

Appunti di Algebra Superiore

Github Repository: [Oxke/appunti/AlgebraSuperiore](#)

Primo semestre, 2025 - 2026, prof. Alberto Canonaco

Libri utili

- Per la parte di algebra omologica Hilton-Stammbach, Osborne e Weibel.
- Dispense sui moduli (su KIRO) utili
- Aluffi, *Algebra Chapter 0*

Il corso è di 60 ore, non perché sia più pesante ma perché dovrebbero esserci ore di esercitazioni (non sarà necessariamente vero ma Canonaco cercherà di andare un po' nel dettaglio, fornire esempi e controesempi per quanto possibile)

0.1 Richiami sugli Anelli

Per convenzione, parlando di **anelli** si parlerà sempre di **anelli con unità**

Definizione 0.1.1: Anello

Un **anello** $A, +, \cdot$ è un gruppo abeliano $A, +$ (con 0 elemento neutro) e contemporaneamente un monoide A, \cdot (con 1 elemento neutro). Inoltre le due operazioni sono legate dalle proprietà distributive

$$a(b + c) = ab + ac \quad ; \quad (b + c)a = ba + ca$$

Diremo che l'anello è **commutativo** se l'operazione \cdot è commutativa

Per quasi tutto ciò che si vedrà in questo corso non è necessario andare a disturbare anelli non commutativi, dunque si useranno quasi sempre anelli commutativi.

Esempio 0.1.1. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{H}, \mathbb{Z}/n\mathbb{Z}$

Esempio 0.1.2. Se A è un anello (commutativo), allora i polinomi a coefficienti in A e con variabili in Λ costituiscono l'anello $A[x_\lambda \mid \lambda \in \Lambda]$

Esempio 0.1.3 (Anello Banale). L'anello composto da un solo elemento $\{0 = 1\}$

Esempio 0.1.4 (Non comm.). A anello, allora l'anello $M_n(A)$ delle matrici $n \times n$ a coefficienti in A non è commutativo se $n > 1$ (e se non è l'anello banale ma dall'anello banale non esiste davvero)

Esempio 0.1.5. Endomorfismi Se $(G, +)$ è un gruppo abeliano, allora $\text{End}(G)$ è anello con $+$ determinato da $(f + g)(a) = f(a) + g(a)$ e \cdot dato dalla composizione $(f \circ g)(a) = f(g(a))$

In generale se G, G' sono gruppi con $(G, +)$ abeliano, allora l'insieme $\text{Hom}(G', G)$ degli omomorfismi da G' a G è un sottogruppo di $G^{G'}$ il gruppo delle funzioni da G' a G .

Infatti se X è un insieme allora G^X è un gruppo con $(f + g)(a) = f(a) + g(a)$

Definizione 0.1.2: Invertibile

$a \in A$ è invertibile a sinistra (destra) se $\exists a' \in A$ tale che $a'a = 1$ ($aa' = 1$).
 a viene detto **invertibile** se $\exists a' \in A$ tale che $a'a = aa' = 1$

Osservazione (invertibile \iff invertibile a destra e sinistra). solo una implicazione non è ovvia. Se $a', a'' \in A$ sono tali che $a'a = aa'' = 1$ allora

$$\begin{aligned}(a'a)a'' &= a'(aa'') \\ 1a'' &= a'' = a' = a'1\end{aligned}$$

quindi a è invertibile e $a^{-1} = a' = a''$

Osservazione (Gruppo degli invertibili). L'insieme degli elementi invertibili forma un gruppo con l'operazione di prodotto e si indica con A^*

In generale, se $1 \neq 0$, allora $A^* \subseteq A \setminus \{0\}$

Definizione 0.1.3: Anello con Divisione

A si dice **anello con divisione** se $A^* = A \setminus \{0\}$. Un campo è un anello con divisione commutativo.

Definizione 0.1.4: Divisore di zero

$a \in A$ è detto **divisore di zero** a sinistra (destra) se $\exists a' \in A \setminus \{0\}$ tale che $aa' = 0$ ($a'a = 0$)

Osservazione. Divisore di zero a sinistra: $aa' = 0$. Invertibile a sinistra: $a'a = 1$

Definizione 0.1.5: Dominio

A viene detto **dominio** se $A \neq 0$ e A non ha divisori di zero. Viene inoltre chiamato **dominio di integrità** se è commutativo.

Esempio 0.1.6. I campi, \mathbb{Z} , se A dominio d'integrità, allora anche $A[x_\lambda \mid \lambda \in \Lambda]$ è dominio d'integrità.

Osservazione. $A \neq 0$ tale che $\forall 0 \neq a \in A$ è invertibile a sinistra, allora A è un anello con divisione.

Dimostrazione. $\exists a' \in A$ tale che $a'a = 1$ ma anche $\exists a'' \in A : a''a' = 1$. Allora a' è invertibile a sinistra e a destra, infatti

$$a'^{-1} = a = a'' \implies a \in A^*$$

□

Definizione 0.1.6: Sottoanello

$A' \subseteq A$ è **sottoanello** di A se $(A', +) < (A, +)$, $ab \in A'$ per ogni $a, b \in A'$ e $1 \in A'$

Esempio 0.1.7. $\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C} \subseteq \mathbb{H}$ sono tutti sottoanelli

Esempio 0.1.8. $A \subseteq A[X]$ sottoanello

Definizione 0.1.7: Ideale

$I \subseteq A$ è un'ideale sinistro (destro) se $(I, +) < (A, +)$ e $ab \in I$ ($ba \in I$), $\forall a \in A$ e $\forall b \in I$.

Un **ideale** bilatero è un ideale sia sinistro che destro.

Esempio 0.1.9. Gli ideali in \mathbb{Z} sono tutti e soli della forma $n\mathbb{Z}$, con $n \in \mathbb{N}$

Osservazione. Se I è un ideale sinistro o destro allora

$$I = A \iff I \cap A^* \neq \emptyset$$

quindi A con divisione \implies gli unici ideali sinistri o destri sono $\{0\}$ e A

Definizione 0.1.8: Anello opposto

L'**anello opposto** di un anello A è A^{op} , con $(A^{op}, +) := (A, +)$ e con prodotto ab in A^{op} definito come ba in A

Osservazione. $(A^{op})^{op} = A$ e $A^{op} = A \iff A$ commutativo

Proposizione 0.1.1 (Anello Quoziente). Se $I \subseteq A$ ideale, allora il gruppo abeliano $A/I, +$ è un anello con prodotto $\overline{a}\overline{b} := \overline{ab}$, dove $\overline{a} := a + I \in A/I$

Definizione 0.1.9: omomorfismo di anelli

Siano A, B anelli. $f : A \rightarrow B$ è **omomorfismo** di anelli se, $\forall a, a' \in A$

- i) $f(a + a') = f(a) + f(a')$
- ii) $f(aa') = f(a)f(a')$
- iii) $f(1_A) = 1_B$

ed è **isomorfismo** se è un omomorfismo biunivoco

Osservazione. f omomorfismo è isomorfismo $\iff \exists f' : B \rightarrow A$ omomorfismo tale che $f' \circ f = \text{id}_A$ e $f \circ f' = \text{id}_B$

Indicheremo $A \cong B$ se esiste un isomorfismo tra A e B

Proposizione 0.1.2. Se $f : A \rightarrow B$ è un omomorfismo allora

1. $A' \subseteq A$ è sottoanello $\implies f(A') \subseteq B$ è sottoanello.
2. $B' \subseteq B$ sottoanello $\implies f^{-1}(B') \subseteq A$ è sottoanello
3. $J \subseteq B$ è ideale (sinistro / destro) $\implies f^{-1}(J) \subseteq A$ è ideale (sinistro / destro). In particolare $\text{Ker } f := f^{-1}(0_B) \subseteq A$ è ideale
4. f **suriettivo** e $I \subseteq A$ ideale $\implies f(I) \subseteq B$ è ideale

Osservazione. $f : A \rightarrow B$ è iniettivo $\iff \text{Ker } f = \{0_A\}$ e in tal caso $A \cong \text{Im } f := f(A)$ che dunque è sottoanello di B

Teorema 0.1.3: Omomorfismo

$f : A \rightarrow B$ è omomorfismo di anelli, $I \subseteq A$ ideale tale che $I \subseteq \text{Ker } f$. Allora

$$\exists \bar{f} : A/I \rightarrow B \text{ omomorfismo tale che } \bar{f}(\bar{a}) = f(a) \quad \forall a \in A$$

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ \pi \downarrow & \nearrow \bar{f} & \\ A/I & & \end{array}$$

Inoltre $\text{im } \bar{f} = \text{im } f$ e $\text{Ker } \bar{f} = \text{Ker } f / I$

Proposizione 0.1.4. *Gli ideali di A/I sono tutti e soli della forma J/I con $J \subseteq A$ ideale tale che $I \subseteq J$*

Teorema 0.1.5: Primo teorema di isomorfismo

$f : A \rightarrow B$ è omomorfismo di anelli, allora $\text{im } f \cong A/\text{Ker } f$

Definizione 0.1.10: Ideale massimale (sinistro / destro)

Un ideale J (sinistro/destro) di A è massimale se $\forall I$ ideale (sinistro/destro) tale che $J \subseteq I \subseteq A$, allora $I = J$ o $I = A$

Osservazione. Esiste sempre un ideale (sinistro/destro) massimale (*lemma di Zorn*)

Definizione 0.1.11

L'ideale generato da $U \subseteq A$ è il più piccolo ideale di A che contiene $U = \bigcap_{U \subseteq I \subseteq A \text{ ideale}} I$ ed esplicitamente è

$$AUA := \left\{ \sum_{i=1}^n a_i u_i b_i : n \in \mathbb{N}, a_i, b_i \in A, u_i \in U \right\}$$

Osservazione. Se A è commutativo e $U = \{u\}$ allora $A\{u\}A = Au = \{au : a \in A\}$ (ideale principale)

Definizione 0.1.12: PID

A è un dominio (d'integrità) a ideali principali (PID) se ogni ideale di A è principale.

Esempio 0.1.10. Campi (non ci sono ideali propri)

Esempio 0.1.11. \mathbb{Z} (con ideali $n\mathbb{Z} = (n)$)

Esempio 0.1.12. $K[X]$ con K campo

0.2 Richiami sui Moduli

Definizione 0.2.1: A -modulo

Un A -modulo (di default sinistro) M è un gruppo abeliano $(M, +)$ con una moltiplicazione per scalare definita da

$$\begin{aligned} \cdot : A \times M &\longrightarrow M \\ (a, x) &\longmapsto ax \in M \end{aligned}$$

e tale che, $\forall a, b \in A$ e $\forall x, y \in M$:

- 1) $a(x + y) = ax + ay$
- 2) $(a + b)x = ax + bx$
- 3) $(ab)x = a(bx)$
- 4) $1x = x$

Osservazione. Se \mathbb{K} è un campo, allora un \mathbb{K} -modulo è uno spazio vettoriale.

Osservazione. Se $(M, +)$ è un gruppo abeliano, data $f : A \times M \rightarrow M$ posso definire $\alpha : A \rightarrow M^M$ come $\alpha(a) = (x \mapsto ax)$, e quindi le proprietà precedenti si traducono in

1. $\alpha(a)(x + y) = \alpha(a)(x) + \alpha(a)(y)$ e dunque $\alpha(a)$ è omomorfismo di gruppi, dunque $\alpha(A) \subseteq \text{End}(M)$
2. $\alpha(a + b) = \alpha(a) + \alpha(b)$ dunque $\alpha : A \rightarrow \text{End}(M)$ è omomorfismo di gruppi
3. $\alpha(a) \circ \alpha(b) = \alpha(ab)$
4. $\alpha(1) = \text{id}_M$

Dalla 2,3,4 $\alpha : A \rightarrow \text{End}(M)$ è omomorfismo di anelli.

Teorema 0.2.1: Secondo teorema di isomorfismo

Sia M un modulo, con $M', M'' \subseteq M$ sottomoduli. Allora

$$M'/(M' \cap M'') \cong (M' + M'')/M''$$

Dimostrazione. Si prenda $f : M' \rightarrow (M' + M'')/M''$ composizione dell'inclusione di M' in $M' + M''$ e della proiezione a quoziente, dunque è un omomorfismo.

Allora $\text{Ker} f = \{x \in M' : x + M'' = M''\} = M' \cap M''$.

Preso $y \in (M' + M'')/M''$, $y = x' + x'' + M'' = x' + M'' = f(x')$ dunque f è suriettiva. Dal primo teorema di isomorfismo segue la tesi. \square

Teorema 0.2.2: Terzo teorema di isomorfismo

Dati $M'' \subseteq M' \subseteq M$ sottomoduli e modulo, allora

$$(M/M')/(M'/M'') \cong M/M'$$

Dimostrazione. Sia f la composizione delle due proiezioni a quoziente, dunque è suriettiva. Allora

$$x \in \text{Ker} f \iff \pi(x) \in \text{Ker} \pi' = M'/M''$$

dunque $\text{Ker} f = M'$ da cui la tesi per il primo teorema di isomorfismo. \square

Proposizione 0.2.3.

1. Sia A un anello, allora un A -modulo M è ciclico se e solo se $\exists I \subseteq A$ ideale sinistro tale che $M \cong A/I$
2. M è semplice se e solo se $\exists I \subseteq A$ ideale sinistro massimale tale che $M \cong A/I$

Dimostrazione. 1. (\Leftarrow) A/I è ciclico (generato da $\bar{1}$). Viceversa per (\Rightarrow) so che $M = Ax$ per un qualche $x \in M$. Considerata $f :_A A \rightarrow M$ data da $a \mapsto ax$, $\text{Ker} f$ è sottomodulo di A , ovvero ideale sinistro. Concludo per il primo teorema di isomorfismo.

2. Se M è semplice allora $\forall 0 \neq x \in M, M = Ax$, dunque M è ciclico e per il punto 1. esiste I ideale sinistro tale che $M \cong A/I$. La proposizione si riduce a dire che A/I è semplice se e solo se I è massimale. Sappiamo che i sottomoduli di A/I sono tutti e soli della forma J/I con $I \subseteq J \subseteq A$ ideale sinistro. Allora $A/I \neq 0 \iff I \neq A$ e gli unici sottomoduli di A/I sono I/I e A/I , ossia gli unici ideali sinistri J tali che $I \subseteq J \subseteq A$ sono I e A .

□

Osservazione. Con il lemma di Zorn si dimostra che $A \neq 0 \implies$ esiste un ideale sinistro massimale (e dunque esiste un sottomodulo semplice)

0.2.1 Prodotti

Definizione 0.2.2: Prodotto

Supponiamo di avere M_λ A -moduli, per $\lambda \in \Lambda$. Allora

$$M := \prod_{\lambda \in \Lambda} M_\lambda \text{ è un } A\text{-modulo detto } \mathbf{prodotto} \text{ degli } M_\lambda$$

con $(x+y)_\lambda := x_\lambda + y_\lambda$ e $(ax)_\lambda = ax_\lambda$ per ogni $\lambda \in \Lambda$ e $x, y \in M$.

$\forall \mu \in \Lambda$ esiste $p_\mu : M \rightarrow M_\mu$, $(x_\lambda)_{\lambda \in \Lambda} \mapsto x_\mu$ che è A -lineare e suriettivo.

Proposizione 0.2.4 (Proprietà universale del prodotto).

Dati $f_\mu : N \rightarrow M_\mu$ A -lineari $\forall \mu \in \Lambda$, allora esiste unico $f : N \rightarrow M$ A -lineare tale che $f_\mu = p_\mu \circ f$

$$\begin{array}{ccc} N & & \\ f_\mu \downarrow & \searrow \exists! f & \\ M_\mu & \xleftarrow{p_\mu} & \prod_{\lambda \in \Lambda} M_\lambda \end{array}$$

Esercizio 0.2.1

Dimostrare la proprietà universale del prodotto

Definizione 0.2.3: Somma diretta

La **somma diretta** (o coprodotto) degli M_λ è

$$M' := \bigoplus_{\lambda \in \Lambda} M_\lambda = \{(x_\lambda)_{\lambda \in \Lambda} \in M : x_\lambda = 0 \text{ per finiti } \lambda \subseteq M\}$$

è sottomodulo.

$\forall \mu \in \Lambda$ esiste

$$i_\mu : M_\mu \longrightarrow M'$$

$$x \longmapsto i_\mu(x) = (x_\lambda)_{\lambda \in \Lambda}, \quad x_\lambda := \begin{cases} x & \lambda = \mu \\ 0 & \lambda \neq \mu \end{cases}$$

che è A -lineare e iniettivo.

Proposizione 0.2.5 (Proprietà universale somma diretta).

$$\begin{array}{ccc} & N & \\ f_\mu \uparrow & \nwarrow \exists! f & \\ M_\mu & \xrightarrow{i_\mu} & \bigoplus_{\lambda \in \Lambda} M_\lambda \end{array}$$

Osservazione. Se $\#\Lambda < +\infty$ allora

$$\bigoplus_{\lambda \in \Lambda} M_\lambda = \prod_{\lambda \in \Lambda} M_\lambda$$

Nota (zione). Se $M_\lambda = M$ per ogni $\lambda \in \Lambda$, si denota

$$\prod_{\lambda \in \Lambda} M =: M^\Lambda \quad \text{e} \quad \bigoplus_{\lambda \in \Lambda} M =: M^{(\Lambda)}$$

Dati $M_\lambda \subseteq M$ sottomoduli, con $\lambda \in \Lambda$, sia

$$f : \bigoplus_{\lambda \in \Lambda} M_\lambda \rightarrow M$$

l'omomorfismo indotto dalle inclusioni $M_\lambda \xrightarrow{i_\lambda} M$, allora

$$\text{im } f =: \sum_{\lambda \in \Lambda} M_\lambda \subseteq M \text{ è sottomodulo}$$

Inoltre f è iniettiva se e solo se $M_\mu \cap \sum_{\lambda \in \Lambda \setminus \{\mu\}} M_\lambda = 0$ per ogni $\mu \in \Lambda$ e in tal caso f induce un isomorfismo tra $\bigoplus_{\lambda \in \Lambda} M_\lambda$ e $\sum_{\lambda \in \Lambda} M_\lambda$ e si può scrivere $\bigoplus_{\lambda \in \Lambda} M_\lambda$ per indicare il sottomodulo di M

Definizione 0.2.4: Linearmente indipendente, base, modulo libero

Sia $U \subseteq M$ un insieme, con M A -modulo. Si dice che U è A -linearmente indipendente se dati $x_1, \dots, x_n \subseteq U$ distinti

$$a_1, \dots, a_n \in A \text{ t.c. } \sum_{i=1}^n a_i x_i = 0 \implies a_1 = \dots = a_n = 0$$

U è detta **base** di M se è linearmente indipendente e genera M , ossia $M = AU$. Si dice che M è **libero** se ammette una base

Esempio 0.2.1. Per ogni Λ , $A^{(\Lambda)}$ è libero con base $\{e_\lambda : \lambda \in \Lambda\}$ dove, per ogni $\lambda \in \Lambda$,

$$(e_\lambda)_i = \begin{cases} 1 & \lambda = i \\ 0 & \lambda \neq i \end{cases}$$

Proposizione 0.2.6. Siano L, M A -moduli, con L libero con base $\{l_\lambda : \lambda \in \Lambda\}$ tale che $l_\lambda \neq l_\mu$ se $\lambda \neq \mu$, allora

$$\forall \lambda \in \Lambda \quad \exists! f : L \rightarrow M \text{ } A\text{-lineare t.c. } f(l_\lambda) = x_\lambda$$

Corollario 0.2.6.1. Un A -modulo è libero se e solo se è isomorfo a $A^{(\Lambda)}$ per qualche Λ

Dimostrazione.

\implies M libero con base $\{x_\lambda : \lambda \in \Lambda\}$ con $x_\lambda \neq x_\mu$ se $\lambda \neq \mu$. Allora per la proposizione

$$\exists! f : A^\Lambda \rightarrow M \text{ } A\text{-lineare t.c. } f(e_\lambda) = x_\lambda$$

per ogni $\lambda \in \Lambda$. Allora $\text{im} f = \langle x_\lambda : \lambda \in \Lambda \rangle_A = M$ e f è iniettivo perché gli x_λ sono linearmente indipendenti.

\impliedby ovvio

□

Corollario 0.2.6.2. *Ogni A -modulo è insomorfo a un quoziente di un modulo libero $(A^{(\Lambda)})$ per un qualche Λ .*

Inoltre un A -modulo è finitamente generato se e solo se è isomorfo a un quoziente di A^n , $n \in \mathbb{N}$

Dimostrazione. Sia $\{x_\lambda\}_{\lambda \in \Lambda}$ un insieme di generatori di un modulo M . Per la proposizione $\exists! f : A^{(\Lambda)} \rightarrow M$ A -lineare tale che $fl_\lambda = x_\lambda$ per ogni $\lambda \in \Lambda$. Allora $\text{Im} f = M$ e dunque per il primo teorema di isomorfismo $M \cong A^{(\Lambda)} / \ker f$.

Per la seconda parte se M è finitamente generato posso scegliere Λ finito e viceversa $M \cong A^n / N$ è finitamente generato perché A^n lo è e $\pi : A^n \rightarrow A^n / N$ è un omomorfismo suriettivo.

□

Proposizione 0.2.7. *A è con divisione se e solo se ogni suo A -modulo è libero*

Dimostrazione.

\implies (complementi di algebra)

\impliedby Sia M un A -modulo semplice. Per ipotesi è libero, allora $M \cong A^{(\Lambda)}$ per un qualche Λ . Ma se $\#\Lambda > 1$ allora $A^{(\Lambda)}$ non è semplice ($A \subseteq A^{(\Lambda)}$ è un sottomodulo non banale). Inoltre $\Lambda \neq \emptyset$ ($A^{(\emptyset)} = \{0\}$ non è semplice).

Ne consegue che $M \cong A$ e dunque A è con divisione

□

Esempio 0.2.2. Con $A = \mathbb{Z}$, $\mathbb{Z}/p\mathbb{Z}$ non è libero

Si può dimostrare che se A è con divisione, allora tutte le basi di un A -modulo (libero) M hanno la stessa cardinalità, che viene detta rango e indicata con $\text{rk}_A M$.

In generale non tutte le basi di un A -modulo libero hanno la stessa cardinalità, esistono infatti anelli A non banali tali che $A \cong_A A^n$ per ogni $n \in \mathbb{N}$.

Esempio 0.2.3. Sia $A = \text{End}_{\mathbb{K}}(V)$ con \mathbb{K} campo e $\dim_{\mathbb{K}}(V) = +\infty$

Si dimostra che se $A \rightarrow B$ è omomorfismo di anelli e il rango dei B -moduli liberi è ben definito allora anche il rango degli A -moduli liberi è ben definito. Di conseguenza se $A \neq 0$ è commutativo allora il rango degli A -moduli liberi è ben definito ($\exists I \subseteq A$ ideale massimale e $\pi : A \rightarrow A/I$ omomorfismo con A/I campo)

0.2.2 restrizione degli scalari

Siano A, B anelli, con $f : A \rightarrow B$ omomorfismo di anelli. Allora se M è un B -modulo allora M è anche un A -modulo con $ax := f(a)x$. Si dice allora che ${}_A M$ è ottenuto da ${}_B M$ per **restrizione degli scalari** attraverso f .

Inoltre se $M' \subseteq M$ è B -sottomodulo allora è anche un A -sottomodulo e se $g : M \rightarrow N$ è B -lineare allora g è anche A -lineare.

Prima della prossima definizione ricordiamo che il **centro** di un anello è sottoanello, con il centro l'insieme degli elementi che commutano con tutti gli altri elementi e indicato con $Z(A)$,

$$Z(A) := \{z \in A : za = az \ \forall a \in A\}$$

Definizione 0.2.5

Sia A commutativo. Allora una A -algebra è un omomorfismo di anelli $f : A \rightarrow B$ tale che $\text{im} f \subseteq Z(B)$

Se f è evidente si dice che B è una A -algebra

Esempio 0.2.4. $M_n(A)$ è una A -algebra con $a \mapsto \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$

Esempio 0.2.5. Se $A = \mathbb{Z}$ per ogni B anello l'unico omomorfismo di anelli $\mathbb{Z} \rightarrow B$ è una \mathbb{Z} -algebra. Infatti l'omomorfismo unico $\mathbb{Z} \rightarrow Z(B)$ deve essere lo stesso di $\mathbb{Z} \rightarrow B$

Definizione 0.2.6: Morfismo di A -algre

Siano $f : A \rightarrow B, g : A \rightarrow C$ A -algre. Un (omo/iso/...)morfismo di A -algre da f a g è $h : B \rightarrow C$ (omo/iso/...)morfismo di anelli tale che $h \circ f = g$

$$\begin{array}{ccc} A & & \\ f \downarrow & \searrow g & \\ B & \xrightarrow{h} & C \end{array}$$

Esempio 0.2.6. Ogni omomorfismo di anelli è omomorfismo di \mathbb{Z} -algre.

Esempio 0.2.7. Sia $f : A \rightarrow B$ una A -algebra. Allora $\forall I \subseteq B$ ideale B/I è A -algebra con $\pi \circ f$

Osservazione (motivazione della definizione). Se $f : A \rightarrow B$ A -algebra, allora B è un anello e A -modulo (per restrizione degli scalari) tale che

$$a(bb') = (ab)b' = b(ab')$$

Lemma 0.2.8. Sia $0 \rightarrow M' \xrightarrow{i} M \xrightarrow{p} M''$ una successione esatta di A -moduli. Siano $f' : M' \rightarrow M'$ e $f'' : M'' \rightarrow M''$ omomorfismi. Allora esiste un diagramma commutativo con righe esatte

$$\begin{array}{ccccccc} 0 & \longrightarrow & A^m & \longrightarrow & A^{m+n} & \longrightarrow & A^n \longrightarrow 0 \\ & & \downarrow f' & & \downarrow f & & \downarrow f'' \\ 0 & \longrightarrow & M' & \xrightarrow{i} & M & \xrightarrow{p} & M'' \longrightarrow 0 \end{array}$$

Dimostrazione.

□

Proposizione 0.2.9. Sia $0 \rightarrow M' \xrightarrow{i} M \xrightarrow{p} M''$ esatta di A -moduli. Allora

1. $Mf.g. \implies M''f.g.$
2. $M', M''f.g. \implies Mf.g.$
3. $M', M''f.p. \implies Mf.p.$

$$4. Mf.g., M''f.p. \implies M'f.g.$$

$$5. M'f.g., Mf.p. \implies M''f.g.$$

Dimostrazione.

1. già visto
2. In esercizio la dimostrazione diretta. In alternativa possiamo applicare il lemma 0.2.2. Infatti esistono $f' : A^m \rightarrow M'$ e $f'' : A^n \rightarrow M''$ omomorfismi suriettivi e per il lemma 0.2.2 il diagramma

$$\begin{array}{ccccccc} 0 & \longrightarrow & A^m & \longrightarrow & A^{m+n} & \longrightarrow & A^n \longrightarrow 0 \\ & & \downarrow f' & & \downarrow f & & \downarrow f'' \\ 0 & \longrightarrow & M' & \xrightarrow{i} & M & \xrightarrow{p} & M'' \longrightarrow 0 \end{array}$$

commuta. Applicando ora il lemma del serpente otteniamo la successione esatta

$$\text{coKer } f' = 0 \rightarrow \text{coKer } f \rightarrow 0 = \text{coKer } f'' \implies \text{coKer } f = 0 \implies Mf.g.$$

3. Si può fare una dimostrazione simile a quella precedente e applicando il lemma del serpente troviamo la successione esatta

$$0 \rightarrow \text{Ker } f' \rightarrow \text{Ker } f \rightarrow \text{Ker } f'' \rightarrow 0 = \text{coKer } f'$$

per il punto 1. M è finitamente generato e dunque M è finitamente presentato.

4. $M''f.p. \implies \exists$ successione esatta $A^m \xrightarrow{g} A^n \xrightarrow{h} M'' \rightarrow 0$. Esiste dunque il diagramma commutativo

$$\begin{array}{ccccccc} A^m & \xrightarrow{g} & A^n & \xrightarrow{h} & M'' & \longrightarrow & 0 \\ & & \downarrow f' & & \downarrow f & & \downarrow \text{id} \\ 0 & \longrightarrow & M' & \xrightarrow{i} & M & \xrightarrow{p} & M'' \longrightarrow 0 \end{array}$$

infatti voglio f tale che $p \circ f = h$ e posso come prima (esercizio). allora per il lemma del serpente trovo che

$$0 \rightarrow \text{coKer } f' \rightarrow \text{coKer } f \rightarrow 0 = \text{coKer } \text{id}_{M''}$$

è una successione esatta, e dunque $\text{coKer } f' \cong \text{coKer } f = M/\text{Im } f$ per cui

$$0 \rightarrow \text{Im } f' \rightarrow M' \rightarrow \text{coKer } f' \rightarrow 0$$

è esatta. Concludiamo che $\text{Im } f' \cong A^m/\text{Ker } f'$ e dunque è $f.g.$, da cui anche M' è finitamente generato per il punto 1.

5. M è finitamente generato, dunque M'' è finitamente generato per il punto 0. Come prima $\exists A^m \rightarrow A^n, A^n \rightarrow M''$ omomorfismi suriettivi e trovo il diagramma del lemma 0.2.2 e applicando il lemma del serpente ottengo la successione esatta

$$\text{Ker } f \rightarrow \text{Ker } f'' \rightarrow 0 = \text{coKer } f'$$

Sia ora $f : A^{m+n} \rightarrow M$ suriettiva, allora

$$0 \rightarrow \text{Ker } f \rightarrow A^{m+n} \rightarrow M \rightarrow 0$$

è esatta, A^{m+n} è finitamente generata, M è finitamente presentato, dunque $\text{Ker } f$ è f.g., quindi per il punto 3. $\text{Ker } f''$ è f.g. e per il punto 0. M è f.p.

□

Esercizio 0.2.2

Dimostrare il punto 1. della dimostrazione precedente direttamente.

Corollario 0.2.9.1. Sia $M = \bigoplus_{i=1}^n M_i$. Allora M è f.g. / f.p. se e solo se M_i è f.g. / f.p. per ogni i .

Dimostrazione. La successione $0 \rightarrow \bigoplus_{i=1}^{n-1} M_i \rightarrow M \rightarrow M_n \rightarrow 0$ è esatta, dunque

\implies usando induzione su n e i punti 1. e 2. della proposizione precedente

$\iff M_n$ è f.g. per il punto 0., ed è f.p. per il punto 4.

□

Osservazione. per il punto 3., se M è f.p. allora ogni $A^n \xrightarrow{p} M \rightarrow 0$ esatta si estende a

$$A^m \rightarrow A^n \xrightarrow{p} M \rightarrow 0$$

Osservazione. Sia A non noetheriano. Allora $\exists M$ A -modulo f.g. non noetheriano, ad esempio $M = A$, ossia $\exists M' \subseteq M$ sottomodulo non f.g. e in tal caso anche quando M è finitamente presentato, ad esempio nel caso $M = A$, M/M' non è f.p. perché contraddirebbe il punto 3.

Uno può chiedersi dato un modulo se i suoi sottomoduli finitamente generati siano anche moduli finitamente presentati. Questo non è in generale vero ma motiva la seguente definizione

Definizione 0.2.7: Modulo coerente

Uno modulo M è detto **coerente** se è finitamente generato e tutti i suoi sottomoduli finitamente generati sono finitamente presentati.

Osservazione. Chiaramente essendo $M \subseteq M$ un sottomodulo, se è coerente è anche f.p.

Definizione 0.2.8: Anello coerente

Un anello A è **coerente** (a sinistra) se ${}_A A$ è A -modulo coerente (ossia tutti gli ideali sinistri f.g. di A sono f.p.)

Osservazione. Se A è noetheriano e M è un A -modulo, allora

$$M \text{ coerente} \iff M \text{ f.p.} \iff M \text{ f.g.} \iff M \text{ noetheriano}$$

in particolare A è coerente.

Dimostrazione. Sappiamo già che M noetheriano se e solo se M f.g. Resta da dimostrare dunque che M noetheriano se e solo se M è coerente. So che $M' \subseteq M$ f.g. è noetheriano (perché M lo è). Allora esiste la successione esatta

$$0 \rightarrow \text{Ker } p \rightarrow A^n \xrightarrow{p} M' \rightarrow 0$$

Ora poiché A è noetheriano, anche A^n lo è, e dunque $\text{Ker } p$ è noetheriano, dunque $\text{Ker } p$ è f.g. e infine M' è f.p. □

Osservazione. Sia A coerente non noetheriano, allora ${}_A A$ è coerente non noetheriano

Esempio 0.2.8. Sia A non noetheriano, $I \subseteq A$ ideale sinistro non f.g., allora A/I è f.g. non f.p. e A/I può anche essere noetheriano.

Un esempio è $A = \mathbb{K}[X_n | n \in \mathbb{N}]$, $I = (X_n | n \in \mathbb{N})$, $A/I = \mathbb{K}$

Osservazione. Sia $f : M \rightarrow N$ A -lineare, con M, N finitamente generati. Allora $\text{Im} f \cong M/\text{Ker} f$ e $\text{coKer} f \cong N/\text{Im} f$ sono finitamente generati (punto 0. della proposizione) ma non necessariamente anche $\text{Ker} f$ se A è non noetheriano.

Proposizione 0.2.10. Sia $0 \rightarrow M' \xrightarrow{i} M \xrightarrow{p} M'' \rightarrow 0$ esatta di A -moduli.

1. M' f.g. e M coerente, allora M'' è coerente
2. M', M'' coerenti, allora M è coerente
3. M è coerente, M'' è f.p., allora M' è coerente

in particolare M', M, M'' sono coerenti se due di essi lo sono.

Dimostrazione. 1. M'' è f.g. per il punto 0. della proposizione 0.2.2. $N'' \subseteq M''$ è f.g., allora c'è una successione esatta

$$0 \rightarrow M' \rightarrow N := p^{-1}(N'') \rightarrow N'' \rightarrow 0$$

Allora N è f.g. per 1. di 0.2.2 e dunque N è f.p. perché M è coerente, da cui N'' è f.p. per 4. di 0.2.2

2. M è f.g. per 1. di 0.2.2, se $N \subseteq M$ sottomodulo finitamente generato, allora esiste la successione esatta

$$0 \rightarrow N' := i^{-1}(N) \rightarrow N \rightarrow N'' := p(N) \rightarrow 0$$

Allora N'' è f.g. per 0. di 0.2.2 da cui N'' è f.p. per la coerenza di M , dunque N' è f.g. per 3. di 0.2.2. Segue dalla coerenza di M' che N' è f.p. e dunque N lo è per 2. di 0.2.2

3. M' è f.g. per 3. di 0.2.2 dunque M' è coerente perché $M' \cong i(M') \subseteq M$ sottomodulo è f.g. e M è coerente.

□

Esercizio 0.2.3

mostrare che

$$\bigoplus_{i=1}^n M_i \text{ coerente} \iff M_i \text{ coerente } \forall i$$

Corollario 0.2.10.1. Sia $f : M \rightarrow N$ A -lineare, M, N coerenti, allora $\text{Ker} f, \text{Im} f, \text{coKer} f$ sono coerenti.

Dimostrazione. $\text{Im} f \cong M/\text{Ker} f$ è f.g. per 0. di 0.2.2

□

Corollario 0.2.10.2. Se A è coerente e M è un A -modulo f.p., allora M è coerente.

Dimostrazione. Basta osservare che per definizione esiste una successione esatta

$$A^m \xrightarrow{f} A^n \rightarrow M \rightarrow 0$$

e in particolare dunque $M \cong \text{coKer} f$ e poiché A^m e A^n sono coerenti, lo è pure M

□

Esempio 0.2.9. Sia A commutativo tale che $A[X_1, \dots, X_n]$ sia coerente $\forall n \in \mathbb{N}$ (ad esempio A noetheriano, per il teorema della base di Hilbert) Allora $A[X_\lambda | \lambda \in \Lambda]$ è coerente $\forall \Lambda$, anche se non è noetheriano per $\#\Lambda = +\infty$ e $A \neq 0$.

Idea della dimostrazione. Sia $I \subseteq B$ ideale f.g., ossia $I = (f_1, \dots, f_n)$. Allora $\exists \Lambda_0 \subseteq \Lambda$ finito tale che $f_1 \in B_0 := A[X_\lambda | \lambda \in \Lambda_0]$ \square

Esempio 0.2.10 (Anello non coerente). Presi A e B come prima, ma supponiamo che $A = \mathbb{K}$ campo. Prendiamo dunque $J := (X_\lambda | \lambda \in \Lambda)$, con $\#\Lambda = +\infty$. Allora preso

$$C = B/J^2$$

non è coerente. Preso infatti ad esempio

$$I = C\overline{X_\lambda} \text{ con } \lambda \in \Lambda$$

è f.g. ma non f.p. perché c'è la successione esatta

$$0 \rightarrow J/J^2 \rightarrow C \rightarrow I \rightarrow 0$$

e J/J^2 è C -modulo annullato da J/J^2 e come $C/(J/J^2) \cong B/J \cong \mathbb{K}$ -modulo ha dimensione ∞ con base $\{\overline{x_\lambda} | \lambda \in \Lambda\}$

Capitolo 1

Categorie

Definizione 1.0.1: Categoria

Una **categoria** C è data da una classe di oggetti $\text{Ob}(C)$ e $\forall X, Y \in \text{Ob}(C)$ da un insieme di morfismi da X a Y indicato con $\text{Hom}(X, Y) = \text{Hom}_C(X, Y) = C(X, Y)$ e da una azione composizione di morfismi, cioè $\forall X, Y, Z \in \text{Ob}(C)$ (anche scritto $X, Y, Z \in C$) un'operazione

$$C(X, Y) \times C(Y, Z) \rightarrow C(X, Z)(f, g) \mapsto g \circ f$$

tale che

$$0. C(X, Y) \cap C(X', Y') \neq \emptyset \implies X = X' \text{ e } Y = Y'$$

1. \circ è associativa, cioè $\forall X, Y, Z, W \in C$ e $\forall f \in C(X, Y)$ e $\forall g \in C(Y, Z)$ e $\forall h \in C(Z, W)$ allora

$$h \circ (g \circ f) = (h \circ g) \circ f$$

2. $\forall X \in C$ esiste $1_X = \text{id}_X \in C(X, X)$ che è elemento neutro di X cioè $\forall Y \in C$ e $\forall f \in C(X, Y)$,

$$f \circ 1_X = f \quad , \quad 1_Y \circ f = f$$

Esempio 1.0.1. La categoria degli insiemi **Set** che ha come oggetti tutti gli insiemi e $\forall X, Y \in \text{Set}$ i morfismi $\text{Set}(X, Y) = \{f : X \rightarrow Y\}$ le funzioni e \circ la composizione di funzioni

Osservazione. Se ho C tale che valgano solo 1. e 2. e non necessariamente 0. posso ottenere la categoria C' che soddisfa anche 0. ponendo $\text{Ob}(C') := \text{Ob}(C)$ e

$$C'(X, Y) := \{X\} \times C(X, Y) \times \{Y\}$$

Esempio 1.0.2. Le categorie concrete, in cui gli oggetti sono insiemi con qualche struttura e i morfismi sono funzioni tra insiemi che preservano la struttura (con \circ sempre la composizione di funzioni). In particolare:

- La categoria **Grp** dei gruppi, dove gli oggetti sono i gruppi e i morfismi gli omomorfismi di gruppi
- La categoria **Rng** degli anelli
- Dato un anello A , la categoria $A - \text{Mod} / \text{Mod} - A$ degli A -moduli sinistri / destri

- Dato un anello commutativo A , la categoria $\mathbf{A-Alg}$ delle A -algebre
- La categoria \mathbf{Top} degli spazi topologici (con funzioni continue come morfismi)

Nota. Dato $f \in C(X, Y)$ si può indicare con $f : X \rightarrow Y$ “come fosse una funzione”

Esempio 1.0.3. Le categorie discrete, cioè tali che gli unici morfismi sono 1_X per ogni $X \in C$.

Esempio 1.0.4. C tale che $\forall X, Y \in C, \#C(X, Y) = 1$, ottengo una relazione \preccurlyeq su $\text{Ob}(C)$ in cui

$$X \preccurlyeq Y \iff C(X, Y) \neq \emptyset$$

e \preccurlyeq è riflessivo (perché $\exists 1_X \in C(X, X) \forall X \in C$) e transitivo, perché $\exists \circ$. Ne consegue che \preccurlyeq è un *preordine*

Viceversa, data una relazione di preordine \preccurlyeq su un insieme (o una classe) S , ottengo una categoria C con $\text{Ob}(C) := S$ e $\forall X, Y \in S$,

$$C(X, Y) := \begin{cases} \{f_{X,Y}\} & \text{se } X \preccurlyeq Y \\ \emptyset & \text{altrimenti} \end{cases}$$

con l'unica composizione possibile

Esempio 1.0.5 (Categoria Vuota). Prendendo $\text{Ob}(C) = \emptyset$

Osservazione. $\forall X \in C$ con C una categoria, $\text{End}_C(X) := C(X, X)$ è un monoide con \circ , ne consegue il prossimo esempio

Esempio 1.0.6 (Monoide). Una categoria con un solo oggetto è un monoide. Viceversa ogni monoide può essere visto come categoria di un solo oggetto.

Esempio 1.0.7 (Diagrammi). Possiamo definire categorie date da diagrammi, in cui si rappresentano i morfismi (non l'identità). Ad esempio:

$$\bullet \longrightarrow \bullet \qquad \bullet \rightrightarrows \bullet \qquad \bullet \longrightarrow \bullet \longleftarrow \bullet$$

sono tre categorie diverse, rispettivamente con 2, 2, e 3 oggetti

Definizione 1.0.2: Categoria opposta

La **categoria opposta** di C è denotata C^{op} ed è definita da

$$\text{Ob}(C^{op}) := \text{Ob}(C) \quad C^{op}(X, Y) := C(Y, X)$$

con composizione in \circ^{op} data da $f \circ^{op} g := g \circ f$

Osservazione.

$$(C^{op})^{op} = C$$

Esempio 1.0.8 (Categoria Prodotto). Siano C_λ per $\lambda \in \Lambda$ delle categorie. Allora la categoria prodotto

$$C := \prod_{\lambda \in \Lambda} C_\lambda$$

è definita da

$$\begin{aligned} \text{Ob}(C) &:= \prod_{\lambda \in \Lambda} \text{Ob}(C_\lambda) \\ C((X_\lambda)_{\lambda \in \Lambda}, (Y_\lambda)_{\lambda \in \Lambda}) &:= \prod_{\lambda \in \Lambda} C_\lambda(X_\lambda, Y_\lambda) \\ (g_\lambda)_{\lambda \in \Lambda} \circ (f_\lambda)_{\lambda \in \Lambda} &:= (g_\lambda \circ f_\lambda)_{\lambda \in \Lambda} \end{aligned}$$

Esempio 1.0.9 (Categoria Coprodotto). La categoria coprodotto

$$C := \coprod_{\lambda \in \Lambda} C_\lambda$$

è definita con $\text{Ob}(C) := \coprod_{\lambda \in \Lambda} \text{Ob}(C_\lambda)$ l'unione disgiunta.

$$\forall X, Y \in C \quad C(X, Y) := \begin{cases} C_\lambda(X, Y) & \text{se } X, Y \in C_\lambda \text{ per qualche } \lambda \in \Lambda \\ \emptyset & \text{altrimenti} \end{cases}$$

con \circ ovvia.

Definizione 1.0.3: Sottocategoria

Sia C una categoria. Allora una sottocategoria C' di C è data da una sottoclasse $\text{Ob}(C') \subseteq \text{Ob}(C)$ e $\forall X, Y \in C'$ da un sottoinsieme $C'(X, Y) \subseteq C(X, Y)$ tale che \circ si restringe a C' e $1_X \in C'(X, X)$ per ogni $X \in C'$. In particolare C' è una categoria.

Esempio 1.0.10. Se C è un monoide (categoria di un oggetto), allora le sottocategorie non vuote di C sono i sottomonoidi.

Definizione 1.0.4: Sottocategoria Piena

Una sottocategoria C' di C si dice **piena** se $C'(X, Y) = C(X, Y)$ per ogni $X, Y \in C'$

Osservazione. Una sottocategoria piena di C equivale a dare una sottoclasse di $\text{Ob}(C)$

Esempio 1.0.11 (Gruppi Abeliani). $\mathbf{Ab} \subseteq \mathbf{Grp}$ sottocategoria piena dei gruppi abeliani. Similmente anche $\mathbf{CRng} \subseteq \mathbf{Rng}$ sottocategoria piena degli anelli commutativi.

Oltre alle sotto-strutture sono anche importanti i quozienti, e anche qui possiamo dare una definizione astratta

Definizione 1.0.5: Congruenza

Una congruenza \sim su una categoria C è data da una relazione di equivalenza \sim su $C(X, Y) \forall X, Y \in C$ tale che

$$\forall X, Y, Z \in C, \forall f, f' \in C(X, Y) \forall g, g' \in C(Y, Z) \quad f \sim f', g \sim g' \implies g \circ f \sim g' \circ f'$$

$$\text{equivalentemente } g \sim g' \implies g \circ f \sim g' \circ f \text{ e } h \circ g \sim h \circ g'$$

Definizione 1.0.6: Quoziente

Sia \sim una congruenza su C , allora possiamo definire la categoria quoziente C/\sim definita da

$$\text{Ob}(C/\sim) = \text{Ob}(C) \quad (C/\sim)(X, Y) := C(X, Y)/\sim \quad \forall X, Y \in C$$

e \circ è indotta da quella di C , ossia

$$\bar{g} \circ \bar{f} := \overline{g \circ f}$$

Esempio 1.0.12 (Omotopia). Sia $C = \mathbf{Top}$ e \sim_h l'omotopia, ossia $f, g : X \rightarrow Y$ sono omotope se $\exists H : X \times [0, 1] \rightarrow Y$ continue tali che

$$f(x) = H(x, 0), \quad g(x) = H(x, 1) \quad \forall x \in X$$

e si ottiene $\mathbf{Toph} := \mathbf{Top} / \sim_h$

Esempio 1.0.13 (Gruppo quoziente). Sia G un gruppo (visto come monoide, ossia categoria di un oggetto) e sia $H \triangleleft G$ e \sim su G data da $a \sim b \iff aH = bH$. Viceversa ogni \sim congruenza su G si può scrivere in tal modo prendendo $H = \{a \in G : a \sim 1\} \triangleleft G$ (esercizio).

Definizione 1.0.7: morfismo invertibile

Sia $f : X \rightarrow Y$ un morfismo in una categoria C . Allora esso è invertibile a sinistra (destra) se $\exists f' : Y \rightarrow X$ tale che $f' \circ f = 1_X$ ($f \circ f' = 1_Y$).

Osservazione. f è invertibile a sinistra (destra) in C , allora f è invertibile a destra (sinistra) in C^{op}

Definizione 1.0.8: Isomorfismo

$f : X \rightarrow Y$ è un **isomorfismo** se $\exists f' : Y \rightarrow X$ tale che $f' \circ f = 1_X$ e $f \circ f' = 1_Y$

Osservazione. f è isomorfismo se e solo se f è invertibile a destra e a sinistra.

Dimostrazione.

\implies ovvio

\impliedby $\exists f', f''$ tale che $f' \circ f = 1_X$ e $f \circ f'' = 1_Y$, allora

$$f' \circ (f \circ f'') = f' = f'' = (f' \circ f) \circ f''$$

e dunque f è invertibile.

In particolare dunque la f' della definizione di isomorfismo è unica e viene denotata f^{-1} \square

Definizione 1.0.9

Siano $X, Y \in C$. Allora X e Y sono isomorfe ($X \cong Y$) se esiste un $f : X \rightarrow Y$ isomorfismo.

Osservazione. 1_X è isomorfismo e $1_X^{-1} = 1_X$. Se f isomorfismo allora f^{-1} isomorfismo e $(f^{-1})^{-1} = f$. Se f, g isomorfismi componibili, allora $g \circ f$ è isomorfismo e $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$

Ne segue che \cong è una relazione di equivalenza su $\mathbf{Ob}(C)$

Definizione 1.0.10

Un morfismo $f : X \rightarrow Y$ in C è detto **monomorfismo** se $\forall Z \in C$ la funzione

$$\begin{aligned} f_* : C(Z, X) &\longrightarrow C(Z, Y) \\ g &\longmapsto f_*(g) = f \circ g \end{aligned}$$

è iniettiva

Definizione 1.0.11: Epimorfismo

f è un **epimorfismo** in C se è monomorfismo in C^{op} , ossia $\forall Z \in C$ la funzione

$$\begin{aligned} f^* : C(Y, Z) &\longrightarrow C(X, Z) \\ g &\longmapsto f^*(g) = g \circ f \end{aligned}$$

è iniettiva.

Proposizione 1.0.1. f è invertibile a sinistra (destra), allora f è monomorfismo (epimorfismo)

Dimostrazione. Basta dimostrare che se f è invertibile a sinistra, allora è mono.

Sappiamo che $\exists f' : Y \rightarrow X$ tale che $f' \circ f = 1_X$. Dobbiamo dimostrare che f_* è iniettiva. Siano $g, h \in C(Z, X)$ tali che $f_*(g) = f_*(h)$. Allora $f \circ g = f \circ h$, da cui $f' \circ f \circ g = f' \circ f \circ h$ e dunque $g = h$ \square

Proposizione 1.0.2. Sia C concreta. Allora

$$f \text{ invertibile a sinistra (destra)} \implies f \text{ iniettiva (suriettiva)} \implies f \text{ mono (epi)}$$

Dimostrazione. Non possiamo usare il trick della categoria opposta, perché non è detto che C^{op} sia ancora concreta.

Sia f' tale che $f' \circ f = 1_X$ ($f \circ f' = 1_Y$), allora chiaramente f iniettiva (suriettiva) perché le composizioni 1_X e 1_Y sono biunivoche.

Se f è iniettiva, allora se f è suriettiva, allora \square

In generale non vale nessuna delle \Leftarrow .

Esempio 1.0.14. In **Set** se $f : X \rightarrow Y$ è suriettiva, allora f è invertibile a sinistra. Infatti basta scegliere (AOC) $f'(y) \in f^{-1}\{y\}$ per ogni $y \in Y$. Inoltre se $X \neq \emptyset$ e $f : X \rightarrow Y$ è iniettiva, allora f è invertibile a sinistra.

Esercizio 1.0.1

In $\mathbf{A} - \mathbf{Mod}$, mostrare che $f : M \rightarrow N$ iniettiva è invertibile a sinistra se e solo se $\text{Im}(f) \subseteq N$ è addendo diretto.

Mostrare che $f : M \rightarrow N$ suriettiva è invertibile a destra se e solo se $\text{Ker}(f) \subseteq M$ è addendo diretto

Concludere che valgono sempre entrambe le implicazioni se e solo se A è semisemplice.

Esempio 1.0.15. In **Set**, se f è mono (epi), allora f è iniettiva (suriettiva).

Infatti, poniamo per assurdo $f : X \rightarrow Y$ non iniettiva, dunque siano $x, y \in X$ tali che $f(x) = f(y)$. Allora preso $Z = \{z\}$ e $g, h : Z \rightarrow X$ tali che $g(z) = x$ e $h(z) = y$ abbiamo che $f \circ g = f \circ h$ da cui $g = h$ e dunque $x = y$

Supponiamo f non suriettiva, mostrare per esercizio $\exists g, h : Y \rightarrow Z$ tali che $g \neq h$ ma $g \circ f = h \circ f$

Esempio 1.0.16. In $\mathbf{A} - \mathbf{Mod}$ $f : M \rightarrow N$ è mono (epi), allora f è iniettiva (suriettiva).

Infatti $i : \text{Ker} f \rightarrow M$ inclusione tale che $f \circ i = 0$ e anche $0 : \text{Ker} f \rightarrow M$ è tale che $f \circ 0 = 0$. Concludiamo che $i = 0$ e dunque $\text{Ker} f = 0$.

Similmente $\pi : N \rightarrow \text{coKer} f$ è tale che $\pi \circ f = 0$ e se f è epi allora $0 = \pi$ e dunque $\text{coKer} f = 0$ e dunque f è suriettiva.

Esempio 1.0.17. In \mathbf{Grp} f mono (epi), allora f iniettiva (suriettiva)

Per mono \implies iniettiva si può usare la stessa dei moduli, mentre per l'altra è un po' più complicato, ma si dimostra che è vero lo stesso

Esempio 1.0.18. In \mathbf{Rng} $f : A \rightarrow B$ mono, allora f iniettiva.

Tuttavia f epi **non implica** f suriettiva. Ad esempio preso $i : \mathbb{Z} \hookrightarrow \mathbb{Q}$ è epi, infatti $\forall A$ anello esiste al più un omomorfismo $\mathbb{Q} \rightarrow A$ ($f : \mathbb{Q} \rightarrow A$ sia omomorfismo, allora $f|_{\mathbb{Z}}$ è l'unico omomorfismo e $f(\frac{a}{b}) = f(a)f(b)^{-1}$). Chiaramente però non è suriettiva.

Definizione 1.0.12: Funtore

Un funtore $F : C \rightarrow D$ tra 2 categorie è dato da una funzione $F : \text{Ob}(C) \rightarrow \text{Ob}(D)$ e $\forall X, X' \in C$ una funzione $F = F_{X,X'} : C(X, X') \rightarrow D(F(X), F(X'))$ tale che

$$F(g \circ f) = F(g) \circ F(f)$$

(se f e g sono componibili in C) e $F(1_X) = 1_{F(X)}$ per ogni $X \in C$

Proposizione 1.0.3. Sia F un funtore e f invertibile a sinistra (destra). Allora $F(f)$ è invertibile a sinistra (destra)

Dimostrazione. $\exists f'$ tale che $f' \circ f = 1_X$, allora $F(f') \circ F(f) = F(f' \circ f) = F(1_X) = 1_{F(X)}$. \square

Osservazione. Segue che f iso, allora $F(f)$ iso e $F(f)^{-1} = F(f^{-1})$

Esempio 1.0.19. Sia $C' \subseteq C$ sottocategoria. Allora $C' \rightarrow C$, $x \mapsto x$ e $f \mapsto f$ è un funtore

Esempio 1.0.20. Se \sim è una congruenza, allora $C \rightarrow C/\sim$ è un funtore, con $x \mapsto x$ e $f \mapsto f$

Esempio 1.0.21 (Funtore dimenticante). $C \rightarrow \mathbf{Set}$ con C categoria discreta e $x \mapsto x$, $f \mapsto f$ è un funtore, che “dimentica” la struttura aggiunta.

Analogamente anche $\mathbf{Rng} \rightarrow \mathbf{Ab}$, con $(A, +, \cdot) \rightarrow (A, +)$ è un funtore dimenticante.

Esempio 1.0.22. Sia $A \rightarrow B$ un omomorfismo di anelli. Allora la restrizione degli scalari è un funtore $B - \mathbf{Mod} \rightarrow A - \mathbf{Mod}$

Esempio 1.0.23. Funtore tra 2 categorie discrete C e D è una funzione $\text{Ob}(C) \rightarrow \text{Ob}(D)$

Esempio 1.0.24. Un funtore tra 2 preordini C e D è una funzione $\text{Ob}(C) \rightarrow \text{Ob}(D)$ che preserva la relazione di preordine.

Esempio 1.0.25. Un funtore tra 2 monoidi è un omomorfismo di monoidi.

Più in generale dato un monoide e una categoria C , un funtore $G \rightarrow C$ è dato da $X \in C$ e da un omomorfismo di monoidi $G \rightarrow \text{End}_C(X)$

Se G è un gruppo un funtore $G \rightarrow C$ è dato da $X \in C$ e un omomorfismo di gruppi $G \rightarrow \text{Aut}_C(X)$. Ad esempio se $C = \mathbf{Set}$ il funtore dà un'azione di un gruppo su un insieme.