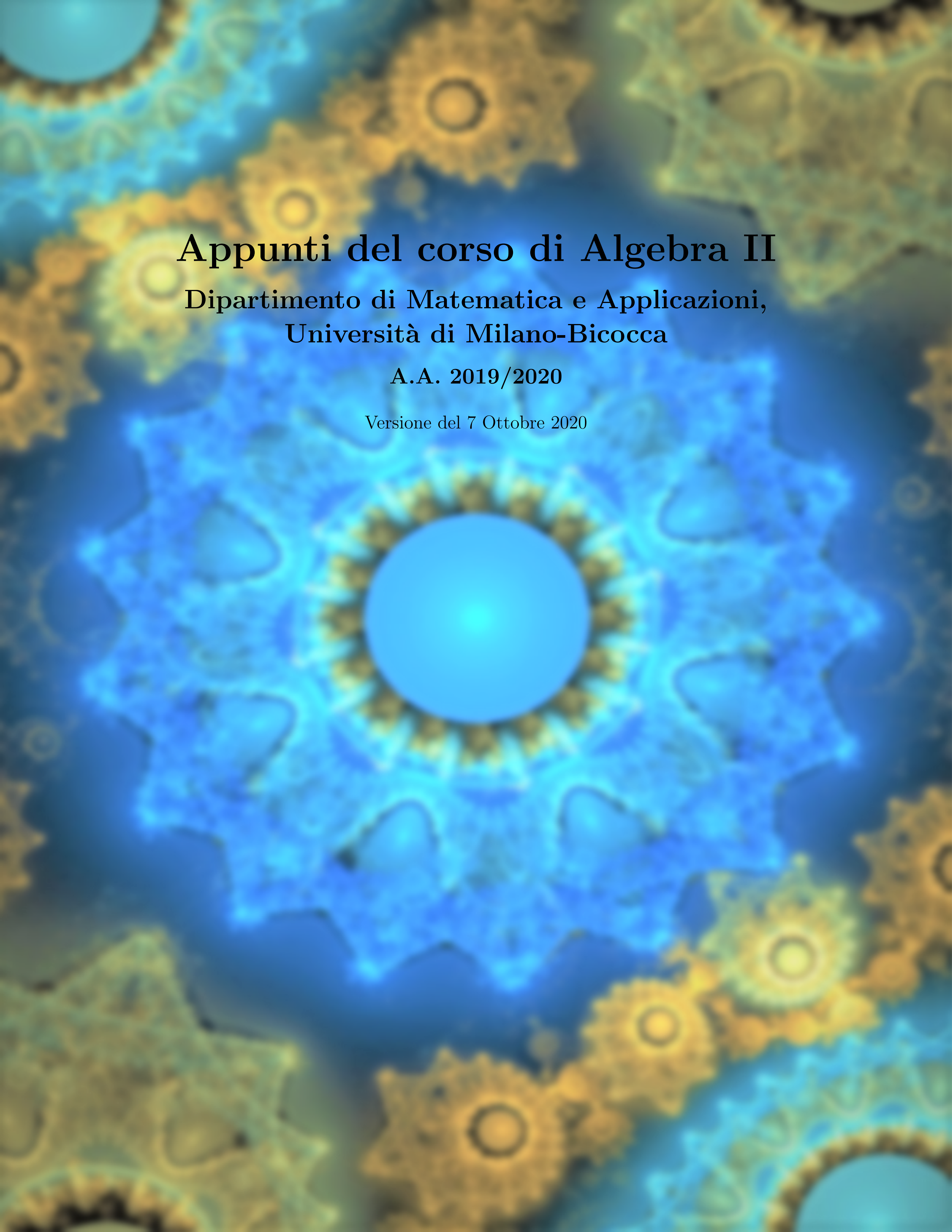

Appunti del corso di Algebra II

Dipartimento di Matematica e Applicazioni,
Università di Milano-Bicocca

A.A. 2019/2020

Versione del 7 Ottobre 2020

Indice

1 Complementi di teoria degli anelli **3**
1.1 Anelli di polinomi in una variabile 3

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

Sia R un anello[1] e sia $R[x] = \left\{ \sum_{i=0}^{n} a_i x^i : a_i \in R,\, n \in \mathbb{N}_0 \right\}$. Presi 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

$$f(x) + g(x) = \sum_{i=0}^{s} (a_i + b_i) x^i$$

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

$$f(x) \cdot g(x) = \sum_{k=0}^{m+n} c_k x^k$$

dove abbiamo posto $c_k = \sum_{i=0}^{k} a_i b_{k-i}$. [2]

Esempio 1.1.1

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

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

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

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[3] con elemento neutro il polinomio identicamente nullo $0_{R[x]} = 0_R$ e unità il polinomio costante $1_{R[x]} = 1_R$.

Di qui in seguito, denoteremo il prodotto di polinomi semplicemente come $f(x)g(x)$ o $f \cdot g$.

Definizione 1.1.2: Anellod di polinomi in una variabile

Tale insieme $R[x]$ è detto anello dei polinomi a coefficienti in R nella variabile x.

Possiamo quindi definire su $R[x]$ il concetto di "grado" di un polinomio.

[1] Useremo la convenzione secondo cui gli anelli sono commutativi unitari e $\mathbb{N} = \{1, 2, ...\}$, $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$.
[2] È solo un modo formale per definire il classico prodotto tra polinomi, come chiarificato dall'esempio.
[3] 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.[4]

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. 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 $\deg^\star(h) = \infty$. $\square$

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. [5]

Proposizione 1.1.4

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

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

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

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

[4] 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 $p(x) = 0$.

[5] 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 $\mathbb{Z}[\sqrt{2}\,] = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$.

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. 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 1.1.4 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 1.1.5

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 1.1.6

Sia R un anello. L'insieme $R^\times$ degli elementi di R che ammettono inverso moltiplicativo è un gruppo detto <u>gruppo moltiplicativo di R</u>.[6]

Se da una parte la proposizione 1.1.4 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.[7]

[6]Tale gruppo viene spesso indicato anche con $\mathcal{U}(R)$ o $R^\star$ ed è anche detto "gruppo delle unità di R".
[7]Vedremo nel *Capitolo 1.4* una generalizzazione degli anelli di polinomi con la struttura di un campo.

Infatti, $x \in R[x]$ non è un elemento invertibile perché il suo inverso $1/x$ non è un polinomio.[8] Risulta quindi naturale chiedersi quali elementi di $R[x]$ siano effettivamente invertibili.

[8] 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.

Proposizione 1.1.7

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 $R[x]^\times = R^\times$. ■

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. [9] 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.

Definizione 1.1.8

Siano R e S due anelli. Diciamo che R è <u>più piccolo</u> 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. 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 $y = x$. □

[9] 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.

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. [10] Più in generale, vale il teorema seguente.

Teorema 1.1.9: 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

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

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

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 1.1.10

Tale omomorfismo di anelli ϕ_s è detto valutazione in s.

Esempio. 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 1.1.11

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 [11] e $\alpha = \phi_t \circ \psi \colon T \to T$.

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

[11] Ricordiamo che per il *Teorema 1.1.4* tale omomorfismo è l'unico che soddisfa $\phi_t(s) = t$ e $\phi_{t_{|_R}} = \mathrm{id}_R$.

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,[12] da cui concludiamo che $T \cong R[s] \cong R[x]$.[13] ■

[12]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 $g = f^{-1}$.

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