Appunti del corso di Algebra II

Dipartimento di Matematica e Applicazioni,
Università di Milano-Bicocca

A.A. 2019/2020

Versione del 3 novembre 2020

Indice

Changelog (versione del 7 Ottobre 2020):

- Reworking completo di varie cose

To do (in ordine di importanza):

- Tutte le annotazioni che ho messo sull'iPad di capitoli 1.1, 1.2, 1.3
- Teoria dei moduli (lezioni dal 06/11/2019 fino alla fine del corso)
- Estensione di campi (lezioni del 25-30/10/19)
- Campi di spezzamento e campi finiti (lezioni del 05-06/11/2019)
- Domini a valutazione discreta (lezioni del 22-23/10/19)
- Capitolo 1.7: sistemare spacing, anello locale che non è dominio, proposizione 1.7.10
- Capitolo 1.5: riduzione mod p, Eisenstein, ciclotomici $x^{p-1} + ... + x + 1$
- Capitolo 1.4: polinomi di Laurent e serie formali (fix i due rif in anelli locali)
- Introduzione?

1 Complementi di teoria degli anelli

1.1 Anelli di polinomi in una variabile

Introduciamo la struttura algebrica dei polinomi, ponendo la convenzione che R indichera' un anello commutativo unitario e $\mathbb{N} = \{1, 2, \dots\}, N_0 = \mathbb{N} \cup \{0\}$.

Definizione 1.1.1: Anello di polinomi in una variabile e operazioni

Sia R un anello commutativo unitario. Denotiamo l'*anello dei polinomi a coefficienti in R nella variabile x* come il seguente insieme

$$R[x] := \left\{ \sum_{i=0}^{n} a_i x^i : a_i \in R,\, n \in \mathbb{N}_0 \right\},$$

dove sono definite due operazioni binarie interne.
Presi infatti due elementi $f(x) = \sum_{i=0}^{m} a_i x^i$ e $g(x) = \sum_{j=0}^{n} b_j x^j$ di $R[x]$, definiamo le operazioni binarie di *somma*

$$+ : R[x] \times R[x] \to R[x],\ \ f(x) + g(x) = \sum_{i=0}^{s} (a_i + b_i) x^i,$$

dove abbiamo posto $s = \max\{m, n\}$ e $a_i = b_j = 0_R$ per $i > m$ e $j > n$, e *prodotto*

$$\cdot : R[x] \times R[x] \to R[x],\ \ f(x) \cdot g(x) = \sum_{k=0}^{m+n} \left(\sum_{i=0}^{k} a_i b_{k-i} \right) x^k.$$

Come visto nel corso di Algebra I, si verifica facilmente che $R[x]$ dotato di tali operazioni di somma e prodotto è un anello commutativo[1] con elemento neutro il polinomio identicamente nullo $0_{R[x]} = 0_R$ e unità il polinomio costante $1_{R[x]} = 1_R$. Vediamone qualche esempio.

Esempio 1.1.2

Se prendiamo $R = \mathbb{Z}$, $f(x) = x^2 + 2x + 3$ e $g(x) = 4x + 5$, si ha che

$$f(x) + g(x) = (1 + 0)x^2 + (2 + 4)x + (3 + 5) = x^2 + 6x + 8,$$

$$\begin{aligned} f(x) \cdot g(x) &= (3 \cdot 0 + 2 \cdot 0 + 1 \cdot 4 + 0 \cdot 5)x^3 + (3 \cdot 0 + 2 \cdot 4 + 1 \cdot 5)x^2 + (3 \cdot 4 + 2 \cdot 5)x + 3 \cdot 5 \\ &= 4x^3 + 13x^2 + 22x + 15. \end{aligned}$$

Di qui in seguito, denoteremo il prodotto di polinomi semplicemente come $f(x)g(x)$ o $f \cdot g$. Possiamo quindi definire su $R[x]$ il concetto di "grado" di un polinomio.

[1] Infatti $a_i b_{k-i} = b_{k-i} a_i$ essendo R un anello commutativo per ipotesi, da cui $f(x) \cdot g(x) = g(x) \cdot f(x)$.

Definizione 1.1.3: Funzione grado; grado di un polinomio

Sia R un anello e sia $f(x) = \sum_{i=0}^{n} a_i x^i \in R[x]$. La funzione $\deg^\star \colon R[x] \to \mathbb{N}_0 \cup \{\infty\}$ definita come

$$\deg^\star(f) = \begin{cases} \max\{k \in \mathbb{N}_0 : a_k \neq 0_R\} & \text{se } f(x) \not\equiv 0_R \\ \infty & \text{se } f(x) \equiv 0_R \end{cases}$$

è detta grado.[2]

Tale definizione coincide con quella classica di grado di un polinomio tranne nel caso in cui $f(x)$ sia identicamente nullo. Infatti, per questa definizione $f(x) \equiv 0_R$ è l'unico polinomio di grado infinito, mentre secondo quella classica anch'esso ha grado 0 in quanto costante.

Esempio 1.1.4

Se consideriamo i polinomi $f(x) = x^2 + 1$, $g(x) \equiv 1$ e $h(x) \equiv 0$ in $\mathbb{Z}[x]$, si ha che $\deg^\star(f) = 2$ e $\deg^\star(g) = 0$, ma $\deg^\star(h) = \infty$.

Possiamo ora dimostrare un risultato che mette in relazione l'anello dei polinomi con quello dei suoi coefficienti, nel caso in cui quest'ultimo sia un dominio di integrità. [3]

Proposizione 1.1.5

Sia R un dominio di integrità. Allora, per ogni $f(x), g(x) \in R[x]$ vale

$$\deg^\star(f \cdot g) = \deg^\star(f) + \deg^\star(g). \ (\star)$$

In particolare, $R[x]$ è un dominio di integrità se e solo se R è un dominio di integrità.

Dimostrazione. Osserviamo innanzitutto che se almeno uno tra $f(x)$ e $g(x)$ è identicamente nullo, allora $(\star)$ è vera perché $f(x)g(x) \equiv 0_R$ e quindi

$$\deg^\star(f \cdot g) = \infty = \deg^\star(f) + \deg^\star(g).$$

D'altra parte, siano $f(x) = \sum_{i=0}^{m} a_i x^i$ e $g(x) = \sum_{j=0}^{n} b_j x^j$ non nulli con $a_m \neq 0_R$ e $b_n \neq 0_R$. Poiché R è un dominio di integrità, $a_m b_n \neq 0_R$, cioè $a_m b_n x^{m+n}$ è il monomio di grado massimo nel prodotto $f(x)g(x)$. Per definizione di grado, concludiamo quindi che

$$\deg^\star(f \cdot g) = m + n = \deg^\star(f) + \deg^\star(g).$$

Sia ora R un dominio di integrità, e mostriamo che lo è anche $R[x]$. Osserviamo innanzitutto che $R[x]$ è un anello commutativo unitario, in quanto eredita tali proprietà da R. Inoltre, presi $f(x), g(x) \in R[x]$ tali che $f(x)g(x) \equiv 0_R$, per quanto appena mostrato vale

[2] Sarebbe più corretto scrivere $\deg^\star(f(x))$, ma si preferisce evitare l'uso di troppe parentesi. Ricordiamo che con $f(x) \equiv k$ si intende il polinomio costante uguale a k. Tale notazione serve per non confondere un polinomio costante $p(x) \equiv 0$ con l'equazione algebrica $p(x) = 0$.

[3] Ricordiamo che un dominio di integrità è un anello commutativo unitario $R \neq \{0_R\}$ senza divisori dello zero, cioè in cui $ab = 0_R$ se e solo se $a = 0_R$ o $b = 0_R$. Esempi di domini di integrità sono $\mathbb{Z}$, le classi di resto $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ con p primo, gli interi gaussiani $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$ e $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$.

$$\deg^\star(f) + \deg^\star(g) = \deg^\star(f \cdot g) = \deg^\star(0_R) = \infty.$$

Dunque, almeno uno fra $f(x)$ e $g(x)$ ha grado infinito ed è quindi il polinomio nullo, cioè $R[x]$ non ha divisori dello zero ed è effettivamente un dominio di integrità. Viceversa, sia $R[x]$ un dominio di integrità. Allora, $R \subseteq R[x]$ è commutativo e unitario in quanto sottoanello, e presi $a, b \in R$, possiamo vedere a e b come polinomi costanti in $R[x]$. Essendo $R[x]$ un dominio di integrità, $ab = 0_R$ se e solo se $a = 0_R$ o $b = 0_R$, da cui anche R non ha divisori dello zero ed è quindi un dominio di integrità. ■

Osserviamo che $(\star)$ non vale quando l'anello R non è un dominio di integrità.

Esempio 1.1.6

Siano $f(x) = 2x + 1$ e $g(x) = 3x + 2$ in $\mathbb{Z}/6\mathbb{Z}\,[x]$. Allora, $\deg^\star(f) = \deg^\star(g) = 1$, ma $f(x)g(x) = 6x^2 + 7x + 2 \equiv_6 x + 2$, da cui $\deg^\star(f \cdot g) = 1 \neq 2 = \deg^\star(f) + \deg^\star(g)$.

Più in generale, se R non è un dominio di integrità, per definizione esistono $a, b \in R$ non nulli tali che $ab = 0_R$. Allora, detti $f(x) = ax$ e $g(x) = bx$, si ha $f(x)g(x) = abx^2 = 0_R x^2 = 0_R$, da cui, essendo $\deg^\star(f) = \deg^\star(g) = 1$, l'uguaglianza $(\star)$ non vale perché

$$\deg^\star(f \cdot g) = \deg^\star(0_R) = \infty \neq 2 = \deg^\star(f) + \deg^\star(g).$$

Dunque, per la proposizione 1.1.5 segue che $(\star)$ vale se e solo se R è un dominio di integrità.

Prima di procedere nello studio degli anelli di polinomi, richiamiamo il concetto di elemento invertibile di un anello. Preso un anello R, sia $R^\times$ l'insieme degli elementi di R che hanno inverso moltiplicativo, cioè l'insieme degli $a \in R$ per cui esiste $b \in R$ tale che $ab = 1_R$. Se esiste, denotiamo l'inverso moltiplicativo di a con a^{-1}. Allora, vale la proposizione seguente.

Proposizione 1.1.7

Sia R un anello. Allora, $R^\times$ è un gruppo rispetto al prodotto.

Dimostrazione. Osserviamo innanzitutto che il prodotto è associativo essendo R un anello, e in particolare 1_R è l'unità anche di $R^\times$. Inoltre, presi $a, b \in R^\times$, per definizione esistono $c, d \in R$ tali che $ac = 1_R$ e $bd = 1_R$, dunque

$$(ab)(dc) = a(bd)c = a1_R c = ac = 1_R,$$

cioè $ab \in R^\times$ è invertibile con inverso dc, da cui $R^\times$ è chiuso rispetto al prodotto. Infine, se $ab = 1_R$ è evidente che anche $a^{-1} = b \in R^\times$, dunque $(R^\times, \cdot)$ è effettivamente un gruppo. ■

Grazie a tale proposizione, la definizione seguente risulta quindi ben posta.

Definizione 1.1.8: Gruppo moltiplicativo di un anello

Sia R un anello unitario commutativo. L'insieme $R^\times$ degli elementi di R che ammettono inverso moltiplicativo è un gruppo detto *gruppo moltiplicativo di* R.[4]

Se da una parte la proposizione 1.1.5 mostra che $R[x]$ può avere la struttura di un dominio di integrità, l'anello dei polinomi $R[x]$ non è mai un campo, nemmeno se lo è R stesso.[5] Infatti, $x \in R[x]$ non è un elemento invertibile perché il suo inverso $1/x$ non è un polinomio.[6] Risulta quindi naturale chiedersi quali elementi di $R[x]$ siano effettivamente invertibili.

Proposizione 1.1.9

Sia R un dominio di integrità. Allora, $R[x]^\times = R^\times$.

Dimostrazione. Poiché ogni elemento di $R^\times$ può essere visto come polinomio costante di $R[x]$, è evidente che $R^\times \subseteq R[x]^\times$. D'altra parte, siano $f(x), g(x) \in R[x]^\times$ tali che $f(x)g(x) = 1_R$. Allora, per la *Proposizione 1.1.1* si ha che

$$\deg^\star(f \cdot g) = \deg^\star(1_R) = 0 = \deg^\star(f) + \deg^\star(g),$$

quindi $\deg^\star(f) = \deg^\star(g) = 0$ essendo il grado non negativo. Questo prova che ogni elemento di $R[x]^\times$ è in realtà una costante invertibile, cioè $R[x]^\times \subseteq R^\times$, dunque $R[x]^\times = R^\times$. ■

Parliamo ora di una idea abbastanza importante che ci permettera' di parlare della *valutazione di un polinomio*.

Osservazione 1.1.10: Una relazione piu' generica di sottoanello

Sia R un anello, e supponiamo di voler aggiungere a R un certo elemento $x \notin R$ senza alcuna relazione con gli altri elementi di R, in modo che la struttura algebrica risultante sia ancora un anello e sia la più piccola possibile. Come possiamo fare?
Poiché ogni anello è chiuso rispetto a somma e prodotto, tale struttura conterrà anche tutte le potenze non negative $\{x^0, x^1, x^2, ...\}$ di x e tutte le combinazioni lineari tra potenze di x ed elementi di R, cioè tutti gli elementi della forma $a_n x^n + ... + a_1 x + a_0$ con $a_0, ..., a_n \in R$. Dunque, l'anello dei polinomi $R[x]$ sembra essere la struttura che soddisfa le nostre richieste, cioè il più piccolo anello contenente sia R che x. Resta solo da formalizzare meglio il concetto di "più piccolo anello", cioè chiarire cosa significa che un anello ne contiene un altro.
A questo scopo, potremmo considerare sull'insieme degli anelli la relazione d'ordine data dall'inclusione, cioè dire che un anello R è più piccolo di un altro anello S se e solo se $R \subseteq S$. Tuttavia, questo non terrebbe conto dell'importanza algebrica degli isomorfismi: infatti, la struttura che stiamo cercando di costruire è definita a meno di isomorfismi, e anelli isomorfi potrebbero essere non confrontabili secondo l'inclusione.[7] Per risolvere tale problema, ha quindi più senso definire che R è più piccolo di S se e solo se S contiene una copia isomorfa dell'anello R, cioè se e solo se esiste un sottanello di S isomorfo a R.

[4] Tale gruppo viene spesso indicato anche con $\mathcal{U}(R)$ o $R^\star$ ed è anche detto "gruppo delle unità di R".
[5] Vedremo nel *Capitolo 1.4* una generalizzazione degli anelli di polinomi con la struttura di un campo.
[6] Più rigorosamente, se $f(x) = x$ fosse invertibile, esisterebbe $g(x) \in R[x]$ tale che $f(x)g(x) = 1_R$, da cui $\deg^\star(f \cdot g) = \deg^\star(1_R) = 0 = \deg^\star(f) + \deg^\star(g)$, cioè $\deg^\star(g) = -\deg^\star(f) = -1 < 0$, assurdo.
[7] Ad esempio, si verifica facilmente che la mappa $\varphi\colon \mathbb{C} \to \mathrm{Mat}_{2\times 2}(\mathbb{R})$, $a + bi \mapsto \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ è un isomorfismo di anelli, ma $\mathbb{C} \not\subseteq \mathrm{Mat}_{2\times 2}(\mathbb{R})$ e $\mathrm{Mat}_{2\times 2}(\mathbb{R}) \not\subseteq \mathbb{C}$, cioè tali anelli non sono confrontabili secondo l'inclusione.

Possiamo ora definire piu' formalmente il concetto appena visto:

Definizione 1.1.11: Anello piu' piccolo

Siano R e S due anelli. Diciamo che R è più piccolo di S (o anche che S contiene R) se e solo se esiste un omomorfismo di anelli iniettivo $\varphi\colon R \to S$.

Si osservi che tale definizione è equivalente a quanto detto sopra: se esiste un monomorfismo (cioè un omomorfismo iniettivo) $\varphi\colon R \to S$, la restrizione $\varphi\colon R \to \varphi(R)$ è un isomorfismo, dunque l'immagine $\varphi(R) \subseteq S$ è un sottoanello di S isomorfo a R.

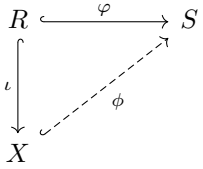
Esempio 1.1.12

Chiaramente $\mathbb{R}$ non è un sottoanello di $\mathbb{R}^2$, in quanto $\mathbb{R} \not\subseteq \mathbb{R}^2$. D'altra parte, la mappa $\varphi\colon \mathbb{R} \to \mathbb{R}^2$, $x \mapsto (x, x)$ è un omomorfismo iniettivo, quindi $\mathbb{R}^2$ contiene una copia isomorfa di $\mathbb{R}$, che geometricamente corrisponde alla bisettrice $y = x$.

Osservazione. Tornando al problema iniziale, sia X la struttura algebrica che stiamo cercando di costruire. Allora, possiamo riformulare le condizioni su X come segue:

- X contiene $R \Rightarrow$ esiste un monomorfismo $\iota\colon R \to X$;
- X è il più piccolo anello contenente sia R che $x \notin R \Rightarrow$ per ogni altro anello S con tali proprietà (cioè tale che esista un monomorfismo $\varphi\colon R \to S$ e contenente un $s \notin R$), abbiamo che X è più piccolo di S, ossia esiste un monomorfismo $\phi\colon X \to S$.

In particolare, richiediamo che tale mappa ϕ soddisfi $\phi(x) = s$ e $\phi(\iota(R)) = \varphi(R)$, cioè che mandi l'elemento aggiunto x nell'elemento aggiunto s e la copia isomorfa $\iota(R)$ di R in X nella copia isomorfa $\varphi(R)$ di R in S.



Osserviamo ora che l'anello dei polinomi $R[x]$ soddisfa effettivamente tali proprietà. Infatti, detta $\iota\colon R \to R[x]$ la mappa di inclusione che manda ogni elemento $r \in R$ nel corrispondente polinomio costante $r \in R[x]$, è evidente che ι sia un monomorfismo, e preso un qualunque monomorfismo $\varphi\colon R \to S$, basta definire $\phi\colon R[x] \to S$ ponendo $\phi(x) = s$ e $\phi(\iota(r)) = \varphi(r)$ per ogni $r \in R$. Tale mappa si estende per linearità su tutto $R[x]$ ponendo

$$\phi\left(\sum_{i=0}^{n} r_i x^i\right) = \sum_{i=0}^{n} \varphi(r_i) s^i$$

ed è facile verificare che ϕ sia un monomorfismo. [8] Più in generale, vale il teorema seguente.

[8] Approfondiremo meglio questa questione nel *Capitolo 2.1* quando tratteremo le estensioni di campi.

Teorema 1.1.13: Proprietà universale

Siano R e S due anelli e sia $\varphi\colon R \to S$ un omomorfismo. Allora, per ogni $s \in S$ esiste un unico omomorfismo di anelli $\phi\colon R[x] \to S$ tale che $\phi(x) = s$ e $\phi_{|_R} = \varphi$.

Dimostrazione. Siano $f(x) = \sum_{i=0}^{m} a_i x^i$ e $g(x) = \sum_{j=0}^{n} b_j x^j$ in $R[x]$ e sia $\phi(f) = \sum_{i=0}^{m} \varphi(a_i) s^i$. Osserviamo innanzitutto che $\phi(f)$ è ben definita. Infatti, $\varphi(a_i) \in S$ e $\phi(f) \in S$ perché somma di prodotti di elementi dell'anello S, che è chiuso rispetto a somma e prodotto. Inoltre, $\phi(x) = \varphi(1_R)s^1 = s$ e $\phi(r) = \varphi(r)s^0 = \varphi(r)$ per ogni $r \in R$, quindi ϕ soddisfa le condizioni richieste. Mostriamo ora che ϕ preserva le operazioni. Infatti,

$$\phi(f+g) = \sum_{i=0}^{\max\{m,n\}} \varphi(a_i + b_i)s^i = \sum_{i=0}^{m} \varphi(a_i)s^i + \sum_{j=0}^{n} \varphi(b_j)s^j = \phi(f) + \phi(g)$$

per la distributività del prodotto rispetto alla somma e perché $\varphi(a_i + b_i) = \varphi(a_i) + \varphi(b_i)$, e

$$\phi(f \cdot g) = \sum_{k=0}^{m+n} \left(\sum_{i=0}^{k} \varphi(a_i b_{k-i}) \right) s^k = \left(\sum_{i=0}^{m} \varphi(a_i)s^i \right) \left(\sum_{j=0}^{n} \varphi(b_j)s^j \right) = \phi(f) \cdot \phi(g)$$

per come è definito il prodotto tra polinomi e perché $\varphi(a_i b_{k-i}) = \varphi(a_i)\varphi(b_{k-i})$ essendo φ un omomorfismo. Poiché $\phi(0_{R[x]}) = \varphi(0_R) = 0_S$ e $\phi(1_{R[x]}) = \varphi(1_R) = 1_S$, concludiamo che tale mappa ϕ è effettivamente un omomorfismo di anelli.

Mostriamo ora che ϕ è unico. Sia $\psi\colon R[x] \to S$ un altro omomorfismo di anelli tale che $\psi(x) = s$ e $\psi_{|_R} = \varphi$. Poiché ψ preserva le operazioni, per ogni $f(x) = \sum_{i=0}^{m} a_i x^i \in R[x]$ vale

$$\psi(f) = \psi\left(\sum_{i=0}^{m} a_i x^i \right) = \sum_{i=0}^{m} \psi(a_i)\psi(x^i) = \sum_{i=0}^{m} \varphi(a_i)\psi(x)^i = \sum_{i=0}^{m} \varphi(a_i)s^i = \phi(f)$$

essendo $\psi(a_i) = \varphi(a_i)$ perché $a_i \in R$ e $\psi(x^i) = \psi(x)^i = s^i$. Dunque, ψ coincide con ϕ per ogni polinomio $f(x) \in R[x]$, da cui ϕ è unico. ■

Nel caso particolare in cui $\varphi = \mathrm{id}_R$ e quindi $R \subseteq S$, la mappa ϕ di cui sopra viene spesso denotata con ϕ_s. In questo caso, $\phi_s(f)$ non è altro che il polinomio $f(x)$ calcolato in $x = s$, cioè $\phi_s(f) = f(s)$, il che spiega l'origine del nome "valutazione in s" per tale mappa.

Definizione 1.1.14: Valutazione di un polinomio

Tale omomorfismo di anelli ϕ_s è detto *valutazione in s*.

Esempio 1.1.15

Se $R = \mathbb{Z}$, $S = \mathbb{Z}[\sqrt{2}]$ e $f(x) = x^2 + 2x + 3 \in \mathbb{Z}[x]$, detta $\phi_{\sqrt{2}} \colon \mathbb{Z}[x] \to \mathbb{Z}[\sqrt{2}]$ la valutazione in $\sqrt{2}$, abbiamo che $\phi_{\sqrt{2}}(f) = (\sqrt{2})^2 + 2\sqrt{2} + 3 = 5 + 2\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$.

Vogliamo ora dimostrare che la *proprietà universale* è una caratteristica propria degli anelli di polinomi, cioè che se T è un anello contenente sia R che un elemento $t \notin R$ e dotato della *proprietà universale*, allora $T \cong R[x]$. Nella dimostrazione ci limiteremo al caso in cui $R \subseteq T$ e $\varphi = \mathrm{id}_R$ (e quindi $R \subseteq S$), ma il caso generale è del tutto analogo.

Teorema 1.1.16

Sia R un anello e sia $T \supseteq R$ un anello contenente un elemento $t \notin R$ e tale che per ogni anello $S \supseteq R$ e per ogni $s \in S$ esista un unico omomorfismo di anelli $\psi \colon T \to S$ con $\psi(t) = s$ e $\psi_{|_R} = \mathrm{id}_R$. Allora, $T \cong R[x]$.

Dimostrazione. Poiché per ipotesi tale proprietà vale per ogni anello $S \supseteq R$, in particolare scegliamo $S = R[s]$ e siano $\phi_t \colon R[s] \to T$ la valutazione in t [9] e $\alpha = \phi_t \circ \psi \colon T \to T$.

$$\begin{array}{ccc} T & \xrightarrow{\psi} & R[s] \\ & \searrow^{\alpha} & \downarrow{\scriptstyle \phi_t} \\ & & T \end{array}$$

Osserviamo innanzitutto che α è ben definito ed è un omomorfismo in quanto composizione di omomorfismi. Inoltre, $\alpha(t) = \phi_t(\psi(t)) = \phi_t(s) = t$ e $\alpha(r) = \phi_t(\psi(r)) = \phi_t(r) = r$ per ogni $r \in R$, cioè $\alpha_{|_R} = \mathrm{id}_R$. D'altra parte, poiché $T \supseteq R$, possiamo scegliere $S = T$ e $s = t$ nell'enunciato del teorema, così sappiamo che esiste un unico omomorfismo $\psi' \colon T \to T$ tale che $\psi'(t) = t$ e $\psi'_{|_R} = \mathrm{id}_R$. Poiché anche l'identità $\mathrm{id}_T \colon T \to T$ soddisfa tali proprietà, per l'unicità di ψ' deve essere $\alpha = \mathrm{id}_T$. Sia ora $\beta = \psi \circ \phi_t \colon R[s] \to R[s]$.

$$\begin{array}{ccc} R[s] & \xrightarrow{\phi_t} & T \\ & \searrow^{\beta} & \downarrow{\scriptstyle \psi} \\ & & R[s] \end{array}$$

Come sopra, osserviamo che β è ben definito ed è un omomorfismo in quanto composizione di omomorfismi. Inoltre, $\beta(s) = \psi(\phi_t(s)) = \psi(t) = s$ e $\beta(r) = \psi(\phi_t(r)) = \psi(r) = r$ per ogni $r \in R$, cioè $\beta_{|_R} = \mathrm{id}_R$. Poiché anche l'identità $\mathrm{id}_{R[s]} \colon R[s] \to R[s]$ soddisfa $\mathrm{id}_{R[s]}(s) = s$ e $\mathrm{id}_{R[s]\,|_R} = \mathrm{id}_R$, e per il *Teorema 1.1.4* esiste un unico omomorfismo con queste proprietà, deve essere $\beta = \mathrm{id}_{R[s]}$. Dunque, essendo $\phi_t \circ \psi = \mathrm{id}_T$ e $\psi \circ \phi_t = \mathrm{id}_{R[s]}$ isomorfismi, lo sono anche ψ e ϕ_t,[10] da cui concludiamo che $T \cong R[s] \cong R[x]$.[11] ■

[9] Ricordiamo che per il *Teorema 1.1.13* tale omomorfismo è l'unico che soddisfa $\phi_t(s) = t$ e $\phi_{t\,|_R} = \mathrm{id}_R$.

[10] In generale, se $f \colon X \to Y$ e $g \colon Y \to X$ sono omomorfismi tali che $g \circ f = \mathrm{id}_X$ e $f \circ g = \mathrm{id}_Y$, allora f e g sono isomorfismi. Infatti, f è iniettivo perché $f(x) = f(x') \Rightarrow x = g(f(x)) = g(f(x')) = x'$, ed è suriettivo perché preso $y \in Y$, si ha che $g(y) \in X$ e $f(g(y)) = y$. In modo del tutto analogo si dimostra che anche g è un isomorfismo, e in particolare risulta quindi che $g = f^{-1}$.

[11] Infatti s è solo un nome qualunque per la variabile dei polinomi a coefficienti in R.

1.2 Anelli di polinomi in n variabili

Vogliamo ora estendere il concetto di anello di polinomi ad un numero finito di variabili. Prima pero' dovrem mo definire e richiamare alcuni oggetti matematici:

Definizione 1.2.1: Insieme dei monomi in n variabili e operazioni

Sia n un intero positivo. Denotiamo con $M = \text{mon}\{x_1, \dots, x_n\}$ l'insieme dei monomi nelle variabili $x_1, \dots, x_n$, cioè $M = \{x_1^{\alpha_1} \cdot \dots \cdot x_n^{\alpha_n} : \alpha_i \in \mathbb{N}_0\}$.

Presi due elementi $u = x_1^{\alpha_1} \cdot \dots \cdot x_n^{\alpha_n}$ e $v = x_1^{\beta_1} \cdot \dots \cdot x_n^{\beta_n}$ di M, è possibile definire su M un'operazione binaria corrispondente al *prodotto* di monomi:

$$u \cdot v = x_1^{\alpha_1+\beta_1} \cdot \dots \cdot x_n^{\alpha_n+\beta_n}.$$

Proposizione 1.2.2

$(M, \cdot)$ e' un monoide commutativo.

Dimostrazione. Osserviamo infatti che:

- $u \cdot v = x_1^{\alpha_1+\beta_1} \cdot \dots \cdot x_n^{\alpha_n+\beta_n} \in M$ perché $\alpha_i + \beta_i \in \mathbb{N}_0$, cioè M è chiuso rispetto a $\cdot$
- tale operazione agisce sugli esponenti delle variabili $x_1, \dots, x_n$ mediante la somma, ed essendo tali esponenti in $\mathbb{N}_0$ e la somma associativa su $\mathbb{N}_0$, anche $\cdot$ è associativo
- esiste un elemento neutro $1_M = x_1^0 \cdot \dots \cdot x_n^0 \in M$
- $u \cdot v = x_1^{\alpha_1+\beta_1} \cdot \dots \cdot x_n^{\alpha_n+\beta_n} = x_1^{\beta_1+\alpha_1} \cdot \dots \cdot x_n^{\beta_n+\alpha_n} = v \cdot u$, cioè M è commutativo.

■

Richiamiamo ora un importante concetto derivante dalla topologia e alcune sue proprietà.

Definizione 1.2.3: Supporto di una funzione

Siano X e Y insiemi non vuoti e sia $f\colon X \to Y$ una funzione. Si definisce supporto di f l'insieme $\text{supp}(f) = \{x \in X : f(x) \neq 0_Y\}$. Se $|\text{supp}(f)| < \infty$, diciamo che f ha supporto *finito*.

Osservazione. Tale definizione ha senso solo se l'insieme Y contiene un elemento neutro 0_Y: nel nostro caso, avendo a che fare con anelli, è naturale identificare tale elemento con l'elemento neutro dell'addizione.

Esempio 1.2.4

1. Sia $f\colon \mathbb{Z} \to \mathbb{R}$ la funzione $f(x) = x^2 - 1$. Allora, $\text{supp}(f) = \mathbb{Z} \setminus \{\pm 1\}$.
2. Se $f\colon \text{Mat}_{2\times 2}(\mathbb{F}_2) \to \mathbb{F}_2$ è il determinante, allora f ha supporto finito perché

$$\text{supp}(f) = \text{GL}(2,\mathbb{F}_2)^{12} = \left\{ \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \right\}$$

Proposizione 1.2.5

Siano $f, g\colon X \to Y$ funzioni e siano $(f+g)(x) = f(x)+g(x)$ e $(f\cdot g)(x) = f(x)\cdot g(x)$. Allora, $\text{supp}(f+g) \subseteq (\text{supp}(f) \cup \text{supp}(g))$ e $\text{supp}(f\cdot g) \subseteq (\text{supp}(f) \cap \text{supp}(g))$.

Dimostrazione. Osserviamo che se $x \in \text{supp}(f+g)$, allora per definizione $f(x)+g(x) \neq 0_Y$, cioè almeno uno tra $f(x)$ e $g(x)$ è non nullo e quindi $x \in (\text{supp}(f) \cup \text{supp}(g))$.
Analogamente, se $x \in \text{supp}(f\cdot g)$, per definizione abbiamo che $f(x)\cdot g(x) \neq 0_Y$, dunque $f(x) \neq 0_Y$ e $g(x) \neq 0_Y$, ossia $x \in (\text{supp}(f) \cap \text{supp}(g))$. ■

Esempio 1.2.6

Siano $f, g\colon \mathbb{Z} \to \mathbb{R}$ le funzioni $f(x) = x^2-3x+2$ e $g(x) = x^2+x-2$. Allora, è evidente che $\text{supp}(f) = \mathbb{Z}\setminus\{1,2\}$ e $\text{supp}(g) = \mathbb{Z}\setminus\{1,-2\}$, ed essendo $(f+g)(x) = 2x^2-2x$ e $(f\cdot g)(x) = (x-1)^2(x-2)(x+2)$, abbiamo che

$$\text{supp}(f+g) = \mathbb{Z}\setminus\{0,1\} \subseteq \mathbb{Z}\setminus\{1\} = \text{supp}(f)\cup\text{supp}(g),$$
$$\text{supp}(f\cdot g) = \mathbb{Z}\setminus\{1,\pm 2\} = \text{supp}(f)\cap\text{supp}(g),$$

in accordo con la *Proposizione 1.2.5.*

Parliamo ora di un certo insieme di funzioni e analizziamone proprieta' e notazione:

Osservazione 1.2.7

Per comodita' di scrittura, sia $I_n = \{1,\dots,n\}$ e sia $\underline{\alpha}\colon I_n \to \mathbb{N}_0$ la funzione che associa alla i-esima variabile x_i l'esponente $\underline{\alpha}(i) = \alpha_i$. Denotiamo con $x^{\underline{\alpha}} = x_1^{\alpha_1}\cdot\ldots\cdot x_n^{\alpha_n} \in M$.

Esempio. Se $M = \text{mon}\{x_1,x_2,x_3,x_4\}$ e $\underline{\alpha}\colon \{1,2,3,4\} \to \mathbb{N}_0$ è la funzione definita come $\underline{\alpha}(1) = 2$, $\underline{\alpha}(2) = \underline{\alpha}(3) = 1$ e $\underline{\alpha}(4) = 0$, abbiamo che $x^{\underline{\alpha}} = x_1^2x_2^1x_3^1x_4^0 = x_1^2x_2x_3 \in M$.

Detto $\mathcal{F} = \mathcal{F}(I_n,\mathbb{N}_0)$ l'insieme delle funzioni $\underline{\alpha}\colon I_n \to \mathbb{N}_0$[13], vi è una corrispondenza biunivoca tra $\mathcal{F}$ e l'insieme dei monomi M. Infatti, ogni monomio $x_1^{\alpha_1}\cdot\ldots\cdot x_n^{\alpha_n}$ corrisponde in modo naturale all'unica funzione $\underline{\alpha} \in \mathcal{F}$ tale che $\underline{\alpha}(i) = \alpha_i$ per ogni $i \in I_n$, e ogni funzione $\underline{\beta} \in \mathcal{F}$ rappresenta univocamente il monomio $x_1^{\beta(1)}\cdot\ldots\cdot x_n^{\beta(n)} \in M$.

Siamo ora in grado di poter introdurre le idee necessarie alla formalizzazione dell'anello dei polinomi in n variabili.

[12] Ricordiamo che $\text{GL}(n,\mathbb{K})$ è il gruppo delle matrici $n\times n$ invertibili con entrate nel campo $\mathbb{K}$.
[13] In generale, dati due insiemi X e Y, si denota con $\mathcal{F}(X,Y)$ l'insieme di tutte le funzioni $f\colon X \to Y$.

Costruzione dell'anello dei polinomi in n variabili.

Sia R un anello commutativo unitario e sia $\mathcal{F}^\times(\mathcal{F},R)=\{r_\_:\mathcal{F}\to R:|\operatorname{supp}(r_\_)|<\infty\}$[14], cioè l'insieme di tutte le funzioni $r_\_$ che associano ad ogni funzione $\underline{\alpha}\in\mathcal{F}$ un elemento $r_{\underline{\alpha}}\in R$ e che sono diverse dall'elemento neutro 0_R solo per un numero finito di elementi di $\mathcal{F}$. Possiamo quindi definire un polinomio nelle variabili $x_1,\dots,x_n$ ponendo

$$f(x_1,\dots,x_n)=\sum_{\underline{\alpha}\in\mathcal{F}} r_{\underline{\alpha}}x^{\underline{\alpha}}.$$

Infatti, $f(x_1,\dots,x_n)$ risulta essere la somma di un numero finito di monomi non nulli, ognuno con il relativo coefficiente $r_{\underline{\alpha}}$. Questo punto è fondamentale: abbiamo scelto $r_\_\in\mathcal{F}^\times(\mathcal{F},R)$ con supporto finito così che soltanto un numero finito degli infiniti monomi di M abbia un coefficiente $r_{\underline{\alpha}}\neq 0_R$. Così facendo, nella sommatoria vi è solo un numero finito di elementi perché tutti gli infiniti altri sono nulli, dunque f è effettivamente un polinomio.

Esempio. Siano $M=\operatorname{mon}\{x,y\}$ e $R=\mathbb{Z}$. Detta $r_\_:\mathcal{F}\to\mathbb{Z}$ la funzione

$$r_{\underline{\alpha}}=\begin{cases}2\underline{\alpha}(1)-\underline{\alpha}(2) & \text{se } \underline{\alpha}(1)+\underline{\alpha}(2)=3\\ 0 & \text{altrimenti}\end{cases}$$

al variare di $\underline{\alpha}\in\mathcal{F}=\mathcal{F}(I_2,\mathbb{N}_0)$, essendo $\underline{\alpha}(1)\geq 0$ e $\underline{\alpha}(2)\geq 0$, è evidente che esista solo un numero finito di funzioni $\underline{\alpha}\in\mathcal{F}$ per cui $\underline{\alpha}(1)+\underline{\alpha}(2)=3$. In tutti gli altri casi abbiamo che $r_{\underline{\alpha}}=0$, quindi $r_\_$ ha supporto finito, cioè $r_\_\in\mathcal{F}^\times(\mathcal{F},R)$. Se identifichiamo $\underline{\alpha}$ con la coppia $(\alpha_1,\alpha_2)=(\underline{\alpha}(1),\underline{\alpha}(2))$,[15] possiamo quindi definire il polinomio

$$\begin{aligned}f(x,y)&=\sum_{\underline{\alpha}\in\mathcal{F}} r_{(\alpha_1,\alpha_2)}x^{\alpha_1}y^{\alpha_2}\\&=r_{(3,0)}x^3y^0+r_{(2,1)}x^2y^1+r_{(1,2)}x^1y^2+r_{(3,0)}x^3y^0+\dots\ [16]\\&=(2\cdot 3-0)x^3+(2\cdot 2-1)x^2y+(2\cdot 1-2)xy^2+(2\cdot 0-3)y^3\\&=6x^3+3x^2y-3y^3.\ \square\end{aligned}$$

Possiamo finalmente definire dell'anello dei polinomi nelle variabili $x_1,\dots,x_n$.

Definizione 1.2.8: Anello dei polinomi in n variabili e operazioni

Sia R un anello commutativo unitario e $n\in\mathbb{N}$. L'*anello dei polinomi in n variabili* e' l'insieme

$$R[x_1,\dots,x_n]=\left\{\sum_{\underline{\alpha}\in\mathcal{F}} r_{\underline{\alpha}}x^{\underline{\alpha}}:r_\_\in\mathcal{F}^\times(\mathcal{F},R)\right\}$$

dotato delle seguenti operazioni binarie di somma e prodotto. Presi due elementi

$$f(x_1,\dots,x_n)=\sum_{\underline{\alpha}\in\mathcal{F}} r_{\underline{\alpha}}x^{\underline{\alpha}}\quad\text{e}\quad g(x_1,\dots,x_n)=\sum_{\underline{\beta}\in\mathcal{F}} s_{\underline{\beta}}x^{\underline{\beta}}$$

[14] Ricordiamo che $\mathcal{F}$ e' l'insieme delle funzioni $\underline{\alpha}\colon I_n\to\mathbb{N}_0$ definto nella pagina precedente

[15] Infatti $\mathcal{F}(I_n,\mathbb{N}_0)\cong\mathbb{N}_0^n$ mediante l'isomorfismo $\varphi\colon\mathcal{F}(I_n,\mathbb{N}_0)\to\mathbb{N}_0^n$, $\underline{\alpha}\mapsto(\underline{\alpha}(1),\dots,\underline{\alpha}(n))$.

[16] Tutti gli altri termini della sommatoria sono nulli perché $\underline{\alpha}(1)+\underline{\alpha}(2)\neq 3$ e quindi, per come abbiamo definito $r_\_$, il coefficiente del monomio $x^{\alpha_1}y^{\alpha_2}$ è $r_{\underline{\alpha}}=0$.

di $R[x_1, \dots, x_n]$, definiamo le operazioni di somma e prodotto

$$f(x_1, \dots, x_n) + g(x_1, \dots, x_n) = \sum_{\underline{\alpha} \in \mathcal{F}} (r_{\underline{\alpha}} + s_{\underline{\alpha}}) x^{\underline{\alpha}}$$

$$f(x_1, \dots, x_n) \cdot g(x_1, \dots, x_n) = \sum_{\underline{\gamma} \in \mathcal{F}} t_{\underline{\gamma}} x^{\underline{\gamma}}$$

dove abbiamo posto $t_{\underline{\gamma}} = \sum_{\underline{\alpha}+\underline{\beta}=\underline{\gamma}} r_{\underline{\alpha}} s_{\underline{\beta}}$.
Anche in questo caso, tali operazioni non sono altro che la formalizzazione delle usuali operazioni di somma e prodotto tra polinomi.

Proposizione 1.2.9

Tali operazioni di somma e prodotto su $R[x_1, \dots, x_n]$ sono ben poste.

Dimostrazione. Nel caso della somma, è sufficiente mostrare che $(r_- + s_-) \in \mathcal{F}^{\times}(\mathcal{F}, R)$, cioè che la somma di due funzioni in $\mathcal{F}^{\times}(\mathcal{F}, R)$ è ancora una funzione in $\mathcal{F}^{\times}(\mathcal{F}, R)$. Osserviamo che $(r_- + s_-)(\underline{\alpha}) = r_{\underline{\alpha}} + s_{\underline{\alpha}} \in R$ per ogni $\underline{\alpha} \in \mathcal{F}$ essendo $r_{\underline{\alpha}}, s_{\underline{\alpha}} \in R$ e R chiuso rispetto alla somma in quanto anello, quindi $r_- + s_-$ è effettivamente una funzione da $\mathcal{F}$ in R. Inoltre, per la *Proposizione 1.2.5* si ha che

$$\operatorname{supp}(r_- + s_-) \subseteq [\operatorname{supp}(r_-) \cup \operatorname{supp}(s_-)]$$

e tale insieme è finito poiché unione di insiemi finiti. Dunque, $r_- + s_-$ ha supporto finito, da cui concludiamo che $(r_- + s_-) \in \mathcal{F}^{\times}(\mathcal{F}, R)$, cioè che $\mathcal{F}^{\times}(\mathcal{F}, R)$ è chiuso rispetto alla somma.

Nel caso del prodotto, dobbiamo mostrare che $t_- \in \mathcal{F}^{\times}(\mathcal{F}, R)$. Osserviamo innanzitutto che per ogni $\underline{\gamma} \in \mathcal{F}$ fissato, la somma

$$t_{\underline{\gamma}} = \sum_{\underline{\alpha}+\underline{\beta}=\underline{\gamma}} r_{\underline{\alpha}} s_{\underline{\beta}}$$

contiene un numero finito di addendi. Infatti, la condizione $\underline{\gamma} = \underline{\alpha} + \underline{\beta} \Rightarrow \underline{\gamma}(i) = \underline{\alpha}(i) + \underline{\beta}(i)$ per ogni $i \in I_n$ implica che $0 \leq \underline{\alpha}(i) \leq \underline{\gamma}(i)$, dunque abbiamo un numero finito di scelte per ogni $\underline{\alpha}(i)$ e quindi anche per $\underline{\alpha}$. Essendo $t_{\underline{\gamma}}$ la somma di un numero finito di prodotti $r_{\underline{\alpha}} s_{\underline{\beta}} \in R$, anche $t_{\underline{\gamma}} \in R$ per ogni $\underline{\gamma} \in \mathcal{F}$, cioè t_- è effettivamente una funzione da $\mathcal{F}$ in R. Infine, osserviamo che sempre per la *Proposizione 1.2.5* si ha che

$$\operatorname{supp}(r_- \cdot s_-) \subseteq [\operatorname{supp}(r_-) \cap \operatorname{supp}(s_-)]$$

dove tale insieme è finito poiché intersezione di insiemi finiti, quindi $(r_- \cdot s_-) \in \mathcal{F}^{\times}(\mathcal{F}, R)$. Dunque, t_- è la somma di un numero finito di funzioni in $\mathcal{F}^{\times}(\mathcal{F}, R)$, e avendo mostrato sopra che $\mathcal{F}^{\times}(\mathcal{F}, R)$ è chiuso rispetto alla somma, concludiamo che $t_- \in \mathcal{F}^{\times}(\mathcal{F}, R)$. ■

Per semplicità di notazione denoteremo di qui in seguito gli elementi di $R[x_1, \dots, x_n]$ come f, g, eccetera, dove si intende che $f = f(x_1, \dots, x_n)$, $g = g(x_1, \dots, x_n)$ e così via. Possiamo quindi finalmente dimostrare la proposizione seguente.

Proposizione 1.2.10

Sia R un anello commutativo. Allora, $R[x_1, \dots, x_n]$ dotato di tali operazioni di somma e prodotto è un anello commutativo.

Dimostrazione. Siano $f = \sum_{\underline{\alpha} \in \mathcal{F}} r_{\underline{\alpha}} x^{\underline{\alpha}}$, $g = \sum_{\underline{\beta} \in \mathcal{F}} s_{\underline{\beta}} x^{\underline{\beta}}$ e $h = \sum_{\underline{\gamma} \in \mathcal{F}} t_{\underline{\gamma}} x^{\underline{\gamma}}$ elementi di $R[x_1, \dots, x_n]$. Osserviamo innanzitutto che

$$\begin{aligned}(f+g)+h &= \sum_{\underline{\alpha} \in \mathcal{F}} (r_{\underline{\alpha}} + s_{\underline{\alpha}}) x^{\underline{\alpha}} + \sum_{\underline{\gamma} \in \mathcal{F}} t_{\underline{\gamma}} x^{\underline{\gamma}} = \sum_{\underline{\alpha} \in \mathcal{F}} (r_{\underline{\alpha}} + s_{\underline{\alpha}} + t_{\underline{\alpha}}) x^{\underline{\alpha}} \\ &= \sum_{\underline{\alpha} \in \mathcal{F}} r_{\underline{\alpha}} x^{\underline{\alpha}} + \sum_{\underline{\beta} \in \mathcal{F}} (s_{\underline{\beta}} + t_{\underline{\beta}}) x^{\underline{\beta}} = f + (g+h)\end{aligned}$$

da cui la somma è associativa. Poiché $(R, +)$ è abeliano, $r_{\underline{\alpha}} + s_{\underline{\alpha}} = s_{\underline{\alpha}} + r_{\underline{\alpha}}$, quindi

$$f + g = \sum_{\underline{\alpha} \in \mathcal{F}} (r_{\underline{\alpha}} + s_{\underline{\alpha}}) x^{\underline{\alpha}} = \sum_{\underline{\alpha} \in \mathcal{F}} (s_{\underline{\alpha}} + r_{\underline{\alpha}}) x^{\underline{\alpha}} = g + f$$

da cui anche $(R[x_1, \dots, x_n], +)$ è un gruppo abeliano con elemento neutro $\sum_{\underline{\alpha} \in \mathcal{F}} 0_{\underline{\alpha}} x^{\underline{\alpha}} = 0_R$, dove $0_{\underline{\alpha}} = 0_R \ \forall \underline{\alpha} \in \mathcal{F}$ è la funzione nulla, e opposto $-f = \sum_{\underline{\alpha} \in \mathcal{F}} -r_{\underline{\alpha}} x^{\underline{\alpha}}$. Inoltre,

$$\begin{aligned}(f \cdot g) \cdot h &= \sum_{\underline{\delta} \in \mathcal{F}} \sum_{\underline{\alpha} + \underline{\beta} = \underline{\delta}} r_{\underline{\alpha}} s_{\underline{\beta}} \, x^{\underline{\delta}} \cdot \sum_{\underline{\gamma} \in \mathcal{F}} t_{\underline{\gamma}} x^{\underline{\gamma}} = \sum_{\underline{\varepsilon} \in \mathcal{F}} \sum_{\underline{\delta} + \underline{\gamma} = \underline{\varepsilon}} \sum_{\underline{\alpha} + \underline{\beta} = \underline{\delta}} r_{\underline{\alpha}} s_{\underline{\beta}} t_{\underline{\gamma}} \, x^{\underline{\varepsilon}} \\ &= \sum_{\underline{\varepsilon} \in \mathcal{F}} \sum_{\underline{\alpha} + \underline{\beta} + \underline{\gamma} = \underline{\varepsilon}} r_{\underline{\alpha}} s_{\underline{\beta}} t_{\underline{\gamma}} \, x^{\underline{\varepsilon}} = \sum_{\underline{\alpha} \in \mathcal{F}} r_{\underline{\alpha}} x^{\underline{\alpha}} \cdot \sum_{\underline{\delta} \in \mathcal{F}} \sum_{\underline{\beta} + \underline{\gamma} = \underline{\delta}} s_{\underline{\beta}} t_{\underline{\gamma}} \, x^{\underline{\delta}} = f \cdot (g \cdot h)\end{aligned}$$

da cui il prodotto è associativo. Essendo R commutativo, $r_{\underline{\alpha}} s_{\underline{\beta}} = s_{\underline{\beta}} r_{\underline{\alpha}}$ e quindi

$$f \cdot g = \sum_{\underline{\delta} \in \mathcal{F}} \sum_{\underline{\alpha} + \underline{\beta} = \underline{\delta}} r_{\underline{\alpha}} s_{\underline{\beta}} \, x^{\underline{\delta}} = \sum_{\underline{\delta} \in \mathcal{F}} \sum_{\underline{\beta} + \underline{\alpha} = \underline{\delta}} s_{\underline{\beta}} r_{\underline{\alpha}} \, x^{\underline{\delta}} = g \cdot f$$

da cui anche $R[x_1, \dots, x_n]$ è commutativo con unità $\sum_{\underline{\alpha} \in \mathcal{F}} 1_{\underline{\alpha}} x^{\underline{\alpha}} = 1_R$ dove $1_{\underline{\alpha}}$ è la funzione che vale 1_R per $\underline{\alpha} = \underline{0}$ e 0_R per ogni altro $\underline{\alpha} \in \mathcal{F}$.[17] Infine,

$$\begin{aligned}(f+g) \cdot h &= \sum_{\underline{\alpha} \in \mathcal{F}} (r_{\underline{\alpha}} + s_{\underline{\alpha}}) x^{\underline{\alpha}} \cdot \sum_{\underline{\gamma} \in \mathcal{F}} t_{\underline{\gamma}} x^{\underline{\gamma}} = \sum_{\underline{\delta} \in \mathcal{F}} \sum_{\underline{\alpha} + \underline{\gamma} = \underline{\delta}} (r_{\underline{\alpha}} + s_{\underline{\alpha}}) t_{\underline{\gamma}} \, x^{\underline{\delta}} \\ &= \sum_{\underline{\delta} \in \mathcal{F}} \sum_{\underline{\alpha} + \underline{\gamma} = \underline{\delta}} r_{\underline{\alpha}} t_{\underline{\gamma}} \, x^{\underline{\delta}} + \sum_{\underline{\delta} \in \mathcal{F}} \sum_{\underline{\alpha} + \underline{\gamma} = \underline{\delta}} s_{\underline{\alpha}} t_{\underline{\gamma}} \, x^{\underline{\delta}} = f \cdot h + g \cdot h\end{aligned}$$

dunque vale la proprietà distributiva e $(R[x_1, \dots, x_n], +, \cdot)$ è un anello commutativo. ∎

[17] Chiaramente si intende che $x^{\underline{0}} = x_1^0 \cdot \dots \cdot x_n^0 = 1_R \cdot \dots \cdot 1_R = 1_R$.

Anche per gli anelli di polinomi in n variabili vale il corrispondente della *Proprietà universale*, che per semplicità ci limiteremo a dimostrare nel caso in cui $R \subseteq S$.

Teorema 1.2.11: Proprietà universale

Sia R un anello commutativo. Allora, per ogni anello commutativo $S \supseteq R$ e per ogni $\underline{s} = (s_1, \dots, s_n) \in S^n$ esiste un unico omomorfismo di anelli $\phi_{\underline{s}} \colon R[x_1, \dots, x_n] \to S$ tale che $\phi_{\underline{s}}(x_i) = s_i$ per ogni $i = 1, \dots, n$ e $\phi_{\underline{s}}|_R = \mathrm{id}_R$.

Dimostrazione. Siano $f = \sum_{\underline{\alpha} \in \mathcal{F}} r_{\underline{\alpha}} x^{\underline{\alpha}}$ e $g = \sum_{\underline{\beta} \in \mathcal{F}} t_{\underline{\beta}} x^{\underline{\beta}}$ due elementi di $R[x_1, \dots, x_n]$. Per ogni monomio $x^{\underline{\alpha}} \in M$ definiamo $\phi_{\underline{s}}(x^{\underline{\alpha}}) = \prod_{i=1}^{n} s_i^{\alpha_i}$, e sia quindi $\phi_{\underline{s}}(f) = \sum_{\underline{\alpha} \in \mathcal{F}} r_{\underline{\alpha}} \phi_{\underline{s}}(x^{\underline{\alpha}})$. Osserviamo innanzitutto che $\phi_{\underline{s}}(f)$ è ben definita. Infatti, $r_{\underline{\alpha}} \in R \subseteq S$ e $\phi_{\underline{s}}(f) \in S$ perché somma di prodotti di elementi dell'anello S, che è chiuso rispetto a somma e prodotto. Inoltre, $\phi_{\underline{s}}(x_i) = s_i$ e $\phi_{\underline{s}}(\rho) = \rho$ per ogni $\rho \in R$, quindi $\phi_{\underline{s}}$ soddisfa le condizioni richieste. Mostriamo ora che $\phi_{\underline{s}}$ preserva le operazioni. Infatti,

$$\phi_{\underline{s}}(f+g) = \sum_{\underline{\alpha} \in \mathcal{F}} (r_{\underline{\alpha}} + t_{\underline{\alpha}}) \phi_{\underline{s}}(x^{\underline{\alpha}}) = \sum_{\underline{\alpha} \in \mathcal{F}} r_{\underline{\alpha}} \phi_{\underline{s}}(x^{\underline{\alpha}}) + \sum_{\underline{\alpha} \in \mathcal{F}} t_{\underline{\alpha}} \phi_{\underline{s}}(x^{\underline{\alpha}}) = \phi_{\underline{s}}(f) + \phi_{\underline{s}}(g)$$

per la proprietà distributiva del prodotto rispetto alla somma, essendo S un anello, e

$$\phi_{\underline{s}}(f \cdot g) = \sum_{\underline{\gamma} \in \mathcal{F}} \sum_{\underline{\alpha} + \underline{\beta} = \underline{\gamma}} r_{\underline{\alpha}} t_{\underline{\beta}} \, \phi_{\underline{s}}(x^{\underline{\gamma}}) = \left(\sum_{\underline{\alpha} \in \mathcal{F}} r_{\underline{\alpha}} \phi_{\underline{s}}(x^{\underline{\alpha}}) \right) \cdot \left(\sum_{\underline{\beta} \in \mathcal{F}} t_{\underline{\beta}} \phi_{\underline{s}}(x^{\underline{\beta}}) \right) = \phi_{\underline{s}}(f) \cdot \phi_{\underline{s}}(g)$$

perché $\phi_{\underline{s}}(x^{\underline{\gamma}}) = \prod_{i=1}^{n} s_i^{\gamma_i} = \prod_{i=1}^{n} s_i^{\alpha_i + \beta_i} = \prod_{i=1}^{n} s_i^{\alpha_i} \cdot \prod_{i=1}^{n} s_i^{\beta_i} = \phi_{\underline{s}}(x^{\underline{\alpha}}) \cdot \phi_{\underline{s}}(x^{\underline{\beta}})$. Poiché $\phi_{\underline{s}}(0_R) = 0_S$ e $\phi_{\underline{s}}(1_R) = 1_S$, concludiamo che tale mappa $\phi_{\underline{s}}$ è effettivamente un omomorfismo di anelli. Mostriamo ora che $\phi_{\underline{s}}$ è unico. Sia $\psi \colon R[x_1, \dots, x_n] \to S$ un altro omomorfismo di anelli tale che $\psi(x_i) = s_i$ per ogni $i = 1, \dots, n$ e $\psi|_R = \mathrm{id}_R$. Allora, per ogni monomio $x^{\underline{\alpha}} \in M$ vale

$$\psi(x^{\underline{\alpha}}) = \psi\left(\prod_{i=1}^{n} x_i^{\alpha_i} \right) = \prod_{i=1}^{n} \psi\left(x_i^{\alpha_i}\right) = \prod_{i=1}^{n} \psi(x_i)^{\alpha_i} = \prod_{i=1}^{n} s_i^{\alpha_i} = \phi_{\underline{s}}(x^{\underline{\alpha}}).$$

Poiché ψ preserva le operazioni, per ogni $f = \sum_{\underline{\alpha} \in \mathcal{F}} r_{\underline{\alpha}} x^{\underline{\alpha}} \in R[x_1, \dots, x_n]$ si ha quindi che

$$\psi(f) = \psi\left(\sum_{\underline{\alpha} \in \mathcal{F}} r_{\underline{\alpha}} x^{\underline{\alpha}} \right) = \sum_{\underline{\alpha} \in \mathcal{F}} \psi(r_{\underline{\alpha}} x^{\underline{\alpha}}) = \sum_{\underline{\alpha} \in \mathcal{F}} \psi(r_{\underline{\alpha}}) \psi(x^{\underline{\alpha}}) = \sum_{\underline{\alpha} \in \mathcal{F}} r_{\underline{\alpha}} \phi_{\underline{s}}(x^{\underline{\alpha}}) = \phi_{\underline{s}}(f)$$

essendo $\psi(r_{\underline{\alpha}}) = r_{\underline{\alpha}}$ perché $r_{\underline{\alpha}} \in R$ e $\psi(x^{\underline{\alpha}}) = \phi_{\underline{s}}(x^{\underline{\alpha}})$ per quanto provato sopra. Dunque, ψ coincide con $\phi_{\underline{s}}$ per ogni polinomio $f \in R[x_1, \dots, x_n]$, da cui $\phi_{\underline{s}}$ è unico. ■

1.3 Anello dei polinomi in più variabili

In questo paragrafo vogliamo generalizzare il concetto di anello dei polinomi ad un numero qualsiasi di variabili "x" appartenenti ad un insieme $\mathcal{X}$ anche infinito. l'anello dei polinomi nel caso in cui le variabili siano degli elementi $x \in \mathcal{X}$. Per fare ciò sono necessarie delle definizioni preliminari degli oggetti che verranno coinvolti.

Definizione 1.3.1: supporto di una funzione

Sia $f : X \longrightarrow Y$ una funzione tra due insiemi dotati di operazioni binarie ed elemento neutro. Si dice *supporto di f* il seguente insieme:

$$supp(f) := \{x \in X \mid f(x) \neq 0_Y\}$$

In particolare, in questa sezione useremo un insieme di funzioni a supporto finito:

$$\mathcal{F}^{\times}(\mathcal{X}, \mathbb{N}_0) := \{\alpha : \mathcal{X} \to \mathbb{N}_0 : |supp(\alpha)| < \infty\}$$

In questo modo $\alpha(x) \neq 0$ solo in un numero finito di $x \in \mathcal{X}$. Questo particolare insieme, d'ora in poi verrà denotato semplicemente come $\mathcal{F}^{\times}$ per evitare di appesantire la notazione. Inoltre su $\mathcal{F}^{\times}$ è possibile definire una struttura algebrica di monoide abeliano tramite la somma puntuale:

$$(\alpha + \beta)(x) = \alpha(x) + \beta(x) \qquad \forall \alpha, \beta \in \mathcal{F}^{\times}$$

$$\textit{con elemento neutro } 0_{\mathcal{F}^{\times}}(x) = 0 \qquad \forall x \in \mathcal{X}$$

La somma definita sopra è ben posta, infatti, se $\alpha, \beta \in \mathcal{F}^{\times} \Rightarrow | \ supp(\alpha) \ |, | \ supp(\beta) \ | < \infty$. Quindi se $x \in supp(\alpha + \beta) \Rightarrow \alpha(x) + \beta(x) \neq 0 \Rightarrow \alpha(x) \neq 0 \vee \beta(x) \neq 0 \Rightarrow x \in supp(\alpha) \cup supp(\beta)$ e quindi, $supp(\alpha + \beta) \subseteq supp(\alpha) \cup supp(\beta)$ che passando alle cardinalità diventa:

$$| \ supp(\alpha+\beta) \ | \leq | \ supp(\alpha) \cup supp(\beta) \ | \leq | \ supp(\alpha) \ | + | \ supp(\beta) \ | < \infty \quad \textit{ovvero} \quad \alpha+\beta \in \mathcal{F}^{\times}$$

Fatte queste considerazioni è possibile definire formalmente *l'insieme dei monomi monici nelle variabili* $x \in \mathcal{X}$:

Definizione 1.3.2: monomi monici

Sia R un anello commutativo e sia $\mathcal{X}$ un insieme.
Per ogni $\alpha \in \mathcal{F}^{\times}$ è definito monomio monico X^{α} la seguente produttoria:

$$X^{\alpha} := \prod_{x \in \mathcal{X}} x^{\alpha(x)} \qquad \textit{con la convenzione} \qquad x^0 = 1_R \ \forall x \in \mathcal{X}$$

L'insieme di tutti i monomi monici su $\mathcal{X}$ è: $\{X^{\alpha} \mid \alpha \in \mathcal{F}^{\times}\} =: M$

E' importante osservare che $\mathcal{X}$ può essere anche un insieme infinito, ma dato che le $\alpha \in \mathcal{F}^{\times}$ si ha che ogni monomio sarà costituito solo da un numero finito di variabili (le altre sono tutte 1_R e pertanto trascurabili).

Esempio 1.3.3

Sia per esempio $R = \mathbb{Z},\ \mathcal{X} = \{x_1, x_2, x_3, x_4\},\ \alpha(x_i) = i\ \forall\ i \in \{1,2,3\}$ *e* $\alpha(x_4) = 0$.
Allora si ha che:

$$X^\alpha := \prod_{x \in \mathcal{X}} x^{\alpha(x)} = x_1 \cdot x_2^2 \cdot x_3^3 \cdot 1 = x_1 x_2^2 x_3^3$$

Sia $\mathcal{F}(\mathcal{F}^\times, R) := \{f : \mathcal{F}^\times \to R : |supp(f)| < \infty\}$, cioè l'insieme delle funzioni f che ad ogni elemento di $\mathcal{F}^\times$ associano un elemento di R e che non valgono 0_R solo per un numero finito di elementi di $\mathcal{F}^\times$.
Sia $r_\_ \in \mathcal{F}(\mathcal{F}^\times, R)$ la funzione che per ogni $\alpha \in \mathcal{F}^\times$ associa l'elemento $r_\alpha \in R$. Osserviamo che ora possiamo definire un qualsiasi polinomio "f" nelle variabili $x \in \mathcal{X}$ come **combinazione lineare di monomi a coefficienti in** R:

$$f = \sum_{\alpha \in \mathcal{F}^\times} r_\alpha X^\alpha$$

e dato che $r_\_ \in \mathcal{F}(\mathcal{F}^\times, R)$ ho che il polinomio f sarà composto da una somma di finita di termini non nulli.

Siamo quindi pronti a definire l'anello dei polinomi nelle variabili $x \in \mathcal{X}$.

Definizione 1.3.4: Anello dei polinomi nelle variabili $x \in \mathcal{X}$

Sia R un anello commutativo.
Si definisce *anello dei polinomi nelle variabili* $x \in \mathcal{X}$ l'insieme:

$$R[\mathcal{X}] := \{f = \sum_{\alpha \in \mathcal{F}^\times} r_\alpha X^\alpha \mid r_\_ \in \mathcal{F}(\mathcal{F}^\times, R)\}$$

con le seguenti operazioni di somma e di prodotto. Dati $f, g \in R[\mathcal{X}]$:

$$f(X) = \sum_{\alpha \in \mathcal{F}^\times} r_\alpha X^\alpha, \quad g(X) = \sum_{\beta \in \mathcal{F}^\times} s_\beta X^\beta$$

$$somma: \quad + : R[\mathcal{X}] \times R[\mathcal{X}] \longrightarrow R[\mathcal{X}] \quad f(X) + g(X) = \sum_{\alpha \in \mathcal{F}^\times} (r_\alpha + s_\alpha) X^\alpha$$

$$prodotto: \quad \cdot : R[\mathcal{X}] \times R[\mathcal{X}] \longrightarrow R[\mathcal{X}] \quad f(X) \cdot g(X) = \sum_{\gamma \in \mathcal{F}^\times} t_\gamma X^\gamma$$

dove abbiamo posto $\gamma = \alpha + \beta$ e $t_\gamma = \sum_{\alpha+\beta=\gamma} r_\alpha s_\beta$. Inoltre,

$$elemento\ neutro: \quad 0_R = \sum_{\alpha \in \mathcal{F}^\times} 0_\alpha X^\alpha, \quad unita'\ moltiplicativa: \quad 1_R = X^0$$

Anche per gli anelli di polinomi in più variabili vale la cosiddetta *Proprietà Universale*.

Proposizione 1.3.5: Proprietà Universale

Sia X un insieme e sia R un anello commutativo.
Allora, per ogni anello commutativo $S \supseteq R$ e per ogni mappa $\varphi\colon \mathcal{X} \to S$ esiste un unico omomorfismo di anelli $\phi\colon R[\mathcal{X}] \to S$ tale che $\phi(X^{\delta_x}) = \varphi(x)\ \forall x \in \mathcal{X}\ e\ \phi|_{|_R} = id_R$, dove:

$$\delta_x\colon \mathcal{X} \to \mathbb{N}, \delta_x(y) = \begin{cases} 1 & \text{se } y = x \\ 0 & \text{se } y \neq x \end{cases}$$

Dimostrazione. Siano $f = \sum_{\alpha \in \mathcal{F}^\times} r_\alpha X^\alpha$, e $g = \sum_{\beta \in \mathcal{F}^\times} s_\beta X^\beta$, due elementi di $R[\mathcal{X}]$. Per ogni monomio $X^\alpha \in M$, sia $\phi(X^\alpha) = \prod_{x \in X} \varphi(x)^{\alpha(x)}$, e sia quindi $\phi(f) = \sum_{\alpha \in \mathcal{F}^\times} r_\alpha \phi(X^\alpha)$. Poiché $r_\alpha \in R \subseteq S$ per ipotesi e $\phi(f) \in S$ perché somma di prodotti di elementi di S (che in quanto anello è chiuso rispetto a somma e prodotto), ϕ è ben definita. Inoltre, $\phi(X^{\delta_x}) = \varphi(x)$ e $\phi(\rho) = \rho$ per ogni $\rho \in R$, quindi ϕ soddisfa le condizioni richieste. [18]
Mostriamo ora che è un omomorfismo di anelli. Infatti,

$$\phi(f+g) = \sum_{\alpha \in \mathcal{F}^\times} (r_\alpha + s_\alpha)\phi(X^\alpha) = \sum_{\alpha \in \mathcal{F}^\times} r_\alpha \phi(X^\alpha) + \sum_{\alpha \in \mathcal{F}^\times} s_\alpha \phi(X^\alpha) = \phi(f) + \phi(g)$$

per la proprietà distributiva del prodotto rispetto alla somma, essendo S un anello, e

$$\phi(f \cdot g) = \sum_{\gamma \in \mathcal{F}^\times} \sum_{\alpha+\beta=\gamma} r_\alpha s_\beta \phi(X^\gamma) = \left(\sum_{\alpha \in \mathcal{F}^\times} r_\alpha \phi(X^\alpha)\right) \cdot \left(\sum_{\beta \in \mathcal{F}^\times} s_\beta \phi(X^\beta)\right) = \phi(f) \cdot \phi(g)$$

perché $\phi(X^\gamma) = \prod_{x \in X} \varphi(x)^{\gamma(x)} = \prod_{x \in X} \varphi(x)^{\alpha(x)} \cdot \prod_{x \in X} \varphi(x)^{\beta(x)} = \phi(X^\alpha) \cdot \phi(X^\beta)$. Poiché $\phi(0_R) = 0_S$ e $\phi(1_R) = 1_S$, concludiamo che ϕ è un omomorfismo di anelli.
Mostriamo ora che ϕ è unico. Sia $\psi\colon R[\mathcal{X}] \to S$ un omomorfismo di anelli tale che $\psi(X^{\delta_x}) = \varphi(x)$ e $\psi_{|_R} = \mathrm{id}_R$. Allora, per ogni monomio $X^\alpha \in M$ vale

$$\psi(X^\alpha) = \psi\left(\prod_{x \in X} x^{\alpha(x)}\right) = \prod_{x \in X} \psi\left(x^{\alpha(x)}\right) = \prod_{x \in X} \psi(X^{\delta_x})^{\alpha(x)} = \prod_{x \in X} \varphi(x)^{\alpha(x)} = \phi(X^\alpha)$$

.
Poiché ψ è un omomorfismo, per ogni $f = \sum_{\alpha \in \mathcal{F}^\times} r_\alpha X^\alpha \in R[\mathcal{X}]$ si ha che

$$\psi(f) = \psi\left(\sum_{\alpha \in \mathcal{F}^\times} r_\alpha X^\alpha\right) = \sum_{\alpha \in \mathcal{F}^\times} \psi(r_\alpha X^\alpha) = \sum_{\alpha \in \mathcal{F}^\times} \psi(r_\alpha)\psi(X^\alpha) = \sum_{\alpha \in \mathcal{F}^\times} r_\alpha \phi(X^\alpha) = \phi(f)$$

essendo $\psi(r_\alpha) = r_\alpha$ perché $r_\alpha \in R$ e $\psi(X^\alpha) = \phi(X^\alpha)$ per quanto appena mostrato. Dunque, ψ coincide con ϕ, che risulta quindi essere unico. ■

[18] δ_x è la funzione tale che per ogni $x \in X$ si abbia $X^{\delta_x} = x$. Infatti, $X^{\delta_x} = \prod_{y \in X} y^{\delta_x(y)} = x^{\delta_x(x)} = x^1 = x$ perché tutti gli altri termini del prodotto hanno esponente 0, essendo per definizione $\delta_x(y) = 0$ se $y \neq x$.

Sia $R[x]$ l'anello dei polinomi a coefficienti in R nella variabile x. Possiamo considerare $R[x]$ stesso come anello dei coefficienti per l'anello dei polinomi nella variabile y, cioè

$$(R[x])[y] = \left\{ \sum_{i=0}^{n} f_i\, y^i : f_i \in R[x],\, n \in \mathbb{N} \right\}.$$

Poiché ogni polinomio di $(R[x])[y]$ può essere visto come un polinomio in due variabili di $R[x,y]$ e ogni polinomio di $R[x,y]$ può essere pensato come un polinomio di $(R[x])[y]$ raccogliendo i termini dello stesso grado in y, questo suggerisce che $(R[x])[y] \simeq R[x,y]$.

Esempio 1.3.6

Sia $f(y) = (x^2+1)y^2 + (2x)y + 3 \in (\mathbb{Z}[x])[y]$. Allora, possiamo vedere $f(y)$ come un polinomio in due variabili $g(x,y) = x^2y^2 + y^2 + 2xy + 3 \in \mathbb{Z}[x,y]$. Viceversa, preso $p(x,y) = xy^2 + 2xy + 3y + 4 \in \mathbb{Z}[x,y]$, raccogliendo i termini dello stesso grado in y possiamo pensare $p(x,y)$ come un polinomio $q(y) = (x)y^2 + (2x+3)y + 4 \in (\mathbb{Z}[x])[y]$.

In generale, se X e Y sono insiemi non vuoti e $(R[X])[Y]$ è l'anello dei polinomi a coefficienti in $R[X]$ e a variabili in Y, detta $X \sqcup Y$ l'unione disgiunta,[19] vale il teorema seguente.

Teorema 1.3.7

Sia R un anello commutativo e siano X e Y non vuoti. Allora, $R[X \sqcup Y] \simeq (R[X])[Y]$.

Dimostrazione. Sia S un anello commutativo tale che $R \subseteq R[X] \subseteq S$ e sia $\varphi_X \colon X \to S$ definita come $\varphi_X(x) = X^{\underline{\delta}_x}$. Presa una qualunque funzione $\varphi_Y \colon Y \to S$, sia $\widetilde{\varphi} \colon X \sqcup Y \to S$ l'unica mappa tale che $\widetilde{\varphi}_{|_X} = \varphi_X$ e $\widetilde{\varphi}_{|_Y} = \varphi_Y$. Allora, per il *Teorema 1.3.1* esiste un unico omomorfismo $\widetilde{\phi} \colon R[X \sqcup Y] \to S$ tale che $\widetilde{\phi}(Z^{\underline{\delta}_z}) = \widetilde{\varphi}(z)$ per ogni $z \in X \sqcup Y$ e $\widetilde{\phi}_{|_R} = \mathrm{id}_R$. Per ogni $\underline{\alpha} \in \mathcal{F}^{\times}(X, \mathbb{N})$, sia $\widetilde{\underline{\alpha}} \in \mathcal{F}^{\times}(X \sqcup Y, \mathbb{N})$ l'unica funzione tale che $\widetilde{\underline{\alpha}}_{|_X} = \underline{\alpha}$ e $\widetilde{\underline{\alpha}}_{|_Y} = \underline{0}$. Allora, possiamo pensare ogni monomio $X^{\underline{\alpha}}$ di $R[X]$ come monomio $Z^{\widetilde{\underline{\alpha}}}$ di $R[X \sqcup Y]$, da cui

$$\begin{aligned}\widetilde{\phi}(Z^{\widetilde{\underline{\alpha}}}) &= \widetilde{\phi}\left(\prod_{z \in X \sqcup Y} z^{\widetilde{\underline{\alpha}}(z)} \right) = \prod_{z \in X \sqcup Y} \widetilde{\phi}\left(z^{\widetilde{\underline{\alpha}}(z)} \right) = \prod_{z \in X \sqcup Y} \widetilde{\phi}\left(Z^{\underline{\delta}_z} \right)^{\widetilde{\underline{\alpha}}(z)} = \prod_{z \in X \sqcup Y} \widetilde{\varphi}(z)^{\widetilde{\underline{\alpha}}(z)} \\ &= \prod_{x \in X} \varphi_X(x)^{\underline{\alpha}(x)} \cdot \prod_{y \in Y} \varphi_Y(y)^{\underline{0}} = \prod_{x \in X} (X^{\underline{\delta}_x})^{\underline{\alpha}(x)} \cdot 1_R = X^{\underline{\alpha}}\end{aligned}$$

per come abbiamo definito $\widetilde{\varphi}$ e $\widetilde{\underline{\alpha}}$ ed usando il fatto che $\widetilde{\phi}$ è un omomorfismo. Quindi, preso $f = \sum_{\underline{\alpha} \in \mathcal{F}^{\times}} r_{\underline{\alpha}} X^{\underline{\alpha}} \in R[X]$, pensando f come elemento $\widetilde{f} = \sum_{\widetilde{\underline{\alpha}} \in \mathcal{F}^{\times}} r_{\widetilde{\underline{\alpha}}} Z^{\widetilde{\underline{\alpha}}} \in R[X \sqcup Y]$ si ha che

$$\widetilde{\phi}(\widetilde{f}\,) = \sum_{\widetilde{\underline{\alpha}} \in \mathcal{F}^{\times}} \widetilde{\phi}(r_{\widetilde{\underline{\alpha}}}) \widetilde{\phi}(Z^{\widetilde{\underline{\alpha}}}) = \sum_{\widetilde{\underline{\alpha}} \in \mathcal{F}^{\times}} r_{\widetilde{\underline{\alpha}}}\, \widetilde{\phi}(Z^{\widetilde{\underline{\alpha}}}) = \sum_{\underline{\alpha} \in \mathcal{F}^{\times}} r_{\underline{\alpha}} X^{\underline{\alpha}} = f$$

perché $\widetilde{\phi}(r_{\widetilde{\underline{\alpha}}}) = r_{\widetilde{\underline{\alpha}}}$ essendo $\widetilde{\phi}_{|_R} = \mathrm{id}_R$, da cui $\widetilde{\phi}_{|_{R[X]}} = \mathrm{id}_{R[X]}$. Inoltre, per ogni $y \in Y$ si ha che $\widetilde{\phi}(Z^{\underline{\delta}_y}) = \widetilde{\varphi}(y) = \varphi_Y(y)$. Poiché $R[X \sqcup Y]$ è un anello commutativo contenente $R[X]$ che

[19] Ricordiamo che l'unione disgiunta di una famiglia di insiemi $\{A_i\}_{i \in I}$ è l'insieme $\bigsqcup_{i \in I} A_i = \bigcup_{i \in I} (A \times \{i\})$. Ad esempio, presi $A_0 = \{3,4,5\}$ e $A_1 = \{5,6\}$, si ha che $A_0 \sqcup A_1 = \{(3,0),(4,0),(5,0),(5,1),(6,1)\}$.

soddisfa la proprietà universale di $(R[X])[Y]$,[20] per la generalizzazione del *Teorema REF DA SISTEMARE* possiamo effettivamente concludere che $R[X \sqcup Y] \simeq (R[X])[Y]$. ■

Nel caso in cui l'insieme delle variabili sia finito, vale il corollario seguente.

Corollario 1.3.8

Sia n un intero positivo. Allora, $R[x_1, \dots, x_n] \simeq (\cdots((R[x_1])[x_2])\cdots)[x_n]$.

Dimostrazione. Procediamo per induzione sul numero n di variabili. Chiaramente, se $n = 1$ allora $R[x_1] \simeq R[x_1]$. Supponiamo quindi che la tesi sia vera per un certo intero $n \geq 1$. Detti $X = \{x_1, \dots, x_n\}$ e $Y = \{x_{n+1}\}$, per il *Teorema 1.3.2 ref da sistemare* si ha che $R[X \sqcup Y] \simeq (R[X])[Y]$ da cui $R[x_1, \dots, x_{n+1}] \simeq (R[x_1, \dots, x_n])[x_{n+1}] \simeq ((\cdots((R[x_1])[x_2])\cdots)[x_n])[x_{n+1}]$. ■

Possiamo quindi estendere agli anelli di polinomi in più variabili anche la *Proposizione 1.1.1.* Per fare ciò, osserviamo innanzitutto che ogni polinomio di $R[X]$ è la somma di un numero finito di monomi non nulli, ognuno con un numero finito di variabili. Dunque, ogni polinomio di $R[X]$ può essere pensato come un polinomio in un numero finito di variabili, o meglio, per ogni $f \in R[X]$ esiste un sottoinsieme delle variabili $X_f \subseteq X$ finito tale che $f \in R[X_f]$.[21]

Proposizione 1.3.9

Sia X un insieme non vuoto e sia R un dominio di integrità. Allora, anche l'anello dei polinomi $R[X]$ è un dominio di integrità.

Dimostrazione. Siano $f, g \in R[X]$ e siano $X_f, X_g \subseteq X$ finiti tali che $f \in R[X_f]$ e $g \in R[X_g]$. Osserviamo innanzitutto che $X_f \cup X_g$ è un sottoinsieme finito di X e $f \cdot g \in R[X_f \cup X_g]$. Dunque, detto $X_f \cup X_g = \{x_1, \dots, x_n\}$, per dimostrare che $R[X]$ è un dominio di integrità è sufficiente provare che $R[x_1, \dots, x_n]$ è un dominio di integrità.[22] Per fare ciò, procediamo per induzione sul numero di variabili. Se $n = 1$, per la *Proposizione 1.1.1 ref da sistemare* sappiamo che $R[y_1]$ è un dominio di integrità. Supponiamo quindi che la tesi valga per un certo intero $n \geq 1$. Allora, per il *Corollario 1.3.3 ref da sistemare* si ha che $R[y_1, \dots, y_{n+1}] \simeq (R[y_1, \dots, y_n])[y_{n+1}]$, ed essendo $R[y_1, \dots, y_n]$ un dominio di integrità per ipotesi induttiva, per la *Proposizione 1.1.1 ref da sistemare* anche $(R[y_1, \dots, y_n])[y_{n+1}]$ è un dominio di integrità, da cui lo è pure $R[y_1, \dots, y_{n+1}]$. Dunque, $R[Y]$ è un dominio di integrità per ogni insieme finito Y, ed in particolare lo è per $Y = X_f \cup X_g$. Per l'arbitrarietà di $f, g \in R[X]$, possiamo concludere che $R[X]$ è un dominio di integrità. ■

[20] Infatti, abbiamo appena mostrato che per ogni anello $S \supseteq R[X]$ e per ogni mappa $\varphi_Y \colon Y \to S$, esiste un unico omomorfismo $\widetilde{\phi} \colon R[X \sqcup Y] \to S$ tale che $\widetilde{\phi}(Z^{\underline{\delta}_y}) = \varphi_Y(y)$ per ogni $y \in Y$ e $\widetilde{\phi}_{|_{R[X]}} = \mathrm{id}_{R[X]}$.

[21] Più formalmente, preso $f = \sum_{\underline{\alpha} \in \mathcal{F}^\times} r_{\underline{\alpha}} X^{\underline{\alpha}} \in R[X]$ sappiamo che $\Omega_f = \mathrm{supp}(r\_) \subseteq \mathcal{F}^\times$ è finito, quindi esiste solo un numero finito di funzioni $\underline{\alpha} \in \mathcal{F}^\times$ per cui il monomio $X^{\underline{\alpha}}$ ha un coefficiente $r_{\underline{\alpha}}$ non nullo. Poiché ogni $\underline{\alpha} \in \mathcal{F}^\times$ ha supporto finito, $X_f = \bigcup_{\underline{\alpha} \in \Omega_f} \mathrm{supp}(\underline{\alpha})$ è finito in quanto unione finita di insiemi finiti.

[22] Se il polinomio $f \cdot g$ si annulla in $R[X]$, allora si annulla anche pensato come polinomio di $R[X_f \cup X_g]$. Dunque, se $R[X_f \cup X_g]$ è un dominio di integrità per ogni $f, g \in R[X]$, allora anche $R[X]$ deve essere un dominio di integrità. Infatti, se esistessero $f, g \in R[X]$ divisori dello zero, per quanto appena detto essi sarebbero divisori dello zero anche in $R[X_f \cup X_g]$, il che contraddice la definizione di dominio di integrità.

Concludiamo con un'osservazione che acquisirà importanza quando passeremo allo studio dell'estensione di campi. Preso un anello commutativo R e un qualunque oggetto $x \notin R$, l'anello dei polinomi $R[x]$ è il più piccolo anello contenente R e x. Infatti, se S è un anello contenente R e x, per la chiusura di S rispetto a somma e prodotto esso conterrà tutte le potenze non negative $\{x^0, x^1, x^2, ...\}$ di x e tutte le combinazioni lineari tra potenze di x ed elementi di R, cioè tutti gli elementi della forma $a_n x^n + ... + a_1 x + a_0$ con $a_0, ..., a_n \in R$. In generale, se X è un insieme non vuoto, possiamo quindi vedere $R[X]$ come la più piccola "estensione" di R contenente X, cioè come il più piccolo anello contenente sia R che X.

1.4 Polinomi di Laurent e serie formali

Vogliamo ora introdurre alcune generalizzazioni del concetto di anello di polinomi molto usate nell'analisi reale e complessa, quali i polinomi di Laurent e le serie di potenze.

Definizione 1.4.1: Polinomi di Laurent e operazioni

Sia R un anello commutativo e sia $R[x, x^{-1}] = \left\{ \sum_{i=-p}^{n} a_i x^i : a_i \in R,\ n, p \in \mathbb{N} \right\}$. Presi due elementi $f = \sum_{i=-p}^{m} a_i x^i$ e $g = \sum_{j=-q}^{n} b_j x^j$ di $R[x, x^{-1}]$, definiamo le operazioni di *somma*

$$f + g = \sum_{i=-r}^{s} (a_i + b_i) x^i$$

dove $s = \max\{m, n\}$, $r = \max\{p, q\}$ e $a_i = b_j = 0$ per $i \notin [-p, m]$ e $j \notin [-q, n]$, e *prodotto*

$$f \cdot g = \sum_{k=-p-q}^{m+n} c_k x^k$$

dove abbiamo posto $c_k = \sum_{i+j=k} a_i b_j$.

Osservazione. Possiamo pensare $R[x, x^{-1}]$ come l'anello dei polinomi $R[x]$ dove però l'esponente della variabile x può essere anche un intero negativo.

Lemma 1.4.2

$R[x, x^{-1}]$ e' un anello commutativo.

Dimostrazione. Da fare. ■

Come per i poliniomi in una variabile, andiamo a definire il grado dei polinomi di Laurent.

Definizione 1.4.3: Grado di un polinomio di Laurent

Siano R un anello commutativo unitario, $R[x, x^{-1}]$ come descritto in precedenza e $f = \sum_{i \geq -q}^{n} a^i x^i \in R[x, x^{-1}]$. Definiamo allora la funzione *grado*

$$\omega : R[x, x^{-1}] \to \mathbb{Z} \cup \{\infty\},\ \omega(f) = \begin{cases} \min\{z \in \mathbb{Z} \mid a_n \neq 0\}, & f \not\equiv 0_R \\ \infty, & f \equiv 0_R \end{cases}$$

Dove la quantita' $\omega(f)$ e' chiamata *grado del polinomio di Laurent f.*

Introduciamo ora un fatto abbastanza intuitivo su questa struttura algebrica:

Lemma 1.4.4

Sia R un anello commutativo unitario. Allora $R[x] \leq R[x, x^{-1}]$, cioe' $R[x]$ e' un sottoanello di $R[x, x^{-1}]$. Inoltre, per ogni $f \in R[x, x^{-1}], f \not\equiv 0_R$ vale che

$$x^{-\omega(f)} \cdot f \in R[x]$$

Dimostrazione. Da fare. ■

Definiamo ora la seconda struttura algebrica di cui vogliamo parlare.

Definizione 1.4.5: Serie di potenze formali, operazioni e grado

Sia $\mathbb{F}$ un campo. Definiamo l'insieme delle *serie di potenze formali* come

$$\mathbb{F}[\![x]\!] = \left\{ \sum_{i \in \mathbb{N}_0} a_i x^i \mid a_i \in \mathbb{F} \right\}$$

Siano $f = \sum_{i \in \mathbb{N}_0} a_i x^i,\ g = \sum_{i \in N_0} b_i x^i$ e definiamo l'operazione di *somma* e *prodotto*

$$+ \ : \mathbb{F}[\![x]\!] \times \mathbb{F}[\![x]\!] \to \mathbb{F}[\![x]\!],\ f + g = \sum_{i \in \mathbb{N}_0} (a_i + b_i) x^i$$
$$\cdot \ : \mathbb{F}[\![x]\!] \times \mathbb{F}[\![x]\!] \to \mathbb{F}[\![x]\!],\ f \cdot g = \sum_{k \in \mathbb{N}_0} \Big(\sum_{\substack{i,j \in \mathbb{N}_0 \\ i+j=k}} (a_i \cdot b_j) x^k \Big)$$

dove tale prodotto viene spesso denotato piu' brevemente con $\sum_{k \in \mathbb{N}_0} c_k x^k$.
Su $\mathbb{F}[\![x]\!]$ e' definita ω, ovvero la funzione *grado*, esattamente come nella *Definizione 1.4.3* dove pero' ovviamente i nostri indici appartengono a $\mathbb{N}_0$.

Lemma 1.4.6

$\mathbb{F}[\![x]\!]$ e' un dominio di integrità.

Dimostrazione. Da fare. ■

Elenchiamo ora alcuni fatti su tale struttura algebrica, uno dei quali richiede conoscenze su anelli locali e massimali, che vedremo nei prossimi sottocapitoli.

Lemma 1.4.7

(i) La funzione grado ω soddisfa che, per ogni $f, g \in \mathbb{F}[\![x]\!], \omega(f \cdot g) = \omega(f) + \omega(g)$.
(ii) Sia $f = \sum_{i \in \mathbb{N}_0} a_i x^i \in \mathbb{F}[\![x]\!]$. La valutazione in 0, ovvero

$$\phi_0 : \mathbb{F}[\![x]\!] \to \mathbb{F},\ \phi_0(f) = a_0$$

e' l'unico omomorfismo di anelli da $\mathbb{F}[\![x]\!]$ a $\mathbb{F}$.

(*iii*) $\mathbb{F}[\![x]\!]^\times = \{f \in \mathbb{F}[\![x]\!] \mid \phi_0(f) \neq 0\} = \{f \in \mathbb{F}[\![x]\!] \mid \omega(f) = 0\}$.

Dimostrazione. i e iii da fare. ii e' per *Proposizione 1.7.15* ■

Consideriamo un anello che unisce la nozione di polinomio di Laurent con quella di serie formale.

Definizione 1.4.8: Serie di potenze di Laurent

Sia $\mathbb{F}$ un campo. Definiamo l'insieme delle *serie di potenze di Laurent* come

$$\mathbb{F}[\![x, x^{-1}]\!] = \left\{ \sum_{i \geq q} a_i x^i \mid q \in \mathbb{Z}, a_i \in \mathbb{F} \right\},$$

Dove definiamo le operazioni di *somma*, *prodotto* e la funzione *grado* esattamente come nel caso dei poliniomi di Laurent.

Lemma 1.4.9

$F[\![x]\!]$ e' un sottoanello di $F[\![x, x^{-1}]\!]$. Inoltre, $F[\![x, x^{-1}]\!]$ e' un campo.

Dimostrazione. da fare. ■

Sketch del capitolo: Polinomi di Laurent ma le dim sono trivial per il capitolo 1.3, serie formali (qui dimostro cose), serie formali di Laurent (c'è una sola dim)

1.5 Riducibilità di polinomi

Concludiamo lo studio degli anelli di polinomi affrontandone il problema della riducibilità.

Definizione 1.5.1

Sia R un dominio di integrità e sia $f(x) \in R[x]$ un polinomio non invertibile[23] e non nullo. Allora, $f(x)$ si dice irriducibile in $R[x]$ se ogni volta che esprimiamo $f(x)$ come un prodotto $f(x) = g(x)h(x)$ di polinomi $g(x), h(x) \in R[x]$, almeno uno fra $g(x)$ e $h(x)$ è invertibile. Se $f(x)$ non è irriducibile in $R[x]$, diciamo che $f(x)$ è riducibile in $R[x]$.

La riducibilità di un polinomio non è un fatto generale, ma dipende dal particolare dominio di integrità preso in esame: non ha alcun senso parlare di "polinomio irriducibile" senza specificare quale sia il dominio d'integrità considerato.

Esempio. Il polinomio $f(x) = 2x+4$ è irriducibile in $\mathbb{Q}[x]$ ma riducibile in $\mathbb{Z}[x]$. Infatti, se fosse $f(x) = g(x)h(x)$, per la *Proposizione 1.1.1* si avrebbe $\deg^\star(f) = 1 = \deg^\star(g)+\deg^\star(h)$. Dunque, almeno uno fra $g(x)$ e $h(x)$ ha grado 0 e risulta quindi invertibile essendo $\mathbb{Q}$ un campo, da cui $f(x)$ è irriducibile in $\mathbb{Q}[x]$. D'altra parte, $2x + 4 = 2(x + 2)$ e né 2 né $x + 2$ sono elementi invertibili in $\mathbb{Z}[x]$, quindi $f(x)$ è riducibile in $\mathbb{Z}[x]$. □

Nel caso in cui il dominio di integrità sia un campo $\mathbb{K}$, poiché ogni elemento non nullo di $\mathbb{K}$ è invertibile, un polinomio non costante $f(x) \in \mathbb{K}[x]$ è riducibile in $\mathbb{K}[x]$ se e solo se può essere espresso come prodotto di due polinomi non costanti di grado minore di $\deg^\star(f)$.

Esempio. Il polinomio $f(x) = x^2+1$ è irriducibile in $\mathbb{R}[x]$ ma riducibile in $\mathbb{C}[x]$. Infatti, se $f(x)$ fosse riducibile in $\mathbb{R}[x]$, per quanto appena detto esso sarebbe il prodotto di due termini di grado 1, il che è impossibile poiché $f(x)$ non ha radici reali. D'altra parte, sappiamo che $x^2 + 1 = (x + i)(x - i)$, dunque $f(x)$ è riducibile in $\mathbb{C}[x]$. □

In generale, stabilire se un polinomio sia o meno irriducibile in un certo dominio di integrità è un problema complesso. Tuttavia, esistono alcuni casi particolari in cui ciò è molto semplice.

Teorema 1.5.2: 1.5.1: Criterio del grado

Sia $\mathbb{K}$ un campo e sia $f(x) \in \mathbb{K}[x]$ un polinomio di grado 2 o 3. Allora, $f(x)$ è riducibile in $\mathbb{K}[x]$ se e solo se $f(x)$ ha una radice in $\mathbb{K}$.

Dimostrazione. Supponiamo che $f(x)$ sia riducibile in $\mathbb{K}[x]$. Allora, per definizione esistono $g(x), h(x) \in \mathbb{K}[x]$ non costanti di grado minore di $\deg^\star(f)$ tali che $f(x) = g(x)h(x)$. Poiché per ipotesi $\deg^\star(g) + \deg^\star(h) = \deg^\star(f) \leq 3$, almeno uno fra $g(x)$ e $h(x)$ ha grado 1, e senza perdita di generalità sia esso $g(x) = ax + b$. Essendo $\mathbb{K}$ un campo, $\alpha = -a^{-1}b \in \mathbb{K}$, da cui $g(\alpha) = a(-a^{-1}b) + b = 0_{\mathbb{K}}$. Dunque, $f(\alpha) = g(\alpha)h(\alpha) = 0_{\mathbb{K}}$, cioè α è una radice di $f(x)$.

Viceversa, supponiamo che esista $\alpha \in \mathbb{K}$ tale che $f(\alpha) = 0_{\mathbb{K}}$. Per il *Teorema di Ruffini* sappiamo che $(x - \alpha)$ divide $f(x)$, cioè $f(x) = (x - \alpha)q(x)$ per un opportuno $q(x) \in \mathbb{K}[x]$. Poiché $\deg^\star(q) = \deg^\star(f) - \deg^\star(x - \alpha) \geq 2 - 1 = 1$, si ha che $f(x)$ è riducibile in $\mathbb{K}[x]$. ■

Tale teorema è particolarmente comodo nel caso dei campi finiti, poiché per stabilire la riducibilità di $f(x) \in \mathbb{F}_p[x]$ è sufficiente verificare se $f(n) \equiv 0 \pmod p$ per $n = 0, 1, \dots, p-1$.

[23] Si intende rispetto al prodotto, cioè per la *Proposizione 1.1.2* prendiamo $f(x) \notin R^\times$.

Esempio. Il polinomio $f(x) = x^3 + x + 1$ è irriducibile in $\mathbb{F}_2[x]$ ma riducibile in $\mathbb{F}_3[x]$. Infatti, $f(0) \equiv f(1) \equiv 1 \not\equiv 0 \pmod 2$ in $\mathbb{F}_2$, ma $f(1) = 3 \equiv 0 \pmod 3$ in $\mathbb{F}_3$. □

Osserviamo che il *Teorema 1.5.1* vale solo nei campi, dunque non è applicabile in $\mathbb{Z}$. Inoltre, esistono polinomi riducibili di grado maggiore o uguale a 4 che non hanno radici.

Esempio. Entrambi i polinomi $f(x) = x^4 + 1$ e $g(x) = x^6 + 1$ non ammettono chiaramente radici reali. Tuttavia, osserviamo che $x^4 + 1 = (x^2 + \sqrt{2}x + 1)(x^2 - \sqrt{2}x + 1)$ e possiamo scomporre $x^6 + 1 = (x^2 + 1)(x^4 - x^2 + 1)$, dunque $f(x)$ e $g(x)$ sono riducibili in $\mathbb{R}[x]$. □

Di qui in seguito ci concentreremo principalmente sul problema della riducibilità in $\mathbb{Z}[x]$.

Definizione 1.5.3

Sia $f(x) = \sum_{i=0}^{n} a_i x^i \in \mathbb{Z}[x]$ un polinomio non nullo. Si definisce contenuto di f il valore di $\mathrm{MCD}(a_0, \dots, a_n)$. Un polinomio si dice primitivo se il suo contenuto è 1.

Esempio. Il polinomio $f(x) = 2x^2 + 3x + 4$ è primitivo perché $\mathrm{MCD}(2, 3, 4) = 1$. D'altra parte, il polinomio $g(x) = 2x^2 + 4$ non è primitivo poiché $\mathrm{MCD}(2, 0, 4) = 2 \neq 1$. □

Osserviamo che presi i due polinomi primitivi $f(x) = x + 1$ e $g(x) = 2x + 3$, anche il loro prodotto $f(x)g(x) = 2x^2 + 5x + 3$ è primitivo, poiché il suo contenuto è $\mathrm{MCD}(2, 5, 3) = 1$. Questo è un fatto generale, come dimostrato dal lemma seguente.

Lemma 1.5.4: 1.5.2: Lemma di Gauss

Il prodotto di due polinomi primitivi è un polinomio primitivo.

Dimostrazione. Siano $f(x)$, $g(x) \in \mathbb{Z}[x]$ polinomi primitivi, e supponiamo per assurdo che $f(x)g(x)$ non sia primitivo. Allora, esiste p primo che divide tutti i coefficienti di $f(x)g(x)$, cioè $f(x)g(x) \equiv 0$ in $\mathbb{F}_p[x]$. Poiché $\mathbb{F}_p[x]$ è un dominio di integrità, deve essere $f(x) \equiv 0$ oppure $g(x) \equiv 0$, da cui p divide tutti i coefficienti di almeno uno fra $f(x)$ e $g(x)$, e tale polinomio risulta quindi non primitivo, assurdo. Dunque, $f(x)g(x)$ è primitivo. ■

Esiste una stretta relazione tra la riducibilità in $\mathbb{Z}[x]$ e quella in $\mathbb{Q}[x]$.

Teorema 1.5.5: 1.5.3

Sia $f(x) \in \mathbb{Z}[x]$ un polinomio irriducibile in $\mathbb{Z}[x]$. Allora, $f(x)$ è irriducibile in $\mathbb{Q}[x]$.

Dimostrazione. Supponiamo per assurdo che $f(x)$ sia riducibile in $\mathbb{Q}[x]$. Allora, esistono $g(x)$, $h(x) \in \mathbb{Q}[x]$ non costanti tali che $f(x) = g(x)h(x)$, dove, a meno di dividere $g(x)$ per il contenuto di f, possiamo assumere senza perdita di generalità che $f(x)$ sia primitivo. Siano a e b il minimo comune multiplo dei denominatori dei coefficienti di $g(x)$ e $h(x)$, rispettivamente, così che $ag(x)$ e $bh(x)$ siano polinomi a coefficienti interi. Detti c_1 e c_2 il contenuto di $ag(x)$ e $bh(x)$, rispettivamente, si ha che $ag(x) = c_1 g'(x)$ e $bh(x) = c_2 h'(x)$, dove $g'(x)$ e $h'(x)$ sono polinomi primitivi. Poiché $abf(x) = ag(x)\, bh(x) = c_1 c_2\, g'(x)h'(x)$ e per il *Lemma 1.5.2* anche $g'(x)h'(x)$ è primitivo, deve essere $ab = c_1 c_2$. Dunque, si ha che $f(x) = g'(x)h'(x)$ dove $g'(x)$, $h'(x) \in \mathbb{Z}[x]$, cioè $f(x)$ è riducibile in $\mathbb{Z}[x]$, assurdo. ■

Sebbene $\mathbb{Q}$ sia un campo più grande di $\mathbb{Z}$, tale teorema mostra che esso non è abbastanza grande per permettere di scomporre in $\mathbb{Q}[x]$ un polinomio irriducibile in $\mathbb{Z}[x]$, ed è quindi necessario passare a campi ancora più grandi quali $\mathbb{R}$ e $\mathbb{C}$. Inoltre, la dimostrazione mostra che se un polinomio $f(x) \in \mathbb{Z}[x]$ è riducibile in $\mathbb{Q}[x]$, allora esso è riducibile anche in $\mathbb{Z}[x]$.

Esempio. Sia $f(x) = 6x^2 - 5x + 1 = (3x - \frac{3}{2})(2x - \frac{2}{3})$ un polinomio riducibile in $\mathbb{Q}[x]$. Utilizzando la notazione del *Teorema 1.5.3*, definiamo $g(x) = (3x - \frac{3}{2})$ e $h(x) = (2x - \frac{2}{3})$. Allora, $a = 2$ e $b = 3$, da cui $ag(x) = 6x - 3$ e $bh(x) = 6x - 2$. Dunque, $c_1 = \text{MCD}(6, 3) = 3$ e $c_2 = \text{MCD}(6, 2) = 2$, da cui $g'(x) = 2x - 1$ e $h'(x) = 3x - 1$ sono polinomi primitivi e $f(x) = g'(x)h'(x) = (2x - 1)(3x - 1)$ risulta quindi riducibile in $\mathbb{Z}[x]$. $\square$

Sketch del capitolo: riduzione mod p, Eisenstein, polinomi ciclotomici, tanti esempi, e tutto quello che Weigel dà per scontato sia stato fatto ad Algebra 1. asdf

1.6 Anelli noetheriani

Lemma 1.6.1

Sia R un anello e siano $a_1, \dots, a_n \in R$. Allora, $I = \sum_{i=1}^{n} Ra_i = \left\{ \sum_{i=1}^{n} r_i a_i : r_i \in R \right\}$ è un ideale[24] di R.

Dimostrazione. Infatti, presi $x = \sum_{i=1}^{n} r_i a_i$ e $y = \sum_{i=1}^{n} s_i a_i$ in I, si ha che

$$x + y = \sum_{i=1}^{n} (r_i + s_i) a_i \in I,$$

$$tx = t \sum_{i=1}^{n} r_i a_i = \sum_{i=1}^{n} (t r_i) a_i \in I,$$

per ogni $t \in R$, da cui $I \lhd R$. ■

Definizione 1.6.2: Ideale generato

Sia R un anello e siano $a_1, \dots, a_n \in R$. Allora, l'ideale $I = \sum_{i=1}^{n} Ra_i$ è detto ideale generato da $a_1, \dots, a_n$ e si denota con $I = \langle a_1, \dots, a_n \rangle$.

L'ideale generato da $a_1, \dots, a_n$ è il più piccolo ideale di R contenente $a_1, \dots, a_n$, e possiamo pensarlo come l'insieme delle combinazioni lineari in R di $a_1, \dots, a_n$.

Esempio. Consideriamo in $\mathbb{Z}$ gli ideali $I = \langle 2 \rangle$ e $J = \langle 2, 3 \rangle$. Allora, $I = \{2n : n \in \mathbb{Z}\} = 2\mathbb{Z}$ è l'insieme dei numeri pari e $J = \{2m + 3n : m, n \in \mathbb{Z}\} = \mathbb{Z}$ perché $1 = 2 \cdot 2 + 3 \cdot (-1) \in J$, da cui $k = 2 \cdot (2k) + 3 \cdot (-k) \in J$ per ogni $k \in \mathbb{Z}$. □

Definizione 1.6.3

Dato un ideale $I \lhd R$, definiamo numero minimo di generatori $d_R(I)$ il più piccolo $n \in \mathbb{N}$ per cui esistano $a_1, \dots, a_n \in R$ tali che $I = \langle a_1, \dots, a_n \rangle$. Se tale $n \in \mathbb{N}$ non esiste, poniamo $d_R(I) = \infty$. Diciamo che $I \lhd R$ è finitamente generato se $d_R(I) < \infty$.

Esempio. Sia $I = \langle 2, x \rangle \lhd \mathbb{Z}[x]$ e supponiamo che $d_{\mathbb{Z}[x]}(I) = 1$, cioè che $I = \langle f(x) \rangle$ per un certo $f(x) \in \mathbb{Z}[x]$ non nullo. Se $\deg^\star(f) = 0$, cioè $f(x) \equiv k$, allora k è pari e I contiene solo polinomi con coefficienti pari, da cui $x \notin I$, assurdo. Se $\deg^\star(f) \geq 1$, allora I contiene solo polinomi di grado almeno 1, cioè $2 \notin I$, assurdo. Dunque $d_{\mathbb{Z}[x]}(I) = 2$. □

Esiste un'importante famiglia di anelli in cui ogni ideale è finitamente generato.

[24] Ricordiamo che I è un ideale di un anello commutativo R se $a - b \in I$ per ogni $a, b \in I$ e se $ra \in I$ per ogni $a \in I$ e $r \in R$. Per ragioni estetiche, si preferisce spesso mostrare equivalentemente che $a + b \in I$ per ogni $a, b \in I$ e non che $a - b \in I$. Infatti, se l'opposto esiste, detto $c = -b$ si ha che $a - b \in I \Leftrightarrow a + c \in I$.

Definizione 1.6.4: Anello noetheriano

Un anello commutativo R si dice noetheriano se ogni suo ideale è finitamente generato, cioè se ogni ideale $I \lhd R$ soddisfa $d_R(I) < \infty$.

Esempio. Sia R un dominio ad ideali principali.[25] Allora, R è un anello noetheriano poiché per definizione di PID si ha che $d_R(I) = 1$ per ogni $I \lhd R$ non banale e $d_R(\{0_R\}) = 0$. In particolare, ogni campo $\mathbb{K}$ è noetheriano perché i suoi unici ideali sono $\{0_\mathbb{K}\}$ e $\mathbb{K} = \langle 1_\mathbb{K} \rangle$. □

Nelle dimostrazioni è spesso utile considerare una caratterizzazione equivalente degli anelli noetheriani in termini di successioni ascendenti di ideali, cioè successioni di ideali $(I_k)_{k\in\mathbb{N}}$ tali che $I_k \subseteq I_{k+1}$ per ogni $k \in \mathbb{N}$.

Proposizione 1.6.5

Sia R un anello commutativo. Allora, R è noetheriano se e solo se per ogni successione ascendente di ideali $(I_k)_{k\in\mathbb{N}}$ esiste $N \in \mathbb{N}$ tale che $I_{N+j} = I_N$ per ogni $j \in \mathbb{N}$.

Dimostrazione. Supponiamo che R sia noetheriano, e sia $(I_k)_{k\in\mathbb{N}}$ una successione ascendente di ideali. Poiché $I_\infty = \bigcup_{k\in\mathbb{N}} I_k$ è un ideale di R,[26] essendo R noetheriano $d_R(I_\infty) = n < \infty$. Siano quindi $a_1, \dots, a_n \in I_\infty$ tali che $I_\infty = \langle a_1, \dots, a_n \rangle$, e siano $k_1, \dots, k_n \in \mathbb{N}$ tali che $a_i \in I_{k_i}$. Detto $N = \max\{k_i : 1 \le i \le n\}$, essendo $(I_k)_{k\in\mathbb{N}}$ ascendente si ha che $a_1, \dots, a_n \in I_N$. Dunque, essendo I_N un ideale, $\sum_{i=1}^{n} r_i a_i \in I_N$ per ogni $r_1, \dots, r_n \in R$, cioè $\sum_{i=1}^{n} R a_i = I_\infty \subseteq I_N$, da cui $I_{N+j} \subseteq I_N \ \forall j \in \mathbb{N}$. Poiché $(I_k)_{k\in\mathbb{N}}$ è ascendente, è anche vero che $I_N \subseteq I_{N+j} \ \forall j \in N$. Combinando le doppie inclusioni, si ha quindi che $I_{N+j} = I_N \ \forall j \in \mathbb{N}$.

Viceversa, supponiamo per assurdo che esista $J \lhd R$ con $d_R(J) = \infty$. Preso $a_0 \in J$, costruiamo la successione $(a_k)_{k\in\mathbb{N}}$ di elementi di J tale che $a_{k+1} \in J \setminus \langle a_0, \dots, a_k \rangle \ \forall k \in \mathbb{N}$. Tale successione esiste poiché J non è finitamente generato, quindi $J \setminus \langle a_0, \dots, a_k \rangle \neq \emptyset$ per ogni $k \in \mathbb{N}$. Si consideri la successione di ideali $(I_k)_{k\in\mathbb{N}}$, $I_k = \langle a_0, \dots, a_k \rangle$. Allora, è evidente che $I_k \subseteq I_{k+1} \ \forall k \in \mathbb{N}$, ma essendo $a_{k+1} \notin I_k$ per come abbiamo definito $(a_k)_{k\in\mathbb{N}}$, risulta essere $I_k \subset I_{k+1}$. Abbiamo quindi costruito una successione ascendente di ideali che viola le ipotesi, perché non esiste $N \in \mathbb{N}$ tale che $I_{N+j} = I_N \ \forall j \in \mathbb{N}$, assurdo. Dunque $d_R(J) < \infty$, e per l'arbitrarietà di J concludiamo che R è noetheriano. ■

Dimostriamo ora un risultato fondamentale nello studio degli anelli noetheriani.

Teorema 1.6.6: Teorema della base di Hilbert

Sia R un anello noetheriano. Allora, anche l'anello dei polinomi $R[x]$ è noetheriano.

[25] Ricordiamo che un dominio ad ideali principali (spesso abbreviato PID) è un dominio di integrità in cui ogni ideale è principale, cioè generato da un solo elemento. Esempi di PID sono $\mathbb{Z}$ e ogni campo $\mathbb{K}$.

[26] Siano $a, b \in I_\infty$ con $a \in I_s$ e $b \in I_t$, dove $s \le t$, cioè $I_s \subseteq I_t$. Poiché $a, b \in I_t$, anche $a + b \in I_t \subseteq I_\infty$, da cui $a + b \in I_\infty$. Inoltre, preso $r \in R$, si ha che $ra \in I_s \subseteq I_\infty$, cioè $ra \in I_\infty$, da cui $I_\infty \lhd R$.

Dimostrazione. Supponiamo per assurdo che $R[x]$ non sia noetheriano, e sia quindi $J \lhd R[x]$ tale che $d_{R[x]}(J) = \infty$. Preso $f_0 \in J$ non nullo di grado minimo, costruiamo la successione di polinomi $(f_k)_{k\in\mathbb{N}}$ tale che f_{k+1} sia il polinomio di grado minimo in $J \setminus \langle f_0, \dots, f_k\rangle \ \forall k \in \mathbb{N}$. Tale successione esiste poiché J non è finitamente generato, quindi $J \setminus \langle f_0, \dots, f_k\rangle \neq \emptyset$ per ogni $k \in \mathbb{N}$. Sia $d_k = \deg^\star(f_k)$ e sia $a_k \neq 0_R$ il coefficiente direttore di f_k. Allora, detta $(I_k)_{k\in\mathbb{N}}$ la successione ascendente di ideali di R definita come $I_k = \langle a_0, \dots, a_k\rangle$, per la *Proposizione 1.6.5* esiste $N \in \mathbb{N}$ tale che $I_{N+j} = I_N \ \forall j \in \mathbb{N}$. In particolare $I_{N+1} = I_N$, ed esistono $r_0, \dots, r_N \in R$ tali che $a_{N+1} = \sum_{i=0}^{N} r_i a_i$. Consideriamo ora il polinomio $h = f_{N+1} - \sum_{i=0}^{N} r_i\, x^{d_{N+1}-d_i} f_i \in J$.[27] Se $h \in \langle f_0, \dots, f_N\rangle$, allora anche $f_{N+1} = h + \sum_{i=0}^{N} r_i\, x^{d_{N+1}-d_i} f_i \in \langle f_0, \dots, f_N\rangle$, il che è assurdo per come abbiamo definito $(f_k)_{k\in\mathbb{N}}$. Poiché il coefficiente del termine di grado d_{N+1} in h è $a_{N+1} - \sum_{i=0}^{N} r_i a_i = 0$, si ha che $h \in J \setminus \langle f_0, \dots, f_N\rangle$ è un polinomio di grado $\deg^\star(h) < d_{N+1}$, e questo viola la minimalità del grado nella scelta di f_{N+1}. Dunque $d_{R[x]}(J) < \infty$, da cui per l'arbitrarietà di J concludiamo che $R[x]$ è noetheriano. ■

Corollario 1.6.7

Sia $n \in \mathbb{N}^+$ e sia R un anello noetheriano. Allora, anche $R[x_1, \dots, x_n]$ è noetheriano.

Dimostrazione. Essendo R noetheriano, per il *Teorema 1.6.6* anche $R[x_1]$ è noetheriano, ed induttivamente sono noetheriani pure $(R[x_1])[x_2], \dots, (\cdots((R[x_1])[x_2])\cdots)[x_n]$. Poiché per il *Corollario SISTEMARE REF* si ha che $R[x_1, \dots, x_n] \simeq (\cdots((R[x_1])[x_2])\cdots)[x_n]$, possiamo concludere che anche $R[x_1, \dots, x_n]$ è noetheriano. ■

Questo risultato non è più valido quando l'insieme delle variabili X è un insieme infinito, ed in particolare, esistono domini di integrità che non sono noetheriani.

Esempio. Sia R un domimio di integrità noetheriano e sia $X = \{x_n : n \in \mathbb{N}\}$ un insieme numerabile di variabili. Per la *Proposizione SISTEMARE REF* sappiamo già che $R[X]$ è un dominio di integrità, quindi è sufficiente mostrare che esso non è noetheriano. Sia $(I_k)_{k\in\mathbb{N}}$ la successione di ideali di $R[X]$ definita come $I_k = \langle x_0, \dots, x_k\rangle$. Allora $I_k \subsetneq I_{k+1}$, poiché $I_k \subseteq I_{k+1}$ ma $x_{k+1} \notin \langle x_0, \dots, x_k\rangle = I_k$. Dunque, $(I_k)_{k\in\mathbb{N}}$ è una successione ascendente di ideali che viola la *Proposizione 1.6.5*, da cui concludiamo che $R[X]$ non è noetheriano. □

La proposizione seguente, molto utile negli esercizi, permette di dimostrare che un anello è noetheriano semplicemente esibendo un omomorfismo suriettivo.

Proposizione 1.6.8: 1.6.4

Sia R un anello noetheriano e sia $\phi\colon R \to S$ un omomorfismo di anelli suriettivo. Allora, anche S è un anello noetheriano.

[27] Vogliamo sfruttare la relazione tra a_{N+1} e $a_1, \dots, a_N$ che abbiamo appena trovato per costruire un polinomio $h \in J \setminus \langle f_0, \dots, f_N\rangle$ di grado minore di d_{N+1}, giungendo quindi ad un assurdo.

Dimostrazione. Siano $J \lhd S$ e $I = \phi^{-1}(J) = \{r \in R : \phi(r) \in J\}$. Poiché I è un ideale di R,[28] che per ipotesi è noetheriano, esistono $a_1, \dots, a_n \in R$ tali che $I = \langle a_1, \dots, a_n \rangle$. Allora, essendo ϕ suriettivo, sappiamo che $J = \phi(I) = \langle \phi(a_1), \dots, \phi(a_n) \rangle$, da cui $d_S(J) \leq d_R(I) = n < \infty$. Dunque, per l'arbitrarietà di J concludiamo che S è noetheriano. ■

Esempio. Sia $\mathbb{Z}[\sqrt{2}\,] = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\} \subseteq \mathbb{R}$. Poiché $\mathbb{Z}$ è un PID, esso è noetheriano, dunque per il *Teorema REF DI CAPITOLO 1.4* anche $\mathbb{Z}[x]$ è noetheriano. Sia $\phi_{\sqrt{2}} \colon \mathbb{Z}[x] \to \mathbb{Z}[\sqrt{2}\,]$ la valutazione in $\sqrt{2}$. Poiché per ogni $a+b\sqrt{2} \in \mathbb{Z}[\sqrt{2}\,]$ si ha che $\phi_{\sqrt{2}}(a+bx) = a+b\sqrt{2}$, tale $\phi_{\sqrt{2}}$ è un omomorfismo suriettivo, quindi per la *Proposizione 1.6.8* anche $\mathbb{Z}[\sqrt{2}\,]$ è noetheriano. □

Un caso particolare della *Proposizione 1.6.8* vale per gli anelli quoziente.

Corollario 1.6.9

Sia R un anello noetheriano e sia $I \lhd R$. Allora, anche R/I è noetheriano.

Dimostrazione. Sia $\pi \colon R \to R/I$, $\pi(r) = r + I$ la proiezione canonica sul quoziente. Poiché π è un omomorfismo suriettivo, per la *Proposizione 1.6.8* anche R/I è noetheriano. ■

Possiamo quindi mostrare che esistono anelli noetheriani che non sono domini di integrità.

Esempio. Poiché $4\mathbb{Z}$ è un ideale di $\mathbb{Z}$, per il *Corollario 1.6.9* anche $\mathbb{Z}/4\mathbb{Z}$ è noetheriano.[29] Tuttavia, esso non è dominio di integrità perché ha divisori dello zero: infatti, $2 \cdot 2 = 0$. □

Proposizione che anello noetheriano ha un ideale massimale, discussione sulla noetherianità che gratuitamente permette la dimostrazione senza il lemma di zorn, dimostrazione che ogni anello ha un ideale massimale usando zorn.

Osservazione. prova

[28] In generale, se $\varphi \colon A \to B$ è un omomorfismo e $J \lhd B$, allora $I = \varphi^{-1}(J) = \{a \in A : \varphi(a) \in J\} \lhd A$. Infatti, presi a, $b \in I$, per definizione $\varphi(a)$, $\varphi(b) \in J$. Dunque, essendo J un ideale e φ un omomorfismo, $\varphi(a+b) = \varphi(a) + \varphi(b) \in J \Rightarrow a + b \in I$ e $\varphi(ra) = \varphi(r)\varphi(a) \in J \Rightarrow ra \in I$ per ogni $r \in A$, da cui $I \lhd A$.

[29] In realtà basta osservare che ogni anello finito è noetheriano poiché $d_R(I) \leq |R| < \infty$ per ogni $I \lhd R$.

1.7 Localizzazione

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

Definizione 1.7.1: Sistema moltiplicativo

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 $2^{-1} = \frac{1}{2} \notin S$. □

Definiamo ora una relazione di equivalenza necessaria per l'argomento.
Sull'insieme delle coppie $(r, s) \in R \times S$ definiamo la relazione $(r, s) \sim (t, u) \Leftrightarrow ru = st$.

Proposizione 1.7.2: 1.7.1

Sia R un dominio di integrità e sia $S \subseteq R$ un suo sistema moltiplicativo. Allora

$$\sim : (R \times S) \times (R \times S) \to \{\mathrm{v}, \mathrm{f}\}$$

definita sulle coppie (r, s) è una relazione di equivalenza.[30]

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. ■

Osservazione. (i) Denotiamo con $\frac{r}{s} = [(r, s)]_\sim$ la classe di equivalenza di (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 $\sim$.

(ii) Nella prossima pagina andremo a definire la "localizzazione", che deve il suo nome alla geometria algebrica[31]. 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.

[30] La 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.

[31] Se 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".

Definizione 1.7.3: Localizzazione e operazioni

Sia R un dominio di integrità e sia S un sistema moltipicativo di R. Allora, l'insieme $S^{-1}R = \{\frac{r}{s} : r \in R, s \in S\}$ è detto localizzazione di R a S. Siano $\frac{r}{s}, \frac{t}{u} \in S^{-1}R$. Definiamo *somma* e *prodotto*:

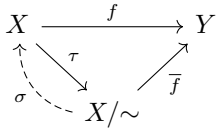
$$\oplus\colon S^{-1}R \times S^{-1}R \to S^{-1}R,\ \frac{r}{s} \oplus \frac{t}{u} = \frac{ru+st}{su}$$
$$\odot\colon S^{-1}R \times S^{-1}R \to S^{-1}R,\ \frac{r}{s} \odot \frac{t}{u} = \frac{rt}{su}.$$

Osservazione. 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 1.7.4: 1.7.2: Lemma della forbice

Siano X e Y insiemi non vuoti e sia $f\colon X \to Y$ una mappa. Sia $\sim$ una relazione di equivalenza su X e $\tau\colon X \to X/\sim$ la proiezione canonica[32]. Allora, esiste una mappa $\overline{f}\colon X/\sim \to Y$ tale che $f = \overline{f} \circ \tau$ 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,[33] esiste $\sigma\colon X/\sim \to X$ tale che $\sigma([x]) \sim x$ per ogni $x \in X$ e $\tau \circ \sigma = \mathrm{id}_{X/\sim}$. Si consideri ora la funzione $\overline{f} = f \circ \sigma\colon X/\sim \to Y$.



Osserviamo innanzitutto che $\overline{f}$ è ben definita, poiché se $[x] = [y]$, allora $\overline{f}([x]) = \overline{f}([y])$ 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, $\left(\overline{f} \circ \tau\right)(x) = f(\sigma(\tau(x))) = f(\sigma([x])) = f(x)$ per ogni $x \in X$ poiché $\sigma([x]) \sim x$, dunque è effettivamente vero che $f = \overline{f} \circ \tau$. Viceversa, sia $\overline{f}\colon X/\sim \to Y$ tale che $f = \overline{f} \circ \tau$. Allora, per ogni $x, y \in X$ con $x \sim y$, cioè $[x] = [y]$, si ha che $f(x) = \overline{f}(\tau(x)) = \overline{f}([x]) = \overline{f}([y]) = \overline{f}(\tau(y)) = f(y)$ come desiderato. ■

Dimostriamo quindi che le operazioni sono precedentemente discusse sono ben poste.

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

[33] L'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 $\sigma([x]) \in X$.

Lemma 1.7.5

Le operazioni $\oplus, \odot$ definite in precedenza su $S^{-1}R$ sono ben poste.

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

$$\begin{array}{ccc} (R,S)\times(R,S) & \xrightarrow{\quad\widetilde{+}\quad} & S^{-1}R \\ & {\scriptstyle\tau}\searrow \quad \nearrow{\scriptstyle\oplus} & \\ & S^{-1}R\times S^{-1}R & \end{array}$$

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 $\frac{ru+st}{su} = \frac{r'u'+s't'}{s'u'}$. Analogamente, sia $\widetilde{\cdot}\colon (R,S)\times(R,S)\to S^{-1}R$ l'operazione definita come $(r,s)\,\widetilde{\cdot}\,(t,u) = \frac{rt}{su}$.

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

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

Osservazione. Per comodità di notazione, denoteremo di qui in seguito le due operazioni $\oplus$ e $\odot$ di $S^{-1}R$ semplicemente con $+$ e $\cdot$, rispettivamente.[34]

Proposizione 1.7.6: 1.7.3. La localizzazione di un anello e' un dominio di integrità

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

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

[34] Per quanto appena provato, possiamo effettivamente vedere tali operazioni come somma e prodotto di "frazioni" con le usuali regole di calcolo delle frazioni.

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 $\frac{rv}{sw}+\frac{tv}{uw}=\frac{ruvw+stvw}{suww}=\frac{ruv+stv}{suw}$ essendo $(ruvw+stvw)suw=(ruv+stv)suww$. 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. ■

Osservazione. Sia $\iota_R\colon R\to S^{-1}R$ definita come $\iota_R(r)=\frac{r}{1_R}$ l'inclusione da R a $S^{-1}R$. Allora 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.

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

Esempio 1.7.7: Sistemi moltiplicativi e relative localizzazioni

(*i*) 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 $\iota_R\colon R\hookrightarrow S^{-1}R$ 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.

(*ii*) 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 $\iota_R\colon R\hookrightarrow S^{-1}R$ 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 $S^{-1}R\simeq R$.

(*iii*) Sia R un dominio di integrità e sia $\mathfrak{p}\lhd R$ un ideale primo.[35] 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,[36] 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 $S^{-1}(R\setminus\mathfrak{p})\cap S^{-1}\mathfrak{p}=\emptyset$.[37] 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 $S^{-1}R=S^{-1}(R\setminus\mathfrak{p})\sqcup S^{-1}\mathfrak{p}=(S^{-1}R)^\times\sqcup S^{-1}\mathfrak{p}$.

Osservazione. Se R è un dominio di integrità, $\{0_R\} \lhd R$ 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 1.7.8: Campo dei quozienti

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 $\mathrm{quot}(R)$.

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

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 $\mathbb{Q} = \mathrm{quot}(\mathbb{Z})$. Quest'ultimo è un fatto generale, come dimostrato dalla proposizione seguente.

Proposizione 1.7.9: 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 $\iota_R \colon R \to \mathrm{quot}(R)$ l'inclusione. Poiché ι_R è un omomorfismo iniettivo, $\ker(\iota_R) = \{0_R\}$ e $\mathrm{Im}(\iota_R)$ è un sottoanello del campo $\mathrm{quot}(R)$. Dunque, per il *primo teorema d'isomorfismo* si ha che $R = R/\ker(\iota_R) \simeq \mathrm{Im}(\iota_R)$. ■

Osservazione. In particolare, $\mathbb{Q} = \mathrm{quot}(\mathbb{Z})$ 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 1.7.10: 1.7.5

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

Dimostrazione. Osserviamo innanzitutto che per la *proposizione 1.7.9* sappiamo che R è isomorfo al sottoanello $\mathrm{Im}(\iota_R)$ del campo $\mathrm{quot}(R)$. Sia quindi $\mathbb{K}$ un campo contenente R e sia ϕ: quot(R) $\to \mathbb{K}$ 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 $\frac{r}{s}, \frac{t}{u} \in \mathrm{quot}(R)$. Allora, si ha che

[37] Un ideale proprio $\mathfrak{p} \lhd R$ 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 $b \in \mathfrak{p}$.

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

[37] Sia $\frac{r}{s} \in S^{-1}\mathfrak{p}$; se fosse $\frac{r}{s} = \frac{t}{u} \in S^{-1}(R \setminus \mathfrak{p})$, 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 $s, t \in S = R \setminus \mathfrak{p}$.

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

$$\phi\left(\frac{r}{s}\cdot\frac{t}{u}\right)=\phi\left(\frac{rt}{su}\right)=rt(su)^{-1}=rs^{-1}tu^{-1}=\phi\left(\frac{r}{s}\right)\cdot\phi\left(\frac{t}{u}\right)$$

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 $\mathrm{Im}(\phi)$ è un sottoanello del campo $\mathbb{K}$ e per il *primo teorema d'isomorfismo* si ha che $\mathrm{quot(R)}=\mathrm{quot(R)}\,/\ker(\phi)\simeq\mathrm{Im}(\phi)$, concludiamo che $\mathbb{K}$ contiene un sottoanello isomorfo a $\mathrm{quot}(R)$ ed è quindi un campo più grande del campo dei quozienti $\mathrm{quot}(R)$. ■

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 $I\lhd R$ e $J\lhd S^{-1}R$, definiamo $S^{-1}I=\{\frac{i}{s}:i\in I,s\in S\}$ e denotiamo con $\overline{J}=\iota_R^{-1}(J)=\{r\in R:\frac{r}{1_R}\in J\}$.

Proposizione 1.7.11: 1.7.6

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

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 $\iota_R\colon R\hookrightarrow S^{-1}R$ è un omomorfismo, la preimmagine $\iota_R^{-1}(J)\subseteq R$ di un ideale $J\lhd S^{-1}R$ è un ideale di R, cioè $\overline{J}\lhd R$. Preso $\frac{j}{s}\in S^{-1}\overline{J}$, 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 $S^{-1}\overline{J}\subseteq J$. 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 $r\in\overline{J}$. Dunque risulta $\frac{r}{s}\in S^{-1}\overline{J}$, da cui $J\subseteq S^{-1}\overline{J}$. Combinando le doppie inclusioni, si ha quindi che $S^{-1}\overline{J}=J$. ■

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

Corollario 1.7.12: 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 1.7.6* sappiamo che $S^{-1}R$ è un dominio di integrità, quindi è sufficiente provare che esso è anche noetheriano. Siano $J\lhd S^{-1}R$ e $\overline{J}=\iota_R^{-1}(J)\lhd R$. Essendo R noetheriano, esistono $a_1,\dots,a_n\in R$ tali che $\overline{J}=\langle a_1,\dots,a_n\rangle$. Dunque, per la *Proposizione 1.7.11* si ha che $J=S^{-1}\overline{J}=\{\frac{j}{s}:j\in\overline{J},s\in S\}=\langle\frac{a_1}{1_R},\dots,\frac{a_n}{1_R}\rangle$ 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 1.7.13: Anello locale

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 1.7.14

(i) 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 $\mathfrak{m} = \mathbb{K} \setminus \mathbb{K}^\times = \{0_\mathbb{K}\} \lhd \mathbb{K}$.

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

(iii) 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 $\mathfrak{m} = \mathbb{K}[\![x]\!] \setminus \mathbb{K}[\![x]\!]^\times = \langle x \rangle \lhd \mathbb{K}[\![x]\!]$.

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

(iv) Sia $\mathbb{K}$ un campo. Allora, $\mathbb{K}[x]$ non è un anello locale. Infatti, sappiamo che per la *Proposizione 1.1.9* vale $\mathbb{K}[x]^\times = \mathbb{K}^\times$, da cui $\mathfrak{m} = \mathbb{K}[x] \setminus \mathbb{K}[x]^\times = \{f(x) \in \mathbb{K}[x] : \deg^\star(f) \geq 1\}$. 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 $\deg^\star(h) = 0$.

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

(v) $R = \mathbb{Z}/4\mathbb{Z}$ e' un anello locale, in quanto $R^\times = R$, tuttavia e' immediato notare che non e' dominio di integrità.

(vi) In generale, R/M^n, dove M e' un anello massimale e $R \neq 0, R$ e' commutativo, e' un esempio valido.

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

Proposizione 1.7.15: 1.7.8

Sia R un anello locale. Allora, $\mathfrak{m} = R \setminus R^\times$ è l'unico ideale massimale[38] di R.

Dimostrazione. Osserviamo innanzitutto che $\mathfrak{m} \lhd R$ è massimale perché, preso $I \lhd R$ 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.[39] D'altra parte, se $J \lhd R$ 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. ■

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

[38] Ricordiamo che un ideale I si dice *massimale* in un anello R se $I \neq R$ e per ogni ideale $J \supseteq I, J = I$ oppure $J = R$.

[39] Infatti, 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 $I = R$.

Proposizione 1.7.16: 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 $\mathrm{MCD}(a, p) = 1$.[40] Si ha quindi che $(\mathbb{Z}/p^k\mathbb{Z})^\times = \{a + p^k\mathbb{Z} : \mathrm{MCD}(a, p) = 1\}$, 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 $\mathbb{Z}/p^k\mathbb{Z}$.[41] 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, $p\mathbb{Z}/n\mathbb{Z} \lhd \mathbb{Z}/n\mathbb{Z}$ è un ideale massimale.[42] Analogamente, anche $q\mathbb{Z}/n\mathbb{Z} \lhd \mathbb{Z}/n\mathbb{Z}$ è massimale, ed essendo $p \neq q$ tali ideali sono distinti.[43] Abbiamo quindi trovato due ideali massimali distinti di $\mathbb{Z}/n\mathbb{Z}$, da cui per la *Proposizione 1.7.15* 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 1.7.15* l'ideale $\mathfrak{m} \lhd R$ è massimale, l'anello quoziente $R/\mathfrak{m}$ risulta essere un campo.

Definizione 1.7.17: Campo dei residui

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

Esempio 1.7.18

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

(*ii*) Si consideri $\mathbb{Z}/p^k\mathbb{Z}$ con p primo e $k \geq 1$ intero. Per quanto appena provato nella *Proposizione 1.7.16*, 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 $\mathrm{res}(\mathbb{Z}/p^k\mathbb{Z}) = (\mathbb{Z}/p^k\mathbb{Z})/(p\mathbb{Z}/p^k\mathbb{Z}) \simeq \mathbb{Z}/p\mathbb{Z}$.

(*iii*) 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 $\mathrm{res}(\mathbb{K}[\![x]\!]) = \mathbb{K}[\![x]\!]/\langle x \rangle = \{a + \langle x \rangle : a \in \mathbb{K}\} \simeq \mathbb{K}$.

Nel caso in cui $\mathfrak{p} \lhd R$ 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.

[40] Secondo l'*Identità di Bézout*, dati due interi a, b non entrambi nulli e detto $d = \mathrm{MCD}(a, b)$, 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 $\mathrm{MCD}(a, p) \leq 1$, cioè $\mathrm{MCD}(a, p) = 1$.

[41] Il 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 $\mathrm{MCD}(a, p) > 1$, cioè, essendo p primo, $\mathrm{MCD}(a, p) = p$. Dunque, $\mathfrak{m} = \{a + p^k\mathbb{Z} : p \mid a\} = p\mathbb{Z}/p^k\mathbb{Z} \lhd \mathbb{Z}/p^k\mathbb{Z}$.

[42] Ricordiamo che preso un ideale $I \lhd R$, l'anello quoziente R/I è un campo se e solo se I è massimale.

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

Proposizione 1.7.19: 1.7.10

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

Dimostrazione. Se $\frac{r}{s} \in S^{-1}R$ allora esiste l'inverso $\frac{u}{t} \in S^{-1}R$ se e solo se $ru = st \in S$. In particolare, avremo che $r \notin \mathfrak{p}$, altrimenti $r \in \mathfrak{p}$ implicherebbe $ru \in \mathfrak{p}$, quindi $ru \notin S$. Pertanto

$$(S^{-1}R)^\times = \left\{ \frac{r}{s} \mid r, s \in S \right\},$$

da cui deduciamo che $S{-}1R = (S-1R)^\times \sqcup S^{-1}\mathfrak{p}$, cioe' $S{-}1R \setminus (S^{-1}R)^\times = S^{-1}\mathfrak{p}$, e $S^{-1}R$ e' un anello locale, e per la *Proposizione 1.7.15* l'unico ideale massimale di $S^{-1}R$ e' $S^{-1}\mathfrak{p}$. Osserviamo che, essendo $\mathfrak{p} \lhd R$ e' un ideale primo, allora $R/\mathfrak{p}$ e' un dominio di integrità. Sia $\pi : R \to R/\mathfrak{p}$ la proiezione canonica, e $\pi_* : S^{-1}R \to \text{quot}(R/\mathfrak{p})$ la mappa data da

$$\pi_*\left(\frac{r}{s}\right) = \frac{\pi(r)}{\pi(s)}, \ \ \frac{r}{s} \in S^{-1}R.$$

Allora π_* e' un omomorfismo suriettivo di anelli. Poiche' $\text{quot}(R/\mathfrak{p})$ e' un campo, $\ker(\pi_*)$ e' un ideale massimale e quindi dev'essere uguale a $S^{-1}\mathfrak{p}$. Dal teorema dell'omomorfismo, abbiamo l'asserto. ■

Osservazione. La precedente proposizione mostra che ogni coppia $(R, \mathfrak{p})$, con R dominio di integrità e $\mathfrak{p} \lhd R$ ideale primo, definisce un anello locale $\mathcal{O}_\mathfrak{p} = S^{-1}R$, per $S = R \setminus \mathfrak{p}$.

Vediamo subito un esempio di quanto appena affermato

Esempio. Sia $R = \mathbb{Z}$ e $\mathfrak{p} = p\mathbb{Z}$, con p primo. Allora

$$\mathcal{O}_\mathfrak{p} = (\mathbb{Z} \setminus p\mathbb{Z})^{-1}\mathbb{Z} = \left\{ \frac{r}{s} \mid r, s \in \mathbb{Z}, p \nmid s \right\} \subseteq \mathbb{Q}$$

e' un anello locale e anche un P.I.D.

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 $\text{res}(S^{-1}\mathbb{Z})$.

asdfasdf

1.8 Domini a valutazione discreta

Introduciamo subito la definizione dell'oggetto in questione, il cui nome viene spesso abbreviato in *d.v.d* (*discrete valuation domain*). La definizione seguente e' un po' misteriosa ma verra' chiarita successivamente con una alternativa che rispecchia davvero il suo nome.

Definizione 1.8.1: Dominio a valutazione discreta

Sia R un dominio di integrità. Allora R si dice *dominio a valutazione discreta* se:
(i) R e' un dominio a ideali principali $(P.I.D)$
(ii) R e' un anello locale
(iii) R non e' un campo.

Esempio. Sia $p \in \mathbb{Z}$, p primo. Allora

$$\mathcal{O}_p = \left\{ \frac{r}{s} \mid r \in \mathbb{Z} \wedge s \in \mathbb{Z} \setminus p\mathbb{Z}^{44} \right\}$$

e' un dominio a valutazione discreta (dimostrarne il perche' magari).

Introduciamo ora formalmente il concetto di *valutazione di un campo* che risultera' chiave per questa sezione.

Definizione 1.8.2: Valutazione di un campo

Siano K un campo, $(G, +, \leq)$ un gruppo abeliano parzialmente ordinato (ovvero dotato di relazione d'ordine parziale che preserva l'operazione di gruppo).
Si dice *valutazione* una mappa $\omega : K \setminus \{0\} \to G$ tale che, per ogni $a, b \in G$,

(i) ω e' suriettivo,
(ii) $\omega(a \cdot b) = \omega(a) + \omega(b)$,
(iii) $\omega(a + b) \geq \min\{\omega(a), \omega(b)\}$,

Se G e' discreto (cioe' numerabile finito o infinito) si dice *valutazione discreta*.

Se vogliamo includere lo 0 nella nostra valutazione, otteniamo la seguente:

Definizione 1.8.3: Valutazione di un campo (estesa)

Siano K un campo, $(G, +, \leq)$ un gruppo abeliano parzialmente ordinato e consideriamo $G \cup \{\infty\}$ dove, per ogni $a \in G$, $a + \infty = \infty + a = \infty$, e $a \leq \infty$. Allora possiamo estendere la precedente definendo $\omega : K \to G$ dove vale inoltre

$$\omega(a) = \infty \iff a = 0$$

Osservazione. Come nel *Capitolo 1* per $\mathbb{N}_0$, consideriamo l'insieme $\overline{\mathbb{Z}} := \mathbb{Z} \cup \{\infty\}$ dotato della somma usuale tra interi dove inoltre, per ogni $a \in \overline{\mathbb{Z}}$

[44] Si noti che tale condizione e' equivalente ad $\text{mcd}(s, p) = 1$.

$$a + \infty = \infty + a = \infty.$$

Allora $(\overline{\mathbb{Z}}, +)$ e' un monoide commutativo, ovvero un semigruppo abeliano con 0.

Il seguente teorema descrive il legame tra i domini a valutazione discreta e i campi con una valutazione discreta.

Teorema 1.8.4

Sia R un dominio di integrità, con campo quoziente K. Allora
(i) Se (K, ω) e' un campo con una valutazione discreta, l'insieme

$$\mathcal{O}_\omega = \{x \in K \mid \omega(x) \geq 0\}$$

e' un dominio a valutazione discreta tale che $K = \text{quot}(\mathcal{O}_\omega)$

(ii) Se R e' un dominio a valutazione discreta, allora esiste una valutazione discreta $\omega : K \to \overline{\mathbb{Z}}$ tale che $R = \mathcal{O}_\omega$.

Dimostrazione. Da fare. ■

Esempio 1.8.5: Valutazione discreta

Siano $R = \mathbb{Z}, p \in \mathbb{Z}$ un numero primo. Sappiamo allora che (algebra I?) per ogni z in $\mathbb{Z} \setminus \{\pm 1, 0\}$ esiste $\varepsilon_p(z) \in \mathbb{N}_0$ tale che p^{ε_p} e' la massima potenza che divide z, cioe' $p^{\varepsilon_p} || \ z$, *se e solo se* $z \in p^{\varepsilon_p}\mathbb{Z} \setminus p^{\varepsilon_p+1}\mathbb{Z}$.

Definiamo allora $\tilde{\varepsilon}_p : \mathbb{Z} \to \mathbb{N}_0 \cup \{\infty\}$ ponendo $\tilde{\varepsilon}_p(0) := \infty$, $\tilde{\varepsilon}_p(z) := \varepsilon_p(z)$ per ogni $z \in \mathbb{Z} \setminus \{0\}$. Proviamo allora che $\tilde{\varepsilon}_p$ soddisfa i quattro assiomi di valutazione discreta.
(i) E' dato dalla definizione di $\tilde{\varepsilon}_p$.
(ii) Siano $x, y \in \mathbb{Z}$, $\tilde{\varepsilon}_p(x) = j$, $\tilde{\varepsilon}_p(y) = k$. Allora esistono $a, b \in \mathbb{Z}$ tali che $x = p^j a$, $y = p^k b$ e $p \nmid a, b$. Segue che $xy = p^{j+k}ab \in p^{j+k}\mathbb{Z}$, ma $p \nmid ab$, altrimenti per definizione di primo dev'essere che $p \mid a$ oppure $p \mid b$, che e' assurdo. Dunque, $xy \in p^{j+k}\mathbb{Z} \setminus p^{j+k+1}\mathbb{Z} \implies \tilde{\varepsilon}_p(xy) = \tilde{\varepsilon}_p(x) + \tilde{\varepsilon}_p(y)$.
(iii) Considerando x, y come nel punto precedente, abbiamo che
$xy \in p^{\min\{\tilde{\varepsilon}_p(x), \tilde{\varepsilon}_p(y)\}}\mathbb{Z} \implies \tilde{\varepsilon}_p(x + y) \geq \min \tilde{\varepsilon}_p(x), \tilde{\varepsilon}_p(y)$.
(iv) Sia $n \in \mathbb{N}_0$. Allora $\tilde{\varepsilon}_p(p^n) = n$, quindi $\tilde{\varepsilon}_p(y)$ e' suriettivo.

Pertanto la nostra funzione e' una valutazione discreta anche $\mathbb{Z}$ non e' un anello locale. Pertanto tale costruzione non e' una prerogativa ristretta solamente ai domini a valutazione discreta.

Nel caso in cui avessimo a che fare con un campo, possiamo intuire che la funzione di valutazione discreta vada leggermente modificata (anche se ho i miei dubbi, dopotutto un campo e' un dominio di integrita')

Esempio 1.8.6: Valutazione discreta su un campo

Sia $\tilde{\varepsilon}_p$ definita come nell' *Esempio 1.8.5*, e proviamo a definire $\tilde{\underline{\varepsilon}}_p : \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$ basandoci su $\tilde{\varepsilon}_p$. Dovremo in qualche modo gestire i vari quozienti, in quanto la condizione critica da soddisfare e' la (ii). Infatti, sia $\frac{1}{s} \in \mathbb{Q}$, allora vorremmo che $\tilde{\underline{\varepsilon}}_p(\frac{1}{s}) + \tilde{\underline{\varepsilon}}_p(s) = \tilde{\varepsilon}_p(1) = 0$. Dato $\frac{r}{s} \in \mathbb{Q}$, poniamo allora $\tilde{\underline{\varepsilon}}_p(\frac{r}{s}) := \tilde{\varepsilon}_p(r) - \tilde{\varepsilon}_p(s)$. Cosi' facendo gli assiomi sono soddisfatti e otteniamo una valutazione discreta.

2 Teoria dei campi

2.1 Estensione di campi

Introduciamo ora un concetto fondamentale nella teoria algebrica dei numeri e nello studio delle radici polinomiali, che costituirà la base della teoria di Galois.

Definizione 2.1.1

Una coppia di campi $\mathbb{K}$ e $\mathbb{L}$ con $\mathbb{K} \subseteq \mathbb{L}$ si dice estensione di campi e si denota con $\mathbb{L}/\mathbb{K}$.

Resta inteso che $\mathbb{K}$ ha le stesse operazioni binarie di $\mathbb{L}$, cioè che $\mathbb{K}$ è un sottocampo di $\mathbb{L}$. Inoltre, in questo caso la notazione $\mathbb{L}/\mathbb{K}$ non ha nulla a che vedere con il quoziente di campi.

Esempio. Se consideriamo $\mathbb{R}$ e $\mathbb{C}$ con le usuali operazioni di somma e prodotto, $\mathbb{R}$ è un sottocampo di $\mathbb{C}$, dunque $\mathbb{C}/\mathbb{R}$ è un'estensione di campi. □

Se $\mathbb{L}/\mathbb{K}$ è un'estensione di campi, sia $\cdot|_{\mathbb{K}\times\mathbb{L}}$ la restrizione a $\mathbb{K}$ della prima componente del prodotto $\cdot : \mathbb{L} \times \mathbb{L} \to \mathbb{L}$ del campo $\mathbb{L}$. Considerando tale moltiplicazione per gli elementi di $\mathbb{K}$ e la usuale somma di $\mathbb{L}$, si ha che $(\mathbb{L}, +, \cdot)$ ha la struttura di uno spazio vettoriale su $\mathbb{K}$. Infatti, possiamo pensare gli elementi di $\mathbb{K}$ come scalari e quelli di $\mathbb{L}$ come vettori.

Definizione 2.1.2

Sia $\mathbb{L}/\mathbb{K}$ un'estensione di campi. Definiamo grado dell'estensione $\mathbb{L}/\mathbb{K}$ la dimensione[45] $\dim_{\mathbb{K}}(\mathbb{L}) \in \mathbb{N} \cup \{\infty\}$ dello spazio vettoriale $\mathbb{L}$ sul campo $\mathbb{K}$, e si denota con $|\mathbb{L} : \mathbb{K}|$.

La scelta del termine "grado", che richiama il concetto di grado di un polinomio, sarà più chiara in seguito, quando approfondiremo i legami tra estensione di campi e polinomi.

Esempio. Se consideriamo $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$ con le usuali operazioni di somma e prodotto, si ha che $|\mathbb{C} : \mathbb{R}| = 2$ perché $\mathcal{B} = \{1, i\}$ è una base per $\mathbb{C}$, e $|\mathbb{R} : \mathbb{Q}| = \infty$ perché $\mathbb{R}$ non è numerabile, quindi non ammette una base finita su $\mathbb{Q}$, che invece è numerabile. □

[45] Ricordiamo che la dimensione di uno spazio vettoriale è la cardinalità di una sua base, cioè un insieme di vettori linearmente indipendenti che generano tutto lo spazio.

Definizione 2.1.3

Sia $\mathbb{L}/\mathbb{K}$ un'estensione di campi. Un elemento $a \in \mathbb{L}$ si dice:
(i) algebrico su $\mathbb{K}$ se esiste un polinomio non nullo $f(x) \in \mathbb{K}[x]$ tale che $f(a) = 0$;
(ii) trascendente su $\mathbb{K}$ se non è algebrico.

Esempio. Se consideriamo $\mathbb{R}/\mathbb{Q}$, l'elemento $a = \sqrt{2}$ è algebrico perché $f(x) = x^2 - 2 \in \mathbb{Q}[x]$ e $f(a) = 0$, mentre e e π sono entrambi elementi trascendenti.[46] □

Sia $\mathbb{L}/\mathbb{K}$ un'estensione di campi e sia $a \in \mathbb{L}$. Detta $\phi_a \colon \mathbb{K}[x] \to \mathbb{L}$ la valutazione in a, essendo ϕ_a un omomorfismo si ha che $\ker(\phi_a) \lhd \mathbb{K}[x]$. SISTEMARE TUTTO.

[46] La dimostrazione è tutt'altro che elementare e prende il nome di *Teorema di Lindemann-Weierstrass*.

Definizione 2.1.4

Sia $\mathbb{L}/\mathbb{K}$ un'estensione di campi e sia $a \in \mathbb{L}$ un elemento algebrico su $\mathbb{K}$. Il generatore monico di $\ker(\phi_a)$ è detto polinomio minimo di a e si denota con $\min_{a,\mathbb{K}}(x) \in \mathbb{K}[x]$.

Proposizione 2.1.5

Sia $\mathbb{L}/\mathbb{K}$ un'estensione di campi e sia $a \in \mathbb{L}$ algebrico su $\mathbb{K}$. Sia $f(x) \in \mathbb{K}[x]$ tale che:
(i) $f(a) = 0$;
(ii) $f(x)$ è monico;
(iii) $f(x)$ è irrudicibile.
Allora, $f(x)$ è il polinomio minimo di a, cioè $f(x) = \min_{a,\mathbb{K}}(x)$.

Dimostrazione. Per (i) si ha che $f(x) \in \ker(\phi_a)$, dunque esiste un polinomio $q(x) \in \mathbb{K}[x]$ tale che $f(x) = q(x) \cdot \min_{a,\mathbb{K}}(x)$. Essendo $f(x)$ irriducibile per (iii), almeno uno fra $q(x)$ e $\min_{a,\mathbb{K}}(x)$ è invertibile; tuttavia, $\min_{a,\mathbb{K}}(x) \notin \mathbb{K}[x]^\times$ e quindi CONCLUDERE ■

Sia $\mathbb{L}/\mathbb{K}$ un'estensione di campi e sia $S \subseteq \mathbb{L}$ un sottoinsieme.

Proposizione 2.1.6

Sia $\mathbb{L}/\mathbb{K}$ un'estensione di campi e sia $a \in \mathbb{L}$ algebrico su $\mathbb{K}$. Allora, $\mathbb{K}(a) = \mathbb{K}[a]$.

Dimostrazione. Sia $f(x) = \sum_{i=0}^{n} c_i x^i \in \mathbb{K}[x]$. Poiché $c_i \in \mathbb{K} \subseteq \mathbb{K}(a)$ e $a \in \mathbb{K}(a) \Rightarrow a^k \in \mathbb{K}(a)$ essendo $\mathbb{K}(a)$ chiuso rispetto al prodotto, $f(a) \in \mathbb{K}(a)$. Dunque, per l'arbitrarietà di $f(x)$ concludiamo che $\mathrm{Im}(\phi_a) = \mathbb{K}[a] \subseteq \mathbb{K}(a)$. FINIRE, ESERCIZIO PER CASA XD COME SEI SIMPATICO ■

Manca anche la lezione del 30/10/2019, al momento è solo cartacea, e contiene cose davvero molto importanti tipo la formula del grado.