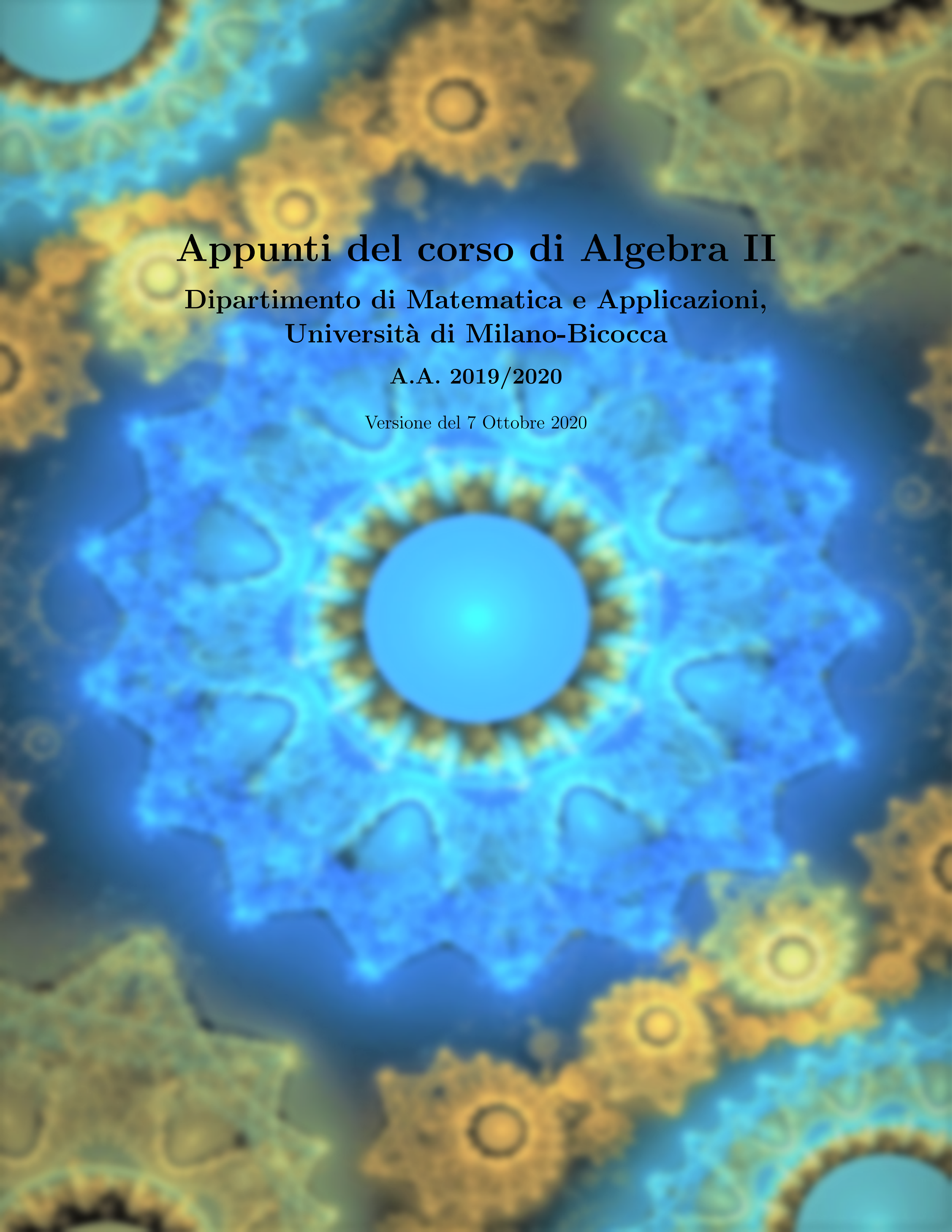

Appunti del corso di Algebra II

Dipartimento di Matematica e Applicazioni,
Università di Milano-Bicocca

A.A. 2019/2020

Versione del 7 Ottobre 2020

Indice

Changelog (versione del 7 Ottobre 2020):

- Reworking completo di varie cose

To do (in ordine di importanza):

- 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
$$\deg^\star(f) = \begin{cases} \max\{k \in \mathbb{N}_0 : a_k \neq 0_R\} & \text{se } f(x) \not\equiv 0_R \\ \infty & \text{se } f(x) \equiv 0_R \end{cases} \quad \text{è detta } \underline{\text{grado}}.$$[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 $R[x]^\times = R^\times$. ■

Come esprimere 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 $a_0, \dots, a_n \in R$. 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 $\mathbb{C} \nsubseteq \mathrm{Mat}_{2\times 2}(\mathbb{R})$ e $\mathrm{Mat}_{2\times 2}(\mathbb{R}) \nsubseteq \mathbb{C}$, cioè tali anelli non sono confrontabili secondo l'inclusione.

Definizione 1.1.10: 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 1.1.11

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.

$$\begin{tikzcd}
R \arrow[r, hook, "\varphi"] \arrow[d, hook, "\iota"'] & S \\
X \arrow[ur, hook, dashed, "\phi"'] &
\end{tikzcd}$$

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 1.1.12: 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 1.1.13: Valutazione di un polinomio

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

Esempio 1.1.14

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 1.1.15

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 $\alpha = \phi_t \circ \psi \colon T \to T$.

$$\begin{tikzcd} T \arrow[r, "\psi"] \arrow[dr, "\alpha"'] & R[s] \arrow[d, "\phi_t"] \\ & T \end{tikzcd}$$

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 $\beta = \psi \circ \phi_t \colon R[s] \to R[s]$.

$$\begin{tikzcd} R[s] \arrow[r, "\phi_t"] \arrow[dr, "\beta"'] & T \arrow[d, "\psi"] \\ & R[s] \end{tikzcd}$$

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 1.1.12* 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.

Definizione 1.2.1: Insieme dei monomi in n variabili

Sia n un intero positivo. Denotiamo con $M = \mathrm{mon}\{x_1, \dots, x_n\}$ 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:

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

Osserviamo che M dotato di tale operazione è un monoide commutativo. Infatti,

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

Per semplicità di notazione, 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 $x^{\underline{\alpha}} = x_1^{\alpha_1} \cdot \dots \cdot x_n^{\alpha_n} \in M$.

Esempio. Se $M = \mathrm{mon}\{x_1, x_2, x_3, x_4\}$ 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 $x^{\underline{\alpha}} = x_1^2 x_2^1 x_3^1 x_4^0 = x_1^2 x_2 x_3 \in M$.

Detto $\mathcal{F} = \mathcal{F}(I_n, \mathbb{N}_0)$ l'insieme delle funzioni $\underline{\alpha} \colon I_n \to \mathbb{N}_0$, [12] vi è una corrispondenza biunivoca tra $\mathcal{F}$ e l'insieme dei monomi M. Infatti, ogni monomio $x_1^{\alpha_1} \cdot \dots \cdot x_n^{\alpha_n}$ 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 $x_1^{\underline{\beta}(1)} \cdot \dots \cdot x_n^{\underline{\beta}(n)} \in M$.

Prima di procedere nella costruzione dei polinomi nelle variabili $x_1, \dots, x_n$, richiamiamo un importante concetto derivante dalla topologia e alcune sue proprietà.

Definizione 1.2.2: 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 $\mathrm{supp}(f) = \{x \in X : f(x) \neq 0_Y\}$. Se $|\mathrm{supp}(f)| < \infty$, diciamo che f ha supporto *finito*.

Si osservi che tale definizione ha senso solo se l'insieme Y contiene un elemento neutro 0_Y: nel nostro caso, avendo a che fare con anelli, 3è naturale identificare tale elemento con l'elemento neutro dell'addizione.

[12] In generale, dati due insiemi X e Y, si denota con $\mathcal{F}(X, Y)$ l'insieme di tutte le funzioni $f \colon X \to Y$.

Esempio 1.2.3

1. Sia $f\colon \mathbb{Z} \to \mathbb{R}$ la funzione $f(x) = x^2 - 1$. Allora, $\operatorname{supp}(f) = \mathbb{Z} \setminus \{\pm 1\}$.
2. Se $f\colon \operatorname{Mat}_{2\times 2}(\mathbb{F}_2) \to \mathbb{F}_2$ è il determinante, allora f ha supporto finito perché $\operatorname{supp}(f) = \operatorname{GL}(2, \mathbb{F}_2)$[13] $= \left\{ \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \right\}$

Proposizione 1.2.4: 1.2.1

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, $\operatorname{supp}(f+g) \subseteq [\operatorname{supp}(f) \cup \operatorname{supp}(g)]$ e $\operatorname{supp}(f \cdot g) \subseteq [\operatorname{supp}(f) \cap \operatorname{supp}(g)]$.

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

Esempio. 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 $\operatorname{supp}(f) = \mathbb{Z} \setminus \{1, 2\}$ e $\operatorname{supp}(g) = \mathbb{Z} \setminus \{1, -2\}$, ed essendo $(f+g)(x) = 2x^2 - 2x$ e $(f \cdot g)(x) = (x-1)^2(x-2)(x+2)$, abbiamo che

$$\operatorname{supp}(f+g) = \mathbb{Z} \setminus \{0, 1\} \subseteq \mathbb{Z} \setminus \{1\} = \operatorname{supp}(f) \cup \operatorname{supp}(g)$$

$$\operatorname{supp}(f \cdot g) = \mathbb{Z} \setminus \{1, \pm 2\} = \operatorname{supp}(f) \cap \operatorname{supp}(g)$$

in accordo con la *Proposizione 1.2.1.* □

Sia R un anello e sia $\mathcal{F}^{\times}(\mathcal{F}, R) = \{r\_ : \mathcal{F} \to R : |\operatorname{supp}(r\_)| < \infty\}$, 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

[13] Ricordiamo che $\operatorname{GL}(n, \mathbb{K})$ è il gruppo delle matrici $n \times n$ invertibili con entrate nel campo $\mathbb{K}$.

$r_{\underline{\alpha}} = 0$, quindi $r\_$ ha supporto finito, cioè $r\_ \in \mathcal{F}^{\times}(\mathcal{F}, R)$. Se identifichiamo $\underline{\alpha}$ con la coppia $(\alpha_1, \alpha_2) = (\underline{\alpha}(1), \underline{\alpha}(2))$,[14] possiamo quindi definire il polinomio

$$\begin{aligned} f(x,y) &= \sum_{\underline{\alpha} \in \mathcal{F}} r_{(\alpha_1,\alpha_2)} x^{\alpha_1} y^{\alpha_2} \\ &= r_{(3,0)} x^3 y^0 + r_{(2,1)} x^2 y^1 + r_{(1,2)} x^1 y^2 + r_{(3,0)} x^3 y^0 + \dots^{15} \\ &= (2 \cdot 3 - 0)x^3 + (2 \cdot 2 - 1)x^2 y + (2 \cdot 1 - 2)xy^2 + (2 \cdot 0 - 3)y^3 \\ &= 6x^3 + 3x^2 y - 3y^3. \ \square \end{aligned}$$

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

[15] 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 $r_{\underline{\alpha}} = 0$.

Possiamo procedere nella costruzione dell'anello dei polinomi nelle variabili $x_1, \dots, x_n$. Detto

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

vogliamo quindi introdurre su tale insieme delle operazioni binarie di somma e prodotto così che esso sia effettivamente un anello. Presi due elementi

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

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 1.2.5: 1.2.2

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 1.2.1* 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 1.2.1* 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 1.2.6: 1.2.3

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 $\underline{\alpha}\in\mathcal{F}$.[16] 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. ■

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

Definizione 1.2.7

Sia R un anello commutativo e sia n un intero positivo. Allora, l'insieme $R[x_1, \dots, x_n]$ è detto anello dei polinomi a coefficienti in R nelle variabili $x_1, \dots, x_n$.

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 1.2.8: 1.2.4: 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. ■