

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
1.2 Anelli di polinomi in n variabili	9
1.3 Anelli di polinomi in più variabili	14
1.4 Polinomi di Laurent e serie formali	18
1.5 Riducibilità di polinomi	19
1.6 Anelli noetheriani	22
1.7 Localizzazione	26
1.8 Domini a valutazione discreta	33
2 Teoria dei campi	34
2.1 Estensione di campi	34
2.2 Estensioni finite	36
2.3 Campi di spezzamento	38
2.4 Campi finiti	40
3 Teoria dei moduli	42
3.1 Moduli	42
3.2 Torsione	46
3.3 Endomorfismi	50
3.4 Moduli in domini a ideali principali	52
3.5 Moduli liberi	56
3.6 Divisori elementari	60
3.7 Forma canonica di Jordan	62

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 $x^{p-1} + \dots + x + 1$
- 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 e sia $R[x] = \left\{ \sum_{i=0}^n a_i x^i : a_i \in R, n \in \mathbb{N}_0 \right\}$.¹ 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. Se prendiamo $R = \mathbb{Z}$, $f(x) = x^2 + 2x + 3$ e $g(x) = 4x + 5$, si ha che

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

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

Come visto nel corso di Algebra I, si verifica facilmente che $R[x]$ dotato di tali operazioni di somma e prodotto è un anello commutativo³ 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

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.

Definizione

Sia R un anello e sia $f(x) = \sum_{i=0}^n a_i x^i \in R[x]$. La funzione $\deg^*: R[x] \rightarrow \mathbb{N}_0 \cup \{\infty\}$ definita come $\deg^*(f) = \begin{cases} \max\{k \in \mathbb{N}_0 : a_k \neq 0_R\} & \text{se } f(x) \not\equiv 0_R \\ \infty & \text{se } f(x) \equiv 0_R \end{cases}$ è detta grado.⁴

¹Useremo la convenzione secondo cui gli anelli sono commutativi unitari e $\mathbb{N} = \{1, 2, \dots\}$, $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$.

²È solo un modo formale per definire il classico prodotto tra polinomi, come chiarificato dall'esempio.

³Infatti $a_i b_{k-i} = b_{k-i} a_i$ essendo R un anello commutativo per ipotesi, da cui $f(x) \cdot g(x) = g(x) \cdot f(x)$.

⁴Sarebbe più corretto scrivere $\deg^*(f(x))$, 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 $p(x) = 0$.

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 $\deg^*(f) = 2$ e $\deg^*(g) = 0$, ma $\deg^*(h) = \infty$. \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 1.1.1

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

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

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

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

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

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

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

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

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. \blacksquare

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, $\deg^*(f) = \deg^*(g) = 1$, ma $f(x)g(x) = 6x^2 + 7x + 2 \equiv_6 x + 2$, da cui $\deg^*(f \cdot g) = 1 \neq 2 = \deg^*(f) + \deg^*(g)$. \square

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

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 $f(x)g(x) = abx^2 = 0_Rx^2 = 0_R$, da cui, essendo $\deg^*(f) = \deg^*(g) = 1$, l'uguaglianza (\star) non vale perché

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

Dunque, per la *Proposizione 1.1.1* 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 1.1.2

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

$$(ab)(dc) = a(bd)c = a1_Rc = ac = 1_R,$$

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

Sia R un anello. L'insieme R^\times degli elementi di R che ammettono inverso moltiplicativo è un gruppo detto gruppo moltiplicativo di R .⁶

Se da una parte la *Proposizione 1.1.1* 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 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.

Proposizione 1.1.3

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

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

quindi $\deg^*(f) = \deg^*(g) = 0$ 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 $R[x]^\times = R^\times$. ■

⁶Tale gruppo viene spesso indicato anche con $\mathcal{U}(R)$ o R^* ed è anche detto “gruppo delle unità di R ”.

⁷Vedremo nel *Capitolo 1.4* una generalizzazione degli anelli di polinomi con la struttura di un campo.

⁸Più rigorosamente, se $f(x) = x$ fosse invertibile, esisterebbe $g(x) \in R[x]$ tale che $f(x)g(x) = 1_R$, da cui $\deg^*(f \cdot g) = \deg^*(1_R) = 0 = \deg^*(f) + \deg^*(g)$, cioè $\deg^*(g) = -\deg^*(f) = -1 < 0$, assurdo.

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 $\{x^0, x^1, x^2, \dots\}$ di x e tutte le combinazioni lineari tra potenze di x ed elementi di R , cioè tutti gli elementi della forma $a_n x^n + \dots + a_1 x + a_0$ 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.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 sottoanello di S isomorfo a R .

Definizione

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 $\varphi: R \rightarrow S$.

Si osservi che tale definizione è equivalente a quanto detto sopra: se esiste un monomorfismo (cioè un omomorfismo iniettivo) $\varphi: R \rightarrow S$, la restrizione $\varphi: R \rightarrow \varphi(R)$ 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 $\varphi: \mathbb{R} \rightarrow \mathbb{R}^2$, $x \mapsto (x, x)$ è un omomorfismo iniettivo, quindi \mathbb{R}^2 contiene una copia isomorfa di \mathbb{R} , che geometricamente corrisponde alla bisettrice $y = x$. \square

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 $\iota: R \rightarrow X$;
- 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 $\varphi: R \rightarrow S$ e contenente un $s \notin R$), abbiamo che X è più piccolo di S , ossia esiste un monomorfismo $\phi: X \rightarrow S$.

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 .

$$\begin{array}{ccc} R & \xrightarrow{\varphi} & S \\ \iota \downarrow & \nearrow \phi & \\ X & & \end{array}$$

⁹ Ad esempio, si verifica facilmente che la mappa $\varphi: \mathbb{C} \rightarrow \text{Mat}_{2 \times 2}(\mathbb{R})$, $a+bi \mapsto \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ è un isomorfismo di anelli, ma $\mathbb{C} \not\subseteq \text{Mat}_{2 \times 2}(\mathbb{R})$ e $\text{Mat}_{2 \times 2}(\mathbb{R}) \not\subseteq \mathbb{C}$, cioè tali anelli non sono confrontabili secondo l'inclusione.

Osserviamo ora che l'anello dei polinomi $R[x]$ soddisfa effettivamente tali proprietà. Infatti, detta $\iota: R \rightarrow R[x]$ 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 $\varphi: R \rightarrow S$, basta definire $\phi: R[x] \rightarrow S$ 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 1.1.4: Proprietà universale

Siano R e S due anelli e sia $\varphi: R \rightarrow S$ un omomorfismo. Allora, per ogni $s \in S$ esiste un unico omomorfismo di anelli $\phi: R[x] \rightarrow S$ 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 $\psi: R[x] \rightarrow S$ 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 $\varphi = \text{id}_R$ 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.

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

Definizione

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 $\phi_{\sqrt{2}}: \mathbb{Z}[x] \rightarrow \mathbb{Z}[\sqrt{2}]$ la valutazione in $\sqrt{2}$, abbiamo che $\phi_{\sqrt{2}}(f) = (\sqrt{2})^2 + 2\sqrt{2} + 3 = 5 + 2\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$. \square

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 $\varphi = \text{id}_R$ (e quindi $R \subseteq S$), ma il caso generale è del tutto analogo.

Teorema 1.1.5

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 $\psi: T \rightarrow S$ con $\psi(t) = s$ e $\psi|_R = \text{id}_R$. 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 $\phi_t: R[s] \rightarrow T$ la valutazione in t^{11} e $\alpha = \phi_t \circ \psi: T \rightarrow T$.

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

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 $\alpha|_R = \text{id}_R$. 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 $\psi': T \rightarrow T$ tale che $\psi'(t) = t$ e $\psi'|_R = \text{id}_R$. Poiché anche l'identità $\text{id}_T: T \rightarrow T$ soddisfa tali proprietà, per l'unicità di ψ' deve essere $\alpha = \text{id}_T$. Sia ora $\beta = \psi \circ \phi_t: R[s] \rightarrow R[s]$.

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

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 $\beta|_R = \text{id}_R$. Poiché anche l'identità $\text{id}_{R[s]}: R[s] \rightarrow R[s]$ soddisfa $\text{id}_{R[s]}(s) = s$ e $\text{id}_{R[s]}|_R = \text{id}_R$, e per il *Teorema 1.1.4* esiste un unico omomorfismo con queste proprietà, deve essere $\beta = \text{id}_{R[s]}$. Dunque, essendo $\phi_t \circ \psi = \text{id}_T$ e $\psi \circ \phi_t = \text{id}_{R[s]}$ isomorfismi, lo sono anche ψ e ϕ_t ,¹² da cui concludiamo che $T \cong R[s] \cong R[x]$.¹³ ■

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

¹²In generale, se $f: X \rightarrow Y$ e $g: Y \rightarrow X$ sono omomorfismi tali che $g \circ f = \text{id}_X$ e $f \circ g = \text{id}_Y$, 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 $g = f^{-1}$.

¹³Infatti 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

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:

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

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 $\underline{\alpha}: I_n \rightarrow \mathbb{N}_0$ la funzione che associa alla i -esima variabile x_i l'esponente $\underline{\alpha}(i) = \alpha_i$. Denotiamo con $x^\alpha = x_1^{\alpha_1} \cdot \dots \cdot x_n^{\alpha_n} \in M$.

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

Detto $\mathcal{F} = \mathcal{F}(I_n, \mathbb{N}_0)$ l'insieme delle funzioni $\underline{\alpha}: I_n \rightarrow \mathbb{N}_0$,¹⁴ 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 $\beta \in \mathcal{F}$ rappresenta univocamente il monomio $x_1^{\beta(1)} \cdot \dots \cdot x_n^{\beta(n)} \in M$.

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

Siano X e Y insiemi non vuoti e sia $f: X \rightarrow Y$ una funzione. Si definisce supporto di f l'insieme $\text{supp}(f) = \{x \in X : f(x) \neq 0_Y\}$.

Esempio. Sia $f: \mathbb{Z} \rightarrow \mathbb{R}$ la funzione $f(x) = x^2 - 1$. Allora, $\text{supp}(f) = \mathbb{Z} \setminus \{\pm 1\}$. \square

Se $|\text{supp}(f)| < \infty$, 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, è naturale identificare tale elemento con l'elemento neutro dell'addizione.

Esempio. Se $f: \text{Mat}_{2 \times 2}(\mathbb{F}_2) \rightarrow \mathbb{F}_2$ è il determinante, allora f ha supporto finito perché $\text{supp}(f) = \text{GL}(2, \mathbb{F}_2) = \left\{ \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \right\}$.¹⁵ \square

¹⁴In generale, dati due insiemi X e Y , si denota con $\mathcal{F}(X, Y)$ l'insieme di tutte le funzioni $f: X \rightarrow Y$.

¹⁵Ricordiamo che $\text{GL}(n, \mathbb{K})$ è il gruppo delle matrici $n \times n$ invertibili con entrate nel campo \mathbb{K} .

Proposizione 1.2.1

Siano $f, g: X \rightarrow Y$ 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. Siano $f, g: \mathbb{Z} \rightarrow \mathbb{R}$ 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 1.2.1*. □

Sia R un anello e sia $\mathcal{F}^\times(\mathcal{F}, R) = \{r_-: \mathcal{F} \rightarrow R : |\text{supp}(r_-)| < \infty\}$, 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 $M = \text{mon}\{x, y\}$ e $R = \mathbb{Z}$. Detta $r_-: \mathcal{F} \rightarrow \mathbb{Z}$ 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 esiste 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 $(\alpha_1, \alpha_2) = (\underline{\alpha}(1), \underline{\alpha}(2))$,¹⁶ possiamo quindi definire il polinomio

$$\begin{aligned} f(x, y) &= \sum_{\underline{\alpha} \in \mathcal{F}} r_{(\alpha_1, \alpha_2)} x^{\alpha_1} y^{\alpha_2} \\ &= r_{(3,0)} x^3 y^0 + r_{(2,1)} x^2 y^1 + r_{(1,2)} x^1 y^2 + r_{(3,0)} x^3 y^0 + \dots \text{¹⁷} \\ &= (2 \cdot 3 - 0)x^3 + (2 \cdot 2 - 1)x^2 y + (2 \cdot 1 - 2)xy^2 + (2 \cdot 0 - 3)y^3 \\ &= 6x^3 + 3x^2 y - 3y^3. \quad \square \end{aligned}$$

¹⁶Infatti $\mathcal{F}(I_n, \mathbb{N}_0) \cong \mathbb{N}_0^n$ mediante l'isomorfismo $\varphi: \mathcal{F}(I_n, \mathbb{N}_0) \rightarrow \mathbb{N}_0^n$, $\underline{\alpha} \mapsto (\alpha(1), \dots, \alpha(n))$.

¹⁷Tutti 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 1.2.2

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

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

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

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

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 1.2.3

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 $\underline{\alpha} \in \mathcal{F}$.¹⁸ 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. ■

¹⁸ Chiaramente si intende che $x^{\underline{0}} = x_1^0 \cdot \dots \cdot x_n^0 = 1_R \cdot \dots \cdot 1_R = 1_R$.

Definizione

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 $R \subseteq S$.

Theorema 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 $\phi_{\underline{s}}: R[x_1, \dots, x_n] \rightarrow S$ tale che $\phi_{\underline{s}}(x_i) = s_i$ per ogni $i = 1, \dots, n$ e $\phi_{\underline{s}|_R} = \text{id}_R$.

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 $\psi: R[x_1, \dots, x_n] \rightarrow S$ un altro omomorfismo di anelli tale che $\psi(x_i) = s_i$ per ogni $i = 1, \dots, n$ e $\psi|_R = \text{id}_R$. Allora, per ogni monomio $x^{\underline{\alpha}} \in M$ vale

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

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 Anelli di polinomi in più variabili

Vogliamo ora generalizzare il concetto di anello di polinomi ad un numero qualsiasi di variabili, anche infinito. Sia X un insieme non vuoto e sia $\mathcal{F}^\times = \mathcal{F}^\times(X, \mathbb{N})$ l'insieme delle funzioni $\underline{\alpha}: X \rightarrow \mathbb{N}$ che hanno supporto finito.¹⁹

Definizione

Sia X un insieme. Denotiamo con $M = \text{mon}\{X\}$ l'insieme dei monomi di X , cioè $M = \{X^\underline{\alpha} : \underline{\alpha} \in \mathcal{F}^\times\}$ dove $X^\underline{\alpha} = \prod_{x \in X} x^{\underline{\alpha}(x)}$.

Poiché abbiamo scelto $\underline{\alpha}$ con supporto finito, osserviamo che ogni monomio di X è il prodotto di un numero finito di elementi di X , anche nel caso in cui X sia un insieme infinito. Inoltre, analogamente al caso dei polinomi in n variabili, M è un monoide commutativo ed esiste una corrispondenza biunivoca tra i monomi di M e le funzioni di \mathcal{F}^\times .

Sia R un anello commutativo e sia $\mathcal{F}^\times(\mathcal{F}^\times, R) = \{f: \mathcal{F}^\times \rightarrow R : |\text{supp}(f)| < \infty\}$, cioè l'insieme delle funzioni che associano ad ogni funzione di \mathcal{F}^\times un elemento dell'anello R , e che sono diverse da 0_R solo per un numero finito elementi di \mathcal{F}^\times . Al variare di $\underline{\alpha} \in \mathcal{F}^\times$, sia $r_- \in \mathcal{F}^\times(\mathcal{F}^\times, R)$ la funzione che associa ad ogni $\underline{\alpha} \in \mathcal{F}^\times$ l'elemento $r_{\underline{\alpha}} \in R$. Osserviamo che possiamo definire un polinomio a variabili in X ponendo

$$f(X) = \sum_{\underline{\alpha} \in \mathcal{F}^\times} r_{\underline{\alpha}} X^{\underline{\alpha}}.$$

Infatti, $f(X)$ è la somma di un numero finito di monomi non nulli, ognuno con un numero finito di variabili e preceduto dal relativo coefficiente $r_{\underline{\alpha}}$.

Sia $R[X] = \left\{ \sum_{\underline{\alpha} \in \mathcal{F}^\times} r_{\underline{\alpha}} X^{\underline{\alpha}} : r_- \in \mathcal{F}^\times(\mathcal{F}^\times, R) \right\}$. Presi due elementi $f(X) = \sum_{\underline{\alpha} \in \mathcal{F}^\times} r_{\underline{\alpha}} X^{\underline{\alpha}}$ e $g(X) = \sum_{\underline{\beta} \in \mathcal{F}^\times} s_{\underline{\beta}} X^{\underline{\beta}}$ di $R[X]$, definiamo su $R[X]$ le operazioni binarie di somma e prodotto

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

$$f(X) \cdot g(X) = \sum_{\underline{\gamma} \in \mathcal{F}^\times} t_{\underline{\gamma}} X^{\underline{\gamma}}$$

dove abbiamo posto $\underline{\gamma} = \underline{\alpha} + \underline{\beta}$ e $t_{\underline{\gamma}} = \sum_{\underline{\alpha} + \underline{\beta} = \underline{\gamma}} r_{\underline{\alpha}} s_{\underline{\beta}}$. In modo del tutto analogo a quanto

visto nel caso di $R[x_1, \dots, x_n]$, si dimostra che tali operazioni sono ben poste e che $R[X]$ dotato di tali operazioni di somma e prodotto è un anello commutativo con elemento neutro il polinomio nullo $\sum_{\underline{\alpha} \in \mathcal{F}^\times} 0_{\underline{\alpha}} X^{\underline{\alpha}} = 0_R$ e unità il monomio banale $X^0 = 1_R$.

Definizione

Sia R un anello commutativo e sia X un insieme non vuoto. Allora, l'insieme $R[X]$ è detto anello dei polinomi a coefficienti in R e a variabili in X .

¹⁹Notare come a differenza dei polinomi in n variabili, ora richiediamo esplicitamente che tali funzioni $\underline{\alpha}$ abbiano supporto finito. Infatti, nel caso dei polinomi in n variabili, X è un insieme finito con n elementi, quindi ogni funzione $\underline{\alpha}: X \rightarrow \mathbb{N}$ ha in realtà supporto finito perché $\text{supp}(\underline{\alpha}) \subseteq X$, che è finito. Dunque, se $|X| < \infty$, non vi è differenza tra $\mathcal{F}^\times(X, \mathbb{N}) = \mathcal{F}(X, \mathbb{N})$.

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

Teorema 1.3.1: Proprietà universale

Sia X un insieme e sia R un anello commutativo. Allora, per ogni anello commutativo $S \supseteq R$ e per ogni mappa $\varphi: X \rightarrow S$ esiste un unico omomorfismo di anelli $\phi: R[X] \rightarrow S$ tale che $\phi(X^{\underline{\delta}_x}) = \varphi(x) \forall x \in X$ e $\phi|_R = \text{id}_R$, dove $\underline{\delta}_x: X \rightarrow \mathbb{N}$, $\underline{\delta}_x(y) = \begin{cases} 1 & \text{se } y = x \\ 0 & \text{se } y \neq x \end{cases}$

Dimostrazione. Siano $f = \sum_{\underline{\alpha} \in \mathcal{F}^\times} r_{\underline{\alpha}} X^{\underline{\alpha}}$ e $g = \sum_{\underline{\beta} \in \mathcal{F}^\times} s_{\underline{\beta}} X^{\underline{\beta}}$ due elementi di $R[X]$. Per ogni monomio $X^{\underline{\alpha}} \in M$, sia $\phi(X^{\underline{\alpha}}) = \prod_{x \in X} \varphi(x)^{\underline{\alpha}(x)}$, e sia quindi $\phi(f) = \sum_{\underline{\alpha} \in \mathcal{F}^\times} r_{\underline{\alpha}} \phi(X^{\underline{\alpha}})$. Poiché $r_{\underline{\alpha}} \in R \subseteq S$ 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, $\phi(X^{\underline{\delta}_x}) = \varphi(x)$ e $\phi(\rho) = \rho$ per ogni $\rho \in R$, quindi ϕ soddisfa le condizioni richieste.²⁰ Mostriamo ora che è un omomorfismo di anelli. Infatti,

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

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

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

perché $\phi(X^{\underline{\gamma}}) = \prod_{x \in X} \varphi(x)^{\underline{\gamma}(x)} = \prod_{x \in X} \varphi(x)^{\underline{\alpha}(x)} \cdot \prod_{x \in X} \varphi(x)^{\underline{\beta}(x)} = \phi(X^{\underline{\alpha}}) \cdot \phi(X^{\underline{\beta}})$. 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 $\psi: R[X] \rightarrow S$ un omomorfismo di anelli tale che $\psi(X^{\underline{\delta}_x}) = \varphi(x)$ e $\psi|_R = \text{id}_R$. Allora, per ogni monomio $X^{\underline{\alpha}} \in M$ vale

$$\psi(X^{\underline{\alpha}}) = \psi \left(\prod_{x \in X} x^{\underline{\alpha}(x)} \right) = \prod_{x \in X} \psi(x^{\underline{\alpha}(x)}) = \prod_{x \in X} \psi(X^{\underline{\delta}_x})^{\underline{\alpha}(x)} = \prod_{x \in X} \varphi(x)^{\underline{\alpha}(x)} = \phi(X^{\underline{\alpha}}).$$

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

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

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

In modo del tutto analogo al *Teorema 1.1.5* è possibile mostrare che, a meno di isomorfismi, $R[X]$ è l'unico anello contenente R avente questa proprietà.

²⁰ $\underline{\delta}_x$ è la funzione tale che per ogni $x \in X$ si abbia $X^{\underline{\delta}_x} = x$. Infatti, $X^{\underline{\delta}_x} = \prod_{y \in X} y^{\underline{\delta}_x(y)} = x^{\underline{\delta}_x(x)} = x^1 = x$ perché tutti gli altri termini del prodotto hanno esponente 0, essendo per definizione $\underline{\delta}_x(y) = 0$ 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. 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 $q(y) = (x)y^2 + (2x + 3)y + 4 \in (\mathbb{Z}[x])[y]$. \square

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,²¹ vale il teorema seguente.

Teorema 1.3.2

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 $\varphi_X: X \rightarrow S$ definita come $\varphi_X(x) = X^{\delta_x}$. Presa una qualunque funzione $\varphi_Y: Y \rightarrow S$, sia $\tilde{\varphi}: X \sqcup Y \rightarrow S$ l'unica mappa tale che $\tilde{\varphi}|_X = \varphi_X$ e $\tilde{\varphi}|_Y = \varphi_Y$. Allora, per il Teorema 1.3.1 esiste un unico omomorfismo $\tilde{\phi}: R[X \sqcup Y] \rightarrow S$ tale che $\tilde{\phi}(Z^{\delta_z}) = \tilde{\varphi}(z)$ per ogni $z \in X \sqcup Y$ e $\tilde{\phi}|_R = \text{id}_R$. Per ogni $\underline{\alpha} \in \mathcal{F}^\times(X, \mathbb{N})$, sia $\tilde{\underline{\alpha}} \in \mathcal{F}^\times(X \sqcup Y, \mathbb{N})$ l'unica funzione tale che $\tilde{\underline{\alpha}}|_X = \underline{\alpha}$ e $\tilde{\underline{\alpha}}|_Y = \underline{0}$. Allora, possiamo pensare ogni monomio $X^\underline{\alpha}$ di $R[X]$ come monomio $Z^{\tilde{\underline{\alpha}}}$ di $R[X \sqcup Y]$, da cui

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

per come abbiamo definito $\tilde{\varphi}$ e $\tilde{\underline{\alpha}}$ ed usando il fatto che $\tilde{\phi}$ 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 $\tilde{f} = \sum_{\tilde{\underline{\alpha}} \in \mathcal{F}^\times} r_{\tilde{\underline{\alpha}}} Z^{\tilde{\underline{\alpha}}} \in R[X \sqcup Y]$ si ha che

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

perché $\tilde{\phi}(r_{\tilde{\underline{\alpha}}}) = r_{\tilde{\underline{\alpha}}}$ essendo $\tilde{\phi}|_R = \text{id}_R$, da cui $\tilde{\phi}|_{R[X]} = \text{id}_{R[X]}$. Inoltre, per ogni $y \in Y$ si ha che $\tilde{\phi}(Z^{\delta_y}) = \tilde{\varphi}(y) = \varphi_Y(y)$. Poiché $R[X \sqcup Y]$ è un anello commutativo contenente $R[X]$ che soddisfa la proprietà universale di $(R[X])[Y]$,²² per la generalizzazione del Teorema 1.1.5 possiamo effettivamente concludere che $R[X \sqcup Y] \simeq (R[X])[Y]$. \blacksquare

²¹ 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 $A_0 \sqcup A_1 = \{(3, 0), (4, 0), (5, 0), (5, 1), (6, 1)\}$.

²² Infatti, abbiamo appena mostrato che per ogni anello $S \supseteq R[X]$ e per ogni mappa $\varphi_Y: Y \rightarrow S$, esiste un unico omomorfismo $\tilde{\phi}: R[X \sqcup Y] \rightarrow S$ tale che $\tilde{\phi}(Z^{\delta_y}) = \varphi_Y(y)$ per ogni $y \in Y$ e $\tilde{\phi}|_{R[X]} = \text{id}_{R[X]}$.

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

Corollario 1.3.3

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 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 $f \in R[X_f]$.²³

Proposizione 1.3.4

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.²⁴ Per fare ciò, procediamo per induzione sul numero di variabili. Se $n = 1$, per la Proposizione 1.1.1 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 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 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. ■

²³Più formalmente, preso $f = \sum_{\underline{\alpha} \in \mathcal{F}^\times} r_{\underline{\alpha}} X^{\underline{\alpha}} \in R[X]$ sappiamo che $\Omega_f = \text{supp}(r_-) \subseteq \mathcal{F}^\times$ 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, $X_f = \bigcup_{\underline{\alpha} \in \Omega_f} \text{supp}(\underline{\alpha})$ è finito in quanto unione finita di insiemi finiti.

²⁴Se 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.

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.

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

Sketch del capitolo: Polinomi di Laurent ma le dim sono triviali 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

Sia R un dominio di integrità e sia $f(x) \in R[x]$ un polinomio non invertibile²⁵ 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 $\deg^*(f) = 1 = \deg^*(g) + \deg^*(h)$. 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 $\mathbb{Z}[x]$. \square

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 $\deg^*(f)$.

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 $\mathbb{C}[x]$. \square

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 1.5.1: 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 $\deg^*(f)$ tali che $f(x) = g(x)h(x)$. Poiché per ipotesi $\deg^*(g) + \deg^*(h) = \deg^*(f) \leq 3$, 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, $a = -a^{-1}b \in \mathbb{K}$, 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 $\deg^*(q) = \deg^*(f) - \deg^*(x - \alpha) \geq 2 - 1 = 1$, si ha che $f(x)$ è riducibile in $\mathbb{K}[x]$. \blacksquare

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 $n = 0, 1, \dots, p-1$.

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 . \square

²⁵Si intende rispetto al prodotto, cioè per la *Proposizione 1.1.2* prendiamo $f(x) \notin R^\times$.

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 $\mathbb{R}[x]$. \square

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

Definizione

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 $\text{MCD}(a_0, \dots, a_n)$. Un polinomio si dice primitivo se il suo contenuto è 1.

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

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 $\text{MCD}(2, 5, 3) = 1$. Questo è un fatto generale, come dimostrato dal lemma seguente.

Lemma 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. \blacksquare

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

Teorema 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 $ag(x) = c_1g'(x)$ e $bh(x) = c_2h'(x)$, dove $g'(x)$ e $h'(x)$ sono polinomi primitivi. Poiché $abf(x) = ag(x)bh(x) = c_1c_2g'(x)h'(x)$ e per il *Lemma 1.5.2* anche $g'(x)h'(x)$ è primitivo, deve essere $ab = c_1c_2$. 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. \blacksquare

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.

1.6 Anelli noetheriani

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 ideale²⁶ di R . 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 $x + y = \sum_{i=1}^n (r_i + s_i) a_i \in I$ e $tx = t \sum_{i=1}^n r_i a_i = \sum_{i=1}^n (tr_i) a_i \in I$ per ogni $t \in R$, da cui $I \triangleleft R$.

Definizione

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 $k \in \mathbb{Z}$. \square

Definizione

Dato un ideale $I \triangleleft R$, definiamo numero minimo di generatori $d_R(I)$ il più piccolo $n \in \mathbb{N}$ per cui esistono $a_1, \dots, a_n \in R$ 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 $I \triangleleft R$ è finitamente generato se $d_R(I) < \infty$.

Esempio. Sia $I = \langle 2, x \rangle \triangleleft \mathbb{Z}[x]$ 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 $\deg^*(f) = 0$, cioè $f(x) \equiv k$, allora k è pari e I contiene solo polinomi con coefficienti pari, da cui $x \notin I$, assurdo. Se $\deg^*(f) \geq 1$, allora I contiene solo polinomi di grado almeno 1, cioè $2 \notin I$, assurdo. Dunque $d_{\mathbb{Z}[x]}(I) = 2$. \square

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

Definizione

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

Esempio. Sia R un dominio ad ideali principali.²⁷ Allora, R è un anello noetheriano poiché per definizione di PID si ha che $d_R(I) = 1$ per ogni $I \triangleleft R$ 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 $\mathbb{K} = \langle 1_{\mathbb{K}} \rangle$. \square

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 $k \in \mathbb{N}$.

²⁶Ricordiamo 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 $a - b \in I \Leftrightarrow a + c \in I$.

²⁷Ricordiamo 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} .

Proposizione 1.6.1

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 ,²⁸ 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 $N = \max\{k_i : 1 \leq i \leq n\}$, 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 $I_N \subseteq I_{N+j} \forall j \in \mathbb{N}$. Combinando le doppie inclusioni, si ha quindi che $I_{N+j} = I_N \forall j \in \mathbb{N}$.

Viceversa, supponiamo per assurdo che esista $J \triangleleft R$ 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 $I_k \subsetneq I_{k+1}$. 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 1.6.2: Teorema della base di Hilbert

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

Dimostrazione. Supponiamo per assurdo che $R[x]$ non sia noetheriano, e sia quindi $J \triangleleft R[x]$ 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 $d_k = \deg^*(f_k)$ 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 1.4.1* 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 $h = f_{N+1} - \sum_{i=0}^N r_i x^{d_{N+1}-d_i} f_i \in J$.²⁹

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 $\deg^*(h) < d_{N+1}$, 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. ■

²⁸Siano $a, b \in I_\infty$ con $a \in I_s$ e $b \in I_t$, dove $s \leq t$,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 $I_\infty \triangleleft R$.

²⁹Vogliamo 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.

Corollario 1.6.3

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 1.6.2 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 1.3.3 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 dominio di integrità noetheriano e sia $X = \{x_n : n \in \mathbb{N}\}$ un insieme numerabile di variabili. Per la Proposizione 1.3.4 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 1.6.1, 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 1.6.4

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

Dimostrazione. Siano $J \triangleleft S$ e $I = \phi^{-1}(J) = \{r \in R : \phi(r) \in J\}$. Poiché I è un ideale di R ,³⁰ 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 1.4.2 anche $\mathbb{Z}[x]$ è noetheriano. Sia $\phi_{\sqrt{2}}: \mathbb{Z}[x] \rightarrow \mathbb{Z}[\sqrt{2}]$ 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 1.6.4 anche $\mathbb{Z}[\sqrt{2}]$ è noetheriano. □

Un caso particolare della Proposizione 1.6.4 vale per gli anelli quoziante.

Corollario 1.6.5

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

Dimostrazione. Sia $\pi: R \rightarrow R/I$, $\pi(r) = r + I$ la proiezione canonica sul quoziante. Poiché π è un omomorfismo suriettivo, per la Proposizione 1.6.4 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 1.6.5 anche $\mathbb{Z}/4\mathbb{Z}$ è noetheriano.³¹ Tuttavia, esso non è dominio di integrità perché ha divisori dello zero: infatti, $2 \cdot 2 = 0$. □

³⁰In generale, se $\varphi: A \rightarrow B$ è un omomorfismo e $J \triangleleft B$, allora $I = \varphi^{-1}(J) = \{a \in A : \varphi(a) \in J\} \triangleleft A$. 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 $I \triangleleft A$.

³¹In realtà basta osservare che ogni anello finito è noetheriano poiché $d_R(I) \leq |R| < \infty$ per ogni $I \triangleleft R$.

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.

1.7 Localizzazione

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

Definizione

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

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

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

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

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

Proposizione 1.7.1

La relazione $\sim: (R \times S) \times (R \times S) \rightarrow \{\text{v, f}\}$ è una relazione di equivalenza.³²

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

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

Definizione

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

Il termine “localizzazione” deve il suo nome alla geometria algebrica.³³ 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.

³²La 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.

³³Se R è un anello di funzioni definito su un oggetto geometrico (come una varietà algebrica, cioè l’insieme delle soluzioni di un sistema di equazioni polinomiali) e vogliamo studiare tale varietà in un certo punto x_0 , definiamo S come l’insieme delle funzioni che non si annullano in x_0 e localizziamo R a S . Allora, $S^{-1}R$ è un anello generalmente più semplice di R che contiene informazioni solo sul comportamento della varietà in un intorno di x_0 , da cui l’origine del termine “locale”.

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

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

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

Lemma 1.7.2: Lemma della forbice

Siano X e Y insiemi non vuoti e sia $f: X \rightarrow Y$ una mappa. Sia \sim una relazione di equivalenza su X e $\tau: X \rightarrow X/\sim$ la proiezione canonica.³⁴ Allora, esiste una mappa $\bar{f}: X/\sim \rightarrow Y$ tale che $\bar{f} = f \circ \tau$ 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,³⁵ esiste $\sigma: X/\sim \rightarrow X$ tale che $\sigma([x]) \sim x$ per ogni $x \in X$ e $\tau \circ \sigma = \text{id}_{X/\sim}$. Si consideri ora la funzione $\bar{f} = f \circ \sigma: X/\sim \rightarrow Y$.

$$\begin{array}{ccc} X & \xrightarrow{f} & Y \\ \uparrow \tau & \nearrow \sigma & \searrow \bar{f} \\ X/\sim & & \end{array}$$

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

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

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

$$\begin{array}{ccc} (R, S) \times (R, S) & \xrightarrow{\tilde{+}} & S^{-1}R \\ & \searrow \tau & \swarrow \oplus \\ & S^{-1}R \times S^{-1}R & \end{array}$$

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 $(r, s) \tilde{+} (t, u) = (r', s') \tilde{+} (t', u')$, 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 $\frac{ru+st}{su} = \frac{r'u'+s't'}{s'u'}$.

³⁴Cioè la mappa che manda ogni elemento $x \in X$ nella sua classe di equivalenza $[x]_\sim$, che per comodità di notazione denoteremo di qui in seguito semplicemente con $[x]$.

³⁵L'assioma della scelta afferma che data una famiglia non vuota di insiemi non vuoti, esiste una funzione che ad ogni insieme della famiglia fa corrispondere un suo elemento. Per poter dimostrare questo lemma è necessario assumere tale assioma, di cui si fa uso nel definire la funzione σ , che altrimenti a priori non esisterebbe. Infatti, X/\sim è la famiglia delle classi di equivalenza di X , ognuna delle quali è non vuota poiché $x \in [x]$, e σ è la funzione che ad ogni classe $[x] \in X/\sim$ fa corrispondere un suo rappresentante $\sigma([x]) \in X$.

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

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

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

Per comodità di notazione, denoteremo di qui in seguito le due operazioni \oplus e \odot di $S^{-1}R$ semplicemente con $+$ e \cdot , rispettivamente.³⁶

Proposizione 1.7.3

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

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

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

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

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

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

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

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

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

$$\begin{aligned} \iota_R(x+y) &= \frac{x+y}{1_R} = \frac{x}{1_R} + \frac{y}{1_R} = \iota_R(x) + \iota_R(y) \\ \iota_R(xy) &= \frac{xy}{1_R} = \frac{x}{1_R} \cdot \frac{y}{1_R} = \iota_R(x) \cdot \iota_R(y) \end{aligned}$$

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.

³⁶Per quanto appena provato, possiamo effettivamente vedere tali operazioni come somma e prodotto di "frazioni" con le usuali regole di calcolo delle frazioni.

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

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

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

Esempio. Sia R un dominio di integrità e sia $\mathfrak{p} \triangleleft R$ un ideale primo.³⁷ 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,³⁸ 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 $S^{-1}(R \setminus \mathfrak{p}) \cap S^{-1}\mathfrak{p} = \emptyset$.³⁹ Sia ora $\frac{r}{s} \in S^{-1}(R \setminus \mathfrak{p})$; allora, anche $\frac{s}{r} \in S^{-1}(R \setminus \mathfrak{p})$ e $\frac{r}{s} \cdot \frac{s}{r} = \frac{1_R}{1_R} = 1_{S^{-1}R}$, cioè $\frac{r}{s}$ è invertibile, da cui $S^{-1}(R \setminus \mathfrak{p}) \subseteq (S^{-1}R)^\times$. D'altra parte, se esistesse $\frac{r}{s} \in S^{-1}\mathfrak{p}$ invertibile, detto $\frac{t}{u} \in S^{-1}R$ il suo inverso si avrebbe $rt = su \in \mathfrak{p}$, il che è assurdo poiché $s, u \in S = R \setminus \mathfrak{p}$ violando la definizione di ideale primo. Dunque $(S^{-1}R)^\times \subseteq S^{-1}(R \setminus \mathfrak{p})$, da cui $S^{-1}R = S^{-1}(R \setminus \mathfrak{p}) \sqcup S^{-1}\mathfrak{p} = (S^{-1}R)^\times \sqcup S^{-1}\mathfrak{p}$. \square

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

Definizione

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

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

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

Proposizione 1.7.4

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

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

³⁷Un ideale proprio $\mathfrak{p} \triangleleft R$ si dice primo se, presi $a, b \in R$, si ha che $ab \in \mathfrak{p}$ se e solo se $a \in \mathfrak{p}$ o $b \in \mathfrak{p}$.

³⁸In generale, se un ideale $I \triangleleft R$ contiene l'unità 1_R , allora $r = r1_R \in I$ per ogni $r \in R$, cioè $I = R$.

³⁹Sia $\frac{r}{s} \in S^{-1}\mathfrak{p}$; 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 $s, t \in S = R \setminus \mathfrak{p}$.

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

Proposizione 1.7.5

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

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

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

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

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

Proposizione 1.7.6

Sia S un sistema moltiplicativo di un dominio di integrità R . Presi $I \triangleleft R$ e $J \triangleleft S^{-1}R$,

- (a) $S^{-1}I \triangleleft S^{-1}R$ e $S^{-1}I = S^{-1}R$ se e solo se $I \cap S \neq \emptyset$;
- (b) $\bar{J} \triangleleft R$ e $S^{-1}\bar{J} = J$.

Dimostrazione. (a) Siano $\frac{i}{s}, \frac{j}{t} \in S^{-1}I$. Allora, $\frac{i}{s} + \frac{j}{t} = \frac{it+js}{st} \in S^{-1}I$ perché $it+js \in I$ per definizione di ideale e $st \in S$ per definizione di sistema moltiplicativo. Analogamente, $\frac{i}{s} \cdot \frac{j}{t} = \frac{ij}{st} \in S^{-1}I$ perché $ij \in I$ e $st \in S$, da cui $S^{-1}I$ è effettivamente un ideale di $S^{-1}R$. Osserviamo ora che se $S^{-1}I = S^{-1}R$, in particolare esiste un elemento $\frac{i}{s} \in S^{-1}I$ tale che $\frac{i}{s} = 1_{S^{-1}R} = \frac{1_R}{1_R}$. Dunque, $i = i(1_R) = s(1_R) = s$, cioè $i = s \in I \cap S$, da cui $I \cap S \neq \emptyset$. Viceversa, supponiamo che $I \cap S \neq \emptyset$. Preso $t \in I \cap S$, si ha che $\frac{t}{t} = \frac{1_R}{1_R} = 1_{S^{-1}R} \in S^{-1}I$, da cui, essendo $S^{-1}I$ un ideale, $\frac{r}{s} \cdot \frac{1_R}{1_R} = \frac{r}{s} \in S^{-1}I$ per ogni $\frac{r}{s} \in S^{-1}R$, cioè $S^{-1}I = S^{-1}R$.

(b) Poiché $\iota_R: R \hookrightarrow S^{-1}R$ è un omomorfismo, la preimmagine $\iota_R^{-1}(J) \subseteq R$ di un ideale $J \triangleleft S^{-1}R$ è un ideale di R , cioè $\bar{J} \triangleleft R$. Preso $\frac{i}{s} \in S^{-1}\bar{J}$, per definizione si ha che $\frac{i}{s} \in J$. Quindi, essendo J un ideale, $\frac{i}{s} = \frac{1_R}{s} \cdot \frac{i}{1_R} \in J$, da cui $S^{-1}\bar{J} \subseteq J$. D'altra parte, preso $\frac{r}{s} \in J$, per definizione di ideale si ha che $\frac{s}{1_R} \cdot \frac{r}{s} = \frac{r}{1_R} \in J$, cioè $r \in \bar{J}$. Dunque risulta $\frac{r}{s} \in S^{-1}\bar{J}$, da cui $J \subseteq S^{-1}\bar{J}$. Combinando le doppie inclusioni, si ha quindi che $S^{-1}\bar{J} = J$. ■

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

Corollario 1.7.7

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

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

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

Definizione

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

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

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

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

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

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

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

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

Esempio. Esempio. □

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

Proposizione 1.7.8

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

Dimostrazione. Osserviamo innanzitutto che $\mathfrak{m} \triangleleft R$ è massimale perché, preso $I \triangleleft R$ tale che $\mathfrak{m} \subsetneq I$, si ha che $I \setminus \mathfrak{m} \neq \emptyset$, cioè $I \cap R^\times \neq \emptyset$, da cui $I = R$ poiché I contiene un elemento invertibile.⁴⁰ D'altra parte, se $J \triangleleft R$ è un ideale massimale, per quanto appena visto deve essere $J \cap R^\times = \emptyset$, cioè $J \subseteq R \setminus R^\times = \mathfrak{m}$ che è già massimale, da cui $J = \mathfrak{m}$ e \mathfrak{m} è unico. ■

⁴⁰Infatti, se I contiene $r \in R^\times$, detto r^{-1} il suo inverso si ha che $r^{-1}r = 1_R \in I$, da cui $I = R$.

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

Proposizione 1.7.9

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

Dimostrazione. Sia $n = p^k$ con p primo e $k \geq 1$ intero. Osserviamo che $a + p^k\mathbb{Z} \in (\mathbb{Z}/p^k\mathbb{Z})^\times$ se e solo se esiste $b \in \mathbb{Z}$ tale che $ab \in 1 + p^k\mathbb{Z}$, cioè $ab \equiv 1 \pmod{p^k}$. In particolare, vale $ab \equiv 1 \pmod{p}$, da cui per l'*Identità di Bézout* si ha che $\text{MCD}(a, p) = 1$.⁴¹ Si ha quindi che $(\mathbb{Z}/p^k\mathbb{Z})^\times = \{a + p^k\mathbb{Z} : \text{MCD}(a, p) = 1\}$, da cui $\mathfrak{m} = \mathbb{Z}/p^k\mathbb{Z} \setminus (\mathbb{Z}/p^k\mathbb{Z})^\times = p\mathbb{Z}/p^k\mathbb{Z}$ è un ideale di $\mathbb{Z}/p^k\mathbb{Z}$.⁴² Dunque, $\mathbb{Z}/p^k\mathbb{Z}$ è effettivamente un anello locale.

Viceversa, supponiamo per assurdo che esistano $p \neq q$ primi con $p \mid n$ e $q \mid n$. Poiché per il *Terzo teorema d'isomorfismo* sappiamo che $(\mathbb{Z}/n\mathbb{Z})/(p\mathbb{Z}/n\mathbb{Z}) \simeq \mathbb{Z}/p\mathbb{Z}$ che è un campo, $p\mathbb{Z}/n\mathbb{Z} \triangleleft \mathbb{Z}/n\mathbb{Z}$ è un ideale massimale.⁴³ Analogamente, anche $q\mathbb{Z}/n\mathbb{Z} \triangleleft \mathbb{Z}/n\mathbb{Z}$ è massimale, ed essendo $p \neq q$ tali ideali sono distinti.⁴⁴ Abbiamo quindi trovato due ideali massimali distinti di $\mathbb{Z}/n\mathbb{Z}$, da cui per la *Proposizione 1.7.8* concludiamo che $\mathbb{Z}/n\mathbb{Z}$ non è locale. ■

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

Definizione

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

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

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

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

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

Proposizione 1.7.10

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

Dimostrazione. Dim ■

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

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

⁴¹ Secondo l'*Identità di Bézout*, dati due interi a, b non entrambi nulli e detto $d = \text{MCD}(a, b)$, esistono $x, y \in \mathbb{Z}$ tali che $ax + by = d$, e d è il più piccolo intero che può essere scritto in questa forma. In questo caso, essendo $ab \equiv 1 \pmod{p}$, esiste $t \in \mathbb{Z}$ tale che $ab + pt = 1$, dunque $\text{MCD}(a, p) \leq 1$, cioè $\text{MCD}(a, p) = 1$.

⁴² 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 $\text{MCD}(a, p) > 1$, cioè, essendo p primo, $\text{MCD}(a, p) = p$. Dunque, $\mathfrak{m} = \{a + p^k\mathbb{Z} : p \mid a\} = p\mathbb{Z}/p^k\mathbb{Z} \triangleleft \mathbb{Z}/p^k\mathbb{Z}$.

⁴³ Ricordiamo che preso un ideale $I \triangleleft R$, l'anello quoziante R/I è un campo se e solo se I è massimale.

⁴⁴ Infatti, sono ideali finiti contenenti un numero diverso di elementi, essendo $|p\mathbb{Z}/n\mathbb{Z}| = \frac{n}{p} \neq \frac{n}{q} = |q\mathbb{Z}/n\mathbb{Z}|$.

1.8 Domini a valutazione discreta

Controllare la correttezza degli appunti delle lezioni del 22-23/10/2019 prima di copiare qui quella parte (incluso l'esempio sulla metrica p-adica).

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

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. \square

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 $\cdot : \mathbb{L} \times \mathbb{L} \rightarrow \mathbb{L}$ 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

Sia \mathbb{L}/\mathbb{K} un'estensione di campi. Definiamo grado dell'estensione \mathbb{L}/\mathbb{K} la dimensione⁴⁵ $\dim_{\mathbb{K}}(\mathbb{L}) \in \mathbb{N} \cup \{\infty\}$ 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. \square

Definizione

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 \square

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

⁴⁵Ricordiamo 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.

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

Definizione

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

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 irriducibile.

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

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 $\text{Im}(\phi_a) = \mathbb{K}[a] \subseteq \mathbb{K}(a)$. 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.

2.2 Estensioni finite

Lezioni del 05-06/11/2019 (appunti grezzi)

Definizione

Un'estensione di campi \mathbb{L}/\mathbb{K} si dice finita se $|\mathbb{L} : \mathbb{K}| < \infty$.

Proposizione

Sia \mathbb{L}/\mathbb{K} un'estensione finita. Allora, ogni elemento $a \in \mathbb{L}$ è algebrico su \mathbb{K} .

Dimostrazione. Sia $\phi_a: \mathbb{K}[x] \rightarrow \mathbb{L}$ la valutazione in a . Poiché $\dim_{\mathbb{K}} \mathbb{K}[x] = \infty$ (una base sono tutti i monomi $1, x, x^2, \dots$) e $|\mathbb{L} : \mathbb{K}| = \dim_K(\mathbb{L}) < \infty$, ϕ_a non è iniettiva, cioè $\ker(\phi_a) \neq \{0_K\}$. Dunque, per $f \in \ker(\phi_a) \setminus \{0_K\}$, si ha $f(a) = \phi_a(f) = 0$. ■

Proposizione

Sia \mathbb{L}/\mathbb{K} un'estensione di campi, e sia $a \in \mathbb{L}$. Allora, sono equivalenti

- (i) a è algebrico su \mathbb{K}
- (ii) $|\mathbb{K}(a) : \mathbb{K}| < \infty$
- (iii) esiste un'estensione finita M/\mathbb{K} , $M \subseteq \mathbb{L}$ tale che $a \in M$

Dimostrazione. Per la proposizione precedente, sappiamo già che (iii) implica (i). Vediamo che (i) implica (ii). Infatti, $K[a] = \text{Im}(\phi_a) \simeq K[x]/\ker(\phi_a)$ è un campo, e $K(a) = K[a]$ implica che $|K[a] : K| = |K[a] : K| = \deg^*(\min_{a,K}) < \infty$. Mostriamo ora che non (i) implica non (ii). Infatti, non (i) sse a è trascendente su \mathbb{K} . Quindi, $\phi_a: K[x] \rightarrow \mathbb{L}$ è iniettiva, e $K(a) \supseteq \text{im}(\phi_a) \simeq K[x]$ perché $K(a)$ contiene il sottospazio vettoriale $\text{im}(\phi_a)$ e $\dim_K(K(a)) = \infty$. Dunque, il fatto che (i) implica (ii) e non (i) implica non (ii), sappiamo che (i) se e solo se (ii). Ma (ii) implica (iii) è banale: infatti prendo $M = K(a)$. ■

Definizione

Sia \mathbb{L}/\mathbb{K} un'estensione di campi. Denotiamo con $\text{alg}_{\mathbb{K}}(\mathbb{L})$ l'insieme degli elementi $a \in \mathbb{L}$ algebrici su \mathbb{K} .

Proposizione

Sia \mathbb{L}/\mathbb{K} un'estensione di campi. Allora, $\text{alg}_{\mathbb{K}}(\mathbb{L})$ è un sottocampo di \mathbb{L} .

Dimostrazione. Siano $a, b \in \text{alg}_{\mathbb{K}}(\mathbb{L})$. Basta dimostrare che $a+b, ab$ e a^{-1} stanno in $\text{alg}_{\mathbb{K}}(\mathbb{L})$. Poiché $a \in \text{alg}_{\mathbb{K}}(\mathbb{L})$, per la proposizione 2 sappiamo che $|K(a) : K| < \infty$. Poiché $b \in \text{alg}_{\mathbb{K}}(\mathbb{L})$, esiste $\min_{b,K}(x) \in K[x] \subseteq K(a)[x]$. Dunque, b è algebrico su $K(a)$, da cui

$$|K(\{a, b\}) : K| = |K(a)(b) : K(a)| \cdot |K(a) : K| < \infty$$

per la Formula del grado. Poiché $a+b, ab, a^{-1} \in K(\{a, b\})$, per la Proposizione 2 sappiamo che $a+b, ab, a^{-1} \in \text{alg}_{\mathbb{K}}(\mathbb{L})$. ■

Trovare esplicitamente i polinomi che annullano $a+b, ab$ e a^{-1} sarebbe stato un incubo!

Definizione

Un campo \mathbb{K} si dice algebricamente chiuso se ogni polinomio $f \in \mathbb{K}[x]$ con $\deg^*(f) \geq 1$ ammette una radice.

Esempio. Per il Teorema Fondamentale dell'Algebra (lui dice Teorema di Gauss) sappiamo che \mathbb{C} è un campo algebricamente chiuso. La dimostrazione è tutt'altro che banale e richiede o l'analisi complessa o la Teoria di Galois. \square

Denotiamo con $\overline{\mathbb{Q}} = \text{alg}_{\mathbb{Q}}(\mathbb{C})$.

Proposizione

$\overline{\mathbb{Q}}$ è un campo algebricamente chiuso.

Dimostrazione. Sia $f = \sum_{i=0}^n a_i x^i \in \overline{\mathbb{Q}}[x]$ con $\deg^*(f) \geq 1$. Poiché $f \in \mathbb{C}[x]$ essendo $\overline{\mathbb{Q}} \subseteq \mathbb{C}$, per il Teorema Fondamentale dell'Algebra esiste $c \in \mathbb{C}$ tale che $f(c) = 0$. Definiamo $M = \overline{\mathbb{Q}}(\{a_0, a_1, \dots, a_n\})$. Allora, per la formula del grado

$$|M : Q| = |M : Q(\{a_0, \dots, a_{n-1}\})| \cdot |Q(\{a_0, \dots, a_{n-1}\}) : Q(\{a_0, \dots, a_{n-2}\})| \cdot \dots$$

Ma sappiamo che $|M : Q(\{a_0, \dots, a_{n-1}\})| \leq \deg^*(\min_{a_n, Q})$ e induttivamente $|M : Q| \leq \prod_{i=0}^n \deg^*(\min_{a_i, Q})$. Quindi, $|M(c) : Q| = |M(c) : M| \cdot |M : Q|$, dove $|M(c) : M| \leq n$ e $|M : Q| \leq \infty$. Dunque, per la Proposizione 2 concludiamo che $c \in \overline{\mathbb{Q}}$. \blacksquare

Proposizione 2.X.Y: Costruzione di Kronecker

Sia \mathbb{K} un campo e sia $f \in \mathbb{K}[x]$ con $\deg^*(f) \geq 1$. Allora, esiste un'estensione \mathbb{L}/\mathbb{K}_0 finita e un elemento $a \in \mathbb{L}$ tale che $f(a) = 0$, dove $\mathbb{K}_0 \simeq \mathbb{K}$.

Dimostrazione. Poiché $K[x]$ è un dominio principale, possiamo scrivere $f = h \cdot f_0$ dove $h \in K[x]$ è primo e dunque irriducibile. Definiamo $L = K[x]/\langle h \rangle$. Poiché $\langle h \rangle \triangleleft K[x]$ è un ideale massimale, tale L è un campo. Definiamo $K_0 = \{b + \langle h \rangle : b \in K\}$, cioè $K_0 = \pi(K)$, dove $\pi: K[x] \rightarrow L$ è la proiezione canonica. Poiché $\langle h \rangle$ è un ideale primo, $K \cap \langle h \rangle \{0_K\}$, quindi la restrizione $\pi_K: K \rightarrow K_0$ è un isomorfismo. Inoltre, $|L : K_0| = \deg^*(h) < \deg^*(f) < \infty$, quindi abbiamo trovato un'estensione finita. Sia $h = \sum_{k=0}^n a_k x^k$, e sia $I = \langle h \rangle$. Detto $a = x + I \in L$, si ha che

$$h(a) = \sum_{k=0}^n a_k (x + I)^k = \sum_{k=0}^n a_k (x^k + I) = \left(\sum_{k=0}^n a_k x^k \right) + I = h + I = I = O_L.$$

Questo mostra che per ogni polinomio troviamo $a \in L$ tale che $f(a) = 0$, come desiderato. \blacksquare

2.3 Campi di spezzamento

Definizione

Sia \mathbb{K} un campo e sia $f \in \mathbb{K}[x]$ con $\deg^*(f) = n \geq 1$. Un'estensione di campi \mathbb{L}/\mathbb{K} si dice campo di spezzamento di $f \in \mathbb{K}[x]$ se esistono $c_1, \dots, c_n \in \mathbb{L}$ e $c_f \in \mathbb{K}$ tali che:

- (i) $f(x) = c_f \prod_{i=1}^n (x - c_i) \in \mathbb{L}[x]$;
- (ii) $\mathbb{L} = \mathbb{K}(\{c_1, \dots, c_n\})$.

La condizione (i) ci dice che f si spezza in fattori lineari su $\mathbb{L}[x]$, e la condizione (ii) serve a limitare la grandezza di \mathbb{L} .

Il Teorema seguente è il teorema di esistenza e unicità del campo di spezzamento.

Teorema 2.3.1

Sia \mathbb{K} un campo e sia $f \in \mathbb{K}[x]$ non nullo con $\deg^*(f) = n \geq 1$. Allora,

- (a) esiste \mathbb{L}/\mathbb{K} campo di spezzamento di f ;
- (b) se \mathbb{L}_1/\mathbb{K} e \mathbb{L}_2/\mathbb{K} sono campi di spezzamento di f , esiste $\alpha: \mathbb{L}_1 \rightarrow \mathbb{L}_2$ isomorfismo di campi tale che la restrizione $\alpha|_{\mathbb{K}} = \text{id}_{\mathbb{K}}$.

Dimostrazione. Parte (a). Idea: esiste $a \in \mathbb{L}$ tale che $f(a) = 0$, quindi $f(x) = (x-a) \cdot f_0$, dove $\deg^*(f_0) = \deg^*(f) - 1$, e uso induzione forte. Come faccio? Definisco $\mathcal{P}(n)$ l'affermazione seguente:

- $\mathcal{P}(n)$: Sia \mathbb{K} un campo e sia $f \in \mathbb{K}[x]$ con $\deg^*(f) = n$. Allora, esiste un'estensione di campi \mathbb{L}/\mathbb{K} e esistono $c_1, \dots, c_n \in \mathbb{L}$ e $c_f \in \mathbb{K}$ tali che:

- (i) $f(x) = c_f \prod_{i=1}^n (x - c_i) \in \mathbb{L}[x]$;
- (ii) $\mathbb{L} = \mathbb{K}(\{c_1, \dots, c_n\})$.

Osserviamo che $\mathcal{P}(1)$ è vera: detto $f = a_1 x + a_0$, basta prendere $L = K$ e $c_1 = -\frac{a_0}{a_1} \in \mathbb{K}$. Infatti, $f = a_1 \cdot (x - c_1)$ e $L = K = K(c_1)$. Assumiamo ora che $\mathcal{P}(k)$ sia vera per ogni $k < n$. Per la Costruzione di Kronecker, esiste \mathbb{L}/\mathbb{K} e $a \in L$ tale che $f(a) = 0$. Detto $K_1 = K(a) \subseteq L$, $f = (x - a) \cdot f_1$, dove $f_1 \in K_1[x]$, poiché per ipotesi induttiva vale $\mathcal{P}(n-1)$, esiste L/K_1 e esistono $c_1, \dots, c_{n-1} \in L$ tali che $f_1(x) = c_f \prod_{i=1}^{n-1} (x - c_i)$ e $L = K_1(\{c_1, \dots, c_{n-1}\})$. Allora, considerando L/K e $c_0 = a$, si ha che $f = c_f \prod_{i=0}^{n-1} (x - c_i) \in L[x]$ e $L = K_1(\{c_1, \dots, c_{n-1}\}) = K(\{c_0, \dots, c_{n-1}\})$, cioè $\mathcal{P}(n)$ è effettivamente vera.

Parte (b). Sia $\alpha: K_1 \rightarrow K_2$ isomorfismo di campi. Definiamo $(-)^{\alpha}: K_1[x] \rightarrow K_2[x]$ che preso $f = \sum_{k=0}^n a_k x^k$ lo manda in $f^{\alpha} = \sum_{k=0}^n \alpha(a_k) x^k$. Allora, tale funzione è un isomorfismo di anelli. Definisco $\mathcal{P}(n)$ l'affermazione seguente:

- $\mathcal{P}(n)$: Siano $\mathbb{K}_1, \mathbb{K}_2$ campi e sia $f \in \mathbb{K}_1[x]$ non nullo con $\deg^*(f) = n$. Allora, detto $\alpha: K_1 \rightarrow K_2$ isomorfismo di campi, L_1/K_1 il campo di spezzamento di $f \in K_1[x]$ e L_2/K_2 il campo di spezzamento di $f^{\alpha} \in K_2[x]$, esiste $\alpha_*: L_1 \rightarrow L_2$ isomorfismo di campi tale che la restrizione $\alpha_*|_{K_1} = \alpha$.

Osserviamo che $\mathcal{P}(1)$ è vera, perché preso $f = a_1x + a_0 = a_1(x - c_1)$, dove $c_1 = -\frac{a_0}{a_1} \in K_1$, e scelgo $L_1 = K_1$; inoltre, $f^\alpha = \alpha(a_1)x + \alpha(a_0)$ e $\alpha(c_1) = \frac{\alpha(a_0)}{\alpha(a_1)}$, cioè $f^\alpha = \alpha(a_1)(x - \alpha(c_1))$ e prendo $L_2 = K_2$, quindi $\alpha: L_1 \rightarrow L_2$ è l'isomorfismo tra campi richiesto. Supponiamo ora che $\mathcal{P}(k)$ sia vera per ogni $k < n$. Sia $f = h \cdot f_0$ di grado n con $h \in K_1[x]$ irriducibile, $\deg^*(h) > 0$. Allora, perché L_1/K_1 è campo di spezzamento per f_1 , esiste $c \in L_1$ tale che $h(c) = 0$. Dunque, $h(x) = (x - c) \cdot h_0(x) \in L_1[x]$. Sia $M_1 = K_1[c]$ (cioè, K_1 con l'aggiunta dell'elemento algebrico c), così che abbiamo $h(x) = (x - c)h_0(x) \in M_1[x]$. Allora, detto $f_1 = h_0(x) \cdot f_0(x) \in M_1[x]$, si ha $\deg^*(f_1) = n - 1$. Da $f = h \cdot f_0$, deduciamo che $f^\alpha = h^\alpha \cdot f_0^\alpha$, dove h^α è anch'esso irriducibile (se fosse $h^\alpha = h_1 \cdot h_2$, avremmo $h = h_1^{\alpha^{-1}} \cdot h_2^{\alpha^{-1}}$ dove $\alpha^{-1}: K_2 \rightarrow K_1$ è la funzione inversa di α). Poiché L_2/K_2 è campo di spezzamento di f^α , esiste $d \in L_2$ tale che $h^\alpha(d) = 0$. Detto $M_2 = K_2[d]$, L_1/M_1 è campo di spezzamento di f_1 e L_2/M_2 è campo di spezzamento di $f_2 = f_1^\alpha/(x - d)$. Resta da mostrare che esiste un isomorfismo di campi $\beta: M_1 \rightarrow M_2$ tale che $\beta(c) = d$, e $\beta|_{K_1} = \alpha$, perché in questo modo $f_1^\beta = f_2$. Infatti $f^\beta = (x - c)^\beta f_1^\beta = (x - d) \cdot f_2 = f^\alpha$, da cui effettivamente $f_1^\beta = f_2$. Per ipotesi induttiva, poiché vale $\mathcal{P}(n-1)$, sappiamo che esiste un isomorfismo tra campi $\beta_*: L_1 \rightarrow L_2$ tale che $\beta_*|_{M_1} = \beta$, da cui $\beta_*|_{K_1} = \beta|_{K_1} = \alpha$, e abbiamo concluso perché ora prendiamo $\alpha_* = \beta_*$, quindi vale $\mathcal{P}(n)$. A quanto pare serve un pezzo del Teorema seguente per concludere. ■

Proposizione 2.3.2

Sia $\alpha: K_1 \rightarrow K_2$ isomorfismo di campi e siano $h \in K_1[x]$ irriducibile, L_1/K_1 estensione di campi, $c \in L_1$ tale che $h(c) = 0$, L_2/K_2 estensione di campi, $d \in L_2$ tale che $h^\alpha(d) = 0$. Allora, esiste un isomorfismo di campi $\beta: K_1[c] \rightarrow K_2[d]$ tale che $\beta|_{K_1} = \alpha$.

Dimostrazione. Vedi appunti cartacei per diagramma commutativo da aggiungere; lui ha anche messo un asterisco a sx nelle funzioni ma non so come metterlo adesso. Senza perdita di generalità siano h monico, cioè $h = \min_{c, K_1}$, e h^α monico (so già che è irriducibile), $h^\alpha(d) = 0$, quindi prendo $h^\alpha = \min_{d, K_2}$. Siano $\phi_c: K_1[x]/\langle h \rangle \rightarrow K_1[c]$, $\phi_d: K_2[x]/\langle h^\alpha \rangle \rightarrow K_2[d]$ le mappe indotte dalle valutazioni, $\alpha: K_1[x]/\langle h \rangle \rightarrow K_2[x]/\langle h^\alpha \rangle$ la mappa indotta da α del Teorema 2.3.1 punto (b). Definisco $\beta = \phi_d \circ \alpha \phi_c^{-1}: K_1[c] \rightarrow K_2[d]$. Questa è un isomorfismo perché composizione di isomorfismi, in quanto tutte le funzioni definite precedentemente sono isomorfismi per il *Primo teorema d'isomorfismo*. La verifica che $\beta|_{K_1} = \alpha$ è banale. Boh, sta cosa è completamente delirante. ■

2.4 Campi finiti

Sia \mathbb{K} un campo e sia $\chi_{\mathbb{K}}: \mathbb{Z} \rightarrow \mathbb{K}$ definita come $\chi_{\mathbb{K}}(n) = \sum_{i=1}^n 1_{\mathbb{K}}$ per $n \geq 0$ (si intende che $\chi_{\mathbb{K}}(0) = 0_{\mathbb{K}}$) e $\chi_{\mathbb{K}}(-n) = -\chi_{\mathbb{K}}(n)$. Allora, $\chi_{\mathbb{K}}$ è un omomorfismo di anelli, quindi $\text{Im}(\chi_{\mathbb{K}}) \subseteq \mathbb{K}$ è un dominio di integrità, da cui $\ker(\chi_{\mathbb{K}}) \triangleleft \mathbb{Z}$ è un ideale primo.

Definizione

Se $\ker(\chi_{\mathbb{K}}) = \{0\}$, allora \mathbb{K} si dice di caratteristica 0, e si scrive $\text{char}(\mathbb{K}) = 0$. Se $\ker(\chi_{\mathbb{K}}) \neq \{0\}$, esiste un primo p tale che $\ker(\chi_{\mathbb{K}}) = p\mathbb{Z}$; in questo caso, \mathbb{K} si dice di caratteristica p , e si scrive $\text{char}(\mathbb{K}) = p$.

Fatto (lo chiamerò Lemma 2.3.3): Sia K un campo finito. Allora χ_K non può essere iniettivo, quindi K è di caratteristica p per un primo p .

(In realtà è una definizione) Se K è un campo di caratteristica $p \neq 0$, $K_0 = \text{Im}(\chi_k) \subseteq K$ è un campo detto campo primo di K , ed è isomorfo a $\mathbb{Z}/p\mathbb{Z}$.

Teorema 2.3.4

Siano E, F campi finiti tali che $|E| = |F|$. Allora, $E \simeq F$

Dimostrazione. Sia $|E| = |F| = q$. Per il Fatto, $\text{char}(E) = p_1$ e $\text{char}(F) = p_2$ per p_1, p_2 primi. Poiché $E_0 \subseteq E$, detto $n_1 = |E : E_0|$, si ha che $|E| = p_1^{n_1}$. Analogamente, poiché $F_0 \subseteq F$, detto $n_2 = |F : F_0|$ si ha che $|F| = p_2^{n_2}$. Dunque $p_1 = p_2 = p$ e $n_1 = n_2 = n$. La dimostrazione dell'isomorfismo continua dopo (dannazione è un sacco disorganizzato negli appunti) ■

Questo teorema non è valido per i gruppi e per gli anelli. Infatti, nei gruppi $|S_3| = |\mathbb{Z}/6\mathbb{Z}| = 6$, ma uno è abeliano e l'altro no, quindi $S_3 \not\simeq \mathbb{Z}/6\mathbb{Z}$. Negli anelli, $\mathbb{Z}/4\mathbb{Z} \not\simeq \mathbb{F}_2[x]/\langle x^2 \rangle$ perché uno ha gruppo additivo ciclico e l'altro no.

Osservare come questo dice che ogni campo finito ha cardinalità p^n per un primo p e $n > 1$. In realtà questo è un se e solo se, cioè, per ogni p^n esiste un campo di ordine p^n . Due strade: considerare lo splitting field E di $x^{p^n} - x$ su $\mathbb{Z}/p\mathbb{Z}$ e mostrare che $|E| = p^n$, oppure costruire un polinomio irriducibile $f(x)$ di grado n in $\mathbb{F}_p[x]$ e considerare il quoziente $\mathbb{F}_p[x]/\langle f \rangle$.

Da questo segue anche che se E, F sono campi finiti tali che $|E| = |F| = q$, allora $E^\times \simeq F^\times \simeq \mathbb{Z}/(q-1)\mathbb{Z}$ (questo perché se G è un gruppo abeliano il cui esponente è $\exp(G) = |G|$, significa che G è ciclico).

Proposizione 2.3.5

Sia $A \subseteq K^\times$ sottoanello di K campo, $|A| < \infty$. Allora, A è un gruppo ciclico.

Dimostrazione. Sia $n = \exp(A)$, e sia $f = x^n - 1$. Allora, $A \subseteq Z_f(K)$ (sta indicando con $Z_f(K)$ qualcosa che ha a che fare con gli zeri...) da cui $|A| \leq \deg^*(f) = n = \exp(A)$. Poiché $\exp(A) \mid |A|$, deve essere $|A| = \exp(A)$, cioè A è ciclico. ■

Conclusione dimostrazione 2.3.4: Sia $\psi_q = (x^{q-1} - 1)x$. Allora $Z_{\psi_q}(E) = E$ e $Z_{\psi_q}(F) = F$, quindi $\psi_q(x) = \prod_{\lambda \in E} (x - \lambda) = \prod_{\mu \in F} (x - \mu)$. Dunque, E/E_0 e F/F_0 sono campi di spezzamento di $\psi_q \in \mathbb{F}_p[x]$. Dunque, per il punto (b) del Teorema 2.3.1 sappiamo che $E \simeq F$.

Notare come questo dimostra che non è ambiguo denotare con \mathbb{F}_p il campo di cardinalità p primo, perché esso è effettivamente l'unico!

Lezione del 12/11/2019 (appunti grezzi)

Definizione

Sia \mathbb{K} un campo con $\text{char}(\mathbb{K}) = p$. Allora, la mappa $F: \mathbb{K} \rightarrow \mathbb{K}$ definita come $F(x) = x^p$ è un omomorfismo di campi detto omomorfismo di Frobenius.

Osserviamo che tale mappa è effettivamente un omomorfismo. Infatti, $F(0_K) = 0_K$, $F(1_K) = 1_K$ e $F(x + y) = \sum_{k=0}^p \binom{p}{k} x^k y^{p-k} = x^p + y^p = F(x) + F(y)$ perché $\binom{p}{k}$ è divisibile per p se $0 < k < p$. Infine, è evidente che $F(xy) = (xy)^p = x^p y^p = F(x)F(y)$.

(Diventerà un Lemma) Osserviamo anche che F è iniettiva, e se $|\mathbb{K}| < \infty$ è pure un automorfismo. Infatti, sappiamo che $\ker(F) \triangleleft \mathbb{K}$, ed essendo $1 \notin \ker(F)$, $\ker(F) = \{0_K\}$ perché gli unici ideali di un campo sono $\{0_K\}$ e K . Dunque F è iniettiva. Se vale anche $|K| < \infty$, essendo F iniettiva su un insieme finito, è chiaramente anche suriettiva, da cui è biettiva e quindi un automorfismo.

Proposizione

Sia K un campo finito, $p = \text{char}(K)$ e $K_0 = \text{Im } \chi_K$. Se $|K| = p^n$, $n = |K : K_0|$, allora $\text{ord}(F) = n$, dove $\text{ord}(F) = n$ è l'ordine di F pensata come elemento di $\text{Sym}(K)$.

Dimostrazione. Sappiamo che K/K_0 è campo di spezzamento di $x^{p^n} - x$, cioè K è l'insieme degli zeri di $x^{p^n} - x$, il che è vero se e solo se $z^{p^n} = F^n(z) = z$ per ogni $z \in \mathbb{K}$. Dunque, $F^n = \text{id}_K$. Resta da verificare che n è effettivamente il minimo intero positivo per cui F^k sia l'identità. Sia quindi $k \in \mathbb{N}^+$ con $k < n$ tale che $F^k = \text{id}_K$. Allora, $z^{p^k} = F^k(z) = z$ per ogni $z \in K$, cioè K è l'insieme degli zeri di $x^{p^k} - x$. Essendo $\deg^*(x^{p^k} - x) = p^k$, tale polinomio ha al più p^k radici, cioè $|K| = |Z_K(x^{p^k} - x)| \leq p^k < p^n$, assurdo. Dunque $F^k \neq \text{id}_K$. ■

Il grado di un'estensione si può chiamare ordine perché è l'ordine di un automorfismo (nel caso dei campi finiti).

3 Teoria dei moduli

3.1 Moduli

Introduciamo ora il concetto di modulo, una generalizzazione del concetto di spazio vettoriale in cui gli scalari costituiscono un anello e non necessariamente un campo.

Definizione

Sia R un anello. Un gruppo abeliano (M, \oplus) dotato di un'operazione $*: R \times M \rightarrow M$ si dice **R -modulo sinistro** se per ogni $r, r_1, r_2 \in R$ e $m, m_1, m_2 \in M$ si ha che:

- (i) $(r_1 + r_2) * m = r_1 * m \oplus r_2 * m$ (distributività sinistra);
- (ii) $r * (m_1 \oplus m_2) = r * m_1 \oplus r * m_2$ (distributività destra);
- (iii) $r_1 * (r_2 * m) = (r_1 r_2) * m$ (associatività);
- (iv) $1_R * m = m$.

Analogamente, un R -modulo destro è un gruppo abeliano (M, \oplus) dotato di un'operazione $*: M \times R \rightarrow M$ per cui valgono proprietà analoghe ma con gli elementi di R scritti a destra. Se R è un anello commutativo, i concetti di R -modulo destro e sinistro coincidono.⁴⁷

Esempio. Ogni spazio vettoriale V su un campo \mathbb{K} può essere pensato come un \mathbb{K} -modulo, dove $*: \mathbb{K} \times V \rightarrow V$ è la moltiplicazione per scalari. Viceversa, essendo \mathbb{K} commutativo, ogni \mathbb{K} -modulo è bilatero e può quindi essere pensato come uno spazio vettoriale su \mathbb{K} . \square

Esempio. Ogni gruppo abeliano G può essere visto come un modulo sull'anello degli interi. Si consideri l'operazione $*: \mathbb{Z} \times G \rightarrow G$ definita come $0 * g = 0_G$, $n * g = g + g + \dots + g$ (somma di n termini) e $(-n) * g = -(n * g)$ per ogni $n > 0$ e $g \in G$. Si verifica facilmente che G dotato di tale operazione soddisfa le proprietà (i)-(iv) ed è quindi uno \mathbb{Z} -modulo. \square

Esempio. Sia R un anello e sia $I \triangleleft R$ un ideale sinistro. Allora, I è un R -modulo sinistro, dove $*: R \times I \rightarrow I$ è il prodotto dell'anello R , ed è ben definito in quanto per definizione di ideale sinistro $r * a = ra \in I$ per ogni $r \in R$ e $a \in I$. \square

Esempio. Sia R un anello e sia n un intero positivo. Si consideri il prodotto cartesiano $R^n = \{(r_1, \dots, r_n) : r_1, \dots, r_n \in R\}$ dotato della moltiplicazione componente per componente $*: R \times R^n \rightarrow R^n$ definita come $r * (r_1, \dots, r_n) = (rr_1, \dots, rr_n)$. Si verifica facilmente che R^n dotato di tale operazione soddisfa le proprietà (i)-(iv) ed è quindi un R -modulo sinistro. \square

L'esempio seguente è particolarmente importante nell'algebra lineare perché permette di dimostrare l'esistenza della forma canonica razionale e di Jordan di una matrice.⁴⁸

Esempio. Sia V uno spazio vettoriale su un campo \mathbb{K} e sia $\alpha \in \text{End}_{\mathbb{K}}(V)$ un endomorfismo di V . Preso $f(x) = \sum_{i=0}^n a_i x^i \in \mathbb{K}[x]$, si consideri l'operazione $*_{\alpha}: \mathbb{K}[x] \times V \rightarrow V$ definita come $f *_{\alpha} v = f_{\alpha}(v)$, dove $f_{\alpha} = \sum_{i=0}^n a_i \alpha^i \in \text{End}_{\mathbb{K}}(V)$.⁴⁹ Allora, si verifica facilmente che V dotato di tale operazione soddisfa le proprietà (i)-(iv) ed è quindi un $\mathbb{K}[x]$ -modulo sinistro. \square

⁴⁷Ogni modulo destro è isomorfo al corrispondente modulo sinistro, e si parla infatti di modulo bilatero.

⁴⁸Riprenderemo questo argomento dopo il *Teorema di struttura per i gruppi abeliani finitamente generati*.

⁴⁹Ricordiamo che l'insieme degli endomorfismi di un gruppo è un anello secondo le operazioni di somma puntuale e di composizione di funzioni. In questo caso, $a_i \alpha^i$ è l'endomorfismo che mappa $v \mapsto a_i \cdot \alpha^i(v)$, dove α^i indica la composizione $\underbrace{\alpha \circ \alpha \circ \dots \circ \alpha}_{i \text{ volte}}$, inteso che $\alpha^0 = \text{id}_V$.

Dimostriamo ora due proprietà dei moduli.

Proposizione 3.1.1

Sia R un anello e sia M un R -modulo sinistro. Allora,

- (a) $0_R \cdot m = 0_M$ per ogni $m \in M$;
- (b) $r \cdot 0_M = 0_M$ per ogni $r \in R$.

Dimostrazione. (a) Per la distributività sinistra $0_R \cdot m = (0_R + 0_R) \cdot m = 0_R \cdot m + 0_R \cdot m$. Dunque, sommando l'opposto $-0_R \cdot m$ ad entrambi i membri, otteniamo che $0_M = 0_R \cdot m$.
(b) Per la distributività destra $r \cdot 0_M = r \cdot (0_M + 0_M) = r \cdot 0_M + r \cdot 0_M$. Dunque, sommando l'opposto $-r \cdot 0_M$ ad entrambi i membri, otteniamo che $0_M = r \cdot 0_M$. ■

Definizione

Sia R un anello e sia M un R -modulo sinistro. Un sottogruppo abeliano $A \subseteq M$ si dice R -sottomodulo di M se $r \cdot a \in A$ per ogni $r \in R$ e $a \in A$.

Un sottomodulo è quindi un sottogruppo abeliano $A \subseteq M$ per cui $(A, \cdot_{R \times A} : R \times A \rightarrow A)$ è di nuovo un R -modulo (sto quindi effettuando una restrizione dell'operazione \cdot).

Proposizione 3.1.2

Sia R un anello, M un R -modulo sinistro e sia $A \subseteq M$ un R -sottomodulo. Allora, $(M/A, \cdot : R \times M/A \rightarrow M/A)$ è un R -modulo sinistro, ove $r \cdot (m + A) = r \cdot m + A$ e $f(r, m + A) = r \cdot m + A$.

Dimostrazione. Diagramma negli appunti cartacei. La dimostrazione è inesistente, ottimo. ■

Proposizione 3.1.3

Sia R un anello, M un R -modulo sinistro, $A, B \subseteq M$ sono R -sottomoduli. Allora, $A + B = \{a + b : a \in A, b \in B\}$ è un R -sottomodulo di M .

Dimostrazione. Sappiamo già che $A + B \subseteq M$ è un sottogruppo abeliano. Siano $a + b \in A + B$ e $r \in R$. Allora, $r \cdot (a + b) = r \cdot a + r \cdot b \in A + B$ perché $r \cdot a \in A$ e $r \cdot b \in B$ per definizione di sottomodulo. ■

Proposizione 3.1.4

Sia R un anello e M un R -modulo sinistro. Per $m \in M$ sappiamo che $R \cdot m = \{r \cdot m : r \in R\}$ è un R -sottomodulo di M . Siano $m_1, \dots, m_n \in M$. Allora, $\sum_{i=1}^n R \cdot m_i = R \cdot m_1 + \dots + R \cdot m_n = \{m \in M : \exists r_1, \dots, r_n \in R : m = \sum_{i=1}^n r_i \cdot m_i\}$ è un R -sottomodulo di M .

Dimostrazione. Usando distributività sx, $R \cdot m$ è un sottogruppo abeliano. Usando associazività, si conclude mostrando che $R \cdot m$ è un R -sottomodulo. Ora procediamo per induzione grazie alla *Proposizione 3.1.3*. ■

Definizione

Sia R un anello e sia M un R -modulo sinistro. Definiamo numero minimo di generatori $d_R(M)$ il più piccolo $n \in \mathbb{N}$ per cui esistono $m_1, \dots, m_n \in M$ tali che $M = \sum_{i=1}^n R \cdot m_i$. Se tale $n \in \mathbb{N}$ non esiste, poniamo $d_R(M) = \infty$. Diciamo che M è finitamente generato se $d_R(M) < \infty$.

Lezione del 13/11/2019 (appunti grezzi)

Manca tutto un primo pezzo, Trenord ti voglio bene anche io
Esistono i corrispondenti dei 3 teoremi di isomorfismo per gli R -moduli.

Teorema 3.x.y: Primo teorema d'isomorfismo

Sia $\phi: M \rightarrow N$ un omomorfismo di R -moduli, dove R è un anello. Allora, l'omomorfismo indotto $\phi_*: M/\ker(\phi) \rightarrow \text{Im}(\phi)$ è un isomorfismo di R -moduli.

Dimostrazione. Dimostrazione mancante. ■

Teorema 3.x.y: Secondo teorema d'isomorfismo

Sia R un anello, M un R -modulo, e siano $A, B \subseteq M$ degli R -sottomoduli. Allora, esiste un isomorfismo di R -moduli $\pi_*: A/(A \cap B) \rightarrow (A + B)/B$.

Dimostrazione. Sia $\tau: M \rightarrow M/B$ la proiezione canonica, cioè $\tau(m) = m + B$, e sia la restrizione $\tau_A = \pi$. Allora, per il *Primo teorema d'isomorfismo* la mappa $\pi_{star}: A/\ker(\pi) \rightarrow \text{Im}(\pi)$ è un isomorfismo. Poiché $\ker(\pi) = \ker(\tau) \cap A = B \cap A$ e $\text{Im}(\pi) = \{a + B : a \in A\} = (A + B)/B$, abbiamo concluso. ■

Teorema 3.x.y: Terzo teorema d'isomorfismo

Sia R un anello, M un R -modulo, $A \subseteq B \subseteq M$ degli R -sottomoduli. Allora, esiste un isomorfismo di R -moduli $\psi_*: (M/A)/(B/A) \rightarrow M/B$.

Dimostrazione. Sia $\psi: M/A \rightarrow B/A$ la mappa definita come $\psi(m + A) = m + B$. Poiché ψ è un omomorfismo di R -moduli, per il *Primo teorema d'isomorfismo* la mappa indotta $\psi_*: (M/A)/\ker(\psi) \rightarrow \text{Im}(\psi)$ è un isomorfismo. Essendo $\text{Im}(\psi) = \{m + B : m \in M\} = M/B$ e $\ker(\psi) = \{m + A : m \in M, m + B = B\} = \{m + A : m \in B\} = B/A$, abbiamo concluso. ■

Proposizione

Sia R un anello, M un R -modulo sinistro e $B \subseteq M$ un R -sottomodulo di M . Allora $d_R(M) \leq d_R(B) + d_R(M/B)$ e $d_R(M/B) \leq d_R(M)$.

Dimostrazione. Se B o M/B non sono finitamente generati, cioè $d_R(B) = \infty$ o $d_R(M/B) = \infty$, la prima equazione è banalmente vera. Siano quindi $d_R(B) = k < \infty$ e $d_R(M/B) = n < \infty$. Allora, esistono $m_1, \dots, m_k \in B$ tali che $B = \sum_{i=1}^k R \cdot m_i$ ed esistono $t_1, \dots, t_n \in M$ tali che $M/B = \sum_{i=1}^n R \cdot (t_i + B)$. Dunque, per ogni $m \in M$ esistono $r_1, \dots, r_n \in R$ tali che $m + B = \sum_{i=1}^n r_i \cdot (t_i + B)$, cioè $m - \sum_{i=1}^n r_i \cdot t_i \in B$. Allora, esistono $s_1, \dots, s_k \in R$ tali che $m - \sum_{i=1}^n r_i \cdot t_i = \sum_{j=1}^k s_j \cdot m_j$, da cui $m = \sum_{i=1}^n r_i \cdot t_i + \sum_{j=1}^k s_j \cdot m_j$, cioè $d_R(M) \leq n + k$.

Per quanto riguarda la seconda diseguaglianza, possiamo assumere che $d_R(M) = n < \infty$, altrimenti è banalmente vera. Dunque, esistono $m_1, \dots, m_n \in M$ tali che $M = \sum_{i=1}^n R \cdot m_i$, quindi per ogni $m \in M$ esistono $r_1, \dots, r_n \in R$ tali che $m = \sum_{i=1}^n r_i \cdot m_i$, da cui $m + B = \sum_{i=1}^n r_i \cdot (m_i + B)$, e per l'arbitrarietà di M significa che $M/B = \sum_{i=1}^n R \cdot (m_i + B)$. Dunque, $d_R(M/B) \leq n$ come desiderato. ■

Proposizione

Sia R un anello commutativo. Allora, R è noetheriano se e solo se ogni sottomodulo di un R -modulo finitamente generato è finitamente generato.

Dimostrazione. Procediamo per induzione su $d = d_R(M)$. Se $d = 1$, esiste $m \in M$ tale che $M = R \cdot m$. Sia $\tau_m: R \rightarrow M$ la mappa definita come $\tau_m(r) = r \cdot m$. Osserviamo che $\tau_m(0) = 0$, $\tau_m(r_1 + r_2) = \tau_m(r_1) + \tau_m(r_2)$ e $\tau_m(r \cdot r_1) = r \cdot r_1 \cdot m = r \cdot \tau_m(r_1)$, quindi τ_m è un omomorfismo di R -moduli. Sia $B \subseteq M$ un R -sottomodulo e sia $I_B = \{r \in R : \tau_m(r) \in B\} \subseteq R$. Poiché I_B è un sottogruppo abeliano e presi $a \in I_B$ e $r \in R$ sappiamo che $r \cdot a \in I_B$ essendo B un sottomodulo, vale $I_B \triangleleft R$. Dunque, essendo R noetheriano per ipotesi, esistono $a_1, \dots, a_n \in I_B$ tale che $I_B = \langle a_1, \dots, a_n \rangle$. Poiché $B = \tau_m(I_B) = \text{Im}(\tau_m|_{I_B})$, per la proposizione precedente concludiamo che $d_R(B) < \infty$. Supponiamo ora per induzione forte che tale affermazione valga per $k \leq d$, e mostriamo che vale per $d+1$. Sia M un R -modulo sinistro con $d_R(M) = d+1$. Allora, esistono $m_0, \dots, m_d \in M$ tali che $M = \sum_{k=0}^d R \cdot m_k$. Sia $B \subseteq M$ un sottomodulo e sia $M_\star = \sum_{k=1}^d R \cdot m_k$. Poiché $d_R(M_\star) \leq d$, $M/M_\star = R \cdot (m_0 + M_\star)$.

Sia $\pi: M \rightarrow M/M_\star$ la proiezione canonica, dove $d_R(M/M_\star) \leq 1$. Per ipotesi induttiva, $d_R(B \cap M_\star) < \infty$, quindi $d_R(\pi(B)) < \infty$. Poiché $\pi(B) = (B + M_\star)/M_\star \subseteq M/M_\star$, per la proposizione precedente $d_R(B) \leq d_R(B \cap M_\star) + d_R(B/(B \cap M_\star))$. Ma per ipotesi induttiva sappiamo che $d_R(B \cap M_\star) < \infty$ e $B/(B \cap M_\star) \simeq \pi(B)$ per il *Secondo teorema d'isomorfismo*, quindi $d_R(B/(B \cap M_\star)) < \infty$ e $d_R(B) < \infty$, da cui la tesi.

Viceversa, sia $M = R$ con il prodotto di R (tale R -modulo è detto R -modulo regolare).⁵⁰ Poiché $B \subseteq R$ è un sottomodulo se e solo se $B \triangleleft R$ è un ideale, per ipotesi sappiamo che $d_R(B) < \infty$ pensando B come sottomodulo, cioè $d_R(B) < \infty$ pensando ora B come ideale, da cui R è noetheriano. ■

⁵⁰Sto pensando $M = R$ come gruppo abeliano secondo il prodotto di R , essendo R commutativo.

3.2 Torsione

Introduciamo ora un concetto fondamentale nello studio degli R -moduli.

Definizione

Sia R un anello e sia M un R -modulo sinistro. Un elemento $m \in M$ si dice elemento di torsione se esiste almeno un $r \in R \setminus \{0_R\}$ tale che $r \cdot m = 0_M$. Un R -modulo sinistro si dice modulo di torsione se ogni suo elemento è di torsione.

Denotiamo con $\text{tor}_R(M)$ l'insieme degli elementi di torsione di M . Allora, è evidente che $m \in M$ è di torsione se e solo se $m \in \text{tor}(M)$, e M è di torsione se e solo se $M = \text{tor}(M)$.

Esempio. Aggiungere esempio con \mathbb{Z} e \mathbb{Q} dall'esame di settembre.

Proposizione 3.2.1

Sia R un dominio di integrità e sia M un R -modulo sinistro. Allora, $\text{tor}(M)$ è un R -sottomodulo di M .

Dimostrazione. Siano $m, n \in \text{tor}(M)$ e sia $r \in R$. Allora, esistono $s_m, s_n \in R \setminus \{0_R\}$ tali che $s_m \cdot m = 0_M$ e $s_n \cdot n = 0_M$. Poiché R è un dominio di integrità, $s_m \cdot s_n \neq 0_R$. Dunque, $s_m \cdot s_n \cdot (m + n) = s_n \cdot (s_m \cdot m) + s_m \cdot (s_n \cdot n) = 0_M$ per la distributività destra, da cui $m + n \in \text{tor}(M)$. Inoltre, $s_m \cdot (r \cdot m) = r \cdot (s_m \cdot m) = r \cdot 0_M = 0_M$, dunque $r \cdot m \in \text{tor}(M)$. ■

Definizione

Sia R un dominio di integrità, M un R -modulo sinistro e sia $A \subseteq M$ un R -sottomodulo di M . Definiamo saturazione di A in M l'insieme $\text{sat}_M(A)$ degli elementi $m \in M$ tali che esiste $r \in R \setminus \{0_R\}$ con $r \cdot m \in A$.

Proposizione 3.2.2

Sia R un dominio di integrità, M un R -modulo sinistro e sia $A \subseteq M$ un R -sottomodulo di M . Allora,

- (a) $\text{sat}_M(A) \subseteq M$ è un R -sottomodulo di M ;
- (b) $\text{tor}(M) = \text{sat}_M(\{0_R\})$;
- (c) $\text{tor}(M/A) = \text{sat}_M(A)/A$.

Dimostrazione. (a) Siano $m, n \in \text{sat}_M(A)$ e sia $r \in R$. Allora, esistono $s_m, s_n \in R \setminus \{0_R\}$ tali che $s_m \cdot m \in A$ e $s_n \cdot n \in A$. Poiché R è un dominio di integrità, $s_m \cdot s_n \neq 0_R$. Dunque, $s_m \cdot s_n \cdot (m + n) = s_n \cdot (s_m \cdot m) + s_m \cdot (s_n \cdot n) \in A$ poiché somma di elementi di A , da cui $n + m \in \text{sat}_M(A)$. Inoltre, $s_m \cdot (r \cdot m) = r \cdot (s_m \cdot m) \in A$ essendo $s_m \cdot m \in A$.

(b) Ovvio per definizione

(c) Per definizione, $\text{tor}(M/A) = \{m + A : \exists r \in R \setminus \{0_R\} : r \cdot (m + A) = 0_{M/A}\}$. Poiché $r \cdot (m + A) = r \cdot m + A = 0_{M/A} = A$ se e solo se $r \cdot m \in A$, si ha $\text{tor}(M/A) = \{m + A : \exists r \in R \setminus \{0_R\} : r \cdot m \in A\} = \{m + A : m \in \text{sat}_M(A)\} = \text{sat}_M(A)/A$. ■

Definizione

Sia R un anello, M un R -modulo sinistro e sia $m \in M$. Allora, si dice annullatore di m in R l'insieme $\text{Ann}_R(m) = \{r \in R : r \cdot m = 0_M\}$.

Osserviamo che m è di torsione se e solo se $\text{Ann}_R(m) \neq \{0_R\}$. Chiaramente, si intende che

$$\text{Ann}_R(M) = \{r \in R : r \cdot m = 0_M \ \forall m \in M\} = \bigcap_{m \in M} \text{Ann}_R(m)$$

e tale insieme si dice annullatore globale di M in R . Si osservi che $\text{Ann}_R(M) \subseteq \text{Ann}_R(m)$ per ogni $m \in M$ e che $\text{Ann}_R(M) \triangleleft R$ (andrebbe dimostrato).

Aggiungere esempi, aggiungere dimostrazione del $\text{sat}(\text{sat}(A))$ usata più avanti, commenti.

Proposizione 3.2.3

Sia A uno \mathbb{Z} -modulo finitamente generato. Allora, sono equivalenti:

- (i) A è di torsione;
- (ii) $\text{Ann}_{\mathbb{Z}}(A) \neq \{0\}$;
- (iii) $|A| < \infty$.

Dimostrazione. Poiché A è finitamente generato, siano $a_1, \dots, a_n \in A$ tali che $A = \sum_{i=1}^n \mathbb{Z} \cdot a_i$.

(i) \Rightarrow (ii) Essendo A di torsione, in particolare anche $a_1, \dots, a_n \in \text{tor}_{\mathbb{Z}}(A)$, quindi esistono $k_1, \dots, k_n \in \mathbb{Z} \setminus \{0\}$ tali che $k_i \cdot a_i = 0_A$. Sia $m = \text{mcm}(k_1, \dots, k_n) \neq 0$ e sia $a \in A$. Allora, esistono $z_1, \dots, z_n \in \mathbb{Z}$ tali che $a = \sum_{i=1}^n z_i \cdot a_i$, e

$$m \cdot a = \sum_{i=1}^n mz_i \cdot a_i = \sum_{i=1}^n z_i \cdot (m \cdot a_i) = 0_A$$

perché $m \cdot a_i = 0_A$ per ogni $i = 1, \dots, n$. Dunque $m \in \text{Ann}_{\mathbb{Z}}(a)$, e per l'arbitrarietà di a si ha che $m \in \text{Ann}_{\mathbb{Z}}(A)$, cioè $\text{Ann}_{\mathbb{Z}}(A) \neq \{0\}$.

(ii) \Rightarrow (iii) Sia $\phi: \mathbb{Z}^n \rightarrow A$ la mappa definita come $\phi(z_1, \dots, z_n) = \sum_{i=1}^n z_i \cdot a_i$. Poiché ϕ è un omomorfismo suriettivo,⁵¹ per il *Primo teorema d'isomorfismo* si ha che $\mathbb{Z}^n / \ker(\phi) \simeq A$. D'altra parte, $\text{Ann}_{\mathbb{Z}}(a_1) \times \dots \times \text{Ann}_{\mathbb{Z}}(a_n) \subseteq \ker(\phi)$, dunque

$$|A| = |\mathbb{Z}^n / \ker(\phi)| \leq \left| \mathbb{Z}^n / \bigoplus_{i=1}^n \text{Ann}_{\mathbb{Z}}(a_i) \right| = \left| \bigoplus_{i=1}^n \mathbb{Z} / \text{Ann}_{\mathbb{Z}}(a_i) \right|. \text{⁵²}$$

Poiché $\{0\} \neq \text{Ann}_{\mathbb{Z}}(A) \subseteq \text{Ann}_{\mathbb{Z}}(a_i) \triangleleft \mathbb{Z}$, siano $k_1, \dots, k_n \in \mathbb{Z}$ con $\text{Ann}_{\mathbb{Z}}(a_i) = k_i \mathbb{Z}$.⁵³ Allora,

$$|A| \leq \left| \bigoplus_{i=1}^n \mathbb{Z} / \text{Ann}_{\mathbb{Z}}(a_i) \right| = k_1 \cdot \dots \cdot k_n < \infty.$$

(iii) \Rightarrow (i) Sia $a \in A$ e sia $\phi_a: \mathbb{Z} \rightarrow A$ la mappa definita come $\phi_a(z) = z \cdot a$. Poiché ϕ_a è un omomorfismo di \mathbb{Z} -moduli e $\mathbb{Z} / \ker(\phi_a) \simeq A$ per il *Primo teorema d'isomorfismo*, essendo $|\mathbb{Z}| = \infty$ e $|A| < \infty$, per il *Principio dei cassetti* deve essere $\ker(\phi_a) \neq \{0\}$. Dunque $\ker(\phi_a) = \text{Ann}_{\mathbb{Z}}(a) \neq \{0\}$, cioè a è un elemento di torsione, e per l'arbitrarietà di a concludiamo che $\text{tor}_{\mathbb{Z}}(A) = A$, da cui A è di torsione. ■

Aggiungere da qualche parte la dimostrazione dell'isomorfismo citato nel punto 2. A questo punto però tanto vale usare la stessa strategia della proposizione seguente, cioè definire $\phi: \bigoplus_{i=1}^n \mathbb{Z} / k_i \mathbb{Z} \rightarrow A$ la mappa $\phi(z_1 + k_1 \mathbb{Z}, \dots, z_n + k_n \mathbb{Z}) = \sum_{i=1}^n z_i \cdot a_i$ e ragionando come sotto

mostrare che è ben posto, suriettivo, e quindi $|A| \leq \left| \bigoplus_{i=1}^n \mathbb{Z} / k_i \mathbb{Z} \right| = k_1 \cdot \dots \cdot k_n < \infty$.

⁵¹Che ϕ sia un omomorfismo è evidente; la suriettività segue dal fatto che A è generato da a_1, \dots, a_n , quindi per ogni $a \in A$ esistono $z_1, \dots, z_n \in \mathbb{Z}$ tali che $a = \sum_{i=1}^n z_i \cdot a_i$.

⁵²La diseguaglianza segue dal fatto che $|\text{Ann}_{\mathbb{Z}}(a_1) \times \dots \times \text{Ann}_{\mathbb{Z}}(a_n)| \leq |\ker(\phi)|$, e l'uguaglianza perché tali anelli sono isomorfi. Andrebbe spiegato meglio, di fatto dice che ad esempio $\mathbb{Z}^2 / \langle (2, 3) \rangle \simeq \mathbb{Z} / 2\mathbb{Z} \oplus \mathbb{Z} / 3\mathbb{Z}$.

⁵³Infatti, essendo \mathbb{Z} un PID, i suoi ideali sono tutti e soli quelli della forma $k\mathbb{Z}$ al variare di $k \in \mathbb{Z}$.

Vale una proposizione simile alla precedente anche nel caso dei $\mathbb{K}[x]$ -moduli.

Proposizione 3.2.4

Sia \mathbb{K} un campo e sia M un $\mathbb{K}[x]$ -modulo sinistro finitamente generato. Allora, sono equivalenti:

- (i) M è di torsione;
- (ii) $\text{Ann}_{\mathbb{K}[x]}(M) \neq \{0_{\mathbb{K}}\}$;
- (iii) $\dim_{\mathbb{K}}(M) < \infty$.

Dimostrazione. Per ipotesi, esistono $m_1, \dots, m_n \in M$ tali che $M = \sum_{i=1}^n \mathbb{K}[x] \cdot m_i$.

(i) \Rightarrow (ii) Essendo M di torsione, anche $m_1, \dots, m_n \in \text{tor}_{\mathbb{K}[x]}(M)$, quindi esistono polinomi $f_1, \dots, f_n \in \mathbb{K}[x] \setminus \{0_{\mathbb{K}}\}$ tali che $f_i \cdot m_i = 0_M$. Sia $g = \text{mcm}(f_1, \dots, f_n) \neq 0_{\mathbb{K}}$ e sia $m \in M$. Allora, esistono $q_1, \dots, q_n \in \mathbb{K}[x]$ tali che $m = \sum_{i=1}^n q_i \cdot m_i$, e

$$g \cdot m = \sum_{i=1}^n (g \cdot q_i) \cdot m_i = \sum_{i=1}^n q_i \cdot (g \cdot m_i) = 0_M$$

perché $g \cdot m_i = 0_M$ per ogni $i = 1, \dots, n$. Dunque $g \in \text{Ann}_{\mathbb{K}[x]}(m)$, e per l'arbitrarietà di m si ha che $g \in \text{Ann}_{\mathbb{K}[x]}(M)$, cioè $\text{Ann}_{\mathbb{K}[x]}(M) \neq \{0_{\mathbb{K}}\}$.

(ii) \Rightarrow (iii) Poiché $\{0_{\mathbb{K}}\} \neq \text{Ann}_{\mathbb{K}[x]}(M) \subseteq \text{Ann}_{\mathbb{K}[x]}(m_i) \triangleleft \mathbb{K}[x]$, sappiamo che esistono dei polinomi $f_1, \dots, f_n \in \mathbb{K}[x] \setminus \{0_{\mathbb{K}}\}$ tali che $\text{Ann}_{\mathbb{K}[x]}(m_i) = \langle f_i \rangle$.⁵⁴ Sia $\phi: \bigoplus_{i=1}^n \mathbb{K}[x]/\langle f_i \rangle \rightarrow M$ la mappa definita come $\phi(q_1 + \langle f_1 \rangle, \dots, q_n + \langle f_n \rangle) = \sum_{i=1}^n q_i \cdot m_i$. Poiché ϕ è un omomorfismo di $\mathbb{K}[x]$ -moduli suriettivo,⁵⁵ essendo $\dim_{\mathbb{K}}(\mathbb{K}[x]/\langle f_i \rangle) = \deg^*(f_i)$ concludiamo che

$$\dim_{\mathbb{K}}(M) \leq \dim_{\mathbb{K}} \left(\bigoplus_{i=1}^n \mathbb{K}[x]/\langle f_i \rangle \right) = \prod_{i=1}^n \deg^*(f_i) < \infty.$$

(iii) \Rightarrow (i) Sia $m \in M$ e sia $\phi_m: \mathbb{K}[x] \rightarrow M$ la mappa definita come $\phi_m(f) = f \cdot m$. Poiché ϕ_m è un omomorfismo di $\mathbb{K}[x]$ -moduli e per il *Primo teorema d'isomorfismo* vale $\mathbb{K}[x]/\ker(\phi_m) \simeq M$, essendo $\dim_{\mathbb{K}}(\mathbb{K}[x]) = \infty$ e $\dim_{\mathbb{K}}(M) < \infty$, deve essere $\ker(\phi_m) \neq \{0_{\mathbb{K}}\}$. Dunque $\ker(\phi_m) = \text{Ann}_{\mathbb{K}[x]}(m) \neq \{0_{\mathbb{K}}\}$, cioè m è un elemento di torsione, e per l'arbitrarietà di m concludiamo che $\text{tor}_{\mathbb{K}[x]}(M) = M$, da cui M è di torsione. ■

Aggiungere qualche commento e spostare l'osservazione finale (vedi foto) nel capitolo sugli endomorfismi. Qualche esempio pratico? Se mi viene in mente lo aggiungo.

⁵⁴ Infatti, essendo $\mathbb{K}[x]$ un PID, i suoi ideali sono tutti e soli quelli della forma $\langle f \rangle$ al variare di $f \in \mathbb{K}[x]$.

⁵⁵ Andrebbe dimostrato che ϕ è ben posto, il che segue dall'aver scelto come f_i i generatori degli annullatori e ragionando componente per componente: se $q_i + \langle f_i \rangle = r_i + \langle f_i \rangle$, allora $q_i = r_i + h f_i$ per un certo $h \in \mathbb{K}[x]$, e la restrizione di ϕ alla i -esima componente è $\phi_i(q_i) = (r_i + h f_i) \cdot m_i = r_i \cdot m_i + h f_i \cdot m_i = r_i \cdot m_i = \phi_i(r_i)$. La suriettività invece risulta evidente dalla definizione.

3.3 Endomorfismi

Lezione del 20/11/2019 (appunti grezzi)

Oggi parliamo del polinomio minimo di un endomorfismo di uno spazio vettoriale di dimensione finita.

Sia K un campo, V un K -spazio vettoriale con $\dim_K(V) < \infty$ e sia $\alpha \in \text{End}_K(V)$. Sia $\phi_\alpha: K[x] \rightarrow \text{End}_K(V)$ definita come $\phi_\alpha(f) = f(\alpha)$, cioè, preso $f(x) = \sum_{k=0}^n a_k x^k$, $\phi_\alpha(f) = \sum_{k=0}^n a_k \alpha^k$, dove α^k indica la composizione k volte inteso che $\alpha^0 = \text{id}_V$. Allora, ϕ_α è una mappa K -lineare, perché $\phi_\alpha(\lambda f + \mu g) = \lambda \phi_\alpha(f) + \mu \phi_\alpha(g)$ per ogni $\lambda, \mu \in K$ e per ogni $f, g \in K[x]$. Inoltre, tale mappa è un omomorfismo di anelli, essendo $\phi_\alpha(f \cdot g) = f(\alpha) \circ g(\alpha)$. Dunque, essendo $\dim(K[x]) = \infty$ e $\dim(\text{End}_K(V)) = \dim_K(V)^2$, per il principio dei cassetti ϕ_α non può essere iniettiva, cioè $\ker(\phi_\alpha) \neq \{0_K\}$. Poiché $\ker(\phi_\alpha) \triangleleft K[x]$ è non banale, esiste un unico generatore monico $\min_\alpha(x) \in \ker(\phi_\alpha)$ cioè $\ker(\phi_\alpha) = \langle \min_\alpha(x) \rangle$.

Definizione

Tale polinomio $\min_\alpha(x)$ si dice polinomio minimo dell'endomorfismo $\alpha \in \text{End}_K(V)$.

Vogliamo ora fare due cose: innanzitutto capire come calcolare il polinomio minimo, e poi, analogamente a GAL, trovare un'opportuna base \mathcal{B} di V tale che $[\alpha]_{\mathcal{B}}$ abbia una forma piacevole (Teorema di Jordan). Adesso ci dedichiamo a fare la prima cosa. Per fare la seconda cosa, c'è un teorema molto generale detto Teorema fondamentale per moduli finitamente generati su un dominio a ideali principali. Applicando questo teorema a $(V, *_\alpha)$ proveremo il Teorema di Jordan (per K campo algebricamente chiuso), e applicandolo a \mathbb{Z} troveremo il Teorema per gruppi abeliani finitamente generati. Inoltre, c'è un altro teorema detto di Decomposizione primaria che permette la caratterizzazione degli endomorfismi diagonalizzabili. Tale seconda cosa è molto complessa, e ci staremo sopra fino a Natale.

Teorema 3.X.Y: Teorema di Cayley-Hamilton

Sia V un K -spazio vettoriale con $\dim_K(V) < \infty$ e sia $\alpha \in \text{End}_K(V)$. Allora, $\min_\alpha(x)$ è un divisore del polinomio caratteristico $\text{char}_\alpha(x) = \det(\alpha - x \cdot \text{id}_V)$.

Dimostrazione. Basta provare che (non ha detto niente lol). ■

Mettiamo a posto qualche pezzo di ieri, quando ha usato la somma diretta come se niente fosse. Sia R un anello e siano M e N degli R -moduli sinistri. Allora, $M \oplus N = \{(m, n) : m \in M, n \in N\}$ è un R -modulo sx, ove $(m_1, n_1) + (m_2, n_2) = (m_1 + m_2, n_1 + n_2)$ e $r \cdot (m, n) = (r \cdot m, r \cdot n)$. Analogamente, se M_1, \dots, M_k sono R -moduli sinistri, poniamo $\bigoplus_{i=1}^n M_i = M_1 \oplus \dots \oplus M_k = \{(m_1, \dots, m_k) : m_i \in M_i\}$ e questo è un R -modulo sx con le ovvie operazioni $(m_1, \dots, m_k) + (m'_1, \dots, m'_k) = (m_1 + m'_1, \dots, m_k + m'_k)$ e $r \cdot (m_1, \dots, m_k) = (r \cdot m_1, \dots, r \cdot m_k)$.

Dimostriamo ora la proposizione che è l'analogia di quella di teoria dei gruppi, che serve per dimostrare che il prodotto diretto interno è isomorfo al prodotto diretto esterno sotto ipotesi ragionevoli (tra l'altro la seconda parte è più bella di come la sta facendo lui).

Proposizione

Sia R un anello, M un R -modulo sinistro e siano $A, B \subseteq M$ degli R -sottomoduli tali che $A \cap B = \{0_M\}$. Allora, $A + B \simeq A \oplus B$. In generale, se ho A_1, \dots, A_k che sono R -sottomoduli di M tali che $A_j \cap \sum_{i \neq j} A_i = \{0_M\}$ per ogni $j = 1, \dots, k$, ho che

$$\sum_{i=1}^k A_i \simeq \bigoplus_{i=1}^k A_i.$$

Dimostrazione. Sia $m \in A + B$; allora, esistono $a_m \in A$ e $b_m \in B$ con $m = a_m + b_m \in A + B$. Siano $a' \in A$, $b' \in B$ tali che $m = a' + b'$. Allora, $a_m + b_m = a + b$ se e solo se $a_m - a' = b' - b_m$. Poiché tale elemento appartiene a $A \cap B = \{0_M\}$, risulta $a' = a_m$ e $b' = b_m$, quindi ogni $m \in A + B$ si scrive in modo unico come somma $a_m + b_m$. Sia $\psi: A + B \rightarrow A \oplus B$ definita come $\psi(m) = (a_m, b_m)$ e sia $\eta: A \oplus B \rightarrow A + B$ definita come $\eta(a, b) = a + b$. Per l'unicità della scrittura di m , tali mappe sono ben definite. Inoltre, $\eta \circ \psi = \text{id}_{A+B}$ e $\psi \circ \eta = \text{id}_{A \oplus B}$, quindi è sufficiente mostrare che questi sono omomorfismi di R -moduli. Questo è facile: prendo $m = a_m + b_m$ e $n = a_n + b_n$, allora $m + n = (a_m + a_n) + (b_m + b_n)$, cioè $a_{m+n} = a_m + a_n$ e $b_{m+n} = b_m + b_n$, quindi ψ è un omomorfismo di gruppi abeliani. Inoltre, preso $r \in R$, $r \cdot m = r \cdot a_m + r \cdot b_m = a_{r \cdot m} + b_{r \cdot m}$, da cui ψ è un omomorfismo di R -moduli. Analogo per η , ho $\eta((a_1, b_1) + (a_2, b_2)) = (a_1 + a_2, b_1 + b_2) = \eta(a_1, b_1) + \eta(a_2, b_2)$ e $\eta(r \cdot (a, b)) = \eta(r \cdot a, r \cdot b) = r \cdot a + r \cdot b = r \cdot \eta(a, b)$.

Procediamo ora per induzione su k . Per $k = 1$ non c'è nulla da dimostrare, per $k = 2$ lo ho già fatto. Supponiamo quindi che $\sum_{i=1}^{k-1} A_i \simeq \bigoplus_{i=1}^{k-1} A_i$ e dimostriamolo per k . Per ipotesi $A_k \cap \sum_{i=1}^{k-1} A_i = \{0\}$, quindi $\sum_{i=1}^k A_i = \sum_{i=1}^{k-1} A_i + A_k \simeq \bigoplus_{i=1}^{k-1} A_i \oplus A_k \simeq \bigoplus_{i=1}^k A_i$. ■

Proposizione

Sia V un K -spazio vettoriale di dimensione finita e sia $\alpha \in \text{End}_K(V)$. Siano $U, W \leq V$ sottospazi vettoriali tali che $\alpha(U) = U$ e $\alpha(W) = W$, cioè U e W sono α -invarianti. Siano $\alpha_U \in \text{End}_K(U)$ e $\alpha_W \in \text{End}_K(W)$ gli endomorfismi indotti. Se $U + W = V$ e $U \cap W = \{0_K\}$, allora $\min_\alpha(x) = \text{mcm}(\min_{\alpha_U}(x), \min_{\alpha_W}(x))$.

Dimostrazione. Poiché $\ker(\phi_\alpha) = \text{Ann}_{K[x]}(V, *_\alpha) = K[x] \min_\alpha(x)$,⁵⁶ vale $(V, *_\alpha) \simeq (U, *_{\alpha_U}) \oplus (W, *_{\alpha_W})$. Dunque $\text{Ann}_{K[x]}(V, *_\alpha) = \text{Ann}_{K[x]}(U, *_{\alpha_U}) \cap \text{Ann}_{K[x]}(W, *_{\alpha_W})$, da cui risulta $K[x] \text{mcm}(\min_{\alpha_U}(x), \min_{\alpha_W}(x)) = K[x] \min_{\alpha_U}(x) \cap K[x] \min_{\alpha_W}(x)$. ■

⁵⁶Dimostrare l'uguaglianza tra \ker e Ann usando le doppie inclusioni.

3.4 Moduli in domini a ideali principali

Lezione del 26/11/2019 (appunti grezzi, non so più cosa stia succedendo qui ad Algebra)

Definizione

Sia R un PID e sia M un R -modulo finitamente generato di torsione. Sia $\mathfrak{p} \triangleleft R$ ideale primo di R . Definiamo $M_{\mathfrak{p}} = \{m \in M : x \cdot m = 0 \forall x \in \mathfrak{p}\} = \{m \in M : \mathfrak{p} \subseteq \text{Ann}_R(M)\}$. Allora, tale $M_{\mathfrak{p}}$ si dice \mathfrak{p} -componente primaria di M (o anche \mathfrak{p} -componente di Fitting).

Teorema

Sia R un PID e sia M un R -modulo sinistro finitamente generato di torsione con $\text{Ann}_R(M) = \mathfrak{p}_1^{\alpha_1} \dots \mathfrak{p}_r^{\alpha_r}$, dove i $\mathfrak{p}_i \triangleleft R$ sono ideali primi non nulli. Allora, $M \simeq \bigoplus_{i=1}^r M_{\mathfrak{p}_i^{\alpha_i}}$.

Dimostrazione. La facciamo la prossima volta, le ultime parole famose. ■

Da qui comincia la lezione di oggi, ci sono cose sparse da spostare in torsione etc

Proposizione

Sia R un dominio di integrità e sia M un R -modulo sinistro finitamente generato. Allora, M è di torsione se e solo se $\text{Ann}_R(M) \neq 0$.

Dimostrazione. Siano $m_1, \dots, m_n \in M$ tali che $M = \sum_{i=1}^n R \cdot m_i$. Allora, $\text{Ann}_R(M) = \bigcap_{i=1}^n \text{Ann}_R(m_i)$. Dunque, se M è di torsione, sappiamo che ogni $\text{Ann}_R(m_i) \neq \{0\}$ da cui $\bigcap_{i=1}^n \text{Ann}_R(m_i) \neq \{0\}$.⁵⁷ Il viceversa a quanto pare lo abbiamo già fatto. ■

Osserviamo che se R è un anello commutativo e M è un R -modulo sinistro con $\text{Ann}_R(M) \neq \{0\}$, essendo $\text{Ann}_R(M) \triangleleft R$, M è canonicamente un $\overline{R} = R/\text{Ann}_R(M)$ -modulo. Aggiungere qui il diagramma commutativo negli appunti cartacei. Verifichiamo che vale il Lemma della forbice. Presi $r_1, r_2 \in R$, si ha che $\tau(r_1) = \tau(r_2)$ se e solo se $r_1 - r_2 \in \text{Ann}_R(\overline{M})$, cioè $r_1 = r_2 + a$ con $a \in \text{Ann}_R(\overline{M})$. Per ogni $m \in M$, si ha quindi che $r_1 \cdot m = (r_2 + a) \cdot m = r_2 \cdot m + a \cdot m = r_2 \cdot m$ essendo $a \cdot m = 0$. Dunque, abbiamo dimostrato che $(r_1, m) \sim (r_2, m)$ implica $r_1 \cdot m = r_2 \cdot m$, quindi per il Lemma della forbice esiste la mappa $\odot: \overline{R} \cdot M \rightarrow M$ tale che $(r + \text{Ann}_R M) \odot m = r \cdot m$.

Teorema 3.X.Y: Teorema cinese del resto

Sia R un anello e siano $I_1, \dots, I_n \triangleleft R$ ideali a due a due coprimi (cioè tali che $I_j + I_k = R$ per ogni $j \neq k$). Sia $\pi: R \rightarrow \bigoplus_{k=1}^n R/I_k$ la mappa definita come $\pi(r) = (r+I_1, \dots, r+I_n)$.

⁵⁷Infatti, presi I, J ideali non banali di un dominio di integrità R , se per assurdo fosse $I \cap J = \{0\}$, essendo $IJ = \{ij : i \in I, j \in J\} \triangleleft R$ un ideale contenuto in $I \cap J = \{0\}$, avremmo che esistono $i \in I \setminus \{0\}$ e $j \in J \setminus \{0\}$ tali che $ij = 0$, assurdo (perché siamo in un dominio di integrità). Il claim segue per induzione.

Allora, ϕ è un omomorfismo di anelli suriettivo con $\ker(\pi) = \bigcap_{k=1}^n I_k$.

Dimostrazione. Che π sia un omomorfismo di anelli è evidente dalla definizione (a casa lo scrivo meglio). Inoltre, $\pi(r) = 0$ se e solo se $r \in \bigcap_{k=1}^n I_k$. Sia $J_k = \bigcup_{j \neq k} I_j \triangleleft R$. Allora, J_k e I_k sono coprimi. Infatti, l'ipotesi che $I_k + I_j = R$ per $j \neq k$ implica che in particolare esistono $a_k \in I_k$ e $b_k \in I_j$ tali che $a_k + b_k = 1_R$. Allora,

$$1_R = (a_1 + b_1) \cdot \dots \cdot (a_k + b_k) = a_1 a_2 \cdot \dots \cdot a_n + b_1 a_2 \cdot \dots \cdot a_n + \dots + b_1 b_2 \cdot \dots \cdot b_n$$

dove detti $d_k = b_1 b_2 \cdot \dots \cdot b_n \in I_1 \dots I_{k-1} I_{k+1} \dots I_n \subseteq J_k$ e $e_k = \text{tutti gli altri termini } \in I_k$, abbiamo che $d_k + e_k = 1_R$, cioè I_k e J_k sono effettivamente coprimi. Sia $\pi_k: R \rightarrow R/I_k$ la proiezione canonica, cioè $\pi(r) = r + I_k$. Allora, $\pi_k(d_j) = 0_{R/I_k}$ se $j \neq k$ e $\pi_k(d_j) = 1_{R/I_k} = 1_R + I_k$ per $j = k$. Dunque, $1_R + I_k = \pi_k(1_R) = \pi_k(d_k + e_k) = \pi_k(d_k) + \pi_k(e_k) = \pi_k(d_k)$ perché $\pi_k(e_k) = 0$. Sia ora $y = (r_1 + I_1, \dots, r_n + I_n) \in \bigoplus_{k=1}^n R/I_k$ e sia $z = \sum_{i=1}^n r_i \cdot d_i$. Allora, $\pi_k(z) = \sum_{i=1}^n \pi_k(r_i) \cdot \pi_k(d_i) = \pi_k(r_k) \cdot \pi_k(d_k) = r_k + I_k$ essendo $\pi_k(r_k) = r_k + I_k$ e $\pi_k(d_k) = 1_R + I_k$, da cui $\pi(z) = y$ e π risulta quindi essere un omomorfismo suriettivo. ■

Ora parliamo di ideali in domini a ideali principali (PID), dove $\mathfrak{p} \triangleleft R$ è primo se e solo se è massimale.

Definizione

Sia R un PID. Definiamo spettro di R l'insieme $\text{spec}(R) = \{\mathfrak{p} \triangleleft R : \mathfrak{p} \neq \{0\} \text{ è primo}\}$.

Proposizione

Sia R un PID e sia $I \triangleleft R$ un ideale non banale. Allora, esistono $n_{\mathfrak{p}}(I)$, $\mathfrak{p} \in \text{spec}(R)$ e $n_{\mathfrak{p}} \in \mathbb{N}$ tali che $\text{supp}(I) = \{\mathfrak{p} \in \text{spec}(R) : n_{\mathfrak{p}}(I) \neq 0\}$ è un insieme finito, e $I = \prod_{\mathfrak{p} \in \text{spec}(R)} \mathfrak{p}^{n_{\mathfrak{p}}(I)}$, dove si intende che $\mathfrak{p}^0 = R$.

Dimostrazione. Sia $I = R \cdot a$. Se $a \in R^\times$, allora $n_{\mathfrak{p}} = 0$ per ogni $\mathfrak{p} \in \text{spec}(R)$. Poiché $I \neq \{0_R\}$, sappiamo che $a \neq 0_R$. Quindi, possiamo assumere che $a \in R^\# = R \setminus (R^\times \cup \{0_R\})$. Allora, esiste $u_a \in R^\times$ e $\varepsilon_p(a) \in \mathbb{N}$ tali che $a = u_a \cdot \prod_{\mathfrak{p} \in \mathfrak{p}} p^{\varepsilon_p(a)}$ dove $\mathfrak{p} \subseteq \text{prim}_0(R)$ è un sistema di rappresentanti rispetto a \sim e $\{p \in \mathfrak{p} : \varepsilon_p(a) \neq 0\}$ è un insieme finito, cioè $|\text{supp}(I)| < \infty$. Dunque $R \cdot a = \prod_{p \in \mathfrak{p}} (R \cdot p)^{\varepsilon_p(a)}$. Dove finisce la dimostrazione? Boh... ■

Sia $(m_{\mathfrak{p}})$ con $\mathfrak{p} \in \text{spec}(R)$ una successione di interi non negativi tali che $\{\mathfrak{p} \in \text{spec}(R) : m_{\mathfrak{p}} \neq 0\}$ sia un insieme finito e $I = \prod_{\mathfrak{p} \in \text{spec}(R)} \mathfrak{p}^{m_{\mathfrak{p}}}$. Allora, $m_{\mathfrak{p}} = n_{\mathfrak{p}}(I)$ per ogni $\mathfrak{p} \in \text{spec}(R)$ come conseguenza della univocità della decomposizione in primi. Sia $I = \prod_{\mathfrak{p} \in \text{spec}(R)} \mathfrak{p}^{n_{\mathfrak{p}}(I)} = \prod_{\mathfrak{p} \in \text{supp}(I)} \mathfrak{p}^{n_{\mathfrak{p}}(I)} = \bigcap_{\mathfrak{p} \in \text{supp}(I)} \mathfrak{p}^{n_{\mathfrak{p}}(I)}$. (Ma sti cazzo di $n_{\mathfrak{p}}$ sono così o sono degli $\eta_{\mathfrak{p}}$?)

Sia R un PID e sia M un R -modulo sinistro di torsione. Allora,

$$\text{Ann}_R(M) = \prod_{\mathfrak{p} \in \text{supp}(\text{Ann}_R(M))} \mathfrak{p}^{n_{\mathfrak{p}}(I)} = \bigcap_{\mathfrak{p} \in \text{supp}(\text{Ann}_R(M))} \mathfrak{p}^{n_{\mathfrak{p}}(I)}$$

da cui per il Teorema cinese e per il primo teorema d'isomorfismo si ha che $\overline{R} = R/\text{Ann}_R(M) \simeq \bigoplus_{\mathfrak{p} \in \text{supp}(\text{Ann}_R(M))} R/\mathfrak{p}^{n_{\mathfrak{p}}}$. Sia $d_{\mathfrak{p}} \in \overline{R}$, $d_{\mathfrak{p}} \in \bigcap_{\mathfrak{q} \neq \mathfrak{p}} \mathfrak{q}^{n_{\mathfrak{q}}}$ dove $\mathfrak{q} \in \text{supp}(\text{Ann}_R(M))$. Allora, $d_{\mathfrak{p}} + \mathfrak{p}^{n_{\mathfrak{p}}} = 1 + \mathfrak{p}^{n_{\mathfrak{p}}}$. Detto $\Omega = \{\mathfrak{p}^{n_{\mathfrak{p}}} : \mathfrak{p} \in \text{supp}(\text{Ann}_R(M))\}$, se $\mathfrak{p}, \mathfrak{q} \in \text{spec}(R)$ e $\mathfrak{p} \neq \mathfrak{q}$, significa che $\mathfrak{p}^m + \mathfrak{q}^n = R$ per ogni $m, n \in \mathbb{N}$, cioè Ω sono a due a due coprimi. Infine, si ha quindi che $1_{\overline{R}} = \sum_{\mathfrak{p} \in \text{supp}(\text{Ann}_R(M))} d_{\mathfrak{p}}$.

Lezione del 27/11/2019 (vedi appunti cartacei)

Lezione del 03/12/2019 (appunti grezzi)

Facciamo un recap. Se R è un PID e M è un R -modulo sinistro finitamente generato di torsione, allora $\text{Ann}_R(M) \neq \{0\}$ ed esistono $\mathfrak{p}_1, \dots, \mathfrak{p}_r \in \text{spec}(R)$ e $\alpha_i \in \mathbb{N}$ tali che $\text{Ann}_R(M) = \prod_{i=1}^r \mathfrak{p}_i^{\alpha_i}$. Sappiamo anche che i $\mathfrak{p}_i^{\alpha_i}$, $\mathfrak{p}_j^{\alpha_j}$ sono a due a due coprimi. Abbiamo visto poi che vale il Teorema cinese del resto, cioè $\overline{R} = R/\text{Ann}_R(M) \simeq \bigoplus_{i=1}^r R/\mathfrak{p}_i^{\alpha_i}$ mediante la mappa π . Inoltre, se prendo $d_1, \dots, d_r \in R$ tali che $\pi(d_i + \text{Ann}_R(M)) = (0, \dots, 1, 0, \dots, 0)$ dove 1 è in posizione i -esima, sappiamo che gli $M_i = d_i \cdot M$ sono R -sottomoduli di M e $M = \bigoplus_{i=1}^r M_i$.

Abbiamo applicato la teoria generale al caso particolare in cui $R = \mathbb{K}[x]$ con \mathbb{K} campo e $(M, \cdot) = (M, *_{\alpha})$. In questo caso, $\text{Ann}_{\mathbb{K}[x]}(M) = \mathbb{K}[x] \cdot \min_{\alpha}(x) \cdot \mathbb{K}[x]$ (forse c'è un $\mathbb{K}[x]$ di troppo), e abbiamo dimostrato che α è un endomorfismo diagonalizzabile se e solo se $\min_{\alpha}(x) = \prod_{i=1}^k (x - \lambda_i)$ con $\lambda_i \neq \lambda_j$ se $i \neq j$, cioè se e solo se il polinomio minimo si spartisce completamente in fattori lineari distinti su $\mathbb{K}[x]$.

Proposizione

Si ha che $M_i = M_{\mathfrak{p}_i^{\alpha_i}} = \{m \in M : \mathfrak{p}_i^{\alpha_i} \cdot m = 0\}$.

Dimostrazione. Osserviamo che $d_i \in \mathfrak{p}_j^{\alpha_j}$ per $j \neq i$, quindi $d_i \in \bigcap_{j \neq i} \mathfrak{p}_j^{\alpha_j}$. Sia $m \in d_i \cdot M$. Allora, $m = d_i \cdot m$ perché $(d_i + \text{Ann}_R(M))^2 = d_i + \text{Ann}_R(M)$, cioè esiste $y \in M$ tale che $m = d_i \cdot y = d_i^2 \cdot y = d_i(d_i \cdot y) = d_i \cdot m$. Per ogni $z \in \mathfrak{p}_i^{\alpha_i}$ tale che $z \cdot d_i \cdot m = 0$ osserviamo che $z \cdot d_i$ (qualcosa, forse è appartenente?) $\mathfrak{p}_i^{\alpha_i} \cap \prod_{j \neq i} \mathfrak{p}_j^{\alpha_j} = \prod_{k=1}^r \mathfrak{p}_k^{\alpha_k} = \mathfrak{p}_1^{\alpha_1} \cap \dots \cap \mathfrak{p}_k^{\alpha_k} = \text{Ann}_R(M)$, e questo prova che $M_i \in M_{\mathfrak{p}_i^{\alpha_i}}$. Sia ora $m \in M_i \in M_{\mathfrak{p}_i^{\alpha_i}}$. Poiché $m = \cdot m$ e $1_{\overline{R}} = \sum_{i=1}^r d_i + \text{Ann}_R(M)$, sappiamo che $m = \sum_{k=1}^r d_k \cdot m = d_i \cdot m$. Per $k \neq i$, l'elemento $d_k \in \bigcap_{j \neq k} \mathfrak{p}_j^{\alpha_j} \subseteq \mathfrak{p}_i^{\alpha_i}$. Dunque $d_k \cdot m = 0$ perché $m \in M_{\mathfrak{p}_i^{\alpha_i}}$, da cui $M_{\mathfrak{p}_i^{\alpha_i}} \subseteq d_i \cdot M = M_i$ come desiderato. ■

Come si applica questa cosa? Sia $R = \mathbb{Z}$ e sia A uno \mathbb{Z} -modulo finitamente generato di torsione. Allora, avevamo visto che $|A| < \infty$, cioè A è un gruppo abeliano finito.⁵⁸ Per quanto appena provato, possiamo scrivere $A = \bigoplus_{i=1}^r A_i$, dove $A_i = A_{p_i^{\alpha_i} \mathbb{Z}} = a \in A : p_i^{\alpha_i} \cdot a = 0 \in \text{Syl}_p(A)$. Sia $|A| = p_1^{n_1} \cdot \dots \cdot p_r^{n_r} \cdot p_{r+1}^{n_{r+1}} \cdot \dots \cdot p_{r+k}^{n_{r+k}}$. Allora, $A_i \subseteq A$ è un sottogruppo, anzi è un p_i -sottogruppo, e $|A_i| = p_i^{\beta_i}$. Infatti, se per assurdo fosse $|A_i| = p_i^{\beta_i} \cdot q^\beta \cdot r$ con $q \neq p_i$ primo e r intero coprimo a p_i e q , dove ovviamente $\beta \geq 1$, per il Teorema di Sylow esiste $Q \subseteq \text{Syl}_q(A_i) \subseteq A_i$ tale che $|Q| = q^\beta \neq 1$, cioè esiste $g \in Q \setminus \{1\}$. Dunque, $g \in \text{Syl}_q(A_i) \subseteq A_i$ da cui, essendo $g^{p_i^{\alpha_i}} = 1$ e $\langle g \rangle \subseteq Q$, per Lagrange $g^{|Q|} = g^{q^\beta} = 1$. Dunque, essendo $\gcd(p, q) = 1$, deve essere $g = 1$, il che è assurdo perché questo forza $Q = \{1\}$. Dunque, essendo $A = \bigoplus_{i=1}^r A_i$, abbiamo che $|A| = \prod p_i^{\beta_i}$, dove β_i è la massima potenza di p_i che divide $|A|$, da cui $A_i \in \text{Syl}_{p_i}(A)$. (In entrambi gli esempi, ho mostrato che un modulo è somma diretta di sottomoduli che si annullano su ideali particolari che contengono l'annullatore globale, credo abbia detto così).

Esempio. Se $|G| = 35$, allora $G \simeq \mathbb{Z}/35\mathbb{Z}$. Infatti, per quanto appena detto si ha che $G \simeq \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z} = \mathbb{Z}/35\mathbb{Z}$, cioè G è ciclico. L'ide è che ho un solo 5-sottogruppo di Sylow e un solo 7-sottogruppo di Sylow, da cui essi sono normali, e si conclude facilmente. \square

Vogliamo arrivare al teorema seguente. Per farlo dovremo prima introdurre i moduli liberi.

Teorema 3.X.Y: Teorema fondamentale sui moduli f.g. per PID

Sia M un R -modulo sinistro finitamente generato di torsione. Allora, esistono degli ideali $\mathfrak{a}_1, \dots, \mathfrak{a}_k \triangleleft R$ tali che $M \simeq \bigoplus_{i=1}^k R/\mathfrak{a}_i$.

Esempio. Se $R = \mathbb{Z}$ e A è uno \mathbb{Z} -modulo di torsione con $|A| = 27$, allora $\mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}_3 \in \{3\mathbb{Z}, 9\mathbb{Z}, 27\mathbb{Z}\}$ e A è isomorfo a uno tra $\mathbb{Z}/27\mathbb{Z}$, $\mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ e $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. \square

⁵⁸Ricordiamo che per ogni $g \in G$ gruppo, la mappa $\chi_g : \mathbb{Z} \rightarrow G$ definita come $\chi_g(k) = g^k$ è un omomorfismo di gruppi. Definiamo esponente di G l'intero positivo $\exp(G)$ tale che $\exp(G)\mathbb{Z} = \bigcap_{g \in G} \ker(\chi_g)$. In realtà c'è una definizione molto più facile ma a lui piace complicarsi la vita.

3.5 Moduli liberi

Definizione

Sia R un anello e sia X un insieme. Un R -modulo sinistro L dotato di una mappa $i_X: X \rightarrow L$ si dice libero su X se per ogni $\phi: X \rightarrow M$ con M che è R -modulo sinistro, esiste un unico $\phi_*: L \rightarrow M$ omomorfismo di R -moduli tale che $\phi = \phi_* \circ i_X$.

Aggiungere diagrammino dagli appunti. Esistono definizioni analoghe per i gruppi, per le algebre, etc. Il concetto di libero è una generalizzazione del concetto di funtore aggiunto. Ma proseguiamo la prossima volta. Se prendo $R = \mathbb{K}$ campo, $M = V$ spazio vettoriale, $X = \mathcal{B}$ base di V e i_X l'inclusione canonica, allora lo spazio vettoriale V lo possiamo vedere come modulo libero sulla base \mathcal{B} . L'idea è che basta definire i valori di una mappa \mathbb{K} -lineare sulla base, e so già come si comporta in tutto lo spazio V .

Lezione del 10/12/2019 (vedi appunti cartacei)

La lezione del 10/12/2019 la ho negli appunti cartacei per ora. Le cose su teoria dei moduli sono davvero troppo a caso come ordine, dovrei davvero risistemarle.

Lezione del 18/12/2019 (appunti grezzi)

Scopo di questa lezione è arrivare al teorema che mostri che se R è un PID, allora ogni R -modulo finitamente generato senza torsione possiamo in realtà vederlo come R -modulo libero su un opportuno insieme finito. Per fare ciò, procediamo step by step.

La somma diretta: sia R un anello e M un R -modulo sinistro. Allora, $M \simeq A \oplus B$, dove A e B sono R -sottomoduli di M , se e solo se dette $\iota_A: A \rightarrow M$, $\iota_B: B \rightarrow M$ le inclusioni e $\pi_A: M \rightarrow A$ e $\pi_B: M \rightarrow B$ le rispettive proiezioni sul quoziente, accade che $\pi_A \circ \iota_A = \text{id}_A$, $\pi_B \circ \iota_B = \text{id}_B$ e $\iota_A \circ \pi_A + \iota_B \circ \pi_B = \text{id}_M$.

Proposizione 3.5.4

Sia R un anello, M un R -modulo sinistro, A un R -sottomodulo di M e $\iota_A: A \rightarrow M$ e $\pi_A: M \rightarrow A$ omomorfismi di R -moduli tali che $\pi_A \circ \iota_A = \text{id}_A$. Allora, $M \simeq A \oplus \ker(\pi_A)$.

Dimostrazione. Sia $\phi: A \oplus \ker(\pi_A) \rightarrow M$ la mappa definita come $\phi(a, x) = \iota_A(a) + x$, dove $a \in A$ e $x \in \ker(\pi_A)$. Chiaramente tale mappa è un omomorfismo di R -moduli. Inoltre, se $\phi(a, x) = 0$, allora $\iota_A(a) = -x$, cioè $a = \pi_A(\iota_A(a)) = \pi_A(-x) = 0$, da cui $a = 0$, cioè $-x = 0$ e quindi $x = 0$, dunque $(a, x) = (0, 0)$ il che mostra che ϕ è iniettiva. Infine, ϕ è anche suriettiva. Infatti, sia $z \in M$ e sia $y = z - \iota_A(\pi_A(z)) \in M$. Allora, $\pi_A(y) = \pi_A(z) - \pi_A(\iota_A(\pi_A(z))) = \pi_A(z) - \pi_A(z) = 0$, dove nell'ultimo passaggio abbiamo usato che $\pi_A \circ \iota_A = \text{id}_A$, da cui $y \in \ker(\pi_A)$. Dunque, $z = \phi(\pi_A(x), y) = \iota_A(\pi_A(z)) + y$, e questo prova la suriettività di ϕ , da cui esso è quindi un isomorfismo e vale quindi $M \simeq A \oplus \ker(\pi_A)$. ■

Vale una proposizione simile nel caso dei moduli liberi.

Proposizione 3.5.5

Sia M un R -modulo sinistro, $\pi: M \rightarrow F$ un omomorfismo suriettivo e F un R -modulo sinistro libero su un insieme Y . Allora, $M \simeq F \oplus \ker(\pi)$.

Dimostrazione. Sia $\iota_X: X \rightarrow F$ una mappa tale che (F, ι_X) sia libero su X , e per ogni $x \in X$ sia $m_x \in M$ tale che $\pi(m_x) = \iota_X(x)$. Sia $\psi: X \rightarrow M$ la mappa definita come $\psi(x) = m_x$.

$$\begin{array}{ccc} X & \xrightarrow{\iota_X} & F \\ \psi \searrow & \nearrow \pi & \downarrow \\ M & \xleftarrow{\psi_*} & \end{array}$$

Essendo F libero su X , sappiamo che esiste un'unica mappa $\psi_*: F \rightarrow M$ tale che $\psi_* \circ \iota_X = \psi$. Resta da verificare che $\pi \circ \psi_* = \text{id}_F$. Poiché $\pi(\psi_*(\iota_X(x))) = \pi(\psi(x)) = \pi(m_x) = \iota_X(x)$, abbiamo che $(\pi \circ \psi_*)(\iota_X(x)) = \iota_X(x)$ per ogni $x \in X$. Abbiamo quindi trovato due mappe che fanno commutare il diagramma seguente:

$$\begin{array}{ccc} X & \xrightarrow{\iota_X} & F \\ \iota_X \searrow & \downarrow \text{id}_F & \swarrow \pi \circ \psi_* \\ F & \xleftarrow{\quad} & \end{array}$$

Tuttavia, essendo F libero, la mappa che fa commutare tale diagramma è unica, da cui $\pi \circ \psi_* = \text{id}_F$. Dunque, presa $\iota_F = \psi_*$, per la *Proposizione 3.5.4* vale $M \simeq F \oplus \ker(\pi)$. ■

Per dimostrare il Teorema, vogliamo procedere per induzione sul numero di generatori di M . Tuttavia, per fare ciò dobbiamo prima essere in grado di dimostrare il passo base e lo step induttivo. Ci servono quindi altre due proposizioni.

Proposizione 3.5.6

Sia R un PID, $\mathbb{K} = \text{quot}(R)$ e sia $M \subseteq \mathbb{K}$ un R -sottomodulo finitamente generato. Allora, $M \simeq R$ oppure $M = \{0\}$.

Dimostrazione. Poiché M è finitamente generato, esistono $m_1, \dots, m_n \in M$ tali che $M = \sum_{i=1}^n R \cdot m_i$. Essendo $M \subseteq \mathbb{K}$, sappiamo che ogni m_i è della forma $m_i = \frac{a_i}{s_i}$ per degli opportuni $a_i \in R$ e $s_i \in R \setminus \{0\}$. Sia $s = s_1 \cdot \dots \cdot s_n$, così che $s \cdot M \subseteq R$ sia un R -sottomodulo (perché?). Siano $r_1, \dots, r_n \in R$; allora, $s \cdot \sum_{i=1}^n r_i \cdot \frac{a_i}{s_i} = \sum_{i=1}^n r_i s_i^\times a_i$ dove $s_i^\times = \prod_{j \neq i} s_j$ (non so cosa stia facendo qui). Dunque, essendo $s \cdot M$ un ideale di R , poiché R è un PID ogni suo ideale è principale, quindi esiste $b \in R$ tale che $s \cdot M = \langle b \rangle$, da cui $M = R \cdot \frac{b}{s}$. Allora, la mappa $\phi_{b/s}: R \rightarrow M$ definita come $\phi_{b/s}(r) = r \cdot \frac{b}{s}$ è un omomorfismo suriettivo. Se $b = 0$, allora banalmente $M = \{0\}$. Se $b \neq 0$, allora $\ker(\phi_{b/s}) = \{0\}$ e $\phi_{b/s}$ è quindi un isomorfismo. ■

Manca ancora un'ultima (spero meno dubbia della precedente) proposizione prima di poter dimostrare il Teorema. Altro che sagra della primavera, qui è la sagra delle proposizioni.

Proposizione 3.5.7

Sia R un anello, F_1 un R -modulo sinistro libero su X e F_2 un R -modulo sinistro libero su Y . Allora, $F_1 \oplus F_2$ è un R -modulo libero su $X \sqcup Y$.

Dimostrazione. Siano $\iota_X: X \rightarrow F_1$ e $\iota_Y: Y \rightarrow F_2$ le mappe dei moduli liberi F_1 e F_2 , rispettivamente, e sia $\iota_{X \sqcup Y}: X \sqcup Y \rightarrow F_1 \oplus F_2$ la mappa definita come $\iota_{X \sqcup Y}(x) = \iota_X(x)$ e $\iota_{X \sqcup Y}(y) = \iota_Y(y)$ per ogni $x \in X$ e $y \in Y$ (sappiamo che tale mappa è ben definita per le proprietà dell'unione disgiunta). Sia M un R -modulo sinistro e sia $\phi: X \sqcup Y \rightarrow M$ una mappa qualunque. Allora, detta $\phi_*: F_1 \oplus F_2 \rightarrow M$ la mappa $\phi_*(f_1, f_2) = \phi_1(f_1) + \phi_2(f_2)$, dove $\phi_1: F_1 \rightarrow M$ e $\phi_2: F_2 \rightarrow M$ sono gli omomorfismi di R -moduli tali che $\phi|_X = \phi_1 \circ \iota_X$ e $\phi|_Y = \phi_2 \circ \iota_Y$ (che credo esistano essendo F_1 e F_2 moduli liberi), si ha che $\phi_* \circ \iota_{X \sqcup Y} = \phi$, il che prova l'esistenza. Resta da mostrare la unicità di tale mappa ϕ_* per concludere che $F_1 \oplus F_2$ è libero. D'altra parte, se $\psi: F_1 \oplus F_2 \rightarrow M$ è una mappa tale che $\psi \circ \iota_{X \sqcup Y} = \phi$, in particolare deve essere $\psi|_X = \phi_1$ e $\psi|_Y = \phi_2$, da cui $\psi(f_1, f_2) = \psi(f_1, 0) + \psi(0, f_2) = \phi_1(f_1) + \phi_2(f_2) = \phi_*(f_1, f_2)$, da cui $\psi = \phi_*$ provando l'unicità di ϕ_* . ■

It's time for the big theorem, boi :)

Teorema 3.5.8

Sia R un PID e sia M un R -modulo sinistro finitamente generato con $\text{tor}_R(M) = \{0\}$. Allora, esiste un insieme finito X con $|X| = d_R(M)$ tale che M è libero su X .

Dimostrazione. Procediamo per induzione sul numero di generatori $d_R(M)$. Se $d_R(M) = 1$, esiste $m \in M$ tale che $M = R \cdot m$. Allora, $\phi_m: R \rightarrow M$ definita come $\phi_r(m) = r \cdot m$ è un omomorfismo di moduli suriettivo, e $\ker(\phi_m) = \text{Ann}_R(m) = \{0\}$ perché per ipotesi $\text{tor}_R(M) = \{0\}$. Dunque ϕ_m è iniettivo, da cui $M \simeq R$, quindi il teorema vale (perchè ogni anello è un modulo libero su se stesso con 1 generatore, in quanto $R = \langle 1_R \rangle$, cioè $\{1_R\}$ è una base). Supponiamo ora che la tesi valga per $d_R(M) \leq n$. Sia M con $d_R(M) = n+1$ e $\text{tor}_R(M) = \{0\}$. Allora, esistono $m_0, \dots, m_n \in M$ tali che $M = \sum_{i=0}^n R \cdot m_i$. Sia $M_0 = \text{sat}_M(R \cdot m_0)$. Allora, $\text{sat}_M(M_0) = \text{sat}_M(\text{sat}_M(M_0)) = M_0$ (il passaggio in mezzo è inutile, il punto è che il sat del sat è ancora il sat), dunque per la Proposizione 3.2.2 si ha che $\text{tor}_R(M/M_0) = \text{sat}_M(M_0)/M_0 = \{0\}$ (perchè il quoziente è M_0/M_0). Poiché $d_R(M/M_0) \leq n$, per ipotesi induttiva M/M_0 è libero e per la Proposizione 3.5.5 vale $M \simeq M_0 \oplus M/M_0$. Dunque, basta far vedere che anche M_0 è libero. Preso $x \in M_0$, (da qui in poi è delirio) sappiamo che esistono $r_x \in R$ e $s_x \in R \setminus \{0\}$ tali che $s_x \cdot x = r_x \cdot m_0$. Sia $\alpha: M_0 \rightarrow \text{quot}(R)$ la mappa $\alpha(x) = \frac{r_x}{s_x}$ se $x \neq 0$ e $\alpha(0) = 0$. Siano $r, r' \in R$ e $s, s' \in R \setminus \{0\}$ con $s \cdot x = r \cdot m_0$ e $s' \cdot x = r' \cdot m_0$. Allora, $ss' \cdot x = s'r \cdot m_0 = sr' \cdot m_0$, cioè $(s'r - sr') \cdot m_0 = 0$, da cui $s'r - sr' \in \text{Ann}_R(m_0) = \{0\}$ e quindi $s'r - sr' = 0$, cioè $\frac{r}{s} = \frac{r'}{s'}$ (a che serve sta cosa?). Mostriamo che α è un omomorfismo iniettivo di R -moduli. Infatti, presi $x, y \in M_0$, siano $s_x \cdot x = r_x \cdot m_0$ e $s_y \cdot y = r_y \cdot m_0$, così che moltiplicando la prima equazione per s_y e la seconda per s_x e sommandole, valga $s_x s_y (x+y) = (s_y r_x + s_x r_y) \cdot m_0$, da cui $\alpha(x+y) = \frac{s_y r_x + s_x r_y}{s_x s_y} = \frac{r_x}{s_x} + \frac{r_y}{s_y} = \alpha(x) + \alpha(y)$. Inoltre, preso $r \neq 0$, $r s_x \cdot x = r r_x \cdot m_0$, quindi $\alpha(r \cdot x) = \frac{r \cdot r_x}{s_x} = r \cdot \alpha(x)$. Per l'iniettività, se $\alpha(x) = 0$ esiste $s_x \in R \setminus \{0\}$ tale che $s_x \cdot x = 0$, cioè $x \in \text{tor}_R(M_0) \subseteq M$, da cui $x = 0$ essendo $\text{tor}_R(M) = \{0\}$. Dunque, per il

Primo teorema d'isomorfismo si ha $M_0 \simeq \text{Im}(\alpha) \subseteq M$. Tuttavia, per la *Proposizione 3.5.6*, essendo $\text{Im}(\alpha)$ un R -sottomodulo di $\text{quot}(R)$, vale $\text{Im}(\alpha) \simeq R$, quindi $M_0 \simeq R$. Poiché R è libero su $\{\cdot\}$ (come detto prima la base è un insieme di cardinalità 1) e per ipotesi induttiva M/M_0 è libero su X' di cardinalità $|X'| = d_R(M) - 1$, concludiamo che M è libero su $X = X' \sqcup \{\cdot\}$ e $|X| = d_R(M)$ come desiderato. ■

Ci sono un sacco di punti che non mi sono chiari: perché il sat del sat è il sat? che succede quando compare un m_0 selvaggio con tutto il delirio degli r_x e s_x ? Alla fine che succede?

3.6 Divisori elementari

Lezione del 07/01/2020 (appunti grezzi)

Sia R un PID e sia F un R -modulo sinistro libero su $X = \{x_1, \dots, x_n\} \subseteq F$, dove X è una base di F . Preso un elemento $z \in F$, siano $r_1, \dots, r_n \in R$ tali che $z = \sum_{i=1}^n r_i \cdot x_i$.

Definizione

L'ideale $\text{con}(z) = \langle r_1, \dots, r_n \rangle \triangleleft R$ si dice contenuto di z .

A priori, tale definizione è strana: per come lo abbiamo posto, sembra che $\text{con}(z)$ dipenda dalla particolare base X scelta. Tuttavia questo non è vero, come mostra la proposizione seguente. Per comodità di notazione, sia $F^* = \text{Hom}(F, R)$.

Proposizione 3.6.1

Sia $z \in F$ e sia $I_z = \{\phi(z) : \phi \in F^*\}$. Allora, I_z è un ideale di R e $\text{con}(z) = I_z$.

Dimostrazione. Sia $x_i^* \in F^*$ definito come $x_i^*(x_j) = \delta_{i,j}$, così che $r_i = x_i^*(z)$, cioè $r_i \in I_z$.⁵⁹ Mostriamo ora che $I_z \triangleleft R$. Innanzitutto, sappiamo che F^* è un R -modulo, perché presi $\phi, \psi \in F^*$ anche $\phi + \psi \in F^*$ e $r \cdot \phi \in F^*$ per ogni $r \in R$. Dunque, la mappa $\underline{}(z) : F^* \rightarrow R$ è un omomorfismo di R -moduli (ma perché chiama le mappe con il trattino, e che cacchio) da cui $\text{Im}(\underline{}(z)) = I_z$, cioè I_z è un R -modulo (e quindi anche un ideale di R). Chiaramente $\text{con}(z) \subseteq I_z$. D'altra parte, preso $\phi \in F^*$, osserviamo che $\phi(z) = \phi\left(\sum_{i=1}^n r_i \cdot x_i\right) = \sum_{i=1}^n r_i \cdot \phi(x_i) \in \text{con}(z)$, da cui $I_z \subseteq \text{con}(I_z)$ e quindi seque che $\text{con}(z) = I_z$ come richiesto. ■

Lemma 3.6.2

Sia R un PID, F un R -modulo sinistro libero su $X = \{x_1, \dots, x_n\}$ e sia $M \subseteq F$ un R -sottomodulo di F . Sia $z \in F$. Allora,

- (a) esiste $\phi \in F^*$ tale che $\text{con}(z) = \langle \phi(z) \rangle$; (sono ideali o moduli? lui scrive $R \cdot \phi(z)$)
- (b) per ogni $\psi \in F^*$ si ha che $\psi(z) \in \text{con}(z)$;
- (c) esiste $x_0 \in M$ tale che per ogni $y \in M$ si abbia $\text{con}(y) \subseteq \text{con}(x_0)$.

Dimostrazione. (a) Poiché R è un PID, ogni suo ideale è principale, da cui essendo $\text{con}(z) \triangleleft R$ sappiamo che esiste $c \in \text{con}(z)$ tale che $\text{con}(z) = \langle c \rangle$. Dunque, per la *Proposizione 3.6.1* esiste $\phi \in F^*$ tale che $c = \phi(z)$.

(b) Segue banalmente dalla *Proposizione 3.6.1* essendo $\text{con}(z) = I_z$.

(c) Poiché R è un PID, esso è noetheriano, dunque esiste $x_0 \in M$ tale che $\text{con}(x_0)$ è massimale in $\{\text{con}(y) : y \in M\}$, cioè se $\text{con}(x_0) \subseteq \text{con}(z)$ per un certo $z \in M$, allora $\text{con}(z) = \text{con}(x_0)$. Resta da mostrare che x_0 soddisfa (c). Per (a), sappiamo che esiste $\phi \in F^*$ tale che $\text{con}(x_0) = \langle \phi(x_0) \rangle$. Ora, per la *Proposizione 3.6.1* basta verificare che $\phi(z) \subseteq \langle \phi(x_0) \rangle$ per ogni $z \in M$ e $\psi \in F^*$. Sia $R \cdot d = R \cdot \phi(x_0) + R \cdot z_0$. Allora, esistono $a, b \in R$ tali che $d = a \cdot \phi(x_0) + b \cdot \phi(z)$, cioè $d = \phi(ax_0 + bz) \in \text{con}(ax_0 + bz)$ per la *Proposizione 3.6.1*.

⁵⁹Osserviamo che tali x_i^* sono una base del duale.

Allora, $\text{con}(x_0) = R \cdot \phi(x_0) \subseteq R \cdot d \in \text{con}(ax_0 + bz)$, da cui $\text{con}(x_0) = \text{con}(ax_0 + bz)$. Dunque, $d \in R \cdot \phi(x_0)$, cioè $\phi(z) \in R \cdot d \subseteq R \cdot \phi(x_0) = \text{con}(x_0)$. Manca da mostrare che $\psi(z) \in \text{con}(x_0)$ per ogni $\psi \in F^*$. Sappiamo che $\psi(x_0) \in \text{con}(x_0)$ per ogni $\psi \in F^*$. Sia $z_0 = z - \frac{\phi(z)}{\phi(x_0)} \cdot x_0$, dove quindi $\frac{\phi(z)}{\phi(x_0)} \in R$. Allora $\phi(z_0) = 0$. Basta dimostrare che $\psi(z_0) \in \text{con}(x_0)$ (nota: mi sono perso). Sia $\psi_0 \in F^*$ tale che $\psi_0 = \psi - \frac{\psi(x_0)}{\phi(x_0)} \cdot \phi$. Osserviamo che $\psi_0(z_0) = \psi(z)$ e $\psi_0(x_0) = 0$. Ora basta mostrare che $\psi_0(z_0) \in \text{con}(x_0)$. Usiamo lo stesso trucco di prima. Sia $R \cdot c = R \cdot \psi_0(z_0) + R \cdot \psi_0(x_0)$. Allora, esistono $p, q \in R$ tali che $x = p \cdot \psi_0(z_0) + q \cdot \psi_0(x_0)$. Dunque,

$$(\phi + \psi_0)(pz_0 + qx_0) = \phi(pz_0) + \phi(qx_0) + \psi_0(pz_0) + \psi_0(qx_0) = q \cdot \phi(x_0) + p \cdot \psi_0(z_0) = c$$

in quanto gli altri due termini sono nulli. Quindi per la *Proposizione 3.6.1* vale $c = (\phi + \psi_0)(pz_0 + qx_0) \in \text{con}(pz_0 + qx_0)$, da cui $R \cdot c \subseteq \text{con}(pz_0 + qx_0)$, dove $\text{con}(x_0) = R \cdot \phi(x_0) \subseteq R \cdot c$. Dunque, $R \cdot \phi(x_0) = \text{con}(pz_0 + qx_0) \ni c$, cioè $R \cdot c = R \cdot \phi(x_0)$, quindi $\psi_0(z_0) \in R \cdot \psi(x_0) = \text{con}(x_0)$ come desiderato. ■

Teorema 3.6.3

Sia R un PID, F un R -modulo libero su $\{y_1, \dots, y_n\}$ e sia $M \subseteq F$ un R -sottomodulo di F . Allora, esistono una base $\{x_1, \dots, x_n\}$ di F e degli elementi $\alpha_1, \dots, \alpha_m \in R \setminus \{0\}$ tali che $\{\alpha_1 x_1, \dots, \alpha_m x_m\}$ sia una base di M . Inoltre, la successione $(R \cdot \alpha_1, \dots, R \cdot \alpha_m)$ è univocamente determinata da M .

Dimostrazione. Dannazione, me la sono persa per lo sciopero, ma c'è sulle sue note. ■

Definizione

Tali $R \cdot \alpha_i$ si dicono divisori elementari di M .

Corollario 3.6.4

Sia R un PID e sia A un R -modulo di torsione finitamente generato. Allora, esistono degli ideali $I_1, \dots, I_n \triangleleft R$ con $\text{Ann}_R(A) \subseteq I_n \subseteq \dots \subseteq I_1 \subsetneq R$ tali che $A \simeq \bigoplus_{k=1}^n R/I_k$.

Ha detto qualcosa su come applicarlo ai gruppi abeliani. Notare come tale teorema+corollario implica il Teorema di Jordan.

Lezione del 08/01/2020 (manca, ha dimostrato le cose scritte nelle sue note sui divisori elementari)

3.7 Forma canonica di Jordan

Lezione del 10/01/2020 (manca, ha parlato di forma canonica e Teorema di Jordan)

Lezione del 14/01/2020 (manca, corollari di Jordan e Cayley-Hamilton)

Lezione del 15/01/2020 (manca, recap del corso, aka questo fottutissimo delirio)