{suw}$ essendo $(ruv + stv)suw = (ruv + stv)suw$. Dunque, vale la proprietà distributiva e $(S^{-1}R, +, \cdot)$ è un anello commutativo con unità $1_{S^{-1}R} = \frac{1_R}{1_R}$. Resta da mostrare che $S^{-1}R$ non ha divisori dello zero. Siano $\frac{r}{s}, \frac{t}{u} \in S^{-1}R$ tali che $\frac{r}{s} \cdot \frac{t}{u} = 0_{S^{-1}R} = \frac{0_R}{1_R}$. Allora $\frac{rt}{su} = \frac{0_R}{1_R}$, cioè $rt = (rt)1_R = (su)0_R = 0_R$, da cui, essendo R un dominio di integrità, $r = 0$ oppure $t = 0$, quindi $\frac{r}{s} = \frac{0_R}{s} = \frac{0_R}{1_R} = 0_{S^{-1}R}$ oppure $\frac{t}{u} = \frac{0_R}{u} = \frac{0_R}{1_R} = 0_{S^{-1}R}$. Dunque, $S^{-1}R$ è effettivamente un dominio di integrità. ■

Sia $\iota_R: R \hookrightarrow S^{-1}R$ definita come $\iota_R(r) = \frac{r}{1_R}$ l'inclusione da R a $S^{-1}R$. Osserviamo che ι_R è un omomorfismo di anelli iniettivo. Infatti, presi $x, y \in R$, si ha che

$$\iota_R(x + y) = \frac{x + y}{1_R} = \frac{x}{1_R} + \frac{y}{1_R} = \iota_R(x) + \iota_R(y)$$

$$\iota_R(xy) = \frac{xy}{1_R} = \frac{x}{1_R} \cdot \frac{y}{1_R} = \iota_R(x) \cdot \iota_R(y)$$

e $\iota_R(0_R) = \frac{0_R}{1_R} = 0_{S^{-1}R}$, $\iota_R(1_R) = \frac{1_R}{1_R} = 1_{S^{-1}R}$. Inoltre, $\iota_R(r) = \iota_R(r')$ se e solo se $\frac{r}{1_R} = \frac{r'}{1_R}$, cioè $r = r'$. Dunque, ι_R è effettivamente un omomorfismo di anelli iniettivo.

⁵Per quanto appena provato, possiamo effettivamente vedere tali operazioni come somma e prodotto di “frazioni” con le usuali regole di calcolo delle frazioni.

Vediamo ora alcuni esempi di sistemi moltiplicativi con le relative localizzazioni.

Esempio. Sia R un dominio di integrità e sia $S = \{1_R\}$. Allora, S è il più piccolo sistema moltiplicativo di R e $S^{-1}R \simeq R$. Infatti, in questo caso l'inclusione $\iota_R: R \hookrightarrow S^{-1}R$ è anche suriettiva, perché preso $\frac{r}{1_R} \in S^{-1}R$ si ha che $\iota_R(r) = \frac{r}{1_R}$, ed è quindi un isomorfismo. \square

Esempio. Sia R un dominio di integrità e sia $S = R^\times$. Poiché R^\times è un gruppo rispetto al prodotto e $0_R \notin R^\times$, tale S è un sistema moltiplicativo di R e $S^{-1}R \simeq R$ perché anche in questo caso l'inclusione $\iota_R: R \hookrightarrow S^{-1}R$ risulta essere suriettiva. Infatti, preso $\frac{r}{s} \in S^{-1}R$, poiché $s \in R^\times$, per definizione esiste $t \in R$ tale che $st = 1_R$. Dunque, $\iota_R(rt) = \frac{rt}{1_R} = \frac{r}{s}$ essendo $(rt)s = r(1_R)$, da cui ι_R è un isomorfismo e $S^{-1}R \simeq R$. \square

Esempio. Sia R un dominio di integrità e sia $\mathfrak{p} \triangleleft R$ un ideale primo.⁶ Detto $S = R \setminus \mathfrak{p}$, osserviamo che $0_R \in \mathfrak{p}$, cioè $0_R \notin S$, e se fosse $1_R \in \mathfrak{p}$, allora $\mathfrak{p} = \langle 1_R \rangle = R$ non sarebbe proprio,⁷ da cui $1_R \in R \setminus \mathfrak{p} = S$. Inoltre, presi $a, b \in S$, se fosse $ab \in \mathfrak{p}$, essendo \mathfrak{p} primo si avrebbe che $a \in \mathfrak{p}$ o $b \in \mathfrak{p}$, assurdo. Dunque, $ab \in S$ e S è un sistema moltiplicativo di R . Mostriamo ora che $S^{-1}R = (S^{-1}R)^\times \sqcup S^{-1}\mathfrak{p}$. Osserviamo che $S^{-1}R = S^{-1}(R \setminus \mathfrak{p}) \sqcup S^{-1}\mathfrak{p}$, dove tale unione è disgiunta poiché $S^{-1}(R \setminus \mathfrak{p}) \cap S^{-1}\mathfrak{p} = \emptyset$.⁸ Sia ora $\frac{r}{s} \in S^{-1}(R \setminus \mathfrak{p})$; allora, anche $\frac{s}{r} \in S^{-1}(R \setminus \mathfrak{p})$ e $\frac{r}{s} \cdot \frac{s}{r} = \frac{1_R}{1_R} = 1_{S^{-1}R}$, cioè $\frac{r}{s}$ è invertibile, da cui $S^{-1}(R \setminus \mathfrak{p}) \subseteq (S^{-1}R)^\times$. D'altra parte, se esistesse $\frac{r}{s} \in S^{-1}\mathfrak{p}$ invertibile, detto $\frac{t}{u} \in S^{-1}R$ il suo inverso si avrebbe $rt = su \in \mathfrak{p}$, il che è assurdo poiché $s, u \in S = R \setminus \mathfrak{p}$ violando la definizione di ideale primo. Dunque $(S^{-1}R)^\times \subseteq S^{-1}(R \setminus \mathfrak{p})$, da cui $S^{-1}R = S^{-1}(R \setminus \mathfrak{p}) \sqcup S^{-1}\mathfrak{p} = (S^{-1}R)^\times \sqcup S^{-1}\mathfrak{p}$. \square

Se R è un dominio di integrità, $\{0_R\} \triangleleft R$ è un ideale primo perché R non ha divisori dello zero, cioè $ab = 0_R$ se e solo se $a = 0_R$ oppure $b = 0_R$. Dunque, per quanto visto nell'ultimo esempio, $S = R \setminus \{0_R\}$ è un sistema moltiplicativo di R e $S^{-1}R = (S^{-1}R)^\times \sqcup \left\{\frac{0_R}{1_R}\right\}$ è un dominio di integrità in cui ogni elemento non nullo è invertibile, cioè un campo.

Definizione

Sia R un dominio di integrità e sia $S = R \setminus \{0_R\}$. Allora, $S^{-1}R$ è un campo detto campo dei quozienti di R e si denota con $\text{quot}(R)$.

Esempio. Se consideriamo \mathbb{Z} , si ha che $\text{quot}(\mathbb{Z}) = \left\{\frac{m}{n} : m \in \mathbb{Z}, n \in \mathbb{Z} \setminus \{0\}\right\} = \mathbb{Q}$. \square

I numeri razionali sono denotati con il simbolo \mathbb{Q} proprio perché essi sono il “quoziente” dei numeri interi. Inoltre, \mathbb{Z} è un sottoanello del campo $\mathbb{Q} = \text{quot}(\mathbb{Z})$. Quest'ultimo è un fatto generale, come dimostrato dalla proposizione seguente.

Proposizione 1.7.4

Ogni dominio di integrità è isomorfo a un sottoanello del suo campo dei quozienti.

Dimostrazione. Sia R un dominio di integrità e sia $\iota_R: R \hookrightarrow \text{quot}(R)$ l'inclusione. Poiché ι_R è un omomorfismo iniettivo, $\ker(\iota_R) = \{0_R\}$ e $\text{Im}(\iota_R)$ è un sottoanello del campo $\text{quot}(R)$. Dunque, per il *Primo teorema d'isomorfismo* si ha che $R = R/\ker(\iota_R) \simeq \text{Im}(\iota_R)$. \blacksquare

⁶Un ideale proprio $\mathfrak{p} \triangleleft R$ si dice primo se, presi $a, b \in R$, si ha che $ab \in \mathfrak{p}$ se e solo se $a \in \mathfrak{p}$ o $b \in \mathfrak{p}$.

⁷In generale, se un ideale $I \triangleleft R$ contiene l'unità 1_R , allora $r = r1_R \in I$ per ogni $r \in R$, cioè $I = R$.

⁸Sia $\frac{r}{s} \in S^{-1}\mathfrak{p}$; se fosse $\frac{t}{u} \in S^{-1}(R \setminus \mathfrak{p})$, essendo $r \in \mathfrak{p}$, si avrebbe che $ru = st \in \mathfrak{p}$. Dunque, essendo \mathfrak{p} primo, dovrebbe essere $s \in \mathfrak{p}$ o $t \in \mathfrak{p}$, il che è assurdo essendo $s, t \in S = R \setminus \mathfrak{p}$.

In particolare, osserviamo che $\mathbb{Q} = \text{quot}(\mathbb{Z})$ non solo contiene \mathbb{Z} come sottoanello, ma è proprio il più piccolo campo contenente \mathbb{Z} . Infatti, se \mathbb{K} è un campo contenente \mathbb{Z} , allora $n^{-1} = \frac{1}{n} \in \mathbb{K}$ per ogni $n \in \mathbb{Z} \setminus \{0\}$ e $m \cdot \frac{1}{n} \in \mathbb{K}$ per ogni $m \in \mathbb{Z}$, da cui $\mathbb{Q} \subseteq \mathbb{K}$. Anche questo è un fatto generale che caratterizza il campo dei quozienti di ogni dominio di integrità.

Proposizione 1.7.5

Sia R un dominio di integrità. Allora, il campo dei quozienti $\text{quot}(R)$ è il più piccolo campo contenente un sottoanello isomorfo a R .

Dimostrazione. Osserviamo innanzitutto che per la *Proposizione 1.7.4* sappiamo che R è isomorfo al sottoanello $\text{Im}(\iota_R)$ del campo $\text{quot}(R)$. Sia quindi \mathbb{K} un campo contenente R e sia $\phi: \text{quot}(R) \rightarrow \mathbb{K}$ la mappa definita come $\phi(\frac{r}{s}) = rs^{-1}$. Tale mappa è ben definita: infatti, $r \in \mathbb{K}$ perché $r \in R \subseteq \mathbb{K}$, e in quanto campo \mathbb{K} contiene anche tutti gli inversi s^{-1} degli elementi $s \in R \setminus \{0_R\}$, da cui $rs^{-1} \in \mathbb{K}$. Inoltre, se $\frac{r}{s} = \frac{r'}{s'}$ per definizione vale $rs' = r's$, quindi $\phi(\frac{r}{s}) = rs^{-1} = r's'^{-1} = \phi(\frac{r'}{s'})$. Siano ora $\frac{r}{s}, \frac{t}{u} \in \text{quot}(R)$. Allora, si ha che

$$\begin{aligned}\phi\left(\frac{r}{s} + \frac{t}{u}\right) &= \phi\left(\frac{ru + st}{su}\right) = (ru + st)(su)^{-1} = rs^{-1} + tu^{-1} = \phi\left(\frac{r}{s}\right) + \phi\left(\frac{t}{u}\right) \\ \phi\left(\frac{r}{s} \cdot \frac{t}{u}\right) &= \phi\left(\frac{rt}{su}\right) = rt(su)^{-1} = rs^{-1}tu^{-1} = \phi\left(\frac{r}{s}\right) \cdot \phi\left(\frac{t}{u}\right)\end{aligned}$$

e $\phi(\frac{r}{s}) = rs^{-1} = 0_{\mathbb{K}}$ se e solo se $r = 0_R$, da cui ϕ è un omomorfismo di campi iniettivo. Poiché $\text{Im}(\phi)$ è un sottoanello del campo \mathbb{K} e per il *Primo teorema d'isomorfismo* si ha che $\text{quot}(R) = \text{quot}(R) / \ker(\phi) \simeq \text{Im}(\phi)$, concludiamo che \mathbb{K} contiene un sottoanello isomorfo a $\text{quot}(R)$ ed è quindi un campo più grande del campo dei quozienti $\text{quot}(R)$. ■

Sia R un dominio di integrità e sia S un sistema moltiplicativo di R . Vogliamo ora studiare le eventuali relazioni tra gli ideali di R e quelli di $S^{-1}R$. Presi gli ideali $I \triangleleft R$ e $J \triangleleft S^{-1}R$, definiamo $S^{-1}I = \{\frac{i}{s} : i \in I, s \in S\}$ e denotiamo con $\bar{J} = \iota_R^{-1}(J) = \{r \in R : \frac{r}{1_R} \in J\}$.

Proposizione 1.7.6

Sia S un sistema moltiplicativo di un dominio di integrità R . Presi $I \triangleleft R$ e $J \triangleleft S^{-1}R$,
(a) $S^{-1}I \triangleleft S^{-1}R$ e $S^{-1}I = S^{-1}R$ se e solo se $I \cap S \neq \emptyset$;
(b) $\bar{J} \triangleleft R$ e $S^{-1}\bar{J} = J$.

Dimostrazione. (a) Siano $\frac{i}{s}, \frac{j}{t} \in S^{-1}I$. Allora, $\frac{i}{s} + \frac{j}{t} = \frac{it+js}{st} \in S^{-1}I$ perché $it + js \in I$ per definizione di ideale e $st \in S$ per definizione di sistema moltiplicativo. Analogamente, $\frac{i}{s} \cdot \frac{j}{t} = \frac{ij}{st} \in S^{-1}I$ perché $ij \in I$ e $st \in S$, da cui $S^{-1}I$ è effettivamente un ideale di $S^{-1}R$. Osserviamo ora che se $S^{-1}I = S^{-1}R$, in particolare esiste un elemento $\frac{i}{s} \in S^{-1}I$ tale che $\frac{i}{s} = 1_{S^{-1}R} = \frac{1_R}{1_R}$. Dunque, $i = i(1_R) = s(1_R) = s$, cioè $i = s \in I \cap S$, da cui $I \cap S \neq \emptyset$. Viceversa, supponiamo che $I \cap S \neq \emptyset$. Preso $t \in I \cap S$, si ha che $\frac{t}{t} = \frac{1_R}{1_R} = 1_{S^{-1}R} \in S^{-1}I$, da cui, essendo $S^{-1}I$ un ideale, $\frac{r}{s} \cdot 1_{S^{-1}R} = \frac{r}{s} \in S^{-1}I$ per ogni $\frac{r}{s} \in S^{-1}R$, cioè $S^{-1}I = S^{-1}R$.
(b) Poiché $\iota_R: R \hookrightarrow S^{-1}R$ è un omomorfismo, la preimmagine $\iota_R^{-1}(J) \subseteq R$ di un ideale $J \triangleleft S^{-1}R$ è un ideale di R , cioè $\bar{J} \triangleleft R$. Preso $\frac{j}{s} \in S^{-1}\bar{J}$, per definizione si ha che $\frac{j}{1_R} \in J$. Quindi, essendo J un ideale, $\frac{j}{s} = \frac{1_R}{s} \cdot \frac{j}{1_R} \in J$, da cui $S^{-1}\bar{J} \subseteq J$. D'altra parte, preso $\frac{r}{s} \in J$, per definizione di ideale si ha che $\frac{s}{1_R} \cdot \frac{r}{s} = \frac{r}{1_R} \in J$, cioè $r \in \bar{J}$. Dunque risulta $\frac{r}{s} \in S^{-1}\bar{J}$, da cui $J \subseteq S^{-1}\bar{J}$. Combinando le doppie inclusioni, si ha quindi che $S^{-1}\bar{J} = J$. ■

Vi è quindi un legame tra la noetherianità di R e quella di una sua localizzazione $S^{-1}R$.

Corollario 1.7.7

Sia R un dominio di integrità noetheriano e sia S un sistema moltiplicativo di R . Allora, anche $S^{-1}R$ è un dominio di integrità noetheriano.

Dimostrazione. Per la *Proposizione 1.7.3* sappiamo che $S^{-1}R$ è un dominio di integrità, quindi è sufficiente provare che esso è anche noetheriano. Siano $J \triangleleft S^{-1}R$ e $\bar{J} = \iota_R^{-1}(J) \triangleleft R$. Essendo R noetheriano, esistono $a_1, \dots, a_n \in R$ tali che $\bar{J} = \langle a_1, \dots, a_n \rangle$. Dunque, per la *Proposizione 1.7.6* si ha che $J = S^{-1}\bar{J} = \{ \frac{j}{s} : j \in \bar{J}, s \in S \} = \langle \frac{a_1}{1_R}, \dots, \frac{a_n}{1_R} \rangle$ è finitamente generato, da cui per l'arbitrarietà di J concludiamo che $S^{-1}R$ è noetheriano. ■

Esiste un'importante famiglia di anelli strettamente legata al concetto di localizzazione.

Definizione

Un anello commutativo R si dice locale se $\mathfrak{m} = R \setminus R^\times$ è un ideale di R .

Un anello locale è quindi un anello i cui elementi non invertibili costituiscono un ideale.

Esempio. Ogni campo \mathbb{K} è un anello locale. Infatti, $\mathbb{K}^\times = \mathbb{K} \setminus \{0_{\mathbb{K}}\}$ poiché per definizione di campo ogni elemento non nullo è invertibile, dunque $\mathfrak{m} = \mathbb{K} \setminus \mathbb{K}^\times = \{0_{\mathbb{K}}\} \triangleleft \mathbb{K}$. □

Esempio. Sia R un dominio di integrità e sia $\mathfrak{p} \triangleleft R$ un ideale primo. Detto $S = R \setminus \mathfrak{p}$, $S^{-1}R$ è un anello locale perché abbiamo mostrato che $S^{-1}R \setminus (S^{-1}R)^\times = S^{-1}\mathfrak{p} \triangleleft S^{-1}R$. □

Esempio. Sia \mathbb{K} un campo. Allora, l'anello $\mathbb{K}[[x]]$ delle serie formali è un anello locale poiché per la *Proposizione 1.4.X* si ha che $\mathfrak{m} = \mathbb{K}[[x]] \setminus \mathbb{K}[[x]]^\times = \langle x \rangle \triangleleft \mathbb{K}[[x]]$. □

Osserviamo che non tutti i domini di integrità sono anche anelli locali.

Esempio. Sia \mathbb{K} un campo. Allora, $\mathbb{K}[x]$ non è un anello locale. Infatti, sappiamo che per la *Proposizione 1.1.2* vale $\mathbb{K}[x]^\times = \mathbb{K}^\times$, da cui $\mathfrak{m} = \mathbb{K}[x] \setminus \mathbb{K}[x]^\times = \{f(x) \in \mathbb{K}[x] : \deg^*(f) \geq 1\}$. Tuttavia, \mathfrak{m} non è un ideale di $\mathbb{K}[x]$ poiché $f(x) = x + 1_{\mathbb{K}}$ e $g(x) = x$ sono elementi di \mathfrak{m} ma $h(x) = f(x) - g(x) = 1_{\mathbb{K}} \notin \mathfrak{m}$ perché $\deg^*(h) = 0$. □

D'altra parte, esistono esempi di anelli locali che non sono domini di integrità.

Esempio. Esempio. □

Esiste una caratterizzazione equivalente degli anelli locali in termini di ideali massimali.

Proposizione 1.7.8

Sia R un anello locale. Allora, $\mathfrak{m} = R \setminus R^\times$ è l'unico ideale massimale di R .

Dimostrazione. Osserviamo innanzitutto che $\mathfrak{m} \triangleleft R$ è massimale perché, preso $I \triangleleft R$ tale che $\mathfrak{m} \subsetneq I$, si ha che $I \setminus \mathfrak{m} \neq \emptyset$, cioè $I \cap R^\times \neq \emptyset$, da cui $I = R$ poiché I contiene un elemento invertibile.⁹ D'altra parte, se $J \triangleleft R$ è un ideale massimale, per quanto appena visto deve essere $J \cap R^\times = \emptyset$, cioè $J \subseteq R \setminus R^\times = \mathfrak{m}$ che è già massimale, da cui $J = \mathfrak{m}$ e \mathfrak{m} è unico. ■

⁹Infatti, se I contiene $r \in R^\times$, detto r^{-1} il suo inverso si ha che $r^{-1}r = 1_R \in I$, da cui $I = R$.

Possiamo quindi caratterizzare tutti e soli gli interi n per cui $\mathbb{Z}/n\mathbb{Z}$ è un anello locale.

Proposizione 1.7.9

L'anello $\mathbb{Z}/n\mathbb{Z}$ è locale se e solo se n è la potenza di un primo.

Dimostrazione. Sia $n = p^k$ con p primo e $k \geq 1$ intero. Osserviamo che $a + p^k\mathbb{Z} \in (\mathbb{Z}/p^k\mathbb{Z})^\times$ se e solo se esiste $b \in \mathbb{Z}$ tale che $ab \in 1 + p^k\mathbb{Z}$, cioè $ab \equiv 1 \pmod{p^k}$. In particolare, vale $ab \equiv 1 \pmod{p}$, da cui per l'*Identità di Bézout* si ha che $\text{MCD}(a, p) = 1$.¹⁰ Si ha quindi che $(\mathbb{Z}/p^k\mathbb{Z})^\times = \{a + p^k\mathbb{Z} : \text{MCD}(a, p) = 1\}$, da cui $\mathfrak{m} = \mathbb{Z}/p^k\mathbb{Z} \setminus (\mathbb{Z}/p^k\mathbb{Z})^\times = p\mathbb{Z}/p^k\mathbb{Z}$ è un ideale di $\mathbb{Z}/p^k\mathbb{Z}$.¹¹ Dunque, $\mathbb{Z}/p^k\mathbb{Z}$ è effettivamente un anello locale.

Viceversa, supponiamo per assurdo che esistano $p \neq q$ primi con $p \mid n$ e $q \mid n$. Poiché per il *Terzo teorema d'isomorfismo* sappiamo che $(\mathbb{Z}/n\mathbb{Z})/(p\mathbb{Z}/n\mathbb{Z}) \simeq \mathbb{Z}/p\mathbb{Z}$ che è un campo, $p\mathbb{Z}/n\mathbb{Z} \triangleleft \mathbb{Z}/n\mathbb{Z}$ è un ideale massimale.¹² Analogamente, anche $q\mathbb{Z}/n\mathbb{Z} \triangleleft \mathbb{Z}/n\mathbb{Z}$ è massimale, ed essendo $p \neq q$ tali ideali sono distinti.¹³ Abbiamo quindi trovato due ideali massimali distinti di $\mathbb{Z}/n\mathbb{Z}$, da cui per la *Proposizione 1.7.8* concludiamo che $\mathbb{Z}/n\mathbb{Z}$ non è locale. ■

Sia R un anello locale e sia $\mathfrak{m} = R \setminus R^\times$. Poiché per la *Proposizione 1.7.8* l'ideale $\mathfrak{m} \triangleleft R$ è massimale, l'anello quoziente R/\mathfrak{m} risulta essere un campo.

Definizione

Sia R un anello locale e sia $\mathfrak{m} = R \setminus R^\times$ il suo unico ideale massimale. Allora, il campo $\text{res}(R) = R/\mathfrak{m}$ è detto campo dei residui di R .

Esempio. Sia \mathbb{K} un campo. Poiché $\mathfrak{m} = \mathbb{K} \setminus \mathbb{K}^\times = \{0_{\mathbb{K}}\}$, si ha che $\text{res}(\mathbb{K}) = \mathbb{K}/\{0_{\mathbb{K}}\} \simeq \mathbb{K}$. □

Esempio. Si consideri $\mathbb{Z}/p^k\mathbb{Z}$ con p primo e $k \geq 1$ intero. Per quanto appena provato nella *Proposizione 1.7.9*, si ha che $\mathfrak{m} = \mathbb{Z}/p^k\mathbb{Z} \setminus (\mathbb{Z}/p^k\mathbb{Z})^\times = p\mathbb{Z}/p^k\mathbb{Z}$, da cui per il *Terzo teorema d'isomorfismo* otteniamo che $\text{res}(\mathbb{Z}/p^k\mathbb{Z}) = (\mathbb{Z}/p^k\mathbb{Z})/(p\mathbb{Z}/p^k\mathbb{Z}) \simeq \mathbb{Z}/p\mathbb{Z}$. □

Esempio. Sia \mathbb{K} un campo. Poiché per la *Proposizione 1.4.X* vale $\mathfrak{m} = \mathbb{K}[[x]] \setminus \mathbb{K}[[x]]^\times = \langle x \rangle$, si ha che $\text{res}(\mathbb{K}[[x]]) = \mathbb{K}[[x]]/\langle x \rangle = \{a + \langle x \rangle : a \in \mathbb{K}\} \simeq \mathbb{K}$. □

Nel caso in cui $\mathfrak{p} \triangleleft R$ sia un ideale primo del dominio di integrità R e $S = R \setminus \mathfrak{p}$, la struttura del campo dei residui dell'anello locale $S^{-1}R$ risulta essere particolarmente interessante.

Proposizione 1.7.10

Sia R un dominio di integrità, $\mathfrak{p} \triangleleft R$ primo e $S = R \setminus \mathfrak{p}$. Allora, $\text{res}(S^{-1}R) \simeq \text{quot}(R/\mathfrak{p})$.

Dimostrazione. Dim ■

Cose, sarebbe carino avere 1.7.10 con il relativo esempio in una pagina a sè stante.

Esempio. Esempio di mostrare che $S = \mathbb{Z} \setminus 13\mathbb{Z}$ è locale e calcolare $\text{res}(S^{-1}\mathbb{Z})$.

¹⁰Secondo l'*Identità di Bézout*, dati due interi a, b non entrambi nulli e detto $d = \text{MCD}(a, b)$, esistono $x, y \in \mathbb{Z}$ tali che $ax + by = d$, e d è il più piccolo intero che può essere scritto in questa forma. In questo caso, essendo $ab \equiv 1 \pmod{p}$, esiste $t \in \mathbb{Z}$ tale che $ab + pt = 1$, dunque $\text{MCD}(a, p) \leq 1$, cioè $\text{MCD}(a, p) = 1$.

¹¹Il complementare di $(\mathbb{Z}/p^k\mathbb{Z})^\times$ in $\mathbb{Z}/p^k\mathbb{Z}$ è costituito da tutte le classi di equivalenza $a + p^k\mathbb{Z}$ per cui $\text{MCD}(a, p) > 1$, cioè, essendo p primo, $\text{MCD}(a, p) = p$. Dunque, $\mathfrak{m} = \{a + p^k\mathbb{Z} : p \mid a\} = p\mathbb{Z}/p^k\mathbb{Z} \triangleleft \mathbb{Z}/p^k\mathbb{Z}$.

¹²Ricordiamo che preso un ideale $I \triangleleft R$, l'anello quoziente R/I è un campo se e solo se I è massimale.

¹³Infatti, sono ideali finiti contenenti un numero diverso di elementi, essendo $|p\mathbb{Z}/n\mathbb{Z}| = \frac{n}{p} \neq \frac{n}{q} = |q\mathbb{Z}/n\mathbb{Z}|$.