

# Istituzioni di Algebra e Geometria 2022-23

Marco Manetti a Roma

*Versione preliminare del 26 gennaio 2023:*

*l'autore ringrazia tutti coloro che segnalano ed hanno segnalato errori ed imprecisioni*

**Avvertenza:** Queste dispense sono ancora nella fase work in progress e contengono inevitabilmente molte lacune, imprecisioni ed errori di stampa. Sono distribuite, senza alcuna garanzia, esclusivamente per gli usi relativi all'insegnamento di Istituzioni di Algebra e Geometria 2022-23, Corso di laurea Magistrale in Matematica Applicata, Sapienza Università di Roma.

# Indice

Capitolo 1. Complessi simpliciali	1
1.1. Convessi in $\mathbb{R}^n$	1
1.2. Complessi simpliciali astratti	5
1.3. Realizzazioni geometriche	10
1.4. Grafi semplici e complessi di cricche	12
1.5. Brevi cenni su categorie e funtori	15
Capitolo 2. Elementi di algebra omologica	17
2.1. Preliminari di teoria dei gruppi	17
2.2. Gruppi abeliani finiti	19
2.3. Gruppi abeliani liberi	20
2.4. Successioni esatte	23
2.5. Gruppi abeliani finitamente generati	26
2.6. Additività del rango	28
2.7. Razionalizzazione di gruppi abeliani	35
2.8. Complessi di catene e omologia	36
Capitolo 3. Omologia simpliciale	43
3.1. Omologia dei complessi simpliciali astratti	43
3.2. Morfismi e classi di contiguità	46
3.3. La successione esatta di Mayer–Vietoris	50
3.4. Il sottocomplesso delle catene ordinate	54
3.5. Numeri di Betti e caratteristica di Eulero–Poincaré	60
3.6. Omologia a coefficienti $\mathbb{T}_2$ e semplici positivi	63
Capitolo 4. Insiemi simpliciali e omologia singolare	67
4.1. Insiemi simpliciali	67
4.2. Omologia degli insiemi simpliciali	71
4.3. Complementi: catene degeneri e complesso di Moore	74
4.4. Introduzione all’omologia singolare	77
4.5. Omologia con coefficienti	83
Capitolo 5. Spazi pseudometrici	85
5.1. Proprietà ed esempi basilari	85
5.2. Le distanze di Hausdorff e del collo di bottiglia	87
5.3. La distanza di contiguità	89
5.4. Distanza di interfoglia	92
Capitolo 6. Omologia Persistente	97
6.1. L’incredibile ubiquità della topologia persistente	97
6.2. Allarga i punti e sfoca le immagini	98
6.3. Complessi filtrati	99
6.4. Moduli di persistenza	103
6.5. Barcode e diagramma di persistenza	108
6.6. Basi cicliche e basi di persistenza	112
6.7. Stabilità del diagramma di persistenza	117
Capitolo 7. Geometria affine e proiettiva	121

7.1.	Il teorema di Menelao	121
7.2.	Indipendenza affine e combinazioni baricentriche	125
7.3.	Spazi e applicazioni affini	129
7.4.	Curve di Bezier	133
7.5.	Spazi proiettivi	135
7.6.	Sistemi di riferimento e coordinate omogenee	140
7.7.	Proiezioni	143
7.8.	Prospettive	148
7.9.	Il birapporto	151
Capitolo 8.	Curve algebriche piane	159
8.1.	Polinomi numerici	159
8.2.	Polinomi omogenei	162
8.3.	Ipersuperfici proiettive	168
8.4.	Curve piane	170
8.5.	Retta tangente e punti di flesso	176
8.6.	Le coniche	179
8.7.	Sistemi lineari	180
8.8.	Curve ellittiche	185
Capitolo 9.	I teoremi della base e degli zeri di Hilbert	189
9.1.	Operazioni sugli ideali	189
9.2.	Polinomi e fattorizzazione unica	192
9.3.	Anelli graduati	196
9.4.	Anelli Noetheriani	199
9.5.	Il risultante	201
9.6.	Il teorema degli zeri di Hilbert	203
Bibliografia		207

## Complessi simpliciali

### 1.1. Convessi in $\mathbb{R}^n$

Ricordiamo che un sottoinsieme  $C \subset \mathbb{R}^n$  si dice **convesso** se per ogni  $x, y \in C$  ed ogni  $t \in [0, 1]$  vale  $tx + (1-t)y \in C$ , ossia se  $C$  contiene il segmento di estremi  $x$  e  $y$ .

ESEMPIO 1.1.1. Il vuoto,  $\mathbb{R}^n$  e ogni sottospazio vettoriale sono sottoinsiemi convessi.

ESEMPIO 1.1.2. Per ogni  $p \in \mathbb{R}^n$  ed ogni  $r \in \mathbb{R}$ ,  $r \geq 0$ , la palla chiusa

$$U_p(r) = \{x \in \mathbb{R}^n \mid \|x - p\| \leq r\}$$

è un sottoinsieme convesso. Infatti per ogni  $x, y \in U_p(r)$  ed ogni  $t \in [0, 1]$  per la disuguaglianza triangolare si ha

$$\|tx + (1-t)y - p\| = \|(t(x-p) + (1-t)(y-p))\| \leq \|t(x-p)\| + \|(1-t)(y-p)\|,$$

e siccome  $t, 1-t$  sono entrambi non negativi

$$\|t(x-p)\| + \|(1-t)(y-p)\| = t\|x-p\| + (1-t)\|y-p\| \leq tr + (1-t)r = r.$$

ESEMPIO 1.1.3. Per ogni coppia di punti  $p, q \in \mathbb{R}^n$  l'insieme

$$C = \{x \in \mathbb{R}^n \mid \|x - p\| \leq \|x - q\|\}$$

è convesso. Denotando con  $\cdot$  il prodotto scalare standard in  $\mathbb{R}^n$ , ossia  $x \cdot y = \sum_i x_i y_i$ , si ha

$$\begin{aligned} C &= \{x \in \mathbb{R}^n \mid \|x - p\|^2 \leq \|x - q\|^2\} = \{x \in \mathbb{R}^n \mid 2x \cdot (q - p) \leq \|q\|^2 - \|p\|^2\} \\ &= \{x \in \mathbb{R}^n \mid (2x - p - q) \cdot (q - p) \leq 0\} \end{aligned}$$

da cui segue che  $C$  è un semispazio chiuso ed anche convesso.

Per **combinazione convessa** di un insieme finito di vettori  $x_0, \dots, x_m \in \mathbb{R}^n$  si intende una qualunque combinazione lineare del tipo

$$\sum_{i=0}^s t_i x_i, \quad \text{con} \quad \sum_{i=0}^s t_i = 1 \quad \text{e} \quad t_i \geq 0 \quad \text{per ogni } i.$$

Si noti che l'unica combinazione convessa di un vettore  $x$  è  $1x = x$  e che le combinazioni convesse di due vettori  $x, y$  sono tutte e sole quelle del tipo  $tx + (1-t)y$  al variare di  $t$  nell'intervallo chiuso  $[0, 1]$ .

Per ogni successione finita  $x_0, \dots, x_p \subset \mathbb{R}^n$  indichiamo con  $\langle x_0, \dots, x_p \rangle \subset \mathbb{R}^n$  l'insieme di tutte le sue combinazioni convesse, ossia:

$$\langle x_0, \dots, x_p \rangle = \left\{ \sum t_i x_i \in \mathbb{R}^n \mid t_i \geq 0, \sum t_i = 1 \right\}.$$

Si pone inoltre per convenzione  $\langle \emptyset \rangle = \emptyset$ .

Si vede facilmente che  $\langle x_0, \dots, x_p \rangle$  è convesso, infatti per ogni  $y = \sum \mu_i x_i, z = \sum \lambda_i x_i \in \langle x_0, \dots, x_p \rangle$  ed ogni  $t \in [0, 1]$  si ha

$$ty + (1-t)z = \sum_{i=0}^p (t\mu_i + (1-t)\lambda_i)x_i \in \langle x_0, \dots, x_p \rangle.$$

LEMMA 1.1.4. Siano  $M \subset \mathbb{R}^n$  e

$$v: \{0, \dots, m\} \rightarrow M, \quad i \mapsto v_i, \quad x: \{0, \dots, p\} \rightarrow M, \quad j \mapsto x_j,$$

due applicazioni surgettive. Allora

$$\langle v_0, \dots, v_m \rangle = \langle x_0, \dots, x_p \rangle.$$

DIMOSTRAZIONE. Per simmetria basta provare che  $\langle v_0, \dots, v_m \rangle \subseteq \langle x_0, \dots, x_p \rangle$ . Scriviamo  $\{0, \dots, m\} = \cup_{j=0}^p S_j$ , con  $S_j = \{i \mid v_i = x_j\}$ . Sia  $y = \sum_i t_i v_i \in \langle v_0, \dots, v_m \rangle$ , allora

$$y = \sum_j \sum_{i \in S_j} t_i v_i = \sum_j \left( \sum_{i \in S_j} t_i \right) x_j = \sum_j \lambda_j x_j,$$

dove  $\lambda_j = \sum_{i \in S_j} t_i$ .  $\square$

Dunque per ogni sottoinsieme finito  $M \subset \mathbb{R}^n$  ha senso definire  $\langle M \rangle$ : presa una qualunque indicizzazione  $M = \{x_0, \dots, x_p\}$  si pone  $\langle M \rangle = \langle x_0, \dots, x_p \rangle$ .

LEMMA 1.1.5. *Un sottoinsieme  $C \subset \mathbb{R}^n$  è convesso se e solo se è chiuso per combinazioni convesse, ossia se per ogni sottoinsieme finito  $M \subset C$  vale  $\langle M \rangle \subset C$ .*

DIMOSTRAZIONE. Una implicazione è ovvia in quanto la definizione di convessità è del tutto equivalente al fatto che  $\langle x, y \rangle \subset C$  per ogni  $x, y \in C$ .

Viceversa, supponiamo  $C$  convesso e dimostriamo per induzione su  $m$  che ogni combinazione convessa di  $m$  elementi di  $C$  appartiene ancora a  $C$ . Si consideri una combinazione convessa

$$y = \sum_{i=0}^m t_i x_i, \quad \sum_{i=0}^s t_i = 1, \quad t_i \geq 0, \quad x_i \in C.$$

Se  $t_0 = 1$  allora  $t_i = 0$  per ogni  $i > 0$  e  $y = x_0 \in C$ . Se  $t_0 < 1$  possiamo scrivere

$$y = t_0 x_0 + (1 - t_0) z, \quad z = \sum_{i=1}^m \frac{t_i}{1 - t_0} x_i.$$

Siccome  $\sum_{i=1}^m \frac{t_i}{1 - t_0} = 1$  per induzione si ha  $z \in C$  e quindi  $y \in C$  per convessità.  $\square$

Più in generale, per ogni sottoinsieme  $M \subset \mathbb{R}^n$  definiamo il suo **inviluppo convesso**  $\langle M \rangle$  come l'insieme di tutte le combinazioni convesse di successioni finite in  $M$ :

$$\langle M \rangle = \left\{ \sum_{i=0}^p t_i x_i \mid p \geq 0, x_i \in M, t_i \geq 0, \sum t_i = 1 \right\}.$$

PROPOSIZIONE 1.1.6. *Per ogni  $M \subset \mathbb{R}^n$  il suo inviluppo convesso  $\langle M \rangle$  è il più piccolo insieme convesso contenente  $M$ .*

DIMOSTRAZIONE. Segue immediatamente dalla definizione che ogni intersezione di insiemi convessi è ancora convessa. Denotiamo provvisoriamente con  $C(M)$  l'intersezione di tutti i convessi che contengono  $M$ . Siccome  $\mathbb{R}^n$  è convesso ne segue che  $M \subset C(M)$ .

Dobbiamo dimostrare che  $\langle M \rangle = C(M)$ . L'inclusione  $\langle M \rangle \subseteq C(M)$  è facile: infatti  $C(M)$  è convesso e quindi chiuso per combinazioni convesse, per ogni  $x_0, \dots, x_p \in M \subset C(M)$  si ha quindi  $\langle x_0, \dots, x_p \rangle \subset C(M)$ .

Viceversa, siccome  $M \subset \langle M \rangle$ , per dimostrare che  $C(M) \subseteq \langle M \rangle$  è sufficiente provare che  $\langle M \rangle$  è convesso.

Siano  $x = \sum_{i=0}^p \mu_i x_i, y = \sum_{j=0}^q \lambda_j y_j \in \langle M \rangle$  e  $t \in [0, 1]$ . Allora

$$tx + (1 - t)y = \sum_i t \mu_i x_i + \sum_j (1 - t) \lambda_j y_j \in \langle x_0, \dots, x_p, y_0, \dots, y_q \rangle \subset \langle M \rangle$$

in quanto  $\sum_i t \mu_i x_i + \sum_j (1 - t) \lambda_j y_j = t(\sum \mu_i) + (1 - t)(\sum \lambda_j) = t + (1 - t) = 1$ .  $\square$

Denotiamo con  $\Delta_{\mathbb{R}}^n \subset \mathbb{R}^{n+1}$  il simpleso topologico standard di dimensione  $n$ , definito come l'inviluppo convesso della base canonica, o equivalentemente come

$$\Delta_{\mathbb{R}}^n = \left\{ (t_0, \dots, t_n) \in \mathbb{R}^{n+1} \mid t_i \geq 0, \sum t_i = 1 \right\}.$$

PROPOSIZIONE 1.1.7. *Per ogni sottoinsieme finito  $M \subset \mathbb{R}^n$ , il suo inviluppo convesso  $\langle M \rangle$  è un sottoinsieme compatto e convesso di  $\mathbb{R}^n$  e coincide con l'intersezione di tutti i convessi che contengono  $M$ .*

DIMOSTRAZIONE. Abbiamo già visto che  $\langle M \rangle$  è convesso e coincide con l'intersezione dei convessi che contengono  $M$ . Rimane solo da dimostrare la compattezza. Il simpleso topologico standard  $\Delta_{\mathbb{R}}^n$  è chiuso (intersezione dei chiusi  $t_i \geq 0$ ,  $\sum t_i = 1$ ) e limitato (è contenuto nell'ipercubo  $[0, 1]^{n+1}$ ). Quindi  $\Delta_{\mathbb{R}}^n$  è compatto.

Se  $M = \{x_0, \dots, x_p\}$ , per definizione di inviluppo convesso, l'applicazione  $f: \Delta_{\mathbb{R}}^p \rightarrow \langle M \rangle$ ,  $f(t) = \sum t_i x_i$  è continua e surgettiva.  $\square$

DEFINIZIONE 1.1.8. Diremo che  $p+1$  vettori  $v_0, \dots, v_p \in \mathbb{R}^n$  sono **affinemente dipendenti** se esistono  $a_0, \dots, a_p \in \mathbb{K}$ , non tutti nulli, e tali che:

$$a_0 v_0 + \dots + a_p v_p = 0, \quad a_0 + \dots + a_p = 0.$$

I medesimi vettori si dicono **affinemente indipendenti** se non sono affinemente dipendenti.

Ad esempio, ogni vettore (anche nullo) è affinemente indipendente; due vettori sono affinemente indipendenti se e solo se sono distinti.

È chiaro che se  $v_0, \dots, v_p$  sono affinemente dipendenti, allora sono anche linearmente dipendenti. Il viceversa non è vero in generale, ad esempio due vettori distinti di  $\mathbb{R}$  sono sempre linearmente dipendenti ed affinemente indipendenti.

LEMMA 1.1.9. *Dati  $v_0, \dots, v_p \in \mathbb{R}^n$  le seguenti condizioni sono equivalenti:*

- (1) *i  $p+1$  vettori  $v_0, \dots, v_p$  sono affinemente dipendenti;*
- (2) *esiste un indice  $i = 0, \dots, p$  tale che i  $p$  vettori  $v_j - v_i$ ,  $j \neq i$ , sono linearmente dipendenti;*
- (3) *per ogni  $i = 0, \dots, p$  i  $p$  vettori  $v_j - v_i$ ,  $j \neq i$ , sono linearmente dipendenti.*

DIMOSTRAZIONE. È ovvio che (3) implica (2). Mostriamo che (2) implica (1); per semplicità supponiamo  $i = 0$  (per  $i \neq 0$  la dimostrazione è sostanzialmente identica). Siano  $a_1, \dots, a_p \in \mathbb{R}$  non tutti nulli e tali che  $\sum_{j=1}^p a_j (v_j - v_0) = 0$ . Se poniamo  $a_0 = -\sum_{j=1}^p a_j$  si ha

$$\sum_{j=0}^p a_j v_j = \sum_{j=1}^p a_j v_j - \sum_{j=1}^p a_j v_0 = \sum_{j=1}^p a_j (v_j - v_0) = 0.$$

Mostriamo adesso che (1) implica (3). Sia  $i$  un indice fissato e siano  $a_0, \dots, a_p \in \mathbb{K}$  non tutti nulli e tali che  $\sum a_j v_j = 0$  e  $\sum a_j = 0$ . Siccome  $a_i = -\sum_{j \neq i} a_j$  esiste almeno un indice  $j \neq i$  tale che  $a_j \neq 0$  e si ha la relazione di dipendenza lineare

$$\sum_{j \neq i} a_j (v_j - v_i) = \sum_{j \neq i} a_j v_j - \left( \sum_{j \neq i} a_j \right) v_i = \sum_{j=0}^p a_j v_j = 0.$$

$\square$

Notiamo che il massimo numero di vettori affinemente indipendenti in  $\mathbb{R}^n$  è  $n+1$ .

TEOREMA 1.1.10 (Teorema di Carathéodory). *Sia  $M \subset \mathbb{R}^n$ . Allora ogni elemento  $x \in \langle M \rangle$  si può scrivere come combinazione convessa*

$$x = \sum_{i=0}^p t_i x_i, \quad t_i \geq 0, \quad \sum t_i = 1,$$

con i vettori  $x_0, x_1, \dots, x_p \in M$  affinemente indipendenti.

DIMOSTRAZIONE. Per induzione su  $p$  basta dimostrare che se in una combinazione convessa  $x = \sum_{i=0}^p t_i x_i$ , con i vettori  $x_0, \dots, x_p$  affinemente dipendenti, allora a meno di permutazioni degli indici possiamo scrivere  $x$  come combinazione convessa di  $x_1, \dots, x_p$ . Supponiamo quindi che esistano  $a_0, \dots, a_p \in \mathbb{R}$  non tutti nulli tali che

$$\sum_{i=0}^p t_i x_i = x, \quad \sum_{i=0}^p a_i x_i = 0, \quad \sum_{i=0}^p a_i = 0.$$

Dunque, per ogni  $\lambda \in \mathbb{R}$  si ha

$$\sum_{i=0}^p (t_i - \lambda a_i) x_i = x, \quad \sum_{i=0}^p (t_i - \lambda a_i) = 1.$$

Siccome gli  $a_i$  non sono tutti nulli esiste almeno un indice  $j$  tale che  $a_j > 0$ . A meno di permutare gli indici possiamo supporre che esista  $0 \leq r < p$  tale che:

- (1)  $a_i > 0$  per  $i \leq r$  e  $a_i \leq 0$  per  $i > r$ ;
- (2)  $0 \leq \frac{t_0}{a_0} \leq \frac{t_1}{a_1} \leq \dots \leq \frac{t_r}{a_r}$ .

Se prendiamo  $\lambda = \frac{t_0}{a_0}$  allora

$$t_0 - \lambda a_0 = 0, \quad t_i - \lambda a_i \geq 0 \quad \forall i > 0,$$

e quindi  $\sum_{i=1}^p (t_i - \lambda a_i)x_i = x$  rappresenta  $x$  come combinazione convessa di  $x_1, \dots, x_p$ .  $\square$

**TEOREMA 1.1.11.** *Per una successione di vettori  $x_0, \dots, x_p \in \mathbb{R}^n$  le seguenti condizioni sono equivalenti:*

- (1) *i vettori  $x_0, \dots, x_p$  sono affinementemente indipendenti;*
- (2) *i vettori  $x_0, \dots, x_p$  sono distinti e per ogni coppia di sottoinsiemi disgiunti  $s, t \subset \{x_0, \dots, x_p\}$  vale  $\langle s \rangle \cap \langle t \rangle = \emptyset$ .*

Se le precedenti condizioni sono soddisfatte, allora l'applicazione

$$f: \Delta_{\mathbb{R}}^p \rightarrow \langle x_0, \dots, x_p \rangle, \quad f(t_0, \dots, t_p) = \sum_{i=0}^p t_i x_i,$$

è un omeomorfismo.

**DIMOSTRAZIONE.** Se esistono due sottoinsiemi disgiunti  $s, t \subset \{x_0, \dots, x_p\}$  tali che  $\langle s \rangle \cap \langle t \rangle \neq \emptyset$  allora esiste un'uguaglianza di combinazioni convesse

$$\sum_{x_i \in s} \lambda_i x_i = \sum_{x_j \in t} \mu_j x_j, \quad \sum \lambda_i = \sum \mu_j = 1.$$

Facendo le differenze troviamo

$$\sum_{x_i \in s} \lambda_i x_i - \sum_{x_j \in t} \mu_j x_j = 0, \quad \sum \lambda_i - \sum \mu_j = 0$$

che è una relazione di dipendenza affine.

Viceversa, supponiamo che i vettori  $x_i$  siano distinti ma affinementemente dipendenti, ossia che  $x_i \neq x_j$  per ogni  $i \neq j$  e che esiste una relazione lineare

$$\sum_{i=0}^p a_i x_i = 0, \quad \sum_{i=0}^p a_i = 0, \quad a_i \in \mathbb{R} \text{ non tutti nulli.}$$

A meno di permutazione degli indici possiamo supporre che esista  $0 \leq r \leq p$  tale che:

- (1)  $a_i > 0$  se  $0 \leq i \leq r$ ,
- (2)  $a_i \leq 0$  se  $r+1 \leq i \leq p$ .

Inoltre, a meno di dividere tutti gli scalari  $a_i$  per  $\sum_{i=1}^r a_i$  possiamo supporre  $\sum_{i=1}^r a_i = 1$  e di conseguenza  $\sum_{i=r+1}^p a_i = -1$ .

Ma allora il punto

$$y = \sum_{i=0}^r a_i x_i = \sum_{i=r+1}^p (-a_i) x_i$$

appartiene all'intersezione degli involuppi convessi  $\langle x_0, \dots, x_r \rangle \cap \langle x_{r+1}, \dots, x_p \rangle$ .

Se le due condizioni equivalenti sono soddisfatte, allora l'applicazione  $f$  è surgettiva per definizione di involuppo convesso. Possiamo scrivere

$$f(t_0, \dots, t_p) = \sum_{i=0}^p t_i x_i = x_0 + \sum_{i=1}^p t_i (x_i - x_0),$$

e dato che i vettori  $x_i - x_0$  sono linearmente indipendenti ne segue che  $f$  è anche iniettiva. Dal punto di vista topologico, l'applicazione  $f$  è continua e bigettiva da un compatto in un Hausdorff e quindi un omeomorfismo.  $\square$

**COROLLARIO 1.1.12** (Teorema di Radon). *Sia  $M \subset \mathbb{R}^n$  un sottoinsieme contenente almeno  $n + 2$  vettori distinti. Esiste allora una scomposizione in unione disgiunta  $M = M_1 \cup M_2$ ,  $M_1 \cap M_2 = \emptyset$ , tale che  $\langle M_1 \rangle \cap \langle M_2 \rangle \neq \emptyset$ .*

**DIMOSTRAZIONE.** Scegliamo  $n + 2$  elementi distinti  $x_0, \dots, x_{n+1} \in M$ , che quindi sono affinementemente dioendenti. Per il Teorema 1.1.11 esistono due sottoinsiemi disgiunti  $s, t \subset \{x_0, \dots, x_{n+1}\}$  tali che  $\langle s \rangle \cap \langle t \rangle \neq \emptyset$ . Basta allora considerare  $M_1 = s$  e  $M_2 = M - s$ .  $\square$

**COROLLARIO 1.1.13** (Teorema di Helly). *Sia  $\mathcal{U}$  una famiglia di sottoinsiemi convessi di  $\mathbb{R}^n$ . Si assuma che per ogni  $X_0, \dots, X_d \in \mathcal{U}$  con  $d \leq n$  si abbia  $X_0 \cap X_1 \cap \dots \cap X_d \neq \emptyset$ . Allora ogni intersezione finita di elementi di  $\mathcal{U}$  è non vuota.*

**DIMOSTRAZIONE.** Supponiamo per assurdo che esistano sottofamiglie finite con intersezione vuota. Sia  $X_0, \dots, X_m \in \mathcal{U}$  una di queste con  $m$  minimo, ossia:

- (1)  $X_0 \cap X_1 \cap \dots \cap X_m = \emptyset$ ;
- (2)  $X_0 \cap \dots \cap \widehat{X_i} \cap \dots \cap X_m \neq \emptyset$  per ogni  $i = 0, \dots, m$ .

Abbiamo usato la notazione sottrattiva standard, nella quale la parte sottostante al segno del “cappello”  $\widehat{\phantom{x}}$  viene omessa.

Per ipotesi  $m > n$ ; scegliendo per ogni  $i = 0, \dots, m$  un elemento

$$x_i \in X_0 \cap \dots \cap \widehat{X_i} \cap \dots \cap X_m,$$

per il Corollario 1.1.12, a meno di permutazioni degli indici esiste  $k$  tale che

$$\langle x_0, \dots, x_k \rangle \cap \langle x_{k+1}, \dots, x_m \rangle \neq \emptyset.$$

Poiché ciascun  $X_i$  è convesso, si ha

$$\langle x_0, \dots, x_k \rangle \subset X_{k+1} \cap \dots \cap X_m, \quad \langle x_{k+1}, \dots, x_m \rangle \subset X_1 \cap \dots \cap X_k,$$

in contraddizione con il fatto che  $X_0 \cap X_1 \cap \dots \cap X_m = \emptyset$ .  $\square$

Si noti che, senza ulteriori ipotesi, il teorema di Helly non vale per la intersezioni infinite: si consideri ad esempio la famiglia delle semirette limitate dal basso di  $\mathbb{R}$ .

### Esercizi.

**ESERCIZIO 1.** Provare che per ogni  $p_1, \dots, p_m \in \mathbb{R}^n$  ed ogni  $r \geq 0$  l'insieme

$$\{x \in \mathbb{R}^n \mid \sum_i \|x - p_i\| \leq r\}$$

è convesso.

**ESERCIZIO 2.** Siano  $C, D$  sottoinsiemi convessi di  $\mathbb{R}^n$ . Dimostrare che il sottoinsieme

$$C + D = \{x + y \in \mathbb{R}^n \mid x \in C, y \in D\}$$

è ancora convesso.

**ESERCIZIO 3.** Dedurre dal Teorema di Carathéodory che l'involuppo convesso di un sottoinsieme compatto di  $\mathbb{R}^n$  è ancora compatto.

## 1.2. Complessi simpliciali astratti

Iniziamo con il fissare alcune notazioni: se  $I$  è un insieme scriveremo  $\Delta^I$  per indicare la famiglia di tutti i sottoinsiemi **finiti e non vuoti** di  $I$ . Nel caso in cui  $I = \{0, 1, \dots, n\}$  scriveremo più semplicemente  $\Delta^n$  in luogo di  $\Delta^{\{0,1,\dots,n\}}$ . È chiaro che  $\Delta^\emptyset = \emptyset$ .

Per ogni insieme finito  $X$  denotiamo con  $|X|$  la sua cardinalità.

**DEFINIZIONE 1.2.1.** Un **complesso simpliciale astratto** è una coppia  $(K, I)$ , dove  $I$  è un insieme, i cui elementi sono detti **vertici**, e  $K$  è un sottoinsieme di  $\Delta^I$  per cui valgono le seguenti condizioni:

- (1)  $\{x\} \in K$  per ogni  $x \in I$ ;
- (2) se  $s \in K$ ,  $t \in \Delta^I$  e  $t \subseteq s$ , allora  $t \in K$ .

Giova osservare che la precedente condizione (2) equivale a dire che se  $s \in K$ , allora  $\Delta^s \subseteq K$ .

Se  $(K, I)$  è un complesso simpliciale astratto, chiameremo **simplessi** gli elementi di  $K$ .

La **dimensione** di un simplesso  $s \in K$  è definita come il numero di elementi di  $s$  diminuito di 1:  $\dim s = |s| - 1$ . Ogni vertice ha dimensione 0. Chiameremo anche  $p$ -simplesso un simplesso di dimensione  $p$ .

Se  $s \in K$  e  $t \subset s$  diremo che  $t$  è una **faccia** di  $s$ , se  $t \subset s$  e  $t \neq s$  diremo che  $t$  è una **faccia propria** di  $s$ . Un simplesso  $s \in K$  si dice **massimale** se non è faccia propria di alcun simplesso in  $K$ .

Segue dalla definizione che esiste una bigezione tautologica tra l'insieme dei vertici di un complesso simpliciale astratto  $(K, I)$  e l'insieme degli 0-simplessi. Dunque  $K$  determina univocamente  $I$  e nel seguito useremo la notazione semplificata  $K = (K, I)$  quando non è necessario esplicitare l'insieme dei vertici.

Nella Definizione 1.2.1 l'aggettivo “astratto” serve per differenziare il concetto dai complessi simpliciali topologici [18]. Per semplicità diremo semplicemente “complesso simpliciale” quando la natura astratta o topologica è chiara dal contesto.

Ogni applicazione di insiemi  $f: I \rightarrow J$  induce in modo naturale un'applicazione

$$f: \Delta^I \rightarrow \Delta^J, \quad f(s) = \text{immagine del sottoinsieme } s \subseteq I \text{ tramite } f.$$

DEFINIZIONE 1.2.2. Un **morfismo**  $f: (K, I) \rightarrow (H, J)$  di complessi simpliciali astratti è un'applicazione  $f: I \rightarrow J$  tale che  $f(s) \in H$  per ogni  $s \in K$ . Denoteremo  $\text{Hom}(K, H)$  la collezione di tutti i morfismi di complessi simpliciali da  $K$  in  $H$ .

Ad esempio:

- (1) se  $v$  è un vertice del simpliciale astratto di  $K$ , allora l'inclusione  $\{v\} \hookrightarrow K$  è un morfismo di complessi simpliciali. Più in generale, se  $\sigma \in K$  allora l'inclusione  $\Delta^\sigma \rightarrow K$  è un morfismo.
- (2) se  $v \in I$  è un qualunque vertice, allora l'applicazione costante  $K \rightarrow \{v\}$  è un morfismo di complessi simpliciali.

DEFINIZIONE 1.2.3. Un **isomorfismo** tra due complessi simpliciali astratti  $(K, I)$  e  $(H, J)$  è un'applicazione bigettiva  $f: I \xrightarrow{\cong} J$  con la proprietà che  $s \in K$  se e solo se  $f(s) \in H$ .

I morfismi di complessi simpliciali astratti si possono comporre nel modo ovvio; composizione di isomorfismi è ancora un isomorfismo. Se  $f: (K, I) \rightarrow (H, J)$  è un isomorfismo, allora  $f^{-1}: (H, J) \rightarrow (K, I)$  è ancora un isomorfismo.

È opportuno precisare che in queste note siamo *interessati esclusivamente alle proprietà dei complessi simpliciali astratti a meno di isomorfismo*, ossia siamo interessati solamente alle relazioni che intercorrono tra i simplessi e non alla loro natura reale.

Se  $(K, I)$  è un complesso simpliciale astratto e  $f: I \xrightarrow{\cong} J$  è un'applicazione bigettiva, allora ponendo  $H = \{f(s) \in \Delta^J \mid s \in K\}$  si ha che  $(H, J)$  è un complesso simpliciale astratto isomorfo a  $(K, I)$ , con l'isomorfismo dato da  $f$ .

ESEMPIO 1.2.4. Per ogni insieme  $I$ , la coppia  $(\Delta^I, I)$  è un complesso simpliciale astratto che viene detto **completo**.

DEFINIZIONE 1.2.5. Dato un complesso simpliciale astratto  $K$ , chiamiamo  **$p$ -scheletro** di  $K$ , denotato con  $K^{(p)}$ , la sottofamiglia di tutti i simplessi di  $K$  di dimensione minore o uguale a  $p$ , ossia la famiglia dei simplessi di  $K$  con al più  $p + 1$  elementi.

Un complesso simpliciale astratto  $(K, I)$  si dice **finito** se  $I$  è un insieme finito ( $\iff K$  è finito). La **dimensione**  $\dim K$  di un complesso simpliciale astratto  $K$  è l'estremo superiore delle dimensioni dei suoi simplessi. In particolare:  $K = K^{(p)}$  se e solo se  $\dim K \leq p$ ,  $\Delta^I$  ha dimensione  $|I| - 1$  e, coerentemente, definiamo uguale a  $-1$  la dimensione del complesso simpliciale vuoto  $\emptyset = \Delta^\emptyset$ .

Ogni complesso simpliciale astratto finito ha dimensione finita, mentre il viceversa è generalmente falso.

Prima di sviluppare la teoria dei complessi simpliciali astratti, illustriamo alcuni esempi significativi.

ESEMPIO 1.2.6. Se  $K$  è un complesso simpliciale astratto, allora lo è anche  $K^{(p)}$  per ogni  $p \geq 0$  (con gli stessi vertici di  $K$ ).

ESEMPIO 1.2.7. Dati due complessi simpliciali astratti  $(K, I)$  e  $(H, J)$ , la loro unione  $(K \cup H, I \cup J)$  e la loro intersezione  $(K \cap H, I \cap J)$  sono ancora complessi simpliciali astratti.

ESEMPIO 1.2.8. Per ogni complesso simpliciale astratto  $K$  si ha  $K = \bigcup_{s \in K} \Delta^s$ . Se  $K$  ha dimensione finita ogni simpleso è contenuto in un simpleso massimale e quindi

$$K = \bigcup_{s \in K, s \text{ massimale}} \Delta^s.$$

ESEMPIO 1.2.9. Dati due complessi simpliciali astratti  $(K, I)$  e  $(H, J)$  la loro **giunzione** è il complesso simpliciale astratto  $(K * H, I \cup J)$ , dove

$$K * H = K \cup H \cup \{s \cup t \mid s \in K, t \in H\}.$$

DEFINIZIONE 1.2.10. Dato un complesso simpliciale astratto  $K$  e un sottoinsieme  $L \subseteq K$ , diremo che  $L$  è un **sottocomplesso** di  $K$  se  $L$  è a sua volta un complesso simpliciale astratto (i cui vertici sono contenuti nei vertici di  $K$ ).

Ad esempio, gli scheletri sono sottocomplessi. Ogni complesso simpliciale astratto  $(K, I)$  è un sottocomplesso di  $\Delta^I$  e per ogni  $s \in K$  si ha che  $\Delta^s$  è un sottocomplesso di  $K$ .

DEFINIZIONE 1.2.11. Un complesso simpliciale astratto si dice **connesso** se non è unione di due sottocomplessi simpliciali non vuoti e disgiunti.

È utile collegare la il concetto di connessione con una relazione di equivalenza sui vertici detta contiguità. Diremo che due vertici  $u, v$  in un complesso simpliciale astratto  $K$  sono direttamente contigui se esiste  $\sigma \in K$  che contiene  $u$  e  $v$ ; equivalentemente  $u$  e  $v$  sono direttamente contigui se  $\{u, v\} \in K$ . La relazione di contiguità diretta è riflessiva e simmetrica, ma non è transitiva in generale. Chiameremo **contiguità** la relazione di equivalenza generata dalla contiguità diretta. In altri termini, due vertici  $u$  e  $v$  sono contigui se esiste una successione finita di vertici  $w_1, \dots, w_n$  tali che

$$\{u, w_1\}, \{w_1, w_2\}, \dots, \{w_n, v\} \in K.$$

LEMMA 1.2.12. *Un complesso simpliciale astratto  $K$  è connesso se e solo se tutti i vertici sono contigui tra loro. In particolare,  $K$  è connesso se e solo se il suo 1-scheletro  $K^{(1)}$  è connesso.*

DIMOSTRAZIONE. Se  $K = \emptyset$  non c'è nulla da dimostrare. Se  $K$  è sconnesso e  $K = L \cup P$  con  $L, P$  complessi simpliciali astratti non vuoti e disgiunti, allora  $\{l, p\} \notin K$  per ogni  $l \in L^{(0)}, p \in P^{(0)}$ : infatti, se per assurdo fosse  $\{l, p\} \in K$  e, tanto per fissare le idee  $\{l, p\} \in L$ , allora  $p \in L$  che è assurdo. Ne consegue che nessun vertice di  $L$  è contiguo ad un vertice di  $P$ .

Viceversa, sia  $(K, I)$  connesso e non vuoto, fissiamo un vertice  $v \in I$  e scriviamo  $I = J \cup (I - J)$  dove  $J$  è l'insieme dei vertici contigui  $v$ ; vogliamo dimostrare che  $J = I$ . Se fosse  $J \neq I$ , siccome  $v \in J \neq \emptyset$ , si avrebbe

$$L := \Delta^J \cap K \neq \emptyset, \quad P := \Delta^{I-J} \cap K \neq \emptyset, \quad L \cap P = \emptyset.$$

Per ipotesi  $K$  è connesso e quindi  $K \neq L \cup P$ . Preso un simpleso  $\{x_0, \dots, x_p\} \in K - (L \cup P)$  possiamo trovare due indici distinti  $j, h$  tali che  $x_j \in J, x_h \in I - J$ . Dato che  $x_j, x_h$  appartengono entrambi a  $\{x_0, \dots, x_p\} \in K$  e  $x_j$  è contiguo a  $v$ , per la proprietà transitiva anche  $x_h$  è contiguo a  $v$ , in contraddizione con l'appartenenza  $x_h \in I - J$ .  $\square$

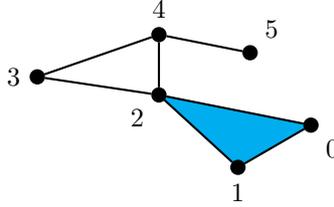
ESEMPIO 1.2.13. Sia  $(K, I)$  un complesso simpliciale astratto finito con  $I \subset \mathbb{R}^n$ . Nelle notazioni della sezione precedente, per ogni sottoinsieme finito  $s \subset \mathbb{R}^n$  indichiamo con  $\langle s \rangle \subset \mathbb{R}^n$  l'involuppo convesso di  $s$ :

$$\langle \emptyset \rangle = \emptyset, \quad \langle \{x_0, \dots, x_p\} \rangle = \left\{ \sum t_i x_i \in \mathbb{R}^n \mid t_i \geq 0, \sum t_i = 1 \right\}, \quad p \geq 0.$$

Se accade che per ogni  $s, t \in K$  si ha  $\langle s \rangle \cap \langle t \rangle = \langle s \cap t \rangle$ , allora possiamo rappresentare  $K$  mediante la sua **realizzazione geometrica**

$$|K| := \bigcup_{s \in K} \langle s \rangle = \bigcup_{s \in K, s \text{ massimale}} \langle s \rangle \subset \mathbb{R}^n.$$

Ad esempio la figura



rappresenta il complesso simpliciale astratto

$$K = \{\{0, 1, 2\}, \{0, 1\}, \{1, 2\}, \{0, 2\}, \{2, 3\}, \{3, 4\}, \{2, 4\}, \{4, 5\}, \{0\}, \{1\}, \{2\}, \{3\}, \{4\}, \{5\}\},$$

i cui scheletri sono:

$$K^{(0)} = \{\{0\}, \{1\}, \{2\}, \{3\}, \{4\}, \{5\}\},$$

$$K^{(1)} = \{\{0, 1\}, \{1, 2\}, \{0, 2\}, \{2, 3\}, \{3, 4\}, \{2, 4\}, \{4, 5\}, \{0\}, \{1\}, \{2\}, \{3\}, \{4\}, \{5\}\},$$

$$K^{(p)} = K \quad \text{per ogni } p \geq 2.$$

Tratteremo in maggiori dettagli le realizzazioni geometriche nella Sezione 1.3.

**ESEMPIO 1.2.14 (Il nervo).** Sia  $\mathcal{U} = \{U_i\}$ ,  $i \in I$ , una famiglia di sottoinsiemi non vuoti di un insieme fissato. Possiamo definire un complesso simpliciale astratto  $(N(\mathcal{U}), I)$  ponendo

$$N(\mathcal{U}) = \{\{i_0, \dots, i_p\} \in \Delta^I \mid U_{i_0} \cap \dots \cap U_{i_p} \neq \emptyset\}.$$

È chiaro che la coppia  $(N(\mathcal{U}), I)$  è un complesso simpliciale astratto. È utile osservare che se  $U_i = U_j$  per ogni  $i, j$  allora il nervo coincide con il complesso simpliciale completo  $\Delta^I$ .

**ESEMPIO 1.2.15 (Complesso  $\text{Hom}^\Delta$ ).** Dati due complessi simpliciali  $K, H$ , il complesso simpliciale  $\text{Hom}^\Delta(K, H)$  dei morfismi da  $K$  in  $H$  ha come vertici l'insieme  $\text{Hom}(K, H)$  di tutti i morfismi da  $K$  in  $H$ ; dati  $n$  morfismi  $f_1, \dots, f_n: K \rightarrow H$  si ha  $\{f_1, \dots, f_n\} \in \text{Hom}^\Delta(K, H)$  se e solo se per ogni  $s \in K$  vale  $f_1(s) \cup \dots \cup f_n(s) \in H$ . Dunque, per come è definito  $\text{Hom}^\Delta$ , l'applicazione

$$K \times \text{Hom}^\Delta(K, H) \rightarrow H, \quad (\sigma, \{f_1, \dots, f_n\}) \mapsto f_1(\sigma) \cup \dots \cup f_n(\sigma),$$

risulta ben definita.

**ESEMPIO 1.2.16 (Catene in un poset).** Ricordiamo che un **poset** (abbreviazione di *partially ordered set*) non è altro che un insieme (parzialmente) ordinato: più precisamente un poset è una coppia  $(I, \leq)$ , con  $I$  insieme e  $\leq$  una relazione che soddisfa le condizioni:

- (riflessiva)  $x \leq x$  per ogni  $x \in I$ ;
- (antisimmetrica) se  $x \leq y$  e  $y \leq x$  allora  $x = y$ ;
- (transitiva) se  $x \leq y$  e  $y \leq z$  allora  $x \leq z$ .

Si scrive  $x < y$  con lo stesso significato di  $x \leq y$  e  $x \neq y$ . Un sottoinsieme  $C \subset I$  si dice una **catena** del poset se  $C$  risulta totalmente ordinato con la relazione di ordine indotta, ossia se per ogni  $x, y \in C$  si ha  $x \leq y$  oppure  $y \leq x$ .

Sia dunque  $(I, \leq)$  un poset. Il complesso simpliciale astratto delle catene finite di  $I$  è  $(b(I), I)$ , dove:

$$b(I) = \{C \subset I \text{ catena finita}\} \subset \Delta^I.$$

Infatti ogni sottoinsieme di un solo elemento è una catena ed ogni sottoinsieme di una catena è ancora una catena. Osserviamo che si può anche scrivere

$$b(I) = \{\{x_0, \dots, x_p\} \in \Delta^I \mid x_0 < x_1 < \dots < x_p\}.$$

ESEMPIO 1.2.17 (Suddivisione baricentrica). Dato un qualunque complesso simpliciale astratto  $(K, I)$ , l'insieme  $K$  è ordinato per inclusione e possiamo definire la sua **suddivisione baricentrica**  $(b(K), K)$  come il complesso delle catene di  $K$ :

$$b(K) = \{\{x_0, \dots, x_p\} \in \Delta^K \mid x_0 \subset x_1 \subset \dots \subset x_p\}.$$

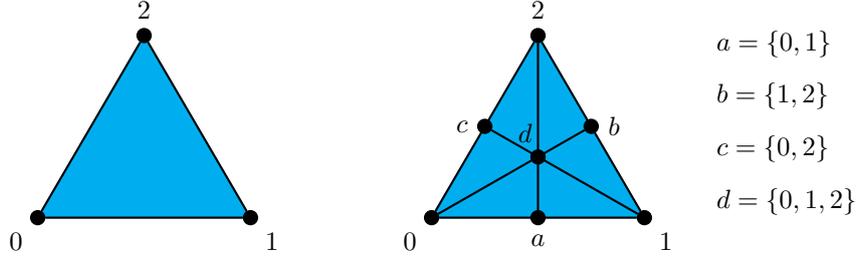


FIGURA 1. Il complesso simpliciale astratto  $\Delta^2$  e la sua suddivisione baricentrica  $b(\Delta^2)$ .

ESEMPIO 1.2.18 (Complesso duale). Per definizione, il **duale** di complesso simpliciale astratto è il nervo dei semplici massimali. Più precisamente, se  $K$  è un complesso simpliciale astratto, un semplice  $s \in K$  si dice **massimale** se non è contenuto propriamente in alcun semplice di  $K$ . Sia  $J \subset K$  la sottofamiglia dei semplici massimali, allora il duale di  $K$  è dato da

$$K^\vee = \{\{s_0, \dots, s_p\} \in \Delta^J \mid s_0 \cap \dots \cap s_p \neq \emptyset\}.$$

In generale, la produzione del duale non è un'operazione reversibile: ad esempio i complessi simpliciali  $\Delta^n$  hanno tutti un unico semplice massimale e quindi hanno tutti lo stesso duale.

ESEMPIO 1.2.19 (Complesso di **Delaunay**). Dato un qualsiasi sottoinsieme  $I \subset \mathbb{R}^n$ , per ogni  $s \in I$  definiamo la sua **regione di Voronoi**<sup>1</sup>  $V_s \subseteq \mathbb{R}^n$  come:

$$V_s = \{x \in \mathbb{R}^n \mid \|x - s\| \leq \|x - t\|, \quad \forall t \in I\}.$$

Per quanto osservato nell'Esempio 1.1.3 si ha che  $V_s$  è intersezione di semispazi chiusi. In particolare  $V_s$  è un chiuso convesso.

È chiaro che  $V_s \neq \emptyset$  per ogni  $s \in I$  e ha quindi perfettamente senso considerare il suo nervo  $D_I := (N(\{V_s\}), I)$ , che viene detto **complesso di Delaunay** del sottoinsieme  $I \subset \mathbb{R}^n$ .

Equivalentemente un semplice  $\{s_0, \dots, s_p\} \in \Delta^I$  appartiene al complesso di Delaunay  $D_I$  se e solo se esiste  $x \in \mathbb{R}^n$  tale che

$$\|x - s_0\| = \|x - s_1\| = \dots = \|x - s_p\| \leq \|x - t\| \quad \text{per ogni } t \in I.$$

In particolare, per ogni  $\{s_0, \dots, s_p\} \in D_I$  i  $p + 1$  punti  $s_0, \dots, s_p$  sono contenuti in una sfera di dimensione  $n - 1$  che non contiene al suo interno alcun punto di  $I$ . Dunque per un sottoinsieme finito  $I$  di  $\mathbb{R}^n$  ed in *posizione generica* il complesso di Delaunay  $D_I$  ha al più dimensione  $n$ .

ESEMPIO 1.2.20 (Witness complex<sup>2</sup>). Siano  $L \subset P \subset \mathbb{R}^n$  due sottoinsiemi finiti e si consideri famiglia  $D \subset \Delta^L$  di sottoinsiemi di  $L$  definita come

$$D = \{S \subset L \mid \exists p \in P \text{ tale che } \|p - x\| \leq \|p - y\| \forall x \in S, y \in L - S\}.$$

<sup>1</sup>Voronoi era un matematico ucraino, mentre Delaunay russo ma di antenati francesi. Il primo si pronuncia più o meno come si scrive, mentre il secondo "deloné".

<sup>2</sup>Ignoro se esiste una traduzione italiana riconosciuta. Inoltre anche in lingua inglese non tutte le definizioni in letteratura coincidono.

È facile vedere che  $\{l\} \in D$  per ogni  $l \in L$  e che in generale  $D$  non è un complesso simpliciale; si definiscono quindi il **witness complex** della coppia  $L, P$  come

$$W_\infty(L, P) = \{s \in D \mid t \in D \quad \forall \emptyset \neq t \subset s\}$$

ed il **weak witness complex** come

$$W_1(L, P) = \{s \in \Delta^L \mid t \in D \quad \forall t \subset s, |t| = 2\}.$$

Si lascia per esercizio verificare che i due witness complex sono complessi simpliciali astratti che hanno  $L$  come insieme di vertici. Più in generale, anche se poco considerato in pratica, per ogni intero positivo  $k$  ha senso considerare il complesso simpliciale

$$W_k(L, P) = \{s \in \Delta^L \mid t \in D \quad \forall t \subset s, 0 < |t| \leq k + 1\}.$$

### Esercizi:

ESERCIZIO 4. Siano  $(K, I), (H, J)$  due complessi simpliciali astratti. Provare un'applicazione  $g: K \rightarrow H$  è indotta da un isomorfismo se e solo se è bigettiva e per ogni  $t, s \in K$  vale  $s \subset t$  se e solo se  $g(s) \subset g(t)$ .

ESERCIZIO 5. Denotiamo con  $b(K)$  la suddivisione baricentrica del complesso simpliciale astratto  $K$ . Provare che:

- (1)  $b(\Delta^0) = \Delta^0$ ;
- (2)  $b(\Delta^n)$  è di tipo cono per ogni  $n \geq 0$ ;
- (3) se  $L$  è un sottocomplesso di  $K$ , allora  $b(L)$  è un sottocomplesso di  $b(K)$ ;
- (4) se  $L, M$  sono sottocomplessi di  $K$ , allora  $b(L \cap M) = b(L) \cap b(M)$  e  $b(L \cup M) = b(L) \cup b(M)$ .

ESERCIZIO 6. Sia  $I \subset \mathbb{R}^n$  un chiuso non vuoto. Provare che le regioni di Voronoi  $V_s$ ,  $s \in I$ , ricoprono  $\mathbb{R}^n$ , ossia  $\mathbb{R}^n = \cup_{s \in I} V_s$ .

### 1.3. Realizzazioni geometriche

In questa sezione studieremo esistenza ed unicità topologica delle realizzazioni geometriche dei complessi simpliciali astratti finiti. Per maggiori dettagli e per il caso dei complessi simpliciali infiniti rimandiamo a [19, Sezione 3.1].

PROPOSIZIONE 1.3.1. Sia  $(K, I)$  un complesso simpliciale astratto con  $I \subset \mathbb{R}^n$  e tale che  $\langle s \rangle \cap \langle t \rangle = \emptyset$  per ogni  $s, t \in K$  tali che  $s \cap t = \emptyset$ . Allora  $\langle s \rangle \cap \langle t \rangle = \langle s \cap t \rangle$  per ogni  $s, t \in K$ .

DIMOSTRAZIONE. L'inclusione  $\langle s \rangle \cap \langle t \rangle \supset \langle s \cap t \rangle$  è vera per ovvi motivi. Dimostriamo per induzione su  $n = \dim(s \cap t)$  che vale l'inclusione opposta

$$(1.1) \quad \langle s \rangle \cap \langle t \rangle \subset \langle s \cap t \rangle.$$

Per  $n = -1$ , ossia se  $s \cap t = \emptyset$ , la (1.1) è vera per ipotesi. Supponiamo quindi  $n \geq 0$ ,  $s = \{s_0, \dots, s_p\}$  e  $t = \{t_0, \dots, t_q\}$  con  $s_i \neq s_j$  e  $t_i \neq t_j$  per ogni  $i \neq j$ ; a meno di permutazioni possiamo inoltre supporre  $s_0 = t_0$ .

Sia dunque  $y \in \langle s \rangle \cap \langle t \rangle$ . Si ha

$$y = \sum_{i=0}^p a_i s_i = \sum_{j=0}^q b_j t_j, \quad 0 \leq a_i, b_j \leq 1, \quad \sum a_i = \sum b_j = 1.$$

Supponiamo per fissare le idee che  $a_0 \leq b_0$  (altrimenti sarà sufficiente scambiare  $s$  con  $t$ ). Se  $a_0 = 1$  allora  $y = s_0 \in \langle s \cap t \rangle$ . Se invece  $a_0 < 1$ , ponendo  $r = \{s_1, \dots, s_p\}$  si ha

$$z := \frac{1}{1 - a_0} (y - a_0 s_0) = \sum_{i=1}^p \frac{a_i}{1 - a_0} s_i \in \langle r \rangle.$$

D'altra parte, siccome  $t_0 = s_0$

$$z = \frac{b_0 - a_0}{1 - a_0} t_0 + \sum_{j=1}^q \frac{b_j}{1 - a_0} t_j \in \langle t \rangle.$$

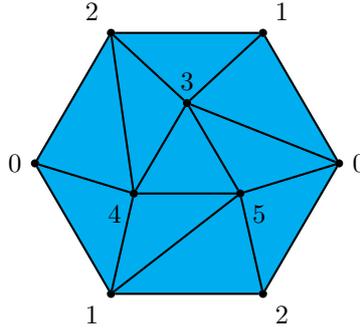


FIGURA 2. Una triangolazione del piano proiettivo reale.

Per l'ipotesi induttiva  $z \in \langle r \cap t \rangle$  e quindi  $y = a_0 s_0 + (1 - a_0)z \in \langle s \cap t \rangle$ .  $\square$

DEFINIZIONE 1.3.2. Siano  $K = (K, I)$  un complesso simpliciale astratto finito e  $f: I \rightarrow \mathbb{R}^n$  un'applicazione tale che  $\langle f(s) \rangle \cap \langle f(t) \rangle = \emptyset$  per ogni coppia di semplici *disgiunti*  $s, t \in K$ . Definiamo la **realizzazione geometrica** di  $K$  tramite  $f$  come

$$|f(K)| = \bigcup_{s \in K} \langle f(s) \rangle \subset \mathbb{R}^n,$$

dotato della topologia di sottospazio. Se  $f$  è il morfismo di inclusione di un sottoinsieme  $I \subset \mathbb{R}^n$  scriveremo semplicemente  $|K|$  in luogo di  $|f(K)|$  (vedi Esempio 1.2.13).

**Nota:** per coerenza con [19] abbiamo usato la notazione  $|K|$  per denotare la realizzazione geometrica, da non confondere con la cardinalità di  $K$ .

Osserviamo che ogni  $f: I \rightarrow \mathbb{R}^n$  come nella Definizione 1.3.2 è necessariamente iniettiva: se  $u, v \in I$  sono due vertici distinti, allora  $\{u\} \cap \{v\} = \emptyset$  e quindi  $f(u) \neq f(v)$ . Ne segue che  $(K, I)$  è isomorfo come complesso simpliciale astratto a  $(f(K), f(I))$ , dove  $f(K) = \{f(s) \mid s \in K\}$ .

Inoltre, segue dal Teorema 1.1.11 che per ogni semplice  $\{x_0, \dots, x_p\} \in K$  i vettori  $f(x_0), \dots, f(x_p)$  sono affinementemente indipendenti, quindi  $n \geq p$  da cui segue  $n \geq \dim K$ , mentre per la Proposizione 1.3.1  $\langle f(s) \rangle \cap \langle f(t) \rangle = \langle f(s) \cap f(t) \rangle$  per ogni  $s, t \in K$ .

TEOREMA 1.3.3. *Ogni complesso simpliciale astratto finito possiede realizzazioni geometriche, tra loro tutte topologicamente equivalenti.*

DIMOSTRAZIONE. Sia  $(K, I)$  un complesso simpliciale astratto finito e sia  $V$  lo spazio vettoriale reale generato da  $I$ : ogni elemento di  $V$  è una combinazione lineare del tipo  $\sum a_i x_i$ , con  $a_i \in \mathbb{R}$  e  $x_i \in I$ . Dato che gli elementi di  $I$  sono una base di  $V$  per ogni  $s, t \in K$  tali che  $s \cap t = \emptyset$  si ha  $\langle s \rangle \cap \langle t \rangle = \emptyset$  e questo ci consente di definire la realizzazione geometrica canonica

$$|K|_{\text{can}} = \bigcup_{s \in K} \langle s \rangle \subset V.$$

Sia adesso  $|f(K)|$  una realizzazione geometrica indotta da  $f: I \rightarrow \mathbb{R}^n$ . Siccome  $I$  è una base di  $V$ , l'applicazione  $f$  si estende in modo unico ad un'applicazione lineare

$$V \rightarrow \mathbb{R}^n, \quad \sum a_i x_i \mapsto \sum a_i f(x_i),$$

che per costruzione si restringe ad un'applicazione continua e surgettiva  $F: |K|_{\text{can}} \rightarrow |f(K)|$ . Siccome  $|K|_{\text{can}}$  è compatto (unione finita di compatti) e  $|f(K)|$  è compatto, basta dimostrare che  $F$  è anche iniettiva. Ma questo segue facilmente dal Teorema 1.1.11 e dalla Proposizione 1.3.1: i dettagli sono lasciati per esercizio.  $\square$

Non è difficile dimostrare che ogni complesso simpliciale astratto finito di dimensione  $k$  possiede una realizzazione geometrica in  $\mathbb{R}^{2k+1}$ . Per **triangolazione** di uno spazio topologico  $X$  si intende una coppia  $(K, f)$  con  $K$  complesso simpliciale astratto e  $f: |K| \rightarrow X$  un omeomorfismo.

Data una realizzazione geometrica di un complesso simpliciale astratto  $(K, I)$  indotta da una inclusione  $I \subset \mathbb{R}^n$  possiamo associare in maniera canonica una realizzazione geometrica della suddivisione baricentrica  $(b(K), K)$  indotta dall'inclusione

$$f: K \rightarrow \mathbb{R}^n, \quad f(\{x_0, \dots, x_p\}) = \frac{1}{p+1} \sum_{i=0}^p x_i.$$

Per future applicazioni è utile avere una stima dall'alto del diametro dei semplici della realizzazione geometrica di  $b(K)$ . Due semplici  $a, b \in K$  appartengono ad un semplice di  $b(K)$  se e solo se uno è contenuto nell'altro. Diciamo

$$a = \{x_0, \dots, x_p\} \subset b = \{x_0, \dots, x_q\}, \quad x_i \in I \subset \mathbb{R}^n, \quad p \leq q.$$

Vale allora la disuguaglianza

$$\|f(a) - f(b)\| \leq \frac{q}{q+1} \max_{0 \leq i, j \leq q} \|x_i - x_j\|.$$

Infatti, possiamo scrivere

$$\begin{aligned} f(a) - f(b) &= \sum_{i=0}^p \frac{x_i}{p+1} - \sum_{j=0}^q \frac{x_j}{q+1} = \sum_{i=0}^p \sum_{j=0}^q \frac{x_i - x_j}{(p+1)(q+1)} \\ &= \sum_{i=0}^p \sum_{j=0, j \neq i}^q \frac{x_i - x_j}{(p+1)(q+1)}. \end{aligned}$$

L'ultima sommatoria ha esattamente  $(p+1)q$  addendi e se  $M$  denota il massimo delle norme  $\|x_i - x_j\|$  al variare di  $i = 0, \dots, p$  e  $j = 0, \dots, q$ , per la disuguaglianza triangolare si ha

$$\|f(a) - f(b)\| \leq \frac{(p+1)q}{(p+1)(q+1)} M = \frac{q}{q+1} M.$$

#### 1.4. Grafi semplici e complessi di cricche

Prima di iniziare conviene avvisare che (quasi) tutta la terminologia in teoria dei grafi è soggetta a variazioni da testo a testo: per solidarietà con l'autore di [13] in queste note chiameremo grafo semplice quello che in letteratura viene generalmente detto grafo. Va anche detto che esistono nozioni più generali (digrafi, multigrafi, grafi orientati, ipergrafi) la cui trattazione va però oltre gli obiettivi di queste note.

**DEFINIZIONE 1.4.1.** Un **grafo semplice** (per completezza: grafo semplice astratto) è un complesso simpliciale astratto di dimensione  $\leq 1$ .

Tradizionalmente un grafo semplice viene denotato con una coppia  $(V, E)$ , dove  $V$  è detto insieme dei **vertici** e  $E$  insieme dei **lati**; ogni lato congiunge due vertici distinti e per ogni coppia di vertici distinti esiste al più un lato che li congiunge. In questa notazione, un complesso simpliciale  $(K, I)$  di dimensione  $\leq 1$  corrisponde alla coppia  $(I, K - K^{(0)})$ , e cioè

$$0\text{-semplici} = \text{vertici}, \quad 1\text{-semplici} = \text{lati}.$$

Sempre nella terminologia tradizionale, dato un grafo semplice  $\Gamma = (V, E)$ , se  $e \in E$  è un lato, i due vertici congiunti da  $e$  sono detti **estremi** di  $e$ .

Per semplicità notazionale, salvo avviso contrario *da questo momento in poi useremo il termine grafo per intendere un grafo semplice finito*, ossia con un numero finito di vertici e lati. Qualora si utilizzi la terminologia tradizionale identificheremo, spesso ed implicitamente, ogni lato con la coppia non ordinata di suoi estremi.

Dato un grafo (semplice finito)  $\Gamma = (V, E)$ , il numero di lati che hanno un dato vertice  $v$  come estremo viene detto **grado** di  $v$  e si denota  $d_\Gamma(v)$ .

**PROPOSIZIONE 1.4.2.** Se  $\Gamma = (V, E)$  è un grafo finito, allora

$$\sum_{v \in V} d_\Gamma(v) = 2|E|.$$

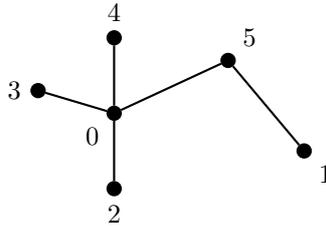
*In particolare vi è un numero pari di vertici di grado dispari.*

DIMOSTRAZIONE. L'insieme  $Z = \{(v, e) \in V \times E \mid v \in e\}$  (stiamo pensando i lati come sottoinsiemi di  $V$  di cardinalità 2) ha cardinalità  $2|E|$ , dato che ogni estremo compare in  $Z$  esattamente due volte per ogni lato. Basta allora osservare per ogni  $v \in V$ , il grado  $d_\Gamma(v)$  è la cardinalità dell'insieme  $\{(v, e) \in Z \mid e \in E\}$ .  $\square$

Nei prossimi esempi elenchiamo alcune tipologie di grafo che rivestono una certa importanza.

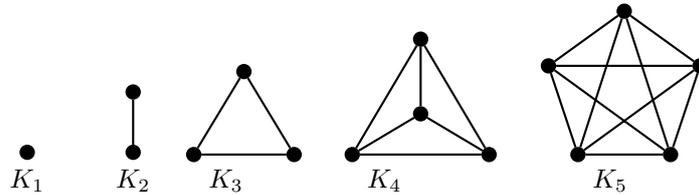
DEFINIZIONE 1.4.3. Sia  $\Gamma = (V, E)$  un grafo e si assume che esista un vertice  $v$  che appartiene ad un solo lato  $l = \{v, w\}$ . Allora la coppia  $\Gamma' = (V - \{v\}, E - \{l\})$  è ancora un grafo che viene detto **potatura** di  $\Gamma$ .

ESEMPIO 1.4.4. Un grafo finito si dice un **albero** se è connesso e se è riconducibile per successive potature ad un punto. Ad esempio il grafo



si può ricondurre per potature al solo vertice 0 e pertanto è un albero.

ESEMPIO 1.4.5. Un grafo  $\Gamma = (V, E)$  si dice **completo** se ogni coppia di vertici distinti è congiunta da un lato. Equivalentemente,  $\Gamma$  è completo se è lo 1-scheletro di  $\Delta^V$ . Per ogni  $n$  esiste un unico grafo completo con  $n$  vertici (a meno di isomorfismo) che si denota  $K_n$ .



È chiaro che  $K_n$  ha  $\binom{n}{2}$  lati e che ogni vertice di  $K_n$  ha grado  $n - 1$ .

TEOREMA 1.4.6. Per ogni grafo finito connesso e non vuoto  $\Gamma = (V, E)$  si hanno le disuguaglianze

$$|V| - 1 \leq |E| \leq \frac{|V|^2 - |V|}{2}.$$

Inoltre vale  $|V| - 1 = |E|$  se e solo se  $\Gamma$  è un albero, e vale  $|E| = (|V|^2 - |V|)/2$  se e solo se  $\Gamma$  è un grafo completo.

DIMOSTRAZIONE. Siccome  $(|V|^2 - |V|)/2$  è esattamente il numero di sottoinsiemi di cardinalità 2 di  $V$ , è ovvio per definizione che  $|E| \leq (|V|^2 - |V|)/2$  e vale l'uguaglianza se e solo se il grafo è completo.

Dimostriamo la disuguaglianza  $|E| - |V| \geq -1$  per induzione su  $|E|$ . Sia  $l \in E$  e consideriamo il grafo  $\Gamma' = (V, E - \{l\})$ . Se  $\Gamma'$  è ancora connesso allora per l'ipotesi induttiva

$$|E| - |V| = 1 + |E - \{l\}| - |V| \geq 1 - 1.$$

Se  $\Gamma'$  non è connesso, allora è unione disgiunta di due grafi connessi  $(V_1, E_1), (V_2, E_2)$ : se  $v_1, v_2$  sono gli estremi di  $l$ , allora ogni vertice di  $V$  è connesso ad uno dei vertici  $v_i$  con un cammino di lati diversi da  $l$ . Basta definire i vertici di  $V_i$  come quelli congiunti a  $v_i$  con un cammino di lati diversi da  $l$ . Ma allora

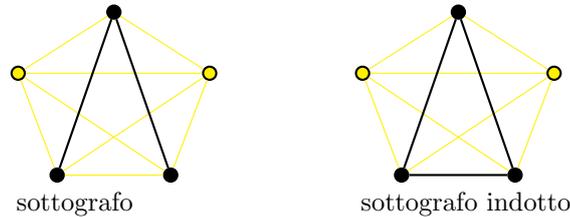
$$|E| - |V| = 1 + |E_1| + |E_2| - |V_1| - |V_2| \geq 1 - 1 - 1 = -1.$$

Per concludere dimostriamo che se  $|E| = |V| - 1$  allora  $\Gamma$  è un albero. Per  $|V| = 0, 1, 2$  non c'è nulla da dimostrare e quindi possiamo supporre per induzione che  $n = |V| \geq 3$  e

che il risultato sia vero per ogni grafo con un numero di vertici minore ad  $n$ . Dalla formula  $2|V| - 2 = 2|E| = \sum_v d_\Gamma(v)$  si deduce che esiste almeno un vertice  $v$  di grado  $\leq 1$ , e siccome  $n > 1$  e  $\Gamma$  è connesso, deve esistere un lato  $e$  che congiunge  $v$  ad un altro vertice  $u \neq v$ , ossia  $e = \{u, v\}$ . Ma allora  $e$  è un semplice massimale, ed è l'unico semplice che contiene propriamente il vertice  $v$ . Questo ci consente di fare la potatura del semplice orientato  $(u, v)$ , ottenendo un nuovo grafo  $\Gamma' = (V', E')$  con  $|V'| = |V| - 1$  e  $|E'| = |E| - 1$ . Dunque  $|E'| = |V'| - 1$  e per induzione possiamo ricondurre  $\Gamma'$  ad un solo vertice mediante una serie finita di potature.  $\square$

Un **sottografo** di un grafo non è altro che un sottocomplesso simpliciale: equivalentemente, un sottografo di  $(V, E)$  è una coppia  $(W, D)$ , con  $W \subset V$ ,  $D \subset E$  e gli estremi di ciascun lato  $e \in D$  appartengono a  $W$ .

Un sottografo  $(W, D) \subset (V, E)$  si dice **indotto** se  $D = E \cap \Delta^W$ . In altri termini, un lato  $e \in E$  appartiene a  $D$  se e solo se gli estremi di  $e$  appartengono a  $W$ .



DEFINIZIONE 1.4.7. Un sottografo  $(W, D) \subset (V, E)$  si dice una **cricca** di  $(V, E)$  se  $(W, D)$  è un grafo finito, non vuoto e completo, ossia isomorfo a  $K_n$  per qualche  $n > 0$ . Chiaramente ogni cricca è determinata dai suoi vertici, ossia da un sottoinsieme non vuoto di  $V$ .

DEFINIZIONE 1.4.8. Sia  $\Gamma = (V, E)$  un grafo. Il **complesso delle cricche** di  $\Gamma$  è il complesso simpliciale astratto

$$\widehat{\Gamma} = \{\text{cricche di } \Gamma\}.$$

Siccome ogni cricca (sottografo finito completo) è univocamente determinato dai suoi vertici, ogni cricca è univocamente determinata da un sottoinsieme finito di  $V$  e possiamo pensare  $\widehat{\Gamma} \subset \Delta^V$ . Equivalentemente si ha

$$\widehat{\Gamma} = \{\{v_0, \dots, v_n\} \in \Delta^V \mid \forall v_i \neq v_j \text{ esiste un lato } e \in E \text{ di estremi } v_i, v_j\}.$$

ed è evidente che da tale descrizione segue che  $(\widehat{\Gamma}, V)$  è un complesso simpliciale astratto.

Possiamo dare una definizione astratta di complesso di cricche nel modo seguente:

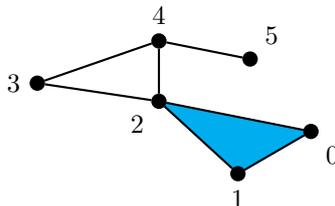
DEFINIZIONE 1.4.9. Diremo che un complesso simpliciale astratto  $(K, I)$  è un **complesso di cricche** se soddisfa la seguente condizione: dato  $s = \{x_0, \dots, x_p\} \in \Delta^I$ , allora  $s \in K$  se e solo se  $\{x_i, x_j\} \in K$  per ogni  $0 \leq i < j \leq p$ .

Segue dalla definizione che ogni complesso di cricche  $K$  è univocamente determinato dal suo 1-scheletro  $K^{(1)}$ . Possiamo riscrivere la Definizione 1.4.9 dicendo che  $(K, I)$  è di cricche se per ogni complesso simpliciale astratto  $(E, I)$  con gli stessi vertici e tale che  $E^{(1)} = K^{(1)}$  si ha  $E \subseteq K$ ; dunque i complessi di cricche sono elementi massimali nelle classi di complessi simpliciali con 1-scheletro fissato.

Proponiamo alcuni esempi per chiarire meglio il concetto.

ESEMPIO 1.4.10. Il grafo  $\Gamma = (V, E)$  è completo se e solo se  $\widehat{\Gamma} = \Delta^V$ .

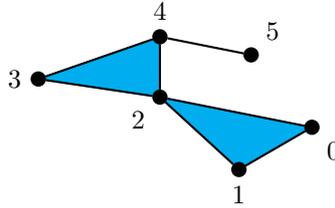
ESEMPIO 1.4.11. Il complesso simpliciale astratto



non è un complesso di cricche. Questo perché si ha:

$$\{2, 3\}, \{2, 4\}, \{3, 4\} \in K \text{ ma } \{2, 3, 4\} \notin K .$$

Aggiungendo  $\{2, 3, 4\}$  a  $K$  otteniamo ancora un complesso simpliciale astratto



che, applicando la definizione, si verifica essere un complesso di cricche.

PROPOSIZIONE 1.4.12. *La restrizione all'1-scheletro*

$$K \mapsto K^{(1)}$$

*induce una bijezione tra le classi di isomorfismo di complessi di cricche e le classi di isomorfismo di grafi semplici.*

DIMOSTRAZIONE. Abbiamo visto che un complesso di cricche è univocamente determinato dal suo 1-scheletro e questo prova che  $K \mapsto K^{(1)}$  è iniettiva sulle classi di isomorfismo. Viceversa, dato un grafo semplice  $(E = E^{(1)}, I)$  possiamo definire un complesso di cricche  $(K, I)$  ponendo

$$K = \{\{x_0, \dots, x_p\} \in \Delta^I \mid \{x_i, x_j\} \in E \text{ per ogni } i, j\}.$$

□

Possiamo generalizzare la definizione di complesso di cricche nel modo seguente.

DEFINIZIONE 1.4.13. Diremo che un complesso simpliciale astratto  $(K, I)$  è  $n$ -determinato se soddisfa la seguente condizione: dato  $s \in \Delta^I$ , allora  $s \in K$  se e solo se  $t \in K$  per ogni  $t \subset s$  con  $\dim t = |t| - 1 \leq n$ .

Chiaramente un complesso simpliciale astratto è completo se e solo se è 0-determinato, ed è di cricche se e solo se è 1-determinato. Per il Teorema di Helly (Corollario 1.1.13), il nervo di una famiglia di sottoinsiemi convessi di  $\mathbb{R}^n$  è  $n$ -determinato.

**Esercizi:**

ESERCIZIO 7. Sia  $K$  un sottocomplesso proprio di  $\Delta^n$ . Provare che se  $K$  è un complesso di cricche, allora  $K$  contiene al più due semplici di dimensione  $n - 1$ .

**1.5. Brevi cenni su categorie e funtori**

Una **categoria**  $\mathbf{C}$  è una struttura che consiste di:

- una classe  $\text{Ob}(\mathbf{C})$  i cui elementi sono detti *oggetti* della categoria;
- per ogni coppia di oggetti  $A, B \in \text{Ob}(\mathbf{C})$  è definito un insieme  $\mathbf{C}(A, B)$  (talvolta denotato  $\text{Hom}(A, B)$ ), detto *insieme dei morfismo da A a B*;
- per ogni terna di oggetti  $A, B, C$  in  $\mathbf{C}$ , un *prodotto di composizione*

$$\mathbf{C}(A, B) \times \mathbf{C}(B, C) \rightarrow \mathbf{C}(A, C), \quad (f, g) \mapsto g \circ f.$$

I suddetti dati devono soddisfare le seguenti condizioni:

- Gli insiemi  $\mathbf{C}(A_1, B_1), \mathbf{C}(A_2, B_2)$  sono disgiunti eccetto il caso in cui  $A_1 = A_2$  e  $B_1 = B_2$ ;
- Per ogni  $f \in \mathbf{C}(A, B), g \in \mathbf{C}(B, C), h \in \mathbf{C}(C, D)$ , vale la legge associativa  $h(gf) = (hg)f$ .

- Per ogni  $A \in \text{Ob}(\mathbf{C})$  esiste un morfismo  $\text{Id}_A \in \mathbf{C}(A, A)$  detto *identità* tale che  $f \text{Id}_A = f$  per ogni  $f \in \mathbf{C}(A, B)$  e  $\text{Id}_A g = g$  per ogni  $g \in \mathbf{C}(B, A)$ .

Nel seguito denoteremo  $A \in \mathbf{C}$  per indicare che  $A$  è un oggetto della categoria  $\mathbf{C}$  e  $f \in \text{Mor}(\mathbf{C})$  per indicare che  $f$  è un morfismo nella categoria  $\mathbf{C}$  (tra due oggetti non identificati o chiari dal contesto).

Siano  $\mathbf{C}$  e  $\mathbf{D}$  due categorie, un **funto**re  $F: \mathbf{C} \rightarrow \mathbf{D}$  è il dato di:

- un'applicazione che ad ogni oggetto  $A$  di  $\mathbf{C}$  associa un oggetto  $F(A)$  di  $\mathbf{D}$ ;
- per ogni  $A, B$  oggetti di  $\mathbf{C}$  un'applicazione  $F: \mathbf{C}(A, B) \rightarrow \mathbf{D}(F(A), F(B))$ .

Le applicazioni precedenti devono preservare i prodotti di composizione e le identità, ossia:

- $F(f \circ g) = F(f) \circ F(g)$ ,
- $F(\text{Id}_A) = \text{Id}_{F(A)}$ .

Gli spazi vettoriali su di un campo fissato e le rispettive applicazioni lineari formano un altro esempio di categoria, così come gli spazi topologici e le applicazioni continue.

I complessi simpliciali astratti, con i rispettivi morfismi è un altro esempio di categoria.

*Memento: da fare, al momento opportuno, gli esempi delle categorie dei complessi simpliciali astratti con classi di contiguità di morfismi, dei gruppi abeliani e dei moduli di persistenza. Forse conviene anticipare a questo capitolo i morfismi tra complessi simpliciali e le classi di contiguità.*

## Elementi di algebra omologica

Obiettivo di questo capitolo è introdurre e studiare i complessi omologici di gruppi abeliani, assieme ad alcune proprietà collegate, a partire dalla caratteristica di Eulero-Poincaré.

Per semplicità notazionale, salvo avviso contrario **tutti i gruppi sono considerati abeliani** e scritti in notazione additiva, con elemento neutro 0, inverso  $-x$  e multipli interi  $nx = x + \dots + x$  ( $n$ -volte) per  $n \in \mathbb{Z}$ .

Con  $\mathbb{Q}^n$  intenderemo lo spazio vettoriale numerico sul campo  $\mathbb{Q}$  dei vettori colonna ad  $n$  componenti e con  $\mathbb{Z}^n \subset \mathbb{Q}^n$  il sottogruppo dei vettori a coordinate intere. Quando ciò non creerà problemi, per semplicità di scrittura in molte occasioni spianeremo le colonne, scrivendo

$$(a_1, \dots, a_n) \in \mathbb{Z}^n \text{ con lo stesso significato di } (a_1, \dots, a_n)^T = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \in \mathbb{Z}^n.$$

Useremo i simboli  $\subset$  e  $\subseteq$  con lo stesso significato di inclusione non necessariamente propria.

### 2.1. Preliminari di teoria dei gruppi

Iniziamo con due semplicissimi risultati la cui evidenziazione è motivata dal fatto che entrano, *mutatis mutandis*<sup>1</sup>, come assiomi in alcune teorie avanzate (non trattate in queste note) e molto astratte come ad esempio l'*omotopia algebrica*.

LEMMA 2.1.1 (Regola del 2 su 3). *Siano  $A \xrightarrow{f} B \xrightarrow{g} C$  due omomorfismi di gruppi. Se due qualsiasi dei tre omomorfismi  $f, g, gf$  sono isomorfismi, allora lo è anche il terzo.*

DIMOSTRAZIONE. Consideriamo il caso in cui  $f$  e  $gf$  sono isomorfismi, lasciando gli altri due per esercizio. Dato che  $gf$  è surgettivo, anche  $g$  è surgettivo. Se  $g(b) = 0$  con  $b \in B$ , allora possiamo scrivere  $b = f(a)$ , dunque  $gf(a) = 0$  e poiché  $gf$  è iniettivo ne consegue che  $a = 0$  ed a maggior ragione  $b = f(0) = 0$ .  $\square$

LEMMA 2.1.2 (Regola del 2 su 6). *Dato un diagramma commutativo*

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

*di 4 gruppi e 6 omomorfismi, se  $f$  e  $g$  sono isomorfismi, allora sono isomorfismi pure i rimanenti quattro omomorfismi.*

DIMOSTRAZIONE. Per la regola del 2 su 3 è sufficiente dimostrare che la freccia diagonale da  $B$  a  $C$  è un isomorfismo. Diamo un nome anche ai rimanenti omomorfismi, trascurando per esigenze grafiche la freccia da  $A$  a  $D$ :

$$\begin{array}{ccc} A & \xrightarrow{\alpha} & B \\ f \downarrow & \beta \swarrow & \downarrow g \\ C & \xrightarrow{\gamma} & D \end{array}$$

<sup>1</sup>Mutatis mutandis = cambiando quel che c'è da cambiare.

Si ha  $f = \beta\alpha$  e  $g = \gamma\beta$ . Siccome  $f$  è surgettivo, anche  $\beta$  è surgettivo; siccome  $g$  è iniettivo, anche  $\beta$  è iniettivo. Dunque  $\beta$  è bigettivo e quindi un isomorfismo.  $\square$

Se  $A, B$  sono due sottogruppi di un gruppo abeliano  $G$ , allora anche  $A \cap B$  e

$$A + B = \{a + b \mid a \in A, b \in B\}$$

sono sottogruppi di  $G$ .

Se  $G, H$  sono due gruppi abeliani, allora anche la loro **somma diretta**

$$G \oplus H = \{(x, y) \mid x \in G, y \in H\}$$

è un gruppo abeliano, con somma  $(x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2)$  ed elemento neutro  $(0, 0)$ . Ad esempio  $\mathbb{Z}^2 = \mathbb{Z} \oplus \mathbb{Z}$ . Si noti che esistono due inclusioni naturali  $G \subset G \oplus H$ ,  $H \subset G \oplus H$ , dove ciascun  $x \in G$  viene identificato con  $(x, 0)$  e ciascun  $y \in H$  viene identificato con  $(0, y)$ .

LEMMA 2.1.3. *Siano  $f: G \rightarrow H$  e  $s: H \rightarrow G$  due omomorfismi di gruppi tali che  $fs = \text{Id}_H$ , ossia  $f(s(h)) = h$  per ogni  $h \in H$ . Allora esiste un isomorfismo  $G \cong H \oplus \ker(f)$ .*

DIMOSTRAZIONE. Osserviamo che dalla relazione  $fs = \text{Id}_H$  segue che  $f$  è surgettivo ed  $s$  è iniettivo. Sia  $s(H) \subset G$  l'immagine dell'omomorfismo  $s$ , allora  $s: H \rightarrow s(H)$  è un isomorfismo e basta quindi dimostrare che  $G = s(H) \oplus \ker(f)$ , ossia che  $s(H) \cap \ker(f) = 0$  e  $s(H) + \ker(f) = G$ .

Se  $x \in s(H) \cap \ker(f)$ , allora  $x = s(h)$  per qualche  $h \in H$  e  $f(x) = 0$ . Ma allora  $h = fs(h) = f(x) = 0$  ed a maggior ragione  $x = 0$ . Dato  $x \in G$  si può scrivere  $x = sf(x) + (x - sf(x))$ . Si ha  $sf(x) \in s(H)$  e  $f(x - sf(x)) = f(x) - fsf(x) = f(x) - \text{Id}_H(f(x)) = 0$ , e dunque  $x - sf(x) \in \ker(f)$ .

Alternativamente, si verifica direttamente che l'omomorfismo di gruppi

$$\alpha: H \oplus \ker(f) \rightarrow G, \quad \alpha(x, y) = s(x) + y,$$

è un isomorfismo con inverso

$$\beta: G \rightarrow H \oplus \ker(f), \quad \beta(x) = (f(x), x - sf(x)).$$

$\square$

L'insieme degli omomorfismi tra due gruppi abeliani è ancora un gruppo abeliano, dove per  $f, g: G \rightarrow H$  omomorfismi si definisce  $f + g: G \rightarrow H$ ,  $(f + g)x = f(x) + g(x)$ .

Siano  $G$  un gruppo abeliano,  $H \subseteq G$  un sottogruppo e  $\pi: G \rightarrow G/H$  la proiezione al quoziente.

1) Esiste una bijezione naturale tra i sottogruppi di  $G/H$  ed i sottogruppi di  $G$  che contengono  $H$ . Secondo tale bijezione, ad un sottogruppo  $K \subseteq G/H$  si associa il sottogruppo

$$\pi^{-1}(K) = \{x \in G \mid \pi(x) \in K\}$$

mentre ad un sottogruppo  $H \subseteq M \subseteq G$  si associa il quoziente  $M/H \subset G/H$ .

2) Se  $f: G \rightarrow P$  è un omomorfismo di gruppi, allora  $f$  si fattorizza al quoziente, ossia esiste  $\bar{f}: G/H \rightarrow P$  tale che  $f = \bar{f}\pi$  se e solo se  $H \subseteq \ker(f)$ . In tal caso, l'immagine di  $\bar{f}$  è uguale all'immagine di  $f$  ed il nucleo di  $\bar{f}$  è uguale a  $\ker(f)/H$ . In particolare:  $\bar{f}$  è surgettiva se e solo se  $f$  è surgettiva;  $\bar{f}$  è iniettiva se e solo se  $\ker(f) = H$ .

3) Sia adesso  $A \subseteq G$  un sottogruppo. Dati  $x \in G$  e  $y \in A$  si ha  $\pi(x) = \pi(y)$  se e solo se  $x - y \in H$ , ossia se e solo se esiste  $h \in H$  tale che  $x = y + h$ . Da ciò segue che

$$\pi^{-1}(\pi(A)) = A + H = \{y + h \mid y \in A, h \in H\}$$

e di conseguenza che  $\pi(A) = \frac{A + H}{H}$ . È chiaro che il nucleo della restrizione  $\pi: A \rightarrow G/H$  è  $A \cap H$ . In conclusione si ha:

- (1)  $\pi: A \rightarrow G/H$  iniettiva se e solo se  $A \cap H = 0$ ;
- (2)  $\pi: A \rightarrow G/H$  surgettiva se e solo se  $A + H = G$ .

## 2.2. Gruppi abeliani finiti

In questa sottosezione riportiamo una dimostrazione del celebre fatto che ogni gruppo abeliano finito  $G$  è somma diretta di gruppi ciclici finiti. Si tratta di un risultato classico dimostrato in quasi tutti i testi di algebra. In queste note daremo una dimostrazione alternativa, diversa da tutte quelle che l'autore è riuscito a trovare in letteratura, sebbene sia molto probabile che la medesima appaia scritta da qualche parte.

Per ogni insieme finito  $X$  denotiamo con  $|X|$  la sua cardinalità: dunque, per ogni gruppo finito  $G$  il suo ordine è uguale a  $|G|$ .

Dato un gruppo abeliano finito  $G$  ed un suo elemento  $x \in G$ , per il teorema di Lagrange l'ordine di  $x$ , ossia il più piccolo intero positivo  $n > 0$  tale che  $nx = 0$ , divide l'ordine di  $G$ . Più in generale per ogni sottogruppo  $H \subset G$ , l'ordine di  $H$  divide l'ordine di  $G$ .

Per ogni intero  $n > 0$  denotiamo con  $\mathbb{Z}/n$  il gruppo ciclico finito di ordine  $n$  e rappresentiamo i suoi elementi con gli interi  $\{0, 1, \dots, n-1\}$  nella maniera evidente, ossia interpretando  $\mathbb{Z}/n$  come il gruppo delle classi di resto della divisione per  $n$ . Ogni sottogruppo di  $\mathbb{Z}/n$  è univocamente determinato dal suo ordine: più precisamente, se  $G \subset \mathbb{Z}/n$  è un sottogruppo di ordine  $m$  allora  $m|n$  (leggasi:  $m$  divide  $n$ ), vale

$$G = \left\{ 0, \frac{n}{m}, \frac{2n}{m}, \dots, \frac{(m-1)n}{m} \right\}$$

e quindi  $G \simeq \mathbb{Z}/m$ . Infatti, se

$$G = \{0, a_1, a_2, \dots, a_{m-1}\}, \quad 0 < a_1 < a_2 < \dots < a_{m-1} < n,$$

allora  $ma_1 = 0$  in  $\mathbb{Z}/n$  e quindi  $n$  divide  $ma_1$ . Si può dunque scrivere  $a_1 = in/m$  per qualche intero  $i > 0$ . Supponiamo  $i > 1$ , allora l'insieme degli interi  $\alpha$  tali che  $0 \leq \alpha a_1 < n$  ha cardinalità  $< m$  ed esiste  $b \in G$  che non è un multiplo di  $a_1$ . Ma questo implica che  $b = \alpha a_1 + r$  per qualche  $r \in G$ ,  $0 < r < a_1$ , in contraddizione con la scelta di  $a_1$ .

Notiamo che ogni omomorfismo tra gruppi ciclici finiti

$$f: \mathbb{Z}/a \rightarrow \mathbb{Z}/b, \quad a, b > 1,$$

è univocamente determinato dal valore  $f(1) \in \{0, \dots, b-1\}$ ; il valore  $f(1)$  non può essere arbitrario ma deve soddisfare la relazione  $af(1) = f(a) \equiv 0 \pmod{b}$ , ossia  $f$  è ben definito se e solo se  $b$  divide il prodotto  $af(1)$ .

In particolare se  $b = ac$  con  $c \in \mathbb{Z}$ , allora l'omomorfismo  $f$  è ben definito se e solo se  $f(1)$  è un multiplo di  $c$ .

**LEMMA 2.2.1.** *Siano  $G$  un gruppo abeliano finito di ordine  $n$  e  $H \subset G$  un sottogruppo. Allora ogni omomorfismo  $f: H \rightarrow \mathbb{Z}/n$  si estende ad un omomorfismo  $G \rightarrow \mathbb{Z}/n$ .*

**DIMOSTRAZIONE.** Dimostriamo il lemma per induzione su  $n - |H|$ . Se  $G = H$  non c'è nulla da dimostrare. Supponiamo quindi  $H \neq G$  e scegliamo un elemento  $x \in G - H$ . Siano  $m$  l'ordine di  $x$  e  $C = \{0, x, 2x, \dots, (m-1)x\} \subset G$  il sottogruppo (ciclico) generato da  $x$ . Per il teorema di Lagrange  $m$  divide  $n$ . Se  $C \cap H$  è un gruppo di ordine  $p$  allora  $p$  divide  $m$  e quindi  $C \cap H = \{0, qx, 2qx, \dots, (p-1)qx\}$ , dove  $q = m/p$ .

Dal fatto che  $f: C \cap H \simeq \mathbb{Z}/p \rightarrow \mathbb{Z}/n$  è ben definito segue che  $f(qx) = a \frac{n}{p}$  per qualche  $a = 0, \dots, p-1$  ed è quindi ben definito l'omomorfismo

$$g: H + C \rightarrow \mathbb{Z}/n, \quad g(h + ix) = f(h) + ia \frac{n}{m}.$$

Dato che  $|H + C| > |H|$  la conclusione segue dall'ipotesi induttiva.  $\square$

**LEMMA 2.2.2.** *Siano  $G$  un gruppo abeliano finito e  $x \in G$  un elemento di ordine massimo. Allora esiste una decomposizione in somma diretta  $G = C \oplus H$ , dove  $C$  è il sottogruppo ciclico generato da  $x$  e dove l'ordine di ogni elemento di  $H$  divide l'ordine di  $x$ .*

**DIMOSTRAZIONE.** Denotiamo con  $n$  l'ordine di  $G$ , con  $m$  l'ordine di  $x$  e con  $C = \{0, x, 2x, \dots, (m-1)x\}$  il sottogruppo generato da  $x$ . Per il Lemma 2.2.1 l'omomorfismo iniettivo

$$f: C \rightarrow \mathbb{Z}/n, \quad f(ax) = a \frac{n}{m}.$$

si estende ad un omomorfismo  $f: G \rightarrow \mathbb{Z}/n$ , la cui immagine  $f(G)$  è un sottogruppo di  $\mathbb{Z}/n$ , e quindi esiste  $p > 0$  che divide  $n$  e tale che

$$f(G) = \{0, p, 2p, \dots, (q-1)p\}, \quad pq = n.$$

Siccome  $f(C) \subset f(G)$  si ha  $p \leq n/m$ ; d'altra parte se  $y \in G$  è tale che  $g(y) = p$ , allora l'ordine di  $y$  è almeno  $n/p$  e quindi  $p = n/m$  per la scelta di  $x$ . Dunque  $f(G) = f(C)$ , ossia  $f: C \rightarrow f(G)$  è un isomorfismo. Quindi  $g = f|_C^{-1} \circ f: G \rightarrow C$  è un omomorfismo di gruppi che estende l'identità su  $C$ .

Basta adesso applicare il Lemma 2.1.3 per dedurre che, denotando  $H = \ker g$  si ha  $G = C \oplus H$ .

Per concludere dobbiamo provare che se  $y \in H$  ha ordine  $r$ , allora  $r$  divide  $m$ . Sia  $s \leq m$  l'ordine di  $x + y$ , allora  $0 = sx + sy$  e siccome  $sx \in C$ ,  $sy \in H$  e  $C \cap H = 0$  si ha  $sx = 0$  e  $sy = 0$ . Da  $sx = 0$  segue  $m|s$  e quindi  $m = s$ , mentre da  $sy = 0$  segue che  $r$  divide  $s = m$ .  $\square$

**TEOREMA 2.2.3** (Decomposizione invariante dei gruppi abeliani finiti). *Sia  $G$  un gruppo abeliano finito. Allora esiste un'unica successione di interi  $n_1, \dots, n_k \geq 2$  tali che:*

- (1)  $G \simeq \mathbb{Z}/n_1 \oplus \dots \oplus \mathbb{Z}/n_k$ ,
- (2)  $n_i$  divide  $n_{i-1}$  per ogni  $i = 2, \dots, k$ .

**DIMOSTRAZIONE.** Sia  $n_1$  il massimo ordine di un elemento di  $G$ , per il lemma precedente si può scrivere  $G \simeq \mathbb{Z}/n_1 \oplus H$  con l'ordine di ciascun elemento di  $H$  che divide  $n_1$ . Ripetendo il ragionamento con  $H$  al posto di  $G$  e iterando quanto basta si dimostra l'esistenza della decomposizione in somma diretta.

Dimostriamo per induzione su  $|G|$  che se

$$G \simeq \mathbb{Z}/n_1 \oplus \dots \oplus \mathbb{Z}/n_k, \quad 1 \leq n_k | n_{k-1} | \dots | n_1,$$

allora i numeri  $n_i > 1$  sono univocamente determinati.

Se  $G = 0$  gli  $n_i$  sono tutti uguali a 1 e non c'è nulla da dimostrare. Se  $G \neq 0$  allora  $n_1 > 1$  è il massimo ordine di un elemento di  $G$ .

Sia  $p \geq 2$  un fattore irriducibile di  $n_1$  e consideriamo l'omomorfismo di moltiplicazione per  $p$ :

$$f: G \rightarrow G, \quad f(x) = px.$$

Dette  $f_i: \mathbb{Z}/n_i \rightarrow \mathbb{Z}/n_i$  le restrizioni di  $f$  si ha  $\ker(f) = \bigoplus_i \ker(f_i)$  e

$$\ker(f_i) = 0 \text{ se } p \nmid n_i, \quad \ker(f_i) = \mathbb{Z}/p \text{ se } p | n_i.$$

Dunque  $|\ker f| = p^s$ , dove  $k \geq s > 0$  è il numero di indici  $i$  tali che  $p | n_i$ . Ma allora  $n_i = pm_i$  per ogni  $i = 1, \dots, s$  e l'immagine di  $f$  è il sottogruppo

$$H = \mathbb{Z}/m_1 \oplus \dots \oplus \mathbb{Z}/m_s \oplus \mathbb{Z}/n_{s+1} \oplus \dots \oplus \mathbb{Z}/n_k,$$

e per l'ipotesi induttiva i numeri  $m_1, \dots, m_s, n_{s+1}, \dots, n_k$  maggiori di 1 sono univocamente determinati dalla classe di isomorfismo di  $H$ .  $\square$

### 2.3. Gruppi abeliani liberi

Sia  $G$  un gruppo abeliano. In analogia con il caso degli spazi vettoriali, diremo che un sottoinsieme  $E \subset G$  **forma una base** di  $G$  se ogni  $x \in G$  può essere scritto in modo unico come combinazione lineare finita a coefficienti interi di elementi di  $E$ . Più dettagliatamente,  $E$  forma una base di  $G$  se:

- (1) per ogni  $x \in G$  esistono  $e_1, \dots, e_n \in E$  e  $a_1, \dots, a_n \in \mathbb{Z}$  tali che  $x = \sum a_i e_i$ ;
- (2) se, per dati  $e_1, \dots, e_n \in E$  elementi distinti e  $a_1, \dots, a_n \in \mathbb{Z}$  interi vale  $\sum a_i e_i = 0$ , allora  $a_i = 0$  per ogni  $i$ .

A differenza degli spazi vettoriali non tutti i gruppi abeliani possiedono una base. Ad esempio in un gruppo finito  $G$  di ordine  $n > 0$ , per ciascun elemento  $e \in E$  vale  $ne = 0$  e quindi la precedente condizione (2) è soddisfatta solo da  $E = \emptyset$ .

DEFINIZIONE 2.3.1. Un gruppo abeliano che possiede una base viene detto **gruppo abeliano libero**.

Ad esempio, per ogni  $n \geq 0$  il gruppo  $\mathbb{Z}^n$  è abeliano libero in quanto ogni suo elemento si scrive in maniera unica come combinazione lineare a coefficienti interi della base canonica:

$$\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} = a_1 \begin{pmatrix} 1 \\ \vdots \\ 0 \end{pmatrix} + \cdots + a_n \begin{pmatrix} 0 \\ \vdots \\ 1 \end{pmatrix}.$$

Ovviamente esistono altre basi di  $\mathbb{Z}^n$  oltre alla base canonica, ad esempio  $\begin{pmatrix} 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix}$  è una base di  $\mathbb{Z}^2$ .

Sia  $f: \mathbb{Z}^m \rightarrow \mathbb{Z}^n$  un omomorfismo e denotiamo come al solito con  $e_1, \dots, e_m$  la base canonica di  $\mathbb{Z}^m$ . Allora

$$f \begin{pmatrix} a_1 \\ \vdots \\ a_m \end{pmatrix} = f \left( \sum_i a_i e_i \right) = \sum a_i f(e_i) = B \begin{pmatrix} a_1 \\ \vdots \\ a_m \end{pmatrix},$$

dove  $B \in M_{n,m}(\mathbb{Z})$  è la matrice che ha come vettori colonna le immagini  $f(e_i)$ .

LEMMA 2.3.2. *Nelle notazioni precedenti  $f$  è un isomorfismo se e solo se  $n = m$  e  $\det(B) = \pm 1$ . In particolare  $\mathbb{Z}^m$  è isomorfo a  $\mathbb{Z}^n$  se e solo se  $n = m$ .*

DIMOSTRAZIONE. Se  $n = m$  e  $\det(B) = \pm 1$  allora  $B$  è invertibile con inversa  $B^{-1}$  a coefficienti interi. Infatti se  $\det(B) = \pm 1$  allora

$$B^{-1} = \frac{(\text{aggiunta classica})}{\det(B)} = \frac{(\text{matrice dei cofattori})^T}{\det(B)} \in M_{n,n}(\mathbb{Z}).$$

Questo implica che  $f$  è invertibile con inverso definito dalla matrice  $B^{-1}$ .

Viceversa se  $f$  è invertibile, il suo inverso  $f^{-1}: \mathbb{Z}^n \rightarrow \mathbb{Z}^m$  è a sua volta rappresentato da una matrice  $C$  tale che  $BC = I$  e  $CB = I$ . Per ben noti fatti di algebra lineare questo implica che  $B, C$  sono matrici quadrate e  $\det(B) \det(C) = \det(I) = 1$ . Siccome le matrici  $B, C$  hanno coefficienti interi pure i loro determinanti sono interi e dunque  $\det(B) = \det(C) = \pm 1$ .  $\square$

LEMMA 2.3.3. *Sia  $f: G \rightarrow \mathbb{Z}^n$  un omomorfismo surgettivo di gruppi. Allora  $G \cong \mathbb{Z}^n \oplus \ker(f)$ .*

DIMOSTRAZIONE. Sia  $e_1, \dots, e_n \in \mathbb{Z}^n$  la base canonica e scegliamo degli elementi  $x_1, \dots, x_n \in G$  tali che  $f(x_i) = e_i$ .

Possiamo quindi definire un omomorfismo di gruppi

$$s: \mathbb{Z}^n \rightarrow G, \quad s \left( \sum a_i e_i \right) = \sum a_i x_i,$$

che soddisfa la condizione  $fs = \text{Id}_{\mathbb{Z}^n}$ . La conclusione segue dal Lemma 2.1.3.  $\square$

TEOREMA 2.3.4. *Sia  $H$  un sottogruppo di  $\mathbb{Z}^n$ . Allora  $H$  è isomorfo a  $\mathbb{Z}^m$  per qualche intero  $0 \leq m \leq n$ . Inoltre, se  $m < n$  allora esiste un elemento  $x \in \mathbb{Z}^n$  tale che  $Nx \notin H$  per ogni intero  $N > 0$ .*

DIMOSTRAZIONE. Dimostriamo il teorema per induzione su  $n$ , con il caso  $n = 0$  ovvio ed il caso  $n = 1$  ben noto (gli unici sottogruppi di  $\mathbb{Z}$  sono  $0 \simeq \mathbb{Z}^0$  e  $(p) \simeq \mathbb{Z}$ ).

Denotiamo con  $\pi: \mathbb{Z}^n \rightarrow \mathbb{Z}$  la proiezione sull'ultima coordinata e con  $M = H \cap \ker \pi$ . Siccome  $M \subset \ker \pi \simeq \mathbb{Z}^{n-1}$  per l'ipotesi induttiva si ha  $H \simeq \mathbb{Z}^h$  con  $0 \leq h \leq n-1$ .

Se  $\pi(H) = 0$ , allora  $M = H \simeq \mathbb{Z}^h$ , mentre se  $\pi(H) \neq 0$  allora  $\pi(H) \simeq \mathbb{Z}$  in quanto sottogruppo di  $\mathbb{Z}$ . Basta adesso applicare il Lemma 2.3.3 all'omomorfismo surgettivo  $\pi: H \rightarrow \pi(H) \cong \mathbb{Z}$  per dedurre che  $H \cong M \oplus \pi(H) \cong \mathbb{Z}^h \oplus \mathbb{Z} = \mathbb{Z}^{h+1}$ .

Abbiamo quindi dimostrato che  $H \simeq \mathbb{Z}^m$  con  $m \leq n$ . Se  $m < n$ , segue dalla dimostrazione che sono possibili due casi:  $H \cap \ker \pi \simeq \mathbb{Z}^h$  con  $h < n-1$  oppure  $\pi(H) = 0$ .

Nel primo caso, siccome  $\ker \pi = \mathbb{Z}^{n-1}$ , per l'ipotesi induttiva esiste  $x \in \ker \pi$  tale che  $Nx \notin H$  per ogni  $N > 0$ . Nel secondo caso  $H \subset \ker \pi$  e quindi  $Ne_n \notin H$  per ogni  $N > 0$ , dove  $e_n = (0, \dots, 1)$  è l'ultimo elemento della base canonica di  $\mathbb{Z}^n$ .  $\square$

**COROLLARIO 2.3.5.** *Sia  $H$  un sottogruppo di  $\mathbb{Z}^n$  tale che il quoziente  $\mathbb{Z}^n/H$  sia un gruppo finito. Allora  $H \simeq \mathbb{Z}^n$ .*

**DIMOSTRAZIONE.** Sia  $p: \mathbb{Z}^n \rightarrow \mathbb{Z}^n/H$  la proiezione al quoziente. Per ogni  $x \in \mathbb{Z}^n$  l'elemento  $p(x)$  ha ordine finito, ossia esiste  $N > 0$  tale che  $Np(x) = 0$ . Ma questo equivale a dire  $Nx \in H$  e per il Teorema 2.3.4 deve essere  $H \simeq \mathbb{Z}^n$ .  $\square$

Nota: dimostreremo più avanti che vale anche il viceversa del Corollario 2.3.5, ossia che per un sottogruppo  $H \subset \mathbb{Z}^n$  vale  $H \simeq \mathbb{Z}^n$  se e solo se  $\mathbb{Z}^n/H$  è finito.

**LEMMA 2.3.6.** *Siano  $G$  un gruppo abeliano ed  $E \subset G$  un suo sottoinsieme. Allora  $E$  forma una base se e solo se per ogni gruppo abeliano  $H$  ed ogni applicazione (di insiemi)  $F: E \rightarrow H$  vi è un unico omomorfismo di gruppi  $f: G \rightarrow H$  tale che  $F(e) = f(e)$  per ogni  $e \in E$ .*

**DIMOSTRAZIONE.** Se  $E$  forma una base di  $G$ , allora ogni applicazione  $F: E \rightarrow H$  a valori in un gruppo abeliano  $H$  si estende ad un omomorfismo  $f: G \rightarrow H$  tramite la formula

$$(2.1) \quad f(a_1e_1 + \cdots + a_n e_n) = a_1F(e_1) + \cdots + a_nF(e_n), \quad a_i \in \mathbb{Z}, \quad e_i \in E,$$

ed il fatto per  $E$  di essere una base implica che  $f$  è ben definito.

L'implicazione inversa, essendo meno rilevante ai fini di queste note, viene lasciata per esercizio al lettore.  $\square$

In particolare, se  $G_1, G_2$  sono gruppi abeliani liberi con basi  $E_1, E_2$ , allora ogni applicazione  $F: E_1 \rightarrow E_2$  si estende in maniera unica ad un omomorfismo di gruppi  $f: G_1 \rightarrow G_2$ , che quindi risulta determinato dalla formula di estensione lineare (2.1); è chiaro che  $F$  è iniettiva (resp.: surgettiva) se e solo se  $f$  è iniettiva (resp.: surgettiva).

In particolare, se  $E_1, E_2$  hanno la stessa cardinalità allora i due gruppi  $G_1, G_2$  sono isomorfi<sup>2</sup>.

**DEFINIZIONE 2.3.7.** Dato un qualunque insieme  $E$  denotiamo con  $\mathbb{Z}^{(E)}$  il gruppo abeliano di tutte le combinazioni lineari formali finite a coefficienti interi di elementi di  $E$ .

Per le usuali regole distributive ogni elemento di  $\mathbb{Z}^{(E)}$  si scrive in maniera unica in forma ridotta, ossia come  $a_1e_1 + \cdots + a_n e_n$ , con  $a_i \in \mathbb{Z}$ ,  $e_i \in E$ ,  $a_i \neq 0$  ed  $e_i \neq e_j$  per ogni  $i \neq j$  (unica a meno di permutazioni degli addendi  $a_i e_i$ , ovviamente):

$$\mathbb{Z}^{(E)} = \{0\} \cup \{ae \mid a \in \mathbb{Z} - \{0\}, e \in E\} \cup \{a_1e_1 + a_2e_2 \mid a_i \in \mathbb{Z} - \{0\}, e_i \in E, e_1 \neq e_2\} \cup \cdots$$

Identificando ciascun  $e \in E$  con  $1e \in \mathbb{Z}^{(E)}$  è chiaro per costruzione che  $E$  è una base di  $\mathbb{Z}^{(E)}$ . Chiameremo  $\mathbb{Z}^{(E)}$  il **gruppo abeliano libero generato da  $E$** . Ad esempio, il gruppo  $\mathbb{Z}^n$  si identifica naturalmente con il gruppo abeliano libero generato dalla base canonica di  $\mathbb{Q}^n$ .

### Esercizi:

**ESERCIZIO 8 (retrazioni).** Con il termine retrazione si intende un diagramma commutativo di omomorfismi di gruppi

$$\begin{array}{ccccc}
 & & Id_A & & \\
 & & \curvearrowright & & \\
 A & \longrightarrow & U & \longrightarrow & A \\
 \downarrow f & & \downarrow g & & \downarrow f \\
 B & \longrightarrow & V & \longrightarrow & B \\
 & & \curvearrowleft & & \\
 & & Id_B & & 
 \end{array}$$

ed in tal caso diremo che  $f$  è un retratto di  $g$ .

- (1) Dimostrare che la relazione di retrazione gode della proprietà transitiva, ossia che se  $f$  è un retratto di  $g$  e se  $g$  è un retratto di  $h$ , allora  $f$  è un retratto di  $h$ .

<sup>2</sup>È vero anche il viceversa [13, Esercizio 14.8], ma la dimostrazione non è affatto banale in quanto non è detto che un ipotetico isomorfismo  $G_1 \rightarrow G_2$  sia indotto da un'applicazione  $E_1 \rightarrow E_2$ .

- (2) Sia  $f$  un retratto di  $g$ , dimostrare che se  $g$  è iniettiva (risp.: surgettiva), allora anche  $f$  è iniettiva (risp.: surgettiva).
- (3) Sia  $e: G \rightarrow G$  un'omomorfismo di gruppi tale che  $e^2 = e$  e si denoti

$$H = \{x \in G \mid e(x) = x\}.$$

Dimostrare che:

- (a)  $H$  è un sottogruppo di  $G$  che coincide con l'immagine di  $e$ ;
- (b) siano  $i: H \rightarrow G$  il morfismo di inclusione e  $p: G \rightarrow H$  l'unico omomorfismo tale che  $ip = e$ . Allora  $i$  e  $p$  sono entrambe dei retratti di  $e$ .

ESERCIZIO 9. Siano  $A, B, C$  tre sottogruppi di un gruppo abeliano  $G$ , si assuma  $C \subseteq A \cap B$  in modo tale che la composizione dell'inclusione  $A \subset G$  con la proiezione al quoziente  $G \rightarrow G/B$  si fattorizza ad un omomorfismo di gruppi quoziente  $f: \frac{A}{C} \rightarrow \frac{G}{B}$ . Provare che  $f$  è surgettivo se e solo se  $A + B = G$  e che  $f$  è iniettivo se e solo se  $C = A \cap B$ .

ESERCIZIO 10. Provare il gruppo  $\mathbb{Q}$  non è abeliano libero. Più in generale provare che se  $G$  è un gruppo abeliano libero allora l'unico omomorfismo  $\mathbb{Q} \rightarrow G$  è quello banale.

ESERCIZIO 11. Provare che un gruppo finito  $T$  non è abeliano libero. Più in generale provare che se  $G$  è un gruppo abeliano libero allora l'unico omomorfismo  $T \rightarrow G$  è quello banale.

ESERCIZIO 12. Siano  $n$  un intero,  $p$  un numero primo e  $f: \mathbb{Z}^n \rightarrow \mathbb{Z}/(p)$  un omomorfismo surgettivo. Provare che esistono due isomorfismi di gruppi  $\alpha: \mathbb{Z}^n \rightarrow \mathbb{Z}^n$  e  $\beta: \mathbb{Z}/(p) \rightarrow \mathbb{Z}/(p)$  tali che

$$\beta f \alpha(a_1, \dots, a_n) \equiv a_1 \pmod{p},$$

e dedurre che  $\ker(f) \cong \mathbb{Z}^n$ . (Suggerimento: dimostrare preliminarmente che esistono due isomorfismi di gruppi  $\gamma: \mathbb{Z}^n \rightarrow \mathbb{Z}^n$  e  $\beta: \mathbb{Z}/(p) \rightarrow \mathbb{Z}/(p)$  tali che  $\beta f \gamma(1, 0, \dots, 0) \equiv 1 \pmod{p}$ .)

## 2.4. Successioni esatte

Il periodo 1940–1955 è stato caratterizzato da un forte sviluppo della topologia algebrica: molte idee maturate in quel periodo hanno influenzato enormemente tutta quanta la matematica degli anni a seguire. Basta citare ad esempio i concetti di Categoria e Funtore e l'utilizzo grafico delle frecce fino ad allora sconosciuto (sembra che il primo ad utilizzare una freccia per indicare un morfismo sia stato Hurewicz nel 1940). Tra le nuove nozioni troviamo anche quelle di *complesso*, *successione esatta*, nonché una tecnica di dimostrazione nota come *caccia al diagramma*.

La caccia al diagramma, dove il termine caccia non è inteso in senso venatorio ma allo stesso modo di caccia al tesoro, è un utile metodo di dimostrazione usato specialmente in algebra omologica. Dato un diagramma commutativo, la caccia al diagramma sfrutta in maniera formale alcune proprietà del diagramma stesso come l'iniettività o la surgettività di alcune applicazioni o come l'esattezza di alcune successioni.

Sappiamo già cosa sono le applicazioni iniettive e surgettive; introduciamo adesso il concetto di successione esatta: fra i tanti possibili diagrammi di gruppi abeliani ed omomorfismi, particolarmente importanti sono quelli a forma di stringa, ossia i diagrammi con le applicazioni disposte in serie:

$$(2.2) \quad \cdots \rightarrow G_n \xrightarrow{f_n} G_{n-1} \xrightarrow{f_{n-1}} G_{n-2} \rightarrow \cdots$$

DEFINIZIONE 2.4.1. Un diagramma di omomorfismi di gruppi abeliani disposti in serie come in (2.2) si dice un **complesso** se  $f_{n-1}f_n = 0$  per ogni  $n$ , ossia se la composizione di omomorfismi contigui è sempre nulla.

Equivalentemente il diagramma (2.2) è un complesso se per ogni  $n$  l'immagine di  $f_n$  è contenuta nel nucleo di  $f_{n-1}$ . Un complesso si dice finito o limitato se contiene solo un numero finito di spazi vettoriali ed applicazioni lineari; tuttavia è utile, in vista di future applicazioni,

considerare anche complessi infiniti o illimitati, nei quali gli indici  $n$  che compaiono nel diagramma sono tutti gli interi contenuti in un intervallo della retta reale.

Naturalmente la scelta degli indici a pedice in (2.2) è puramente decorativa e possiamo anche denotare complessi in altre forme, come ad esempio:

$$\begin{aligned} \cdots \rightarrow G_a \xrightarrow{f_a} G_b \xrightarrow{f_b} G_c \xrightarrow{f_c} G_d \rightarrow \cdots, \\ 0 \rightarrow G_{\text{Adamo}} \rightarrow G_{\text{Caino}} \rightarrow \cdots \rightarrow G_{\text{nonno}} \rightarrow G_{\text{babbo}} \rightarrow G_{\text{me}} \rightarrow 0. \end{aligned}$$

Tuttavia, i due stili maggiormente usati in algebra sono quello *omologico*, con i numeri interi a pedice in ordine decrescente come in (2.2), e lo stile *coomologico*, con i numeri interi in apice ed in ordine crescente:

$$\cdots \rightarrow G^n \xrightarrow{f_n} G^{n+1} \xrightarrow{f_{n+1}} G^{n+2} \rightarrow \cdots.$$

DEFINIZIONE 2.4.2. Un diagramma di omomorfismi di gruppi abeliani disposti in serie come in (2.2) si dice una **successione esatta** se per ogni  $n$  il nucleo di  $f_{n-1}$  è uguale all'immagine di  $f_n$ .

In particolare ogni successione esatta è anche un complesso, mentre il viceversa è generalmente falso: ad esempio, il diagramma

$$0 \rightarrow G \rightarrow 0$$

è un complesso qualunque sia il gruppo  $G$ , mentre è una successione esatta se e solo se  $G = 0$ .

ESEMPIO 2.4.3. Sia  $f: H \rightarrow G$  un omomorfismo di gruppi. Allora:

- (1)  $f$  iniettivo se e solo se  $0 \rightarrow H \xrightarrow{f} G$  esatta;
- (2)  $f$  surgettivo se e solo se  $H \xrightarrow{f} G \rightarrow 0$  esatta;
- (3)  $f$  isomorfismo se e solo se  $0 \rightarrow H \xrightarrow{f} G \rightarrow 0$  esatta.

ESEMPIO 2.4.4. Supponiamo che

$$G_3 \xrightarrow{f_3} G_2 \xrightarrow{f_2} G_1 \xrightarrow{f_1} G_0$$

sia una successione esatta. Allora le seguenti condizioni sono equivalenti:

- (1)  $f_3$  è surgettiva;
- (2)  $f_2 = 0$ ;
- (3)  $f_1$  è iniettiva.

Infatti, per l'esattezza in  $G_1$  il nucleo di  $f_1$  è uguale all'immagine di  $f_2$ ; in particolare  $f_2$  è nulla se e solo se  $\ker f_1 = 0$ , ossia se e solo se  $f_1$  è iniettiva. Similmente, per l'esattezza in  $G_2$  il nucleo di  $f_2$  è uguale all'immagine di  $f_3$  ed in particolare  $f_2 = 0$  se e solo se  $f_3$  è surgettiva.

ESEMPIO 2.4.5. Supponiamo che

$$G_0 \xrightarrow{f_0} G_1 \xrightarrow{f_1} G_2 \xrightarrow{f_2} G_3 \xrightarrow{f_3} G_4$$

sia una successione esatta. Allora le seguenti condizioni sono equivalenti:

- (1)  $f_0$  è surgettiva e  $f_3$  è iniettiva;
- (2)  $f_1 = f_2 = 0$ ;
- (3)  $G_2 = 0$ .

I ragionamenti da fare sono analoghi a quelli dell'esempio precedente e lasciati per esercizio al lettore.

DEFINIZIONE 2.4.6. Una **successione esatta corta** è una successione esatta del tipo

$$(2.3) \quad 0 \rightarrow U \xrightarrow{f} V \xrightarrow{g} W \rightarrow 0.$$

Dunque, la (2.3) è una successione esatta corta se e solo se  $f$  è iniettiva,  $g$  è surgettiva e  $\ker g = f(U)$ .

In particolare, se (2.3) è una successione esatta si ha  $W = g(V)$  e  $f: U \rightarrow \ker g$  è un isomorfismo.

LEMMA 2.4.7. Sia  $0 \rightarrow A \xrightarrow{f} B \xrightarrow{g} C \rightarrow 0$  una successione esatta corta di gruppi abeliani finiti. Allora l'ordine di  $B$  è uguale al prodotto degli ordini di  $A$  e  $C$ .

DIMOSTRAZIONE. Per i ben noti teoremi di omomorfismo, il morfismo  $g$  induce un isomorfismo di gruppi  $B/f(A) \simeq C$  e quindi  $|C| = |B/f(A)| = |B|/|f(A)| = |B|/|A|$ .  $\square$

ESEMPIO 2.4.8. Consideriamo una successione esatta

$$0 \rightarrow V_1 \xrightarrow{f_1} V_2 \xrightarrow{f_2} V_3 \xrightarrow{f_3} V_4 \rightarrow 0;$$

indichiamo con  $U = \ker f_3 = f_2(V_2)$  e con  $i: U \rightarrow V_3$  il morfismo di inclusione. Allora la precedente successione si spezza in due successioni esatte corte

$$0 \rightarrow V_1 \xrightarrow{f_1} V_2 \xrightarrow{f_2} U \rightarrow 0, \quad 0 \rightarrow U \xrightarrow{i} V_3 \xrightarrow{f_3} V_4 \rightarrow 0.$$

TEOREMA 2.4.9 (Lemma dei 5). Sia dato il seguente diagramma commutativo di gruppi abeliani:

$$\begin{array}{ccccccccc} E_1 & \xrightarrow{d_1} & E_2 & \xrightarrow{d_2} & E_3 & \xrightarrow{d_3} & E_4 & \xrightarrow{d_4} & E_5 \\ \downarrow \alpha_1 & & \downarrow \alpha_2 & & \downarrow \beta & & \downarrow \alpha_4 & & \downarrow \alpha_5 \\ H_1 & \xrightarrow{h_1} & H_2 & \xrightarrow{h_2} & H_3 & \xrightarrow{h_3} & H_4 & \xrightarrow{h_4} & H_5 \end{array}$$

con entrambe le righe esatte.

- (1) se  $\alpha_1$  è surgettiva e  $\alpha_2, \alpha_4$  sono iniettive, allora  $\beta$  è iniettiva;
- (2) se  $\alpha_5$  è iniettiva e  $\alpha_2, \alpha_4$  sono surgettive, allora  $\beta$  è surgettiva;
- (3) se  $\alpha_1, \alpha_2, \alpha_4, \alpha_5$  sono bigettive, allora  $\beta$  è bigettiva.

DIMOSTRAZIONE. Dimostriamo solo il primo punto; la dimostrazione del secondo è del tutto simile ed è lasciata per esercizio. Il terzo punto segue banalmente dai primi due.

Sia  $x \in E_3$  tale che  $\beta(x) = 0$ , allora  $\alpha_4 d_3(x) = h_3 \beta(x) = 0$  ed essendo per ipotesi  $\alpha_4$  iniettiva si ha  $d_3(x) = 0$ . La prima riga è esatta e quindi esiste  $y \in E_2$  tale che  $x = d_2(y)$ ; siccome  $h_2 \alpha_2(y) = \beta d_2(y) = \beta(x) = 0$  e la riga inferiore è esatta, esiste  $z \in H_1$  tale che  $h_1(z) = \alpha_2(y)$ . Adesso usiamo la surgettività di  $\alpha_1$  per trovare  $w \in E_1$  tale che  $\alpha_1(w) = z$ , quindi  $\alpha_2 d_1(w) = h_1 \alpha_1(w) = h_1(z) = \alpha_2(y)$ . Per l'iniettività di  $\alpha_2$  si ha  $y = d_1(w)$  e quindi  $x = d_2(y) = d_2 d_1(w) = 0$ .  $\square$

Data una successione esatta corta  $0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0$  di gruppi abeliani, in generale i due gruppi  $B$  e  $A \oplus C$  non sono isomorfi, come ad esempio nella successione esatta

$$0 \rightarrow \mathbb{Z} \xrightarrow{\cdot 2} \mathbb{Z} \xrightarrow{d} \mathbb{Z}/2 \rightarrow 0.$$

Abbiamo però la seguente immediata conseguenza del Lemma 2.3.3.

COROLLARIO 2.4.10. Sia  $0 \rightarrow K \xrightarrow{f} G \xrightarrow{g} \mathbb{Z}^n \rightarrow 0$  una successione esatta corta di gruppi abeliani. Allora esiste un isomorfismo  $G \cong K \oplus \mathbb{Z}^n$ .

**Esercizi:**

ESERCIZIO 13. Si consideri il diagramma commutativo di gruppi abeliani

$$\begin{array}{ccccccc} & & & & 0 & & \\ & & & & \downarrow & & \\ & & & & P_1 & & \\ & N_1 & \longrightarrow & M_1 & \longrightarrow & P_1 & \\ & \downarrow & & \downarrow & & \downarrow & \\ 0 & \longrightarrow & N_2 & \longrightarrow & M_2 & \longrightarrow & P_2 \\ & & \downarrow & & \downarrow & & \\ & & N_3 & \xrightarrow{f} & M_3 & & \\ & & \downarrow & & & & \\ & & 0 & & & & \end{array}$$

in cui tutte le righe e tutte le colonne sono successioni esatte. Provare che l'applicazione  $f$  è iniettiva.

ESERCIZIO 14. Si consideri un diagramma commutativo di spazi vettoriali di dimensione finita e applicazioni lineari

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \xrightarrow{f} & B & \xrightarrow{g} & C & \longrightarrow & 0 \\ & & \downarrow \alpha & & \downarrow \beta & & \downarrow \gamma & & \\ 0 & \longrightarrow & A & \xrightarrow{f} & B & \xrightarrow{g} & C & \longrightarrow & 0 \end{array}$$

con le righe successioni esatte corte. Dimostrare che il polinomio caratteristico di  $\beta$  è il prodotto dei polinomi caratteristici di  $\alpha$  e  $\gamma$ .

## 2.5. Gruppi abeliani finitamente generati

DEFINIZIONE 2.5.1. Sia  $G$  gruppo abeliano. Un elemento  $x \in G$  è detto **di torsione** se esiste un intero  $n > 0$  tale che  $nx = 0$ .

Il sottoinsieme degli elementi di torsione di  $G$  verrà indicato con  $T(G)$ . Il gruppo  $G$  si dice **senza torsione** se  $T(G) = 0$ . Il gruppo  $G$  si dice **di torsione** se  $T(G) = G$ .

Ad esempio, ogni gruppo finito è di torsione mentre i gruppi  $\mathbb{Z}^n$ ,  $\mathbb{Q}$ ,  $\mathbb{R}$ ,  $\mathbb{C}$  sono senza torsione.

La torsione commuta con le somme dirette e con la restrizione a sottogruppi, ossia  $T(G \oplus H) = T(G) \oplus T(H)$ , mentre se  $H \subseteq G$  è un sottogruppo si ha  $T(H) = T(G) \cap H$ .

LEMMA 2.5.2. *Sia  $G$  un gruppo abeliano. Allora  $T(G)$  è un sottogruppo di  $G$  ed il quoziente  $G/T(G)$  è senza torsione.*

DIMOSTRAZIONE. Chiaramente  $0 \in T(G)$ ; se  $x, y \in T(G)$  esistono due interi  $n, m > 0$  tali che  $nx = my = 0$  e quindi  $nm(x \pm y) = 0$ .

Dire che il quoziente  $G/T(G)$  è senza torsione equivale a dire che se  $x \in G$ ,  $n > 0$  e  $nx \in T(G)$ , allora  $x \in T(G)$ . Ma se  $m(nx) = 0$  per qualche  $m > 0$  allora  $(nm)x = 0$  e dunque  $x \in T(G)$ .  $\square$

Ogni omomorfismo di gruppi  $f: G \rightarrow H$  si restringe ad un omomorfismo  $f: T(G) \rightarrow T(H)$  tra i rispettivi sottogruppi di torsione. Infatti se  $x \in T(G)$  e  $nx = 0$  per qualche intero  $n > 0$ , allora  $nf(x) = f(nx) = 0$  e quindi anche  $f(x)$  è di torsione. In particolare se  $G = T(G)$  e  $T(H) = 0$  l'unico omomorfismo  $f: G \rightarrow H$  è quello nullo: in altri termini, *non esistono omomorfismi non banali da un gruppo di torsione ad un gruppo senza torsione.*

Inoltre, siccome  $f: T(G) \rightarrow T(H)$ , passando ai quozienti il morfismo  $f$  si fattorizza ad un omomorfismo di gruppi  $\bar{f}: G/T(G) \rightarrow H/T(H)$ .

OSSERVAZIONE 2.5.3. Se  $0 \rightarrow G \rightarrow H \rightarrow F \rightarrow 0$  è una successione esatta corta di gruppi abeliani, la restrizione ai sottogruppi di torsione induce una successione  $0 \rightarrow T(G) \rightarrow T(H) \rightarrow T(F) \rightarrow 0$  che però **non** è esatta in generale. Similmente il passaggio al quoziente induce una successione  $0 \rightarrow G/T(G) \rightarrow H/T(H) \rightarrow F/T(F) \rightarrow 0$ , pure questa non esatta in generale. In entrambi i casi basta considerare come controesempio la "solita" successione esatta

$$0 \rightarrow \mathbb{Z} \xrightarrow{\cdot 2} \mathbb{Z} \rightarrow \mathbb{Z}/2 \rightarrow 0.$$

Se  $S$  è un qualunque sottoinsieme di un gruppo abeliano  $G$  denoteremo con  $\langle S \rangle \subset G$  il sottogruppo generato da  $S$ . Equivalentemente  $\langle S \rangle$  è l'insieme di tutte le espressioni del tipo

$$n_1 s_1 + \cdots + n_k s_k, \quad k \geq 0, \quad n_i \in \mathbb{Z}, \quad s_i \in S.$$

Per definizione, un elemento  $x \in G$  non è di torsione se e solo se l'omomorfismo di gruppi

$$\mathbb{Z} \rightarrow G, \quad n \mapsto nx$$

è iniettivo, e dato che l'immagine di tale omomorfismo è  $\langle x \rangle$  si ha la seguente casistica:

- (1)  $x$  è di torsione e  $\langle x \rangle$  è un gruppo finito ciclico;

(2)  $x$  non è di torsione e  $\langle x \rangle \simeq \mathbb{Z}$  è il gruppo ciclico infinito.

DEFINIZIONE 2.5.4. Diremo che un gruppo abeliano  $G$  è **finitamente generato** se è generato da un numero finito di elementi, ossia

$$G = \langle x_1, \dots, x_n \rangle = \left\{ \sum_{i=1}^n a_i x_i \mid a_i \in \mathbb{Z} \right\}.$$

Ad esempio, ogni gruppo finito è finitamente generato (basta prendere come generatori tutti gli elementi). Il gruppo  $\mathbb{Z}^n$  è senza torsione, è generato dalla “base canonica”

$$e_1 = (1, 0, \dots, 0), \quad e_2 = (0, 1, \dots, 0), \quad \dots, \quad e_n = (0, 0, \dots, 1),$$

ed è quindi finitamente generato. Se  $G$  è un gruppo finitamente generato e  $f: G \rightarrow H$  è un omomorfismo surgettivo di gruppi, allora anche  $H$  è finitamente generato: se  $x_1, \dots, x_n$  generano  $G$  allora  $f(x_1), \dots, f(x_n)$  generano  $H$ . In particolare ogni quoziente di un gruppo finitamente generato è finitamente generato.

LEMMA 2.5.5. *Un gruppo abeliano è finito se e solo se è finitamente generato e di torsione.*

DIMOSTRAZIONE. Una implicazione è chiara, ogni gruppo finito è finitamente generato ed è di torsione. Viceversa, se un gruppo abeliano di torsione  $G$  è generato da  $x_1, \dots, x_n$  allora per ogni indice  $i$  esiste un intero  $r_i > 0$  tale che  $r_i x_i = 0$ . Presa una qualunque combinazione lineare a coefficienti interi  $y = a_1 x_1 + \dots + a_n x_n$ , sostituendo eventualmente ad ogni  $a_i$  il resto della divisione per  $r_i$  non è restrittivo supporre  $0 \leq a_i < r_i$ . Ne segue che  $G$  possiede al più  $r_1 r_2 \dots r_n$  elementi distinti.  $\square$

TEOREMA 2.5.6. *Ogni gruppo abeliano  $G$  finitamente generato senza torsione (ossia con  $T(G) = 0$ ) è isomorfo a  $\mathbb{Z}^n$  per qualche  $n$ .*

DIMOSTRAZIONE. Sia  $G$  gruppo abeliano senza torsione e generato da una successione finita di elementi  $x_1, \dots, x_m \in G$ . Questo significa che l'omomorfismo di gruppi

$$\mathbb{Z}^m \rightarrow G, \quad (a_1, \dots, a_m) \mapsto \sum_{i=1}^m a_i x_i,$$

è surgettivo.

A meno di permutazioni nella successione  $x_1, \dots, x_m$  possiamo supporre che esista un intero  $0 \leq n \leq m$  tale che:

(1) l'omomorfismo di gruppi

$$f: \mathbb{Z}^n \rightarrow G, \quad f(a_1, \dots, a_n) = \sum_{i=1}^n a_i x_i,$$

è iniettivo.

(2) per ogni  $n < j \leq m$  l'omomorfismo di gruppi

$$f_j: \mathbb{Z}^{n+1} \rightarrow G, \quad f_j(a_1, \dots, a_n, b) = \sum_{i=1}^n a_i x_i + b x_j,$$

non è iniettivo.

Denotiamo con  $M = f(\mathbb{Z}^n) \subset G$  l'immagine di  $f$ : è chiaro che  $f$  è un isomorfismo sull'immagine e quindi  $M \simeq \mathbb{Z}^n$ .

Per ogni  $j = n+1, \dots, m$  scegliamo un elemento non nullo  $e_j$  del nucleo di  $f_j$ : se  $e_j = (a_{j,1}, \dots, a_{j,n}, b_j)$  possiamo supporre  $b_j \geq 0$  (altrimenti si sostituisce  $e_j$  con  $-e_j$ ).

Dall'iniettività di  $f$  segue  $b_j > 0$  e dal fatto che  $f_j(e_j) = 0$  segue  $b_j x_j \in M$ . Siccome  $x_i \in M$  per ogni  $i = 1, \dots, n$ , se  $b$  denota il prodotto dei  $b_j$  allora si ha  $b x_i \in M$  per ogni  $i = 1, \dots, m$ .

Per ipotesi il gruppo  $G$  è senza torsione, quindi l'omomorfismo  $b: G \rightarrow G$  di moltiplicazione per  $b$  è iniettivo e quindi un isomorfismo sull'immagine  $b(G)$ ; ma  $b(G)$  è il sottogruppo generato da  $b x_1, \dots, b x_m$  e quindi  $b(G) \subset M \simeq \mathbb{Z}^n$ . Basta allora applicare il Teorema 2.3.4 per dedurre che  $b(G)$  è isomorfo a  $\mathbb{Z}^h$  per qualche intero  $h \leq n \leq m$ .  $\square$

Dato un qualunque gruppo abeliano  $G$  abbiamo una successione esatta

$$0 \rightarrow T(G) \xrightarrow{i} G \xrightarrow{p} \frac{G}{T(G)} \rightarrow 0$$

con  $i$  morfismo di inclusione e  $p$  proiezione al quoziente.

Siccome  $p$  è surgettivo, se  $G$  è finitamente generato allora anche  $G/T(G)$  è finitamente generato. Per il Lemma 2.5.2 il gruppo  $G/T(G)$  è senza torsione, per il Teorema 2.5.6 si ha  $G/T(G) \cong \mathbb{Z}^n$  con l'intero  $n$  univocamente determinato per il Lemma 2.3.2.

**DEFINIZIONE 2.5.7.** Sia  $G$  un gruppo abeliano finitamente generato. Se  $G/T(G) \cong \mathbb{Z}^n$  il numero  $n$  viene detto **rango** di  $G$  e si scrive  $n = \text{rank}(G)$ .

**ESEMPIO 2.5.8.** Sia  $H$  un gruppo finito e  $G = H \oplus \mathbb{Z}^n$ . Allora  $G$  è finitamente generato e  $\text{rank}(G) = n$ . Infatti  $G$  è generato dagli elementi di  $H$  e dalla base canonica di  $\mathbb{Z}^n$ . Inoltre  $H = T(G)$  e quindi  $G/T(G) = G/H = \mathbb{Z}^n$ .

**TEOREMA 2.5.9.** Sia  $G$  un gruppo abeliano finitamente generato. Allora  $T(G)$  è un sottogruppo finito ed esiste un isomorfismo (non canonico)  $G \cong T(G) \oplus \mathbb{Z}^n$  con  $n = \text{rank}(G)$ .

**DIMOSTRAZIONE.** Per definizione di rango si ha  $G/T(G) \cong \mathbb{Z}^n$  e quindi si ha una successione esatta

$$0 \rightarrow T(G) \rightarrow G \rightarrow \mathbb{Z}^n \rightarrow 0$$

e basta applicare il Corollario 2.4.10 per avere un isomorfismo  $G \cong T(G) \oplus \mathbb{Z}^n$ .

La proiezione sul primo addendo diretto  $G \rightarrow T(G)$  è surgettiva, quindi anche  $T(G)$  è finitamente generato ed è quindi un gruppo finito per il Lemma 2.5.5.  $\square$

**COROLLARIO 2.5.10.** Sia  $H$  un sottogruppo di un gruppo  $G$  finitamente generato è ancora finitamente generato e  $\text{rank}(H) \leq \text{rank}(G)$ .

**DIMOSTRAZIONE.** Abbiamo visto che esiste una successione esatta

$$0 \rightarrow T(G) \rightarrow G \xrightarrow{p} \mathbb{Z}^n \rightarrow 0, \quad n = \text{rank}(G).$$

Restringendo  $p$  al sottogruppo  $H$  otteniamo una successione esatta

$$0 \rightarrow T(G) \cap H \rightarrow H \xrightarrow{p} p(H) \rightarrow 0,$$

e siccome  $p(H) \subset \mathbb{Z}^n$  si ha  $p(H) = \mathbb{Z}^m$  con  $m \leq n$ . Ma allora  $H \cong (T(G) \cap H) \oplus \mathbb{Z}^m$  per il Corollario 2.4.10. Per concludere basta osservare che  $T(G) \cap H$  è un sottogruppo del gruppo finito  $T(G)$  e quindi  $H$  è finitamente generato di rango  $m$ .  $\square$

### Esercizi:

**ESERCIZIO 15.** Sia  $G$  gruppo abeliano. Un elemento  $x \in G$  si dice divisibile se per ogni intero  $n > 0$  esiste  $y \in G$  tale che  $ny = x$ .

Dimostrare che in un gruppo abeliano finitamente generato non esistono elementi divisibili diversi da 0.

**ESERCIZIO 16.** Sia  $S$  un insieme di generatori di un gruppo abeliano  $G$ . Dimostrare che  $G$  è un gruppo di torsione se e solo se  $S \subset T(G)$ .

## 2.6. Additività del rango

Iniziamo con il richiamare la nozione di **conucleo** di un omomorfismo. Dato un omomorfismo di gruppi abeliani  $f: G \rightarrow H$ , l'immagine  $f(G)$  è un sottogruppo (normale in quanto  $H$  abeliano) di  $H$  e si definisce il conucleo di  $f$  come il gruppo quoziente

$$\text{coker}(f) = \frac{H}{f(G)}.$$

Se denotiamo con  $\pi: H \rightarrow \text{coker}(f)$  la proiezione al quoziente, per definizione si ha una successione esatta

$$G \xrightarrow{f} H \xrightarrow{\pi} \text{coker}(f) \rightarrow 0.$$

Viceversa, se  $G \xrightarrow{f} H \xrightarrow{p} K \rightarrow 0$  è una successione esatta, per i classici teoremi di omomorfismo dei gruppi, essendo  $p$  surgettivo, si ha un isomorfismo di gruppi

$$K \cong \frac{H}{\ker p} = \frac{H}{f(G)} = \text{coker}(f).$$

Sempre dai classici teoremi di teoria dei gruppi segue la seguente proprietà universale del conucleo:

*Sia  $G \xrightarrow{f} H$  un omomorfismo di gruppi con proiezione sul conucleo  $H \xrightarrow{\pi} \text{coker}(f)$ . Per ogni omomorfismo di gruppi  $q: H \rightarrow K$  tale che  $qf = 0$  esiste, ed è unico, un omomorfismo di gruppi  $\bar{q}: \text{coker}(f) \rightarrow K$  tale che  $q = \bar{q}\pi$ .*

Infatti, dire che  $qf = 0$  equivale a dire  $f(G) \subseteq \ker q$  e questa è condizione necessaria e sufficiente affinché  $q$  si fattorizzi al quoziente  $H/f(G)$ . L'unicità segue dal fatto che  $\pi$  è surgettivo.

Consideriamo adesso un *quadrato commutativo* di gruppi abeliani, ossia un diagramma commutativo del tipo

$$\begin{array}{ccc} A & \xrightarrow{\beta} & B \\ \downarrow \alpha & & \downarrow \gamma \\ C & \xrightarrow{\delta} & D \end{array}$$

Se  $x \in \ker \alpha$ , allora  $\gamma\beta(x) = \delta\alpha(x) = 0$  e quindi  $\beta(x) \in \ker \gamma$ . Dunque il quadrato commutativo definisce per restrizione un omomorfismo  $\beta: \ker(\alpha) \rightarrow \ker(\gamma)$ . Si noti che se  $\beta: A \rightarrow B$  è iniettivo, allora anche  $\beta: \ker(\alpha) \rightarrow \ker(\gamma)$  è iniettivo.

Si consideri adesso la proiezione sul conucleo  $\pi: D \rightarrow \text{coker}(\gamma)$ . Allora  $\pi\delta\alpha = \pi\gamma\beta = 0$  poiché  $\pi\gamma = 0$  e per la proprietà universale del conucleo, l'omomorfismo  $\pi\delta$  si fattorizza ad un omomorfismo tra i conuclei  $\bar{\delta}: \text{coker}(\alpha) \rightarrow \text{coker}(\gamma)$ :

$$\begin{array}{ccccccc} & & \ker(\alpha) & \xrightarrow{\beta} & \ker(\gamma) & & \\ & & \downarrow & & \downarrow & & \\ \ker(\beta) & \longrightarrow & A & \xrightarrow{\beta} & B & \longrightarrow & \text{coker}(\beta) \\ \downarrow \alpha & & \downarrow \alpha & & \downarrow \gamma & & \downarrow \bar{\gamma} \\ \ker(\delta) & \longrightarrow & C & \xrightarrow{\delta} & D & \longrightarrow & \text{coker}(\delta) \\ & & \downarrow & & \downarrow & & \\ & & \text{coker}(\alpha) & \xrightarrow{\bar{\delta}} & \text{coker}(\gamma) & & \end{array}$$

Consideriamo adesso due quadrati commutativi con un lato in comune

$$\begin{array}{ccccc} A & \xrightarrow{\beta} & B & \xrightarrow{\sigma} & E \\ \downarrow \alpha & & \downarrow \gamma & & \downarrow \tau \\ C & \xrightarrow{\delta} & D & \xrightarrow{\mu} & F \end{array}$$

Le precedenti osservazioni ci forniscono gli omomorfismi

$$\ker(\alpha) \xrightarrow{\beta} \ker(\gamma) \xrightarrow{\sigma} \ker(\tau), \quad \text{coker}(\alpha) \xrightarrow{\bar{\delta}} \text{coker}(\gamma) \xrightarrow{\bar{\mu}} \text{coker}(\tau).$$

LEMMA 2.6.1 (Lemma del serpente, prima versione). *Sia dato un diagramma commutativo di gruppi abeliani*

$$\begin{array}{ccccccc} N_1 & \xrightarrow{f} & M_1 & \xrightarrow{g} & P_1 & \longrightarrow & 0 \\ \downarrow \alpha & & \downarrow \beta & & \downarrow \gamma & & \\ 0 & \longrightarrow & N_2 & \xrightarrow{h} & M_2 & \xrightarrow{k} & P_2 \end{array}$$



È importante osservare che  $\varphi$  è diversa dall'applicazione “canonica”  $(a, b) \mapsto (f(a), g(b))$  che farebbe commutare il diagramma qualora la freccia verticale a destra fosse  $g$  invece di  $-g$ . Siccome  $g$  e  $-g$  hanno gli stessi nucleo e conucleo ed è immediato osservare che l'inclusione  $A \subset A \oplus B$  e la proiezione  $B \oplus C \rightarrow C$  inducono isomorfismi  $\ker(\varphi) = \ker(gf)$ ,  $\text{coker}(\varphi) = \text{coker}(gf)$ . Applicando il lemma del serpente si ottiene quindi la successione esatta lunga della Figura 1.

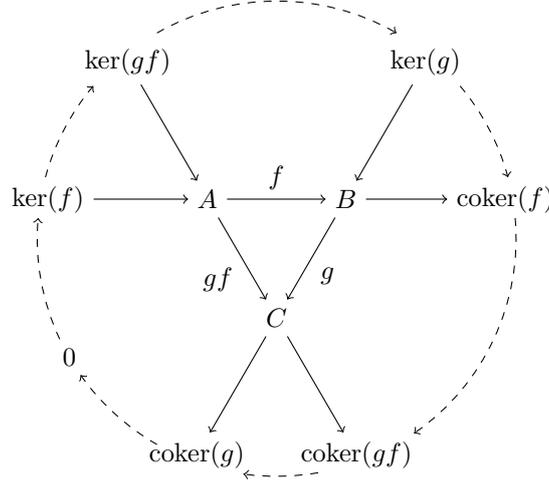


FIGURA 1. Il mulino vento, con la ruota esterna successione esatta.

LEMMA 2.6.4. *Sia*

$$0 \rightarrow \mathbb{Z}^n \xrightarrow{f} \mathbb{Z}^m \xrightarrow{g} \mathbb{Z}^p \rightarrow 0$$

*una successione esatta corta di gruppi abeliani. Allora  $n + p = m$ .*

DIMOSTRAZIONE. Per il Corollario 2.4.10 esiste un isomorfismo

$$\mathbb{Z}^m \cong \ker(g) \oplus \mathbb{Z}^p \cong \mathbb{Z}^n \oplus \mathbb{Z}^p = \mathbb{Z}^{n+p}$$

e quindi  $m = n + p$ . □

Siamo adesso in grado di applicare il lemma del serpente a due importanti risultati di teoria dei gruppi.

DEFINIZIONE 2.6.5. Un gruppo  $G$  si dice **Hopfiano** se ogni omomorfismo surgettivo  $G \rightarrow G$  è un isomorfismo.

Non tutti i gruppi sono Hopfiani: ad esempio l'omomorfismo

$$\prod_{i=1}^{\infty} \mathbb{Z} \rightarrow \prod_{i=1}^{\infty} \mathbb{Z}, \quad (a_1, a_2, a_3, \dots) \mapsto (a_2, a_3, \dots),$$

è surgettivo ma non iniettivo.

TEOREMA 2.6.6. *Ogni gruppo abeliano finitamente generato è Hopfiano.*

DIMOSTRAZIONE. Dimostriamo prima che i gruppi  $\mathbb{Z}^n$  sono Hopfiani. Se  $g: \mathbb{Z}^n \rightarrow \mathbb{Z}^n$  è surgettivo, allora il suo nucleo è finitamente generato e senza torsione, quindi isomorfo a  $\mathbb{Z}^m$  per qualche  $m$ . Per il Lemma 2.6.4 si ha  $n = n + m$  e quindi  $\ker(g) = \mathbb{Z}^0$ , ossia  $g$  è anche iniettivo.

I gruppi finiti sono Hopfiani per ovvii motivi di cardinalità.

Passiamo adesso al caso generale. Sia  $G$  un gruppo abeliano finitamente generato e sia  $g: G \rightarrow G$  un omomorfismo surgettivo. Se  $x \in T(G)$  è di torsione allora anche  $g(x)$  è di torsione e quindi  $g$  si restringe ad un omomorfismo  $g_T: T(G) \rightarrow T(G)$  e si fattorizza ad un omomorfismo surgettivo  $\bar{g}: G/T(G) \rightarrow G/T(G)$ .

Si ha quindi un diagramma commutativo con le righe esatte

$$\begin{array}{ccccccc} 0 & \longrightarrow & T(G) & \longrightarrow & G & \longrightarrow & G/T(G) \longrightarrow 0 \\ & & \downarrow g_T & & \downarrow g & & \downarrow \bar{g} \\ 0 & \longrightarrow & T(G) & \longrightarrow & G & \longrightarrow & G/T(G) \longrightarrow 0 \end{array}$$

Il gruppo  $G/T(G)$  è Hopfiano in quanto senza torsione, quindi  $\ker(\bar{g}) = 0$  e per il lemma del serpente anche  $g_T$  è surgettivo. Quindi  $g_T$  è anche iniettivo e sempre per il lemma del serpente  $\ker(g) = 0$ .  $\square$

OSSERVAZIONE 2.6.7. La definizione di gruppo Hopfiano si applica anche ai gruppi non abeliani. In tal caso è però falso che ogni gruppo non abeliano finitamente generato è Hopfiano.

TEOREMA 2.6.8 (Additività del rango). *Sia*

$$0 \rightarrow G_1 \xrightarrow{f} G_2 \xrightarrow{g} G_3 \rightarrow 0$$

*una successione esatta corta di gruppi abeliani finitamente generati. Allora*

$$\text{rank}(G_1) + \text{rank}(G_3) = \text{rank}(G_2).$$

DIMOSTRAZIONE. Proponiamo tre distinte dimostrazioni: due subito e la terza nella prossima sezione.

*Prima dimostrazione.* Abbiamo già dimostrato il teorema in due casi particolari, più precisamente:

- (1) se  $G_1, G_2$  e  $G_3$  sono senza torsione (Lemma 2.6.4);
- (2) se  $G_1, G_2$  sono senza torsione e  $G_3$  è un gruppo finito (Corollario 2.3.5).

Passiamo adesso al caso generale, dove per semplicità notazionale indichiamo  $T_i = T(G_i)$ . Abbiamo un diagramma commutativo con le righe esatte

$$\begin{array}{ccccccc} 0 & \longrightarrow & T_2 & \longrightarrow & G_2 & \longrightarrow & G_2/T_2 \longrightarrow 0 \\ & & \downarrow g_T & & \downarrow g & & \downarrow \bar{g} \\ 0 & \longrightarrow & T_3 & \longrightarrow & G_3 & \longrightarrow & G_3/T_3 \longrightarrow 0 \end{array}$$

Per definizione di rango si ha  $\text{rank}(G_i) = \text{rank}(G_i/T_i)$  e se denotiamo con  $H$  il nucleo di  $\bar{g}$  si ha

$$\text{rank}(H) = \text{rank}(G_2/T_2) - \text{rank}(G_3/T_3) = \text{rank}(G_2) - \text{rank}(G_3),$$

e rimane da dimostrare che  $G_1$  ha lo stesso rango di  $H$ . Identificando  $G_1$  con la sua immagine  $f(G_1)$  si ha  $G_1 = \ker(g)$ ,  $T_1 = G_1 \cap T_2 = \ker(g) \cap T_2 = \ker(g_T)$  e per il lemma del serpente abbiamo una successione esatta

$$0 \rightarrow T_1 \rightarrow G_1 \rightarrow H \rightarrow \text{coker}(g_T) \rightarrow 0$$

che si spezza in due successioni esatte corte

$$0 \rightarrow T_1 \rightarrow G_1 \rightarrow \frac{G_1}{T_1} \rightarrow 0, \quad 0 \rightarrow \frac{G_1}{T_1} \rightarrow H \rightarrow \text{coker}(g_T) \rightarrow 0.$$

Siccome  $\frac{G_1}{T_1}, H$  sono senza torsione e  $\text{coker}(g_T)$  è finito si ha

$$\text{rank}(G_1) = \text{rank}(G_1/T_1) = \text{rank}(H).$$

Si noti che in generale  $\text{coker}(g_T) \neq 0$  che equivale a dire  $G_1/T_1 \neq H$  che equivale a dire che

$$\frac{G_1}{T_1} \rightarrow \frac{G_2}{T_2} \rightarrow \frac{G_3}{T_3} \rightarrow 0$$

non è esatta.

*Seconda dimostrazione.* La seconda dimostrazione che proponiamo si basa sul seguente lemma.

LEMMA 2.6.9. *Sia  $G$  un gruppo abeliano finitamente generato di rango  $r$  e sia  $n = |T(G)|$  l'ordine del sottogruppo di torsione. Allora per ogni primo  $p > n$  l'omomorfismo di "moltiplicazione per  $p$ "*

$$p: G \rightarrow G, \quad p(x) = px,$$

*è iniettivo ed il suo conucleo è un gruppo finito di ordine  $p^r$ .*

DIMOSTRAZIONE. Per definizione di rango esiste una successione esatta corta  $0 \rightarrow T(G) \rightarrow G \rightarrow \mathbb{Z}^r \rightarrow 0$ . Se  $p > |T(G)|$  e  $x \in T(G)$ , allora l'ordine di  $x$  non divide  $p$  e quindi  $px \neq 0$ . Questo significa che l'omomorfismo  $p: T(G) \rightarrow T(G)$  è iniettivo, e siccome  $T(G)$  è un gruppo finito,  $p: T(G) \rightarrow T(G)$  è anche surgettivo. Viceversa l'omomorfismo  $p: \mathbb{Z}^r \rightarrow \mathbb{Z}^r$  è iniettivo ma non è surgettivo: più precisamente il suo conucleo è dato dalla somma diretta di  $\mathbb{Z}/(p)$  con se stesso  $r$  volte ed ha ordine  $p^r$ .

Applicando il lemma del serpente al diagramma

$$\begin{array}{ccccccccc} 0 & \longrightarrow & T(G) & \longrightarrow & G & \longrightarrow & \mathbb{Z}^r & \longrightarrow & 0 \\ & & p \downarrow \simeq & & p \downarrow & & p \downarrow & & \\ 0 & \longrightarrow & T(G) & \longrightarrow & G & \longrightarrow & \mathbb{Z}^r & \longrightarrow & 0 \end{array}$$

si deduce che le due frecce verticali a destra sono iniettive con il medesimo conucleo.  $\square$

Ritorniamo alla seconda dimostrazione dell'additività del rango. Sia  $p$  un numero primo sufficientemente grande, allora le tre frecce verticali del diagramma

$$\begin{array}{ccccccccc} 0 & \longrightarrow & G_1 & \longrightarrow & G_2 & \longrightarrow & G_3 & \longrightarrow & 0 \\ & & p \downarrow & & p \downarrow & & p \downarrow & & \\ 0 & \longrightarrow & G_1 & \longrightarrow & G_2 & \longrightarrow & G_3 & \longrightarrow & 0 \end{array}$$

sono iniettive ed il lemma del serpente fornisce una successione esatta corta di conuclei

$$0 \rightarrow (\mathbb{Z}/(p))^{r_1} \rightarrow (\mathbb{Z}/(p))^{r_2} \rightarrow (\mathbb{Z}/(p))^{r_3} \rightarrow 0$$

dove  $r_i$  è il rango di  $G_i$ . Per il Lemma 2.4.7 si ha  $p^{r_2} = p^{r_1} p^{r_3}$  che è del tutto equivalente a  $r_2 = r_1 + r_3$ .  $\square$

ESEMPIO 2.6.10. Sia

$$0 \rightarrow G_0 \xrightarrow{f_1} G_1 \xrightarrow{f_2} \dots \xrightarrow{f_n} G_n \rightarrow 0$$

una successione esatta finita di gruppi abeliani finitamente generati. Allora vale la formula

$$\sum_{i=0}^n \text{rank}(G_i) = 0.$$

Denotiamo, per ogni  $i = 2, \dots, n-1$  con  $K_i = f_i(G_{i-1}) = \ker(f_{i+1}) \subset G_i$ . Si hanno allora le successioni esatte corte

$$\begin{array}{ccccccc} 0 & \rightarrow & G_0 & \xrightarrow{f_1} & G_1 & \xrightarrow{f_2} & K_2 \rightarrow 0 \\ 0 & \rightarrow & K_2 & \longrightarrow & G_2 & \xrightarrow{f_3} & K_3 \rightarrow 0 \\ & & & & \dots & & \\ 0 & \rightarrow & K_{n-1} & \longrightarrow & G_{n-1} & \xrightarrow{f_n} & G_n \rightarrow 0 \end{array}$$

che per l'additività del rango inducono le uguaglianze

$$\begin{array}{l} \text{rank}(G_0) - \text{rank}(G_1) + \text{rank}(K_2) = 0 \\ -\text{rank}(K_2) + \text{rank}(G_2) - \text{rank}(K_3) = 0 \\ \dots \end{array}$$

$$(-1)^n (\text{rank}(K_{n-1}) - \text{rank}(G_{n-1}) + \text{rank}(G_n)) = 0$$

che sommate tra loro diventano  $\sum_{i=0}^n \text{rank}(G_i) = 0$ .

ESEMPIO 2.6.11. Si consideri un successione esatta corta di gruppi abeliani

$$0 \rightarrow T \xrightarrow{i} A \xrightarrow{g} B \rightarrow 0$$

con  $T$  gruppo di torsione. Allora si hanno una successione esatta

$$0 \rightarrow T \xrightarrow{i} T(A) \xrightarrow{g} T(B) \rightarrow 0$$

ed un isomorfismo  $A/T(A) \simeq B/T(B)$ .

Infatti, identificando  $T$  con la sua immagine  $f(T)$  si ha  $T \subset T(A)$  e quindi  $T$  coincide con il nucleo della restrizione  $g_T: T(A) \rightarrow T(B)$ . Il lemma del serpente applicato al diagramma

$$\begin{array}{ccccccccc} 0 & \longrightarrow & T(A) & \longrightarrow & A & \longrightarrow & A/T(A) & \longrightarrow & 0 \\ & & \downarrow g_T & & \downarrow g & & \downarrow \bar{g} & & \\ 0 & \longrightarrow & T(B) & \longrightarrow & B & \longrightarrow & B/T(B) & \longrightarrow & 0 \end{array}$$

dà un isomorfismo  $\ker(\bar{g}) \simeq \operatorname{coker}(g_T)$ . Ma  $\ker(\bar{g})$  è senza torsione mentre  $\operatorname{coker}(g_T)$  è di torsione e ciò è possibile solo se  $\ker(\bar{g}) = \operatorname{coker}(g_T) = 0$ , ossia solo se  $\bar{g}$  è un isomorfismo e  $g_T$  è surgettiva.

Data una matrice  $M$  a coefficienti interi, possiamo pensarla come una matrice a coefficienti razionali e considerarne il suo rango  $\operatorname{rank}(M)$ : ricordiamo dai corsi di algebra lineare che il esso può essere definito, tra le altre cose, come:

- (1) il massimo numero di colonne di  $M$  linearmente indipendenti su  $\mathbb{Q}$ ;
- (2) il massimo intero  $r$  tale che esiste una sottomatrice quadrata di ordine  $r$  con determinante diverso da 0.

LEMMA 2.6.12. *Sia  $L_M: \mathbb{Z}^m \rightarrow \mathbb{Z}^n$  l'omomorfismo indotto da una matrice  $M \in M_{n,m}(\mathbb{Z})$  tramite la solita regola del prodotto righe per colonne e sia  $r$  il rango di  $M$ , pensata come matrice a coefficienti razionali. Allora  $\ker L_M \simeq \mathbb{Z}^{m-r}$  e  $L_M(\mathbb{Z}^m) \simeq \mathbb{Z}^r$ . In particolare,  $\operatorname{rank}(\ker L_M) = m - r$  e  $\operatorname{rank}(\operatorname{Im}(L_M)) = r$ .*

DIMOSTRAZIONE. Indichiamo con  $G = L_M(\mathbb{Z}^m)$  l'immagine di  $M$ . Siccome  $G \subset \mathbb{Z}^n$  e  $\ker L_M \subset \mathbb{Z}^m$ , entrambi i gruppi sono finitamente generati e senza torsione, dunque  $\ker L_M \simeq \mathbb{Z}^p$ ,  $G \simeq \mathbb{Z}^q$  per opportuni interi  $p, q$  tali che  $p + q = m$ ; ci basta quindi dimostrare che  $q = r$ .

Siano  $e_1, \dots, e_m \in \mathbb{Z}^m \subset \mathbb{Q}^m$  i vettori della base canonica. A meno di permutazioni possiamo supporre che  $L_M(e_1), \dots, L_M(e_r)$  siano linearmente indipendenti in  $\mathbb{Q}^n$ . Siccome  $r = \operatorname{rank}(M)$  si ha che  $L_M(\mathbb{Q}^m) = \operatorname{Span}(L_M(e_1), \dots, L_M(e_r))$  e quindi per ogni  $x \in G$  esistono  $a_1, \dots, a_r \in \mathbb{Q}$  tali che  $x = \sum_{i=1}^r a_i L_M(e_i)$ . Equivalentemente, per ogni  $x \in G$  esistono interi  $d > 0$  (il denominatore comune degli  $a_i$ ) e  $b_1, \dots, b_r \in \mathbb{Z}$  tali che  $nx = \sum_{i=1}^r b_i L_M(e_i)$ .

Ne segue che l'applicazione

$$f: \mathbb{Z}^r \rightarrow G, \quad f(b_1, \dots, b_r) = \sum b_i L_M(e_i),$$

è iniettiva e per ogni  $x \in G$  esiste un intero  $n > 0$  tale che  $nx$  appartiene all'immagine di  $f$ . In conclusione il conucleo di  $f$  è di torsione e per l'additività del rango  $q = r$ .  $\square$

TEOREMA 2.6.13 (Teorema del rango). *Siano dati due omomorfismi di gruppi  $\mathbb{Z}^m \xrightarrow{L_M} \mathbb{Z}^n \xrightarrow{L_N} \mathbb{Z}^p$  definiti da due matrici  $M \in M_{n,m}(\mathbb{Z})$ ,  $N \in M_{p,n}(\mathbb{Z})$  e tali che  $NM = 0$ , ossia tali che  $\operatorname{Im}(L_M) \subset \ker(L_N)$ . Allora vale la formula*

$$\operatorname{rank} \frac{\ker L_N}{\operatorname{Im}(L_M)} = n - \operatorname{rank}(M) - \operatorname{rank}(N).$$

DIMOSTRAZIONE. Per il Lemma 2.6.12 il gruppo abeliano  $\operatorname{Im}(L_M)$  ha rango  $\operatorname{rank}(M)$  ed il gruppo abeliano  $\ker(L_N)$  ha rango  $n - \operatorname{rank}(N)$ . Per concludere basta applicare il teorema di additività del rango alla successione esatta corta

$$0 \rightarrow \operatorname{Im}(M) \rightarrow \ker(N) \rightarrow \frac{\ker N}{\operatorname{Im}(M)} \rightarrow 0.$$

$\square$

**Esercizi:**

ESERCIZIO 17. Si consideri il seguente diagramma commutativo di gruppi abeliani:

$$\begin{array}{ccccccc}
 & & 0 & & 0 & & 0 \\
 & & \downarrow & & \downarrow & & \downarrow \\
 0 & \longrightarrow & N_1 & \longrightarrow & M_1 & \longrightarrow & P_1 \longrightarrow 0 \\
 & & \downarrow & & \downarrow & & \downarrow \\
 0 & \longrightarrow & N_2 & \xrightarrow{f} & M_2 & \xrightarrow{g} & P_2 \longrightarrow 0 \\
 & & \downarrow & & \downarrow & & \downarrow \\
 0 & \longrightarrow & N_3 & \longrightarrow & M_3 & \longrightarrow & P_3 \longrightarrow 0 \\
 & & \downarrow & & \downarrow & & \downarrow \\
 & & 0 & & 0 & & 0
 \end{array}$$

Si assuma che le colonne siano esatte e che  $gf = 0$ . Provare che ogni riga è un complesso e che se due righe sono esatte allora è esatta anche la terza.

**2.7. Razionalizzazione di gruppi abeliani**

Imitando la costruzione che dagli interi porta ai razionali è possibile assegnare in maniera naturale ad ogni gruppo abeliano  $G$  uno spazio vettoriale su  $\mathbb{Q}$ , che viene denotato, a seconda delle circostanze, con  $G_{\mathbb{Q}}$  oppure con  $G \otimes \mathbb{Q}$ .

Denotiamo con  $\mathbb{Z}^*$  l'insieme dei numeri interi diversi da 0. Dato un gruppo abeliano  $G$  consideriamo la relazione di equivalenza  $\sim$  sull'insieme  $G \times \mathbb{Z}^*$  definita come

$$(x, n) \sim (y, m) \text{ se esistono } a, b \in \mathbb{Z}^* \text{ tali che } (ax, an) = (by, bm).$$

Per mostrare che  $\sim$  è una relazione di equivalenza, l'unica verifica non banale è la transitività: se  $(x, n) \sim (y, m)$  e  $(y, m) \sim (z, l)$  e  $a, b, c, d \in \mathbb{Z}^*$  sono tali che  $(ax, an) = (by, bm)$  e  $(cy, cm) = (dz, dl)$ , allora  $(acx, acn) = (bdz, bdl)$ .

Per agevolare le prossime verifiche di buona definizione è utile osservare che  $\sim$  è la più piccola relazione di equivalenza per cui  $(x, n) \sim (ax, an)$  per ogni  $a \in \mathbb{Z}^*$ .

Denotiamo con  $G_{\mathbb{Q}}$  l'insieme quoziente e con  $\frac{x}{n} \in G_{\mathbb{Q}}$  la classe di equivalenza di  $(x, n)$ . Notiamo che per ogni  $x \in G$  ed ogni  $a, n \in \mathbb{Z}^*$  si ha  $\frac{x}{n} = \frac{ax}{an}$ .  $G_{\mathbb{Q}}$  ha una struttura di gruppo abeliano, dove la somma è data da

$$\frac{x}{n} + \frac{y}{m} = \frac{mx + ny}{nm}.$$

L'elemento neutro è  $\frac{0}{1}$ , mentre l'opposto è  $-\frac{a}{n} = \frac{-a}{n}$ . Lasciamo al lettore il semplice compito di verificare che la somma è ben definita e definisce una struttura di gruppo abeliano. È utile osservare che  $\frac{0}{n} = \frac{0}{1}$  per ogni  $n \in \mathbb{Z}^*$ .

LEMMA 2.7.1. Per ogni gruppo abeliano  $G$ , l'applicazione  $G \rightarrow G_{\mathbb{Q}}$ ,  $x \mapsto \frac{x}{1}$  è un omomorfismo di gruppi il cui nucleo è il sottogruppo di torsione  $T(G)$ .

DIMOSTRAZIONE. La verifica che si tratta di un omomorfismo è immediata. Un elemento  $x \in G$  appartiene al nucleo se e solo se  $\frac{x}{1} = \frac{0}{1}$  in  $G_{\mathbb{Q}}$ , se e solo se esistono  $a, b \in \mathbb{Z}^*$  tali che  $(ax, a) = (b0, b)$ , se e solo se esiste  $a \in \mathbb{Z}^*$  tali che  $ax = 0$ , se e solo se  $x$  è di torsione.  $\square$

Il gruppo abeliano  $G_{\mathbb{Q}}$  possiede in aggiunta una struttura di spazio vettoriale su  $\mathbb{Q}$ , dove il prodotto per scalare è definito come

$$\frac{a}{b} \cdot \frac{x}{n} = \frac{ax}{bn}, \quad a \in \mathbb{Z}, b, n \in \mathbb{Z}^*, x \in G.$$

Chiameremo lo spazio vettoriale  $G_{\mathbb{Q}}$  la **razionalizzazione** di  $G$ .

ESEMPIO 2.7.2. Se  $G = T(G)$  è un gruppo di torsione, allora  $G_{\mathbb{Q}} = 0$ . Infatti per ogni  $x \in G$  esiste  $m \in \mathbb{Z}^*$  tale che  $mx = 0$  e quindi per ogni  $n \in \mathbb{Z}^*$  si ha  $(x, n) \sim (0, 1)$  in quanto  $(m \cdot x, m \cdot n) = (mn \cdot 0, mn \cdot 1)$ .

ESEMPIO 2.7.3. Sia  $G \simeq \mathbb{Z}^n$  un gruppo abeliano libero di rango  $n$ , allora  $G_{\mathbb{Q}}$  ha dimensione  $n$  come spazio vettoriale. Più precisamente, se  $e_1, \dots, e_n$  è una base di  $G$  come gruppo abeliano libero, allora  $\frac{e_1}{1}, \dots, \frac{e_n}{1}$  è una base di  $G_{\mathbb{Q}}$  come spazio vettoriale.

Vediamo prima che i vettori  $\frac{e_i}{1}$  sono linearmente indipendenti: se  $\sum_i a_i \frac{e_i}{1} = 0$  per opportuni  $a_1, \dots, a_n \in \mathbb{Q}$ , moltiplicando per un denominatore comune possiamo supporre  $a_i \in \mathbb{Z}$  e quindi

$$\sum_i a_i \frac{e_i}{1} = \sum_i \frac{a_i e_i}{1} = \frac{\sum_i a_i e_i}{1} = 0$$

e questo equivale a dire che  $\sum_i a_i e_i$  appartiene al sottogruppo di torsione, che essendo nullo implica  $\sum_i a_i e_i = 0$  e quindi  $a_i = 0$  per ogni  $i$ .

Per mostrare che generano, sia  $\frac{x}{n} \in G_{\mathbb{Q}}$ ; allora esistono  $a_1, \dots, a_n \in \mathbb{Z}$  tali che  $\sum_i a_i e_i = x$  e quindi

$$\frac{x}{n} = \sum_i \frac{a_i e_i}{n}.$$

Ogni omomorfismo di gruppi  $f: G \rightarrow H$  determina un'applicazione lineare

$$f_{\mathbb{Q}}: G_{\mathbb{Q}} \rightarrow H_{\mathbb{Q}}, \quad f_{\mathbb{Q}}\left(\frac{x}{n}\right) = \frac{f(x)}{n}.$$

Tale assegnazione commuta con la composizione e preserva le identità ed i morfismi nulli, ossia  $(fg)_{\mathbb{Q}} = f_{\mathbb{Q}}g_{\mathbb{Q}}$ , che  $\text{Id}_{\mathbb{Q}} = \text{Id}$  e  $0_{\mathbb{Q}} = 0$ .

TEOREMA 2.7.4. *La razionalizzazione trasforma successioni esatte in successioni esatte.*

DIMOSTRAZIONE. Vogliamo dimostrare che se  $G \xrightarrow{f} H \xrightarrow{g} K$  è una successione esatta di gruppi abeliani, allora anche la successione  $G_{\mathbb{Q}} \xrightarrow{f_{\mathbb{Q}}} H_{\mathbb{Q}} \xrightarrow{g_{\mathbb{Q}}} K_{\mathbb{Q}}$  è esatta. Siccome  $gf = 0$  vale anche  $g_{\mathbb{Q}}f_{\mathbb{Q}} = (gf)_{\mathbb{Q}} = 0$ . Sia  $\frac{x}{n} \in \ker(g_{\mathbb{Q}})$ , allora  $(g(x), n) \sim (0, 1)$  e quindi esiste  $a \in \mathbb{Z}^*$  tale che  $ag(x) = g(ax) = 0$ . Ma allora esiste  $y \in G$  tale che  $f(y) = ax$  e dunque  $f_{\mathbb{Q}}\left(\frac{y}{an}\right) = \frac{ax}{an} = \frac{x}{n}$ .  $\square$

COROLLARIO 2.7.5. *Se  $G$  è un gruppo abeliano finitamente generato, allora  $\text{rank}(G) = \dim_{\mathbb{Q}} G_{\mathbb{Q}}$ .*

DIMOSTRAZIONE. Basta applicare il Teorema 2.7.4 alla successione esatta

$$0 \rightarrow T(G) \rightarrow G \rightarrow G/T(G) \cong \mathbb{Z}^{\text{rank}(G)} \rightarrow 0$$

e usare i due esempi precedenti.  $\square$

*Terza dimostrazione dell'aditività del rango.* Sia  $0 \rightarrow G \rightarrow H \rightarrow K \rightarrow 0$  una successione esatta di gruppi abeliani finitamente generati. Allora  $0 \rightarrow G_{\mathbb{Q}} \rightarrow H_{\mathbb{Q}} \rightarrow K_{\mathbb{Q}} \rightarrow 0$  è una successione esatta di spazi vettoriali e per il teorema del rango (visto ad Algebra Lineare) si ha  $\dim H_{\mathbb{Q}} = \dim G_{\mathbb{Q}} + \dim K_{\mathbb{Q}}$ . Basta adesso applicare il Corollario 2.7.5.

## 2.8. Complessi di catene e omologia

Iniziamo con la definizione di complesso di catene di gruppi abeliani, dove il termine *catene* specifica una ben definita convenzione sugli indici, che sono interi ed in ordine decrescente.

DEFINIZIONE 2.8.1. Un complesso di catene di gruppi abeliani è una successione  $\{C_n\}_{n \in \mathbb{Z}}$  di gruppi abeliani insieme a degli omomorfismi  $d = d_n: C_n \rightarrow C_{n-1}$  detti **differenziali**, tali che  $d \circ d: C_n \rightarrow C_{n-2}$  risulti essere il morfismo nullo.

$$\cdots \xrightarrow{d_{n+1}} C_{n+1} \xrightarrow{d_n} C_n \xrightarrow{d_{n-1}} C_{n-1} \xrightarrow{d_{n-2}} C_{n-2} \cdots$$

Per semplicità parleremo semplicemente di complessi omettendo il termine catene. Si noti che nei complessi di catene il differenziale abbassa gli indici a pedice di 1. Per semplicità notazionale denoteremo spesso un complesso  $\{C_n, d_n\}_{n \in \mathbb{Z}}$  con  $(C, d)$  lasciando gli indici sottintesi, o più semplicemente con  $C$ , sottintendendo anche i differenziali.

DEFINIZIONE 2.8.2. Un morfismo di complessi  $f: (C, d) \rightarrow (D, \delta)$  è una successione di omomorfismi di gruppi  $\{f_n: C_n \rightarrow D_n\}_{n \in \mathbb{Z}}$  che commutano coi differenziali  $d$ , ossia per ogni intero  $n$  vale l'uguaglianza  $f_{n-1} \circ d_n = \delta_n \circ f_n$  così da rendere commutativo il seguente diagramma:

$$\begin{array}{ccccccc} \cdots & \longrightarrow & C_n & \xrightarrow{d_n} & C_{n-1} & \longrightarrow & \cdots \\ & & \downarrow f_n & & \downarrow f_{n-1} & & \\ \cdots & \longrightarrow & D_n & \xrightarrow{\delta_n} & D_{n-1} & \longrightarrow & \cdots \end{array}$$

Diremo inoltre che un morfismo di complessi  $f: C \rightarrow D$  è un isomorfismo (resp.: iniettivo, surgettivo) se  $f_n: C_n \rightarrow D_n$  è un isomorfismo (resp.: iniettivo, surgettivo) per ogni  $n$ .

DEFINIZIONE 2.8.3. Dato un complesso  $(C, d)$  possiamo definire:

- i **cicli** come gli elementi nei nuclei dei differenziali; per ogni  $n$  il nucleo  $Z_n(C) := \ker(d_n) \subseteq C_n$  è detto gruppo degli  $n$ -cicli;
- i **bordi** come gli elementi immagine dei differenziali; per ogni  $n$  definiamo il gruppo degli  $n$ -bordi  $B_n(C) := d_{n+1}(C_{n+1}) \subseteq C_n$ .

Osserviamo inoltre che la proprietà dei differenziali  $d \circ d = 0$  implica in particolar modo l'inclusione  $B_n(C) \subseteq Z_n(C)$  ed è quindi possibile considerare il quoziente tra cicli e bordi.

DEFINIZIONE 2.8.4. Definiamo l' $n$ -esimo gruppo di omologia come il quoziente:

$$H_n(C) := \frac{Z_n(C)}{B_n(C)}.$$

Diremo che il complesso  $C$  è **aciclico** se  $H_n(C) = 0$  per ogni  $n$ : ciò equivale a dire che il complesso  $C$  è una successione esatta.

OSSERVAZIONE 2.8.5. Dato un complesso  $C$ , la condizione  $d^2 = 0$  (ossia  $d_n d_{n+1} = 0$  per ogni  $n$ ) implica che per ogni  $n$  il differenziale  $d_n: C_n \rightarrow C_{n-1}$  si fattorizza ad un omomorfismo

$$\frac{C_n}{B_n(C)} \xrightarrow{\bar{d}_n} Z_{n-1}(C)$$

e si verifica immediatamente che  $\ker \bar{d}_n = H_n(C)$ ,  $\text{coker } \bar{d}_n = H_{n-1}(C)$ .

Una verifica diretta mostra che un morfismo di complessi  $f: A \rightarrow B$  porta cicli in cicli e bordi in bordi, di conseguenza risultano ben definiti a livello di omologia gli omomorfismi  $f: H_n(A) \rightarrow H_n(B)$ .

DEFINIZIONE 2.8.6. Un morfismo di complessi  $f: A \rightarrow B$  è detto un **quasi-isomorfismo** se per ogni  $n$  le applicazioni  $f_n: H_n(A) \rightarrow H_n(B)$  sono isomorfismi.

Ogni isomorfismo di complessi è anche un quasi-isomorfismo, mentre il viceversa è generalmente falso.

DEFINIZIONE 2.8.7. Sia  $C = \{\cdots C_n \xrightarrow{d} C_{n-1} \cdots\}$  un complesso. Un **sottocomplesso**  $D \subseteq C$  è il dato di una successione di sottogruppi  $D_n \subseteq C_n$  tali che  $d(D_n) \subseteq D_{n-1}$  per ogni  $n$ .

Se  $D \subseteq C$  è un sottocomplesso, l'inclusione  $D \rightarrow C$  è un morfismo iniettivo di complessi. Bisogna fare **attenzione** al fatto che in generale i morfismi indotti in omologia  $H_n(D) \rightarrow H_n(C)$  **non sono** iniettivi in generale. Similmente se  $D \rightarrow E$  è un morfismo surgettivo di complessi, allora non è detto che i morfismi  $H_n(D) \rightarrow H_n(E)$  siano surgettivi (vedi Esempio 2.8.10).

ESEMPIO 2.8.8. Sia  $D$  un sottocomplesso di un complesso di catene  $C$ . Se per qualche intero  $n$  si ha che  $D_i = C_i$  per  $i = n-1, n, n+1$ , allora l'inclusione  $D \subset C$  induce un isomorfismo  $H_n(D) \rightarrow H_n(C)$ : infatti  $H_n(C)$  dipende solo dal segmento  $C_{n+1} \xrightarrow{d} C_n \xrightarrow{d} C_{n-1}$  che coincide con il corrispondente segmento del sottocomplesso  $D$ .

DEFINIZIONE 2.8.9. Un diagramma di morfismi di complessi

$$0 \rightarrow C \xrightarrow{f} D \xrightarrow{g} E \rightarrow 0$$

si dice una **successione esatta corta** di complessi se per ogni  $n$  si ha che

$$0 \rightarrow C_n \xrightarrow{f_n} D_n \xrightarrow{g_n} E_n \rightarrow 0$$

è una successione esatta corta di gruppi abeliani.

ESEMPIO 2.8.10. Possiamo interpretare il diagramma commutativo

$$\begin{array}{ccccccc} 0 & \longrightarrow & 0 & \longrightarrow & \mathbb{Z} & \xrightarrow{\text{Id}} & \mathbb{Z} & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & \text{Id} & \downarrow & & \\ 0 & \longrightarrow & \mathbb{Z} & \xrightarrow{\text{Id}} & \mathbb{Z} & \longrightarrow & 0 & \longrightarrow & 0 \end{array}$$

come una successione esatta corta di complessi  $0 \rightarrow C \xrightarrow{f} D \xrightarrow{g} E \rightarrow 0$  concentrati nei gradi 0, 1, ossia  $C_n = D_n = E_n = 0$  per ogni  $n$  eccetto  $C_0 = D_0 = D_1 = E_1 = \mathbb{Z}$ . Si noti che  $D$  è aciclico, mentre  $H_0(C) = H_1(E) = \mathbb{Z}$ ; in particolare  $H_0(C) \rightarrow H_0(D)$  non è iniettiva e  $H_1(D) \rightarrow H_1(E)$  non è surgettiva.

ESEMPIO 2.8.11. Dato il diagramma commutativo di gruppi abeliani

$$\begin{array}{ccccccc} 0 & \longrightarrow & A & \xrightarrow{f} & B & \xrightarrow{p} & D & \longrightarrow & 0 \\ & & \downarrow \alpha & & \downarrow \beta & & \downarrow \gamma & & \\ 0 & \longrightarrow & L & \xrightarrow{g} & M & \xrightarrow{q} & N & \longrightarrow & 0 \end{array}$$

con le righe esatte e le frecce verticali surgettive, consideriamo il complesso di catene

$$C: \quad 0 \rightarrow A \xrightarrow{(f, \alpha)} B \oplus L \xrightarrow{\beta - g} M \rightarrow 0$$

dove  $A = C_1$  si considera in grado 1 (e quindi  $C_0 = B \oplus L$  in grado 0 e  $C_{-1} = M$  in grado  $-1$ ),  $(f, \alpha)a = (f(a), \alpha(a))$  e  $(\beta - g)(b, l) = \beta(b) - g(l)$ . Siccome  $f$  è iniettiva e  $\beta$  è surgettiva, a maggior ragione  $(f, \alpha)$  è iniettiva e  $\beta - g$  è surgettiva: in altri termini  $H_1(C) = H_{-1}(C) = 0$ .

Vogliamo mostrare che esiste un isomorfismo naturale  $H_0(C) \cong \ker \gamma$ . Consideriamo l'omomorfismo

$$\varphi: C_0 = B \oplus L \rightarrow D, \quad \varphi(b, l) = p(b).$$

Se  $(b, l) \in Z_0(C)$  allora  $\beta(b) = g(l)$  e

$$\gamma\varphi(b, l) = \gamma p(b) = q\beta(b) = qg(l) = 0.$$

Dunque  $\varphi$  si restringe ad un omomorfismo di gruppi  $\varphi: Z_0(C) \rightarrow \ker \gamma$  che vogliamo dimostrare essere surgettivo. Dato  $d \in \ker \gamma$ , esiste  $b \in B$  tale che  $p(b) = d$ ; inoltre  $q\beta(b) = \gamma p(b) = \gamma(d) = 0$  e per l'esattezza della seconda riga si deduce che esiste  $l \in L$  tale che  $\beta(b) = g(l)$ . Dunque  $(b, l) \in Z_0(C)$  e  $\varphi(b, l) = d$ .

Per dimostrare che  $H_0(C) \cong \ker \gamma$  basta dimostrare che il nucleo di  $\varphi: Z_0(C) \rightarrow \ker \gamma$  è esattamente  $B_0(C)$ . Dato  $(b, l) \in Z_0(C)$  tale che  $\varphi(b, l) = p(b) = 0$ , per l'esattezza della prima riga esiste  $a \in A$  tale che  $b = f(a)$ . Ma allora  $g(l) = \beta(b) = \beta f(a) = g\alpha(a)$  e per l'iniettività di  $g$  si deduce  $(b, l) = (f, \alpha)a \in B_0(C)$ .

TEOREMA 2.8.12. *Data una successione esatta corta di complessi*

$$0 \rightarrow C \xrightarrow{f} D \xrightarrow{g} E \rightarrow 0$$

sono canonicamente definiti degli omomorfismi  $\partial_n: H_n(E) \rightarrow H_{n-1}(C)$  tali che si ottenga la successione esatta (infinita):

$$(2.4) \quad \cdots \rightarrow H_n(C) \xrightarrow{f} H_n(D) \xrightarrow{g} H_n(E) \xrightarrow{\partial_n} H_{n-1}(C) \xrightarrow{f} H_{n-1}(D) \rightarrow \cdots$$

detta in gergo successione esatta lunga di omologia.

DIMOSTRAZIONE. La dimostrazione si ottiene mediante un uso ripetuto del lemma del serpente. Per semplicità notazionale indichiamo con il medesimo simbolo  $d$  i differenziali dei tre complessi. Per ogni intero  $n$  si ha un diagramma commutativo con le righe esatte

$$\begin{array}{ccccccccc} 0 & \longrightarrow & C_n & \longrightarrow & D_n & \longrightarrow & E_n & \longrightarrow & 0 \\ & & \downarrow d & & \downarrow d & & \downarrow d & & \\ 0 & \longrightarrow & C_{n-1} & \longrightarrow & D_{n-1} & \longrightarrow & E_{n-1} & \longrightarrow & 0 \end{array}$$

che per il lemma del serpente ci fornisce, per ogni  $n \in \mathbb{Z}$ , una successione esatta

$$0 \rightarrow Z_n(C) \rightarrow Z_n(D) \rightarrow Z_n(E) \rightarrow \frac{C_{n-1}}{B_{n-1}(C)} \rightarrow \frac{D_{n-1}}{B_{n-1}(D)} \rightarrow \frac{E_{n-1}}{B_{n-1}(E)} \rightarrow 0.$$

Poiché il differenziale  $d: C_n \rightarrow C_{n-1}$  si fattorizza ad un omomorfismo  $\bar{d}: \frac{C_n}{B_n(C)} \rightarrow Z_{n-1}(C)$  i cui nucleo e conucleo sono rispettivamente  $H_n(C)$  e  $H_{n-1}(C)$  (idem per i complessi  $D, E$ ), per ogni  $n$  si ha un diagramma commutativo con le righe esatte

$$\begin{array}{ccccccccc} \frac{C_n}{B_n(C)} & \longrightarrow & \frac{D_n}{B_n(D)} & \longrightarrow & \frac{E_n}{B_n(E)} & \longrightarrow & 0 \\ & & \downarrow \bar{d} & & \downarrow \bar{d} & & \downarrow \bar{d} & & \\ 0 & \longrightarrow & Z_{n-1}(C) & \longrightarrow & Z_{n-1}(D) & \longrightarrow & Z_{n-1}(E) & \longrightarrow & 0 \end{array}$$

che per l'Osservazione 2.8.5 ed il lemma del serpente ci fornisce, per ogni  $n$ , una successione esatta

$$H_n(C) \rightarrow H_n(D) \rightarrow H_n(E) \rightarrow H_{n-1}(C) \rightarrow H_{n-1}(D) \rightarrow H_{n-1}(E).$$

Mettendo assieme tutte queste successioni esatte si ottiene la successione esatta lunga di omologia.  $\square$

COROLLARIO 2.8.13. *Sia*

$$0 \rightarrow C \xrightarrow{f} D \xrightarrow{g} E \rightarrow 0$$

*una successione esatta corta di complessi. Allora  $f$  è un quasi-isomorfismo se e solo se  $E$  è aciclico.*

DIMOSTRAZIONE. Consideriamo la successione esatta lunga di omologia

$$\cdots \rightarrow H_{n+1}(E) \rightarrow H_n(C) \xrightarrow{f} H_n(D) \xrightarrow{g} H_n(E) \xrightarrow{\partial_n} H_{n-1}(C) \xrightarrow{f} H_{n-1}(D) \rightarrow \cdots$$

Se  $E$  è aciclico allora per ogni  $n$  si ha  $H_{n+1}(E) = H_n(E) = 0$  e dall'esattezza della successione si deduce che  $H_n(C) \xrightarrow{f} H_n(D)$  è iniettiva e surgettiva. Viceversa, se  $f$  è un quasi-isomorfismo allora per ogni  $n$  il morfismo  $H_n(C) \xrightarrow{f} H_n(D)$  è surgettivo ed il morfismo  $H_{n-1}(C) \xrightarrow{f} H_{n-1}(D)$  è iniettivo. L'esattezza della successione implica allora che  $H_n(E) = 0$ .  $\square$

DEFINIZIONE 2.8.14. Dati due complessi di catene  $C, D$ , una **omotopia** da  $C$  a  $D$ , scritta  $h: C \rightarrow D[1]$ , è una successione  $h = \{h_n\}$  di omomorfismi di gruppi

$$h_n: C_n \rightarrow D_{n+1}.$$

Nella definizione di omotopia non si richiede alcuna regola di commutazione con i differenziali il simbolo  $[1]$  viene messo per indicare che gli omomorfismi dell'omotopia aumentano gli indici di 1.

DEFINIZIONE 2.8.15. Una **contrazione** di un complesso di catene  $(C, d)$  è una omotopia  $h: C \rightarrow C[1]$  tale che  $dh + hd = \text{Id}$ : con ciò intendiamo che se  $h = \{h_n\}$ , allora per ogni  $n$  vale

$$d_{n+1}h_n + h_{n-1}d_n = \text{Id}_C: C_n \rightarrow C_n.$$

Un complesso che possiede una contrazione si dice **contraibile**.

LEMMA 2.8.16. *Ogni complesso contraibile è aciclico.*

DIMOSTRAZIONE. Sia  $C$  un complesso che possiede una contrazione  $h: C \rightarrow C[1]$  e sia  $x \in Z_n(C)$ . Allora, siccome  $d(x) = 0$  a maggior ragione  $hd(x) = 0$  e quindi

$$x = \text{Id}(x) = dh(x) + hd(x) = dh(x) \in B_n(C).$$

□

È generalmente falso che i complessi aciclici sono contraibili: ad esempio il complesso

$$0 \rightarrow \mathbb{Z} \xrightarrow{\cdot 2} \mathbb{Z} \xrightarrow{d} \mathbb{Z}/2 \rightarrow 0$$

è aciclico ma non è contraibile. Infatti  $\mathbb{Z}/2$  è di torsione, mentre  $\mathbb{Z}$  è senza torsione e poiché ogni omomorfismo manda elementi di torsione in elementi di torsione, non esiste alcun omomorfismo  $h: \mathbb{Z}/2 \rightarrow \mathbb{Z}$  tale che  $dh$  sia l'identità.

DEFINIZIONE 2.8.17. Due morfismi di complessi  $f, g: (C, d) \rightarrow (D, \delta)$  si dicono **omotopi** se esiste un'omotopia  $h: C \rightarrow D[1]$  tale che

$$f - g = \delta h + hd, \text{ ossia } f_n - g_n = \delta_{n+1}h_n + h_{n-1}d_n \quad \forall n.$$

$$\begin{array}{ccccccc} \cdots & \longrightarrow & C_{n+1} & \xrightarrow{d} & C_n & \xrightarrow{d} & C_{n-1} & \longrightarrow & \cdots \\ & & \downarrow f-g & \swarrow h & \downarrow f-g & \swarrow h & \downarrow f & & \\ \cdots & \longrightarrow & D_{n+1} & \xrightarrow{\delta} & D_n & \xrightarrow{\delta} & D_{n-1} & \longrightarrow & \cdots \end{array}$$

In particolare un complesso  $C$  è contraibile se e solo se  $\text{Id}_C$  è omotopa all'applicazione nulla.

OSSERVAZIONE 2.8.18. L'omotopia sopra definita è una relazione di equivalenza e per indicare che  $f, g$  sono omotope scriveremo  $f \sim g$ . Infatti, prendendo  $h = 0$  si ottiene  $f \sim f$ ; se  $f - g = \delta h + hd$  allora ponendo  $k_n = -h_n$  per ogni  $n$  si ha  $g - f = \delta k + kd$ ; se  $f - g = \delta h + hd$  e  $g - l = \delta k + kd$ , allora  $f - l = \delta(h + k) + (h + k)d$ .

LEMMA 2.8.19. Due morfismi di complessi  $f, g: C \rightarrow D$  omotopi,  $f \sim g$ , inducono gli stessi morfismi in omologia  $f = g: H_n(C) \rightarrow H_n(D)$ , per ogni  $n$ .

DIMOSTRAZIONE. Bisogna dimostrare che se  $f \sim g$  e  $x \in Z_n(C)$ , allora  $f(x) - g(x) \in B_n(D)$ . Siccome  $dx = 0$  si ha

$$f(x) - g(x) = \delta h(x) + hd(x) = \delta h(x) \in \delta(D_{n+1}) = B_n(D).$$

□

DEFINIZIONE 2.8.20. Un morfismo di complessi  $f: C \rightarrow D$  si dice un'**equivalenza omotopica** se esiste un morfismo di complessi  $g: D \rightarrow C$  tale che la composizione  $gf: C \rightarrow C$  è omotopa all'identità  $\text{Id}_C$  e  $fg: D \rightarrow D$  è omotopa all'identità  $\text{Id}_D$ :

$$C \text{ omotopo a } D \iff fg \sim \text{Id}_D, \quad gf \sim \text{Id}_C.$$

LEMMA 2.8.21. Le equivalenze omotopiche sono quasi-isomorfismi.

DIMOSTRAZIONE. Sia  $f: C \rightarrow D$  un'equivalenza omotopica. Per definizione esiste un morfismo di complessi  $g: D \rightarrow C$  tale che  $gf \sim \text{Id}_C$  e  $fg \sim \text{Id}_D$ . Per ogni  $n$  abbiamo un diagramma commutativo

$$\begin{array}{ccc} H_n(C) & \xrightarrow{f} & H_n(D) \\ gf \downarrow & \swarrow g & \downarrow fg \\ H_n(C) & \xrightarrow{f} & H_n(D) \end{array}$$

e per il lemma precedente le due frecce verticali sono le identità. Dunque, in omologia,  $f$  e  $g$  sono isomorfismi ed uno l'inverso dell'altro. □

**Esercizi:**

ESERCIZIO 18. Sia  $f: C \rightarrow D$  è un quasi-isomorfismo di complessi con  $f_n: C_n \rightarrow D_n$  surgettivo per ogni  $n$ . Dimostrare che  $f_n: Z_n(C) \rightarrow Z_n(D)$  è surgettivo per ogni  $n$ .

ESERCIZIO 19. Sia

$$0 \rightarrow C \xrightarrow{f} D \xrightarrow{g} E \rightarrow 0$$

una successione esatta corta di complessi. Provare che  $g$  è un quasi-isomorfismo se e solo se  $C$  è aciclico.

ESERCIZIO 20. Sia  $C$  un complesso di catene di gruppi abeliani finitamente generati. Si assuma che  $2x = 0$  per ogni  $n$  ed ogni  $x \in C_n$ . Dimostrare che  $C$  è aciclico se e solo se è contraibile.



## Omologia simpliciale

### 3.1. Omologia dei complessi simpliciali astratti

DEFINIZIONE 3.1.1. Siano  $(K, I)$  un complesso simpliciale astratto e  $p \geq 0$  un intero. Un  **$p$ -simpleso orientato** di  $K$  è un'applicazione di insiemi  $x: \{0, 1, \dots, p\} \rightarrow I$  la cui immagine appartiene a  $K$ . Denoteremo  $K_p$  l'insieme dei  $p$ -simplessi orientati di  $K$ .

Dato che ogni applicazione  $x: \{0, 1, \dots, p\} \rightarrow I$  la possiamo rappresentare mediante una  $(p+1)$ -upla  $(x_0, \dots, x_p)$  di elementi di  $I$  (dove  $x_i$  è l'immagine di  $i$  tramite  $x$ ), possiamo scrivere

$$K_p = \{(x_0, \dots, x_p) \in I^{p+1} \mid \{x_0, \dots, x_p\} \in K\}.$$

Osserviamo che, poiché sono ammesse ripetizioni,  $K_p$  è non vuoto per ogni  $p$ , anche nel caso in cui  $K$  è un complesso finito. Ad esempio, per ogni  $a \in I$  si ha  $(a, \dots, a) \in K_p$  per ogni  $p$ .

Se  $f: \{0, \dots, q\} \rightarrow \{0, \dots, p\}$  è una qualunque applicazione, dato  $x \in K_p$  possiamo considerare la sua composizione con  $f$  ed ottenere un nuovo simpleso orientato  $f^*x \in K_q$ :

$$f^*x := x \circ f: \{0, 1, \dots, q\} \rightarrow I.$$

Poiché l'immagine di  $f^*x$  è contenuta nell'immagine di  $x$ , si ha che l'immagine di  $f^*x$  è un elemento di  $K$ . Equivalentemente possiamo definire  $f^*$  come

$$f^*(x_0, \dots, x_p) = (x_{f(0)}, \dots, x_{f(p)}).$$

Ad esempio, se consideriamo le applicazioni

$$\delta_i: \{0, \dots, p-1\} \rightarrow \{0, \dots, p\}, \quad 0 \leq i \leq p, \quad \delta_i(j) = \begin{cases} j & \text{se } j < i, \\ j+1 & \text{se } j \geq i \end{cases},$$

allora

$$\delta_i^*(x_0, \dots, x_p) = (x_0, \dots, \hat{x}_i, \dots, x_p) = (x_0, \dots, x_{i-1}, x_{i+1}, \dots, x_p).$$

Date due applicazioni  $\{0, \dots, r\} \xrightarrow{g} \{0, \dots, q\} \xrightarrow{f} \{0, \dots, p\}$ , per l'associatività del prodotto di composizione si ha

$$g^*f^* = (fg)^*: K_p \rightarrow K_r.$$

DEFINIZIONE 3.1.2. Dato un complesso simpliciale astratto  $K$  ed un intero  $p$ , definiamo il gruppo  $C_p(K)$  delle  **$p$ -catene** in  $K$  come il gruppo abeliano libero generato da  $K_p$ . In altri termini, una  $p$ -catena in  $K$  è una combinazione lineare finita di  $p$ -simplessi orientati a coefficienti interi:

$$C_p(K) = \left\{ \sum_{\text{finita}} a_i s_i \mid s_i \in K_p, a_i \in \mathbb{Z} \right\}.$$

Consideriamo adesso, per ogni  $p > 0$ , l'omomorfismo di gruppi  $d_p: C_p(K) \rightarrow C_{p-1}(K)$  definito sui generatori del gruppo libero dalla formula  $d_p x = \sum_{i=0}^p (-1)^i \delta_i^* x$ , ossia

$$d_p(x_0, \dots, x_p) = \sum_{i=0}^p (-1)^i (x_0, \dots, \hat{x}_i, \dots, x_p), \quad (x_0, \dots, x_p) \in K_p.$$

In particolare, per  $p = 1, 2$ :

$$d_1(x_0, x_1) = x_1 - x_0, \quad d_2(x_0, x_1, x_2) = (x_1, x_2) - (x_0, x_2) + (x_0, x_1).$$

LEMMA 3.1.3. *Nelle notazioni precedenti si ha  $d_{p-1}d_p = 0$  per ogni  $p$  e quindi*

$$C(K) := \cdots \rightarrow C_4(K) \xrightarrow{d_4} C_3(K) \xrightarrow{d_3} C_2(K) \xrightarrow{d_2} C_1(K) \xrightarrow{d_1} C_0(K) \rightarrow 0$$

*è un complesso di catene.*

DIMOSTRAZIONE. Non è restrittivo dimostrare  $d_{p-1}d_p = 0$  per  $p \geq 2$  e basta mostrare che per ogni generatore  $(x_0, \dots, x_p) \in K_p$  vale  $d_{p-1}d_p(x_0, \dots, x_p) = 0$ . Qui bisogna fare un conto:

$$\begin{aligned} d_{p-1}d_p(x_0, \dots, x_p) &= d_{p-1} \sum_{i=0}^p (-1)^i (x_0, \dots, \widehat{x}_i, \dots, x_p) = \sum_{i=0}^p (-1)^i d_{p-1}(x_0, \dots, \widehat{x}_i, \dots, x_p) \\ &= \sum_{i=0}^p (-1)^i \left( \sum_{j=0}^{i-1} (-1)^j (\dots, \widehat{x}_j, \dots, \widehat{x}_i, \dots) + \sum_{j=i+1}^p (-1)^{j-1} (\dots, \widehat{x}_i, \dots, \widehat{x}_j, \dots) \right) \\ &= \sum_{j < i} (-1)^{i+j} (\dots, \widehat{x}_j, \dots, \widehat{x}_i, \dots) + \sum_{j > i} (-1)^{i+j-1} (\dots, \widehat{x}_i, \dots, \widehat{x}_j, \dots). \end{aligned}$$

Scambiando  $i$  con  $j$  nella seconda sommatoria ci accorgiamo che tutti gli addendi si cancellano con quelli della prima sommatoria e quindi il totale ha somma nulla.  $\square$

Possiamo quindi definire l'**omologia** del complesso simpliciale astratto  $K$  come l'omologia del complesso di catene  $C(K)$ :

$$H_n(K) := H_n(C(K)) = \frac{Z_n(K)}{B_n(K)},$$

dove  $Z_n(K) = \ker d_n$  è il sottogruppo degli  $n$ -cicli e  $B_n(K) = d_{n+1}(C_{n+1}(K))$  è il sottogruppo degli  $n$ -bordi.

È chiaro che complessi simpliciali isomorfi hanno la stessa omologia. Ogni isomorfismo  $f: (K, I) \xrightarrow{\cong} (H, J)$  induce in maniera naturale delle bigezioni

$$f: K_p \xrightarrow{\cong} H_p, \quad f(x_0, \dots, x_p) = (f(x_0), \dots, f(x_p)), \quad p \geq 0,$$

che inducono un isomorfismo di complessi  $f: C_*(K) \xrightarrow{\cong} C_*(H)$ .

ESEMPIO 3.1.4. Il complesso vuoto ha omologia banale. Infatti  $K = \emptyset$  implica  $K_p = \emptyset$  per ogni  $p$  e quindi  $C_p(K) = 0$  per ogni  $p$ .

ESEMPIO 3.1.5. Sia  $K = \Delta^{\{v\}}$  un complesso simpliciale con un solo vertice  $v$ . Allora per ogni  $p \geq 0$  esiste un unico  $p$ -simpleso orientato

$$(v, v, \dots, v) \in K_p.$$

Dunque  $C_p(K) = \mathbb{Z}$  per ogni  $p$ , il differenziale  $d_p: C_p(K) \rightarrow C_{p-1}(K)$  è

$$d_p(v, \dots, v) = \sum_{i=0}^p (v, \dots, v) = \begin{cases} (v, \dots, v) & \text{se } p \text{ pari} \\ 0 & \text{se } p \text{ dispari} \end{cases}$$

e quindi il complesso di catene diventa

$$\cdots C_4(K) = \mathbb{Z} \xrightarrow{\text{Id}} C_3(K) = \mathbb{Z} \xrightarrow{0} C_2(K) = \mathbb{Z} \xrightarrow{\text{Id}} C_1(K) = \mathbb{Z} \xrightarrow{0} C_0(K) = \mathbb{Z}$$

la cui omologia è  $H_0(K) = C_0(K) = \mathbb{Z}$ ,  $H_n(K) = 0$  per  $n \neq 0$ .

ESEMPIO 3.1.6. Per ogni insieme non vuoto  $I$  si ha  $H_0(\Delta^I) = \mathbb{Z}$ . Infatti  $H_0(\Delta^I)$  è per definizione il conucleo dell'omomorfismo

$$C_1(\Delta^I) \xrightarrow{d_1} C_0(\Delta^I), \quad d_1(x, y) = x - y, \quad x, y \in I.$$

Sia  $d_0: C_0(\Delta^I) \rightarrow \mathbb{Z}$  l'unico omomorfismo di gruppi tale che  $d_0(x) = 1$  per ogni  $x \in I$ , ossia

$$d_0\left(\sum_i a_i x_i\right) = \sum a_i, \quad a_i \in \mathbb{Z}, \quad x_i \in I,$$

e dimostriamo che

$$C_1(\Delta^I) \xrightarrow{d_1} C_0(\Delta^I) \xrightarrow{d_0} \mathbb{Z} \rightarrow 0$$

è una successione esatta. Per ipotesi  $I \neq \emptyset$ , fissato un vertice  $v \in I$  si ha  $d_0(nv) = n$  e quindi  $d_0$  è surgettiva. Per ogni generatore  $(x, y)$  di  $C_1(\Delta^I)$  si ha  $d_0d_1(x, y) = d_0(y - x) = 1 - 1 = 0$  e quindi  $d_0d_1 = 0$ . Viceversa sia  $z = \sum a_i x_i \in \ker(d_0)$ , allora  $\sum a_i = 0$ ,

$$d_1\left(\sum a_i(v, x_i)\right) = \sum a_i x_i - \sum a_i v = \sum a_i x_i$$

e quindi  $z \in B_0(\Delta^I)$ . Quindi il nucleo di  $d_0$  coincide con il sottogruppo degli 0-bordi e per i classici teoremi di isomorfismo dei gruppi  $H_0(\Delta^I) = \mathbb{Z}$ .

**TEOREMA 3.1.7.** *Se  $(K, I)$  è un complesso simpliciale astratto connesso e non vuoto, allora  $H_0(K) = \mathbb{Z}$ .*

**DIMOSTRAZIONE.** Abbiamo già dimostrato che  $H_0(\Delta^I) = \mathbb{Z}$ , basta quindi dimostrare che l'inclusione  $H_0(K) = H_0(\Delta^I)$ ; siccome  $K$  e  $\Delta^I$  hanno gli stessi vertici si ha  $Z_0(K) = C_0(K) = C_0(\Delta^I) = Z_0(\Delta^I)$  e di conseguenza basta provare che  $B_0(K) = B_0(\Delta^I)$ . Siccome  $C_1(K) \subseteq C_1(\Delta^I)$  è chiaro che  $d(C_1(K)) \subseteq d(C_1(\Delta^I))$ . Siccome  $d(C_1(\Delta^I))$  è il sottogruppo generato dagli elementi  $d(v, w) = (w) - (v)$ ,  $v, w \in I$ , basta considerare una catena finita di 1-simplessi

$$\{v, u_1\}, \{u_1, u_2\}, \dots, \{u_n, w\} \in K,$$

e scrivere

$$d(v, w) = d(v, u_1) + d(u_1, u_2) + \dots + d(u_n, w) \in d(C_1(K)).$$

□

**ESEMPIO 3.1.8.** Per prendere pratica con i gruppi di omologia dimostriamo direttamente che il primo gruppo di omologia del segmento  $K = \Delta^{\{a,b\}}$  di estremi  $a, b$  si annulla.

A tale scopo conviene eseguire un cambio di base del gruppo abeliano libero  $C_1(K)$ , considerando come nuova base

$$e_1 = (a, a), \quad e_2 = (b, b), \quad e_3 = (a, b) + (b, a), \quad e_4 = (a, b).$$

Abbiamo

$$de_1 = (a) - (a) = 0, \quad de_2 = (b) - (b) = 0, \quad de_3 = (b) - (a) + (a) - (b) = 0, \quad de_4 = (b) - (a),$$

e quindi  $Z_1(K)$  è il sottogruppo generato da  $e_1, e_2, e_3$ .

Per provare che  $H_1(K) = 0$  basta osservare che  $e_1, e_2, e_3 \in B_1(K)$ . Infatti si ha

$$d(a, a, a) = (a, a) - (a, a) + (a, a) = e_1, \quad d(b, b, b) = (b, b) = e_2,$$

$$d(b, a, b) + d(b, b, b) = (a, b) - (b, b) + (b, a) + (b, b) = e_3.$$

**ESEMPIO 3.1.9.** Sia  $K = \Delta^{\{a,b,c\}} - \{a, b, c\}$  il triangolo vuoto di vertici  $a, b, c$  e dimostriamo che  $H_1(K) = \mathbb{Z}$ . Come nell'esempio precedente conviene considerare la base di  $C_1(K)$  data da

$$e_1 = (a, a), \quad e_2 = (b, b), \quad e_3 = (c, c), \quad e_4 = (a, b) + (b, a), \quad e_5 = (b, c) + (c, b),$$

$$e_6 = (c, a) + (a, c), \quad e_7 = (a, b), \quad e_8 = (b, c), \quad e_9 = (c, a).$$

Si verifica immediatamente che

$$Z_1(K) = \left\{ \sum_{i=1}^9 a_i e_i \mid a_7 = a_8 = a_9 \right\}.$$

Siccome ogni simpleso di  $K$  contiene al massimo due vertici, possiamo scrivere

$$C_2(K) = C_2(\Delta^{\{a,b\}}) + C_2(\Delta^{\{b,c\}}) + C_2(\Delta^{\{c,a\}})$$

e di conseguenza

$$B_1(K) = B_1(\Delta^{\{a,b\}}) + B_1(\Delta^{\{b,c\}}) + B_1(\Delta^{\{c,a\}}).$$

Per quanto visto nell'esempio precedente si ha  $B_1(K) = \text{Span}(e_1, \dots, e_6)$  e quindi  $Z_1(K) = B_1(K) \oplus \mathbb{Z}(e_7 + e_8 + e_9)$ , ossia  $H_1(K) = \mathbb{Z}$  con generatore uguale alla classe di omologia del ciclo  $(a, b) + (b, c) + (c, a)$ .

**Esercizi:**

ESERCIZIO 21. Siano  $K$  un complesso simpliciale astratto e  $b(K)$  la sua suddivisione baricentrica. Per ogni  $p$ -simpleso orientato  $x = (x_0, \dots, x_p) \in K_p$  ed ogni permutazione  $\sigma$  di  $\{0, \dots, p\}$  definiamo il  $p$ -simpleso orientato  $\sigma(x) \in b(K)_p$  come

$$\sigma(x) = (\{x_{\sigma(0)}, \dots, x_{\sigma(p)}\}, \{x_{\sigma(1)}, \dots, x_{\sigma(p)}\}, \dots, \{x_{\sigma(p-1)}, x_{\sigma(p)}\}, \{x_{\sigma(p)}\}).$$

Dimostrare che esiste un morfismo di complessi di catene  $f: C(K) \rightarrow C(b(K))$  tale che

$$f(x) = \sum_{\sigma} (-1)^{\sigma} \sigma(x), \quad \text{per ogni } p \geq 0, x \in K_p,$$

dove la sommatoria è fatta su tutte le permutazioni di  $\{0, \dots, p\}$  e  $(-1)^{\sigma}$  indica la segnatura. (Suggerimento: dimostrare che la composizione di  $f$  con gli omomorfismi  $C_p(b(K)) \rightarrow C_{p-1}(b(K))$  indotti dalle applicazioni

$$\partial_i: b(K)_p \rightarrow b(K)_{p-1}, \quad \partial_i(x_0, \dots, x_p) = (x_0, \dots, \widehat{x}_i, \dots, x_p),$$

si annulla per ogni  $i > 0$ .)

ESERCIZIO 22. Ai fini del calcolo dell'omologia è utile introdurre un altro complesso di catene, detto **aumentato**. A tal fine si considera l'omomorfismo  $d_0: C_0(K) \rightarrow \mathbb{Z}$  che vale 1 su ciascun generatore  $x \in K_0$ . In altri termini

$$d_0\left(\sum_i a_i(x_i)\right) = \sum a_i, \quad a_i \in \mathbb{Z}, \quad (x_i) \in K_0.$$

Dato che per ogni  $(x_0, x_1) \in K_1$  si ha  $d_0 d_1(x_0, x_1) = d_0(x_1 - x_0) = 1 - 1 = 0$ , ha senso definire il complesso di catene aumentato

$$\overline{C(K)} := \dots \rightarrow C_4(K) \xrightarrow{d_4} C_3(K) \xrightarrow{d_3} C_2(K) \xrightarrow{d_2} C_1(K) \xrightarrow{d_1} C_0(K) \xrightarrow{d_0} \mathbb{Z} \rightarrow 0,$$

in cui  $\mathbb{Z}$  è posizionato in grado  $-1$ . Si definisce poi l'omologia aumentata del complesso simpliciale  $K$  come

$$\overline{H}_n(K) := H_n(\overline{C(K)}).$$

Dimostrare che per ogni complesso simpliciale astratto non vuoto  $K$  si ha  $\overline{H}_n(K) = H_n(K)$  per ogni  $n > 0$  ed esiste un isomorfismo di gruppi  $H_0(K) \cong \overline{H}_0(K) \oplus \mathbb{Z}$ .

### 3.2. Morfismi e classi di contiguità

I complessi di catene, e quindi anche i gruppi di omologia, si comportano bene, ossia in modo functoriale, rispetto ai morfismi di complessi simpliciali astratti: sia  $f: (K, I) \rightarrow (H, J)$  un morfismo di complessi simpliciali astratti. Allora per ogni simpleso orientato  $(x_0, \dots, x_p) \in K_p$  si ha  $(f(x_0), \dots, f(x_p)) \in H_p$ . È dunque definito un morfismo di complessi di catene

$$f: C_*(K) \rightarrow C_*(H)$$

definito sui generatori dalla formula

$$f(x_0, \dots, x_p) = (f(x_0), \dots, f(x_p)), \quad (x_0, \dots, x_p) \in K_p, p \geq 0.$$

Che si tratti di un morfismo di complessi è quasi ovvio in quanto

$$\begin{aligned} fd(x_0, \dots, x_p) &= f\left(\sum_{i=0}^p (-1)^i (x_0, \dots, \widehat{x}_i, \dots, x_p)\right) = \sum_{i=0}^p (-1)^i (f(x_0), \dots, \widehat{x}_i, \dots, f(x_p)) \\ &= \sum_{i=0}^p (-1)^i (f(x_0), \dots, \widehat{f(x_i)}, \dots, f(x_p)) = df(x_0, \dots, x_p). \end{aligned}$$

Abbiamo quindi che  $f$  definisce dei morfismi in omologia  $f: H_n(K) \rightarrow H_n(H)$ . Appare inoltre evidente che tale costruzione commuta con i prodotti di composizione: dati due morfismi di complessi simpliciali astratti  $(K, I) \xrightarrow{f} (H, J) \xrightarrow{g} (S, T)$ , il morfismo indotto  $gf: H_n(K) \rightarrow H_n(S)$  è uguale alla composizione di  $f: H_n(K) \rightarrow H_n(H)$  e  $g: H_n(H) \rightarrow H_n(S)$ .

DEFINIZIONE 3.2.1. Sia  $(K, I)$  un complesso simpliciale astratto. Diremo che  $K$  è **stellato** rispetto ad un vertice  $v \in I$  se vale la condizione

$$(3.1) \quad \sigma \cup \{v\} \in K \text{ per ogni } \sigma \in K.$$

Diremo che  $(K, I)$  è un **cono** se esiste almeno un vertice rispetto al quale è stellato.

Ad esempio: il complesso simpliciale vuoto non è un cono (non esiste alcun vertice); per ogni insieme non vuoto  $I$  il complesso simpliciale completo  $\Delta^I$  è un cono, infatti è stellato rispetto ad ogni suo vertice.

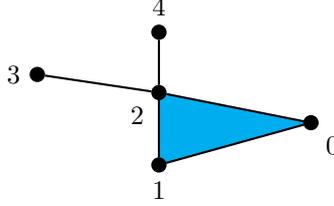


FIGURA 1. Un cono, con il vertice 2 che soddisfa (3.1).

TEOREMA 3.2.2. Sia  $(K, I)$  un complesso simpliciale che è un cono. Allora, per ogni vertice  $v \in I$  il morfismo di inclusione  $i: \{v\} \hookrightarrow K$  induce un isomorfismo in omologia. Di conseguenza  $H_0(K) = \mathbb{Z}$  e  $H_n(K) = 0$  per ogni  $n > 0$ .

DIMOSTRAZIONE. Dimostriamo prima il teorema nel caso in cui  $(K, I)$  sia stellato rispetto al vertice  $v$ , mostrando che il morfismo tra complessi di catene indotto da  $i$  è una equivalenza omotopica.

Denotiamo con  $f: K \rightarrow \{v\}$  l'unico morfismo possibile, ossia quello che manda tutti i vertici in  $v$ . È chiaro che  $fi$  è l'identità, mentre  $if: K \rightarrow K$  manda tutti i vertici in  $v$ .

Si consideri adesso l'omotopia  $h: C_*(K) \rightarrow C_*(K)[1]$  definita sui semplici orientati come

$$h(x_0, \dots, x_p) = (v, x_0, \dots, x_p) - (v, v, \dots, v).$$

L'ipotesi che  $K$  sia un cono di vertice  $v$  garantisce che  $h$  è ben definita. Si ha

$$(dh + hd)(x_0) = dh(x_0) = d(v, x_0) - d(v, v) = x_0 - v - v + v = (\text{Id} - if)(x_0)$$

mentre per  $p > 0$  vale

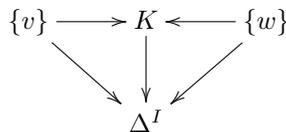
$$\begin{aligned} dh(x_0, \dots, x_p) &= d(v, x_0, \dots, x_p) - d(v, \dots, v) \\ &= (x_0, \dots, x_p) + \sum_{i=0}^p (-1)^{i+1} (v, x_0, \dots, \hat{x}_i, \dots, x_p) - \sum_{i=0}^{p+1} (-1)^i (v, v, \dots, v). \end{aligned}$$

$$\begin{aligned} hd(x_0, \dots, x_p) &= h \left( \sum_{i=0}^p (-1)^i (x_0, \dots, \hat{x}_i, \dots, x_p) \right) \\ &= \sum_{i=0}^p (-1)^i (v, x_0, \dots, \hat{x}_i, \dots, x_p) - \sum_{i=0}^p (-1)^i (v, v, \dots, v) \end{aligned}$$

e siccome  $\sum_{i=0}^{p+1} (-1)^i + \sum_{i=0}^p (-1)^i = \sum_{i=0}^{p+1} (-1)^i + \sum_{i=1}^{p+1} (-1)^{i-1} = 1$ , dalla somma delle precedenti formule si ottiene

$$(dh + hd)(x_0, \dots, x_p) = (x_0, \dots, x_p) - (v, \dots, v) = (\text{Id} - if)(x_0, \dots, x_p).$$

Supponiamo adesso che  $v \in I$  sia un vertice qualsiasi e scegliamo un vertice  $w \in I$  rispetto al quale  $K$  risulti stellato. Siccome  $\Delta^I$  è stellato rispetto ad entrambi i vertici  $v$  e  $w$ , i morfismi di inclusione



inducono in omologia dei diagrammi commutativi

$$\begin{array}{ccccc}
 H_n(\{v\}) & \longrightarrow & H_n(K) & \xleftarrow{\simeq} & H_n(\{w\}) & n \in \mathbb{Z} \\
 & \searrow \simeq & \downarrow & \swarrow \simeq & & \\
 & & H_n(\Delta^I) & & & 
 \end{array}$$

con le tre frecce etichettate  $\simeq$  isomorfismi in virtù del caso particolare precedentemente trattato. Ma allora, per la regola del 2 su 3 anche i rimanenti due morfismi sono bigettivi.  $\square$

**ESEMPIO 3.2.3.** Per ogni insieme non vuoto  $I$  il complesso simpliciale astratto completo  $\Delta^I$  è un cono e quindi  $H_0(\Delta^I) = \mathbb{Z}$  e  $H_n(\Delta^I) = 0$  per ogni  $n \neq 0$ .

**COROLLARIO 3.2.4.** Siano  $K$  un complesso simpliciale astratto e  $L \subseteq K$  un sottocomplesso. Se  $H$  e  $K$  sono coni, allora il morfismo di inclusione  $L \rightarrow K$  induce un isomorfismo in omologia.

**DIMOSTRAZIONE.** Preso un qualsiasi vertice  $v$  di  $L$  si hanno le inclusioni  $\{v\} \subset L \subset K$  e per il Teorema 3.2.2 entrambe le inclusioni  $\{v\} \subset L$  e  $\{v\} \subset K$  inducono isomorfismi in omologia. Quindi, per la regola del 2 su 3 anche l'inclusione  $L \subseteq K$  induce un isomorfismo in omologia.  $\square$

**COROLLARIO 3.2.5.** Siano  $K$  un complesso simpliciale astratto e  $L \subseteq K$  un sottocomplesso. Se  $H$  e  $K$  sono entrambi connessi e non vuoti, allora il morfismo di inclusione  $L \rightarrow K$  induce un isomorfismo  $H_0(L) \simeq H_0(K) = \mathbb{Z}$ .

**DIMOSTRAZIONE.** Siano  $I, J$  gli insiemi dei vertici di  $K$  e  $L$  rispettivamente; per definizione di sottocomplesso  $J \subset I$ . La stessa dimostrazione del Teorema 3.1.7 mostra che i morfismi di inclusione  $K \subset \Delta^I$  e  $L \subset \Delta^J$  inducono isomorfismi tra gli  $H_0$  (che sono tutti isomorfi a  $\mathbb{Z}$ ). Per concludere basta osservare che per il Corollario 3.2.4 l'inclusione di coni  $\Delta^J \subset \Delta^I$  induce un isomorfismo in omologia.  $\square$

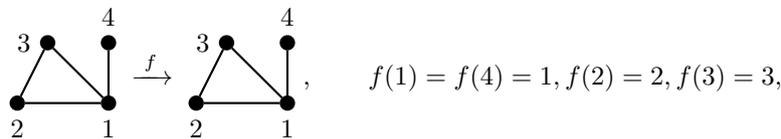
Introduciamo adesso la relazione di contiguità tra morfismi, iniziando da un caso particolare detto di contiguità diretta.

**DEFINIZIONE 3.2.6.** Due morfismi  $f, g: (K, I) \rightarrow (H, J)$  di complessi simpliciali astratti si dicono **direttamente contigui** se per ogni  $s \in K$  si ha  $f(s) \cup g(s) \in H$ .

Equivalentemente possiamo dire che  $f, g: (K, I) \rightarrow (H, J)$  sono direttamente contigui se per ogni  $s \in K$  esiste  $\sigma \in H$  tale che  $f(s) \subseteq \sigma, g(s) \subseteq \sigma$ .

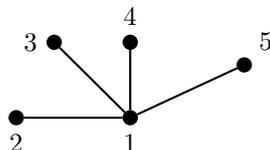
**ESEMPIO 3.2.7.** Un complesso simpliciale astratto  $K$  è stellato rispetto ad un vertice  $v$  se e solo se l'identità su  $K$  è direttamente contigua all'applicazione  $K \rightarrow K$  che vale costantemente  $\{v\}$ .

**ESEMPIO 3.2.8.** Il morfismo



è direttamente contiguo all'identità.

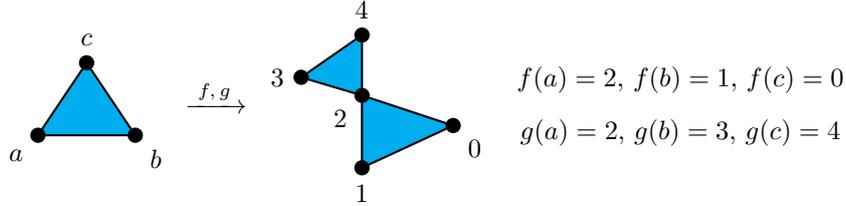
La relazione di contiguità diretta gode chiaramente delle proprietà riflessiva e simmetrica, ma non della proprietà transitiva: ad esempio se  $K = \Delta^0, H$  è il complesso simpliciale



e  $f_i: K \rightarrow H$  è il morfismo che manda l'unico vertice di  $K$  nel vertice  $i$  di  $H$ , allora  $f_1$  è direttamente contiguo a ogni  $f_i$ , ma  $f_2$  ed  $f_3$  non sono direttamente contigui tra loro.

Chiameremo **contiguità** la relazione di equivalenza generata dalla contiguità diretta: più concretamente, due morfismi di complessi simpliciali astratti  $f, g: (K, I) \rightarrow (H, J)$  si dicono contigui se esiste una successione finita di morfismi di complessi  $\varphi_1, \dots, \varphi_n: (K, I) \rightarrow (H, J)$  con  $f = \varphi_0, g = \varphi_n$  e  $\varphi_i$  direttamente contiguo a  $\varphi_{i+1}$  per ogni  $i = 1, \dots, n - 1$ .

Ad esempio i due morfismi



sono contigui poiché entrambi direttamente contigui al morfismo costante sul vertice 2.

Osserviamo che  $f, g: K \rightarrow H$  sono contigui come morfismi se e solo se sono contigui come vertici del complesso simpliciale  $\text{Hom}^\Delta$  (Esempio 1.2.15).

**PROPOSIZIONE 3.2.9.** *La relazione di contiguità è preservata per composizione, e cioè, dati 4 morfismi di complessi simpliciali astratti  $K \xrightarrow{f,g} H \xrightarrow{p,q} L$ , se  $f$  è contiguo a  $g$  e  $p$  è contiguo a  $q$ , allora  $pf$  è contiguo a  $qg$ .*

**DIMOSTRAZIONE.** Usando la proprietà transitiva ci possiamo ricondurre immediatamente al caso in cui  $f$  è direttamente contiguo a  $g$  e  $p$  è direttamente contiguo a  $q$ . Sia allora  $s \in K$  un simpleso, esistono allora due semplici  $t \in H$  e  $r \in L$  tali che  $f(s), g(s) \subseteq t, p(t), q(t) \subseteq r$  da cui segue  $pf(s), qg(s) \subset r$ .  $\square$

Una delle conseguenze della Proposizione 3.2.9 è che ha perfettamente senso considerare diagrammi commutativi a meno di contiguità.

Per terminare la sezione, dimostriamo che morfismi contigui inducono lo stesso morfismo in omologia.

**TEOREMA 3.2.10.** *Siano  $f, g: K \rightarrow L$  due morfismi contigui di complessi simpliciali astratti. Allora per ogni intero  $n$  vale*

$$f = g: H_n(K) \rightarrow H_n(L).$$

**DIMOSTRAZIONE.** Non è affatto restrittivo supporre  $f$  e  $g$  direttamente contigui, ossia che  $f(s) \cup g(s) \in L$  per ogni  $s \in K$ . In tal caso per ogni  $(x_0, \dots, x_p) \in K_p$  si ha

$$(f(x_0), \dots, f(x_i), g(x_i), \dots, g(x_p)) \in L_{p+1} \quad \forall i = 0, \dots, p,$$

e possiamo definire un'omotopia  $h: C_*(K) \rightarrow C_*(L)[1]$  ponendo sui semplici orientati

$$h(x_0, \dots, x_p) = \sum_{i=0}^p (-1)^i (f(x_0), \dots, f(x_i), g(x_i), \dots, g(x_p)).$$

Per ogni  $(x_0, \dots, x_p) \in K_p$  si ha

$$\begin{aligned} dh(x_0, \dots, x_p) &= \sum_{i=0}^p (-1)^i d(f(x_0), \dots, f(x_i), g(x_i), \dots, g(x_p)) \\ &= \sum_{0 \leq j \leq i \leq p} (-1)^{i+j} (\dots, \widehat{f(x_j)}, \dots, f(x_i), g(x_i), \dots, g(x_p)) \\ &\quad - \sum_{0 \leq i \leq j \leq p} (-1)^{i+j} (f(x_0), \dots, f(x_i), g(x_i), \dots, \widehat{g(x_j)}, \dots), \\ hd(x_0, \dots, x_p) &= \sum_{j=0}^p (-1)^j h(x_0, \dots, \widehat{x_j}, \dots, x_p) \\ &= \sum_{0 \leq i < j \leq p} (-1)^{i+j} (f(x_0), \dots, f(x_i), g(x_i), \dots, \widehat{g(x_j)}, \dots) \\ &\quad - \sum_{0 \leq j < i \leq p} (-1)^{i+j} (\dots, \widehat{f(x_j)}, \dots, f(x_i), g(x_i), \dots, g(x_p)). \end{aligned}$$

Dunque

$$\begin{aligned} (hd + dh)(x_0, \dots, x_p) &= \sum_{i=0}^p (f(x_0), \dots, f(x_{i-1}), g(x_i), \dots, g(x_p)) - (f(x_0), \dots, f(x_i), g(x_{i+1}), \dots, g(x_p)) \\ &= (g(x_0), \dots, g(x_p)) - (f(x_0), \dots, f(x_p)) \end{aligned}$$

e quindi  $h$  è un'omotopia tra i due morfismi di complessi di catene  $f, g: C_*(K) \rightarrow C_*(L)$ .  $\square$

### Esercizi:

ESERCIZIO 23. Siano  $K$  e  $H$  due complessi simpliciali astratti con  $H$  di tipo cono. Dimostrare:

- (1) tutti i morfismi di complessi  $K \rightarrow H$  sono contigui tra loro;
- (2) se  $K$  è connesso, allora tutti i morfismi  $\Delta^0 \rightarrow K$  sono contigui tra loro;
- (3) se  $K$  è connesso, allora tutti i morfismi  $H \rightarrow K$  sono contigui tra loro.

### 3.3. La successione esatta di Mayer-Vietoris

Dati due complessi di catene  $C, D$  possiamo considerare il complesso somma diretta

$$C \oplus D := \dots \rightarrow C_n \oplus D_n \xrightarrow{(x,y) \mapsto (dx, dy)} C_{n-1} \oplus D_{n-1} \rightarrow \dots$$

Segue immediatamente dalla definizione del differenziale in  $C \oplus D$  che per ogni  $n$  si ha

$$Z_n(C \oplus D) = Z_n(C) \oplus Z_n(D), \quad B_n(C \oplus D) = B_n(C) \oplus B_n(D),$$

e quindi  $H_n(C \oplus D) = H_n(C) \oplus H_n(D)$ .

Ad un quadrato commutativo di morfismi di complessi di catene

$$\begin{array}{ccc} C & \xrightarrow{i} & D \\ \downarrow j & & \downarrow p \\ E & \xrightarrow{q} & F \end{array}$$

possiamo associare un diagramma in serie

$$(3.2) \quad 0 \rightarrow C \xrightarrow{f} D \oplus E \xrightarrow{g} F \rightarrow 0, \quad f(x) = (i(x), j(x)), \quad g(y, z) = p(y) - q(z),$$

con la proprietà che  $gf = 0$ .

LEMMA 3.3.1. *Nelle notazioni precedenti, se (3.2) è una successione esatta corta di complessi di catene, allora esiste una successione esatta lunga di omologia*

$$\cdots \rightarrow H_n(C) \xrightarrow{f} H_n(D) \oplus H_n(E) \xrightarrow{g} H_n(F) \rightarrow H_{n-1}(C) \rightarrow \cdots$$

*Inoltre, se  $j$  è un quasi-isomorfismo, allora anche  $p$  è un quasi-isomorfismo. Se  $i$  è un quasi-isomorfismo, allora  $q$  è un quasi-isomorfismo*

DIMOSTRAZIONE. La prima parte è conseguenza immediata dalla successione esatta lunga di omologia e dagli isomorfismi naturali  $H_n(D \oplus E) = H_n(D) \oplus H_n(E)$ .

Supponiamo adesso che  $j: H_n(C) \rightarrow H_n(E)$  sia bigettiva per ogni  $n$ , a maggior ragione  $H_n(C) \xrightarrow{f=(i,j)} H_n(D) \oplus H_n(E)$  è iniettiva per ogni  $n$  e dalla successione esatta lunga di omologia segue che  $H_n(D) \oplus H_n(E) \xrightarrow{g} H_n(F)$  è surgettiva per ogni  $n$ . D'altra parte per ogni  $(y, z) \in H_n(D) \oplus H_n(E)$  si ha

$$p(y - ij^{-1}(z)) = p(y) - pij^{-1}(z) = p(y) - qjj^{-1}(z) = p(y) - q(z) = g(y, z)$$

e questo prova che  $p: H_n(D) \rightarrow H_n(F)$  è surgettiva. Se  $y \in H_n(D)$  e  $p(y) = 0$ , allora  $(y, 0) \in \ker(g) = f(H_n(C))$  ed esiste  $x \in H_n(C)$  tale che  $i(x) = y, j(x) = 0$ . Ma  $j$  è iniettiva, quindi  $x = 0$  ed a maggior ragione  $y = 0$ .

Abbiamo quindi provato che se  $j$  è un quasi-isomorfismo allora  $p$  è un quasi-isomorfismo. Per ovvi motivi di simmetria si ha anche che se  $i$  è un quasi-isomorfismo allora  $q$  è un quasi-isomorfismo. □

Consideriamo adesso un insieme  $I$  e due sottocomplessi simpliciali astratti  $K, L \subseteq \Delta^I$  i cui rispettivi insiemi di vertici possono essere strettamente contenuti in  $I$ . Abbiamo visto che le loro unione  $K \cup L$  ed intersezione  $K \cap L$  sono ancora sottocomplessi simpliciali astratti.

TEOREMA 3.3.2 (Mayer-Vietoris). *Nelle notazioni precedenti esiste una successione esatta lunga di omologia*

$$\cdots \rightarrow H_n(K \cap L) \rightarrow H_n(K) \oplus H_n(L) \rightarrow H_n(K \cup L) \rightarrow H_{n-1}(K \cap L) \rightarrow \cdots \rightarrow H_0(K \cup L) \rightarrow 0.$$

*Se l'inclusione  $K \cap L \subseteq L$  induce un isomorfismo in omologia, allora anche l'inclusione  $K \subseteq K \cup L$  induce un isomorfismo in omologia.*

DIMOSTRAZIONE. Per un simpleso ordinato  $(x_0, \dots, x_p)$  le seguenti condizioni sono equivalenti:

- (1)  $(x_0, \dots, x_p) \in (K \cup L)_p$ ;
- (2)  $\{x_0, \dots, x_p\} \in K \cup L$ ;
- (3)  $\{x_0, \dots, x_p\} \in K$  oppure  $\{x_0, \dots, x_p\} \in L$ ;
- (4)  $(x_0, \dots, x_p) \in K_p$  oppure  $(x_0, \dots, x_p) \in L_p$ ;

e quindi  $(K \cup L)_p = K_p \cup L_p$ . Similmente  $(K \cap L)_p = K_p \cap L_p$ . Da ciò segue che esiste una successione esatta corta di complessi di catene

$$(3.3) \quad 0 \rightarrow C_*(K \cap L) \xrightarrow{f} C_*(K) \oplus C_*(L) \xrightarrow{g} C_*(K \cup L) \rightarrow 0,$$

dove morfismi  $f$  e  $g$  sono definiti sui semplici orientati come

$$\begin{aligned} f(x_0, \dots, x_p) &= ((x_0, \dots, x_p), (x_0, \dots, x_p)), \\ g((x_0, \dots, x_p), (y_0, \dots, y_p)) &= (x_0, \dots, x_p) - (y_0, \dots, y_p). \end{aligned}$$

Basta adesso applicare il Lemma 3.3.1. □

COROLLARIO 3.3.3. *Nelle ipotesi del Teorema 3.3.2, se  $K \cap L = \emptyset$ , allora  $H_n(K \cup L) = H_n(K) \oplus H_n(L)$ .*

DIMOSTRAZIONE.  $H_n(\emptyset) = 0$  per ogni  $n$ . □

ESEMPIO 3.3.4. Se il complesso simpliciale astratto  $K$  è formato da  $n$  vertici senza alcun simpleso di dimensione positiva, allora  $H_0(K) = \mathbb{Z}^n$  e  $H_p(K) = 0$  per ogni  $p \neq 0$ .

ESEMPIO 3.3.5 (Omologia delle sfere). Per ogni  $n \geq 0$  definiamo la *sfera simpliciale*  $S^n$  come lo  $n$ -scheletro di  $\Delta^{n+1}$ , ossia

$$S^n = \{s \subset \{0, 1, \dots, n+1\} \mid |s| \leq n+1\} = \Delta^{n+1} - \{0, \dots, n+1\}.$$

Il nome sfera è motivato dalla rappresentazione geometrica di  $S^n$ : infatti  $S^1$  è un triangolo vuoto (omeomorfo alla circonferenza),  $S^2$  è il bordo di un tetraedro (omeomorfo alla usuale sfera bidimensionale) ecc.. In maniera informale, possiamo quindi pensare ad  $S^n$  come il dato combinatorio corrispondente ad un “buco”  $n$ -dimensionale.

Si ha  $S^0 = \{\{0\}, \{1\}\}$ , quindi  $H_0(S^0) = \mathbb{Z}^2$  e  $H_i(S^0) = 0$  per ogni  $i > 0$ . Per  $n > 0$  la sfera  $S^n$  è connessa e si ha il seguente risultato.

PROPOSIZIONE 3.3.6. *Nelle notazioni precedenti, per ogni  $n > 0$  vale*

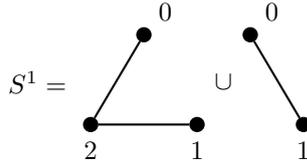
$$H_0(S^n) = H_n(S^n) = \mathbb{Z}, \quad H_i(S^n) = 0 \quad \text{per ogni } i \neq 0, n.$$

DIMOSTRAZIONE. Presentiamo una dimostrazione che utilizza la successione esatta di Mayer–Vietoris; una diversa dimostrazione sarà data in seguito.

Possiamo scrivere  $S^n = K \cup L$ , dove  $L = \Delta^n = \Delta^{\{0, \dots, n\}}$  e  $K = S^n - \{0, \dots, n\}$ . Si osserva che  $K$  è stellato rispetto al vertice  $\{n+1\}$ . Quindi

$$H_0(L) = H_0(K) = \mathbb{Z}, \quad H_i(K) = H_i(L) = 0 \quad \text{per ogni } i > 0.$$

Inoltre  $K \cap L = \Delta^n - \{0, \dots, n\} = S^{n-1}$ .



Dalla successione di Mayer–Vietoris, per ogni  $i, n > 0$  si ha

$$\dots \rightarrow 0 = H_{i+1}(K) \oplus H_{i+1}(L) \rightarrow H_{i+1}(S^n) \rightarrow H_i(S^{n-1}) \rightarrow H_i(K) \oplus H_i(L) = 0 \rightarrow \dots$$

da cui segue  $H_{i+1}(S^n) \simeq H_i(S^{n-1})$ . Per induzione su  $n$  si deduce immediatamente che  $H_i(S^n) = 0$  per ogni  $i > n \geq 0$ . Sempre per induzione su  $n$ , per concludere la dimostrazione basta provare che  $H_1(S^1) = \mathbb{Z}$  e  $H_1(S^n) = 0$  per ogni  $n > 1$ .

Riguardo al caso  $S^1$ , per Mayer–Vietoris si ha una successione esatta

$$0 \rightarrow H_1(S^1) \rightarrow H_0(S^0) = \mathbb{Z}^2 \rightarrow H_0(K) \oplus H_0(L) = \mathbb{Z}^2 \rightarrow H_0(S^1) = \mathbb{Z} \rightarrow 0.$$

Se ne deduce che  $H_1(S^1)$  è un sottogruppo di  $\mathbb{Z}^2$  e quindi isomorfo a  $\mathbb{Z}^m$  per qualche  $m$ , che per l’additività del rango deve essere  $m = 1$ .

Per  $n > 1$  si ha invece una successione esatta

$$0 \rightarrow H_1(S^n) \rightarrow H_0(S^{n-1}) \rightarrow H_0(K) \oplus H_0(L)$$

e basta osservare che l’inclusione di complessi simpliciali connessi  $S^{n-1} \subset L$  induce un isomorfismo tra i rispettivi  $H_0$ . A maggior ragione il morfismo  $H_0(S^{n-1}) \rightarrow H_0(K) \oplus H_0(L)$  è iniettivo e quindi  $H_1(S^n) = 0$ .  $\square$

**3.3.1. Potatura.** Come ulteriore applicazione della successione esatta di Mayer–Vietoris mostriamo che le operazioni di **potatura** di un complesso simpliciale astratto non cambiano l’omologia.

Siano  $M$  un complesso simpliciale astratto ed  $s = (x_0, \dots, x_p) \in M_p$  un simpleso orientato non degenere di dimensione positiva (ossia  $x_i \neq x_j$  per ogni  $i \neq j$  e  $p > 0$ ). Si assuma che  $\{x_0, \dots, x_p\}$  sia un simpleso massimale (ossia non contenuto in alcun simpleso di dimensione maggiore) e che  $\{x_0, \dots, x_p\}$  sia l’unico simpleso di  $M$  che contiene strettamente  $\{x_1, \dots, x_p\}$ .

Sia  $K \subset P$  ottenuto togliendo i due semplici  $\{x_0, \dots, x_p\}$  e  $\{x_1, \dots, x_p\}$ ; è chiaro per costruzione che  $K$  è un sottocomplesso simpliciale, che viene detto una **potatura** di  $s$  da  $P$ . Più in generale, parleremo di potatura (di una successione di semplici orientati) per intendere una successione finita di operazioni come sopra, vedi Figura 2.

Consideriamo adesso il sottocomplesso  $L = \Delta^{\{x_0, \dots, x_p\}}$ , allora  $P = K \cup L$  ed i due sottocomplessi  $L, K \cap L$  sono entrambi stellati rispetto al vertice  $x_0$ .

Per il Corollario 3.2.4 l'inclusione  $K \cap L \subset L$  induce un isomorfismo in omologia, e per il teorema di Mayer-Vietoris anche l'inclusione  $K \subset P$  induce un isomorfismo in omologia.

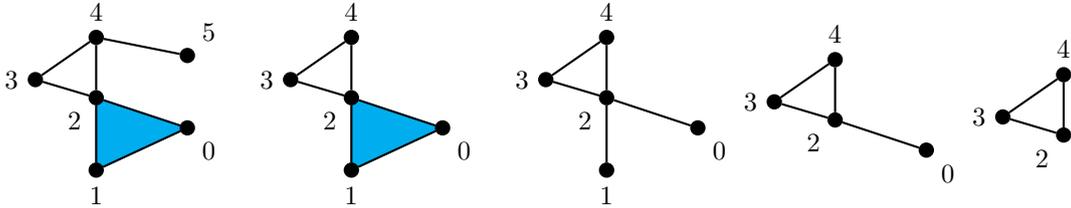


FIGURA 2. La potatura dei semplici orientati  $(4, 5)$ ,  $(2, 1, 0)$ ,  $(2, 1)$  e  $(2, 0)$ .

Per transitività hanno la stessa omologia pure due complessi simpliciali astratti che si ottengono come potature (di semplici distinti) di un medesimo complesso simpliciale astratto (vedi Figura 3).

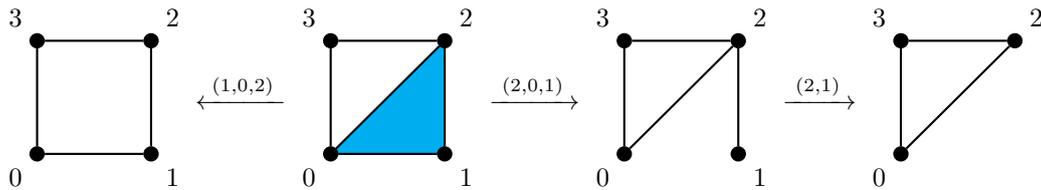
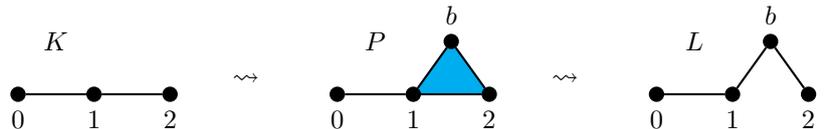


FIGURA 3. I bordi del quadrato e del triangolo si ottengono per potature da un medesimo complesso simpliciale astratto (il secondo da sinistra).

**3.3.2. Baricentri aggiunti.** Possiamo formalizzare la procedura di Figura 3 nel modo seguente. Siano  $(K, I)$  un complesso simpliciale astratto  $\{x_0, \dots, x_p\} \in K$  un semplice massimale di dimensione  $p$ ,  $b \notin I$  e definiamo un nuovo complesso simpliciale

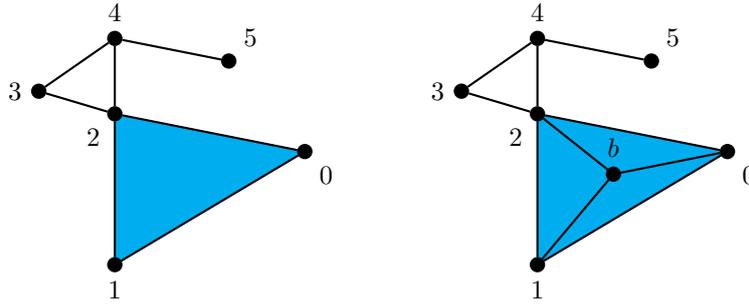
$$P = K \cup \Delta^{\{b, x_0, \dots, x_p\}} \subset \Delta^{I \cup \{v\}}.$$

È chiaro che  $K \cap \Delta^{\{b, x_0, \dots, x_p\}} = \Delta^{\{x_0, \dots, x_p\}}$  e quindi, per Mayer-Vietoris si ha che l'inclusione  $K \subset P$  è un isomorfismo in omologia. A questo punto possiamo eseguire su  $P$  la potatura del semplice orientato  $(b, x_0, \dots, x_p)$  ed ottenere un nuovo complesso simpliciale  $L$  che ha la stessa omologia di  $K$ :

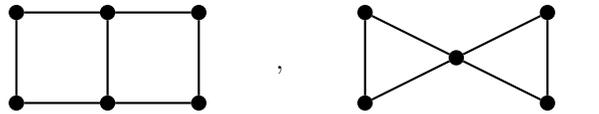


Diremo che per passare da  $K$  ad  $L$  abbiamo **aggiunto il baricentro** al semplice massimale  $\{x_0, \dots, x_p\}$ . In pratica, abbiamo prima eliminato da  $K$  il semplice  $\{x_0, \dots, x_p\}$  e poi abbiamo aggiunto tutti i  $2^{p+1} - 1$  semplici del tipo  $\{b, x_{i_1}, \dots, x_{i_q}\}$ , con  $0 \leq q \leq p$  e  $0 \leq i_1 < \dots < i_q \leq p$  (Figura 4).

**Esercizi:**

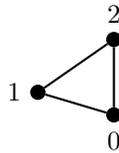
FIGURA 4. Aggiunta del baricentro al semplice massimale  $\{0, 1, 2\}$ .

ESERCIZIO 24. Mediante potature, aggiunte di baricentri e loro operazioni inverse, trasformare l'uno nell'altro i seguenti complessi simpliciali unidimensionali:



### 3.4. Il sottocomplesso delle catene ordinate

Se vogliamo calcolare esplicitamente i gruppi di omologia di un complesso simpliciale astratto ci troviamo di fronte alla difficoltà di lavorare con insiemi di semplici orientati  $K_p$  molto grandi e mai vuoti anche per  $p$  molto maggiore della dimensione del complesso simpliciale. Ad esempio, nel caso del triangolo vuoto



si ha che  $K_p$  contiene esattamente  $3(2^{p+1} - 1)$  elementi (esercizio: dimostrare).

Per ovviare a tale inconveniente si possono considerare i sottocomplessi di catene ordinate. Sia  $(K, I)$  un complesso simpliciale astratto e dotiamo  $I$  di una **relazione di ordine totale**  $\leq$ . Ricordiamo che per ordine totale si intende una relazione di ordine  $\leq$  con la proprietà che per ogni  $x, y$  si ha  $x \leq y$  oppure  $y \leq x$ . Le possibili relazioni di ordine totale su un insieme sono tante, almeno quanto le permutazioni, e per i nostri scopi ne va bene una qualunque.

A questo punto, per ogni intero  $p \geq 0$  possiamo considerare il sottoinsieme dei  **$p$ -simplessi ordinati**

$$K_p^< = \{(x_0, \dots, x_p) \in K_p \mid x_0 < x_1 < \dots < x_p\},$$

ed il sottoinsieme dei  **$p$ -simplessi debolmente ordinati**

$$K_p^{\leq} = \{(x_0, \dots, x_p) \in K_p \mid x_0 \leq x_1 \leq \dots \leq x_p\}.$$

Osserviamo con immenso piacere che se  $K$  ha dimensione  $n$ , allora  $K_p^< = \emptyset$  per ogni  $p > n$ , e comunque che  $K_p^<$  è notevolmente più piccolo di  $K_p$ : ad esempio, per il complesso simpliciale astratto  $\Delta^n$ , l'insieme  $K_p$  contiene  $(n+1)^{p+1}$  elementi, mentre  $K_p^<$  e  $K_p^{\leq}$  ne contengono rispettivamente  $\binom{n+1}{p+1}$  e  $\binom{n+p+1}{p+1}$ .

Un'altra osservazione che ci riempie di gioia è che se  $(x_0, \dots, x_p) \in K_p^<$  (resp.:  $\in K_p^{\leq}$ ) allora per ogni indice  $i$  si ha  $(x_0, \dots, \hat{x}_i, \dots, x_p) \in K_{p-1}^<$  (resp.:  $\in K_{p-1}^{\leq}$ ).

Indichiamo con  $C_p(K, <) \subset C_p(K)$  il gruppo abeliano libero generato da  $K_p^{<}$ . Al variare di  $p$  questi gruppi definiscono un sottocomplesso di catene  $C_*(K, <) \subseteq C_*(K)$  in quanto chiuso per il differenziale

$$d(x_0, \dots, x_p) = \sum_{i=0}^p (-1)^i (x_0, \dots, \widehat{x}_i, \dots, x_p).$$

Similmente, indichiamo con  $C_p(K, \leq) \subset C_p(K)$  il gruppo abeliano libero generato da  $K_p^{\leq}$ . Come sopra questi gruppi definiscono un sottocomplesso di catene  $C_*(K, \leq) \subseteq C_*(K)$ . Vogliamo dimostrare il seguente risultato

TEOREMA 3.4.1. *Nelle notazioni precedenti le inclusioni di complessi*

$$C_*(K, <) \subseteq C_*(K, \leq) \subseteq C_*(K)$$

*inducono isomorfismi in omologia:*

$$H_n(C_*(K, <)) = H_n(C_*(K, \leq)) = H_n(C_*(K)) = H_n(K), \quad \text{per ogni } n.$$

La dimostrazione è abbastanza lunga e laboriosa e per chiarezza espositiva viene spezzata in una serie di lemmi.

LEMMA 3.4.2. *L'inclusione  $i: C_*(K, <) \rightarrow C_*(K, \leq)$  è un'equivalenza omotopica e quindi un isomorfismo in omologia.*

DIMOSTRAZIONE. Consideriamo la proiezione  $\pi: C_*(K, \leq) \rightarrow C_*(K, <)$  definita per estensione lineare delle applicazioni  $\pi: K_p^{\leq} \rightarrow K_p^{<}$  definite come:

$$\pi(x_0, \dots, x_p) = \begin{cases} (x_0, \dots, x_p) & \text{se } (x_0, \dots, x_p) \in K_p^{<}, \\ 0 & \text{se } (x_0, \dots, x_p) \in K_p^{\leq} - K_p^{<}. \end{cases}$$

È chiaro che  $\pi i = \text{Id}$ ; vogliamo dimostrare che esiste un'omotopia  $h: C_*(K, \leq) \rightarrow C_*(K, \leq)[1]$  tale che  $dh + hd = \text{Id} - i\pi$ . Dato  $(x_0, \dots, x_p) \in K_p^{<}$  definiamo  $h(x_0, \dots, x_p) = 0$ ; se invece  $(x_0, \dots, x_p) \in K_p^{\leq} - K_p^{<}$  e  $0 \leq k < p$  è il più piccolo indice tale che  $x_k = x_{k+1}$  definiamo

$$h(x_0, \dots, x_p) = (-1)^k (x_0, \dots, x_{k-1}, x_k, x_k, x_{k+1}, \dots, x_p).$$

Si noti che  $(x_0, \dots, x_{k-1}, x_k, x_k, x_{k+1}, \dots, x_p)$  contiene, nelle posizioni  $k, k+1, k+2$  tre vertici consecutivi uguali. Se proviamo che

$$(dh + hd)(x_0, \dots, x_p) = \begin{cases} 0 & \text{se } (x_0, \dots, x_p) \in K_p^{<}, \\ (x_0, \dots, x_p) & \text{se } (x_0, \dots, x_p) \in K_p^{\leq} - K_p^{<}, \end{cases}$$

allora l'estensione lineare di  $h$  a tutto  $C_*(K, \leq)$  soddisfa la condizione  $dh + hd = \text{Id} - i\pi$ .

Se  $(x_0, \dots, x_p) \in K_p^{<}$ , si ha banalmente che  $(dh + hd)(x_0, \dots, x_p) = 0$ . Esaminiamo quindi il caso  $(x_0, \dots, x_p) \in K_p^{\leq} - K_p^{<}$  e sia  $0 \leq k < p$  il più piccolo indice tale che  $x_k = x_{k+1}$ . Per definizione

$$h(x_0, \dots, x_p) = (-1)^k (x_0, \dots, x_k, x_k, x_{k+1}, \dots, x_p),$$

da cui

$$\begin{aligned}
dh(x_0, \dots, x_p) &= (-1)^k \sum_{j=0}^{k-1} (-1)^j (x_0, \dots, \widehat{x}_j, \dots, x_{k-1}, x_k, x_k, x_{k+1}, \dots, x_p) \\
&\quad + (-1)^{2k} (x_0, \dots, x_p) + (-1)^{2k+1} (x_0, \dots, x_p) + (-1)^{2(k+1)} (x_0, \dots, x_p) \\
&\quad + (-1)^k \sum_{j=k+2}^p (-1)^{j+1} (x_0, \dots, x_k, x_k, x_{k+1}, x_{k+2}, \dots, \widehat{x}_j, \dots, x_p) \\
&= (-1)^k \sum_{j=0}^{k-1} (-1)^j (x_0, \dots, \widehat{x}_j, \dots, x_{k-1}, x_k, x_k, x_{k+1}, \dots, x_p) \\
&\quad + (x_0, \dots, x_p) \\
&\quad + (-1)^k \sum_{j=k+2}^p (-1)^{j+1} (x_0, \dots, x_k, x_k, x_{k+1}, x_{k+2}, \dots, \widehat{x}_j, \dots, x_p).
\end{aligned}$$

Usando il fatto che  $x_k = x_{k+1}$  possiamo scrivere

$$d(x_0, \dots, x_p) = \sum_{j=0}^{k-1} (-1)^j (x_0, \dots, \widehat{x}_j, \dots, x_p) + \sum_{j=k+2}^p (-1)^j (x_0, \dots, \widehat{x}_j, \dots, x_p),$$

$$\begin{aligned}
hd(x_0, \dots, x_p) &= (-1)^{k-1} \sum_{j=0}^{k-1} (-1)^j (x_0, \dots, \widehat{x}_j, \dots, x_{k-1}, x_k, x_k, x_{k+1}, \dots, x_p) \\
&\quad + (-1)^k \sum_{j=k+2}^p (-1)^j (x_0, \dots, x_k, x_k, x_{k+1}, \dots, \widehat{x}_j, \dots, x_p).
\end{aligned}$$

e sommando otteniamo

$$(dh + hd)(x_0, \dots, x_p) = (x_0, \dots, x_p).$$

□

La dimostrazione che l'inclusione  $i: C_*(K, \leq) \hookrightarrow C_*(K)$  induce un isomorfismo in omologia è simile ma decisamente più complicata. In realtà, con una dimostrazione ancora più difficile si potrebbe anche dimostrare che  $i$  è una equivalenza omotopica (ma noi non lo faremo!).

Useremo il seguente approccio: si introduce una successione numerabile di sottocomplessi

$$C_*(K, \leq) = C^0 \subset C^1 \subset \dots \subset C_*(K)$$

tali che:

- (1) le inclusioni  $C^k \subset C^{k+1}$  inducono isomorfismi in omologia;
- (2)  $H_n(C^k) = H_n(C_*(K))$  per ogni  $k > n$ .

Le precedenti proprietà implicano che per ogni  $n \geq 0$  si ha

$$H_n(C_*(K, \leq)) = H_n(C^0) = H_n(C^1) = \dots = H_n(C^{n+1}) = H_n(C_*(K)),$$

e quindi che l'inclusione  $C_*(K, \leq) \subseteq C_*(K)$  è un isomorfismo in omologia.

Faremo uso del seguente lemma di algebra omologica.

**LEMMA 3.4.3.** *Siano  $C$  un complesso di catene e  $D \subset C$  un sottocomplesso. Se esiste una omotopia  $h: C \rightarrow C[1]$  tale che:*

- (1)  $h(D) \subset D$ ;
- (2) l'immagine di  $f := \text{Id}_C - dh - hd: C \rightarrow C$  è contenuta in  $D$ ;

allora l'inclusione  $D \subset C$  è una equivalenza omotopica e quindi induce un isomorfismo in omologia:  $H_n(D) = H_n(C)$  per ogni  $n$ .

DIMOSTRAZIONE. Iniziamo dimostrando che  $f: C \rightarrow D$  è un morfismo di complessi: siccome  $d^2 = 0$  si ha

$$df = d(\text{Id} - dh - hd) = d - d^2h - dh d = d - dh d = d - dh d - h d^2 = (\text{Id} - dh - hd)d = f d.$$

Se denotiamo con  $i: D \rightarrow C$  l'inclusione e con  $k$  la restrizione di  $h$  a  $D$  si ha

$$\text{Id}_D - fi = kd + dk, \quad \text{Id}_C - if = hd + dh.$$

□

Torniamo al nostro complesso simpliciale astratto  $(K, I)$  dotato di un ordinamento totale  $\leq$  su  $I$ .

Per ogni coppia di interi non negativi  $p, k \geq 0$  consideriamo il sottoinsieme di semplici orientati:

$$K_p^k = \{(x_0, \dots, x_p) \in K_p \mid x_0 \leq x_1 \leq \dots \leq x_{p-k}\}.$$

Osserviamo che:

- (1)  $K_p^k = K_p$  per ogni  $k \geq p$ ;
- (2)  $K_p^0 = \{(x_0, \dots, x_p) \in K_p \mid x_0 \leq x_1 \leq \dots \leq x_p\} = K_p^{\leq}$ .
- (3) se  $(x_0, \dots, x_p) \in K_p^k$ , allora  $(x_0, \dots, \widehat{x}_i, \dots, x_p) \in K_{p-1}^k$  per ogni  $i = 0, \dots, p$ .

Definiamo quindi  $C^k$  come il sottocomplesso di  $C_*(K)$  tale che  $C_p^k \subset C_p(K)$  è il sottogruppo generato da  $K_p^k$ . Siccome  $C_p^k = C_p(K)$  per ogni  $k \geq p$  si ha che l'inclusione  $C^k \subset C(K)$  induce un isomorfismo  $H_p(C^k) = H_p(C_*(K))$  per ogni  $k > p$ .

LEMMA 3.4.4. *Per ogni  $k \geq 0$  fissato l'inclusione di complessi di catene  $C^k \subset C^{k+1}$  è un quasi-isomorfismo.*

DIMOSTRAZIONE. Consideriamo l'omotopia  $h: C^{k+1} \rightarrow C^{k+1}[1]$  definita sui generatori, ossia sui semplici  $(x_0, \dots, x_p) \in K_p^{k+1}$  con  $x_0 \leq \dots \leq x_{p-k-1}$ , come

$$h(x_0, \dots, x_p) = 0 \quad \text{se } k > p,$$

mentre se  $k \leq p$  poniamo

$$h(x_0, \dots, x_p) = (-1)^j (x_0, \dots, x_{j-1}, x_{p-k}, x_j, \dots, x_p)$$

dove  $0 \leq j \leq p - k$  è il più piccolo indice tale che  $x_{p-k} \leq x_j$ . L'omotopia  $h$  risulta ben definita in quanto

$$x_0 \leq \dots \leq x_{j-1} \leq x_{p-k} \leq x_j \leq \dots \leq x_{p-k-1}.$$

Si osserva che  $h(C_p^k) \subset C_{p+1}^k$  e quindi, per il Lemma 3.4.3 basta dimostrare che

$$(3.4) \quad (dh + hd - \text{Id})(C_p^{k+1}) \subseteq C_p^k$$

per ogni  $p$ .

Se  $k \geq p$  l'inclusione (3.4) è ovvia in quanto  $C_p^k = C_p^{k+1}$ ; supponiamo quindi  $k < p$ .

Fissiamo  $(x_0, \dots, x_p) \in K_p^{k+1}$  (quindi  $x_0 \leq \dots \leq x_{p-k-1}$ ) e sia  $0 \leq j \leq p - k$  è il più piccolo indice tale che  $x_{p-k} \leq x_j$ . Si ha

$$h(x_0, \dots, x_p) = (-1)^j (x_0, \dots, x_{j-1}, x_{p-k}, x_j, \dots, x_p),$$

$$(x_0, \dots, x_{j-1}, x_{p-k}, x_j, \dots, \widehat{x}_h, \dots, x_p) \in K_p^k \quad \text{per ogni } h \geq p - k,$$

e quindi

$$\begin{aligned} dh(x_0, \dots, x_p) &= (-1)^j d(x_0, \dots, x_{j-1}, x_{p-k}, x_j, \dots, x_p) \\ &= (-1)^j \sum_{l=0}^{j-1} (-1)^l (x_0, \dots, \widehat{x}_l, \dots, x_{j-1}, x_{p-k}, x_j, \dots, x_p) + (-1)^{2j} (x_0, \dots, x_p) \\ &\quad + (-1)^j \sum_{l=j}^{p-k-1} (-1)^{l+1} (x_0, \dots, x_{j-1}, x_{p-k}, x_j, \dots, \widehat{x}_l, \dots, x_{p-k-1}, x_{p-k}, \dots, x_p) + y, \end{aligned}$$

per un opportuno elemento  $y \in C_p^k$ . Similmente:

$$\begin{aligned} d(x_0, \dots, x_p) &= \sum_{l=0}^{j-1} (-1)^l (x_0, \dots, \widehat{x}_l, \dots, x_{j-1}, \dots, x_p) \\ &\quad + \sum_{l=j}^{p-k-1} (-1)^l (x_0, \dots, x_j, \dots, \widehat{x}_l, \dots, x_{p-k-1}, \dots, x_p) + z, \end{aligned}$$

con  $z \in C_{p-1}^k$ , da cui

$$\begin{aligned} hd(x_0, \dots, x_p) &= (-1)^{j-1} \sum_{l=0}^{j-1} (-1)^l (x_0, \dots, \widehat{x}_l, \dots, x_{j-1}, x_{p-k}, x_j, \dots, x_p) \\ &\quad + (-1)^j \sum_{l=j}^{p-k-1} (-1)^l (x_0, \dots, x_j, x_{p-k}, x_j, \dots, \widehat{x}_l, \dots, x_{p-k-1}, \dots, x_p) + h(z). \end{aligned}$$

Sommando si ottiene

$$(dh + hd)(x_0, \dots, x_p) = (x_0, \dots, x_p) + y + h(z).$$

□

Adesso il Teorema 3.4.1 segue immediatamente dai lemmi precedenti e dal fatto che  $H_p(C^k) = H_p(C_*(K))$  per ogni  $k > p$ .

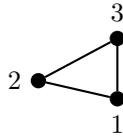
**COROLLARIO 3.4.5.** *Per un complesso simpliciale astratto  $K$  si ha  $H_n(K) = 0$  per ogni  $n > \dim K$ .*

**DIMOSTRAZIONE.** Scegliamo un ordinamento totale  $\leq$  dei vertici, allora  $K_n^< = \emptyset$  per ogni  $n > \dim K$  e quindi  $C_n(K, <) = 0$  per ogni  $n > \dim K$ . A maggior ragione  $H_n(K) = H_n(C_*(K, <)) = 0$  per ogni  $n > \dim K$ . □

Usando il complesso  $C_*(K, <)$  delle catene ordinate possiamo calcolare direttamente, se necessario con l'aiuto del computer, l'omologia di alcuni complessi simpliciali astratti.

Infatti, per ogni  $p \geq 0$  l'ordinamento sui vertici si estende, in maniera lessicografica ad un ordinamento totale sull'insieme dei  $p$ -simplessi e quindi definisce in maniera univoca un isomorfismo  $C_p(K, <) = \mathbb{Z}^{k_p}$ , dove  $k_p$  denota il numero dei simplessi di  $K$  di dimensione  $p$ .

**ESEMPIO 3.4.6.** Nel triangolo vuoto di vertici 1, 2, 3



la base canonica di  $C_0$  è  $(1), (2), (3)$  mentre la base canonica di  $C_1$  è  $(1, 2), (1, 3), (2, 3)$ . Il differenziale

$$C_1 = \oplus_{i < j} \mathbb{Z}(i, j) \xrightarrow{d} \oplus_i \mathbb{Z}(i) = C_0$$

è

$$d(a(1, 2) + b(1, 3) + c(2, 3)) = (-a - b)(1) + (a - c)(2) + (c + b)(3),$$

ed è rappresentato dalla matrice

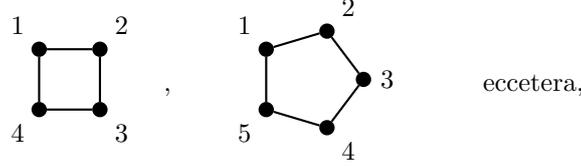
$$D = \begin{pmatrix} -1 & -1 & 0 \\ 1 & 0 & -1 \\ 0 & 1 & 1 \end{pmatrix} \in M_{3,3}(\mathbb{Z}).$$

Per connessione  $H_0 = \mathbb{Z}$ , mentre

$$H_1 = \ker(d) = \{(a, b, c) \mid a = c = -b\} = \{(n, -n, n) \mid n \in \mathbb{Z}\} \cong \mathbb{Z}$$

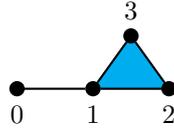
è il sottogruppo generato dal ciclo  $(1, 2) - (1, 3) + (2, 3)$ .

Aggiungendo baricentri a semplici massimali si ottengono i grafi



che pertanto hanno la stessa omologia del triangolo vuoto.

ESEMPIO 3.4.7. Sia  $K$  il complesso simpliciale astratto



Nel complesso delle catene ordinate di  $K$  le basi canoniche di  $C_0(K, <)$ ,  $C_1(K, <)$  e  $C_2(K, <)$  sono rispettivamente:

- $(0), (1), (2), (3)$ ;
- $(0, 1), (1, 2), (1, 3), (2, 3)$ ;
- $(1, 2, 3)$ .

I differenziali sono dati dalle matrici

$$D_1 = \begin{pmatrix} -1 & 0 & 0 & 0 \\ 1 & -1 & -1 & 0 \\ 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & 1 \end{pmatrix}, \quad D_2 = \begin{pmatrix} 0 \\ 1 \\ -1 \\ 1 \end{pmatrix}$$

(esercizio: perché?). Dato che  $K$  è un cono già sappiamo come è fatta l'omologia senza bisogno di proseguire i calcoli.

Usando i complessi delle catene ordinate possiamo dare una diversa alternativa del calcolo dell'omologia delle sfere (Proposizione 3.3.6).

PROPOSIZIONE 3.4.8. Sia  $S^{n-1} = \Delta^n - \{0, 1, \dots, n\}$ ,  $n \geq 2$ . Allora

$$H_0(S^{n-1}) = H_{n-1}(S^{n-1}) = \mathbb{Z}, \quad H_i(S^{n-1}) = 0 \text{ per ogni } i \neq 0, n-1.$$

DIMOSTRAZIONE. Il caso  $n = 2$  è già stato analizzato nell'Esempio 3.4.6; possiamo quindi considerare il caso  $n > 2$ .

Si osservi che  $C_p(S^{n-1}, <) = C_p(\Delta^n, <)$  per ogni  $p \neq n$  e  $C_n(\Delta^n, <) = \mathbb{Z}(0, 1, \dots, n) \cong \mathbb{Z}$ . Sia  $E$  il complesso di catene che vale  $E_n = C_n(\Delta^n, <)$  e  $E_p = 0$  per ogni  $p \neq n$ , allora l'inclusione  $C(K, <) \subset C(\Delta^n, <)$  si estende in maniera ovvia ad una successione esatta corta di complessi

$$0 \rightarrow C(S^{n-1}, <) \rightarrow C(\Delta^n, <) \rightarrow E \rightarrow 0$$

e la successione esatta lunga di omologia ci fornisce le successioni esatte

$$H_{p+1}(E) \rightarrow H_p(S^{n-1}) \rightarrow H_p(\Delta^n) \rightarrow H_p(E)$$

e siccome  $H_{p+1}(E) = H_p(E) = 0$  per ogni  $p \neq n-1, n$  si ha che  $H_p(S^{n-1}) = H_p(\Delta^n)$  per ogni  $p < n-1$ . Si ha poi una successione esatta

$$0 = H_n(\Delta^n) \rightarrow H_n(E) = \mathbb{Z} \rightarrow H_{n-1}(S^{n-1}) \rightarrow H_{n-1}(\Delta^n) = 0$$

da cui segue  $H_{n-1}(S^{n-1}) = \mathbb{Z}$ . Infine se  $p > n$  si ha  $C_p(S^{n-1}, <) = 0$  ed a maggior ragione  $H_p(S^{n-1}) = 0$ .  $\square$

### 3.5. Numeri di Betti e caratteristica di Eulero-Poincaré

La **caratteristica di Eulero-Poincaré** di un complesso simpliciale astratto finito  $K$  si definisce mediante la formula

$$\chi(K) = \sum_{n=0}^{\dim K} (-1)^n k_n,$$

dove  $k_n$  indica il numero di semplici di dimensione  $n$  in  $K$ .

Per un complesso simpliciale astratto finito  $K$  i gruppi  $C_p(K)$  sono tutti finitamente generati e quindi pure tutti i gruppi di omologia  $H_n(K)$  sono finitamente generati. I loro ranghi vengono detti **numeri di Betti** e sono denotati  $b_n(K) = \text{rank } H_n(K)$ .

Fissiamo un ordinamento totale sui vertici di  $K$ , abbiamo visto che la sua estensione lessicografica determina un ordinamento totale in  $K_n^<$  per ogni  $n$  e quindi degli isomorfismi canonici  $C_n(K, <) \simeq \mathbb{Z}^{k_n}$ .

Tramite questi isomorfismi possiamo scrivere il complesso delle catene ordinate nella forma

$$\dots \mathbb{Z}^{k_{n+1}} \xrightarrow{d_{n+1}} \mathbb{Z}^{k_n} \xrightarrow{d_n} \mathbb{Z}^{k_{n-1}} \rightarrow \dots \xrightarrow{d_1} \mathbb{Z}^{k_0}.$$

Ogni morfismo  $d_i$  si rappresenta con una matrice a coefficienti interi; applicando il teorema del rango 2.6.13 si ha la formula

$$(3.5) \quad b_n(K) = k_n - \text{rank } d_n - \text{rank } d_{n+1}$$

dove si conviene che  $d_i = 0$  per ogni  $i \leq 0$  ed ogni  $i > \dim K$ .

Ad esempio, per il complesso simpliciale  $K = \Delta^m$ , per ogni  $n = 0, \dots, m$  si ha  $k_n = \binom{m+1}{n+1}$  e quindi

$$\chi(\Delta^m) = \sum_{n=0}^m (-1)^n \binom{m+1}{n+1} = 1 - \sum_{i=0}^{m+1} (-1)^i \binom{m+1}{i} = 1 - (1-1)^{m+1} = 1.$$

La caratteristica di Eulero-Poincaré è quindi una quantità di facile calcolo la cui importanza si deve al fatto che dipende solo dall'omologia di  $K$ .

**TEOREMA 3.5.1** (di Eulero-Poincaré). *Dato un complesso simpliciale astratto finito  $K$  si ha*

$$\chi(K) = \sum_{n=0}^{\dim K} (-1)^n b_n(K) = \sum_{n=0}^{\dim K} (-1)^n \text{rank } H_n(K).$$

**DIMOSTRAZIONE.** Per una dimostrazione immediata basta prendere la somma a segni alterni di tutte le uguaglianze (3.5).

Possiamo anche evitare di usare il teorema del rango seguendo il seguente ragionamento. Sia  $d$  la dimensione di  $K$ , possiamo allora fissare un ordinamento totale sui vertici e calcolare l'omologia usando il complesso delle catene ordinate:

$$0 \rightarrow C_d(K, <) \xrightarrow{d} \dots C_1(K, <) \xrightarrow{d} C_0(K, <) \rightarrow 0.$$

Per costruzione ciascun  $C_n(K, <)$  è un gruppo abeliano libero di rango  $k_n$  ed il complesso di catene ordinate si spezza in una serie di successioni esatte corte di gruppi abeliani finitamente generati:

$$0 \rightarrow Z_n \rightarrow C_n(K, <) \rightarrow B_{n-1} \rightarrow 0, \quad 0 \rightarrow B_n \rightarrow Z_n \rightarrow H_n(K) \rightarrow 0.$$

Per l'additività del rango si ha quindi per ogni  $n$ :

$$k_n = \text{rank } C_n(K, <) = \text{rank } Z_n + \text{rank } B_{n-1}, \quad b_n(K) = \text{rank } H_n(K) = \text{rank } Z_n - \text{rank } B_n$$

e quindi

$$\begin{aligned} \sum_n (-1)^n (k_n - b_n(K)) &= \sum_n (-1)^n (\text{rank } B_{n-1} + \text{rank } B_n) \\ &= \sum_n ((-1)^n + (-1)^{n-1}) \text{rank } B_n = 0. \end{aligned}$$

□

ESEMPIO 3.5.2. Usiamo le formule (3.5) per calcolare i numeri di Betti della 2-sfera simpliciale  $S = \Delta^{\{0,1,2,3\}} - \{0,1,2,3\}$ . Si ha  $k_0 = k_2 = 4$ ,  $k_1 = 6$  ed i differenziali  $d_1, d_2$  del complesso delle catene ordinate sono rappresentati dalle matrici

$$D_1 = \begin{pmatrix} -1 & -1 & -1 & 0 & 0 & 0 \\ 1 & 0 & 0 & -1 & -1 & 0 \\ 0 & 1 & 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix} \quad D_2 = \begin{pmatrix} 1 & 1 & 0 & 0 \\ -1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & 1 \end{pmatrix}.$$

Applicando il procedimento di eliminazione di Gauss si vede facilmente che  $D_1$  e  $D_2$  hanno entrambe rango 3, e quindi

$$b_0 = 4 - 3 - 0 = 1, \quad b_1 = 6 - 3 - 3 = 0, \quad b_2 = 4 - 3 = 1.$$

ESEMPIO 3.5.3. Siano  $K$  un complesso simpliciale e  $L \subset K$  un sottocomplesso tali che  $K - L$  contenga un solo elemento  $s$ , che è necessariamente un simplesso massimale in  $K$ . Se  $s$  ha dimensione  $p$ , considerando le catene ordinate (rispetto ad un qualunque ordinamento dei vertici) si ha una successione esatta di complessi

$$0 \rightarrow C_*(L, <) \rightarrow C_*(K, <) \rightarrow \mathbb{Z}[-p]s \rightarrow 0,$$

dove il complesso  $\mathbb{Z}[-p]s$  è generato da  $s$  in grado  $p$  e 0 in grado  $\neq p$ . Si ha quindi una successione esatta lunga di omologia

$$0 \rightarrow H_n(L) \rightarrow H_n(K) \xrightarrow{g} \mathbb{Z} \rightarrow H_{n-1}(L) \rightarrow H_{n-1}(K) \rightarrow 0$$

e ci sono due possibilità.

1) se  $g = 0$  allora  $H_n(L) = H_n(K)$  ed esiste una successione esatta corta  $0 \rightarrow \mathbb{Z} \rightarrow H_{n-1}(L) \rightarrow H_{n-1}(K) \rightarrow 0$ .

2) se  $g \neq 0$  allora l'immagine di  $g$  è isomorfa a  $\mathbb{Z}$ , mentre il conucleo di  $g$  è un gruppo di torsione. Si hanno dunque due successioni esatte

$$0 \rightarrow H_n(L) \rightarrow H_n(K) \xrightarrow{g} \text{Im}(g) = \mathbb{Z} \rightarrow 0, \quad 0 \rightarrow \text{coker}(g) \rightarrow H_{n-1}(L) \rightarrow H_{n-1}(K) \rightarrow 0.$$

Dalla prima segue un isomorfismo (non canonico)  $H_n(K) = H_n(L) \oplus \mathbb{Z}$ , mentre dalla seconda (vedi Esempio 2.6.11) seguono una successione esatta ed un isomorfismo

$$0 \rightarrow \text{coker}(g) \rightarrow T(H_{n-1}(L)) \rightarrow T(H_{n-1}(K)) \rightarrow 0, \quad \frac{H_{n-1}(L)}{T(H_{n-1}(L))} = \frac{H_{n-1}(K)}{T(H_{n-1}(K))}.$$

Nel primo caso  $b_{n-1}(K) = b_{n-1}(L) - 1$  e  $b_i(K) = b_i(L)$  per ogni  $i \neq n-1$ ; nel secondo caso  $b_n(K) = b_n(L) + 1$  e  $b_i(K) = b_i(L)$  per ogni  $i \neq n$ . In entrambi i casi la caratteristica di Eulero-Poincaré aumenta di  $(-1)^n$ , ossia  $\chi(K) = \chi(L) + (-1)^n$ .

TEOREMA 3.5.4. Per ogni grafo semplice finito connesso  $(V, E)$ , denotando con  $K \subset \Delta^V$  il corrispondente complesso simpliciale di dimensione  $\leq 1$ , si hanno gli isomorfismi:

$$H_0(K) = \mathbb{Z}, \quad H_1(K) = \mathbb{Z}^{|E|-|V|+1}, \quad H_n(K) = 0, \quad n > 1.$$

In particolare  $(V, E)$  è un albero se e solo se  $H_1(K) = 0$ .

DIMOSTRAZIONE. Siccome  $K$  è connesso, si ha  $H_0(K) = \mathbb{Z}$ , ed il complesso delle catene ordinate diventa

$$0 \rightarrow C_1(K, <) = \bigoplus_{e \in E} \mathbb{Z}e \xrightarrow{d} C_0(K, <) = \bigoplus_{v \in V} \mathbb{Z}v \rightarrow 0$$

da cui segue che  $H_1(K) = \ker(d)$  è un sottogruppo di  $C_1(K, <) = \mathbb{Z}^{|E|}$  ed è dunque isomorfo a  $\mathbb{Z}^r$  per qualche  $r$ . Per l'additività del rango si ha  $r = |E| - |V| + 1$ .  $\square$

OSSERVAZIONE 3.5.5. Nella dimostrazione del Teorema 3.5.4 abbiamo visto che i gruppi di omologia di un grafo connesso tengono conto solamente della caratteristica di Eulero-Poincaré e non tengono conto di altri importanti aspetti combinatori che pure risultano importanti in teoria dei grafi.

Una maniera per perdere meno informazioni è quella di trovare dei modi naturali per associare ad un grafo dei complessi simpliciali, la cui omologia riflette alcune proprietà combinatorie del grafo di partenza.

Una maniera standard è quella di considerare per ogni grafo  $\Gamma = (V, E)$  il corrispondente complesso delle cricche

$$\widehat{\Gamma} = \{\text{cricche di } \Gamma\},$$

del quale calcolare i gruppi di omologia  $H_n(\widehat{\Gamma})$  i cui elementi non banali vengono detti **cavità topologiche** di  $\Gamma$ .

Riepilogando: *la trasformazione di un grafo semplice nel corrispondente complesso di cricche ha l'effetto di trasformare alcune caratteristiche da combinatorie in topologico-omotopiche*<sup>1</sup>.

**Numeri di Betti relativi.** In previsione dello studio dell'omologia persistente è utile introdurre una versione relativa dei numeri di Betti.

**DEFINIZIONE 3.5.6.** Siano  $K$  un complesso simpliciale finito e  $L \subset K$  un sottocomplesso. Definiamo  $b_n(K, L)$  come il rango dell'immagine dell'omomorfismo  $H_n(L) \rightarrow H_n(K)$  indotto dall'inclusione  $L \hookrightarrow K$ .

Cerchiamo adesso l'analogo della Formula (3.5) per i numeri di Betti relativi. Scegliamo un ordinamento totale dei vertici di  $K$  e prendiamo l'ordinamento indotto sui vertici di  $L$ . Sotto tali ipotesi  $C_*(L, <)$  è un sottocomplesso di  $C_*(K, <)$  ed il morfismo  $H_n(L) \rightarrow H_n(K)$  è indotto dall'inclusione  $C_*(L, <) \subseteq C_*(K, <)$ . Denotiamo con:

- (1)  $a$  il rango del differenziale  $d: C_n(L, <) \rightarrow C_{n-1}(L, <)$ ,
- (2)  $b$  il rango del differenziale  $d: C_{n+1}(K, <) \rightarrow C_n(K, <)$ ,
- (3)  $c$  il rango dell'applicazione

$$f: C_n(L, <) \oplus C_{n+1}(K, <) \rightarrow C_n(K, <), \quad f(x, y) = x + dy.$$

Per quanto dimostrato nel Lemma 2.6.12, i tre numeri  $a, b, c$  coincidono con i ranghi delle matrici a coefficienti  $0, \pm 1$  che rappresentano le tre applicazioni nelle basi date dai semplici ordinati. Vale la formula:

$$(3.6) \quad b_n(K, L) = c - a - b.$$

Infatti,  $c$  è il rango di  $\text{Im}(f) = C_n(L, <) + B_n(K, <)$  e se  $l = \text{rank}(C_n(L, <))$  allora il rango di  $Z_n(L, <)$  è  $l - a$ . Dalla successione esatta

$$0 \rightarrow C_n(L, <) \cap B_n(K, <) \rightarrow C_n(L, <) \oplus B_n(K, <) \rightarrow C_n(L, <) + B_n(K, <) \rightarrow 0$$

segue che il rango di  $C_n(L) \cap B_n(K)$  è uguale a  $b + l - c$ . Per concludere basta osservare che l'immagine di  $H_n(L) \rightarrow H_n(K)$  è isomorfa al quoziente  $Z_n(L, <)/(Z_n(L, <) \cap B_n(K, <))$  e che  $Z_n(L, <) \cap B_n(K, <) = C_n(L, <) \cap B_n(K, <)$ .

Possiamo riscrivere la formula (3.6) in un modo funzionale ai calcoli nel modo seguente. Per ogni  $n$  denotiamo con  $k_n$  (risp.:  $l_n$ ) il numero degli  $n$ -simplessi ordinati di  $K$  (risp.: di  $L$ ). Ordiniamo poi  $K_n^<$  in modo tale che i primi  $l_n$  elementi siano gli  $n$ -simplessi ordinati di  $L$ . Otteniamo quindi una base di  $C_n(K, <)$  i cui primi elementi sono una base di  $C_n(L, <)$ . Rispetto a tali basi i differenziali  $d: C_{n+1}(L, <) \rightarrow C_n(L, <)$ , e  $d: C_{n+1}(K, <) \rightarrow C_n(K, <)$  sono definiti rispettivamente mediante matrici  $A_n$  e  $B_n$ . Nelle notazioni precedenti  $a = \text{rank}(A_{n-1})$ ,  $b = \text{rank}(B_n)$ . Inoltre  $B_n$  è una matrice a blocchi

$$B_n = \begin{pmatrix} A_n & U_n \\ 0 & C_n \end{pmatrix}.$$

Allora si ha  $c = l_n + \text{rank}(C_n)$  e quindi

$$(3.7) \quad b_n(K, L) = l_n + \text{rank}(C_n) - \text{rank}(A_{n-1}) - \text{rank}(B_n).$$

<sup>1</sup>In attesa di maggiori chiarimenti, possiamo provvisoriamente interpretare il termine topologico-omotopico come osservabile mediante gli strumenti tipici della topologia algebrica, quali ad esempio i gruppi di omologia.

Infatti, se  $V \subset C_{n+1}(K, <)$  indica il sottogruppo generato dagli ultimi  $k_{n+1} - l_{n+1}$  elementi della base, l'immagine di  $f$  è uguale all'immagine della sua restrizione al sottospazio  $C_n(L, <) \oplus V$ , che è rappresentata nelle basi date dalla matrice a blocchi

$$\begin{pmatrix} I & U_n \\ 0 & C_n \end{pmatrix}$$

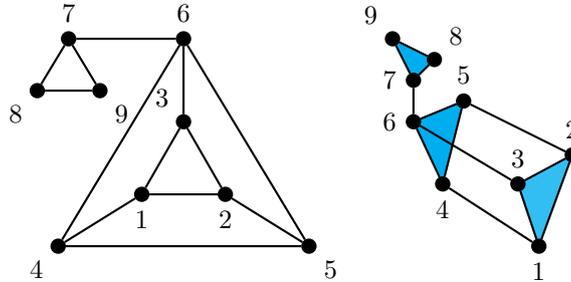
il cui rango è  $l_n + \text{rank}(C_n)$ .

**Esercizi:**

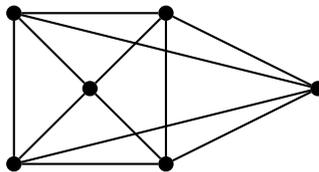
ESERCIZIO 25. Siano  $\Gamma = (V, E)$  un grafo e  $r > 0$  un intero. Definiamo  $\Gamma_r \subset \Delta^V$  come la famiglia dei sottoinsiemi finiti e non vuoti  $W \subset V$  per cui il nel sottografo indotto di vertici  $W$ , ogni vertice ha grado  $\geq |W| - r$ .

Provare che  $\Gamma_r$  è un complesso simpliciale astratto e che  $\Gamma_1$  è il complesso di cricche del grafo  $\Gamma$ .

ESERCIZIO 26. Calcolare i gruppi di omologia del seguente grafo semplice (a sinistra) e del corrispondente complesso di cricche (a destra):



ESERCIZIO 27. Mostrare che il complesso di cricche del grafo



ha la stessa omologia della sfera simpliciale  $S^2$  e pertanto possiede delle cavità topologiche 2-dimensionali non banali.

**3.6. Omologia a coefficienti  $\mathbb{T}_2$  e semplici positivi**

Sia  $(K, I)$  un complesso simpliciale astratto. Abbiamo definito il gruppo delle  $p$ -catene orientate  $C_p(K)$  come il gruppo abeliano libero generato da  $K_p$ .

Analogamente possiamo definire le  $p$ -catene orientate a coefficienti in un qualunque campo  $\mathbb{K}$ . Più precisamente definiamo  $C_p(K, \mathbb{K})$  come lo spazio vettoriale su  $\mathbb{K}$  generato da  $K_p$ , ossia

$$C_p(K, \mathbb{K}) = \left\{ \sum_i a_i s_i \mid s_i \in K_p, a_i \in \mathbb{K} \text{ e } a_j \neq 0 \text{ per finiti } j \right\}.$$

La stessa formula del differenziale su  $C_*(K)$  definisce un differenziale. I corrispondenti gruppi di omologia, che a posteriori sono spazi vettoriali su  $\mathbb{K}$ , vengono denotati  $H_n(K, \mathbb{K})$ .

Dal un punto di vista teorico, il calcolo dei gruppi  $H_n(K, \mathbb{K})$  non aggiunge alcuna nuova informazione, nel senso che essi sono determinati univocamente, a meno di isomorfismo, dai gruppi  $H_n(K)$ ; questo segue dal cosiddetto *teorema dei coefficienti universali*, risultato per nulla banale e non trattato in queste note.

Per un complesso simpliciale finito  $K$  segue facilmente dalla formula (3.5) che la dimensione di  $H_n(K, \mathbb{K})$  come  $\mathbb{K}$  spazio vettoriale dipende solo dalla caratteristica del campo  $\mathbb{K}$ ,

è uguale al numero di Betti  $b_n(K)$  se  $\mathbb{K}$  ha caratteristica 0 ed è maggiore od uguale a  $b_n(K)$  se  $\mathbb{K}$  ha caratteristica positiva.

Sebbene meno informativi rispetto ai gruppi di omologia “tradizionali”, i gruppi  $H_n(K, \mathbb{K})$  hanno il vantaggio di essere più facilmente calcolabili. Ciò è particolarmente vero quando  $\mathbb{K}$  è il campo con due elementi, ossia  $\mathbb{K} = \mathbb{T}_2 = \{0, 1\}$ . Siccome  $1 = -1$  in  $\mathbb{T}_2$ , il differenziale  $d_p: C_p(K, \mathbb{T}_2) \rightarrow C_{p-1}(K, \mathbb{T}_2)$  assume la forma semplificata

$$d_p(x_0, \dots, x_p) = \sum_{i=0}^p (x_0, \dots, \hat{x}_i, \dots, x_p).$$

Possiamo fare di meglio definendo  $D_p(K)$  come lo spazio vettoriale su  $\mathbb{T}_2$  generato dai semplici di  $K$  di dimensione  $p$ :

$$D_p(K) = \left\{ \sum_i a_i s_i \mid s_i \in K, \dim s_i = p, a_i \in \mathbb{T}_2, a_j = 1 \text{ per finiti } j \right\}.$$

Consideriamo poi le applicazioni lineari  $d: D_p(K) \rightarrow D_{p-1}(K)$  definite sugli elementi della base come

$$d\{x_0, \dots, x_p\} = \sum_{i=0}^p \{x_0, \dots, \hat{x}_i, \dots, x_p\},$$

ossia

$$s \in K, \dim s = p \quad \Rightarrow \quad d(s) = \sum_{t \subset s, \dim t = p-1} t.$$

**TEOREMA 3.6.1.** *Il diagramma di applicazioni*

$$\dots \rightarrow D_p(K) \xrightarrow{d} D_{p-1} \rightarrow \dots \xrightarrow{d} D_0 \rightarrow 0$$

è un complesso i cui gruppi di omologia sono  $H_n(K, \mathbb{T}_2)$ .

**DIMOSTRAZIONE.** Scegliamo un ordinamento totale  $\leq$  sull'insieme dei vertici di  $K$ . Le stesse argomentazioni fatte precedentemente mostrano che i gruppi di omologia del sottocomplesso delle catene ordinate  $C_*(K, \mathbb{T}_2, <)$ , dove

$$C_p(K, \mathbb{T}_2, <) = \left\{ \sum a_i (x_0, \dots, x_p) \mid a_i \in \mathbb{T}_2, x_0 < \dots < x_p \right\},$$

sono gli stessi del complesso  $C_*(K, \mathbb{T}_2, <)$ .

Basta adesso osservare che le applicazioni lineari

$$C_p(K, \mathbb{T}_2, <) \rightarrow D_p(K), \quad (x_0, \dots, x_p) \mapsto \{x_0, \dots, x_p\},$$

definiscono un isomorfismo di complessi.  $\square$

Anche grazie al teorema precedente, il calcolo dei gruppi  $H_n(K, \mathbb{T}_2)$  è molto più semplice dal punto di vista algoritmico e computazionale rispetto al calcolo di  $H_n(K)$ , e questo rappresenta un vantaggio specialmente per complessi simpliciali molto grandi.

Un celebre algoritmo per il calcolo dell'omologia a coefficienti in  $\mathbb{T}_2$  prevede che un complesso simpliciale finito  $K$  sia dotato del seguente dato aggiuntivo:

**Dato aggiuntivo:** Una numerazione dei semplici

$$K = \{s_1, s_2, \dots, s_N\}$$

tale che, per ogni  $1 \leq h \leq N$  la sottofamiglia

$$K^h = \{s_1, s_2, \dots, s_h\}$$

sia un sottocomplesso simpliciale.

Equivalentemente, viene dato su  $K$  un ordinamento totale  $\leq$  tale che per ogni  $\sigma \in \mathbb{K}$  il suo segmento iniziale  $\{\tau \in K \mid \tau \leq \sigma\}$  è un sottocomplesso.

Un tale dato aggiuntivo esiste sempre: ad esempio possiamo prima numerare i vertici,  $s_1, \dots, s_{N_1}$ , poi i semplici di dimensione 1,  $s_{N_1+1}, \dots, s_{N_2}$ , poi i semplici di dimensione 2 e così via.

DEFINIZIONE 3.6.2. Nelle notazioni precedenti, il semplice  $s_h$  si dice **positivo** se compare con coefficiente 1 in un ciclo di  $D_*(K^h)$ . Altrimenti si dice **negativo**.

Più precisamente, un  $s_h$  è positivo se e solo se esistono  $1 \leq i_1 < i_2 < \dots < i_r < h$  tali che  $\dim s_{i_j} = \dim s_h$  per ogni  $j = 1, \dots, r$  e

$$d\left(s_h + \sum_j s_{i_j}\right) = 0.$$

È chiaro che ogni 0-simplesso è positivo, mentre la distinzione dei semplici di dimensione superiore in positivi e negativi dipende dalla scelta dell'ordinamento su  $K$ . È utile osservare che il semplice  $s_h$  è positivo in  $K$  se e solo se è positivo in  $K^h$ .

ESEMPIO 3.6.3. Sia  $\sigma \in K$  un  $p$ -simplesso non massimale. Allora il primo  $(p+1)$ -simplesso  $\tau$  che contiene  $\sigma$  è negativo.

Infatti, per ogni scelta di  $\tau_1, \dots, \tau_k < \tau$  nel differenziale  $d(\tau + \sum \tau_i)$  il semplice  $\sigma$  compare con coefficiente 1.

Introduciamo alcune notazioni:

- (1) per ogni  $h$ , sia  $P_p(K^h) \subset D_p(K^h)$  il sottospazio vettoriale generato dai  $p$ -simplessi positivi di  $K^h$ ;
- (2) per ogni  $h$ , sia  $N_p(K^h) \subset D_p(K^h)$  il sottospazio vettoriale generato dai  $p$ -simplessi negativi di  $K^h$ .

Chiaramente  $D_p(K^h) = P_p(K^h) \oplus N_p(K^h)$ .

LEMMA 3.6.4. *Nelle notazioni precedenti, per ogni  $h, p$  l'applicazione  $d: N_p(K^h) \rightarrow D_{p-1}(K^h)$  è iniettiva.*

DIMOSTRAZIONE. Supponiamo per assurdo che esista  $v \in N_p(K^h)$  tale che  $dv = 0$  e  $v \neq 0$ . Allora  $v = s_{i_1} + \dots + s_{i_k}$  con  $k > 0$ ,  $i_1 < i_2 < \dots < i_k$  ed ogni  $s_{i_j}$  un  $p$ -simplesso negativo. Ma questo è assurdo perché la condizione  $dv = 0$  implica che  $s_{i_k}$  è positivo.  $\square$

LEMMA 3.6.5. *Nella situazione precedente, sia  $s_h$  un  $p$ -simplesso positivo. Allora esiste un'unico vettore  $v_h \in N_p(K^{h-1})$  tale che  $d(s_h + v_h) = 0$ .*

DIMOSTRAZIONE. Dimostriamo prima l'unicità. Siano  $v_h, w_h \in N_p(K^{h-1})$  tali che  $d(s_h + v_h) = d(s_h + w_h) = 0$ ; allora  $d(v_h - w_h) = 0$  e  $v_h = w_h$  per il lemma precedente.

Dimostriamo l'esistenza per induzione su  $h$ . Siccome  $s_h$  è positivo esiste un vettore  $u \in D_p(K^{h-1})$  tale che  $d(s_h + u) = 0$ ; scriviamo  $u = v + w$  con  $v \in N_p(K^{h-1})$  e  $w \in P_p(K^{h-1})$ .

Se  $w = s_{i_1} + \dots + s_{i_k}$ , con ogni  $s_{i_j}$  positivo, per l'ipotesi induttiva esistono vettori  $v_1, \dots, v_k \in N_p(K^{h-1})$  tali che  $d(s_{i_j} + v_j) = 0$  per ogni  $j$ . Ma allora  $dw = d(\sum_j v_j)$  e di conseguenza  $d(s_h + v + \sum_j v_j) = 0$ .  $\square$

Il lemmi precedenti ci offrono un metodo ricorsivo per classificare i semplici in positivi e negativi. Sia  $h = 1, \dots, N$  e supponiamo di aver già determinato il sottoinsieme dei semplici negativi di  $K^{h-1}$ . Se  $p = \dim s_h$  e  $s_{i_1}, \dots, s_{i_k}$  sono i  $p$ -simplessi negativi di  $K^{h-1}$ , allora  $s_h$  è positivo se e solo se i vettori  $ds_h, ds_{i_1}, \dots, ds_{i_k}$  sono linearmente dipendenti in  $D_{p-1}(K^h)$ .

TEOREMA 3.6.6. *Nelle notazioni precedenti,  $\dim H_p(K, \mathbb{T}_2) = \dim P_p(K) - \dim N_{p+1}(K)$ , ossia la dimensione di  $H_p(K, \mathbb{T}_2)$  è uguale alla differenza tra il numero dei  $p$ -simplessi positivi ed il numero dei  $(p+1)$ -simplessi negativi.*

DIMOSTRAZIONE. Per ogni  $q$  si consideri l'applicazione lineare  $f: D_q(K) \rightarrow D_q(K)$  definita sui  $q$ -simplessi da  $f(s_h) = s_h$  se  $s_h$  è negativo,  $f(s_h) = s_h + v_h$  se  $s_h$  è positivo, dove  $v_h \in N_q(K^{h-1})$  è il vettore descritto nel Lemma 3.6.5.

Nella base data dai  $q$ -simplessi, l'applicazione  $f$  si rappresenta con una matrice triangolare con tutti 1 sulla diagonale. Quindi  $f$  è un isomorfismo e si ha  $D_q(K) = f(N_q(K)) \oplus f(P_q(K)) = N_q(K) \oplus f(P_q(K))$ . Siccome  $d(s_h + v_h) = 0$  si ha  $f(P_q(K)) \subset \ker d$  e quindi  $D_q(K) = N_q(K) + \ker d$ . D'altra parte, per il Lemma 3.6.4  $N_q(K) \cap \ker d = 0$  e quindi  $D_q(K) = N_q(K) \oplus \ker d$ .

Per concludere basta osservare che  $f$  determina un isomorfismo tra  $P_p(K)$  ed il nucleo di  $d: D_p(K) \rightarrow D_{p-1}(K)$  e che l'immagine di  $d: D_{p+1}(K) \rightarrow D_p(K)$  è uguale all'immagine dell'applicazione iniettiva  $d: N_{p+1}(K) \rightarrow D_p(K)$ .  $\square$

**Un possibile algoritmo.** Fissato un intero  $p \geq 0$  siamo interessati a calcolare la dimensione  $\beta^{h,l}$  dell'immagine del morfismo  $H_p(K^h, \mathbb{T}_2) \rightarrow H_p(K^l, \mathbb{T}_2)$  indotto dall'inclusione  $K^h \subset K^l$  per ogni coppia di indici  $1 \leq h \leq l \leq N$ .

*Primo passo:* Per ogni  $h$  ed ogni  $r \geq 0$  si determina il numero  $(r, h) \in \mathbb{N}$  degli  $r$ -simplessi contenuti in  $K^h$ ; dunque  $\sum_r (r, h) = h$  per ogni  $h$ .

*Secondo passo:* Per ogni  $r$  si prendono in ordine crescente gli  $r$ -simplessi  $\tau_1^r, \dots, \tau_{(r,N)}^r$  di  $K = K^N$  e si denota con

$$\alpha_r: \{1, \dots, (r, N)\} \rightarrow \{1, \dots, N\}$$

l'applicazione strettamente crescente tale che  $\tau_i^r = \sigma_{\alpha_r(i)}$ .

*Terzo passo:* per ogni  $h$  determiniamo i  $p+1$ -simplessi negativi di  $K^h$  ed il loro numero  $(p+1, h)^-$ . A tal fine sia  $A$  la matrice, a coefficienti  $0, 1$ , del differenziale  $d: D_{p+1}(K) \rightarrow D_p(K)$  nelle basi  $\tau_1^{p+1}, \dots, \tau_{(p+1,N)}^{p+1}$  e  $\tau_1^p, \dots, \tau_{(p,N)}^p$  e sia  $B$  una sua riduzione a scala tramite operazioni sulle righe. Abbiamo dimostrato che  $\tau_i^{p+1}$  è negativo se e solo se la matrice  $B$  ha un pivot nella colonna  $i$  e quindi  $(p+1, h)^-$  è uguale al numero di indici  $i$  tali che  $\alpha_{p+1}(i) \leq h$  e  $B$  contiene un pivot nella colonna  $i$ .

*Quarto passo:* Si determinano, alla stessa maniera del terzo passo, per ogni  $h$ , il numero  $(p, h)^+$  dei  $p$ -simplessi positivi di  $K^h$ .

*Quinto passo* Sia  $C$  la sottomatrice di  $A$  (terzo passo) ottenuta considerando solo le colonne contenenti i pivot, in particolare le  $(p+1, N)^-$  colonne di  $C$  sono linearmente indipendenti. Per  $h \leq l$  fissati sia  $C_{h,l}$  la sottomatrice di  $C$  ottenuta considerando le colonne dalla  $(p+1, h)^- + 1$  alla  $(p+1, l)^-$  e le righe dalla  $(p, h) + 1$  alla  $(p, l)$ . Allora vale la formula

$$(3.8) \quad \beta^{h,l} = (p, h)^+ - (p+1, l)^- + \text{rank}(C_{h,l}).$$

Il quinto passo richiede una spiegazione; nelle notazioni della Formula (3.6), si ha  $a = (p, h)^-$ ,  $b = (p+1, l)^-$  e quindi basta dimostrare che il rango dell'applicazione

$$f: D_p(K^h) \oplus D_{p+1}(K^l) \rightarrow D_p(K^l), \quad f(x, y) = x + dy,$$

è uguale a  $(p, h) + \text{rank}(C_{h,l})$ .

Sia  $\eta_1, \dots, \eta_{(p,N)^-}$  la successione ordinata dei  $(p+1)$ -simplessi negativi. Siccome l'immagine di  $d: D_{p+1}(K^l) \rightarrow D_p(K^l)$  è uguale all'immagine di  $d: N_{p+1}(K^l) \rightarrow D_p(K^l)$ , l'immagine di  $f$  è uguale all'immagine della sua restrizione

$$f: D_p(K^h) \oplus N_{p+1}(K^l) \rightarrow D_p(K^l), \quad f(x, y) = x + dy.$$

Poi, dato che  $d(N_{p+1}(K^l)) \subset D_p(K^h)$ , possiamo sostituire a  $N_{p+1}(K^l)$  il sottospazio  $V$  generato dai simplessi negativi non contenuti in  $K^h$ .

Rispetto alle basi  $\tau_1^p, \dots, \tau_{(p,h)}^p, \eta_{(p+1,h)+1}, \dots, \eta_{(p+1,l)}$  di  $D_p(K^h) \oplus V$  e  $\tau_1^p, \dots, \tau_{(p,l)}^p$  di  $D_p(K^l)$ , l'applicazione  $f$  è data da una matrice a blocchi del tipo

$$\begin{pmatrix} I & * \\ 0 & C_{h,l} \end{pmatrix}$$

il cui rango è esattamente  $(p, h) + \text{rank}(C_{h,k})$ .

## Insiemi simpliciali e omologia singolare

*Questo capitolo può essere omissso senza pregiudicare la comprensione generale del testo*

I complessi simpliciali astratti possiedono diverse rigidità che in certi casi sono un ostacolo al buon funzionamento della teoria. Vogliamo quindi trovare un analogo concetto (non una generalizzazione, si badi bene) che permette ugualmente di produrre gruppi di omologia in maniera functoriale e che poi risulti di più agile utilizzo.

La risposta a questo problema (non banale) è stata trovata nel periodo 1960-80 da svariati matematici, primo tra tutti Daniel Kan, che hanno mostrato come la teoria degli *insiemi simpliciali* ha tutte le caratteristiche richieste, ed altre ancora che la rendono il punto di incontro di teorie matematiche apparentemente molto distanti (e quindi un argomento più che consono per un corso di Istituzioni di Algebra e Geometria).

Tra le altre cose, il passaggio dai complessi simpliciali astratti agli insiemi simpliciali permette di sostituire il concetto di contiguità con la nozione di omotopia, quest'ultima formalmente simile alla classica definizione di omotopia usata in topologia.

### 4.1. Insiemi simpliciali

Se  $n \geq 0$  è un intero non negativo denotiamo  $[n] = \{0, \dots, n\}$  considerato come insieme *ordinato*, ossia dotato della usuale relazione di ordine  $\leq$ . Scriveremo inoltre  $f: [n] \rightarrow [m]$  per indicare un'applicazione *monotona non decrescente*

$$f: \{0, \dots, n\} \rightarrow \{0, \dots, m\}, \quad f(0) \leq f(1) \leq \dots \leq f(n).$$

LEMMA 4.1.1 (Fattorizzazione epi-moni). *Ogni morfismo  $f: [n] \rightarrow [m]$  si fattorizza in modo unico come  $f = hg$  con  $g: [n] \rightarrow [p]$  surgettiva e  $h: [p] \rightarrow [m]$  iniettiva.*

DIMOSTRAZIONE. Se l'immagine  $f([n]) \subset [m]$  contiene  $p + 1$  elementi, esiste un'unica applicazione bigettiva e monotona  $h: [p] \rightarrow f([n])$  e si definisce  $g$  come la composizione

$$g: [n] \xrightarrow{f} f([n]) \xrightarrow{h^{-1}} [p].$$

□

Particolare importanza hanno i morfismi **faccia**:

$$\delta_k: [n-1] \rightarrow [n], \quad \delta_k(p) = \begin{cases} p & \text{se } p < k \\ p+1 & \text{se } p \geq k \end{cases}, \quad k = 0, \dots, n,$$

ed i morfismi **degenerazione**:

$$\sigma_k: [n+1] \rightarrow [n], \quad \sigma_k(p) = \begin{cases} p & \text{se } p \leq k \\ p-1 & \text{se } p > k \end{cases}, \quad k = 0, \dots, n.$$

Si noti che  $\delta_k: [n-1] \rightarrow [n]$  è l'unica applicazione iniettiva monotona la cui immagine non contiene  $k$  e che  $\sigma_k: [n+1] \rightarrow [n]$  è l'unica applicazione surgettiva monotona tale che il bersaglio  $k$  è colpito due volte (da  $k$  e  $k+1$ ).

Le regole di commutazione di facce e degenerazioni sono regolate dal seguente lemma.

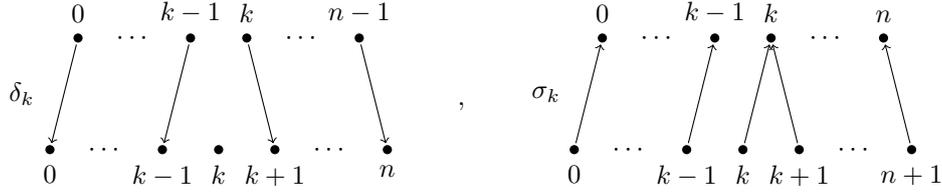


FIGURA 1. Facce e degenerazioni

LEMMA 4.1.2 (Identità cosimpliciali). *Nelle notazioni precedenti si ha*

$$(4.1) \quad \begin{aligned} \delta_i \delta_j &= \delta_{j+1} \delta_i \quad \text{per ogni } i \leq j; \\ \sigma_i \sigma_j &= \sigma_j \sigma_{i+1} \quad \text{per ogni } i \geq j; \\ \sigma_i \delta_j &= \begin{cases} \delta_{j-1} \sigma_i & \text{per ogni } j > i+1 \\ \text{Id} & \text{per } j = i, i+1 \\ \delta_j \sigma_{i-1} & \text{per ogni } j < i. \end{cases} \end{aligned}$$

DIMOSTRAZIONE. La dimostrazione è del tutto elementare ma decisamente noiosa; qui proviamo solamente le regole di commutazione delle facce e per le altre ci fidiamo dei tanti di libri di testo dove le identità cosimpliciali sono riportate (e quasi sempre lasciate per esercizio). Siano dunque  $i \leq j \leq n$ . La composizione

$$[n-1] \xrightarrow{\delta_j} [n] \xrightarrow{\delta_i} [n+1].$$

è iniettiva monotona ed il complementare dell'immagine è esattamente  $\{i, \delta_i(j)\} = \{i, j+1\}$ . Analogamente, la composizione

$$[n-1] \xrightarrow{\delta_i} [n] \xrightarrow{\delta_{j+1}} [n+1].$$

è iniettiva monotona ed il complementare dell'immagine è esattamente  $\{j+1, \delta_{j+1}(i)\} = \{i, j+1\}$ . Dunque le due applicazioni iniettive monotone  $\delta_i \delta_j$  e  $\delta_{j+1} \delta_i$  hanno la stessa immagine e quindi coincidono.

Va osservato che con il semplice cambio di indici  $h = j+1$  e  $k = i$ , da tale identità segue

$$\delta_h \delta_k = \delta_k \delta_{h-1}, \quad \text{per ogni } h > k.$$

□

OSSERVAZIONE 4.1.3. Possiamo raffinare ulteriormente la fattorizzazione epi-moni osservando che ogni  $f: [n] \rightarrow [m]$  possiede un'unica decomposizione del tipo

$$(4.2) \quad f = \delta_{i_1} \cdots \delta_{i_k} \sigma_{j_1} \cdots \sigma_{j_h}$$

con

$$m \geq i_1 > i_2 > \cdots > i_k \geq 0, \quad 0 \leq j_1 < \cdots < j_h < n.$$

La dimostrazione è lasciata per esercizio.

DEFINIZIONE 4.1.4. Un **insieme simpliciale**  $X_\bullet$  è una collezione di insiemi ed applicazioni così definita:

- (1) per ogni intero  $n \geq 0$  è dato un insieme  $X_n$ ;
- (2) per ogni applicazione monotona  $f: [n] \rightarrow [m]$  è data un'applicazione  $f^*: X_m \rightarrow X_n$ .

Le applicazioni  $f^*$  devono soddisfare le seguenti *condizioni di controvarianza*:

- (1) se  $\text{Id}: [n] \rightarrow [n]$  è l'identità allora anche  $\text{Id}^*: X_n \rightarrow X_n$  è l'identità;
- (2) dati comunque  $[n] \xrightarrow{f} [m] \xrightarrow{g} [p]$  si ha  $(gf)^* = f^* g^*: X_p \rightarrow X_n$ .

Dato un insieme simpliciale  $X_\bullet$ , per semplicità di notazione denotiamo

$$\begin{aligned} \partial_i &= \delta_i^*: X_n \rightarrow X_{n-1}, & i &= 0, \dots, n. \\ s_i &= \sigma_i^*: X_n \rightarrow X_{n+1}, & i &= 0, \dots, n. \end{aligned}$$

ESEMPIO 4.1.5. Ad ogni insieme  $U$  è associato in modo canonico un insieme simpliciale  $X_\bullet$  ponendo  $X_n = U$  per ogni  $n$  e  $f^* = \text{Id}_U$  per ogni  $f: [n] \rightarrow [m]$ .

ESEMPIO 4.1.6. Se  $(K, I)$  è un complesso simpliciale astratto, la famiglia  $K_\bullet$  degli insiemi  $K_p$  ( $p$ -simplessi orientati) ha una struttura di insieme simpliciale, dove per ogni  $f: [n] \rightarrow [m]$  si definisce

$$f^*: K_m \rightarrow K_n, \quad f^*(x_0, \dots, x_m) = (x_{f(0)}, \dots, x_{f(m)}).$$

Ad esempio se  $f: [3] \rightarrow [2]$  è l'applicazione

$$f(0) = f(1) = 1, \quad f(2) = f(3) = 2,$$

e  $K$  è il complesso simpliciale astratto e completo dei supereroi si ha

$$f^*(\text{Batman}, \text{Superman}, \text{Superciuk}) = (\text{Superman}, \text{Superman}, \text{Superciuk}, \text{Superciuk}).$$

Equivalentemente, se interpretiamo

$$K_n = \{x: [n] \rightarrow I \mid \{x_0, \dots, x_n\} \in K\}$$

allora l'applicazione  $f^*$  coincide con la composizione a destra con  $f$ , ossia  $f^*x = x \circ f$ ; da questa descrizione segue immediatamente che per ogni  $[n] \xrightarrow{f} [m] \xrightarrow{g} [p]$  si ha

$$(gf)^*x = x \circ gf = (g^*x) \circ f = f^*(g^*x).$$

Si osservi che

$$\partial_i(x_0, \dots, x_m) = \delta_i^*(x_0, \dots, x_m) = (x_0, \dots, \widehat{x}_i, \dots, x_m),$$

$$s_i(x_0, \dots, x_m) = \sigma_i^*(x_0, \dots, x_m) = (x_0, \dots, x_{i-1}, x_i, x_i, x_{i+1}, \dots, x_m).$$

Alla stessa maniera si ha che se  $I$  è totalmente ordinato, allora i simplessi debolmente ordinati

$$K_n^{\leq} = \{(x_0, \dots, x_n) \in K_n \mid x_0 \leq \dots \leq x_n\}$$

formano al variare di  $n$  un insieme simpliciale.

ESEMPIO 4.1.7. Per ogni intero  $p \geq 0$  si definisce l'insieme simpliciale  $\Delta[p]_\bullet$  ponendo

$$\Delta[p]_n = \{x: [n] \rightarrow [p] \text{ monotone}\}, \quad n \geq 0,$$

$$x \in \Delta[p]_m, \quad f: [n] \rightarrow [m], \quad f^*x = x \circ f: [n] \rightarrow [p].$$

Notiamo che l'insieme simpliciale  $\Delta[p]_\bullet$  coincide con i simplessi debolmente ordinati del complesso simpliciale  $\Delta^p$ . Questo implica, tra l'altro, che nella analogie topologiche  $\Delta[1]_\bullet$  deve essere pensato come l'intervallo  $[0, 1]$ ,  $\Delta[2]_\bullet$  come il triangolo pieno a più in generale  $\Delta[p]_\bullet$  come il  $p$ -simplesso topologico (realizzazione geometrica di  $\Delta^p$ ).

ESEMPIO 4.1.8. Per ogni insieme parzialmente ordinato  $(S, \leq)$  possiamo definire un insieme simpliciale  $X_\bullet$  ponendo per ogni  $n \geq 0$

$$X_n = \{x: [n] \rightarrow S \mid x_0 \leq x_1 \leq \dots \leq x_n\},$$

e per ogni  $f: [n] \rightarrow [m]$ ,

$$f^*: X_m \rightarrow X_n, \quad f^*(x) = x \circ f.$$

ESEMPIO 4.1.9 (Spazio classificante). Dato un gruppo  $G$  con elemento neutro  $e$ , il suo **spazio classificante** è l'insieme simpliciale  $BG_\bullet$  definito nel modo seguente:

- (1)  $BG_0 = \{e\}$ ,  $BG_n = G^n = \{(g_n, \dots, g_1) \mid g_i \in G\}$ ;
- (2) per ogni  $f: [m] \rightarrow [n]$  si pone  $f^*(g_n, \dots, g_1) = (h_m, \dots, h_1)$  dove

$$h_i = \begin{cases} g_{f(i)}g_{f(i)-1} \cdots g_{f(i-1)+1} & \text{se } f(i) > f(i-1) \\ e & \text{se } f(i) = f(i-1) \end{cases}$$

Lasciamo al lettore la verifica che  $BG_\bullet$  è un insieme simpliciale.

ESEMPIO 4.1.10. Dati due insiemi simpliciali  $X_\bullet, Y_\bullet$  la famiglia dei prodotti cartesiani  $X_n \times Y_n$  possiede una naturale struttura simpliciale dove, per ogni  $f: [n] \rightarrow [m]$  si definisce

$$f^*: X_m \times Y_m \rightarrow X_n \times Y_n, \quad f^*(x, y) = (f^*x, f^*y).$$

Il corrispondente insieme simpliciale viene detto il **prodotto** di  $X_\bullet, Y_\bullet$  e si denota con il simbolo  $X_\bullet \times Y_\bullet$ .

ESEMPIO 4.1.11. Un (multi)grafo orientato può essere pensato come il dato di: un insieme  $V$  (vertici), un insieme  $E$  (lati) e due applicazioni  $a, p: E \rightarrow V$ . Graficamente ogni lato  $e \in E$  va pensato come un cammino orientato che unisce il vertice di partenza  $p(e)$  con il vertice di arrivo  $a(e)$ .

Ad ogni grafo orientato possiamo associare un insieme simpliciale  $X_\bullet$  ponendo

$$X_n = V \amalg (E \times S_n), \quad n \geq 0,$$

dove  $\amalg$  denota l'unione disgiunta e

$$S_n = \{f: [n] \rightarrow \{0, 1\} \text{ monotona non costante}\}.$$

In particolare  $X_0 = V$  e  $X_1 = V \cup E$  ( $S_1$  contiene solo l'identità); si noti che  $S_n$  contiene esattamente  $n$  applicazioni.

Data  $f: [n] \rightarrow [m]$  l'applicazione  $f^*: X_m \rightarrow X_n$  è definita nel modo seguente:

- (1)  $f^*(v) = v$  per  $v \in V$ ;
- (2)  $f^*(e, \alpha) = (e, \alpha f)$  se  $\alpha f \in S_n$ ;
- (3) se  $(e, \alpha) \in E \times S_m$  e  $\alpha f$  è costante si pone:
  - (a)  $f^*(e, \alpha) = a(e) \in V$  se  $\alpha f \equiv 0$ ,
  - (b)  $f^*(e, \alpha) = p(e) \in V$  se  $\alpha f \equiv 1$ .

Lasciamo al lettore la semplice verifica che  $X_\bullet$  è un insieme simpliciale.

DEFINIZIONE 4.1.12. Un **morfismo di insiemi simpliciali**  $\alpha: X_\bullet \rightarrow Y_\bullet$  è una successione di applicazioni  $\alpha_n: X_n \rightarrow Y_n$  tali che per ogni  $f: [n] \rightarrow [m]$  si ha  $f^* \alpha_m = \alpha_n f^*$ .

I morfismi simpliciali si compongono nel modo ovvio ( $(\alpha \circ \beta)_n = \alpha_n \circ \beta_n$ ) e la composizione è ancora un morfismo di insiemi simpliciali

ESEMPIO 4.1.13. Ecco alcuni esempi di morfismi di insiemi simpliciali:

- 1) Ogni  $\alpha: [n] \rightarrow [m]$  induce un morfismo di insiemi simpliciali

$$\alpha: \Delta[n]_\bullet \rightarrow \Delta[m]_\bullet, \quad \alpha_p(x) = \alpha \circ x, \quad x: [p] \rightarrow [n].$$

- 2) Ogni morfismo  $\beta: K \rightarrow L$  di complessi simpliciali astratti induce un morfismo di insiemi simpliciali

$$\beta: K_\bullet \rightarrow L_\bullet, \quad \beta_n(x_0, \dots, x_n) = (\beta(x_0), \dots, \beta(x_n)).$$

- 3) Ogni omomorfismo di gruppi  $\gamma: G \rightarrow H$  induce un morfismo di insiemi simpliciali

$$\gamma: BG_\bullet \rightarrow BH_\bullet, \quad \gamma(g_n, \dots, g_1) = (\gamma(g_n), \dots, \gamma(g_1)).$$

- 4) Dati due insiemi simpliciali  $X_\bullet$  e  $Y_\bullet$ , le proiezioni naturali sui fattori

$$X_\bullet \times Y_\bullet \rightarrow X_\bullet, \quad X_\bullet \times Y_\bullet \rightarrow Y_\bullet,$$

sono morfismi simpliciali.

ESEMPIO 4.1.14. Siano  $0 \leq k \leq p$  interi; per ogni  $n \geq 0$  denotiamo con  $\widehat{k} \in \Delta[p]_n$  l'applicazione  $[n] \rightarrow [p]$  che vale costantemente  $k$ . Allora per ogni insieme simpliciale  $X$  le applicazioni  $X_n \rightarrow \Delta[p]_n$ ,  $x \mapsto \widehat{k}$  per ogni  $x$ , definiscono un morfismo di insiemi simpliciali, dato che per ogni  $f: [n] \rightarrow [m]$  si ha  $f^* \widehat{k} = \widehat{k}$ .

ESEMPIO 4.1.15. L'Esempio 4.1.14 è un caso particolare di morfismo costante, ossia di un morfismo definito nel modo seguente.

Per ogni intero  $n \geq 0$  denotiamo con  $u: [n] \rightarrow [0]$  l'unica applicazione possibile. Dati due insiemi simpliciali  $X_\bullet, Y_\bullet$  ed un elemento  $y \in Y_0$ , le applicazioni costanti

$$X_n \rightarrow Y_n, \quad x \mapsto u^*(y)$$

definiscono un morfismo di insiemi simpliciali.

### 4.2. Omologia degli insiemi simpliciali

Sia  $X_\bullet$  insieme simpliciale fissato. Applicando le condizioni di controvarianza alle identità cosimpliciali (4.1) otteniamo, per ogni insieme simpliciale le **identità simpliciali**:

$$\begin{aligned} \partial_i: X_n \rightarrow X_{n-1}, \quad s_i: X_n \rightarrow X_{n+1}, \quad i = 0, \dots, n, \\ \partial_j \partial_i = \partial_i \partial_{j+1} \quad \text{per ogni } i \leq j; \\ s_j s_i = s_{i+1} s_j \quad \text{per ogni } i \geq j; \\ (4.3) \quad \partial_j s_i = \begin{cases} s_i \partial_{j-1} & \text{per ogni } j > i + 1 \\ \text{Id} & \text{per } j = i, i + 1 \\ s_{i-1} \partial_j & \text{per ogni } j < i. \end{cases} \end{aligned}$$

Per ogni  $n$  denotiamo con  $C_n(X_\bullet)$  il gruppo abeliano libero generato da  $X_n$ . Per ogni  $f: [n] \rightarrow [m]$ , l'applicazione indotta  $f^*: X_m \rightarrow X_n$  si estende per linearità ad un omomorfismo di gruppi abeliani liberi  $f^*: C_m(X_\bullet) \rightarrow C_n(X_\bullet)$ . In particolare le facce e le degenerazioni inducono omomorfismi

$$\partial_i: C_n(X_\bullet) \rightarrow C_{n-1}(X_\bullet), \quad s_i: C_n(X_\bullet) \rightarrow C_{n+1}(X_\bullet), \quad i = 0, \dots, n.$$

LEMMA 4.2.1. *Nelle notazioni precedenti, gli omomorfismi*

$$\partial: C_n(X_\bullet) \rightarrow C_{n-1}(X_\bullet), \quad \partial = \sum_{i=0}^n (-1)^i \partial_i, \quad n > 0,$$

soddisfano le identità  $\partial^2 = 0$  e quindi definiscono un complesso di gruppi abeliani.

DIMOSTRAZIONE. Sia  $n \geq 0$  fissato e mostriamo le precedenti identità su  $C_n(X_\bullet)$ ; per  $n = 0, 1$  non c'è nulla da dimostrare e quindi possiamo supporre  $n \geq 2$ .

$$\partial^2 = \sum_{j=0}^{n-1} \sum_{i=0}^n (-1)^{i+j} \partial_j \partial_i = \sum_{j=0}^{n-1} \sum_{i=0}^j (-1)^{i+j} \partial_j \partial_i + \sum_{j=0}^{n-1} \sum_{i=j+1}^n (-1)^{i+j} \partial_j \partial_i$$

Nella prima sommatoria usiamo le identità simpliciali e nella seconda scambiamo  $i$  con  $j$

$$\partial^2 = \sum_{j=0}^{n-1} \sum_{i=0}^j (-1)^{i+j} \partial_i \partial_{j+1} + \sum_{i=0}^{n-1} \sum_{j=i+1}^n (-1)^{i+j} \partial_i \partial_j$$

Nella prima sommatoria sostituiamo  $j$  con  $j - 1$  e nella seconda scambiamo i simboli di sommatoria

$$\partial^2 = \sum_{j=1}^n \sum_{i=0}^{j-1} (-1)^{i+j-1} \partial_i \partial_j + \sum_{j=1}^n \sum_{i=0}^{j-1} (-1)^{i+j} \partial_i \partial_j = 0.$$

□

Dunque

$$C(X_\bullet): \quad \cdots \xrightarrow{\partial} C_2(X_\bullet) \xrightarrow{\partial} C_1(X_\bullet) \xrightarrow{\partial} C_0(X_\bullet) \rightarrow 0$$

è un complesso di catene ed ha quindi senso considerare i gruppi di omologia

$$H_n(X_\bullet) = H_n(C(X_\bullet)).$$

Segue immediatamente dalla definizione che se  $K_\bullet$  è l'insieme simpliciale dei semplici orientati di un complesso simpliciale astratto  $K$ , allora  $H_n(K) = H_n(K_\bullet)$  per ogni  $n$ .

ESEMPIO 4.2.2. Siccome ogni elemento di  $\Delta[n]_p$  può essere interpretato come una successione  $(x_0, \dots, x_p)$  con  $0 \leq x_0 \leq x_1 \leq \dots \leq x_p \leq n$  si ha che  $C(\Delta[n]_\bullet)$  coincide con il complesso  $C(\Delta^n, \leq)$  delle catene debolmente ordinate del complesso simpliciale astratto  $\Delta^n$  e quindi  $H_p(\Delta[n]_\bullet) = H_p(\Delta^n)$  per ogni  $p$ , ossia  $H_0(\Delta[n]_\bullet) = \mathbb{Z}$  e  $H_p(\Delta[n]_\bullet) = 0$  per ogni  $p \neq 0$ .

Dato un morfismo di insiemi simpliciali  $\alpha: X_\bullet \rightarrow Y_\bullet$ , i morfismi  $\alpha_n: X_n \rightarrow Y_n$  commutano con le facce  $\partial_i$ ; lo stesso vale per le loro estensioni lineari  $\alpha_n: C_n(X_\bullet) \rightarrow C_n(Y_\bullet)$  ed è quindi definito un morfismo di complessi di catene  $\alpha: C(X_\bullet) \rightarrow C(Y_\bullet)$  che a sua volta induce omomorfismi in omologia.

TEOREMA 4.2.3. *Sia  $X_\bullet$  un insieme simpliciale. Allora la proiezione*

$$X_\bullet \times \Delta[1]_\bullet \rightarrow X_\bullet$$

*induce un isomorfismo in omologia.*

DIMOSTRAZIONE. Per ogni  $n \geq 0$  l'insieme  $\Delta[1]_n = \{\alpha: [n] \rightarrow [1]\}$  contiene esattamente  $n+2$  elementi ciascuno dei quali si può rappresentare come una  $n+1$ -upla  $(y_0, \dots, y_n)$  con  $0 \leq y_0 \leq \dots \leq y_n \leq 1$ : la  $n+1$ -upla  $(y_0, \dots, y_n)$  corrisponde all'applicazione  $[n] \rightarrow [1]$ ,  $i \mapsto y_i$ .

Per ogni coppia di interi  $n, k \geq 0$  definiamo

$$T_n^k = \{(y_0, \dots, y_n) \in \Delta[1]_n \mid y_i = 0 \text{ per ogni } i \leq n-k\}.$$

Osserviamo che

$$T_n^0 = \Delta[0]_n = \{(0, \dots, 0)\} \subset T_n^1 \subset T_n^2 \subset \dots \subset T_n^k = \Delta[1]_n \text{ per ogni } k > n.$$

Osserviamo inoltre che i sottoinsiemi  $T_n^k$  si comportano bene rispetto agli operatori  $\partial_i$ , e più precisamente:

- (1)  $\partial_i T_n^k \subset T_{n-1}^k$  per ogni  $n > 0$  ed ogni  $0 \leq i \leq n$ ;
- (2)  $\partial_i T_n^k \subset T_{n-1}^{k-1}$  per ogni  $n > 0$  ed ogni  $n-k < i \leq n$ .

Consideriamo gli operatori

$$\tau: T_n^k \rightarrow T_{n+1}^k, \quad \tau(y_0, \dots, y_n) = (0, y_0, \dots, y_n).$$

Dato un qualunque elemento  $y \in T_n^k$ , sono di immediata verifica le relazioni:

- (1)  $\partial_0 \tau(y) = y$ ;
- (2)  $\partial_{i+1} \tau(y) = y$  se  $0 \leq i \leq n-k$ ;
- (3)  $\partial_{i+1} \tau(y) \in T_n^{k-1}$  se  $i > n-k$  e  $0 \leq i \leq n$ ;
- (4)  $\partial_{i+1} \tau(y) = \tau \partial_i(y)$  se  $n > 0$  e  $0 \leq i \leq n$ .

Per ogni  $k \geq 0$  consideriamo il sottocomplesso  $C^k \subset C(X_\bullet \times \Delta[1]_\bullet)$  generato in grado  $n$  dagli elementi di  $X_n \times T_n^k$ .

Siccome  $T_n^0$  contiene un solo elemento, il morfismo  $C(X_\bullet \times \Delta[1]_\bullet) \rightarrow C(X_\bullet)$  indotto dalla proiezione stabilisce un isomorfismo  $C^0 \simeq C(X_\bullet)$ , quindi  $H_n(C^0) = H_n(X_\bullet)$ .

D'altra parte  $C_n^k = C_n(X_\bullet \times \Delta[1]_\bullet)$  per ogni  $k > n$  e quindi  $H_n(C^k) = H_n(X_\bullet \times \Delta[1]_\bullet)$  per ogni  $k \geq n+2$ .

Per dimostrare il teorema sarà quindi sufficiente provare che ogni inclusione  $C^k \subset C^{k+1}$  è un quasi-isomorfismo. Per il Lemma 3.4.3 basta trovare, per ogni  $k > 0$ , un'omotopia  $h: C^k \rightarrow C^{k+1}$  tale che:

- (1)  $h(C^{k-1}) \subset C^{k-1}$ ;
- (2) se  $\phi = \partial h + h \partial - \text{Id}$ , allora  $\phi(C^k) \subset C^{k-1}$ .

Sia quindi  $k > 0$  fissato e definiamo le applicazioni

$$h_n: C_n^k \rightarrow C_{n+1}^k, \quad h_n(x, y) = \begin{cases} (-1)^{n-k+1} (s_{n-k+1} x, \tau y) & \text{se } n+1 \geq k, \\ 0 & \text{se } n+1 < k. \end{cases}$$

La condizione  $h(C^{k-1}) \subset C^{k-1}$  è chiara; occupiamoci adesso di studiare, per ogni  $n \geq 0$ , l'immagine dell'operatore  $\phi = \partial h + h \partial - \text{Id}: C_n^k \rightarrow C_n^k$ ; trattiamo separatamente i tre casi  $k > n+1$ ,  $k = n+1$  e  $k < n+1$ .

1) Se  $k > n+1$  allora  $C_n^k = C_n^{k-1}$  e quindi l'immagine di  $\phi$  è contenuta in  $C_n^{k-1}$ .

2) Se  $k = n+1$  si ha  $\phi = \partial h - \text{Id}$  e per ogni  $(x, y) \in X_n \times T_n^k$ , siccome  $\partial_0 s_0 = \text{Id}$  si ha

$$\phi(x, y) = \sum_{i=0}^{n+1} (-1)^i (\partial_i s_0 x, \partial_i \tau y) - (x, y) = \sum_{i=1}^{n+1} (-1)^i (\partial_i s_0 x, \partial_i \tau y)$$

e ogni elemento nella sommatoria a destra appartiene a  $T_n^{k-1} = T_n^n$ . Quindi anche in questo caso l'immagine di  $\phi$  è contenuta in  $C_n^{k-1}$ .

3) Se  $k < n + 1$  e  $(x, y) \in X_n \times T_n^k$ , usando le identità simpliciali

$$\partial_{n-k+1}s_{n-k+1} = \text{Id}, \quad \partial_i s_{n-k+1} = s_{n-k} \partial_i, \quad 0 \leq i \leq n-k,$$

e le uguaglianze  $\partial_i \tau y = y$  per ogni  $0 \leq i \leq n-k+1$ , si ha:

$$\begin{aligned} \partial h(x, y) &= \sum_{i=0}^{n+1} (-1)^{n-k+1+i} (\partial_i s_{n-k+1} x, \partial_i \tau y) \\ &= \sum_{i=0}^{n-k} (-1)^{n-k+1+i} (\partial_i s_{n-k+1} x, y) + (x, y) + \sum_{i=n-k+2}^{n+1} (-1)^{n-k+1+i} (\partial_i s_{n-k+1} x, \partial_i \tau y) \\ &= \sum_{i=0}^{n-k} (-1)^{n-k+1+i} (s_{n-k} \partial_i x, y) + (x, y) + \sum_{i=n-k+2}^{n+1} (-1)^{n-k+1+i} (\partial_i s_{n-k+1} x, \partial_i \tau y), \\ h \partial(x, y) &= \sum_{i=0}^{n-k} (-1)^{n-k+i} (s_{n-k} \partial_i x, y) + \sum_{i=n-k+1}^n (-1)^{n-k+i} (s_{n-k} \partial_i x, \tau \partial_i y). \end{aligned}$$

Dunque

$$\phi(x, y) = \sum_{i=n-k+2}^{n+1} (-1)^{n-k+1+i} (\partial_i s_{n-k+1} x, \partial_i \tau y) + \sum_{i=n-k+1}^n (-1)^{n-k+i} (s_{n-k} \partial_i x, \tau \partial_i y)$$

ed è chiaro che ogni addendo in ciascuna sommatoria appartiene a  $C_n^{k-1}$ .  $\square$

Per ogni insieme simpliciale  $X_\bullet$  possiamo considerare i due morfismi di insiemi simpliciali

$$i_0, i_1: X_\bullet \rightarrow X_\bullet \times \Delta[1]_\bullet$$

$$i_0(x) = (x, (0, 0, \dots, 0)), \quad i_1(x) = (x, (1, 1, \dots, 1)).$$

La verifica che si tratta di morfismi di insiemi simpliciali è immediata in quanto per ogni  $f: [n] \rightarrow [m]$  si ha

$$f^*(0, \dots, 0) = (0, \dots, 0), \quad f^*(1, \dots, 1) = (1, \dots, 1).$$

**COROLLARIO 4.2.4.** *Nelle notazioni precedenti, per ogni insieme simpliciale  $X_\bullet$  i due morfismi di insiemi simpliciali*

$$i_0, i_1: X_\bullet \rightarrow X_\bullet \times \Delta[1]_\bullet$$

*inducono lo stesso isomorfismo in omologia*

$$i_0 = i_1: H_n(X_\bullet) \xrightarrow{\cong} H_n(X_\bullet \times \Delta[1]_\bullet).$$

**DIMOSTRAZIONE.** Per il teorema precedente la proiezione  $\pi: X_\bullet \times \Delta[1]_\bullet \rightarrow X_\bullet$  induce un isomorfismo in omologia e siccome  $\pi i_0 = \pi i_1 = \text{Id}$  si ha che

$$i_0, i_1: H_n(X_\bullet) \rightarrow H_n(X_\bullet \times \Delta[1]_\bullet)$$

coincidono entrambi con l'inverso dell'isomorfismo

$$\pi: H_n(X_\bullet \times \Delta[1]_\bullet) \xrightarrow{\cong} H_n(X_\bullet).$$

$\square$

**DEFINIZIONE 4.2.5.** Diremo che due morfismi di insiemi simpliciali  $\alpha, \beta: X_\bullet \rightarrow Y_\bullet$  sono **direttamente omotopi**, e scriveremo  $\alpha \Rightarrow \beta$ , se esiste un morfismo di insiemi simpliciali

$$\theta: X_\bullet \times \Delta[1]_\bullet \rightarrow Y_\bullet$$

tale che

$$\alpha = \theta i_0, \quad \beta = \theta i_1.$$

In tal caso

La relazione di omotopia diretta gode della proprietà riflessiva, ossia  $\alpha \Rightarrow \alpha$  per ogni  $\alpha: X_\bullet \rightarrow Y_\bullet$ : basta infatti considerare il morfismo di insiemi simpliciali

$$\theta = \alpha \times \text{Id}: X_\bullet \times \Delta[1]_\bullet \rightarrow Y_\bullet, \quad \theta(x, y) = (\alpha(x), y).$$

DEFINIZIONE 4.2.6. Due morfismi di insiemi simpliciali  $\alpha, \beta: X_\bullet \rightarrow Y_\bullet$  si dicono **omotopi** se esiste uno zigzag finito di omotopie dirette

$$\begin{array}{ccccc} & \gamma_0 & & \dots & & \gamma_n & \\ & \swarrow & & & & \swarrow & \\ \alpha & & & & & & \beta \\ & \searrow & & \dots & & \searrow & \\ & \gamma_1 & & & & \gamma_{n-1} & \end{array}$$

La definizione è analoga alla definizione di omotopia di applicazioni continue, dato che  $\Delta[1]_\bullet$  è l'analogo simpliciale dell'intervallo chiuso  $[0, 1]$ ; la necessità di prendere lo zigzag serve a garantire le proprietà simmetrica e transitiva dell'omotopia.

Ad esempio, se  $\alpha, \beta$  sono direttamente omotopi, allora  $\beta, \alpha$  sono omotopi, come segue considerando lo zigzag

$$\begin{array}{ccc} & \alpha & \\ \alpha \times \text{Id} \swarrow & & \searrow \\ \alpha & & \beta \end{array}$$

La relazione di omotopia si comporta bene con le composizioni, nel senso descritto dal seguente lemma.

LEMMA 4.2.7. *Siano  $\alpha, \beta: X_\bullet \rightarrow Y_\bullet$  due morfismi (direttamente) omotopi di insiemi simpliciali. Allora:*

- (1) *per ogni morfismo di insiemi simpliciali  $f: Y_\bullet \rightarrow Z_\bullet$ , i due morfismi  $f\alpha$  e  $f\beta$  sono (direttamente) omotopi;*
- (2) *per ogni morfismo di insiemi simpliciali  $g: W_\bullet \rightarrow X_\bullet$ , i due morfismi  $\alpha g$  e  $\beta g$  sono (direttamente) omotopi.*

DIMOSTRAZIONE. Consideriamo prima il caso in cui  $\alpha$  e  $\beta$  sono direttamente omotopi, ossia che esiste  $\theta: X_\bullet \times \Delta[1]_\bullet \rightarrow Y_\bullet$  tale che  $\alpha = \theta i_0$ ,  $\beta = \theta i_1$ . Siccome  $\alpha = \theta i_0$  e  $\beta = \theta i_1$  si ha  $f\alpha = (f\theta)i_0$  e  $f\beta = (f\theta)i_1$ , che prova che  $\alpha$  e  $\beta$  sono direttamente omotopi.

Similmente se consideriamo il morfismo di insiemi simpliciali

$$g \times \text{Id}: W_\bullet \times \Delta[1]_\bullet \rightarrow X_\bullet \times \Delta[1]_\bullet, \quad (w, y) \mapsto (g(w), y),$$

si ha  $i_k g = (g \times \text{Id})i_k$  per ogni  $k = 0, 1$  e quindi

$$\alpha g = \theta i_0 g = \theta(g \times \text{Id})i_0, \quad \beta g = \theta i_1 g = \theta(g \times \text{Id})i_1.$$

In generale,  $\alpha$  e  $\beta$  sono connesse da uno zigzag finito di omotopie dirette, applicando il precedente risultato a ciascuna freccia  $\Rightarrow$  dello zigzag si ottiene la dimostrazione.  $\square$

COROLLARIO 4.2.8. *Due morfismi omotopi di insiemi simpliciali  $\alpha, \beta: X_\bullet \rightarrow Y_\bullet$  inducono lo stesso morfismo in omologia.*

DIMOSTRAZIONE. Non è restrittivo supporre  $\alpha$  e  $\beta$  direttamente omotopi, e sia  $\theta$  come nella Definizione 4.2.5. Siccome  $i_0, i_1$  inducono lo stesso morfismo in omologia, pure i morfismi  $\theta i_0$  e  $\theta i_1$  inducono lo stesso morfismo in omologia.  $\square$

### 4.3. Complementi: catene degeneri e complesso di Moore

Questa sezione non è essenziale per il seguito e può essere pertanto omessa ad una prima lettura.

LEMMA 4.3.1. *Sia  $X_\bullet$  un insieme simpliciale. Nelle notazioni precedenti, gli omomorfismi*

$$\begin{aligned}\partial: C_n(X_\bullet) &\rightarrow C_{n-1}(X_\bullet), & \partial &= \sum_{i=0}^n (-1)^i \partial_i, \\ s: C_n(X_\bullet) &\rightarrow C_{n+1}(X_\bullet), & s &= \sum_{i=0}^n (-1)^i s_i,\end{aligned}$$

soddisfano le seguenti identità:

$$\partial^2 = 0, \quad s^2 = 0, \quad \partial s + s\partial = 0.$$

DIMOSTRAZIONE. Abbiamo già dimostrato che  $\partial^2 = 0$ . Proviamo adesso che  $s^2 = 0$ .

$$s^2 = \sum_{j=0}^{n+1} \sum_{i=0}^n (-1)^{i+j} s_j s_i = \sum_{i=0}^n \sum_{j=0}^i (-1)^{i+j} s_j s_i + \sum_{i=0}^n \sum_{j=i+1}^{n+1} (-1)^{i+j} s_j s_i$$

Nella prima sommatoria usiamo le identità simpliciali e nella seconda scambiamo  $i$  con  $j$

$$s^2 = \sum_{i=0}^n \sum_{j=0}^i (-1)^{i+j} s_{i+1} s_j + \sum_{j=0}^n \sum_{i=j+1}^{n+1} (-1)^{i+j} s_i s_j$$

Nella prima sommatoria sostituiamo  $i$  con  $i-1$  e nella seconda scambiamo i simboli di sommatoria

$$s^2 = \sum_{i=1}^{n+1} \sum_{j=0}^{i-1} (-1)^{i+j-1} s_i s_j + \sum_{i=1}^{n+1} \sum_{j=0}^{i-1} (-1)^{i+j} s_i s_j = 0$$

Rimane da dimostrare che  $\partial s = -s\partial$ . Se  $n = 0$  abbiamo  $s\partial = 0$  e  $\partial s = \partial_0 s_0 - \partial_1 s_0 = \text{Id} - \text{Id} = 0$  e quindi per l'uguaglianza  $\partial s + s\partial = 0$  possiamo assumere  $n \geq 1$ .

$$\partial s = \sum_{j=0}^{n+1} \sum_{i=0}^n (-1)^{i+j} \partial_j s_i$$

Siccome  $\partial_j s_i = \text{Id}$  per  $j = i, i+1$  possiamo scrivere

$$\partial s = \sum_{i=1}^n \sum_{j=0}^{i-1} (-1)^{i+j} \partial_j s_i + \sum_{i=0}^{n-1} \sum_{j=i+2}^{n+1} (-1)^{i+j} \partial_j s_i$$

E usando le identità simpliciali

$$\partial s = \sum_{i=1}^n \sum_{j=0}^{i-1} (-1)^{i+j} s_{i-1} \partial_j + \sum_{i=0}^{n-1} \sum_{j=i+2}^{n+1} (-1)^{i+j} s_i \partial_{j-1}$$

Scambiando  $i$  con  $i+1$  nella prima e  $j$  con  $j+1$  nella seconda si ottiene

$$\partial s = \sum_{i=0}^{n-1} \sum_{j=0}^i (-1)^{i+j+1} s_i \partial_j + \sum_{i=0}^{n-1} \sum_{j=i+1}^n (-1)^{i+j+1} s_i \partial_j$$

$$\partial s = - \sum_{i=0}^{n-1} \sum_{j=0}^n (-1)^{i+j} s_i \partial_j = -s\partial.$$

□

Sia  $X_\bullet$  un insieme simpliciale; come nel caso dei complessi simpliciali astratti è possibile trovare dei sottocomplessi molto più piccoli di  $C(X_\bullet)$  che calcolano la stessa omologia. A tal fine osserviamo che per ogni  $0 \leq k \leq n$  l'operatore  $\partial s_k: C_n(X_\bullet) \rightarrow C_n(X_\bullet)$  è uguale a

$$\begin{aligned}(4.4) \quad \partial s_k &= \sum_{i=0}^{n+1} (-1)^i \partial_i s_k = \sum_{i=0}^{k-1} (-1)^i \partial_i s_k + \sum_{i=k+2}^{n+1} (-1)^i \partial_i s_k \\ &= \sum_{i=0}^{k-1} (-1)^i s_{k-1} \partial_i + \sum_{i=k+2}^{n+1} (-1)^i s_k \partial_{i-1},\end{aligned}$$

e quindi se denotiamo con  $D_n(X_\bullet) \subset C_n(X_\bullet)$  il sottogruppo abeliano libero generato dagli elementi del tipo  $s_k x$ , con  $0 \leq k \leq n-1$  e  $x \in X_{n-1}$ , si ha  $\partial(D_n(X_\bullet)) \subset D_{n-1}(X_\bullet)$  e quindi tali sottogruppi definiscono un sottocomplesso  $D(X_\bullet) \subset C(X_\bullet)$ , detto delle **catene degeneri** e che però non è quello che cerchiamo dato che:

LEMMA 4.3.2. *Nelle notazioni precedenti il complesso  $D(X_\bullet)$  è aciclico.*

DIMOSTRAZIONE. La Formula (4.4) ci consente di definire una catena ascendente di sottocomplessi

$$0 = D^{-1} \subset D^0 \subset D^1 \subset \cdots \subset D(X_\bullet),$$

dove  $D^k$  è il sottocomplesso generato da tutti gli elementi del tipo  $s_k x$ , con  $0 \leq k \leq p$ . Più precisamente, per ogni  $n \geq 0$ ,  $D_n^k \subset D_n(X_\bullet)$  è il sottogruppo abeliano libero generato dagli elementi del tipo  $s_i x$ , con  $0 \leq i \leq \min(k, n-1)$  e  $x \in X_{n-1}$ . Siccome  $D_n^k = D_n(X_\bullet)$  per ogni  $k \geq n-1$ , per dimostrare che  $D_n(X_\bullet)$  è aciclico basta dimostrare che per ogni  $k \geq 0$  l'inclusione  $D^{k-1} \subset D^k$  è un quasi-isomorfismo.

A tal fine considerando l'omotopia  $h = (-1)^k s_k : D^k \rightarrow D^{k-1}$ ; per un elemento del tipo  $s_h x \in D_n^{k-1}$ ,  $h < k$ , si ha

$$(-1)^k h(s_h x) = s_k s_h x = s_h s_{k-1} x \in D_n^{k-1}.$$

Ponendo  $\phi = \partial h + h \partial - \text{Id}$ , vogliamo dimostrare che per ogni generatore  $s_h x \in D_n^k$ ,  $n > 1$ ,  $h \leq k$ ,  $x \in X_{n-1}$ , si ha  $\phi(s_h x) \in D_n^{k-1}$ . Se  $h < k$  abbiamo già visto che  $h(s_h x)$  appartiene al sottocomplesso  $D^{k-1}$  e a maggior ragione  $\phi(s_h x) \in D^{k-1}$ . Se  $h = k$ , usando la Formula (4.4) e le identità simpliciali si ha

$$\begin{aligned} (-1)^k \phi(s_k x) &= \sum_{i=0}^{k-1} (-1)^i s_{k-1} \partial_i s_k x + \sum_{i=k+2}^{n+1} (-1)^i s_k \partial_{i-1} s_k x + \sum_{i=0}^n (-1)^i s_k \partial_i s_k x - (-1)^k s_k x \\ &= \sum_{i=0}^{k-1} (-1)^i s_{k-1} \partial_i s_k x - \sum_{i=k+1}^n (-1)^i s_k \partial_i s_k x + \sum_{i=0}^n (-1)^i s_k \partial_i s_k x - (-1)^k s_k x \\ &= \sum_{i=0}^{k-1} (-1)^i s_{k-1} \partial_i s_k x + \sum_{i=0}^k (-1)^i s_k \partial_i s_k x - (-1)^k s_k x \\ &= \sum_{i=0}^{k-1} (-1)^i s_{k-1} \partial_i s_k x + \sum_{i=0}^{k-1} (-1)^i s_k \partial_i s_k x \\ &= \sum_{i=0}^{k-1} (-1)^i s_{k-1} \partial_i s_k x + \sum_{i=0}^{k-1} (-1)^i s_k s_{k-1} \partial_i x \\ &= \sum_{i=0}^{k-1} (-1)^i s_{k-1} \partial_i s_k x + \sum_{i=0}^{k-1} (-1)^i s_{k-1} s_{k-1} \partial_i x \in D_n^{k-1}. \end{aligned}$$

□

Sia  $X_\bullet$  un insieme simpliciale, definiamo  $N_0(X_\bullet) = C_0(X_\bullet)$  e per ogni  $n > 0$

$$N_n(X_\bullet) = \{a \in C_n(X_\bullet) \mid \partial_i a = 0 \text{ per ogni } 0 < i \leq n\}.$$

Se  $a \in N_n(X_\bullet)$  si ha  $\partial a = \partial_0 a$  e per ogni  $i \geq 0$  vale

$$\partial_i \partial a = \partial_i \partial_0 a = \partial_0 \partial_{i+1} a = 0,$$

e quindi  $\partial a \in N_{n-1}(X_\bullet)$ , ossia i sottogruppi  $N_n(X_\bullet)$  definiscono un sottocomplesso  $N(X_\bullet) \subset C(X_\bullet)$  detto **complesso di Moore** dell'insieme simpliciale.

TEOREMA 4.3.3. *Nelle notazioni precedenti si ha  $C(X_\bullet) = N(X_\bullet) \oplus D(X_\bullet)$  e l'inclusione di complessi di catene  $N(X_\bullet) \subset C(X_\bullet)$  induce un isomorfismo in omologia.*

DIMOSTRAZIONE. Dato che  $D_0(X_\bullet) = 0$ ,  $N_0(X_\bullet) = C_0(X_\bullet)$  basta provare che per ogni  $n > 0$  si ha  $C_n(X_\bullet) = N_n(X_\bullet) \oplus D_n(X_\bullet)$ . Per provare che  $N_n(X_\bullet) \cap D_n(X_\bullet) = 0$  supponiamo

per assurdo che esista  $0 \neq a \in N_n(X_\bullet) \cap D_n(X_\bullet)$  e sia  $0 \leq p \leq n-1$  il più piccolo intero per cui è possibile scrivere  $a = \sum_{i=0}^p s_i(a_i)$ , con  $a_i \in C_{n-1}(X_\bullet)$ . Allora

$$\begin{aligned} 0 = \partial_{p+1}(a) &= \sum_{i=0}^{p-1} \partial_{p+1} s_i(a_i) + a_p = \sum_{i=0}^{p-1} s_i \partial_p(a_i) + a_p, \\ s_p(a_p) &= - \sum_{i=0}^{p-1} s_p s_i \partial_p(a_i) = - \sum_{i=0}^{p-1} s_i s_{p-1} \partial_p(a_i), \end{aligned}$$

da cui segue

$$y = \sum_{i=0}^{p-1} s_i(a_i - s_{p-1} \partial_p(a_i)),$$

in contraddizione con la definizione di  $p$ .

Per dimostrare che  $C_n(X_\bullet) = N_n(X_\bullet) + D_n(X_\bullet)$  sia  $a \in C_n(X_\bullet)$  e sia  $-1 \leq p \leq n$  il più piccolo intero tale che  $\partial_i a = 0$  per ogni  $1 \leq i \leq n-p$ . Se  $p = -1$  allora  $a \in N_n(X_\bullet)$ . Se  $p \geq 0$  consideriamo la catena  $b = a - s_{n-p} \partial_{n-p} a$ . Allora

$$\partial_{n-p} b = \partial_{n-p} a - \partial_{n-p} s_{n-p} \partial_{n-p} a = \partial_{n-p} a - \partial_{n-p} a = 0,$$

mentre se  $1 \leq i < n-p$  si ha

$$\partial_i b = \partial_i a - \partial_i s_{n-p} \partial_{n-p} a = -s_{n-p-1} \partial_i \partial_{n-p} a = -s_{n-p-1} \partial_{n-p-1} \partial_i a = 0.$$

Per induzione su  $p$  si ha  $b \in N_n(X_\bullet) + D_n(X_\bullet)$  e quindi

$$a = b + s_{n-p} \partial_{n-p} a \in N_n(X_\bullet) + D_n(X_\bullet).$$

Per concludere, abbiamo dimostrato che il sottocomplesso  $D(X_\bullet)$  delle catene degeneri è aciclico e quindi

$$H_n(C(X_\bullet)) = H_n(N(X_\bullet)) \oplus H_n(D(X_\bullet)) = H_n(N(X_\bullet)).$$

□

**OSSERVAZIONE 4.3.4.** Per evitare un errore comune, se per ogni  $n$  definiamo  $M_n \subset C_n(X_\bullet)$  come il sottogruppo abeliano libero generato dagli elementi di  $X_n - \cup_i s_i(X_{n-1})$ , è chiaro che  $C_n(X_\bullet) = M_n \oplus D_n(X_\bullet)$  per ogni  $n$ , ma la successione degli  $M_n$  **non** è in generale un sottocomplesso. Consideriamo ad esempio l'insieme simpliciale  $\Delta_\bullet^1$  dei simplessi orientati del complesso simpliciale astratto  $\Delta^1$ . Allora  $(0, 1, 0) \in M_2$  ma

$$\partial(0, 1, 0) = (1, 0) - (0, 0) + (0, 1) = (1, 0) - s_0(0) + (0, 1) \notin M_1.$$

#### 4.4. Introduzione all'omologia singolare

Per ogni  $n \geq 0$  consideriamo l'applicazione "base canonica"  $e: [n] \rightarrow \mathbb{R}^{n+1}$ :

$$e_0 = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \quad e_1 = \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix}, \quad \dots \quad e_n = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix}.$$

Definiamo poi il **simplesso topologico standard** di dimensione  $n$ , denotato  $\Delta_{\mathbb{R}}^n$ , come l'involuppo convesso di  $e([n])$ :

$$\Delta_{\mathbb{R}}^n = \langle e([n]) \rangle = \left\{ \sum_{i=0}^n t_i e_i \mid t_i \geq 0, \sum t_i = 1 \right\} = \left\{ (t_0, \dots, t_n) \in \mathbb{R}^{n+1} \mid t_i \geq 0, \sum t_i = 1 \right\}$$

(per semplicità di scrittura intendiamo il vettore riga  $(t_0, \dots, t_n)$  con lo stesso significato del corrispondente vettore colonna). Abbiamo già osservato che ciascun  $\Delta_{\mathbb{R}}^n$  è un sottospazio metrico compatto e connesso di  $\mathbb{R}^{n+1}$ .

Ogni morfismo  $f: [n] \rightarrow [m]$  si estende ad un diagramma commutativo

$$\begin{array}{ccc} [n] & \xrightarrow{f} & [m] \\ \downarrow e & & \downarrow e \\ \mathbb{R}^{n+1} & \xrightarrow{f_{\mathbb{R}}} & \mathbb{R}^{m+1} \end{array}$$

dove  $f_{\mathbb{R}}$  è l'unica applicazione lineare che fa commutare il diagramma. In concreto:

$$f_{\mathbb{R}} \left( \sum_{i=0}^n t_i e_i \right) = \sum_{i=0}^n t_i e_{f(i)} \iff f_{\mathbb{R}}(t_0, \dots, t_n) = \left( \sum_{\{i|f(i)=0\}} t_i, \dots, \sum_{\{i|f(i)=m\}} t_i \right).$$

Sono evidenti sia la continuità di  $f_{\mathbb{R}}$  sia le proprietà functoriali della precedente costruzione, ossia  $\text{Id}_{\mathbb{R}} = \text{Id}$  e  $(fg)_{\mathbb{R}} = f_{\mathbb{R}} g_{\mathbb{R}}$ . È anche immediato osservare che i semplici topologici standard sono stabili per le applicazioni  $f_{\mathbb{R}}$ , ossia che:

$$f: [n] \rightarrow [m] \implies f_{\mathbb{R}}: \Delta_{\mathbb{R}}^n \rightarrow \Delta_{\mathbb{R}}^m.$$

In particolare:

$$(\delta_i)_{\mathbb{R}}(t_0, \dots, t_n) = (t_0, \dots, t_{i-1}, 0, t_i, \dots, t_n),$$

$$(\sigma_i)_{\mathbb{R}}(t_0, \dots, t_n) = (t_0, \dots, t_{i-1}, t_i + t_{i+1}, t_{i+2}, \dots, t_n),$$

e per ogni applicazione faccia  $\delta_i: [n] \rightarrow [n+1]$  si ha un omeomorfismo

$$(\delta_i)_{\mathbb{R}}: \Delta_{\mathbb{R}}^n \xrightarrow{\cong} \{(t_0, \dots, t_{n+1}) \in \Delta_{\mathbb{R}}^{n+1} \mid t_i = 0\}.$$

**DEFINIZIONE 4.4.1.** Un  $n$ -**simplexso singolare** di uno spazio topologico  $X$  è un'applicazione continua  $\alpha: \Delta_{\mathbb{R}}^n \rightarrow X$ . L'insieme degli  $n$ -simplexsi singolari di  $X$  viene denotato  $S_n(X)$ .

Per ogni morfismo  $f: [n] \rightarrow [m]$  possiamo definire

$$f^*: S_m(X) \rightarrow S_n(X), \quad f^* \alpha = \alpha \circ f_{\mathbb{R}},$$

ed è immediato osservare che tutto ciò definisce un insieme simpliciale  $S_{\bullet}(X)$ , detto **insieme singolare** dello spazio topologico  $X$ .

**DEFINIZIONE 4.4.2.** Il complesso  $C(S_{\bullet}(X))$  viene detto complesso delle **catene singolari** di  $X$  ed i gruppi

$$H_n(X) \xlongequal{\text{per definizione}} H_n(S_{\bullet}(X))$$

sono detti gruppi di **omologia singolare** dello spazio topologico  $X$ .

Lo studio dell'omologia singolare è uno degli argomenti principali dei corsi di topologia algebrica; in queste note ci limiteremo a dimostrare la loro invarianza omotopica ed a enunciare (senza dimostrazioni) alcuni teoremi fondamentali. Per approfondimenti e maggiori dettagli rimandiamo a [3, 4, 9, 10, 21].

**ESEMPIO 4.4.3.** Se  $X = \emptyset$ , allora  $S_n(X) = \emptyset$  per ogni  $n \geq 0$  e quindi  $H_n(\emptyset) = 0$  per ogni  $n$ .

**ESEMPIO 4.4.4.** Se  $X = *$  è formato da un solo punto, allora  $S_n(X)$  contiene solo il simplexso singolare costante  $c_n: \Delta_{\mathbb{R}}^n \rightarrow *$  e quindi  $\partial_i c_n = c_{n-1}$  per ogni  $n > 0$   $0 \leq i \leq n$ . Per ogni  $n > 0$  si ha

$$\partial c_n = \sum_{i=0}^n (-1)^i \partial_i c_n = \sum_{i=0}^n (-1)^i c_{n-1} = \begin{cases} c_{n-1} & \text{se } n \text{ pari,} \\ 0 & \text{se } n \text{ dispari.} \end{cases}$$

Dunque il complesso delle catene singolari diventa

$$\cdots \rightarrow C_4 = \mathbb{Z} \xrightarrow{\text{Id}} C_3 = \mathbb{Z} \xrightarrow{0} C_2 = \mathbb{Z} \xrightarrow{\text{Id}} C_1 = \mathbb{Z} \xrightarrow{0} C_0 = \mathbb{Z} \rightarrow 0$$

che ha come omologia  $H_0 = \mathbb{Z}$  e  $H_n = 0$  per ogni  $n > 0$ .

Alternativamente, si può osservare che  $S_{\bullet}(*)$  coincide con l'insieme simpliciale dei simplexsi orientati di  $\Delta^0$ , di cui abbiamo già calcolato l'omologia.

OSSERVAZIONE 4.4.5. Per definizione  $S_0(X) = X$  (ogni 0-simplesso  $\Delta_{\mathbb{R}}^0 \rightarrow X$  viene identificato con la sua immagine).

Siccome esiste un ovvio omeomorfismo

$$\Delta_{\mathbb{R}}^1 \rightarrow [0, 1], \quad (t_0, t_1) \mapsto t_1,$$

esiste una naturale bigezione tra  $S_1(X)$  e l'insieme dei cammini continui  $[0, 1] \rightarrow X$ . Ogni cammino continuo  $\alpha: [0, 1] \rightarrow X$  corrisponde all'1-simplesso singolare

$$\alpha': \Delta_{\mathbb{R}}^1 \rightarrow X, \quad \alpha'(t_0, t_1) = \alpha(t_1).$$

Per ogni cammino  $\alpha: [0, 1] \rightarrow X$  scriveremo

$$\partial\alpha = \partial\alpha' = \partial_0\alpha' - \partial_1\alpha' = \alpha'(0, 1) - \alpha'(1, 0) = \alpha(1) - \alpha(0).$$

LEMMA 4.4.6. *Per ogni spazio topologico  $X$ , il gruppo  $H_0(X)$  è abeliano libero generato dalle componenti connesse per archi.*

DIMOSTRAZIONE. Sia  $Y \subset X = S_0(X)$  un insieme di rappresentanti delle componenti connesse per archi. Denotando con  $F \subset C_0(S_{\bullet}(X))$  il sottogruppo libero generato da  $Y$  basta dimostrare che esiste una decomposizione in somma diretta  $C_0(S_{\bullet}(X)) = F \oplus B_0(S_{\bullet}(X))$ .

Per ogni  $x \in X$  esistono  $y \in Y$  ed un cammino  $\alpha: [0, 1] \rightarrow X$  tali che  $\alpha(0) = y$  e  $\alpha(1) = x$ . Possiamo allora scrivere

$$(x) = (y) + \partial\alpha \in C_0(S_{\bullet}(X));$$

dunque ogni generatore di  $C_0(S_{\bullet}(X))$  appartiene a  $F + B_0(S_{\bullet}(X))$  e questo implica che  $F + B_0(S_{\bullet}(X)) = C_0(S_{\bullet}(X))$ .

Sia  $p: X \rightarrow \pi_0(X)$  l'applicazione che ad ogni punto di  $x$  associa la sua componente connessa per archi: per costruzione la sua restrizione a  $Y$  è bigettiva. Denotiamo con  $G$  il gruppo abeliano libero generato da  $\pi_0(X)$ , allora  $p$  si estende ad un omomorfismo surgettivo  $p: C_0(S_{\bullet}(X)) \rightarrow G$  e la sua restrizione  $p: F \rightarrow G$  è un isomorfismo. Per ogni cammino  $\alpha$  si ha  $p\partial\alpha = p(\alpha(1)) - p(\alpha(0)) = 0$  e quindi  $p(B_0(S_{\bullet}(X))) = 0$ . Ma questo implica che  $F \cap B_0(S_{\bullet}(X)) = 0$  e di conseguenza che  $C_0(S_{\bullet}(X)) = F \oplus B_0(S_{\bullet}(X))$ .  $\square$

PROPOSIZIONE 4.4.7. *Siano  $X$  uno spazio topologico e  $x_0 \in X$  un punto base. Esiste allora un omomorfismo canonico di gruppi  $\theta: \pi_1(X, x_0) \rightarrow H_1(X)$ .*

DIMOSTRAZIONE. Iniziamo per definire  $\theta$  insiemisticamente e dimostriamo successivamente che è un omomorfismo. Sia  $\alpha: [0, 1] \rightarrow X$  è un cammino chiuso con punto base  $\alpha(0) = \alpha(1) = x_0$ , allora lo 1-simplesso singolare  $\alpha'(1-t, t) = \alpha(t)$  è un ciclo in  $C_1(S_{\bullet}(X))$ : infatti

$$\partial\alpha' = \partial_0\alpha' - \partial_1\alpha' = \alpha'(0, 1) - \alpha'(1, 0) = \alpha(1) - \alpha(0) = x_0 - x_0 = 0.$$

Se  $\alpha, \beta: [0, 1] \rightarrow X$  sono due cammini chiusi omotopi e con punto base  $x_0$ , vogliamo dimostrare che la differenza  $\alpha' - \beta'$  è un bordo in  $C(S_{\bullet}(X))$  e quindi che i cicli  $\alpha'$  e  $\beta'$  definiscono la stessa classe di omologia.

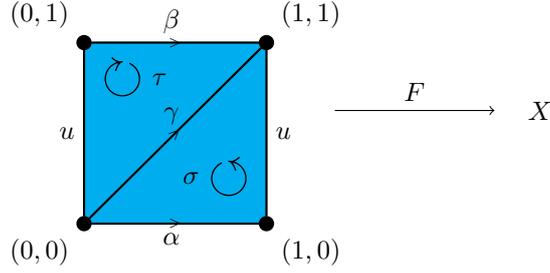
Denotiamo con  $u: [0, 1] \rightarrow X$  il cammino costante  $u(t) = x_0$ . Per ipotesi esiste un'omotopia di cammini  $F: [0, 1]^2 \rightarrow X$ :

$$F(t, 0) = \alpha(t), \quad F(t, 1) = \beta(t), \quad F(0, s) = F(1, s) = x_0, \quad s, t \in [0, 1].$$

Consideriamo adesso il cammino "diagonale"  $\gamma: [0, 1] \rightarrow X$ ,  $\gamma(t) = F(t, t)$  ed i due semplici singolari (vedi Figura 2)  $\sigma, \tau: \Delta_{\mathbb{R}}^2 \rightarrow X$ ,

$$\sigma(t_0, t_1, t_2) = F(t_0(0, 0) + t_1(1, 0) + t_2(1, 1)) = F(t_1 + t_2, t_2),$$

$$\tau(t_0, t_1, t_2) = F(t_0(0, 0) + t_1(0, 1) + t_2(1, 1)) = F(t_2, t_1 + t_2).$$

FIGURA 2. I cammini chiusi  $\alpha$  e  $\beta$  sono omologhi.

Le facce di  $\sigma, \tau$  sono (ricordarsi che  $t_0 + t_1 + t_2 = 1$ ):

$$\begin{aligned} \partial_0\sigma(t_0, t_1) &= \sigma(0, t_0, t_1) = F(1, t_1) = u(t_1) = u'(t_0, t_1), & \Rightarrow \partial_0\sigma &= u', \\ \partial_1\sigma(t_0, t_1) &= \sigma(t_0, 0, t_1) = F(t_1, t_1) = \gamma(t_1) = \gamma'(t_0, t_1), & \Rightarrow \partial_1\sigma &= \gamma', \\ \partial_2\sigma(t_0, t_1) &= \sigma(t_0, t_1, 0) = F(t_1, 0) = \alpha(t_1) = \alpha'(t_0, t_1), & \Rightarrow \partial_2\sigma &= \alpha', \\ \partial_0\tau(t_0, t_1) &= \tau(0, t_0, t_1) = F(t_1, 1) = \beta(t_1) = \beta'(t_0, t_1), & \Rightarrow \partial_0\tau &= \beta', \\ \partial_1\tau(t_0, t_1) &= \tau(t_0, 0, t_1) = F(t_1, t_1) = \gamma(t_1) = \gamma'(t_0, t_1), & \Rightarrow \partial_1\tau &= \gamma', \\ \partial_2\tau(t_0, t_1) &= \tau(t_0, t_1, 0) = F(0, t_1) = u(t_1) = u'(t_0, t_1), & \Rightarrow \partial_2\tau &= u', \end{aligned}$$

da cui segue

$$\partial(\sigma - \tau) = (\partial_0 - \partial_1 + \partial_2)(\sigma - \tau) = \alpha' - \beta'.$$

La precedente costruzione  $\alpha \mapsto \alpha'$  permette quindi di definire un'applicazione di insiemi  $\theta: \pi(X, x_0) \rightarrow H_1(X)$ . Se  $\sigma \in S_2(X)$  è il semplice che vale costantemente  $x_0$ , allora  $\partial\sigma = u' - u' + u' = u'$  e quindi  $u'$  è un bordo.

Per concludere resta da dimostrare che per ogni coppia di cammini chiusi  $\alpha, \beta: [0, 1] \rightarrow X$  con punto base  $x_0$  si ha  $\theta(\alpha\beta) = \alpha' + \beta'$  in  $H_1(X)$ . Si consideri il 2-simplesso singolare

$$\sigma(s_0, s_1, s_2) = \begin{cases} \alpha(s_1 + 2s_2) = \alpha(1 + s_2 - s_0) & \text{se } s_0 \geq s_2 \\ \beta(s_2 - s_0) = \beta(2s_2 + s_1 - 1) & \text{se } s_0 \leq s_2 \end{cases}.$$

Se  $s_0 = s_2$  allora  $s_1 + 2s_2 = 1$  e  $s_2 - s_0 = 0$  e quindi  $\sigma$  è ben definito poiché  $\alpha(1) = \beta(0)$ . Si ha:

$$\partial_0\sigma(t_0, t_1) = \sigma(0, t_0, t_1) = \beta(t_1) = \beta'(t_0, t_1)$$

$$\partial_2\sigma(t_0, t_1) = \sigma(t_0, t_1, 0) = \alpha(t_1) = \alpha'(t_0, t_1)$$

$$\partial_1\sigma(t_0, t_1) = \sigma(t_0, 0, t_1) = \begin{cases} \alpha(2t_1) & \text{se } t_1 \leq t_0 \iff t_1 \leq 1/2 \\ \beta(t_1 - t_0) = \beta(2t_1 - 1) & \text{se } t_1 \geq t_0 \iff t_1 \geq 1/2 \end{cases}$$

Ricordando la definizione di prodotto di giunzione di cammini chiusi si ha dunque che  $\partial_1\sigma = (\alpha\beta)'$  è omologo (=equivalente in omologia) a  $\partial_0\sigma + \partial_2\sigma = \alpha' + \beta'$ .  $\square$

Riportiamo senza dimostrazione, che è lunga ma non particolarmente difficile, il seguente risultato che estende la precedente proposizione.

**TEOREMA 4.4.8.** *Siano  $X$  uno spazio topologico connesso per archi e  $x_0 \in X$  un punto base. Allora l'omomorfismo  $\theta: \pi_1(X, x_0) \rightarrow H_1(X)$  è surgettivo ed ha come nucleo il sottogruppo dei commutatori, ossia il sottogruppo generato da tutti i prodotti del tipo  $\alpha\beta\alpha^{-1}\beta^{-1}$  al variare di  $\alpha, \beta \in \pi_1(X, x_0)$ .*

Possiamo reinterpretare il teorema dicendo che negli spazi connessi per archi, il primo gruppo di omologia è il più grande quoziente abeliano del gruppo fondamentale.

*La costruzione dei semplici singolari commuta con i prodotti:* infatti, per ogni coppia di spazi topologici  $X_1, X_2$ , dare un'applicazione continua  $\alpha: \Delta_{\mathbb{R}}^n \rightarrow X_1 \times X_2$  è la stessa cosa che

dare le due componenti  $\alpha_i: \Delta_{\mathbb{R}}^n \rightarrow X_i$ ,  $i = 1, 2$ . Ne segue che esiste un isomorfismo canonico

$$S_{\bullet}(X_1 \times X_2) = S_{\bullet}(X_1) \times S_{\bullet}(X_2).$$

Ogni applicazione continua  $\phi: X \rightarrow Y$  induce per composizione un morfismo di insiemi simpliciali  $\phi_{\bullet}: S_{\bullet}(X) \rightarrow S_{\bullet}(Y)$ :

$$\phi_n: S_n(X) \rightarrow S_n(Y), \quad \phi_n \alpha = \phi \circ \alpha, \quad \alpha: \Delta_{\mathbb{R}}^n \rightarrow X.$$

Infatti, per ogni  $f: [n] \rightarrow [m]$  ed ogni  $\alpha \in S_m(X)$  si ha:

$$f^*(\phi_n \alpha) = (\phi_n \alpha) \circ f_{\mathbb{R}} = \phi \circ \alpha \circ f_{\mathbb{R}} = \phi \circ (f^* \alpha) = \phi_n(f^* \alpha).$$

È chiaro che se  $\phi$  è un omeomorfismo, allora  $\phi_{\bullet}$  è un isomorfismo di insiemi simpliciali.

Di conseguenza ogni applicazione continua  $\phi: X \rightarrow Y$  induce un morfismo di complessi di catene  $\phi: C(S_{\bullet}(X)) \rightarrow C(S_{\bullet}(Y))$  e quindi dei morfismi tra gruppi di omologia singolare

$$\phi: H_n(X) \rightarrow H_n(Y).$$

DEFINIZIONE 4.4.9. Per ogni  $p \geq 0$  è definito in maniera canonica un morfismo di insiemi simpliciali

$$(-)_{\mathbb{R}}: \Delta[p]_{\bullet} \rightarrow S_{\bullet}(\Delta_{\mathbb{R}}^p), \quad f \mapsto f_{\mathbb{R}}.$$

Infatti, per ogni  $\alpha \in \Delta[p]_m$  ed ogni  $f: [n] \rightarrow [m]$  si ha

$$f^*(\alpha_{\mathbb{R}}) = \alpha_{\mathbb{R}} \circ f_{\mathbb{R}} = (\alpha \circ f)_{\mathbb{R}} = (f^* \alpha)_{\mathbb{R}}.$$

Per future applicazioni è utile osservare che se  $f: [n] \rightarrow [p]$  è il morfismo costante  $f(i) = k$ ,  $\forall i$ , allora  $f_{\mathbb{R}}: \Delta_{\mathbb{R}}^n \rightarrow \Delta_{\mathbb{R}}^p$  vale costantemente  $e_k$ .

LEMMA 4.4.10. Per ogni spazio topologico  $X$  le due applicazioni continue

$$j_0, j_1: X \rightarrow X \times \Delta_{\mathbb{R}}^1, \quad j_0(x) = (x, e_0), \quad j_1(x) = (x, e_1),$$

inducono lo stesso morfismo in omologia singolare

$$j_0 = j_1: H_*(X) \rightarrow H_*(X \times \Delta_{\mathbb{R}}^1).$$

(Nota: vedremo a posteriori che  $j_0, j_1$  sono isomorfismi in omologia in quanto equivalenze omotopiche).

DIMOSTRAZIONE. Definiamo il morfismo di insiemi simpliciali

$$H: S_{\bullet}(X) \times \Delta[1]_{\bullet} \rightarrow S_{\bullet}(X) \times S_{\bullet}(\Delta_{\mathbb{R}}^1) = S_{\bullet}(X \times \Delta_{\mathbb{R}}^1), \quad H(x, f) = (x, f_{\mathbb{R}}).$$

Siano  $i_0, i_1: S_{\bullet}(X) \rightarrow S_{\bullet}(X) \times \Delta[1]_{\bullet}$  i morfismi di insiemi simpliciali definiti nel Corollario 4.2.4. È chiaro dalle definizioni che per  $a = 0, 1$  si ha

$$j_a = Hi_a: S_{\bullet}(X) \rightarrow S_{\bullet}(X) \times \Delta[1]_{\bullet} \rightarrow S_{\bullet}(X \times \Delta_{\mathbb{R}}^1)$$

e siccome  $i_0, i_1$  inducono lo stesso morfismo in omologia, a maggior ragione lo stesso vale per  $j_0, j_1$ .  $\square$

Ricordiamo che due applicazioni continue  $f, g: X \rightarrow Y$  si dicono omotope se esiste un'applicazione continua  $F: X \times [0, 1] \rightarrow Y$  tale che  $f(x) = F(x, 0)$  e  $g(x) = F(x, 1)$ . Usando l'omeomorfismo canonico

$$[0, 1] \rightarrow \Delta_{\mathbb{R}}^1, \quad t \mapsto (1-t)e_0 + te_1,$$

possiamo dire che  $f$  è omotopa a  $g$  se esiste un'applicazione continua  $F: X \times \Delta^1(\mathbb{R}) \rightarrow Y$  tale che  $f(x) = F(x, e_0)$ ,  $g(x) = F(x, e_1)$ .

TEOREMA 4.4.11. Due applicazioni continue omotope  $f, g: X \rightarrow Y$  inducono gli stessi morfismi in omologia  $f = g: H_n(X) \rightarrow H_n(Y)$ .

DIMOSTRAZIONE. Sia  $F: X \times \Delta_{\mathbb{R}}^1 \rightarrow Y$  continua tale che  $f = Fj_0$  e  $g = Fj_1$ . Siccome le due immersioni  $j_0, j_1: X \rightarrow X \times \Delta_{\mathbb{R}}^1$  inducono gli stessi morfismi in omologia, a maggior ragione lo stesso vale per le composizioni  $Fj_0$  e  $Fj_1$ .  $\square$

In particolare se  $f: X \rightarrow X$  è omotopa all'identità, allora  $f$  induce l'identità in omologia.

Ricordiamo che un'applicazione continua  $f: X \rightarrow Y$  si dice un'equivalenza omotopica se esiste  $g: Y \rightarrow X$  continua e tale che entrambe le composizioni  $gf$  e  $fg$  sono omotope all'identità, su  $X$  e  $Y$  rispettivamente.

**COROLLARIO 4.4.12.** *Ogni equivalenza omotopica induce isomorfismi in omologia.*

**DIMOSTRAZIONE.** Siano  $f: X \rightarrow Y$  e  $g: Y \rightarrow X$  continue con entrambe le composizioni  $gf$  e  $fg$  omotope all'identità. Allora entrambe le composizioni

$$H_n(X) \xrightarrow{f} H_n(Y) \xrightarrow{g} H_n(X), \quad H_n(Y) \xrightarrow{g} H_n(X) \xrightarrow{f} H_n(Y),$$

sono le applicazioni identiche e quindi  $g$  è l'inversa di  $f$  in omologia.  $\square$

In particolare tutti gli spazi topologici contraibili (ad esempio i sottoinsiemi convessi di  $\mathbb{R}^n$ ) hanno la stessa omologia del punto.

Enunciamo adesso senza dimostrazione alcuni teoremi riguardanti l'omologia singolare.

**TEOREMA 4.4.13 (Omologia delle sfere).** *Sia  $S^n = \{x \in \mathbb{R}^{n+1} \mid \|x\| = 1\}$  la sfera di dimensione  $n$ . Per ogni  $n > 0$  si ha:*

$$H_0(S^n) = H_n(S^n) = \mathbb{Z}, \quad H_i(S^n) = 0 \text{ per ogni } i \neq 0, n.$$

*In particolare  $S^n$  è omotopicamente equivalente a  $S^m$  se e solo se  $n = m$ . Più in generale, se  $X = S^{n_1} \times \cdots \times S^{n_k}$  è un prodotto di sfere, con  $n_i > 0$  per ogni  $i$ , allora per ogni  $m$  il gruppo  $H_m(X)$  è abeliano libero di rango uguale al numero di sottoinsiemi  $A \subset \{1, \dots, k\}$  tali che  $m = \sum_{i \in A} n_i$ .*

Ad esempio, se  $n_i = 1$  per ogni  $i$ , ossia  $X = (S^1)^k$ , allora il gruppo  $H_m(X)$  è abeliano libero di rango  $\binom{k}{m}$ .

**TEOREMA 4.4.14.** *Se  $X$  è una varietà differenziabile compatta, i gruppi di omologia  $H_i(X)$  sono finitamente generati.*

**TEOREMA 4.4.15.** *Sia  $|K| \subset \mathbb{R}^n$  la realizzazione geometrica di un complesso simpliciale astratto  $K$ . Allora  $H_n(|K|) = H_n(K)$  per ogni  $n$ .*

**TEOREMA 4.4.16 (Successione esatta di Mayer-Vietoris).** *Siano  $U, V \subset X$  due aperti tali che  $X = U \cup V$ . Allora esiste una successione esatta lunga*

$$\cdots \rightarrow H_n(U \cap V) \rightarrow H_n(U) \oplus H_n(V) \rightarrow H_n(X) \rightarrow H_{n-1}(U \cap V) \rightarrow \cdots \rightarrow H_0(X) \rightarrow 0.$$

*Se l'inclusione  $U \cap V \subseteq V$  induce un isomorfismo in omologia, allora anche l'inclusione  $U \subseteq X$  induce un isomorfismo in omologia.*

La dimostrazione della successione esatta di Mayer-Vietoris in omologia singolare è in parte simile al caso dei complessi simpliciali, ma con una complicazione aggiuntiva. Infatti le inclusioni  $U \subset X$  e  $V \subset X$  inducono due inclusioni di insiemi simpliciali  $S_\bullet(U) \subset S_\bullet(X)$ ,  $S_\bullet(V) \subset S_\bullet(X)$  tali che  $S_\bullet(U) \cap S_\bullet(V) = S_\bullet(U \cap V)$  e lo stesso argomento usato nella dimostrazione del Teorema 3.3.2 mostra che esiste una successione esatta

$$\begin{aligned} \cdots \rightarrow H_n(U \cap V) \rightarrow H_n(U) \oplus H_n(V) \rightarrow H_n(S_\bullet(U) \cup S_\bullet(V)) \rightarrow H_{n-1}(U \cap V) \rightarrow \cdots \\ \cdots \rightarrow H_0(U) \oplus H_0(V) \rightarrow H_0(S_\bullet(U) \cup S_\bullet(V)) \rightarrow 0. \end{aligned}$$

Data la natura dei semplici singolari in generale si ha  $S_\bullet(U) \cup S_\bullet(V) \neq S_\bullet(X)$  e quindi per concludere è necessario ricorrere al seguente teorema.

**TEOREMA 4.4.17 (di suddivisione dei semplici).** *Sia  $X = \cup_i U_i$  un (qualunque) ricoprimento aperto di uno spazio topologico  $X$ . Allora l'inclusione di insiemi simpliciali*

$$\bigcup_i S_\bullet(U_i) \subset S_\bullet(X)$$

*induce un'equivalenza omotopica di complessi di catene*

$$C_*\left(\bigcup_i S_\bullet(U_i)\right) = \bigoplus_i C_*(S_\bullet(U_i)) \rightarrow C_*(S_\bullet(X))$$

e di conseguenza un isomorfismo in omologia

$$H_n\left(\bigcup_i S_\bullet(U_i)\right) = H_n(S_\bullet(X)), \quad \forall n.$$

#### 4.5. Omologia con coefficienti

Sia  $X_\bullet$  un insieme simpliciale. Abbiamo definito il gruppo delle  $p$ -catene  $C_p(X_\bullet)$  come il gruppo abeliano libero generato da  $X_p$ . Dato che i gruppi abeliani liberi sono anche detti  $\mathbb{Z}$ -moduli liberi, spesso si usa la notazione  $H_n(X_\bullet, \mathbb{Z})$  per indicare  $H_n(X_\bullet)$ . La stessa notazione si applica sia ai complessi simpliciali astratti, sia agli spazi topologici.

La stessa identica costruzione si può fare considerando un qualsiasi campo  $\mathbb{K}$  e definire  $C_p(X_\bullet, \mathbb{K})$  come lo spazio vettoriale su  $\mathbb{K}$  generato da  $X_p$ . Tutta la teoria generale si comporta allo stesso modo (con spazi vettoriali al posto di gruppi abeliani ed applicazioni lineari al posto degli omomorfismi) ed otteniamo un complesso di catene  $C(X_\bullet, \mathbb{K})$  i cui spazi vettoriali di omologia sono denotati  $H_n(X_\bullet, \mathbb{K})$ . Lo stesso si può fare per complessi simpliciali astratti e spazi topologici.

In linea teorica, lo studio dei gruppi  $H_n(X, \mathbb{K})$  non ci fornisce alcuna ulteriore informazione su  $X$  dato che per un teorema generale di algebra omologica (lo studio dei complessi di catene) detto **teorema dei coefficienti universali**, i gruppi  $H_n(X, \mathbb{Z}) = H_n(X)$  determinano univocamente i gruppi  $H_n(X, \mathbb{K})$ . Ad esempio è abbastanza facile dimostrare che se  $\mathbb{K}$  è un campo di caratteristica 0, allora  $H_n(X, \mathbb{K})$  è uno spazio vettoriale di dimensione uguale al rango di  $H_n(X, \mathbb{Z})$ . Se la caratteristica del campo è positiva allora la dimensione è maggiore od uguale al rango e la differenza dipende (in maniera ben definita ma di lunga e laboriosa descrizione) dal sottogruppo di torsione di  $H_{n-1}(X, \mathbb{Z})$ .

Tuttavia, lo studio dei gruppi di omologia con coefficienti è importante per almeno tre ordini di motivi:

- (1) i gruppi  $H_n(X, \mathbb{K})$  sono generalmente più semplici da calcolare rispetto ai gruppi  $H_n(X)$ . Ad esempio in *topologia computazionale*, dove si ha a che fare con complessi simpliciali astratti  $K$  con moltissimi vertici, il calcolo di  $H_n(K, \mathbb{Z}/(2))$  richiede una potenza computazionale molto minore di quella necessaria per determinare  $H_n(K, \mathbb{Z})$ .
- (2) alcuni teoremi generali forniscono strumenti per calcolare i gruppi  $H_n(X, \mathbb{K})$  per opportuni campi  $\mathbb{K}$  ma non i gruppi  $H_n(X, \mathbb{Z})$ . Ad esempio, per  $X$  varietà differenziabile, il *teorema di de Rham* fornisce una ricetta per il calcolo degli spazi vettoriali duali di  $H_n(X, \mathbb{R})$  in termini di forme differenziali su  $X$ .
- (3) i gruppi  $H_n(X, \mathbb{K})$  intervengono naturalmente in svariate teorie matematiche. Ad esempio:
  - (a) con  $\mathbb{K} = \mathbb{Z}/2$  in *omologia persistente* e nella teoria delle *classi caratteristiche*;
  - (b) con  $\mathbb{K} = \mathbb{Q}$  in *omotopia razionale* e *teoria di Hodge*;
  - (c) con  $\mathbb{K} = \mathbb{R}, \mathbb{C}$  in *geometria algebrica* e *teoria di de Rham*.



## Spazi pseudometrici

Vogliamo introdurre una struttura matematica che si pone a metà strada tra gli spazi metrici e gli spazi topologici.

Innanzitutto estendiamo, nel modo naturale, la relazione di ordine e l'operazione di somma all'insieme  $[0, +\infty] = [0, +\infty] \cup \{+\infty\}$ , ossia:

$$a + \infty = +\infty, \quad a \leq +\infty, \quad \forall a \in [0, +\infty].$$

Notiamo che, con tale ordinamento, ogni sottoinsieme di  $[0, +\infty]$  possiede estremo inferiore ed estremo superiore. È curioso osservare che, in totale spregio all'intuizione, nel caso del sottoinsieme vuoto  $\emptyset \subset [0, +\infty]$  si ha

$$\inf \emptyset = +\infty > 0 = \sup \emptyset :$$

Infatti  $[0, +\infty]$  è contemporaneamente l'insieme dei maggioranti e dei minoranti del sottoinsieme vuoto.

**DEFINIZIONE 5.0.1.** Uno **spazio pseudo-metrico** è una coppia  $(X, d)$  con  $X$  insieme e  $d: X \times X \rightarrow [0, +\infty]$  un'applicazione, detta **pseudo-distanza** o più semplicemente **distanza**, che soddisfa le seguenti proprietà:

- (1)  $d(x, x) = 0$  per ogni  $x \in X$ ;
- (2)  $d(x, y) = d(y, x)$  per ogni  $x, y \in X$ ;
- (3)  $d(x, y) \leq d(x, z) + d(z, y)$  per ogni  $x, y, z \in X$ .

È immediato dalle definizioni che uno spazio pseudo-metrico  $(X, d)$  è uno spazio metrico nel senso usuale se in aggiunta alle precedenti valgono le due ulteriori condizioni:

- $d(x, y) = 0$  solo se  $x = y$ ;
- $d(x, y) < +\infty$  per ogni  $x, y \in X$ .

Nelle prossime sezioni, dopo aver studiato le prime proprietà degli spazi pseudo-metrici, illustreremo alcuni esempi che rivestiranno un certo interesse nel prossimo capitolo.

### 5.1. Proprietà ed esempi basilari

Ogni spazio metrico è un esempio di spazio pseudo-metrico. Ogni spazio pseudo-metrico  $(X, d)$  è anche uno spazio topologico, con gli aperti definiti nel modo usuale, ossia  $U \subset X$  è aperto se e solo se per ogni  $x \in U$  esiste  $r > 0$  tale che  $B_d(x, r) = \{y \in X \mid d(x, y) < r\} \subset U$ .

**DEFINIZIONE 5.1.1.** Diremo che uno spazio pseudo-metrico  $(X, d)$  è **di Hausdorff** se  $d(x, y) \neq 0$  per ogni  $x \neq y$ .

È immediato verificare che uno spazio pseudo-metrico è di Hausdorff se e solo se la topologia indotta è di Hausdorff.

**ESEMPIO 5.1.2.** Siano  $(X, d)$  uno spazio pseudo-metrico e  $f: Y \rightarrow X$  un'applicazione qualsiasi. Allora la funzione

$$\delta: Y \times Y \rightarrow [0, +\infty], \quad \delta(y_1, y_2) = d(f(y_1), f(y_2)),$$

è una pseudo-distanza su  $Y$ .

ESEMPIO 5.1.3. Sia  $X$  l'insieme delle funzioni  $f: \mathbb{R} \rightarrow \mathbb{R}$  monotone decrescenti, ossia tali che  $f(x) \leq f(y)$  per ogni  $x \geq y$ .

Date  $f, g \in X$  definiamo

$$I(f, g) = \{\epsilon \in [0, +\infty[ \mid f(x) \geq g(x + \epsilon) \text{ e } g(x) \geq f(x + \epsilon) \quad \forall x \in \mathbb{R}\}$$

$$d_{\bowtie}(f, g) = \begin{cases} +\infty & \text{se } I(f, g) = \emptyset \\ \inf I(f, g) & \text{se } I(f, g) \neq \emptyset \end{cases}.$$

Allora la coppia  $(X, d_{\bowtie})$  è uno spazio pseudo-metrico.

Le condizioni  $d_{\bowtie}(f, f) = 0$  e  $d_{\bowtie}(f, g) = d_{\bowtie}(g, f)$  sono evidenti, così come la disuguaglianza triangolare  $d_{\bowtie}(f, g) \leq d_{\bowtie}(f, h) + d_{\bowtie}(h, g)$  qualora  $d_{\bowtie}(f, h) + d_{\bowtie}(h, g) = +\infty$ . Supponiamo quindi che  $a = d_{\bowtie}(f, h) < +\infty$  e  $b = d_{\bowtie}(h, g) < +\infty$ . Siccome ogni funzione in  $X$  è decrescente, se  $\epsilon \in I(f, g)$  e  $\delta > \epsilon$ , allora  $\delta \in I(f, g)$ , ciò significa che per ogni  $\epsilon > 0$  ed ogni  $x \in \mathbb{R}$  vale

$$f(x) \geq h(x + a + \epsilon), \quad h(x) \geq f(x + a + \epsilon), \quad h(x) \geq g(x + b + \epsilon), \quad g(x) \geq h(x + b + \epsilon),$$

da cui segue

$$f(x) \geq h(x + a + \epsilon) \geq g(x + a + b + 2\epsilon), \quad g(x) \geq h(x + b + \epsilon) \geq f(x + a + b + 2\epsilon),$$

$$a + b + 2\epsilon \in I(f, g), \quad d_{\bowtie}(f, g) \leq a + b + 2\epsilon \quad \forall \epsilon > 0.$$

Da notare che lo spazio pseudo-metrico  $(X, d_{\bowtie})$  **non** è di Hausdorff. Infatti per le funzioni

$$f(x) = \begin{cases} 1 & \text{se } x \leq 0 \\ 0 & \text{se } x > 0 \end{cases}, \quad g(x) = \begin{cases} 1 & \text{se } x < 0 \\ 0 & \text{se } x \geq 0 \end{cases},$$

vale  $f(x) \geq g(x) \geq f(x + \epsilon)$  per ogni  $x$  ed ogni  $\epsilon > 0$  da cui segue  $d_{\bowtie}(f, g) = 0$ .

ESEMPIO 5.1.4. Sia  $(X, d)$  uno spazio pseudo-metrico e consideriamo l'applicazione

$$\delta: X \times X \rightarrow [0, +\infty], \quad \delta(x, y) = \min(1, d(x, y)).$$

Allora  $\delta$  è una pseudo-distanza che induce la stessa topologia di  $d$ .

Dato uno spazio pseudo-metrico  $(X, d)$  segue immediatamente dalle proprietà di  $d$  che la relazione “ $x \sim y$  se e solo se  $d(x, y) = 0$ ” è una relazione di equivalenza. Se  $x_1 \sim x_2$  e  $y_1 \sim y_2$ , per la disuguaglianza triangolare si ottiene

$$d(x_2, y_2) \leq d(x_2, x_1) + d(x_1, y_1) + d(y_1, y_2) = d(x_1, y_1),$$

$$d(x_1, y_1) \leq d(x_1, x_2) + d(x_2, y_2) + d(y_2, y_1) = d(x_2, y_2),$$

e quindi  $d(x_1, y_1) = d(x_2, y_2)$ , ossia  $d$  si fattorizza ad una applicazione al quoziente

$$d: \frac{X}{\sim} \times \frac{X}{\sim} \rightarrow [0, +\infty].$$

Lasciamo al lettore la semplice verifica che  $(X/\sim, d)$  è uno spazio pseudo-metrico di Hausdorff.

DEFINIZIONE 5.1.5. Sia  $(X, d)$  uno spazio pseudo-metrico. Per ogni sottoinsieme  $A \subset X$ , l'applicazione *distanza da A* è definita come:

$$d_A: X \rightarrow [0, +\infty], \quad d_A(x) = \inf_{y \in A} d(x, y).$$

Ad esempio, se  $A = X$  allora  $d_A$  vale costantemente 0, mentre se  $A = \emptyset$  allora  $d_A$  vale costantemente  $+\infty$ .

LEMMA 5.1.6. Siano  $(X, d)$  uno spazio pseudo-metrico e  $A \subset X$ . Allora per ogni  $x, y \in X$  vale la disuguaglianza “triangolare”:

$$d_A(x) \leq d_A(y) + d(x, y).$$

DIMOSTRAZIONE. Non è restrittivo supporre  $d_A(y) + d(x, y) < +\infty$  ed è sufficiente dimostrare che  $d_A(x) \leq d_A(y) + d(x, y) + r$  per ogni  $r > 0$ .

Sia dunque  $r > 0$  fissato, siccome  $d_A(y) < +\infty$  esiste  $z \in A$  tale che  $d(y, z) \leq d_A(y) + r$ . Ma allora

$$d_A(x) \leq d(x, z) \leq d(y, z) + d(y, x) \leq d_A(y) + r + d(x, y).$$

□

LEMMA 5.1.7. *Siano  $(X, d)$  uno spazio pseudo-metrico e  $A \subset X$ . Allora, nella topologia indotta dalla pseudo-metrica, per ogni  $r \in [0, +\infty]$  l'insieme*

$$V_r(A) = \{x \in X \mid d_A(x) < r\} = \{x \in X \mid B_d(x, r) \cap A \neq \emptyset\}$$

è un aperto e

$$\overline{A} = \{x \in X \mid d_A(x) = 0\},$$

è la chiusura di  $A$ .

DIMOSTRAZIONE. Se  $r = 0$  allora  $V_r(A) = \emptyset$ . Se  $r > 0$  e  $x \in V_r(A)$ , per definizione di  $d_A$  esiste un punto  $a \in A$  tale che  $d_A(x) \leq d(x, a) < r$ . Preso un  $\delta > 0$  tale che  $d(x, a) + \delta < r$ , segue dalla disuguaglianza triangolare che  $d(a, z) < r$  per ogni  $z \in B_d(x, \delta)$  da cui segue  $x \in B_d(x, \delta) \subset V_r(A)$ .

Sia  $x \in X$ ; per definizione di chiusura vale  $x \in \overline{A}$  se e solo se per ogni  $\delta > 0$  esiste  $y \in A$  tale che  $d(x, y) < \delta$  e questo vale se e solo se  $d_A(x) = 0$ . □

LEMMA 5.1.8. *Siano  $(X, d)$  e  $(Y, \delta)$  due spazi pseudo-metrici e sia  $f: X \rightarrow Y$  un'applicazione di Lipschitz, ossia esiste un numero reale positivo  $C > 0$  tale che  $\delta(f(x), f(y)) \leq Cd(x, y)$  per ogni  $x, y \in X$ . Allora  $f$  è continua rispetto alle topologie indotte dalle pseudo-distanze.*

DIMOSTRAZIONE. Esercizio. □

ESEMPIO 5.1.9. Sia  $X$  insieme dotato di una funzione  $f: X \times X \rightarrow [0, +\infty]$  tale che  $f(x, x) = 0$  per ogni  $x$  e  $f(x, y) = f(y, x)$  per ogni  $x, y \in X$ . Ad esempio,  $X$  può essere un grafo semplice pesato e  $f(x, y)$  l'inverso del peso del lato di estremi  $x, y$ .

Partendo da  $f$  possiamo definire diverse pseudo-distanze su  $X$ , come ad esempio:

(1) **distanza del minimo cammino (shortest-path)**

$$d_s(x, y) = \inf_{S(x, y)} \sum_i f(x_i, x_{i+1});$$

(2) **distanza del collo di bottiglia (bottleneck)**<sup>1</sup>

$$d_b(x, y) = \inf_{S(x, y)} \max_i f(x_i, x_{i+1});$$

dove entrambi gli estremi inferiori sono presi sull'insieme  $S(x, y)$  di tutte le successioni finite  $x_0, x_1, \dots, x_n \in X$  tali che  $x_0 = x$  e  $x_n = y$ . La verifica che si tratta di pseudo-distanze è quasi ovvia.

## 5.2. Le distanze di Hausdorff e del collo di bottiglia

Dato uno spazio pseudo-metrico  $(X, d)$  esistono varie costruzioni di pseudo-distanze sull'insieme delle parti  $\mathcal{P}(X)$ ; in questa sezione ne vedremo due, dette rispettivamente *distanza di Hausdorff* e *distanza del collo di bottiglia*.

Per ogni sottoinsieme  $A \subset X$  ed ogni  $r \in [0, +\infty]$  abbiamo definito il sottoinsieme

$$V_r(A) = \{x \in X \mid d_A(x) < r\} = \{x \in X \mid B_d(x, r) \cap A \neq \emptyset\}$$

che abbiamo visto essere aperto nella topologia indotta.

DEFINIZIONE 5.2.1. Dati due sottoinsiemi  $A, B$  di uno spazio pseudo-metrico  $(X, d)$ , la loro **distanza di Hausdorff** è definita come

$$d_H(A, B) = \inf\{r \in [0, +\infty] \mid A \subset V_r(B) \text{ e } B \subset V_r(A)\}.$$

<sup>1</sup>Sarebbe più corretto dire "distanza del cammino con il minimo collo di bottiglia".

È chiara la simmetria  $d_H(A, B) = d_H(B, A)$  mentre dal fatto che  $A \subset \bar{A}$  segue che  $d_H(A, A) = 0$ . Si noti che se  $A = \emptyset$  allora  $d_H(A, B) = +\infty$  qualunque sia  $B$ .

Rimane da dimostrare la disuguaglianza triangolare, ossia che per  $A, B, C$  sottoinsiemi di  $X$  vale  $d_H(A, B) \leq d_H(A, C) + d_H(C, B)$ .

Non è restrittivo supporre  $d_H(A, C) + d_H(C, B) < +\infty$  e denotiamo  $r = d_H(A, C)$ ,  $s = d_H(C, B)$ . Per simmetria basta dimostrare che per ogni  $\varepsilon > 0$  vale  $A \subset V_B(r + s + 2\varepsilon)$ , ossia che per ogni  $a \in A$  esiste  $x \in B$  tale che  $d(a, x) < r + s + 2\varepsilon$ .

Sia  $a \in A$ , allora esiste  $y \in C$  tale che  $d(a, y) < r + \varepsilon$ . Poi esiste  $x \in B$  tale che  $d(y, x) < s + \varepsilon$  e tutto segue dalla disuguaglianza triangolare per la distanza  $d$ .

**ESEMPIO 5.2.2.** Nel piano  $\mathbb{R}^2$ , dotato della distanza euclidea, la distanza di Hausdorff tra un insieme limitato ed uno illimitato è  $+\infty$ . La distanza di Hausdorff tra le due circonferenze  $x^2 + y^2 = 1$  e  $(x - 5)^2 + y^2 = 1$  è 5.

**OSSERVAZIONE 5.2.3.** Nel caso di due sottoinsiemi finiti  $I, J \subseteq X$  possiamo sostituire l'estremo inferiore con il minimo e la distanza di Hausdorff può essere definita come

$$d_H(I, J) = \min \left\{ r \mid \begin{array}{l} \text{esistono applicazioni } \phi: I \rightarrow J, \psi: J \rightarrow I \text{ tali che} \\ d(x, \phi(x)) \leq r, d(y, \psi(y)) \leq r \text{ per ogni } x \in I, y \in J \end{array} \right\}.$$

**LEMMA 5.2.4.** *Dati due sottoinsiemi  $A, B$  di uno spazio pseudo-metrico  $(X, d)$ , la distanza  $d_H(A, B)$  è l'estremo inferiore dell'insieme degli  $r \in [0, +\infty]$  tali che per ogni  $a \in A$  ed ogni  $b \in B$  esistono  $x \in B$  ed  $y \in A$  tali che  $d(a, x) < r$  e  $d(b, y) < r$ .*

**DIMOSTRAZIONE.** Per simmetria basta dimostrare che per  $r \in [0, +\infty]$  fissato vale  $A \subset V_r(B)$  se e solo se per ogni  $a \in A$  esiste  $x \in B$  tale che  $d(a, x) < r$ . Questo segue immediatamente dalla definizione di  $d_A$  e dalle proprietà dell'estremo inferiore.  $\square$

Applicando l'assioma della scelta al lemma precedente otteniamo immediatamente il seguente risultato.

**LEMMA 5.2.5.** *Siano  $A, B$  sottoinsiemi di uno spazio pseudo-metrico  $(X, d)$  tali che  $d_H(A, B) < +\infty$ . Allora per ogni  $r > d_H(A, B)$  esistono due applicazioni  $f: A \rightarrow B$  e  $g: B \rightarrow A$  tali che  $d(a, f(a)) < r$  per ogni  $a \in A$  e  $d(b, g(b)) < r$  per ogni  $b \in B$ .*

**OSSERVAZIONE 5.2.6.** In certi casi può essere interessante considerare la seguente generalizzazione nella definizione della distanza di Hausdorff. Supponiamo di avere uno spazio pseudo-metrico  $(X, d)$  dotato di un'applicazione  $r: X \rightarrow [0, +\infty]$  che soddisfa la condizione

$$r(x) \leq r(y) + d(x, y) \text{ per ogni } x, y \in X.$$

Per ogni sottoinsieme  $A \subset X$  ed ogni  $t \in [0, +\infty]$  denotiamo

$$W_t(A) = \{x \in X \mid d_A(x) < t\} \cup \{x \in X \mid r(x) < t\}$$

e definiamo

$$\tilde{d}(A, B) = \inf \{t \in [0, +\infty] \mid A \subset W_t(B) \text{ e } B \subset W_t(A)\}.$$

Per mostrare che anche  $\tilde{d}$  è una pseudo-distanza si può ragionare nel modo seguente. Se  $r = d_C$  è la distanza da un sottoinsieme  $C \subset X$  si ha  $\tilde{d}(A, B) = d_H(A \cup C, B \cup C)$ . Nel caso generale prendiamo un qualsiasi insieme  $C$  non vuoto e disgiunto da  $X$ , ed estendiamo la pseudo-distanza  $d$  ad una pseudo distanza  $\delta: (X \cup C) \times (X \cup C) \rightarrow [0, +\infty]$  ponendo  $\delta(x, y) = d(x, y)$  se  $x, y \in X$ ,  $\delta(c, d) = 0$  se  $c, d \in C$  e  $\delta(x, c) = \delta(c, x) = r(x)$  se  $x \in X$  e  $c \in C$ . Allora  $r = d_C$  e ci siamo ricondotti al caso particolare.

Occupiamoci adesso della distanza bottleneck. Per future applicazioni conviene definire direttamente tale distanza nel contesto più generale dell'Osservazione 5.2.6, ossia di uno spazio pseudo-metrico  $(X, d)$  dotato di una funzione "di rumore"  $r: X \rightarrow [0, +\infty]$  tale che

$$(5.1) \quad r(x) \leq d(x, y) + r(y), \quad \forall x, y \in X.$$

Tipicamente si considera come funzione di rumore la funzione  $r = d_C$ , distanza da un sottoinsieme  $C \subset X$ , vedi Lemma 5.1.6.

Osserviamo che, siccome  $d(x, y) = d(y, x) \geq 0$  per ogni  $x, y \in X$  la condizione (5.1) equivale a dire che  $r(y) \leq r(x) + d(x, y)$  per ogni  $x, y \in X$ .

Dati due sottoinsiemi  $A, B \subset X$ , per *appaiamento parziale* tra  $A$  e  $B$  si intende una terna  $(P, Q, f)$ , con  $P \subset A$ ,  $Q \subset B$  e  $f: P \rightarrow Q$  bigettiva: è consentito a  $P, Q$  di essere vuoti. Vi è un'ovvia bigezione  $(P, Q, f) \rightarrow (Q, P, f^{-1})$  tra gli appaiamenti parziale tra  $A$  e  $B$  e quelli tra  $B$  ed  $A$ .

Definiamo il costo di un appaiamento parziale come

$$\begin{aligned} c(P, Q, f) &= \sup \left( \{d(x, f(x)) \mid x \in P\} \cup \{r(x) \mid x \in (A - P) \cup (B - Q)\} \right) \\ &= \sup \left( \{d(x, f^{-1}(x)) \mid x \in Q\} \cup \{r(x) \mid x \in (A - P) \cup (B - Q)\} \right) \\ &= c(Q, P, f^{-1}). \end{aligned}$$

Definiamo poi la **distanza bottleneck**

$$d_b(A, B) = \inf c(P, Q, f) = \inf c(Q, P, f^{-1}),$$

dove l'estremo inferiore è calcolato sull'insieme di tutti gli appaiamenti parziali tra  $A$  e  $B$ .

È immediato osservare che  $d_b(A, A) = 0$  e  $d_b(A, B) = d_b(B, A)$  per ogni  $A, B \subset X$ . La dimostrazione della disuguaglianza triangolare

$$d_b(A, B) \leq d_b(A, C) + d_b(C, B)$$

richiede invece alcune considerazioni non banali.

Ovviamente basta considerare il caso in cui  $a = d_b(A, C)$  e  $b = d_b(C, B)$  sono entrambi  $< +\infty$ . Sia  $\delta > 0$  fissato: scegliamo un appaiamento parziale  $(P, Q, f)$  di  $A$  e  $C$  tale che  $c(P, Q, f) \leq a + \delta$  ed un appaiamento parziale  $(R, S, g)$  di  $C$  e  $B$  tale che  $c(R, S, g) \leq b + \delta$ .

Possiamo allora considerare la composizione  $(f^{-1}(Q \cap R), g(Q \cap R), gf)$  che è un accoppiamento parziale di  $A$  e  $B$ . Per provare che  $d_b(A, B) \leq a + b + 2\delta$  basta dimostrare che  $c(f^{-1}(Q \cap R), g(Q \cap R), gf) \leq c(R, S, g) + c(P, Q, f)$ ; a tal fine dobbiamo analizzare separatamente 5 casi possibili:

- 1) se  $x \in A - P$ , allora  $r(x) \leq c(P, Q, f)$ ;
- 2) se  $x \in B - S$ , allora  $r(x) \leq c(R, S, g)$ ;
- 3) se  $x \in P$  e  $f(x) \notin R$  allora

$$r(x) \leq d(x, f(x)) + r(f(x)) \leq c(P, Q, f) + c(R, S, g);$$

- 4) se  $x \in S - g(R \cap Q)$  allora esiste unico  $y \in R - Q$  tale che  $x = g(y)$  e si ha

$$r(x) \leq d(x, y) + r(y) \leq c(R, S, g) + c(P, Q, f);$$

- 5) se  $x \in f^{-1}(Q \cap R)$  allora

$$d(x, gf(x)) \leq d(x, f(x)) + d(f(x), gf(x)) \leq c(P, Q, f) + c(R, S, g).$$

### 5.3. La distanza di contiguità

La distanza di contiguità si applica alla classe dei complessi simpliciali astratti filtrati, che saranno di importanza fondamentale nello studio dell'omologia persistente.

**DEFINIZIONE 5.3.1.** Sia  $K$  un complesso simpliciale astratto. Una **funzione filtrante** su  $K$  è un'applicazione  $f: K \rightarrow \mathbb{R}$  tale che se  $s \in K$  e  $r \subset s$  allora  $f(r) \leq f(s)$ .

Equivalentemente, un'applicazione  $f: K \rightarrow \mathbb{R}$  è una funzione filtrante se per ogni  $t \in \mathbb{R}$  il sottoinsieme **di livello**

$$K(t) = \{s \in K \mid f(s) \leq t\} = f^{-1}(] - \infty, t])$$

è un sottocomplesso simpliciale.

I sottocomplessi  $K(t)$  soddisfano le condizioni

$$(5.2) \quad \bigcap_t K(t) = \emptyset, \quad \bigcup_t K(t) = K, \quad K(s) = \bigcap_{t>s} K(t) \text{ per ogni } s \in \mathbb{R}.$$

Viceversa, è facile dimostrare che ogni famiglia  $K(t)$ ,  $t \in \mathbb{R}$ , di sottocomplessi simpliciali di  $K$  che soddisfa le condizioni (5.2) è la famiglia dei sottoinsiemi di livello della funzione filtrante  $f(\sigma) = \inf\{t \in \mathbb{R} \mid \sigma \in K(t)\}$ .

Per semplicità notazionale, quando non ci saranno rischi di ambiguità, chiameremo semplicemente **complesso filtrato** una coppia  $(K, f)$  con  $K$  complesso simpliciale astratto e  $f: K \rightarrow \mathbb{R}$  funzione filtrante.

ESEMPIO 5.3.2. Dato un complesso simpliciale astratto  $(K, I)$ , ogni applicazione  $f: I \rightarrow \mathbb{R}$  si estende ad una funzione filtrante

$$f: K \rightarrow \mathbb{R}, \quad f(\{x_0, \dots, x_p\}) = \max_i f(x_i).$$

ESEMPIO 5.3.3. Dato un qualunque sottoinsieme  $Y$  di uno spazio metrico  $(X, d)$ , la funzione

$$f: \Delta^Y \rightarrow [0, +\infty[, \quad f(\{y_0, \dots, y_p\}) = \frac{1}{2} \max_{i,j} d(y_i, y_j),$$

è filtrante. Il complesso filtrato  $(\Delta^Y, f)$  viene chiamato, con un leggero abuso, **filtrazione di Vietoris-Rips** di  $Y$ .

Vedremo ulteriori ed interessanti esempi di complessi filtrati nei prossimi capitoli.

DEFINIZIONE 5.3.4. Un **morfismo**  $\phi: (K, f) \rightarrow (H, g)$  di complessi filtrati è un morfismo di complessi simpliciali astratti  $\phi: K \rightarrow H$  che preserva i sottocomplessi di livello, ossia tale che  $\phi(K(t)) \subset H(t)$  per ogni  $t \in \mathbb{R}$ .

Il nostro prossimo obiettivo è quello di introdurre una struttura di spazio pseudo-metrico in una qualunque famiglia di complessi filtrati.

DEFINIZIONE 5.3.5. Sia  $\epsilon \geq 0$  un numero reale. Un  **$\epsilon$ -morfismo**  $\phi: (K, f) \rightarrow (H, g)$  di complessi filtrati è un morfismo di complessi simpliciali astratti  $\phi: K \rightarrow H$  tale che  $\phi(K(t)) \subset H(t + \epsilon)$  per ogni  $t \in \mathbb{R}$ .

È chiaro che i morfismi di complessi filtrati sono esattamente gli 0-morfismi. La composizione di un  $\epsilon$ -morfismo con un  $\varrho$ -morfismo, qualora sia definita, è un  $(\epsilon + \varrho)$ -morfismo. Infine, un  $\epsilon$ -morfismo è automaticamente un  $\varrho$ -morfismo per ogni  $\varrho \geq \epsilon$ .

La condizione  $\phi(K(t)) \subset H(t + \epsilon)$  può essere descritta in termini di funzioni filtranti grazie al seguente lemma.

LEMMA 5.3.6. *Siano  $(K, f)$ ,  $(H, g)$  due complessi filtrati ed  $\epsilon \geq 0$ . Per un morfismo di complessi simpliciali  $\phi: K \rightarrow H$  le seguenti condizioni sono equivalenti:*

- (1)  $\phi(K(t)) \subset H(t + \epsilon)$  per ogni  $t \in \mathbb{R}$ , ossia  $\phi$  è un  $\epsilon$ -morfismo;
- (2)  $g(\phi(s)) \leq f(s) + \epsilon$  per ogni  $s \in K$ .

DIMOSTRAZIONE. Se  $g(\phi(s)) \leq f(s) + \epsilon$  per ogni  $s \in K$ , allora per ogni  $t \in \mathbb{R}$  ed ogni  $s \in K(t)$  si ha  $f(s) \leq t$ ,  $g(\phi(s)) \leq f(s) + \epsilon \leq t + \epsilon$  e quindi  $\phi(s) \in H(t + \epsilon)$ .

Viceversa, se  $\phi(K(t)) \subset H(t + \epsilon)$  per ogni  $t \in \mathbb{R}$  allora, dato  $s \in K$  si ha  $s \in K(f(s))$ ; dunque  $\phi(s) \in H(f(s) + \epsilon)$  che equivale a dire  $g(\phi(s)) \leq f(s) + \epsilon$ .  $\square$

DEFINIZIONE 5.3.7. Sia  $\epsilon \geq 0$ . Una  $\epsilon$ -contiguità tra due complessi filtrati  $(K, f)$ ,  $(H, g)$  è una coppia di  $\epsilon$ -morfismi  $\phi: (K, f) \rightarrow (H, g)$ ,  $\psi: (H, g) \rightarrow (K, f)$  tale che per ogni  $t \in \mathbb{R}$  si ha:

- (1) la composizione  $\psi\phi: K(t) \rightarrow K(t + 2\epsilon)$  è contigua al morfismo di inclusione  $K(t) \subset K(t + 2\epsilon)$ ;
- (2) la composizione  $\phi\psi: H(t) \rightarrow H(t + 2\epsilon)$  è contigua al morfismo di inclusione  $H(t) \subset H(t + 2\epsilon)$ .

Diremo che due complessi filtrati sono  $\epsilon$ -contigui se esiste una  $\epsilon$ -contiguità tra loro.

Dal fatto che la relazione di contiguità commuta con le composizioni (Proposizione 3.2.9) si ha che ogni  $\epsilon$ -contiguità  $\phi: (K, f) \rightarrow (H, g)$ ,  $\psi: (H, g) \rightarrow (K, f)$ , è automaticamente una

$\rho$ -contiguità per ogni  $\rho \geq \epsilon$ . Si consideri infatti, per ogni  $t \in \mathbb{R}$ , il diagramma

$$\begin{array}{ccccccc} K(t) & \longrightarrow & K(t+2\epsilon) & \longrightarrow & K(t+\epsilon+\rho) & \longrightarrow & K(t+2\rho) \\ & \searrow \phi & & \uparrow \psi & & \uparrow \psi & \nearrow \psi \\ & & H(t+\epsilon) & \longrightarrow & H(t+\rho) & & \end{array}$$

con le frecce orizzontali i morfismi di inclusione. Siccome il triangolo a sinistra commuta a meno di contiguità, mentre il rettangolo centrale ed il triangolo a destra sono commutativi in senso stretto, tutto il diagramma è commutativo a meno di contiguità. In particolare la composizione

$$K(t) \xrightarrow{\phi} H(t+\rho) \xrightarrow{\psi} K(t+2\rho)$$

è contigua all'inclusione  $K(t) \rightarrow K(t+2\rho)$ .

DEFINIZIONE 5.3.8 (Distanza di contiguità). Dati due complessi filtrati  $(K, f)$ ,  $(H, g)$  definiamo

$$d_c((K, f), (H, g)) = \inf\{\epsilon \geq 0 \mid (K, f), (H, g) \text{ sono } \epsilon\text{-contigui}\}.$$

Poniamo inoltre  $d_c((K, f), (H, g)) = +\infty$  se non esiste alcuna  $\epsilon$ -contiguità.

È chiaro che  $d_c((K, f), (K, f)) = 0$  e che  $d_c((K, f), (H, g)) = d_c((H, g), (K, f))$ .

TEOREMA 5.3.9. *Dati tre complessi filtrati  $(K, f)$ ,  $(H, g)$  e  $(L, h)$ , si ha*

$$d_c((K, f), (L, h)) \leq d_c((K, f), (H, g)) + d_c((H, g), (L, h)).$$

*Dunque la distanza di contiguità definisce una struttura di spazio pseudo-metrico su un qualunque insieme di complessi filtrati.*

DIMOSTRAZIONE. Denotiamo con  $d_c((K, f), (H, g)) = a$ ,  $d_c((H, g), (L, h)) = b$ . Se  $\max(a, b) = +\infty$  non c'è nulla da dimostrare. Se invece  $a, b < +\infty$ , come capita spesso con le disuguaglianze triangolari, dimostriamo che per ogni  $\delta > 0$  si ha

$$d_c((K, f), (L, h)) \leq a + b + 2\delta.$$

Per ipotesi esiste  $0 \leq \epsilon \leq a + \delta$  ed una  $\epsilon$ -contiguità

$$\phi: (K, f) \rightarrow (H, g), \quad \psi: (H, g) \rightarrow (K, f).$$

Similmente esiste  $0 \leq \rho \leq b + \delta$  ed una  $\rho$ -contiguità

$$\eta: (H, g) \rightarrow (L, h), \quad \mu: (L, h) \rightarrow (H, g).$$

Per concludere basta dimostrare che le composizioni

$$\eta\phi: (K, f) \rightarrow (L, h), \quad \psi\mu: (L, h) \rightarrow (K, f)$$

formano una  $(\epsilon + \rho)$ -contiguità. Per simmetria, basta mostrare che per ogni  $t \in \mathbb{R}$  la composizione

$$K(t) \xrightarrow{\phi} H(t+\epsilon) \xrightarrow{\eta} L(t+\epsilon+\rho) \xrightarrow{\mu} H(t+\epsilon+2\rho) \xrightarrow{\psi} K(t+2\epsilon+2\rho)$$

è contigua all'inclusione  $K(t) \rightarrow K(t+2\epsilon+2\rho)$ . Ma questo segue dal fatto che la relazione di contiguità commuta con le composizioni e che si ha un diagramma commutativo a meno di contiguità

$$\begin{array}{ccccc} K(t) & \longrightarrow & K(t+2\epsilon) & \longrightarrow & K(t+2\epsilon+2\rho) \\ & \searrow \phi & & \searrow \phi & \nearrow \psi \\ & & H(t+\epsilon) & \longrightarrow & H(t+\epsilon+2\rho) \\ & & & \searrow \eta & \nearrow \mu \\ & & & & L(t+\epsilon+\rho) \end{array}$$

con le frecce orizzontali i morfismi di inclusione. □

Siccome gli isomorfismi di complessi filtrati sono 0-contiguità, complessi filtrati isomorfi hanno pseudo-distanza nulla tra loro e quindi  $d_c$  definisce una struttura di spazio pseudo-metrico in qualsiasi famiglia di classi di isomorfismo di complessi filtrati.

TEOREMA 5.3.10. *Siano  $A, B$  sottoinsiemi di uno spazio metrico  $(X, d)$  e dotiamo i complessi simpliciali completi  $\Delta^A, \Delta^B$  delle filtrazioni di Vietoris-Rips. Allora*

$$d_c(\Delta^A, \Delta^B) \leq d_H(A, B).$$

DIMOSTRAZIONE. Supponiamo  $d_H(A, B) < +\infty$  e proviamo che per ogni numero reale  $r > d_H(A, B)$  vale  $d_c(\Delta^A, \Delta^B) \leq r$ .

Abbiamo visto che esistono due applicazioni  $f: A \rightarrow B$  e  $g: B \rightarrow A$  tali che  $d(a, f(a)) < r$  e  $d(b, g(b)) < r$  per ogni  $a \in A$  ed ogni  $b \in B$ .

Il morfismo di complessi simpliciali  $f: \Delta^A \rightarrow \Delta^B$  è un  $r$ -morfismo, ossia  $f(\Delta^A(t)) \subset \Delta^B(t+r)$  per ogni  $t \in \mathbb{R}$ . Infatti se  $\{x_0, \dots, x_n\} \in \Delta^A(t)$ , per come è definita la filtrazione si ha  $d(x_i, x_j) \leq 2t$  per ogni  $i, j$  e quindi

$$d(f(x_i), f(x_j)) \leq d(f(x_i), x_i) + d(x_i, x_j) + d(x_j, f(x_j)) < t + 2r.$$

Similmente  $g(\Delta^B(t)) \subset \Delta^A(t+r)$  per ogni  $t \in \mathbb{R}$  e resta da provare che le composizioni  $gf$  e  $fg$  sono contigue alle inclusioni.

Mostriamo che  $gf$  è direttamente contigua all'inclusione  $A(t) \subset A(t+2r)$  per ogni  $t$  ossia che per ogni  $\{x_0, \dots, x_n\} \in \Delta^A(t)$  vale  $\{x_0, \dots, x_n, gf(x_1), \dots, gf(x_n)\} \in \Delta^A(t+2r)$ . Per ogni  $x \in A$  vale  $d(x, gf(x)) \leq d(x, f(x)) + d(f(x), gf(x)) < 2r$  e quindi, per ogni  $i, j = 1, \dots, n$  si ha:

- (1)  $d(x_i, x_j) \leq 2t \leq 2(t+2r)$ ;
- (2)  $d(x_i, gf(x_j)) \leq d(x_i, x_j) + d(x_j, gf(x_j)) \leq 2t + 2r \leq 2(t+2r)$ ;
- (3)  $d(gf(x_i), gf(x_j)) \leq d(x_i, x_j) + d(x_i, gf(x_i)) + d(x_j, gf(x_j)) \leq 2t + 4r$ .

Per simmetria anche la composizione  $fg$  è direttamente contigua all'inclusione  $B(t) \subset B(t+2r)$  per ogni  $t$ .

Dunque la coppia  $(f, g)$  è una  $r$ -contiguità e quindi  $d_c(\Delta^A, \Delta^B) \leq r$ .  $\square$

#### 5.4. Distanza di interfoglia

Introduciamo adesso uno degli oggetti principali di queste note.

DEFINIZIONE 5.4.1. Sia  $T \subset \mathbb{R}$  un sottoinsieme. Un **modulo di persistenza** su  $T$  è il dato di:

- (1) per ogni  $t \in T$  un gruppo abeliano  $A(t)$ ;
- (2) per ogni  $s, t \in T$  con  $s \leq t$  un omomorfismo di gruppi  $a_s^t: A(s) \rightarrow A(t)$ .

Gli omomorfismi  $a_s^t$  devono soddisfare le seguenti condizioni:

- $a_s^s = \text{Id}_{A(s)}$  per ogni  $s$ ;
- $a_t^r \circ a_s^t = a_s^r$  per ogni  $s \leq t \leq r$ .

Per convenzione, quando l'insieme  $T$  non viene nominato, si intende un modulo di persistenza su  $\mathbb{R}$ .

Dal punto di vista notazionale, indicheremo i moduli di persistenza su  $T$  con delle terne  $(A, a, T)$ , dove  $A$  denota la totalità dei gruppi  $A(s)$  ed  $a$  la totalità degli omomorfismi  $a_s^t$ . Quando  $T = \mathbb{R}$  si scrive semplicemente  $(A, a)$  al posto di  $(A, a, \mathbb{R})$ .

In alcuni casi, per ulteriore semplicità notazionale, scriveremo solamente  $(A, T)$  al posto di  $(A, a, T)$ , ed  $A$  al posto di  $(A, a, \mathbb{R})$ .

OSSERVAZIONE 5.4.2. In linea teorica possiamo definire i moduli di persistenza su ogni insieme parzialmente ordinato, e più in generale su ogni categoria piccola. Tali trattazioni vanno al di là dei nostri obiettivi e vengono ignorate.

**ESEMPIO 5.4.3.** Sia  $K$  un complesso simpliciale filtrato, con sottocomplessi di livello  $K(t)$ . Per ogni  $n \geq 0$  possiamo definire il modulo di persistenza  $(H_n, h)$  ponendo  $H_n(t) = H_n(K(t))$  e  $h_s^t: H_n(s) \rightarrow H_n(t)$  il morfismo in omologia indotto dall'inclusione di complessi simpliciali  $K(s) \subset K(t)$ .

Se  $f: K \rightarrow \mathbb{R}$  è la funzione filtrante associata e l'insieme dei vertici di  $K$  è dotato di un ordinamento totale tale che l'applicazione  $f: K^{(0)} \rightarrow \mathbb{R}$  è monotona, allora il morfismo  $h_{t,s}$  è indotto dal morfismo tra complessi di catene ordinate  $C_*(K(s), <) \rightarrow C_*(K(t), <)$ .

**ESEMPIO 5.4.4.** Siano  $X$  uno spazio topologico e  $f: X \rightarrow \mathbb{R}$  continua; per ogni  $t \in \mathbb{R}$  denotiamo  $X(t) = \{x \in X \mid f(x) \leq t\}$ . Per ogni  $n \geq 0$  possiamo definire il modulo di persistenza  $(H_n, h)$  ponendo  $H_n(t) = H_n(K(t))$  e  $h_s^t: H_n(s) \rightarrow H_n(t)$  il morfismo in omologia singolare indotto dall'inclusione  $X(s) \subset X(t)$ .

La nozione di modulo di persistenza è molto generale e, al fine di estrarre invarianti algebrici significativi, è necessario aggiungere condizioni di regolarità e finitezza. Le più comuni sono elencate nelle seguenti quattro definizioni.

**DEFINIZIONE 5.4.5.** Un modulo di persistenza  $(A, a, T)$  si dice **q-tame** se per ogni  $s, t \in T$ , con  $s > t$ , l'immagine di  $a_t^s: A(t) \rightarrow A(s)$  è un sottogruppo finitamente generato.

**DEFINIZIONE 5.4.6.** Un modulo di persistenza  $(A, a, T)$  si dice **semicontinuo** se per ogni  $t \in T$  esiste  $\varepsilon > 0$  tale che  $a_t^s$  è un isomorfismo per ogni  $s \in T \cap [t, t + \varepsilon[$ .

**DEFINIZIONE 5.4.7.** Un modulo di persistenza  $(A, a, T)$  si dice **di tipo finito** se  $T$  è un insieme finito ed il gruppo  $A(t)$  è finitamente generato per ogni  $t \in T$ .

**DEFINIZIONE 5.4.8.** Sia  $\Delta \geq 0$  un numero reale non negativo; un modulo di persistenza  $(A, a, T)$  si dice un  **$\Delta$ -modulo** se per ogni  $t, s \in T$  con  $s - t \geq \Delta$  si ha  $a_t^s = 0$ .

Esiste una nozione naturale di morfismo che rende i moduli di persistenza su di un  $T$  fissato una categoria.

**DEFINIZIONE 5.4.9.** Un **morfismo**  $f: (P, p, T) \rightarrow (Q, q, T)$  di moduli di persistenza su  $T$  è il dato, per ogni  $t \in T$  di un omomorfismo di gruppi  $f_t: P(t) \rightarrow Q(t)$  tale che per ogni  $s \leq t$  si ha un diagramma commutativo

$$\begin{array}{ccc} P(s) & \xrightarrow{p_s^t} & P(t) \\ \downarrow f_s & & \downarrow f_t \\ Q(s) & \xrightarrow{q_s^t} & Q(t) \end{array}$$

Un **isomorfismo** è un morfismo  $f$  tale che ogni  $f_t$  è un isomorfismo di gruppi abeliani.

Dato un qualunque morfismo  $f: (P, p, T) \rightarrow (Q, q, T)$  possiamo definire nella maniera ovvia il suo nucleo ed il suo conucleo, che risultano ancora essere moduli di persistenza su  $T$ :

$$\ker(f)(t) = \ker(f_t: P(t) \rightarrow Q(t)), \quad \text{coker}(f)(t) = \text{coker}(f_t: P(t) \rightarrow Q(t)).$$

**DEFINIZIONE 5.4.10.** Per un dato numero reale  $\Delta \geq 0$ , diremo che  $f$  ha  $\Delta$ -nucleo (resp.:  $\Delta$ -conucleo) se  $\ker(f)$  (resp.:  $\text{coker}(f)$ ) è un  $\Delta$ -modulo.

Sempre in maniera ovvia si definisce la somma diretta di due moduli di persistenza sulla stessa base  $T$ :

$$(P \oplus Q)(t) = P(t) \oplus Q(t), \quad t \in T.$$

Dato  $(P, p)$  un modulo di persistenza su  $T$  e  $\delta \in \mathbb{R}$  possiamo definire il traslato di  $P$  tramite  $\delta$  come il modulo di persistenza  $(P[\delta], p[\delta])$  su

$$T - \delta = \{t - \delta \mid t \in T\},$$

ponendo

$$P[\delta](t) = P(t + \delta), \quad p[\delta]_t^s = p_{t+\delta}^{s+\delta}.$$

È chiaro che  $P[\delta + \kappa] = (P[\delta])[\kappa]$  e che la traslazione possiede le principali proprietà functoriali: in particolare, per ogni morfismo  $f: P \rightarrow Q$  è definito il morfismo

$$f[\delta]: P[\delta] \rightarrow Q[\delta], \quad f[\delta]_t = f_{t+\delta},$$

che si comporta bene rispetto alla composizione.

Se  $T - \delta = T$ , allora è definito un morfismo canonico “di sospensione”

$$s^\delta: P \rightarrow P[\delta], \quad s_t^\delta = p_t^{t+\delta}: P(t) \rightarrow P[\delta](t).$$

Da questo momento, fino al termine della sezione consideriamo solamente moduli di persistenza su  $T = \mathbb{R}$ .

**DEFINIZIONE 5.4.11.** Dato un numero reale  $\varepsilon$  e due moduli di persistenza  $(P, p)$  e  $(Q, q)$  su  $\mathbb{R}$ , un morfismo  $P \rightarrow Q[\varepsilon]$  viene detto  $\varepsilon$ -**morfismo** da  $P$  a  $Q$

In altri termini, un  $\varepsilon$ -morfismo da  $P$  a  $Q$  è una famiglia di omomorfismi di gruppi

$$f_t: P(t) \rightarrow Q(t + \varepsilon), \quad t \in \mathbb{R},$$

tali che per ogni  $s \leq t$  si ha un diagramma commutativo

$$\begin{array}{ccc} P(s) & \xrightarrow{p_s^t} & P(t) \\ \downarrow f_s & & \downarrow f_t \\ Q(s + \varepsilon) & \xrightarrow{q_{s+\varepsilon}^{t+\varepsilon}} & Q(t + \varepsilon) \end{array}$$

Ad esempio, per ogni  $\varepsilon \geq 0$  il morfismo di sospensione  $s^\varepsilon: P \rightarrow P[\varepsilon]$  è un  $\varepsilon$ -morfismo. Più in generale, per ogni  $\varepsilon$ -morfismo  $f: P \rightarrow Q[\varepsilon]$  ed ogni  $\delta \geq 0$  si ha che

$$s^\delta f = f[\delta]s^\delta: P \rightarrow Q[\varepsilon + \delta]$$

è un  $(\varepsilon + \delta)$ -morfismo.

È chiaro dalle definizioni che gli 0-morfismi sono esattamente i morfismi definiti precedentemente, mentre l’analogo dell’isomorfismo per gli  $\varepsilon$ -morfismi viene detta  $\varepsilon$ -interfoggia.

**DEFINIZIONE 5.4.12.** Dato un numero reale  $\varepsilon \geq 0$ , chiameremo  $\varepsilon$ -**interfoggia** tra due moduli di persistenza  $(P, p)$  e  $(Q, q)$  su  $\mathbb{R}$  il dato di due  $\varepsilon$ -morfismi

$$f: P \rightarrow Q[\varepsilon], \quad g: Q \rightarrow P[\varepsilon],$$

tali che le composizioni siano i morfismi di sospensione:

$$g[\varepsilon]f = s^{2\varepsilon}, \quad f[\varepsilon]g = s^{2\varepsilon}.$$

Si noti che la nozione di 0-interfoggia è del tutto equivalente a quella di isomorfismo. Si noti anche che se esiste una  $\varepsilon$ -interfoggia  $f: P \rightarrow Q[\varepsilon]$ ,  $g: Q \rightarrow P[\varepsilon]$ , allora esiste anche una  $\rho$ -interfoggia per ogni  $\rho \geq \varepsilon$ , ad esempio:

$$s^{\rho-\varepsilon}f: P \rightarrow Q[\rho], \quad s^{\rho-\varepsilon}g: Q \rightarrow P[\rho].$$

**LEMMA 5.4.13.** *Sia*

$$f: P \rightarrow Q[\varepsilon], \quad g: Q \rightarrow P[\varepsilon],$$

*una  $\varepsilon$ -interfoggia. Allora i due morfismi  $f, g$  hanno entrambi  $2\varepsilon$ -nucleo e  $2\varepsilon$ -conucleo.*

**DIMOSTRAZIONE.** Per simmetria basta considerare il morfismo  $f$ . Siano  $t \in \mathbb{R}$  e  $x \in P(t)$  tale che  $f_t(x) = 0$ . Allora  $p_t^{t+2\varepsilon}(x) = g_{t+\varepsilon}f_t(x) = 0$ ; quindi  $p_t^{t+2\varepsilon}$  si annulla sul nucleo. Similmente se  $x \in \text{coker}(f)_t$  è rappresentato da  $y \in Q(t + \varepsilon)$ , allora  $q_{t+\varepsilon}^{t+3\varepsilon}$  è rappresentato da  $f_{t+2\varepsilon}g_{t+\varepsilon}(y)$  che quindi appartiene all’immagine di  $f$ .  $\square$

**DEFINIZIONE 5.4.14.** Dati due moduli di persistenza  $P, Q$  su  $\mathbb{R}$ , definiamo la **distanza interfoggia**

$$d_i(P, Q) = \inf \{ \varepsilon \geq 0 \mid \text{esiste una } \varepsilon\text{-interfoggia tra } P \text{ e } Q \}.$$

Si ha  $d_i(P, Q) = +\infty$  se e solo se non esistono interfoglie tra  $P$  e  $Q$ .

ESEMPIO 5.4.15. Dato che ogni isomorfismo è una 0-interfoggia, se  $P, Q$  sono due moduli di persistenza isomorfi, allora  $d_i(P, Q) = 0$ . Il viceversa è generalmente falso, ad esempio i due moduli

$$(P, p) = \begin{cases} P(t) = 0 & \text{se } t \leq 0 \\ P(t) = \mathbb{Z} & \text{se } t > 0 \\ p_s^t = \text{Id} & \text{per } s > 0 \end{cases}, \quad (Q, q) = \begin{cases} Q(t) = 0 & \text{se } t < 0 \\ Q(t) = \mathbb{Z} & \text{se } t \geq 0 \\ q_s^t = \text{Id} & \text{per } s \geq 0 \end{cases}$$

non sono isomorfi ma sono  $\varepsilon$ -interfogliati per ogni  $\varepsilon > 0$

PROPOSIZIONE 5.4.16. *La distanza di interfoggia definisce una struttura di spazio pseudo-metrico su una qualunque insieme di moduli di persistenza su  $\mathbb{R}$ .*

DIMOSTRAZIONE. L'unica verifica non completamente banale è quella della disuguaglianza triangolare. Siano  $P, Q, R$  moduli di persistenza e si assuma  $d_i(P, Q) + d_i(Q, R) < +\infty$ ; vogliamo dimostrare che per ogni  $\varepsilon > d_i(P, Q)$  ed ogni  $\delta > d_i(Q, R)$  esiste una  $\varepsilon + \delta$ -interfoggia tra  $P$  e  $R$ .

Scegliamo una  $\varepsilon$ -interfoggia

$$f_t: P(t) \rightarrow Q(t + \varepsilon), \quad g_t: Q(t) \rightarrow P(t + \varepsilon), \quad t \in \mathbb{R},$$

ed una  $\delta$ -interfoggia

$$h_t: Q(t) \rightarrow R(t + \delta), \quad k_t: R(t) \rightarrow Q(t + \delta), \quad t \in \mathbb{R}.$$

Si vede immediatamente che

$$h_{t+\varepsilon}f_t: P(t) \rightarrow R(t + \varepsilon + \delta), \quad g_{t+\delta}k_t: R(t) \rightarrow P(t + \varepsilon + \delta)$$

è la  $\varepsilon + \delta$ -interfoggia cercata.  $\square$

Mettiamoci adesso nella situazione dell'Esempio 5.4.3 e mostriamo che la distanza di interfoggia non supera la distanza di contiguità.

TEOREMA 5.4.17. *Siano  $K$  e  $L$  due complessi filtrati,  $n \geq 0$ , e consideriamo i due moduli di persistenza  $H_n(K(t)), H_n(L(t))$ . Allora*

$$d_i(H_n(K(t)), H_n(L(t))) \leq d_c(K, L).$$

DIMOSTRAZIONE. Non è restrittivo supporre  $d_c(K, L) < +\infty$  e basta dimostrare che se esiste una  $\varepsilon$ -contiguità  $f_t: K(t) \rightarrow L(t + \varepsilon)$ ,  $g_t: L(t) \rightarrow K(t + \varepsilon)$  allora esiste anche una  $\varepsilon$ -interfoggia tra  $H_n(K(t))$  e  $H_n(L(t))$ . Per definizione,  $g_{t+\varepsilon}f_t$  è contigua all'inclusione  $K(t) \subset K(t + 2\varepsilon)$ . Dato che morfismi contigui inducono lo stesso morfismo in omologia si ha che  $g_{t+\varepsilon}f_t = h_t^{t+2\varepsilon}: H_n(K(t)) \rightarrow H_n(K(t + 2\varepsilon))$ . Per simmetria vale anche  $f_{t+\varepsilon}g_t = h_t^{t+2\varepsilon}: H_n(L(t)) \rightarrow H_n(L(t + 2\varepsilon))$  e quindi i due  $\varepsilon$ -morfismi  $f_t, g_t$  definiscono una  $\varepsilon$ -interfoggia.  $\square$

OSSERVAZIONE 5.4.18. Dati due spazi topologici  $X, Y$  dotati di funzioni continue  $f: X \rightarrow \mathbb{R}$  e  $g: Y \rightarrow \mathbb{R}$ , il lettore volenteroso può provare a definire la "distanza di omotopia" tra  $(X, f)$  e  $(Y, g)$  e dimostrare l'analogo del Teorema 5.4.17.



## Omologia Persistente

Per **analisi topologica dei dati** (TDA) si intende un insieme di tecniche, prevalentemente di natura topologica e statistica, che consentono di analizzare grandi quantità di dati in maniera estremamente stabile rispetto alle componenti di rumore, ossia rispetto a piccole e generiche perturbazioni dei dati raccolti.

Uno dei metodi topologici più usati in TDA è detto **omologia persistente**. Questo strumento permette di descrivere caratteristiche dei dati sotto forma di “buchi”, il cui numero e qualità dipende da uno o più parametri reali: l’abilità di identificare i “buchi” più persistenti al variare dei parametri fornisce un metodo piuttosto potente nell’analisi dei dati.

Attualmente il software open-source di riferimento in ambito scientifico per la TDA è *Mapper* [15].

### 6.1. L’incredibile ubiquità della topologia persistente

*Riportiamo in questa breve sezione un estratto dall’articolo di Massimo Ferri (Università di Bologna) pubblicato su Maddmaths il 12 agosto 2015 e recuperabile per intero al sito [maddmaths.simai.eu/divulgazione/focus/lincredibile-ubiquita-della-topologia-persistente/](http://maddmaths.simai.eu/divulgazione/focus/lincredibile-ubiquita-della-topologia-persistente/).*

C’è una branca della matematica chiamata “Topologia persistente” che ha applicazioni spesso sorprendenti all’analisi della forma e ai problemi di classificazione e recupero dei dati. Cerchiamo di capire meglio di cosa si tratta.

La geometria offre ottimi strumenti alla visione artificiale e alla pattern recognition. I problemi di classificazione, riconoscimento, ricerca di difetti, recupero in database estesi si risolvono talvolta trovando una trasformazione (euclidea, affine o proiettiva) che sovrapponga un’immagine a un’altra; qui l’algebra matriciale risulta vincente. Soprattutto, però, questi problemi si affrontano associando ad ogni immagine una stringa di misure geometriche (descrittori di forma) compiute su di essa ed eseguendo classificazione, riconoscimento, ecc. sulle stringhe invece che sulle immagini. Questa prassi funziona benissimo su pezzi meccanici, veicoli, oggetti rigidi: per esempio Google riconosce un monumento anche se fotografato da un’angolazione insolita. Però le cose cambiano con immagini di origine naturale; la rigidità della geometria diventa un ostacolo: riconoscere la somiglianza fra un uomo seduto e uno in piedi è problematico.

È qui che la topologia, molto più “libera” della geometria, sembra essere la carta giusta da giocare. Invece che dalla sovrapposibilità mediante trasformazioni geometriche, l’equivalenza fra due spazi topologici  $X, Y$  è data dall’eventuale esistenza di un omeomorfismo  $\varphi: X \rightarrow Y$ , cioè una funzione continua con inversa continua. L’uomo seduto e l’uomo in piedi sono omeomorfi, cioè esiste fra loro un omeomorfismo, ma non una trasformazione geometrica. Allora basta sostituire la geometria con la topologia, l’algebra matriciale con l’omeomorfismo? Purtroppo ci sono due problemi.

In genere è difficile capire se due spazi sono omeomorfi o no. Allora interviene la topologia algebrica, che associa a uno spazio degli enti (invarianti) che risultano uguali per spazi omeomorfi. Perciò se due spazi  $X, Y$  hanno invarianti diversi sono sicuramente non omeomorfi (purtroppo il viceversa non vale).

Invarianti di questo tipo sono i numeri di Betti:  $b_0(X)$  è il numero di componenti connesse (o 0-cicli), in pratica il numero di pezzi separati da cui è composto  $X$ ;  $b_1(X)$  conta i buchi fatti “a circonferenza” di  $X$  (o 1-cicli, come quello di una ciambella);  $b_2(X)$  conta i vuoti bidimensionali di  $X$  (come quelli di un pallone o di una camera d’aria; 2-cicli) e così via. Per

capire davvero il significato di questi concetti occorrono definizioni formali; non sono male l'articolo di Wikipedia *Betti number* e il più generale *Omologia*.

C'è un secondo problema: la geometria è troppo rigida, ma la topologia è troppo libera. La battuta “per un topologo una tazza con manico e una ciambella sono la stessa cosa” è fondata: i due oggetti sono omeomorfi; i numeri di Betti naturalmente coincidono:  $b_0 = 1$ ,  $b_1 = 1$ ,  $b_2 = 0$  eccetera per entrambi.

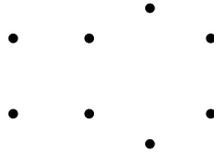
L'idea base della topologia persistente è di associare il concetto di forma non solo a uno spazio topologico  $X$ , ma ad una coppia  $(X, f)$  dove  $f$  è una funzione continua (che chiameremo *funzione filtrante*) definita su  $X$ , a valori solitamente nei numeri reali. A questo punto la topologia algebrica (in particolare il suo settore omologia, di cui fanno parte i numeri di Betti) viene applicata ad ogni insieme di sottolivello  $X(t)$ , costituito dai punti  $x \in X$  per cui  $f(x) \leq t$ . Per esempio possiamo appoggiare una tazza  $X$  e una ciambella  $Y$  di eguale altezza sul tavolo, e usare come funzione  $f$  la quota, ossia la distanza dal pavimento. Entrambi gli oggetti hanno quota minima  $a$  e massima  $c$ . Se  $a - \epsilon$  è un numero appena sotto ad  $a$ , allora  $X(a - \epsilon) = Y(a - \epsilon) = \emptyset$ ; invece  $X(c) = X$ ,  $Y(c) = Y$ . Se applichiamo l'omologia agli insiemi di sottolivello intermedi, ecco che possiamo distinguere tazza e ciambella! In realtà la teoria è più complicata (e più informativa) e si avvale di suoi specifici descrittori di forma: numeri di Betti persistenti, diagrammi di persistenza, barcode.

## 6.2. Allarga i punti e sfoca le immagini

**persistente** agg. [part. pres. di *persistere*]. - Che permane costantemente nel tempo, che si prolunga oltre il previsto o comunque per un lungo periodo; continuo, ostinato: ...

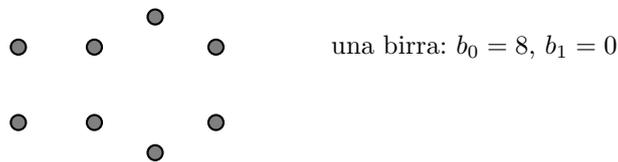
(dal Dizionario Treccani).

Consideriamo la seguente costellazione di 8 stelle nel cielo



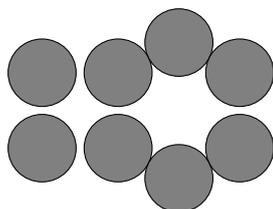
e chiediamoci quale figura rappresenta.

Una persona sobria vede solamente 8 punti separati, quindi una figura con 8 componenti connesse contraibili, ossia  $b_0 = 8$  e  $b_1 = 0$ . Dopo una birretta (ed una salsiccia) inizia a vedere le immagini un po' sfocate:



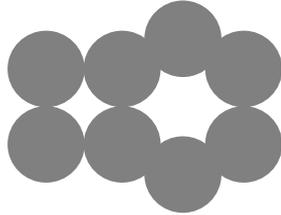
una birra:  $b_0 = 8$ ,  $b_1 = 0$

ma i numeri di Betti iniziali persistono. Continuando a bere birre e mangiare salsicce, all'ottava birra le immagini diventano talmente sfocate da cambiare la topologia



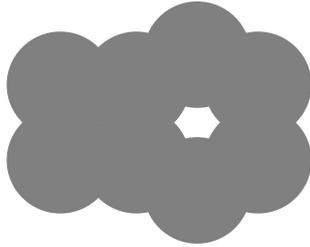
8 birre:  $b_0 = 4$ ,  $b_1 = 0$

Alla nona birra la topologia cambia ancora:



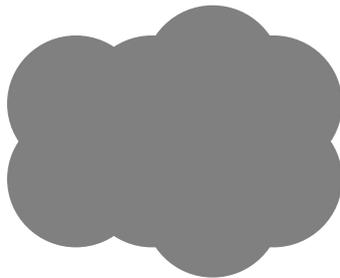
9 birre:  $b_0 = 1, b_1 = 2$

Alla tredicesima birra quello che si vede è:



13 birre:  $b_0 = 1, b_1 = 1$

mentre alla diciassettesima birra, quello che si vede dalla lettiga dell'ambulanza è:



17 birre:  $b_0 = 1, b_1 = 0$

Dunque dovendo decidere quanti “buchi” ci sono nella figura, osserviamo che il buco a sinistra ha *persistenza* 4, ossia è durato 4 birre (dalla 9 alla 12), mentre quello a destra ha *persistenza* 8 (dalla nona alla 16a birra). Quindi la figura ha avuti per 4 birre 1 buco e per altre 4 birre 2 buchi. Nella misura in cui il numero di birre viene considerato una giusta misura di persistenza, possiamo valutare i due eventi con uguale probabilità.

### 6.3. Complessi filtrati

In queste note ci occuperemo solamente della parte “algebro-geometrica” dell’omologia persistente. Con riferimento alla Figura 1, studieremo nelle prossime sezioni con sufficiente dettaglio i passaggi (b) e (c), mentre studieremo in questa sezione il passaggio (a) in alcuni casi molto particolari. Per quanto riguarda l’interpretazione, che richiede strumenti di natura analitica e statistica, rimandiamo alla letteratura sull’argomento: un buon punto di partenza è dato dagli articoli [2, 6, 7, 23].

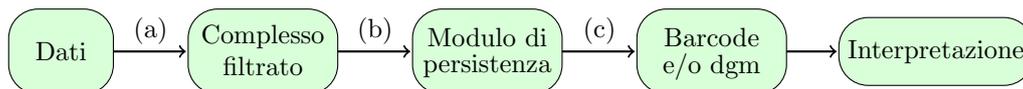


FIGURA 1. La catena di montaggio dell’omologia persistente.

Riscriviamo ed ampliamo la nozione di complesso simpliciale filtrato.

**DEFINIZIONE 6.3.1.** Sia  $K$  un complesso simpliciale astratto. Una **funzione filtrante** su  $K$  è un’applicazione  $f: K \rightarrow \mathbb{R}$  tale che se  $s \in K$  e  $r \subset s$  allora  $f(r) \leq f(s)$ .

Equivalentemente, un'applicazione  $f: K \rightarrow \mathbb{R}$  è una funzione filtrante se per ogni  $t \in \mathbb{R}$  il sottoinsieme **di livello**

$$K(t) = \{s \in K \mid f(s) \leq t\} = f^{-1}(]-\infty, t])$$

è un sottocomplesso simpliciale. Abbiamo già osservato che i sottocomplessi di livello soddisfano le condizioni

$$(5.2) \quad \bigcap_t K(t) = \emptyset, \quad \bigcup_t K(t) = K, \quad K(s) = \bigcap_{t>s} K(t) \text{ per ogni } s \in \mathbb{R},$$

e che ogni famiglia  $K(t)$ ,  $t \in \mathbb{R}$ , di sottocomplessi simpliciali di  $K$  che soddisfa tali condizioni è la famiglia dei sottoinsiemi di livello della funzione filtrante  $f(\sigma) = \inf\{t \in \mathbb{R} \mid \sigma \in K(t)\}$ .

Per semplicità notazionale, quando non ci saranno rischi di ambiguità, chiameremo semplicemente **complesso filtrato** una coppia  $(K, f)$  con  $K$  complesso simpliciale astratto e  $f: K \rightarrow \mathbb{R}$  funzione filtrante.

Ecco altri esempi di complessi filtrati, in aggiunta a 5.3.2 e 5.3.3.

**ESEMPIO 6.3.2.** Dato un complesso simpliciale astratto  $(K, I)$  ed una applicazione  $d: I \times I \rightarrow \mathbb{R}$  tale che  $d(x, y) = d(y, x) \geq 0$  per ogni  $x, y \in I$ , possiamo definire una funzione filtrante

$$f: K \rightarrow [0, +\infty[, \quad f(\{x_0, \dots, x_p\}) = \max_{i,j} d(x_i, x_j).$$

**ESEMPIO 6.3.3.** Siano  $X$  un insieme finito e  $\mathcal{U} = \{U_i\}$ ,  $i \in I$ , una famiglia di sottoinsiemi di  $X$ . Sul complesso simpliciale dato dal nervo di  $\mathcal{U}$  (Esempio 1.2.14):

$$N(\mathcal{U}) = \{\{i_0, \dots, i_p\} \in \Delta^I \mid U_{i_0} \cap \dots \cap U_{i_p} \neq \emptyset\}$$

possiamo considerare la funzione filtrante

$$f: N(\mathcal{U}) \rightarrow \mathbb{R}, \quad f(\{i_0, \dots, i_p\}) = \frac{1}{|U_{i_0} \cap \dots \cap U_{i_p}|}.$$

**ESEMPIO 6.3.4.** Sia  $K$  un complesso simpliciale astratto e sia  $K(0) \subset K(1) \subset K(2) \subset \dots$  una catena ascendente di sottocomplessi simpliciali tali che  $\cup_n K(n) = K$ . Allora la funzione

$$f: K \rightarrow [0, +\infty[, \quad f(x) = \min\{n \mid x \in K(n)\}$$

è una funzione filtrante tale che  $K(n) = \{x \in K \mid f(x) \leq n\}$ .

Dato un complesso filtrato  $(K, f)$ , l'immagine  $f(K) \subset \mathbb{R}$  viene detto **luogo dei valori critici** di  $f$ . Segue dalla definizione dei sottocomplessi di livello che per ogni valore critico  $t$  si ha  $K(s) \neq K(t)$  per ogni  $s < t$ .

Diremo che un complesso filtrato  $(K, f)$  è di **tipo finito** se  $K$  è un complesso simpliciale astratto finito. In particolare ogni complesso filtrato di tipo finito possiede un numero finito di valori critici.

Diremo che un complesso filtrato  $(K, f)$  è **localmente di tipo finito** se  $K(t)$  è un sottocomplesso finito per ogni  $t \in \mathbb{R}$ . In tal caso luogo dei valori critici è chiuso, discreto e inferiormente limitato: infatti per ogni  $t$  il luogo dei valori critici della restrizione di  $f: K(t) \rightarrow \mathbb{R}$  è finito e dunque per ogni  $t \in \mathbb{R}$  l'intersezione  $f(K) \cap ]-\infty, t]$  è finita.

**LEMMA 6.3.5.** *Sia  $(K, f)$  un complesso filtrato localmente di tipo finito. Allora un numero reale  $t$  è un valore critico se e solo se  $K(s) \neq K(t)$  per ogni  $s < t$ .*

**DIMOSTRAZIONE.** Facile esercizio. □

I prossimi esempi descrivono alcuni casi del passaggio (a) di Figura 1.

**ESEMPIO 6.3.6.** Si consideri un ben definito insieme  $I$  di matematici, ad esempio l'insieme dei docenti afferenti al Dipartimento di Matematica Guido Castelnuovo il 18 settembre 2021. Il complesso simpliciale astratto  $(K, I)$  delle collaborazioni scientifiche di  $I$  è definito dalla regola che un elemento  $\{x_0, \dots, x_p\} \in \Delta^I$  appartiene a  $K$  se e solo se esiste (almeno) una pubblicazione in cui tra gli autori figurano  $x_0, \dots, x_p$ .

La funzione filtrante temporale  $f: K \rightarrow \mathbb{R}$  è definita ponendo  $f(s)$  come l'anno della prima pubblicazione avente  $s$  come sottoinsieme di autori.

ESEMPIO 6.3.7 (Cf. [20]). Si consideri l'insieme  $I$  dei personaggi di un film e per ogni coppia  $(x, y) \in I \times I$  sia  $d(x, y)$  il numero di scene (o se preferite il numero di fotogrammi) in cui  $x, y$  compaiono simultaneamente. Si consideri adesso il complesso di cricche  $(K, I)$ , dove  $\{x_0, \dots, x_p\} \in K$  se e solo se  $d(x_i, x_j) > 0$  per ogni  $i, j$ .

Una possibile funzione filtrante  $f: K \rightarrow \mathbb{R}$  sensata in tale situazione è data da

$$f(\{x_0, \dots, x_p\}) = \max_{i,j} \frac{1}{d(x_i, x_j)}.$$

Costruzioni analoghe hanno senso, o perlomeno sono state studiate, quando  $I$  è l'insieme dei cellulari agganciati ad un insieme di antenne in corrispondenza di un attentato terroristico e  $d(x, y)$  il numero di telefonate/messaggini intercorsi tra  $x$  e  $y$ .

Nel seguito, useremo i termini **nuvola di punti** e **point cloud** per indicare un sottoinsieme  $I \subset \mathbb{R}^n$  con un numero finito ma molto grande di elementi, ossia  $n \ll |I| < \infty$ . Inoltre per ogni  $x \in \mathbb{R}^n$  ed ogni numero reale  $r$  denotiamo

$$U_x(r) = \{y \in \mathbb{R}^n \mid \|x - y\| \leq r\}.$$

Ciascun  $U_x(r)$  è un chiuso limitato che, per ogni  $r > 0$  coincide con la chiusura della sua parte interna (la palla aperta di raggio  $r$ ). Chiameremo  $U_x(r)$  il disco chiuso di centro  $x$  e raggio  $r$ .

ESEMPIO 6.3.8 (Complessi di Čech e Vietoris–Rips). Dato un qualsiasi sottoinsieme  $I \subset \mathbb{R}^n$ , per ogni numero reale positivo  $r \geq 0$  possiamo definire i complessi simpliciali astratti  $C_I(r)$  e  $V_I$  nel modo seguente:

$$C_I(r) = \{\{x_0, \dots, x_p\} \in \Delta^I \mid U_{x_0}(r) \cap \dots \cap U_{x_p}(r) \neq \emptyset\}, \quad (\text{Čech}),$$

$$V_I(r) = \{\{x_0, \dots, x_p\} \in \Delta^I \mid \|x_i - x_j\| \leq 2r \text{ per ogni } i, j\}, \quad (\text{Vietoris–Rips}).$$

È evidente che se  $r \leq t$  allora  $V_I(r) \subseteq V_I(t)$  e  $C_I(r) \subseteq C_I(t)$  (vedi Figura 2). Una semplice applicazione della disuguaglianza triangolare mostra che  $C_I(r) \subseteq V_I(r) \subseteq C_I(2r)$ .

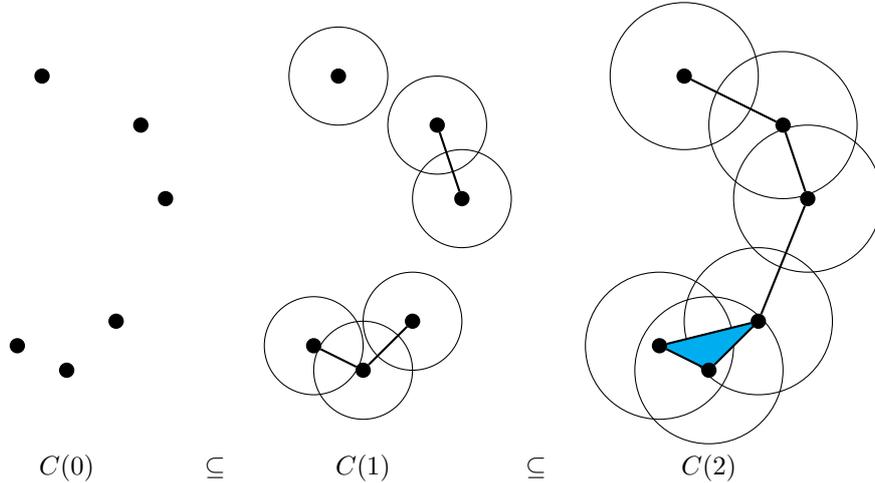


FIGURA 2. Filtrazione di Čech. Credits: la figura è tratta da [17].

È facile descrivere i complessi di Vietoris–Rips e Čech come sottocomplessi di livello per delle opportune funzioni filtranti, che denoteremo rispettivamente  $v, c$ .

Nel caso Vietoris–Rips, sia  $K = \Delta^I$  e si consideri la funzione filtrante

$$v: K \rightarrow [0, +\infty[, \quad v(\{x_0, \dots, x_p\}) = \frac{1}{2} \max_{i,j} \|x_i - x_j\|.$$

È chiaro per definizione che  $K(t) = V_I(t)$  per ogni  $t$ .

Nel caso Čech si prende  $K = \Delta^I$  assieme alla funzione filtrante

$$c: K \rightarrow [0, +\infty[, \quad c(\{x_0, \dots, x_p\}) = \min\{r \in \mathbb{R} \mid U_{x_0}(r) \cap \dots \cap U_{x_p}(r) \neq \emptyset\},$$

ed è chiaro per definizione che  $K(t) = C_I(t)$  per ogni  $t$ . Il fatto che  $c$  sia ben definita richiede un semplice ragionamento topologico: sia  $\{x_0, \dots, x_p\} \in K$  fissato e scegliamo un numero reale  $R > 0$  sufficientemente grande e tale che  $U_{x_0}(R) \cap \dots \cap U_{x_p}(R) \neq \emptyset$ . Adesso consideriamo il sottoinsieme chiuso e limitato (quindi compatto):

$$Z = \{(y, r) \in U_{x_0}(R) \times [0, R] \mid \|y - x_i\| \leq r, \forall i\}.$$

Per le ipotesi su  $R$  si ha

$$(y, r) \in Z \iff r \leq R \text{ e } y \in U_{x_0}(r) \cap \dots \cap U_{x_p}(r).$$

In particolare il compatto  $Z$  è non vuoto ed ha senso definire

$$c(\{x_0, \dots, x_p\}) = \min_{(y, r) \in Z} r.$$

**ESEMPIO 6.3.9 (Complessi Alpha).** Dato un qualsiasi sottoinsieme non vuoto  $I \subset \mathbb{R}^n$ , per ogni  $u \in I$  ed ogni numero reale positivo  $r > 0$  denotiamo  $R_u(r) = U_u(r) \cap V_u$ , dove  $U_u(r)$  è il disco di centro  $u$  e raggio  $r$ , e  $V_u$  è la regione di Voronoi di  $u$ , definita nell'Esempio 1.2.14:

$$V_u := \{x \in \mathbb{R}^n \mid \|x - u\| \leq \|x - v\| \quad \forall v \in I\}.$$

Il complesso simpliciale Alpha( $r$ ) è definito come il nervo della famiglia  $\{R_u(r)\}$ ,  $u \in I$  (vedi Figura 3).

Equivalentemente un simpleso  $\{s_0, \dots, s_p\} \in \Delta^I$  appartiene al complesso Alpha( $r$ ) se e solo se esiste  $x \in \mathbb{R}^n$  tale che:

$$\|x - s_0\| = \|x - s_1\| = \dots = \|x - s_p\| \leq \min(r, \|x - t\|) \text{ per ogni } t \in I.$$

Possiamo riscrivere le due condizioni precedenti dicendo che un simpleso  $\{s_0, \dots, s_p\} \in \Delta^I$  appartiene al complesso Alpha( $r$ ) se e solo se esiste in  $\mathbb{R}^n$  un disco chiuso di raggio  $\leq r$  la cui parte interna non interseca  $I$  ma il cui bordo contiene  $s_0, \dots, s_p$ .

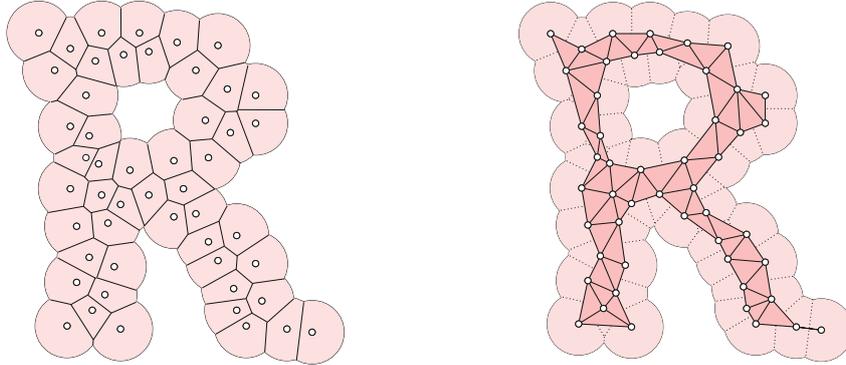


FIGURA 3. A sinistra una nuvola di punti in  $\mathbb{R}^2$  (i pallini  $\circ$ ) e le intersezioni  $R_u(r)$  delle regioni di Voronoi  $V_u$  con le palle  $B(u, r)$  (in rosa chiaro). A destra il complesso Alpha( $r$ ) (in rosa scuro). Credits: la figura è tratta da [5]

Per scrivere i complessi Alpha come sottocomplessi di livello, basta prendere la restrizione al sottocomplesso di Delaunay  $D_I \subset \Delta^I$  della funzione filtrante che definisce la filtrazione di Čech.

Riassumendo gli esempi precedenti, ad ogni sottoinsieme finito e non vuoto  $I \subset \mathbb{R}^n$  abbiamo associato tre diversi complessi filtrati:  $(\Delta^I, v)$ ,  $(\Delta^I, c)$  e  $(D_I, \alpha)$ , nell'ordine dal più semplice (ma meno informativo) al più complesso (ma anche con più informazioni).

ESEMPIO 6.3.10 (Grafì pesati). Un altro caso molto studiato, e formalmente analogo all'Esempio 6.3.7, riguarda i grafì pesati. Per **grafo pesato** si intende un un grafo semplice finito  $G = (V, E)$  equipaggiato di una funzione “peso”  $w: E \rightarrow [0, +\infty[$ , che ad ogni lato associa un numero reale positivo. Indichiamo con  $w(E) = \{w_0 > w_1 > \dots > w_n\}$  la successione insieme dei pesi dei vari lati del grafo, in ordine decrescente. Per ogni  $k = 0, \dots, n$  possiamo considerare il sottografo

$$G_k = (V, E_k) \subset G, \quad E_k = \{e \in E \mid w(e) \geq w_k\}.$$

In altri termini il grafo  $G_k$  ha gli stessi vertici di  $G$  ed ha come lati quelli di peso  $\geq w_k$ . Abbiamo allora una filtrazione di grafì

$$G_0 \subset G_1 \subset \dots \subset G_n = G.$$

Una tale filtrazione di grafì produce una filtrazione dei complessi di cricche associati.

### Esercizi.

ESERCIZIO 28. Sia  $I \subset \mathbb{R}^2$  l'insieme dei vertici di un esagono regolare di lato 1. Determinare il complesso di Vietoris–Rips  $V_I(2)$ .

ESERCIZIO 29. Dato un  $I \subset \mathbb{R}^n$  provare che  $\text{Alpha}(r) \subset D_I \cap C(r)$  e mostrare con un esempio che in generale  $\text{Alpha}(r) \neq D_I \cap C_I(r)$ .

## 6.4. Moduli di persistenza

Secondo alcuni la persistenza è “semplice, naturale ed intuitiva”. Tuttavia per poterla raccontare correttamente e in modo monosemantico è necessario sviluppare un apposito linguaggio.

Riprendiamo dalla Sezione 5.4 la definizione di modulo di persistenza

DEFINIZIONE 6.4.1. Sia  $T \subset \mathbb{R}$  un sottoinsieme. Un **modulo di persistenza** su  $T$  è il dato di:

- (1) per ogni  $t \in T$  un gruppo abeliano  $A(t)$ ;
- (2) per ogni  $s, t \in T$  con  $s \leq t$  un omomorfismo di gruppi  $a_s^t: A(s) \rightarrow A(t)$ .

Gli omomorfismi  $a_s^t$  devono soddisfare le seguenti condizioni:

- $a_s^s = \text{Id}_{A(s)}$  per ogni  $s$ ;
- $a_t^r \circ a_s^t = a_s^r$  per ogni  $s \leq t \leq r$ .

Per convenzione, quando l'insieme  $T$  non viene nominato, si intende un modulo di persistenza su  $\mathbb{R}$

Se  $A = (A(t), a_s^t)$  è un modulo di persistenza su  $\mathbb{R}$ , allora possiamo prendere la sua restrizione  $A|_T$  ad qualunque sottoinsieme  $T \subset \mathbb{R}$  e ottenere un modulo di persistenza su  $T$ . Viceversa, se  $T \subset \mathbb{R}$  è chiuso e  $A = (A(t), a_s^t, T)$  è un modulo di persistenza su  $T$ , allora possiamo vedere  $A$  come la restrizione a  $T$  di un modulo di persistenza  $\tilde{A}$  su  $\mathbb{R}$  definito nel modo seguente:

$$\tilde{A}(s) = \begin{cases} 0 & \text{se } s < t \forall t \in T \\ A(\max(T \cap ]-\infty, s]) & \text{altrimenti.} \end{cases}$$

$$\tilde{a}_s^r = \begin{cases} 0 & \text{se } s < t \forall t \in T \\ a_{\max(T \cap ]-\infty, s])}^{\max(T \cap ]-\infty, r])} & \text{altrimenti.} \end{cases}$$

In riferimento alle costruzioni precedenti, nel caso in cui  $T$  è un sottoinsieme chiuso e discreto di  $\mathbb{R}$ , chiameremo l'operazione  $A \mapsto A|_T$  **discretizzazione** di  $A$ , e l'operazione  $A \mapsto \tilde{A}$  **estensione semicontinua** di  $A$ .

Sebbene molti risultati, come ad esempio il teorema di esistenza e stabilità del diagramma di persistenza, valgono per moduli  $q$ -tame (vedi [16]), per semplicità espositiva

tratteremo esclusivamente moduli di persistenza di tipo finito. Tale restrizione non influisce negativamente sulla stragrande maggioranza delle applicazioni pratiche. Riportiamo, in maggior dettaglio, la definizione di modulo di persistenza di tipo finito:

**DEFINIZIONE 6.4.2.** Sia  $T = \{t_0 < t_1 < t_2 < \dots < t_m\}$  un insieme finito di numeri reali. Un **modulo di persistenza** di tipo finito su  $T$  è una successione di omomorfismi di gruppi abeliani finitamente generati

$$(6.1) \quad P(t_0) \xrightarrow{p_0} P(t_1) \xrightarrow{p_1} P(t_2) \xrightarrow{p_2} \dots \xrightarrow{p_{m-1}} P(t_m)$$

indicizzata in ordine crescente dagli elementi di  $T$ .

Prima di illustrare alcuni esempi facciamo alcune considerazioni di tipo notazionale.

- (1) Nelle notazioni del capitolo precedente, per ogni  $i \leq j$  il morfismo  $p_{t_i}^{t_j}$  non è altro che la composizione  $p_{j-1} \circ \dots \circ p_i$ .
- (2) È spesso utile estendere convenzionalmente ogni modulo di persistenza  $P$  su  $T \subset \mathbb{R}$  ad un modulo di persistenza su  $T \cup \{+\infty\}$  ponendo  $P(+\infty) = 0$ .
- (3) Esiste un modo naturale di estendere la Definizione 6.4.2 se il sottoinsieme  $T$  viene rimpiazzato da una successione finita monotona  $t_0 \leq t_1 \leq \dots$  di numeri reali: in tal caso bisogna però imporre che  $p_i = \text{Id}$  se  $t_i = t_{i+1}$ .

**ESEMPIO 6.4.3.** Siano  $V$  uno spazio vettoriale ed  $f: V \rightarrow V$  un endomorfismo nilpotente, diciamo  $f^n = 0$  per qualche  $n > 0$ . Se poniamo  $V(0) = V$  e  $V(i) = f^i(V)$  per ogni  $i > 0$ , si ha un modulo di persistenza

$$(6.2) \quad 0 \rightarrow V(0) \xrightarrow{f} V(1) \xrightarrow{f} V(2) \xrightarrow{f} \dots \xrightarrow{f} V(n) = 0,$$

con le applicazioni  $p_i = f$  surgettive per  $i \geq 0$ .

**ESEMPIO 6.4.4.** Sia  $(K, f)$  un complesso filtrato di tipo finito e sia  $n \geq 0$  fissato. Sia  $t_0 < t_1 < \dots < t_m$  la successione dei valori critici di  $f$  in ordine crescente. Gli  $n$ -esimi gruppi di omologia della catena ascendente dei sottocomplessi di livello  $K(t_0) \subset K(t_1) \subset \dots$  determinano un pre-modulo di persistenza di tipo finito

$$(6.3) \quad H_n(K(t_0)) \xrightarrow{p_0} H_n(K(t_1)) \xrightarrow{p_1} H_n(K(t_2)) \xrightarrow{p_2} \dots \xrightarrow{p_{m-1}} H_n(K(t_m)),$$

dove  $p_s$  è il morfismo indotto in omologia dall'inclusione  $K(t_s) \subset K(t_{s+1})$ . Osserviamo inoltre che, essendo per ipotesi  $K(t)$  un complesso simpliciale astratto finito per ogni  $t$ , i gruppi di omologia  $H_n(K(t_i))$  sono finitamente generati.

Giova osservare che per ogni  $i \leq j$  l'immagine dell'applicazione  $H_n(K(t_i)) \rightarrow H_n(K(t_j))$  è il gruppo

$$\frac{Z_n(K(t_i))}{C_n(K(t_i)) \cap B_n(K(t_j))}.$$

**ESEMPIO 6.4.5.** Dato un modulo di persistenza di tipo finito

$$\dots P(t_i) \xrightarrow{p_i} P(t_{i+1}) \xrightarrow{p_{i+1}} P(t_{i+2}) \xrightarrow{p_{i+2}} \dots$$

chiameremo cancellazione di  $P(t_{i+1})$  il modulo di persistenza

$$\dots P(t_i) \xrightarrow{p_{i+1} \circ p_i} P(t_{i+2}) \xrightarrow{p_{i+2}} \dots$$

ottenuto eliminando  $P(t_{i+1})$  e componendo  $p_i$  con  $p_{i+1}$ . Se  $\tilde{P}$  e  $\tilde{Q}$  sono rispettivamente le estensioni semicontinue del suddetto modulo e della sua cancellazione in  $P(t_{i+1})$ , allora  $Q(t) = P(t)$  se  $t < t_{i+1}$  oppure se  $t \geq t_{i+2}$ , mentre se  $t_{i+1} \leq t < t_{i+2}$  si ha  $Q(t) = P(t_i)$  e  $P(t) = P(t_{i+1})$ . Esiste quindi un morfismo naturale  $f: Q \rightarrow P$  definito da  $f_t = \text{Id}$  se  $t < t_{i+1}$  oppure se  $t \geq t_{i+2}$  e  $f_t = p_i$  se  $t_{i+1} \leq t < t_{i+2}$ . In particolare,  $f$  è un isomorfismo se e solo se  $p_i$  è un isomorfismo.

Vogliamo adesso estrarre alcuni invarianti discreti dai moduli di persistenza semicontinui di tipo finito; a tale scopo facciamo lo stesso per i moduli di persistenza di tipo finito su insiemi finiti, assicurandoci poi che moduli con estensioni isomorfe abbiano gli stessi invarianti.

DEFINIZIONE 6.4.6. Dato un modulo di persistenza  $P$  su un insieme finito  $T = \{t_0 < \dots < t_m\}$ , diremo che un elemento  $x \in P(t_i)$  è **primordiale** se non appartiene all'immagine di  $p_{i-1}$ .

In particolare gli elementi primordiali non sono mai nulli ed ogni elemento di  $P(t_0)$  non nullo è primordiale. Per semplicità notazionale,  $i \leq j$  denotiamo  $p_{i,j} = p_{t_i}^{t_j}$ , ossia  $p_{i,j}: P(t_i) \rightarrow P(t_j)$  è la composizione di  $p_i, p_{i+1}, \dots, p_{j-1}$ : si ha  $p_{i,i} = \text{Id}$ ,  $p_{i,i+1} = p_i$  eccetera.

Se  $x \in P(t_i)$  è primordiale, diremo anche che  $x$  **nasce**, oppure che è creato, in  $t_i$ .

DEFINIZIONE 6.4.7. Diremo che un elemento primordiale  $x \in P(t_i)$  **muore**, od anche che viene distrutto, in  $t_j$  se:

$$j > i, \quad p_{i,j}(x) = 0, \quad p_{i,j-1}(x) \neq 0.$$

In tal caso chiameremo  $[t_i, t_j[ \subset \mathbb{R}$  l'**intervallo di vita** di  $x$ . Se  $x$  è immortale, ossia se  $x \in P(t_i)$  e  $p_{i,j}(x) \neq 0$  per ogni  $j \geq i$ , allora diremo che  $x$  muore all'infinito e gli assegniamo  $[t_i, +\infty[$  come suo intervallo di vita.

Dato un modulo di persistenza  $P$  come nella Definizione 6.4.2, per ogni coppia di interi  $0 \leq i \leq j \leq m$  definiamo

$$P^{i,j} = \frac{P(t_i)}{\ker(p_{i,j})} \cong \text{Im}(p_{i,j}).$$

Dunque ciascun morfismo  $p_{i,j}$  si fattorizza come composizione di un morfismo surgettivo  $P(t_i) \rightarrow P^{i,j}$  ed un morfismo iniettivo  $P^{i,j} \rightarrow P(t_j)$ . Informalmente, il gruppo  $P^{i,j}$  rappresenta gli elementi di  $P(t_i)$  che sono ancora vivi in  $t_j$ . Osserviamo inoltre che:

- (1) se  $i \leq j \leq k$  allora  $\ker(p_{i,j}) \subseteq \ker(p_{i,k})$  ed è quindi definito un morfismo *surgettivo*  $P^{i,j} \rightarrow P^{i,k}$ ;
- (2) se  $i \leq h \leq j$ , siccome  $p_{i,j} = p_{h,j} \circ p_{i,h}$ , per un elemento  $x \in P(t_i)$  si ha

$$x \in \ker(p_{i,j}) \iff p_{i,h}(x) \in \ker(p_{h,j})$$

e quindi  $p_{i,h}: P(t_i) \rightarrow P(t_h)$  si fattorizza ad un morfismo *iniettivo*  $\overline{p_{i,h}}: P^{i,j} \rightarrow P^{h,j}$ .

Dunque, per ogni quaterna  $i \leq h \leq k \leq j$  di numeri naturali si ha un quadrato commutativo

$$(6.4) \quad \begin{array}{ccc} P^{i,k} & \longrightarrow & P^{h,k} \\ \downarrow & & \downarrow \\ P^{i,j} & \longrightarrow & P^{h,j} \end{array}$$

con le frecce orizzontali iniettive e le frecce verticali surgettive.

In particolare, per ogni  $i < j$  si ha un diagramma commutativo

$$\begin{array}{ccccccc} 0 & \longrightarrow & P^{i-1,j-1} & \xrightarrow{\sigma_{i,j}} & P^{i,j-1} & \longrightarrow & \text{coker}(\sigma_{i,j}) \longrightarrow 0 \\ & & \downarrow & & \downarrow & & \downarrow \gamma_{i,j} \\ 0 & \longrightarrow & P^{i-1,j} & \xrightarrow{\tau_{i,j}} & P^{i,j} & \longrightarrow & \text{coker}(\tau_{i,j}) \longrightarrow 0 \end{array}$$

con le righe esatte e le frecce verticali surgettive. Informalmente, il conucleo di  $\sigma_{i,j}$  (rispettivamente: di  $\tau_{i,j}$ ) rappresenta le classi primordiali di  $P(t_i)$  che sono ancora vive in  $P(t_{j-1})$  (rispettivamente: di  $P(t_j)$ ). Da ciò segue che il nucleo di  $\gamma_{i,j}$  è il gruppo che rappresenta le classi primordiali di  $P(t_i)$  che muoiono in  $P(t_j)$ .

Se il modulo di persistenza è di tipo finito, per ipotesi i gruppi  $P(t_i)$  sono tutti finitamente generati, e quindi lo sono anche i gruppi  $P^{i,j}$ : ed i loro ranghi

$$\beta_P^{i,j} = \text{rank}(P^{i,j})$$

vengono detti **numeri di Betti persistenti**. Per le precedenti osservazioni, i numeri

$$\mu_P^{i,j} = \text{rank}(\ker(\gamma_{i,j})),$$

rappresentano la “misura dimensionale” degli elementi che nascono in  $t_i$  e muoiono in  $t_j$ ; chiameremo  $\mu_P^{i,j}$  la **molteplicità** dell’intervallo di vita  $[t_i, t_j[$ .

Scriveremo semplicemente  $\beta^{i,j}$  e  $\mu^{i,j}$  quando il modulo  $P$  è chiaro dal contesto, ad esempio se non ce ne sono altri nel discorso.

LEMMA 6.4.8. *Se  $i \leq h \leq k \leq j$ , ossia se  $[t_h, t_k[ \subset [t_i, t_j[$ , allora:*

- (1)  $\beta^{h,k} \geq \beta^{i,j}$ , e cioè i numeri di Betti persistenti sono una funzione decrescente sugli intervalli di vita;
- (2)  $(\beta^{h,k} - \beta^{h,j}) \geq (\beta^{i,k} - \beta^{i,j})$ .

DIMOSTRAZIONE. Dal fatto che nel quadrato commutativo (6.4) le frecce orizzontali sono iniettive segue che  $\beta^{i,k} \leq \beta^{h,k}$ , mentre dal fatto le frecce verticali sono surgettive segue che  $\beta^{i,j} \leq \beta^{i,k}$ .

Ribaltando il quadrato (6.4) rispetto alla diagonale principale ed aggiungendo al diagramma i nuclei dei morfismi orizzontali (che prima del ribaltamento erano verticali) otteniamo un diagramma commutativo con le righe esatte

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \longrightarrow & P^{i,k} & \longrightarrow & P^{i,j} & \longrightarrow & 0 \\ & & \downarrow & & \downarrow \sigma & & \downarrow & & \\ 0 & \longrightarrow & B & \longrightarrow & P^{h,k} & \longrightarrow & P^{h,j} & \longrightarrow & 0 \end{array}$$

e con il morfismo  $\sigma$  iniettivo. A maggior ragione la restrizione  $\sigma|_A: A \rightarrow B$  è iniettiva e quindi per l’additività del rango

$$\beta^{h,k} - \beta^{h,j} = \text{rank}(B) \geq \text{rank}(A) = \beta^{i,k} - \beta^{i,j}.$$

□

Per l’additività del rango abbiamo:

$$\begin{aligned} \mu^{i,j} &= \text{rank}(\ker(\gamma_{i,j})) = \text{rank}(\text{coker}(\sigma_{i,j})) - \text{rank}(\text{coker}(\tau_{i,j})) \\ &= \text{rank}(P^{i,j-1}) - \text{rank}(P^{i-1,j-1}) - \text{rank}(P^{i,j}) + \text{rank}(P^{i-1,j}) \\ &= \beta^{i,j-1} - \beta^{i-1,j-1} - \beta^{i,j} + \beta^{i-1,j} = (\beta^{i,j-1} - \beta^{i,j}) - (\beta^{i-1,j-1} - \beta^{i-1,j}). \end{aligned}$$

Le molteplicità  $\mu^{i,j}$  misurano solamente le classi mortali. Per “contare” le classi immortali, se si introducono:

$$P^{i,\infty} = \frac{P(t_i)}{\cup_{j>i} \ker(p_{i,j})}, \quad \beta^{i,\infty} = \text{rank}(P^{i,\infty}), \quad \mu^{i,\infty} = \beta^{i,\infty} - \beta^{i-1,\infty}.$$

Il gruppo  $P^{i,\infty}$  rappresenta le classi di  $P(t_i)$  che non muoiono; dato che il morfismo  $P(t_{i-1}) \rightarrow P(t_i)$  si fattorizza ad un morfismo iniettivo  $P^{i-1,\infty} \xrightarrow{\sigma} P^{i,\infty}$  il cui conucleo (di rango  $\mu^{i,\infty}$ ) rappresenta le classi di  $P(t_i)$  che sono primordiali e immortali. Chiameremo  $\mu^{i,\infty}$  la **molteplicità** dell’intervallo di vita  $[t_i, +\infty[$ .

Quindi i numeri di Betti persistenti determinano le molteplicità; viceversa le molteplicità determinano i numeri di Betti persistenti in virtù del seguente risultato.

LEMMA 6.4.9 (Lemma fondamentale dell’omologia persistente). *Dato un modulo di persistenza di tipo finito*

$$P(t_0) \xrightarrow{p_0} P(t_1) \xrightarrow{p_1} P(t_2) \xrightarrow{p_2} \dots P(t_m),$$

valgono le formule:

$$\begin{aligned}
\mu^{i,j} &= (\beta^{i,j-1} - \beta^{i,j}) - (\beta^{i-1,j-1} - \beta^{i-1,j}) \\
\mu^{i,\infty} &= \beta^{i,\infty} - \beta^{i-1,\infty} \\
(6.5) \quad \beta^{h,k} &= \sum_{i=0}^h \sum_{k < j \leq \infty} \mu^{i,j} = \sum_{i=0}^h \left( \mu^{i,\infty} + \sum_{j=k+1}^m \mu^{i,j} \right) \\
\beta^{h,\infty} &= \sum_{i=0}^h \mu^{i,\infty},
\end{aligned}$$

dove  $\beta^{-1,h} = \beta^{-1,\infty} = 0$  per convenzione.

**DIMOSTRAZIONE.** Le prime due formule sono essenzialmente la definizione formale delle molteplicità degli intervalli di vita, motivate dalle considerazioni euristiche su nascita e morte degli elementi. La quarta equazione segue immediatamente dalla seconda osservando che  $\beta^{-1,\infty} = 0$ .

Per quanto riguarda la terza, siccome  $\beta^{i,\infty} = \beta^{i,m}$  e  $\mu^{i,\infty} = \beta^{i,m} - \beta^{i-1,m}$ , per ogni  $i \leq k$  si ha

$$\begin{aligned}
\mu^{i,\infty} + \sum_{j=k+1}^m \mu^{i,j} &= \beta^{i,m} - \beta^{i-1,m} + \sum_{j=k+1}^m (\beta^{i,j-1} - \beta^{i,j}) - \sum_{j=k+1}^{\infty} (\beta^{i-1,j-1} - \beta^{i-1,j}) \\
&= \beta^{i,k} - \beta^{i-1,k}.
\end{aligned}$$

Dato che  $\beta^{-1,k} = 0$  si ottiene finalmente

$$\sum_{i=0}^h \mu^{i,\infty} + \sum_{k < j \leq m} \mu^{i,j} = \sum_{i=0}^k (\beta^{i,k} - \beta^{i-1,k}) = \beta^{h,k}.$$

□

**COROLLARIO 6.4.10.** *Dato un pre-modulo di persistenza localmente di tipo finito*

$$P(t_0) \xrightarrow{p_0} P(t_1) \xrightarrow{p_1} P(t_2) \xrightarrow{p_2} \dots,$$

con molteplicità  $\mu^{i,j}$  si ha:

- (1) se  $p_i: P(t_i) \rightarrow P(t_{i+1})$  è surgettivo, allora  $\mu^{i+1,j} = 0$  per ogni  $j > i + 1$ ;
- (2) se  $p_j: P(t_j) \rightarrow P(t_{j+1})$  è iniettivo, allora  $\mu^{i,j+1} = 0$  per ogni  $i \leq j$ .

In particolare, se  $p_i: P(t_i) \rightarrow P(t_{i+1})$  è un isomorfismo, allora  $\mu^{i+1,j} = \mu^{h,i+1} = 0$  per ogni  $h < i + 1$  ed ogni  $j > i + 1$ . In altri termini, gli intervalli di vita che hanno  $t_{i+1}$  come estremo hanno tutti molteplicità nulla.

**DIMOSTRAZIONE.** Basta osservare che nel primo caso basta osservare che nessun elemento nasce in  $P(t_{i+1})$ , mentre nel secondo caso nessun elemento muore in  $P(t_{j+1})$ . □

**6.4.1. Il lemma degli scatti (snapping lemma).** Consideriamo un modulo di persistenza  $P$  di tipo finito

$$P(t_0) \xrightarrow{p_0} P(t_1) \xrightarrow{p_1} P(t_2) \xrightarrow{p_2} \dots \xrightarrow{p_{m-1}} P(t_m),$$

prendiamo la sua estensione semicontinua  $\tilde{P}$  e poi la restrizione  $Q = \tilde{P}|_S$  ad un sottoinsieme finito  $S = \{s_0 < \dots < s_n\}$ .

Lo snapping lemma ci dice come calcolare le molteplicità  $\mu_Q^{i,j}$  in funzione delle molteplicità  $\mu_P^{i,j}$ .

**LEMMA 6.4.11 (Snapping).** *Nelle notazioni precedenti, per ogni  $0 \leq a < b \leq n$  si ha*

$$\mu_Q^{a,b} = \sum_{t_i \in ]s_{a-1}, s_a], t_j \in ]s_{b-1}, s_b]} \mu_P^{i,j}.$$

Inoltre, se  $s_n \geq t_m$  si ha

$$\mu_Q^{a,\infty} = \sum_{t_i \in ]s_{a-1}, s_a]} \mu_P^{i,\infty},$$

dove si intende  $s_{-1} = -\infty$ .

DIMOSTRAZIONE. Oltre che  $s_{-1} = -\infty$  poniamo per convenzione  $t_{-1} = -\infty$ ,  $Q(s_{-1}) = P(t_{-1}) = 0$ . Definiamo i quattro indici  $-1 \leq i, j, h, k \leq m$  nel modo seguente:

- (1)  $i = \max\{l \mid t_l \leq s_{a-1}\}$ ;
- (2)  $j = \max\{l \mid t_l \leq s_a\}$ ;
- (3)  $h = \max\{l \mid t_l \leq s_{b-1}\}$ ;
- (4)  $k = \max\{l \mid t_l \leq s_b\}$ .

Per come è stato definito  $Q$  si ha:

$$\beta_Q^{a-1,b-1} = \beta_P^{i,h}, \quad \beta_Q^{a-1,b} = \beta_P^{i,k}, \quad \beta_Q^{a,b-1} = \beta_P^{j,h}, \quad \beta_Q^{a,b} = \beta_P^{j,k}.$$

Applicando il lemma fondamentale dell'omologia persistente si ottiene

$$\begin{aligned} \mu_Q^{a,b} &= (\beta_Q^{a,b-1} - \beta_Q^{a,b}) - (\beta^{a-1,b-1})_Q - \beta_Q^{i-1,j} \\ &= (\beta_P^{j,h} - \beta_P^{j,k}) - (\beta_P^{i,h} - \beta_P^{i,k}). \end{aligned}$$

Siccome

$$\begin{aligned} \beta_P^{j,h} - \beta_P^{j,k} &= \sum_{r=0}^j \left( \mu_P^{r,\infty} + \sum_{s=h+1}^m \mu_P^{r,s} \right) - \sum_{r=0}^j \left( \mu_P^{r,\infty} + \sum_{s=k+1}^m \mu_P^{r,s} \right) \\ &= \sum_{r=0}^j \sum_{s=h+1}^k \mu_P^{r,s}, \end{aligned}$$

e similmente

$$\beta_P^{i,h} - \beta_P^{i,k} = \sum_{r=0}^i \sum_{s=h+1}^k \mu_P^{r,s},$$

si ottiene

$$\mu_Q^{a,b} = \sum_{r=i+1}^j \sum_{s=h+1}^k \mu_P^{r,s} = \sum_{t_i \in ]s_{a-1}, s_a], t_j \in ]s_{b-1}, s_b]} \mu_P^{i,j}.$$

Se  $s_n \geq t_m$  allora  $\beta_Q^{a,\infty} = \beta_Q^{a,n} = \beta_P^{i,m} = \beta_P^{j,\infty}$ ,  $\beta_Q^{a-1,\infty} = \beta_P^{i,\infty}$  e quindi

$$\begin{aligned} \mu_Q^{a,\infty} &= \beta_Q^{a,\infty} = \beta_Q^{a-1,\infty} = \beta_P^{j,\infty} - \beta_P^{i,\infty} \\ &= \sum_{s=i+1}^j \mu_P^{s,\infty} = \sum_{t_i \in ]s_{a-1}, s_a]} \mu_P^{i,\infty}. \end{aligned}$$

□

### 6.5. Barcode e diagramma di persistenza

Denotiamo con  $\mathcal{I} \subset \mathcal{P}(\mathbb{R})$  la famiglia di tutti gli intervalli del tipo  $[a, b[ \subset \mathbb{R}$ , con  $a < b \leq +\infty$ . Per ogni modulo di persistenza di tipo finito

$$P: P(t_0) \xrightarrow{p_0} P(t_1) \xrightarrow{p_1} P(t_2) \xrightarrow{p_2} \dots \xrightarrow{p_{m-1}} P(t_m),$$

denotiamo con  $\mu: \mathcal{I} \rightarrow \mathbb{N}$  la sua funzione di molteplicità, che associa ad ogni intervallo di vita la sua molteplicità. Più precisamente, nelle notazioni precedenti:

$$\mu([a, b[) = \begin{cases} \mu^{i,j} & \text{se } a = t_i, b = t_j, \\ \mu^{i,\infty} & \text{se } a = t_i, b = +\infty \\ 0 & \text{altrimenti.} \end{cases}$$

Tra le varie conseguenze del Corollario 6.4.10 vi è quello che la funzione di molteplicità è invariante rispetto alla cancellazione degli isomorfismi. Più precisamente, supponiamo che

in (6.1) si abbia  $p_k$  bigettivo per qualche  $k \geq 0$ ; allora la sua caratteristica è uguale a quella del modulo di persistenza ottenuto “cancellando”  $P(t_{k+1})$ , ossia

$$\dots \xrightarrow{p_{k-1}} P(t_k) \xrightarrow{p_{k+1}p_k} P(t_{k+2}) \xrightarrow{p_{k+2}} P(t_{k+3}) \dots$$

Ci sono vari modi di visualizzare graficamente le caratteristiche dei moduli di persistenza: nei più usati in letteratura (barcode, digramma di persistenza, diagramma landscape ecc.) viene fatto uso del concetto di funzione polidroma.

Fino agli inizi del XX secolo, i matematici parlavano senza imbarazzo di funzioni polidrome, ossia di funzioni che ad un punto del dominio associano più punti del codominio. Tale concetto, che sembrava scomparso, sta ritornando prepotentemente all’attenzione in teoria della persistenza (ma non solo).

**DEFINIZIONE 6.5.1.** Siano  $S, X$  due insiemi. Una **funzione polidroma** di base  $S$  e indici  $X$ , graficamente denotata  $f: S \rightsquigarrow X$ , è un’applicazione che ad ogni elemento  $s \in S$  associa un sottoinsieme  $f(s)$  di  $X$ .

Dunque, dare una funzione polidroma  $f: S \rightsquigarrow X$  è la stessa cosa che dare un’applicazione da  $f$  nell’insieme delle parti di  $X$ .

Esempi classici di funzioni polidrome sono la radice quadrata ed il logaritmo di numeri complessi.

**DEFINIZIONE 6.5.2.** Sia  $\mathcal{I}$  la famiglia di tutti gli intervalli di  $\mathbb{R}$  del tipo  $[a, b[$ , con  $a < b \leq +\infty$ . Chiameremo **barcode** una funzione polidroma  $\phi: \mathcal{I} \rightsquigarrow \mathbb{R}$  tale che  $\phi([a, b[) \cap \phi([c, d[) = \emptyset$  se  $[a, b[ \neq [c, d[$ .

Chiameremo **molteplicità** di un intervallo  $[a, b[$  (nel barcode  $\phi$ ) la cardinalità dell’insieme  $\phi([a, b[)$ . Diremo che due barcode  $\phi, \psi$  sono isomorfi se ogni intervallo  $[a, b[ \in \mathcal{I}$  ha la medesima molteplicità in  $\phi, \psi$ .

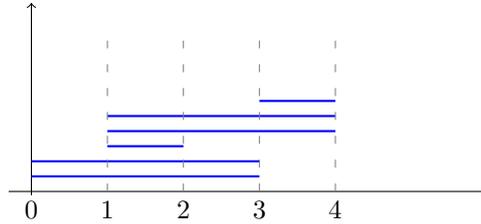


FIGURA 4. Un esempio di barcode, con gli intervalli  $[0, 3[$  e  $[1, 4[$  di molteplicità 2, gli intervalli  $[1, 2[$  e  $[3, 4[$  di molteplicità 1 (e tutti gli altri di molteplicità 0).

Per comprendere il motivo del nome barcode, supponiamo che la somma di tutte le molteplicità sia finita; allora esistono al più un numero finito di intervalli, diciamo  $I_1, \dots, I_n \subset \mathbb{R}$  di molteplicità positiva. In tale situazione il barcode si può rappresentare graficamente a foggia di *lasagna*, ossia come unione di barre orizzontali in  $\mathbb{R}^2$  in numero uguale alla somma delle molteplicità: in buona sostanza, per ogni  $j$  l’intervallo  $I_j \times \{0\}$  viene traslato in verticale per valori distinti in quantità uguale alla molteplicità (vedi Figura 4).

Ad ogni modulo di persistenza di tipo finito si associa una classe di isomorfismo di barcode, in cui le molteplicità degli intervalli sono esattamente le molteplicità degli intervalli di vita.

**ESEMPIO 6.5.3.** Calcoliamo i barcode degli 0-cicli e 1-cicli del complesso filtrato di Vietoris–Rips della (micro)nuvola di punti  $I = \{(0, 0), (4, 0), (0, 4), (5, 5)\} \subset \mathbb{R}^2$ . I valori critici della funzione filtrante  $v: \Delta^I \rightarrow \mathbb{R}$  sono tutte e sole le semidistanze tra coppie di punti di  $I$  e sono quindi

$$0 < 2 < \sqrt{13}/2 < \sqrt{8} < 5/\sqrt{2}.$$

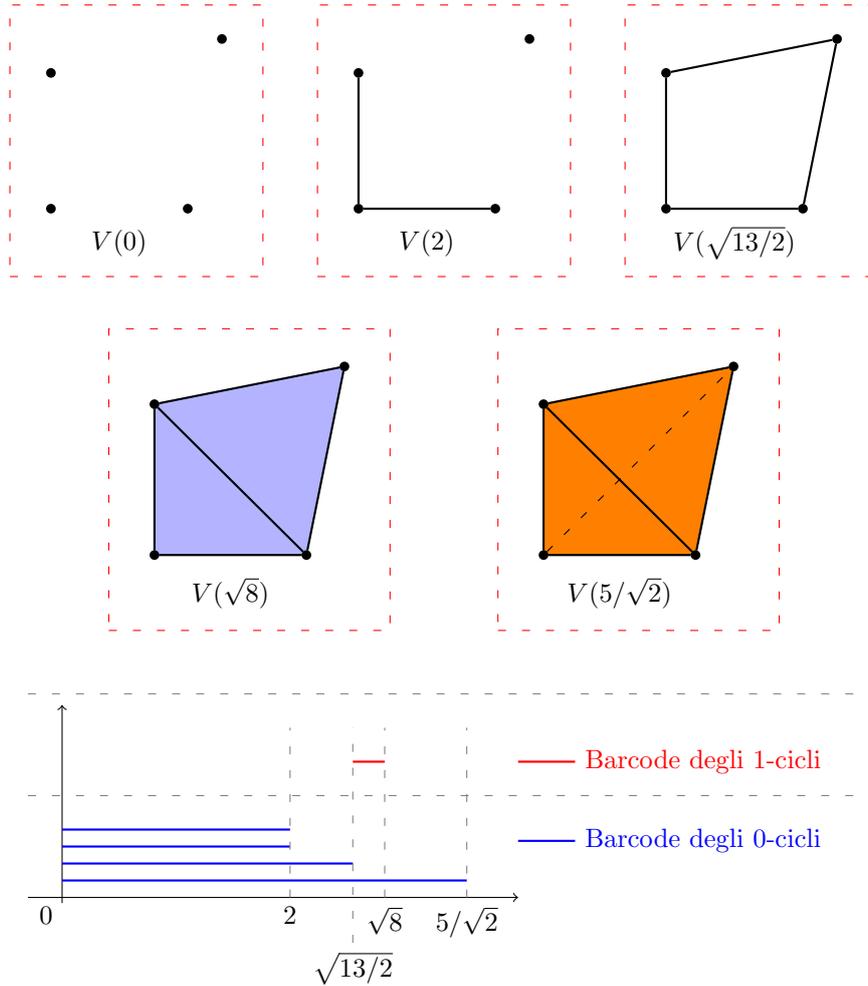


FIGURA 5. Descrizione nell'Esempio 6.5.3.

La Figura 5 mostra i sottocomplessi di livello  $V(t) = \{x \in \Delta^I \mid v(x) \leq t\}$  per ciascuno dei 5 valori critici (in celeste i 2-simplessi massimali ed in arancio i 3-simplessi massimali).

Siccome  $H_i(V(t)) = 0$  per ogni  $t$  ed ogni  $i > 1$ , gli unici moduli di persistenza omologici non banali sono quelli in grado 0 e grado 1. Nella parte inferiore di Figura 5 sono mostrati i barcode degli 0-cicli (intervalli di vita delle componenti connesse, in blu) e degli 1-cicli (intervalli di vita dei buchi a circonferenza, in rosso).

Oltre al barcode, un altro modo di rappresentazione è dato dal diagramma di persistenza, detto anche diagramma delle molteplicità, che non è altro che il grafico del barcode.

Prima di entrare nel merito della questione, è utile fare qualche considerazione aggiuntiva sulle funzioni polidrome e sui loro grafici.

In accordo con quanto affermato da Jacobson ([12, p. 5]) per le funzioni monodrome (quelle usuali), il miglior modo per formalizzare il concetto di funzione polidroma è definendo in maniera rigorosa quello che a posteriori può essere considerato il suo grafico.

DEFINIZIONE 6.5.4 (cf. [1, Defn. 2.2]). Siano  $S, X$  due insiemi. Una **rappresentazione polidroma**<sup>1</sup> di base  $S$  e indici  $X$  è un sottoinsieme  $T \subset S \times X$ . Per ogni  $s \in S$ , la **molteplicità**  $\mu_s$  di  $s$  in  $T$  è per definizione la cardinalità della fibra  $p^{-1}(s)$ , dove  $p: T \rightarrow S$  è la restrizione a  $T$  della proiezione sul primo fattore. Equivalentemente

$$\mu_s = |\{x \in X \mid (s, x) \in T\}|.$$

<sup>1</sup>In inglese “multiset representation”.

Qualora  $X = \mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$  eccetera, diremo che la rappresentazione polidroma è naturale, intera, razionale, reale eccetera.

È chiaro come ogni funzione polidroma  $f: S \rightsquigarrow X$ ,  $s \mapsto f(s) \subset X$ , è univocamente determinata dal suo grafico

$$T = \cup_{s \in S} \{s\} \times f(s) \subseteq S \times X$$

che è una rappresentazione polidroma. Viceversa, ogni rappresentazione polidroma  $T \subset S \times X$  è il grafico della funzione polidroma  $f: S \rightsquigarrow X$ ,  $f(s) = i_s^{-1}(T)$ , dove  $i_s: X \rightarrow S \times X$ ,  $i_s(x) = (s, x)$ .

**DEFINIZIONE 6.5.5.** Due rappresentazioni polidrome  $T \subset S \times X$ ,  $R \subset S \times Y$  sulla medesima base  $S$  si dicono **equivalenti per cambio di indici**, od anche per **reindicizzazione**, se esiste un'applicazione bigettiva  $f: T \rightarrow R$  che commuta con le proiezioni sulla base, ossia se per ogni  $(s, x) \in T$  vale  $f(s, x) = (s, y)$  per qualche  $y \in Y$ .

Chiameremo **multi-insieme**<sup>2</sup>, od anche **insieme con ripetizioni**, una classe di equivalenza di rappresentazioni polidrome per cambio di indici.

Ad esempio le due rappresentazioni polidrome di base  $\mathbb{N}$ :

$$T = \{(s, x) \in \mathbb{N} \times \mathbb{N} \mid s < x < 2s\}, \quad R = \{(s, y) \in \mathbb{N} \times \mathbb{Z} \mid 3s < y < 4s\},$$

definiscono lo stesso multi-insieme: una possibile reindicizzazione è data dall'applicazione bigettiva  $T \rightarrow R$ ,  $(s, x) \mapsto (s, x + 2s)$ .

È chiaro che la molteplicità di un elemento della base è invariante per reindicizzazione, ossia per cambio di indici e segue dall'assioma della scelta che due rappresentazioni polidrome sulla medesima base  $S$  sono equivalenti per cambio di indici se e solo se hanno la stessa molteplicità in ogni  $s \in S$ . Quindi per ogni multi-insieme risultano ben definite sia la sua base  $S$  sia le sue molteplicità per ogni  $s \in S$ .

**ESEMPIO 6.5.6.** Per ogni applicazione  $p: X \rightarrow S$  possiamo considerare la sua "inversa polidroma"  $f: S \rightsquigarrow X$ ,  $f(s) = p^{-1}(s)$ ; quindi possiamo interpretare l'applicazione  $p: X \rightarrow S$  come un multi-insieme di base  $S$ , più precisamente come la classe di equivalenza della rappresentazione polidroma di base  $S$  data dal grafico di  $p$ , ossia

$$\{(p(t), t) \mid t \in T\} = \{(s, x) \mid s \in S, x \in p^{-1}(s)\} \subset S \times T.$$

In tale multi-insieme la molteplicità di un  $s \in S$  è esattamente la cardinalità della fibra  $p^{-1}(s)$ . Due applicazioni  $p: T \rightarrow S$  e  $q: R \rightarrow S$  rappresentano lo stesso multi-insieme se e solo se esiste un'applicazione bigettiva  $f: T \rightarrow R$  tale che  $qf = p$ .

Ogni multi-insieme può essere ottenuto in questo modo, infatti ogni rappresentazione polidroma  $T \subset S \times X$  è equivalente per cambio di indici al grafico della proiezione  $p: T \rightarrow S$ .

**DEFINIZIONE 6.5.7.** Sia  $\kappa$  un numero cardinale infinito. Un multi-insieme si dice di taglia  $\kappa$  se tutte le sue fibre hanno cardinalità  $\leq \kappa$ , equivalentemente, se è definito da una rappresentazione polidroma con insieme degli indici di cardinalità  $\kappa$ . Quando non viene fatto riferimento alla taglia si intende implicitamente che essa sia la più piccola possibile,  $\kappa = \aleph_0$ .

**OSSERVAZIONE 6.5.8.** Il riferimento alla taglia si comprende tenendo presente il paradosso di Russell. Infatti, mentre la collezione di tutti i multi-insiemi di base  $S$  non è un insieme, risulta invece essere un insieme la collezione di tutti i multi-insiemi di base  $S$  e taglia fissata.

**DEFINIZIONE 6.5.9.** Un **diagramma di persistenza** è un multi-insieme di base il **semipiano esteso**:

$$S = \{(a, b) \mid a < b \leq +\infty\} \subset (\mathbb{R} \cup \{+\infty\}) \times (\mathbb{R} \cup \{+\infty\}).$$

Un diagramma di persistenza può essere quindi determinato sia da una rappresentazione polidroma  $T \subset S \times X$  che da un'applicazione  $v: T \rightarrow S$ . In queste note, per mantenere uniformità di notazioni, rappresenteremo sempre un diagramma di persistenza con una coppia  $(T, v)$ , dove  $T$  è un insieme e  $v: T \rightarrow S$  è un'applicazione. Due applicazioni  $v_1: T_1 \rightarrow S$ ,  $v_2: T_2 \rightarrow S$  definiscono lo stesso diagramma se e solo se esiste un'applicazione bigettiva

<sup>2</sup>In inglese multiset.

$f: T_1 \rightarrow T_2$  tale che  $v_1 = v_2 f$ . Data una qualsiasi famiglia  $v_i: T_i \rightarrow S$ ,  $i \in I$ , di diagrammi di persistenza risulta ben definita la sua unione disgiunta  $\coprod_{i \in I} T_i \rightarrow S$ : più concretamente, si tratta del multi-insieme definito dalla rappresentazione polidroma

$$\Gamma \subset S \times I \times (\cup_i T_i), \quad \Gamma = \{(s, i, t) \mid t \in T_i, v_i(t) = s\}.$$

Ad ogni barcode  $\phi: \mathcal{T} \rightsquigarrow \mathbb{R}$  corrisponde il diagramma di persistenza in cui la molteplicità di  $(a, b) \in S$  è uguale alla cardinalità di  $\phi([a, b])$ .

Riepilogando, abbiamo la seguente definizione di diagramma di persistenza di un modulo di persistenza.

DEFINIZIONE 6.5.10. Dato un modulo di persistenza di tipo finito

$$P: P(t_0) \xrightarrow{p_0} P(t_1) \xrightarrow{p_1} P(t_2) \xrightarrow{p_2} \dots \xrightarrow{p_{m-1}} P(t_m),$$

il suo **diagramma di persistenza**, o **diagramma delle molteplicità**  $\text{dgm}(P)$  è il multi-insieme con base il semipiano esteso  $S$  nel quale:

- (1) per ogni  $i < j$  il punto  $(t_i, t_j)$  ha molteplicità  $\mu^{i,j}$ ;
- (2) per ogni  $i$  il punto  $(t_i, +\infty)$  ha molteplicità  $\mu^{i,\infty}$ ;
- (3) in tutti gli altri punti la molteplicità è uguale a 0.

OSSERVAZIONE 6.5.11. Ai fini esclusivamente grafici, si può rappresentare il punto  $(a, \infty) \in S$  come la semiretta  $\{(a, y) \mid y \geq a\} \subset \mathbb{R}^2$ .

## 6.6. Basi cicliche e basi di persistenza

Abbiamo visto che per una matrice  $A \in M_{n,m}(\mathbb{Z})$ , il suo rango come matrice a coefficienti razionali o reali è uguale al rango dell'immagine di  $A: \mathbb{Z}^m \rightarrow \mathbb{Z}^n$  come gruppo abeliano. Da ciò segue che i numeri di Betti della omologia a coefficienti razionali sono uguali a quelli dell'omologia a coefficienti interi; grazie alla Formula (3.6) le stesse considerazioni si applicano ai numeri di Betti persistenti.

Dunque, nello studio delle molteplicità nei moduli di persistenza derivanti da complessi filtrati non è restrittivo studiare le omologie a coefficienti in un campo, dove abbiamo a disposizione migliori strumenti per comprendere la loro struttura algebrica ed i corrispondenti diagrammi di persistenza.

Innanzitutto possiamo rifare le stesse considerazioni con la dimensione al posto del rango ed abbiamo

$$(6.6) \quad \begin{aligned} \beta^{i,j} &= \dim P^{i,j} = \dim P(t_i) - \dim \ker(p_{i,j}) = \text{rank}(p_{i,j}), \\ \mu^{i,j} &= \text{rank}(p_{i,j-1}) - \text{rank}(p_{i-1,j-1}) - \text{rank}(p_{i,j}) + \text{rank}(p_{i-1,j}). \end{aligned}$$

ESEMPIO 6.6.1. Lo studio delle molteplicità  $\mu^{i,j}$  del modulo di persistenza dell'Esempio 6.4.3 ci restituisce quantità già studiate nei corsi di algebra lineare. Infatti, in tal caso per ogni  $i \leq j$  si ha

$$\text{rank}(p_{i,j}) = \begin{cases} \text{rank}(f^j) & \text{per } i \geq 0, \\ 0 & \text{per } i < 0, \end{cases}$$

da cui segue che  $\mu^{i,j} = 0$  per ogni  $0 < i < j$ , mentre

$$\mu^{0,j} = \text{rank}(f^{j-1}) - \text{rank}(f^j) = \text{numero di blocchi di Jordan di ordine } \geq j.$$

*Attenzione:* la ben nota catena di disuguaglianze  $\mu^{0,1} \geq \mu^{0,2} \geq \dots$  che vale nel caso specifico dell'Esempio 6.4.3, non vale per un generico modulo di persistenza. In aggiunta, non è difficile dimostrare (esercizio per il lettore) che ogni successione  $\mu^{i,j} \in \mathbb{N}$ ,  $0 \leq i < j$ , appare come dato di molteplicità di un modulo di persistenza.

DEFINIZIONE 6.6.2 (base persistenza). Sia

$$P(t_0) \xrightarrow{p_0} P(t_1) \xrightarrow{p_1} P(t_2) \xrightarrow{p_2} \dots \xrightarrow{p_{m-1}} P(t_m)$$

un modulo di persistenza di spazi vettoriali su di un campo  $\mathbb{K}$  e sia  $\mathcal{B}_i$  una base (non ordinata) dello spazio vettoriale  $P(t_i)$  per ogni indice  $i$ . L'unione  $\mathcal{B} = \cup_i \mathcal{B}_i$  viene detta una **base di persistenza** se, detto  $\mathcal{B}'_i = \{e \in \mathcal{B}_i \mid p_i(e) \neq 0\}$ , si ha:

- (1)  $p_i(e) \in \mathcal{B}_{i+1}$  per ogni  $e \in \mathcal{B}'_i$ ;
- (2) l'applicazione  $p_i: \mathcal{B}'_i \rightarrow \mathcal{B}_{i+1}$  è iniettiva.

DEFINIZIONE 6.6.3 (base ciclica). Sia

$$P(t_0) \xrightarrow{p_0} P(t_1) \xrightarrow{p_1} P(t_2) \xrightarrow{p_2} \cdots P(t_m)$$

un modulo di persistenza di spazi vettoriali su di un campo  $\mathbb{K}$  e sia  $\mathcal{B}_i^\dagger$  un sottoinsieme dello spazio vettoriale  $P(t_i)$  per ogni indice  $i$ . L'unione  $\mathcal{B}^\dagger = \cup_i \mathcal{B}_i^\dagger$  viene detta una **base ciclica** se per ogni  $i$ , l'unione disgiunta degli elementi diversi da 0 del tipo  $p_{h,i}(e)$ , al variare di  $h \leq i$  e  $e \in \mathcal{B}_h^\dagger$ , è una base (non ordinata) di  $P(t_i)$ .

Rimandiamo alla sottosezione 6.6.1 per una dimostrazione che le basi di persistenza e le basi cicliche esistono sempre.

È chiaro dalle definizioni che i concetti di base ciclica e di base di persistenza sono sostanzialmente equivalenti; più precisamente, sia

$$P(t_0) \xrightarrow{p_0} P(t_1) \xrightarrow{p_1} P(t_2) \xrightarrow{p_2} \cdots P(t_m)$$

un modulo di persistenza di spazi vettoriali su di un campo  $\mathbb{K}$ :

- (1) se  $\mathcal{B} = \cup_i \mathcal{B}_i$  è una base di persistenza, allora  $\mathcal{B}^\dagger = \cup_i (\mathcal{B}_i - p_{i-1}(\mathcal{B}_{i-1}))$  è una base ciclica ed ogni elemento di  $\mathcal{B}_j$  si scrive in modo unico come  $p_{i,j}(e)$  con  $i \leq j$  ed  $e \in \mathcal{B}_i^\dagger$ .
- (2) se  $\mathcal{B}^\dagger = \cup_i \mathcal{B}_i^\dagger$  è una base ciclica, allora l'insieme degli elementi diversi da 0 del tipo  $p_{h,i}(e)$ , al variare di  $h \leq i$  e  $e \in \mathcal{B}_h^\dagger$ , è una base di persistenza.

Le basi di persistenza sono omogenee rispetto ai nuclei ed alle immagini di tutti i morfismi  $p_{i,j}$ , ossia vale il seguente lemma.

LEMMA 6.6.4. *Nelle notazioni della Definizione 6.6.2, per ogni base di persistenza  $\mathcal{B}$  ed ogni  $i \leq j$  si ha*

$$(6.7) \quad \begin{aligned} \ker(p_{i,j}) &= \text{Span}(\{e \in \mathcal{B}_i \mid p_{i,j}(e) = 0\}), \\ \text{Im}(p_{i,j}) &= \text{Span}(\{p_{i,j}(e) \mid e \in \mathcal{B}_i, p_{i,j}(e) \neq 0\}). \end{aligned}$$

In particolare,

$$\beta^{i,j} \text{ è uguale al numero di elementi di } e \in \mathcal{B}_i \text{ tali che } p_{i,j}(e) \neq 0.$$

DIMOSTRAZIONE. Sia  $n$  la dimensione di  $P(t_i)$  e scegliamo un ordinamento

$$\mathcal{B}_i = \{e_1, \dots, e_n\}$$

in modo tale che per qualche  $r \leq n$  si abbia  $p_{i,j}(e_h) \neq 0$  se  $h \leq r$  e  $p_{i,j}(e_h) = 0$  se  $h > r$ . Siccome  $p_{i,j}(e_1), \dots, p_{i,j}(e_r)$  sono elementi distinti di  $\mathcal{B}_j$  si ha che il rango di  $p_{i,j}$  è  $\geq r$  e quindi  $\dim \ker(p_{i,j}) \leq n - r$  per il teorema del rango. D'altra parte,  $e_{r+1}, \dots, e_n \in \ker(p_{i,j})$  e quindi  $\dim \ker(p_{i,j}) \geq n - r$ . Ne consegue che  $p_{i,j}$  ha rango  $r$  e che valgono le due uguaglianze (6.7).  $\square$

Data una base di persistenza  $\mathcal{B}$ , denotiamo con  $\mathcal{B}^\dagger \subseteq \mathcal{B}$  la corrispondente base ciclica, ossia  $\mathcal{B}_i^\dagger = \mathcal{B}^\dagger \cap \mathcal{B}_i = \mathcal{B}_i - p_{i-1}(\mathcal{B}_{i-1}^\dagger)$ . Segue dal Lemma 6.6.4 che  $\text{Span}(\mathcal{B}_i^\dagger)$  è un complementare dell'immagine di  $p_{i-1}$  in  $P(t_i)$ ; in particolare  $\mathcal{B}_i^\dagger$  ha intersezione vuota con l'immagine di  $p_{i-1}$ ; in altri termini, *la base ciclica coincide con il sottoinsieme degli elementi primordiali della base di persistenza.*

Poniamo poi, per ogni  $i < j$ ,

$$\mathcal{B}_{i,j}^\dagger = \{e \in \mathcal{B}_i^\dagger \mid p_{i,j}(e) = 0, p_{i,j-1}(e) \neq 0\},$$

$$\mathcal{B}_{i,\infty}^\dagger = \mathcal{B}_i^\dagger - \cup_j \mathcal{B}_{i,j}^\dagger = \{e \in \mathcal{B}_i^\dagger \mid p_{i,j}(e) \neq 0, \forall j > i\}.$$

Il seguente teorema è quindi conseguenza immediata del Lemma 6.6.4 e del lemma fondamentale dell'omologia persistente.

TEOREMA 6.6.5. *Nelle notazioni della Definizione 6.6.2, per ogni base ciclica  $\mathcal{B}^\dagger$  ed ogni  $i \leq j$  si ha che per ogni intervallo di vita  $[t_i, t_j]$  la molteplicità  $\mu^{i,j}$  è uguale alla cardinalità di  $\mathcal{B}_{i,j}^\dagger$ , ossia al numero di elementi della base di persistenza che nascono in  $t_i$  e muoiono in  $t_j$ .*

*Similmente la molteplicità  $\mu^{i,\infty}$  è uguale alla cardinalità di  $\mathcal{B}_{i,\infty}^\dagger$ .*

COROLLARIO 6.6.6. *Siano  $\mathcal{B}$  ed  $\mathcal{C}$  due basi di persistenza dello stesso modulo di persistenza di tipo finito  $P$ . Allora esiste una bigezione  $f: \mathcal{B} \rightarrow \mathcal{C}$  la cui estensione lineare è un isomorfismo di moduli di persistenza.*

DIMOSTRAZIONE. Per ogni  $i < j \leq +\infty$  gli insiemi  $\mathcal{B}_{i,j}^\dagger$  e  $\mathcal{C}_{i,j}^\dagger$  hanno la stessa cardinalità. Prendiamo una qualunque bigezione  $f: \mathcal{B}^\dagger \rightarrow \mathcal{C}^\dagger$  tale che  $f(\mathcal{B}_{i,j}^\dagger) = \mathcal{C}_{i,j}^\dagger$  per ogni  $i < j \leq +\infty$  ed estendiamo ad una bigezione  $f: \mathcal{B} \rightarrow \mathcal{C}$  ponendo

$$f(p_{i,s}(e)) = p_{i,s}(f(e)), \quad e \in \mathcal{B}_{i,j}, \quad i < s < j \leq +\infty.$$

□

Ogni base ciclica fornisce un rappresentante canonico del diagramma di persistenza:

COROLLARIO 6.6.7. *Sia  $\mathcal{B}^\dagger$  una base ciclica di un modulo di persistenza di tipo finito  $P$ . Allora l'applicazione*

$$v: \mathcal{B}^\dagger \rightarrow S, \quad v(e) = (t_i, t_j) \text{ per } e \in \mathcal{B}_{i,j}^\dagger$$

*rappresenta il diagramma di persistenza  $\text{dgm}(P)$ .*

Grazie alle basi di persistenza possiamo visualizzare graficamente lo snapping lemma; per semplicità espositiva faremo questo solo per le cosiddette  $\epsilon$ -discretizzazioni, lasciando al lettore interessato il compito di estendere al caso generale.

Sia

$$P: \quad P(t_0) \xrightarrow{p_0} P(t_1) \xrightarrow{p_1} P(t_2) \xrightarrow{p_2} \cdots P(t_m)$$

un modulo di persistenza di tipo finito su  $T = \{t_0, \dots, t_m\}$  ed estendiamo a tutto  $\mathbb{R}$  in maniera semicontinua, ossia  $P(s) = P(\max(T \cap ] - \infty, s])$ .

Dati due numeri reali  $\epsilon > 0$ ,  $a \leq t_0$  ed un intero  $n$  tale che  $a + n\epsilon \geq t_m$ , diremo che il modulo di persistenza

$$Q: \quad P(a) \rightarrow P(a + \epsilon) \rightarrow \cdots \rightarrow P(a + n\epsilon)$$

è una  $\epsilon$ -discretizzazione di  $P$ .

LEMMA 6.6.8 (Snapping monodirezionale). *Nelle notazioni precedenti siano  $v: \text{dgm}(P) \rightarrow S$  e  $v: \text{dgm}(Q) \rightarrow S$  i diagrammi di persistenza di  $P, Q$  rispettivamente. Allora un'applicazione **iniettiva**  $\phi: \text{dgm}(Q) \rightarrow \text{dgm}(P)$  tale che:*

(1) *se  $e \in \text{dgm}(Q)$  e  $v(e) = (x, y)$  allora*

$$v(\phi(e)) \in ]x - \epsilon, x] \times ]y - \epsilon, y];$$

(2) *se  $e \in \text{dgm}(Q)$  e  $p(e) = (x, +\infty)$  allora*

$$v(\phi(e)) \in ]x - \epsilon, x] \times \{+\infty\};$$

(3)  *$v(\text{dgm}(P) - \phi(\text{dgm}(Q))) \subset \cup_i ]a + (i-1)\epsilon, a + i\epsilon]^2$ ; in particolare ogni elemento non appartenente all'immagine di  $\phi$  ha un intervallo di vita di ampiezza minore di  $\epsilon$ .*

DIMOSTRAZIONE. Sebbene sia possibile dedurre questa versione dello snapping dalla precedente con argomenti di tipo combinatorio, è istruttivo dare un approccio più diretto. Siccome ogni  $P(a + i\epsilon)$  è del tipo  $P(t_i)$  per qualche  $i$ , ogni base di persistenza  $\mathcal{B}$  di  $P$  determina in maniera univoca una base di persistenza  $\mathcal{C}$  di  $Q$ : se  $t_i \in T$  è il massimo di  $T \cap ] - \infty, a + j\epsilon]$  basta prendere  $\mathcal{C}_j \subset P(a + j\epsilon)$  una copia di  $\mathcal{B}_i$ .

Prendendo gli elementi primordiali in  $\mathcal{B}$  e  $\mathcal{C}$  otteniamo due rappresentazioni due diagrammi di persistenza  $v: \mathcal{B}^\dagger \rightarrow S$  e  $v: \mathcal{C}^\dagger \rightarrow S$ .

Per ogni elemento primordiale  $e \in \mathcal{C}_j^\dagger \subset P(a + j\epsilon)$  esiste un unico elemento primordiale  $\phi(e) \in \mathcal{B}^\dagger$  tale che  $p(\phi(e)) = e$  ( $p$  indica il generico morfismo  $p_s^t$  nell'estensione semicontinua di  $P$ ). Necessariamente  $\phi(e) \in P(t_i)$  per qualche  $t_i \in ]a + (j-1)\epsilon, a + j\epsilon]$ . Inoltre  $e$  muore in

$a + k\epsilon$ , allora  $\phi(e)$  deve morire in un punto dell'intervallo  $]a + (k-1)\epsilon, a + k\epsilon]$ . Ragionamenti simili per le classi che muoiono all'infinito. Per costruzione, l'immagine di  $\phi$  è data da tutti e soli gli elementi di  $\mathcal{B}^\dagger$  il cui intervallo di vita contiene almeno un valore delle serie aritmetica  $a, a + \epsilon, \dots, a + n\epsilon$ .  $\square$

Vediamo adesso ad una versione bidirezionale dello snapping; per semplicità espositiva tratteremo solo il caso di  $\epsilon$ -discretizzazioni, ma il lettore volenteroso può adattare l'argomento ad situazioni più generali.

Consideriamo una serie aritmetica del tipo  $t_i = t_0 + i\epsilon$ ,  $i = 0, \dots, 2n + 1$  ed un modulo di persistenza di tipo finito

$$(6.8) \quad P(t_0) \rightarrow D(t_1) \rightarrow P(t_2) \rightarrow \dots \rightarrow P(2n) \rightarrow D(2n+1)$$

in cui l'ultimo  $P(2n) \rightarrow D(2n+1)$  è un isomorfismo. Siano  $v: \mu_P \rightarrow S$  e  $v: \mu_D \rightarrow S$  i diagrammi di persistenza dei moduli di persistenza "pari"

$$P: \quad P(t_0) \rightarrow P(t_2) \rightarrow \dots \rightarrow P(2n)$$

e "dispari"

$$D: \quad D(t_1) \rightarrow D(t_3) \rightarrow \dots \rightarrow D(2n+1).$$

LEMMA 6.6.9 (Snapping bidirezionale). *Nelle notazioni precedenti esiste un appaiamento parziale*

$$\text{dgm}(P) \supset A \xrightarrow{f \text{ bigettiva}} B \subset \text{dgm}(D)$$

tale che:

- (1) se  $a \in A$  e  $v(a) = (x, y)$  allora  $v(f(a))$  è uno dei 4 valori  $(x \pm \epsilon, y \pm \epsilon)$ ;
- (2) se  $a \in A$  e  $v(a) = (x, +\infty)$  allora  $v(f(a))$  è uno dei 2 valori  $(x \pm \epsilon, +\infty)$ ;
- (3) se  $a \in \text{dgm}(P) - A$  allora  $v_a = (t_{2i}, t_{2i+2})$  per qualche  $i$ ;
- (4) se  $b \in \text{dgm}(D) - B$  allora  $v(b) = (t_{2i+1}, t_{2i+3})$  per qualche  $i$ ;

DIMOSTRAZIONE. Prendiamo una base di persistenza del modulo (6.8); è chiaro che le restrizioni  $\mathcal{B}$  e  $\mathcal{C}$  di tale base ai pari e dispari rispettivamente sono ancora due basi di persistenza di  $P$  e  $D$  rispettivamente.

Denotiamo con la stessa lettera  $p$  tutti i morfismi  $P(t_i) \rightarrow D(t_{i+1})$ ,  $D(t_j) \rightarrow DP(t_{j+1})$  e definiamo

$$T = \{e \in \mathcal{B}^\dagger \mid p(e) \in \mathcal{C}^\dagger\}, \quad R = \{e \in \mathcal{C}^\dagger \mid p(e) \in \mathcal{B}^\dagger\}.$$

Per le proprietà delle basi di persistenza, entrambe le applicazioni  $p: T \rightarrow \mathcal{C}^\dagger$  e  $p: R \rightarrow \mathcal{B}^\dagger$  sono iniettive. Mostriamo che  $T \cap p(R) = \emptyset$ ; infatti, se esistesse  $e = p(u) \in T \cap p(R)$  l'elemento  $p(e) = p^2(u)$  non potrebbe appartenere a  $\mathcal{C}^\dagger$ . Alla stessa maniera si prova  $p(T) \cap R = \emptyset$ .

Dunque abbiamo un appaiamento parziale  $A = T \cup p(R) \xrightarrow{f} p(T) \cup R \subset B$  dove  $f|_T = p$  e  $f|_R^{-1} = p$ .

Per costruzione è chiaro che se  $e \in T$  e  $v(e) = (x, y)$  allora  $v(f(e))$  è uno dei due valori  $(x + \epsilon, y \pm \epsilon)$ , mentre se  $e \in p(R)$  e  $v(e) = (x, y)$  allora  $v(f(e))$  è uno dei due valori  $(x - \epsilon, y \pm \epsilon)$ . Siccome  $P(2n) \simeq D(2n+1)$  per ipotesi, un elemento  $e \in \mathcal{B}$  è immortale in  $P$  se e solo se  $p(e)$  è immortale in  $D$  e questo implica il punto 2).

Se  $e \in \mathcal{B}^\dagger - A$  allora  $p(e) = 0$  e quindi il suo intervallo di vita in  $P$  è del tipo  $[t_{2i}, t_{2i+2}[$ : infatti se fosse  $p(e) \neq 0$  si avrebbe  $p(e) \in \mathcal{C} - \mathcal{C}^\dagger$  e quindi esiste  $u \in \mathcal{C}$  tale che  $p^2(u) = p(e)$  da cui  $p(u) = e$ . Dal fatto che  $e \notin A$  segue che  $u \notin \mathcal{C}^\dagger$ , dunque  $u = p^2(z)$  e  $e = p^2(p(z))$  in contraddizione con il fatto che  $e$  è primordiale. La prova che se  $b \in \text{dgm}(D) - B$  allora  $v(b) = (t_{2i+1}, t_{2i+3})$  per qualche  $i$  è del tutto simile.

Il lettore faccia attenzione che nei punti 3 e 4 non vale il viceversa.  $\square$

**6.6.1. Esistenza delle basi di persistenza.** Dimostriamo adesso l'esistenza di basi cicliche e di persistenza come conseguenza di alcuni risultati di scomposizione in somma diretta, di cui faremo nello studio della stabilità.

Iniziamo con un semplice lemma di algebra lineare.

LEMMA 6.6.10. *Siano  $g: V \rightarrow W$  un'applicazione lineare tra spazi vettoriali,  $v \in V$  tale che  $g(v) \neq 0$  e  $H \subseteq W$  un sottospazio tale che  $W = \text{Span}(g(v)) \oplus H$ . Allora vale*

$$V = \text{Span}(v) \oplus g^{-1}(H), \quad \text{dove} \quad g^{-1}(H) = \{u \in V \mid g(u) \in H\}.$$

DIMOSTRAZIONE. Sia  $x \in V$ , per ipotesi esistono unici  $a \in \mathbb{K}$  e  $h \in H$  tali che  $g(x) = ag(v) + h$ . Ma allora  $x - av \in g^{-1}(H)$  e quindi  $x = av + (x - av) \in \text{Span}(v) + g^{-1}(H)$ . Se  $x \in \text{Span}(v) \cap g^{-1}(H)$ , allora  $x = av$  per qualche  $a \in \mathbb{K}$  e  $g(x) = ag(v) \in H$ . Siccome  $g(v) \notin H$  deve essere  $a = 0$  quindi  $x = av = 0$ ; questo dimostra che  $\text{Span}(v) \cap g^{-1}(H) = 0$ , da cui la tesi.  $\square$

Nei lemmi seguenti indicheremo con

$$P: P(t_0) \xrightarrow{p_0} P(t_1) \xrightarrow{p_1} P(t_2) \xrightarrow{p_2} \cdots P(t_m)$$

un modulo di persistenza di tipo finito di spazi vettoriali.

LEMMA 6.6.11. *Nelle notazioni precedenti si assuma  $P(t_0) \neq 0$  e sia  $0 \leq j \leq m$  il massimo intero tale che  $p_{0,j} \neq 0$ . Allora per ogni  $e \in P(t_0)$  tale che  $p_{0,j}(e) \neq 0$  esiste una decomposizione in somma diretta  $P = E \oplus H$  dove  $E$  è il sottomodulo di persistenza generato dai  $j+1$  vettori  $e, p_{0,1}(e), \dots, p_{0,j}(e)$ .*

DIMOSTRAZIONE. Scegliamo una decomposizione in somma diretta  $P(t_j) = \text{Span}(p_{0,j}(e)) \oplus H_j$ .

Per il Lemma 6.6.10 possiamo trovare, per ogni  $s = 0, \dots, j$ , una decomposizione in somma diretta  $P(t_h) = \text{Span}(p_{0,h}(e)) \oplus H_h$  tale che  $p_h(H_h) \subseteq H_{h+1}$  per ogni  $h < j$ : ad esempio si può prendere, in maniera ricorsiva,  $H_{j-1} = p_{j-1}^{-1}(H_j)$ ,  $H_{j-2} = p_{j-2}^{-1}(H_{j-1})$  e così via. Abbiamo quindi definito due sottomoduli di persistenza

$$H_0 \xrightarrow{p_0} \cdots \longrightarrow H_j \xrightarrow{p_j} P(t_{j+1}) \longrightarrow \cdots \xrightarrow{p_{m-1}} P(t_m),$$

$$\text{Span}(e) \xrightarrow{p_0} \cdots \longrightarrow \text{Span}(p_{0,j}(e)) \xrightarrow{p_j} 0 \longrightarrow \cdots \xrightarrow{p_{m-1}} 0,$$

la cui somma diretta è  $P$ .  $\square$

LEMMA 6.6.12. *Nelle notazioni precedenti si assuma  $P(t_m) \neq 0$  e sia  $0 \leq j \leq m$  il minimo intero tale che  $p_{j,m} \neq 0$ . Allora per ogni  $e \in P(t_j)$  e  $\alpha \in P(t_m)^\vee$  tali che  $\alpha(p_{j,m}(e)) \neq 0$  esiste una decomposizione in somma diretta  $P = E \oplus H$  dove  $E$  è il sottomodulo di persistenza generato dai  $m-j+1$  vettori  $e, p_{j,j+1}(e), \dots, p_{j,m}(e)$  e  $H(t_i) = \ker(\alpha \circ p_{i,m})$  per ogni  $i$ .*

DIMOSTRAZIONE. Consideriamo la decomposizione in somma diretta  $P(t_m) = \text{Span}(p_{j,m}(e)) \oplus \ker(\alpha)$ . Ponendo  $H_i = p_{i,m}^{-1}(\ker(\alpha))$  per ogni  $i$ , si ha  $H_i = P(t_i)$  per  $i < j$  e  $P(t_s) = \text{Span}(p_{j,s}(e)) \oplus H_s$  per  $s \geq j$ . Dunque  $P$  è la somma diretta dei due sottomoduli di persistenza

$$P(t_0) \xrightarrow{p_0} \cdots \longrightarrow P(t_{j-1}) \xrightarrow{p_{j-1}} H_j \longrightarrow \cdots \xrightarrow{p_{m-1}} H_m,$$

$$0 \xrightarrow{p_0} \cdots \longrightarrow 0 \xrightarrow{p_{j-1}} \text{Span}(e) \longrightarrow \cdots \xrightarrow{p_{m-1}} \text{Span}(p_{j,m}(e)).$$

$\square$

TEOREMA 6.6.13. *Ogni modulo di persistenza di tipo finito di spazi vettoriali possiede basi di persistenza e basi cicliche.*

DIMOSTRAZIONE. Nelle notazioni della Definizione 6.6.2 ragioniamo per induzione sulla somma  $\sum_{i=0}^k \dim P(t_i)$  delle dimensioni degli spazi vettoriali. Possiamo usare indifferentemente sia il Lemma 6.6.11 che il Lemma 6.6.12; dovendo sceglierne uno usiamo il primo.

Se  $P(t_i) = 0$  per ogni  $i$  non c'è nulla da dimostrare, altrimenti sia  $i \geq 0$  il più piccolo indice tale che  $P(t_i) \neq 0$ . Sia  $j$  il più grande indice tale che  $p_{i,j} \neq 0$  e scegliamo un vettore  $e \in P(t_i)$  tale che  $p_{i,j}(e) \neq 0$ .

Per il Lemma 6.6.11 esiste una scomposizione in somma diretta di sottomoduli di persistenza  $P = E \oplus H$ , dove  $e$  è una base ciclica di  $E$ . Per induzione  $E$  ed  $H$  possiedono basi

di persistenza (risp.: cicliche) e la loro unione è una base di persistenza (risp.: ciclica) per  $P$ .  $\square$

OSSERVAZIONE 6.6.14. Vi è un'altra dimostrazione, forse meno elegante e più algoritmica, del Teorema 6.6.13 che ha il vantaggio di estendersi, con l'aiuto del lemma di Zorn, ad ogni modulo di persistenza di spazi vettoriali definito su un sottoinsieme bene ordinato di  $\mathbb{R}$ . Diamo una traccia di tale dimostrazione lasciando al lettore interessato il compito di completare i dettagli.

Se  $V$  è uno spazio vettoriale,  $U \subset V$  un sottospazio e  $\mathcal{A} \subset V$  un sottoinsieme, diremo che  $\mathcal{A}$  è una cobase di  $U$  in  $V$  se i vettori di  $\mathcal{A}$  sono linearmente indipendenti e se  $U \oplus \text{Span}(\mathcal{A}) = V$ , ossia se la proiezione di  $\mathcal{A}$  al quoziente  $V/U$  è una base.

Nelle notazioni della Definizione 6.6.2 si consideri la sequenza di istruzioni:

- prendere una cobase  $\mathcal{B}_{0,j}$  di  $\ker(p_{0,j-1})$  in  $\ker(p_{0,j})$  per ogni  $j > 0$ ;
- prendere una cobase  $\mathcal{B}_{0,\infty}$  di  $\ker(p_{0,m})$  in  $P(t_0)$ ;
- estendere  $p_0(\mathcal{B}_{0,j})$  ad una cobase  $\mathcal{B}_{1,j}$  di  $\ker(p_{1,j-1})$  in  $\ker(p_{1,j})$  per ogni  $j > 1$ ;
- estendere  $p_0(\mathcal{B}_{0,\infty})$  ad una cobase  $\mathcal{B}_{1,\infty}$  di  $\ker(p_{1,m})$  in  $P(t_1)$ ;
- estendere  $p_1(\mathcal{B}_{1,j})$  ad una cobase  $\mathcal{B}_{2,j}$  di  $\ker(p_{2,j-1})$  in  $\ker(p_{2,j})$  per ogni  $j > 2$ ;
- estendere  $p_1(\mathcal{B}_{1,\infty})$  ad una cobase  $\mathcal{B}_{2,\infty}$  di  $\ker(p_{2,m})$  in  $P(t_2)$ ;
- eccetera eccetera.

L'unione di tutti i  $\mathcal{B}_{i,j}$  sarà la base di persistenza cercata.

OSSERVAZIONE 6.6.15. Il metodo in assoluto più SNOB, e tuttavia ampiamente usato in letteratura, per dimostrare il Teorema 6.6.13 è quello di usare il teorema di classificazione dei moduli graduati finitamente generati sull'anello ad ideali principali dei polinomi.

### Esercizi:

ESERCIZIO 30. Usare l'esistenza delle basi di persistenza per dimostrare che un modulo di persistenza di tipo finito a valori spazi vettoriali è determinato, a meno di isomorfismo, dalla successione delle molteplicità  $\mu^{i,j}$ .

ESERCIZIO 31. Nelle notazioni di 6.6.2, mostrare che dare una base di persistenza equivale a dare, per ogni  $i = 0, \dots, m$  una base  $\mathcal{B}_i$  di  $P(t_i)$  e  $m - i$  sottoinsiemi  $\mathcal{B}_{i,j} \subset \mathcal{B}_i$ ,  $i < j \leq m$ , tali che:

- (1)  $\cup_{i < s \leq j} \mathcal{B}_{i,s}$  è una base di  $\ker(p_{i,j})$  per ogni  $i < j$ ;
- (2)  $p_i(\mathcal{B}_{i,j}) \subset \mathcal{B}_{i+1,j}$  per ogni  $j > i + 1$ .

## 6.7. Stabilità del diagramma di persistenza

Riepilogando, da un insieme finito di dati (point cloud, grafo pesato ecc.) mediante varie procedure (Vietoris–Rips, complessi di cricche ecc.) si ottiene un complesso filtrato  $(K, f)$  di tipo finito.

I gruppi di omologia permettono di associare al complesso filtrato  $(K, f)$  una successione di moduli di persistenza  $H_n(K(t_\bullet))$ ,  $n \in \mathbb{N}$ , tutti di tipo finito.

Sia  $t_0 < t_1 < \dots$  la successione dei suoi valori critici in ordine crescente (abbiamo già dimostrato che ogni intervallo limitato contiene un numero finito di valori critici). Per ogni intero  $n \geq 0$  fissato, gli  $n$ -esimi gruppi di omologia della catena ascendente dei sottocomplessi di livello  $K(t_0) \subset K(t_1) \subset \dots$  determinano un diagramma di persistenza

$$(6.9) \quad 0 \rightarrow H_n(K(t_0)) \xrightarrow{p_0} H_n(K(t_1)) \xrightarrow{p_1} H_n(K(t_2)) \xrightarrow{p_2} \dots,$$

dove  $p_s$  è il morfismo indotto in omologia dall'inclusione  $K(t_s) \subset K(t_{s+1})$ . Osserviamo inoltre che, essendo per ipotesi  $K(t)$  un complesso simpliciale astratto finito per ogni  $t$ , i gruppi di omologia  $H_n(K(t_i))$  sono finitamente generati.

È chiaro dalle definizioni che un elemento può nascere e morire solo su dei valori critici di  $f$ , pertanto gli estremi degli intervalli di vita sono sempre dei valori critici. In linea teorica per ogni complesso simpliciale filtrato  $(K, f)$  abbiamo una successione infinita di moduli

di persistenza; nella pratica, quasi sempre  $K$  ha dimensione finita e quindi il modulo di persistenza  $H_n(K(t_\bullet))$  è banale per ogni  $n > \dim K$ .

Esiste il problema della stabilità rispetto a piccole perturbazioni. Ad esempio, prendendo una nuvola di punti  $I \subset \mathbb{R}^n$  possiamo ad essa associare il complesso filtrato di Vietoris–Rips  $(K, v)$ ,  $K = \Delta^I$ . Se spostiamo anche di pochissimo i punti di  $I$ , i valori critici di  $v$  cambiano e si ha una diversa filtrazione di sottocomplessi di livello.

Quello che succede, e che tra poco formalizzeremo e dimostreremo, è che a seguito di una piccola perturbazione:

- (1) le classi di omologia persistente che si creano (per effetto della perturbazione) hanno una breve durata di vita;
- (2) le classi di omologia persistente che si distruggono (per effetto della perturbazione) avevano una breve durata di vita;
- (3) ogni classe con intervallo di vita  $[a, b[$  sufficientemente lungo<sup>3</sup> si “trasforma” in una classe con intervallo di vita  $[a', b'[$ , con  $a$  vicino ad  $a'$  e  $b$  vicino ad  $b'$ .

Da ciò traiamo il seguente insegnamento:

1) ha senso interpretare come significativi solo gli intervalli di vita lunghi, mentre quelli corti devono essere considerati “rumore topologico” e quindi non significativi del dato che si vuole interpretare.

2) Abbiamo già dimostrato che nella filtrazione di Vietoris–Rips, piccole perturbazioni del point cloud (nel senso della distanza di Hausdorff) producono piccole perturbazioni del complesso filtrato (nel senso della distanza di contiguità), che a loro volta producono piccole perturbazioni (nel senso della distanza di interfoglia) del modulo di persistenza.

Dimostreremo tra poco (Corollario 6.7.4) che piccole perturbazioni del modulo di persistenza producono piccole perturbazioni del diagramma di persistenza nel senso della distanza bottleneck.

La proprietà che a piccole perturbazioni dei dati devono corrispondere piccole perturbazioni del diagramma di persistenza viene detta **stabilità** ed è l’ingrediente senza il quale quello che abbiamo sviluppato non sarebbe altro che un bell’esercizio intellettuale senza alcuna applicazione pratica. In generale ogni tipo di passaggio dai dati ai complessi filtrati, per avere un qualche interesse applicativo, dovrà soddisfare la condizione di stabilità.

3) Recentemente si intravedono alcune applicazioni dell’omologia persistente anche in ambiti della matematica pura, come ad esempio la geometria algebrica [14]. In tale ambito, più che come spazio metrico, l’insieme dei barcode ci interessa maggiormente come insieme degli oggetti di una categoria tale che il passaggio da complessi filtrati a barcode sia un funtore [1].

Qualora  $S$  sia uno spazio pseudo-metrico, con funzione distanza  $d$ , accessoriatamente con una funzione di rumore  $r$ , possiamo estendere la distanza bottleneck ai multi-insiemi di base  $S$ . Per ogni insieme non vuoto  $X$ , definiamo una pseudo-distanza ed una funzione di rumore sul prodotto  $S \times X$  ponendo

$$d((s_1, x_1), (s_2, x_2)) = d(s_1, s_2), \quad r(s, x) = r(s).$$

Dati due multi-insiemi  $A, B$  di base  $S$ , scegliamo due rappresentazioni polidrome che li rappresentano  $A', B' \subset S \times X$  sullo stesso insieme di indici e definiamo

$$d_b(A, B) = d_b(A', B')$$

dove  $d_b(A', B')$  è la distanza bottleneck definita alla Sezione 5.2. Per vedere che tale definizione non dipende dalla scelta delle rappresentazioni polidrome, siano  $A'', B'' \subset S \times Y$  e  $\alpha: A' \rightarrow A'', \beta: B' \rightarrow B''$  sono due applicazioni bigettive che commutano con le proiezioni su  $S$ ; siccome  $d(\alpha(a), \beta(b)) = d(a, b)$ ,  $r(\alpha(a)) = r(a)$ , e  $r(\beta(b)) = r(b)$ , la ovvia bigezione

<sup>3</sup>Ossia contenente un numero abbastanza alto, in senso statistico, di valori critici.

tra appaiamenti parziali indotta dalla coppia  $\alpha, \beta$  lascia invariati i costi e quindi la distanza bottleneck risulta ben definita.

In particolare, prendendo sul semipiano esteso

$$S = \{(a, b) \mid a \leq b\} \subset (\mathbb{R} \cup \{+\infty\}) \times (\mathbb{R} \cup \{+\infty\})$$

la pseudo-distanza  $d$  e la funzione di rumore  $r$  date da

$$d((a, b), (c, d)) = \max(|a - c|, |b - d|), \quad r(a, b) = \frac{1}{2}(b - a),$$

possiamo definire la distanza bottleneck su qualunque insieme di diagrammi di persistenza. Si noti che

$$r(a, b) = \frac{1}{2}(b - a) = d\left((a, b), \left(\frac{a+b}{2}, \frac{a+b}{2}\right)\right)$$

è la funzione distanza dalla diagonale di  $(\mathbb{R} \cup \{+\infty\})^2$ .

**TEOREMA 6.7.1.** *Sia  $f: P \rightarrow Q$  un morfismo surgettivo di moduli di persistenza di tipo finito su  $T \subset \mathbb{R}$  e sia  $0 < \varepsilon < +\infty$  tale che  $f$  abbia  $\varepsilon$ -kernel. Esiste allora un'applicazione iniettiva*

$$g: \text{dgm}(Q) \rightarrow \text{dgm}(P)$$

tale che:

- (1) gli elementi estranei all'immagine di  $g$  hanno tempo di vita  $\leq \varepsilon$ .
- (2) se  $e \in \text{dgm}(Q)$  e  $v(e) = (a, b)$ , allora  $vg(e) = (a, c)$  con  $b \leq c \leq b + \varepsilon$ .

**DIMOSTRAZIONE.** Prima di procedere, osserviamo che se  $T = \{t_0 < \dots < t_m\}$ , allora l'ipotesi di avere  $\varepsilon$ -kernel implica che  $f: P(t_m) \rightarrow Q(t_m)$  è un isomorfismo e quindi  $x \in P$  è immortale se e solo se  $f(x)$  è immortale.

Ragioniamo per induzione sulla somma delle dimensioni degli spazi vettoriali. Possiamo supporre che  $P(t_0)$  e  $Q(t_0)$  non siano entrambi nulli. Se  $Q(t_0) \neq 0$  allora anche  $P(t_0) \neq 0$ , quindi non è restrittivo supporre  $P(t_0) \neq 0$  ed è ben definito il massimo intero  $j$  tale che  $p_{0,j} \neq 0$ .

Se  $Q(t_0) = 0$  ed  $e \in P(t_0)$  è tale che  $p_{0,j}(e) \neq 0$ , allora  $f(e) = 0$  ed a maggior ragione  $fp_{0,i}(e) = 0$  per ogni  $i$ . Dunque si ha  $P = E \oplus H$  con  $e$  base ciclica di  $E$ . Dunque  $\text{dgm}(P)$  è l'unione disgiunta di  $\text{dgm}(E)$  e  $\text{dgm}(H)$ . Siccome  $E \subset \ker(f)$  l'intervallo di vita di  $e$  ha ampiezza  $\leq \varepsilon$  e la restrizione  $H \rightarrow Q$  è surgettiva. Per induzione esiste  $g: \text{dgm}(Q) \rightarrow \text{dgm}(H)$  che soddisfa le ipotesi del teorema.

Se  $Q(t_0) \neq 0$  sia  $h$  il massimo intero tale che  $q_{0,h} \neq 0$  e siano  $e_1, e_2 \in P(t_0)$  tali che  $p_{0,j}(e_1) \neq 0, fp_{0,h}(e_2) \neq 0$ . Allora per  $e$  uguale ad almeno uno dei tre vettori  $e_1, e_2, e_1 + e_2$  si ha  $p_{0,j}(e) \neq 0, fp_{0,h}(e) = q_{0,h}(f(e)) \neq 0$ .

Dunque si hanno due decomposizioni  $P = E \oplus H, Q = f(E) \oplus K$  dove  $e$  è base ciclica di  $E$  e  $f(e)$  base ciclica di  $f(E)$ . Si ha inoltre un diagramma commutativo di successioni esatte corte

$$\begin{array}{ccccccccc} 0 & \longrightarrow & E & \longrightarrow & P & \longrightarrow & H & \longrightarrow & 0 \\ & & \downarrow f|_E & & \downarrow f & & \downarrow \bar{f} & & \\ 0 & \longrightarrow & f(E) & \longrightarrow & Q & \longrightarrow & K & \longrightarrow & 0 \end{array}$$

Siccome  $f|_E$  è surgettiva, il lemma del serpente implica che  $\bar{f}$  è surgettivo con  $\varepsilon$ -kernel. Al morfismo  $\bar{f}$  si applica l'ipotesi induttiva. D'altra parte  $\text{dgm}(P) = \{e\} \cup \text{dgm}(H)$ ,  $\text{dgm}(Q) = \{f(e)\} \cup \text{dgm}(K)$ ,  $v(e) = (t_0, t_{j+1}), v(f(e)) = (t_0, t_{h+1})$ . Siccome  $p_{0,h+1}(e) \in \ker(f)$  si ha

$$p_{t_0}^{t_{h+1} + \varepsilon} = p_{t_{h+1}}^{t_{h+1} + \varepsilon}(p_{0,h+1}(e)) = 0$$

e questo implica che  $t_{h+1} + \varepsilon \geq t_{j+1}$ , ossia  $t_{h+1} \leq t_{j+1} \leq t_{h+1} + \varepsilon$ .  $\square$

**TEOREMA 6.7.2.** *Sia  $f: P \rightarrow Q$  un morfismo iniettivo di moduli di persistenza di tipo finito su  $T \subset \mathbb{R}$  e sia  $0 < \varepsilon < +\infty$  tale che  $f$  abbia  $\varepsilon$ -cokernel. Esiste allora un'applicazione iniettiva*

$$g: \text{dgm}(P) \rightarrow \text{dgm}(Q)$$

tale che:

- (1) gli elementi in  $\text{dgm}(Q)$  estranei all'immagine di  $g$  hanno tempo di vita  $\leq \varepsilon$ .  
(2) se  $e \in \text{dgm}(P)$  e  $v(e) = (a, b)$ , allora  $vg(e) = (c, b)$  con  $a - \varepsilon \leq c \leq a$ .

DIMOSTRAZIONE. Prima di procedere, osserviamo che se  $T = \{t_0 < \dots < t_m\}$ , allora l'ipotesi di avere  $\varepsilon$ -cokernel implica che  $f: P(t_m) \rightarrow Q(t_m)$  è un isomorfismo e quindi  $x \in P$  è immortale se e solo se  $f(x)$  è immortale.

Ragioniamo per induzione sulla somma delle dimensioni degli spazi vettoriali. Sia  $h \leq m$  il massimo intero per cui  $Q(t_h) \neq 0$  e  $j$  il minimo intero tale che  $q_{j,h} \neq 0$ . Sia  $\alpha \in Q(t_h)^\vee$  tale che  $\alpha q_{j,h} \neq 0$ . Distinguiamo due casi:

1)  $\alpha f(P(t_h)) = 0$ : consideriamo la decomposizione  $Q = E \oplus H$  con  $H(t_i) = \ker(\alpha p_{i,h})$  e osserviamo che  $f(P) \subset H$  ed il morfismo iniettivo  $f: P \rightarrow H$  ha ancora  $\varepsilon$ -cokernel. Inoltre  $\mu_Q = \mu_H \cup \mu_E$  e  $\mu_E$  contiene un solo elemento con tempo di vita  $\leq \varepsilon$ .

2)  $\alpha f(P(t_h)) \neq 0$  e sia  $k$  il più piccolo intero tale che  $p_{k,h} \neq 0$ . Siccome  $f$  è iniettiva esiste  $\beta \in Q(t_h)^\vee$  tale che  $\beta f p_{k,h} \neq 0$ .

A meno di cambiare  $\alpha$  con  $\beta$  oppure con  $\alpha + \beta$ , non è restrittivo assumere  $\alpha q_{j,h} \neq 0$  e  $\alpha f p_{k,h} \neq 0$ . Prendendo  $H(t_i) = \ker(\alpha q_{i,h})$  e  $K(t_i) = \ker(\alpha q_{i,h} f)$  abbiamo  $f: K \rightarrow H$  iniettiva e due decomposizioni in somma diretta  $P = K \oplus U$ ,  $Q = H \oplus E$ , dove  $E, U$  hanno entrambi un generatore ciclico  $e \in Q(t_j)$  e  $u \in P(t_k)$  rispettivamente.

Si ha un diagramma commutativo di successioni esatte corte

$$\begin{array}{ccccccccc} 0 & \longrightarrow & K & \longrightarrow & P & \longrightarrow & U & \longrightarrow & 0 \\ & & \downarrow f|_K & & \downarrow f & & \downarrow \bar{f} & & \\ 0 & \longrightarrow & H & \longrightarrow & Q & \longrightarrow & E & \longrightarrow & 0 \end{array}$$

Siccome  $\bar{f}$  è iniettivo ne segue che anche  $f: K \rightarrow H$  ha  $\varepsilon$ -conucleo e le stesse considerazioni del teorema precedente mostrano che  $t_k - t_j \leq \varepsilon$ .  $\square$

COROLLARIO 6.7.3. Sia  $f: P \rightarrow Q$  un morfismo di moduli di persistenza di tipo finito e sia  $0 < \varepsilon < +\infty$  tale che  $f$  abbia  $\varepsilon$ -kernel e  $\varepsilon$ -cokernel. Allora  $d_B(\text{dgm}(P), \text{dgm}(Q)) \leq \varepsilon$ .

DIMOSTRAZIONE. Sia  $R \subset Q$  l'immagine di  $f$ . Allora  $f: P \rightarrow R$  è surgettivo con  $\varepsilon$ -kernel e  $R \rightarrow Q$  è iniettivo con  $\varepsilon$ -cokernel. Basta adesso applicare i risultati dei due teoremi precedenti per produrre un appaiamento parziale tra  $\text{dgm}(P)$  e  $\text{dgm}(Q)$  il cui costo è  $\leq \varepsilon$ .  $\square$

COROLLARIO 6.7.4. Siano  $P, Q$  due moduli di persistenza di tipo finito. Allora

$$d_B(\text{dgm}(P), \text{dgm}(Q)) \leq 3d_i(P, Q).$$

DIMOSTRAZIONE. Possiamo supporre  $d_i(P, Q) < \infty$  e basta dimostrare che se  $P, Q$  sono  $\varepsilon$ -interfogliati allora  $d_B(\text{dgm}(P), \text{dgm}(Q)) \leq 3\varepsilon$ .

Abbiamo visto che se  $f: P \rightarrow Q[\varepsilon]$  è una componente di una  $\varepsilon$ -interfoglia, allora  $f$  ha  $2\varepsilon$ -kernel e  $2\varepsilon$ -cokernel.

Prendendo come  $T = \{t_0 < \dots < t_m\} \subset \mathbb{R}$  un sottoinsieme finito contenente tutti i valori critici di  $P$  e  $Q[\varepsilon]$  e tale che  $f: P(t_m) \rightarrow Q[\varepsilon](t_m)$  sia un isomorfismo, per il corollario precedente  $d_B(\text{dgm}(P), \text{dgm}(Q[\varepsilon])) \leq 2\varepsilon$ . Per concludere basta osservare che  $\text{dgm}(Q)$  è ottenuto da  $\text{dgm}(Q[\varepsilon])$  componendo con la traslazione in  $S$  di vettore  $(\varepsilon, \varepsilon)$ .  $\square$

Nella dimostrazione del Corollario 6.7.4 abbiamo usato solo una minima parte delle condizioni conseguenti alla  $\varepsilon$ -interfoglia ed è quindi ragionevole attendersi una disuguaglianza migliore tra le distanze bottleneck e interfoglia. Infatti, vale il seguente teorema (non banale) che riportiamo senza dimostrazione.

TEOREMA 6.7.5 (teorema di isometria). Per due moduli di persistenza di tipo finito  $P, Q$  si ha  $d_B(\text{dgm}(P), \text{dgm}(Q)) = d_i(P, Q)$ .

Osserviamo inoltre che non è difficile dare una diversa dimostrazione del Corollario 6.7.4 usando le  $\varepsilon$ -discretizzazioni e gli snapping lemma mono e bidirezionali, vedi ad esempio [16].

## Geometria affine e proiettiva

Indicheremo con  $\mathbb{K}$  un campo fissato e non nullo, ossia con  $1 \neq 0$ . Le figure presentate si riferiscono al caso  $\mathbb{K} = \mathbb{R}$  e sono un valido aiuto alla comprensione dei risultati, non solo su  $\mathbb{R}$  ma anche su campi di caratteristica  $\neq 2$ . Occorre fare attenzione che in caratteristica 2 accadono alcuni fenomeni decisamente controintuitivi (vedi Esempio 7.6.4) e per i quali il disegno potrebbe essere fuorviante.

Per spazio vettoriale intenderemo sempre uno spazio vettoriale di *dimensione finita* su  $\mathbb{K}$ . Per ogni spazio vettoriale  $V$  indicheremo con  $V^\vee$  il suo duale e con  $\text{GL}(V)$  il gruppo di tutti gli endomorfismi lineari di  $V$  invertibili, dotato del prodotto di composizione.

### 7.1. Il teorema di Menelao

Dati tre punti  $p = (p_1, p_2)$ ,  $q = (q_1, q_2)$  e  $r = (r_1, r_2)$  del piano Cartesiano  $\mathbb{R}^2$ , è noto a tutti che si dicono allineati se appartengono ad una medesima retta, ossia se sono contenuti nel sottoinsieme di equazione  $ax + by + c = 0$ , con  $a, b, c$  costanti non tutte nulle.

Dunque, i suddetti  $p, q, r$  sono allineati se e solo se esistono  $a, b, c$  non tutti nulli tali che

$$a \begin{pmatrix} p_1 \\ q_1 \\ r_1 \end{pmatrix} + b \begin{pmatrix} p_2 \\ q_2 \\ r_2 \end{pmatrix} + c \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix},$$

ossia se il rango per righe<sup>1</sup> della matrice

$$\begin{pmatrix} p_1 & q_1 & r_1 \\ p_2 & q_2 & r_2 \\ 1 & 1 & 1 \end{pmatrix}$$

è al più 2. Siccome per ogni matrice il rango per righe è uguale al rango per colonne si ha che  $p, q, r$  sono allineati se e solo se se esistono scalari  $\alpha, \beta, \gamma$  non tutti nulli tali che

$$\alpha \begin{pmatrix} p_1 \\ p_2 \\ 1 \end{pmatrix} + \beta \begin{pmatrix} q_1 \\ q_2 \\ 1 \end{pmatrix} + \gamma \begin{pmatrix} r_1 \\ r_2 \\ 1 \end{pmatrix} = 0$$

ossia se e solo se valgono le equazioni:

$$(7.1) \quad \alpha p + \beta q + \gamma r = 0, \quad \alpha + \beta + \gamma = 0.$$

Notiamo che le equazioni (7.1) hanno perfettamente senso per un qualunque spazio vettoriale su qualunque campo.

**DEFINIZIONE 7.1.1.** Sia  $V$  uno spazio vettoriale su di un campo  $\mathbb{K}$ . Diremo che tre punti  $p, q, r \in V$  sono **allineati** se esistono  $\alpha, \beta, \gamma \in \mathbb{K}$  non tutti nulli tali che

$$\alpha p + \beta q + \gamma r = 0, \quad \alpha + \beta + \gamma = 0.$$

Osserviamo che se i tre punti  $p, q, r$  non sono distinti, allora sono allineati (se ad esempio  $p = q$  basta prendere  $\alpha = 1, \beta = -1$  e  $\gamma = 0$ ).

**LEMMA 7.1.2.** *Siano  $V$  spazio vettoriale e  $p, q, r \in V$  con  $p \neq q$ . Allora  $p, q, r$  sono allineati se e solo se esiste  $t \in \mathbb{K}$  tale che  $r = (1 - t)p + tq$ ; in tal caso  $t$  è unico.*

<sup>1</sup>Ricordiamo che il rango per righe (resp.: colonne) è il massimo numero di righe (resp.: colonne) linearmente indipendenti.

DIMOSTRAZIONE. Per ogni  $p, q \in V$  ed ogni  $t \in \mathbb{K}$  i tre punti  $p, q, r = (1-t)p + tq$  sono allineati poiché  $(1-t) + tq - r = 0$ .

Viceversa, se  $p, q, r$  sono allineati e  $p \neq 0$  esistono  $\alpha, \beta, \gamma \in \mathbb{K}$  non tutti nulli tali che

$$\alpha p + \beta q + \gamma r = 0, \quad \alpha + \beta + \gamma = 0.$$

Se fosse  $\gamma = 0$  si avrebbe  $\alpha = -\beta \neq 0$  da cui  $\alpha(p - q) = 0$  in contraddizione con l'ipotesi  $p \neq q$ . Dunque  $\gamma \neq 0$  e possiamo scrivere

$$r = \frac{-\alpha}{\gamma}p + \frac{-\beta}{\gamma}q.$$

Ponendo  $t = \frac{-\beta}{\gamma}$  si ha

$$\frac{-\alpha}{\gamma} = \frac{\gamma + \beta}{\gamma} = 1 - t$$

e quindi  $r = (1-t)p + tq$ .

Per quanto riguarda l'unicità di  $t$ , se  $r = (1-t)p + tq = (1-s)p + sq$  con  $t, s \in \mathbb{K}$ , facendo la differenza si ottiene

$$0 = (s-t)p + (t-s)q = (t-s)(q-p),$$

da cui  $s = t$ . □

Dunque, per ogni  $p \neq q$  l'applicazione

$$(7.2) \quad f_{p,q}: \mathbb{K} \rightarrow V, \quad f(t) = (1-t)p + tq,$$

induce una bigezione tra il campo  $\mathbb{K}$  e l'insieme dei vettori allineati con  $p, q$ . Si noti che  $f_{p,q}(0) = p$ ,  $f_{p,q}(1) = q$ . Chiameremo l'immagine di  $f_{p,q}$  **retta affine** passante per  $p, q$ , che denoteremo  $\overline{pq}$ .

Per ogni  $r \in \overline{pq}$  definiamo il **rappporto semplice**

$$(r, p, q) = f_{p,q}^{-1}(r).$$

In altri termini, il rapporto semplice si ricava dalle seguenti equivalenze:

$$(r, p, q) = t \iff r = (1-t)p + tq \iff r - p = t(q - p).$$

Il perché del nome rapporto semplice si capisce bene quando  $V = \mathbb{K}^1 = \mathbb{K}$ ; in tal caso si può dividere per  $q - p \in \mathbb{K}$  e quindi  $(r, p, q) = (r - p)/(q - p)$ .

Il rapporto semplice **non** è invariante per permutazioni: se  $p, q, r$  sono distinti e  $(r, p, q) = t$  si ha

$$(7.3) \quad \begin{aligned} (r, p, q) = t, \quad (p, q, r) = \frac{1}{1-t}, \quad (q, r, p) = \frac{t-1}{t}, \\ (p, r, q) = \frac{t}{t-1}, \quad (q, p, r) = \frac{1}{t}, \quad (r, q, p) = 1-t, \end{aligned}$$

dove le precedenti formule (7.3) hanno senso poiché  $t \neq 0$  ( $r \neq p$ ) e  $t \neq 1$  ( $r \neq q$ ). Mostriamo solamente il calcolo di  $(p, q, r)$  lasciando le altre verifiche per esercizio. Se  $(r, p, q) = t$  allora  $r = (1-t)p + tq$  da cui

$$(r, p, q) = t \iff r = (1-t)p + tq \iff p = \frac{t}{t-1}q + \frac{1}{1-t}r \iff (p, q, r) = \frac{1}{1-t}.$$

**TEOREMA 7.1.3** (Teorema di Menelao, prima versione). *Siano dati tre punti  $a, b, c \in V$  non allineati e si considerino tre punti  $c' \in \overline{ab}$ ,  $a' \in \overline{bc}$ ,  $b' \in \overline{ac}$ . Se  $a' \neq b, c$ ,  $b' \neq a, c$  e  $c' \neq a, b$  allora  $a', b', c'$  sono allineati se e solo se*

$$(a, c', b)(b, a', c)(c, b', a) = 1.$$

DIMOSTRAZIONE. Per semplicità notazionale indichiamo

$$(a, c', b) = r, \quad (b, a', c) = s, \quad (c, b', a) = t.$$

Dalle formule (7.3) si ricavano i valori

$$(a', b, c) = \frac{s}{s-1}, \quad (b', a, c) = \frac{1}{1-t}, \quad (c', a, b) = \frac{r}{r-1},$$

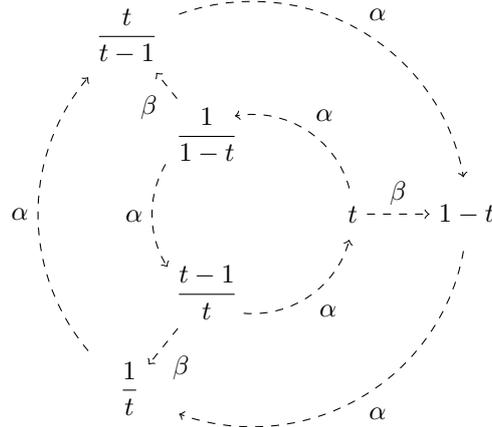


FIGURA 1. Le applicazioni

$$\alpha, \beta: \mathbb{K} - \{0, 1\} \rightarrow \mathbb{K} - \{0, 1\}, \quad \alpha(t) = \frac{1}{1-t}, \quad \beta(t) = 1-t,$$

soddisfano le relazioni  $\alpha^3 = \beta^2 = \text{Id}$ ,  $\alpha\beta = \beta\alpha^2$  e definiscono la rappresentazione del gruppo simmetrico  $\Sigma_3$  determinata dall'azione sui rapporti semplici.

che equivalgono alle uguaglianze

$$(7.4) \quad a' = \frac{1}{1-s}b + \frac{s}{s-1}c, \quad b' = \frac{t}{t-1}a + \frac{1}{1-t}c, \quad c' = \frac{1}{1-r}a + \frac{r}{r-1}b.$$

Si considerino i vettori di  $\mathbb{K}^n \times \mathbb{K}$ :

$$A = \begin{pmatrix} a \\ 1 \end{pmatrix}, \quad B = \begin{pmatrix} b \\ 1 \end{pmatrix}, \quad C = \begin{pmatrix} c \\ 1 \end{pmatrix}, \quad A' = \begin{pmatrix} a' \\ 1 \end{pmatrix}, \quad B' = \begin{pmatrix} b' \\ 1 \end{pmatrix}, \quad C' = \begin{pmatrix} c' \\ 1 \end{pmatrix}.$$

Allora i tre vettori  $A, B, C$  sono linearmente indipendenti e la matrice  $(A, B, C) \in M_{n+1,3}(\mathbb{K})$  ha rango 3. Le uguaglianze in (7.4) forniscono immediatamente le uguaglianze

$$A' = \frac{1}{1-s}B + \frac{s}{s-1}C, \quad B' = \frac{t}{t-1}A + \frac{1}{1-t}C, \quad C' = \frac{1}{1-r}A + \frac{r}{r-1}B$$

che nel formalismo del prodotto righe x colonne si possono scrivere come

$$(A', B', C') = (A, B, C) \begin{pmatrix} 0 & \frac{t}{t-1} & \frac{1}{1-r} \\ \frac{1}{1-s} & 0 & \frac{r}{r-1} \\ \frac{s}{s-1} & \frac{1}{1-t} & 0 \end{pmatrix}.$$

Per il Lemma 7.2.2 i vettori  $A', B', C'$  sono allineati se e solo se la matrice  $(A', B', C')$  ha rango  $< 3$  e questo vale se e solo se la matrice  $3 \times 3$  nella formula precedente ha rango  $< 3$ . Adesso basta calcolare il determinante

$$\begin{vmatrix} 0 & \frac{t}{t-1} & \frac{1}{1-r} \\ \frac{1}{1-s} & 0 & \frac{r}{r-1} \\ \frac{s}{s-1} & \frac{1}{1-t} & 0 \end{vmatrix} = \frac{1-srt}{(1-r)(1-s)(1-t)},$$

che si annulla se e solo se  $srt = 1$  e questo conclude la dimostrazione del teorema.  $\square$

Vediamo adesso l'interpretazione in geometria Euclidea del teorema di Menelao, con i punti  $a, b, c, a', b', c'$  considerati in  $\mathbb{R}^2$ . Per ogni  $p, q \in \mathbb{R}^2$  denotiamo con  $|pq| = \|p - q\|$  la

distanza Euclidea e osserviamo che se  $p, q, r$  sono allineati e distinti, allora

$$(p, r, q) = \pm \frac{|pr|}{|qr|}$$

dove il segno  $-$  vale se e solo se  $r$  è compreso tra  $p$  e  $q$ , ossia se  $r$  appartiene al segmento di estremi  $p, q$ . Infatti  $(p, r, q) = t \in \mathbb{R}$  se e solo se  $p = (1-t)r + tq$  se e solo se  $p-r = t(q-r)$  da cui  $|t| = \frac{\|p-r\|}{\|q-r\|}$ . Sempre dalla formula  $p-r = t(q-r)$  segue che  $t$  è negativo se e solo se i vettori  $p-r$  e  $q-r$  hanno direzioni opposte, ossia se e solo se  $r$  è compreso tra  $p, q$ .

Se  $a', b', c'$  sono allineati, prendendo i valori assoluti dei rapporti semplici nella formula del Teorema 7.1.3 si ottiene

$$(7.5) \quad \frac{|ac'|}{|bc'|} \frac{|ba'|}{|ca'|} \frac{|cb'|}{|ab'|} = 1.$$

mentre dall'analisi dei segni segue che il numero dei punti  $a', b', c'$  appartenenti ai lati del triangolo è pari.

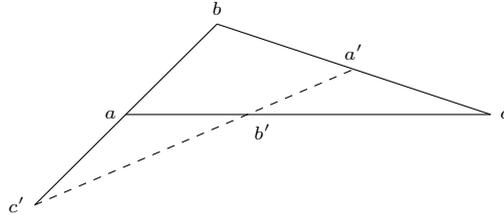


FIGURA 2. Il teorema di Menelao.

Viceversa, se vale (7.5) ed un numero pari di punti  $a', b', c'$  appartiene al perimetro del triangolo allora  $(a, c', b)(b, a', c)(c, b', a) = 1$  e tali punti risultano allineati.

Esiste una versione alternativa del Teorema di Menelao, molto celebre nella grafica computerizzata, e nel cui enunciato intervengono alcune generalizzazioni delle funzioni  $f_{p,q}(t) = (1-t)p + tq$  introdotte in (7.2).

**TEOREMA 7.1.4 (Menelao, seconda versione).** *Per ogni terna di punti  $p, q, r \in V$  si consideri l'applicazione*

$$f_{p,q,r}: \mathbb{K}^2 \rightarrow V, \quad f_{p,q,r}(t, s) = (1-s)f_{p,q}(t) + sf_{q,r}(t).$$

Allora  $f_{p,q,r}(t, s) = f_{p,q,r}(s, t)$  per ogni  $s, t \in \mathbb{K}$ .

La dimostrazione è banale, mentre tutt'altro che evidente è la relazione tra le due versioni del teorema di Menelao. Infatti, sviluppando i conti si ha

$$f_{p,q,r}(t, s) = (1-s)(1-t)p + (1-s)tq + s(1-t)q + str = (1-s)(1-t)p + (s+t-2st)q + str$$

che risulta simmetrica nelle variabili  $s, t$ .

Qui mostriamo solamente come la seconda versione segue dalla prima. Si considerino tre punti non allineati  $p, q, r$ , due scalari  $t, s \in \mathbb{K}$  e si guardi alla Figura 3

Il Teorema 7.1.3 applicato ai triangoli di vertici  $f_{p,q}(s), q, f_{q,r}(s)$  e  $f_{p,q}(t), q, f_{q,r}(t)$  rispettivamente ci dà le due uguaglianze:

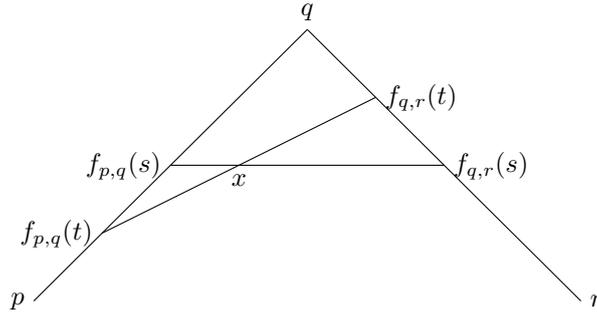
$$(f_{p,q}(s), f_{p,q}(t), q)(q, f_{q,r}(t), f_{q,r}(s))(f_{q,r}(s), x, f_{p,q}(s)) = 1,$$

$$(f_{p,q}(t), f_{p,q}(s), q)(q, f_{q,r}(s), f_{q,r}(t))(f_{q,r}(t), x, f_{p,q}(t)) = 1.$$

I quattro rapporti semplici dove non compare  $x$  si calcolano facilmente in funzione di  $s, t$ :

$$(f_{p,q}(s), f_{p,q}(t), q) = \frac{s-t}{1-t}, \quad (f_{p,q}(t), f_{p,q}(s), q) = \frac{t-s}{1-s},$$

$$(q, f_{q,r}(t), f_{q,r}(s)) = \frac{t}{t-s}, \quad (q, f_{q,r}(s), f_{q,r}(t)) = \frac{s}{s-t}$$

FIGURA 3. Il punto  $x = f_{p,q,r}(t, s) = f_{p,q,r}(s, t)$  per  $s \neq t$ .

da cui segue

$$(f_{q,r}(s), x, f_{p,q}(s)) = \frac{(1-t)(t-s)}{(s-t)t} = \frac{t-1}{t} \iff (x, f_{p,q}(s), f_{q,r}(s)) = t \iff x = f_{p,q,r}(s, t),$$

$$(f_{q,r}(t), x, f_{p,q}(t)) = \frac{(1-s)(s-t)}{(t-s)s} = \frac{s-s}{t} \iff (x, f_{p,q}(t), f_{q,r}(t)) = s \iff x = f_{p,q,r}(t, s).$$

### Esercizi

ESERCIZIO 32. Nella notazioni del Teorema 7.1.4, e per  $\mathbb{K} = \mathbb{R}$ , mostrare che  $t \mapsto \gamma(t) = f_{p,q,r}(t, t)$  è una parametrizzazione della parabola passante per  $p, r$  e con derivate  $\gamma'(p) = q - p$ ,  $\gamma'(r) = r - q$ .

## 7.2. Indipendenza affine e combinazioni baricentriche

Quando si passa da 3 a più punti in uno spazio vettoriale  $V$ , esistono due modi naturali di estendere la Definizione 7.1.1. Nel primo di questi, diremo che  $p_0, \dots, p_n \in V$  sono allineati se appartengono tutti ad una medesima retta affine: equivalentemente, se ogni terna  $p_{i_1}, p_{i_2}, p_{i_3}$  è allineata.

DEFINIZIONE 7.2.1. Sia  $V$  uno spazio vettoriale su  $\mathbb{K}$ . Dati  $p+1$  vettori  $v_0, \dots, v_p \in V$ , si dicono **affinamente dipendenti** se esistono  $a_0, \dots, a_p \in \mathbb{K}$ , non tutti nulli, e tali che:

$$a_0 v_0 + \dots + a_p v_p = 0, \quad a_0 + \dots + a_p = 0.$$

I medesimi vettori si dicono **affinamente indipendenti** se non sono affinamente dipendenti.

È chiaro che se  $v_0, \dots, v_p$  sono affinamente dipendenti, allora sono anche linearmente dipendenti. Il viceversa non è vero in generale, ad esempio tre vettori in  $\mathbb{K}^2$  sono sempre linearmente dipendenti ma sono affinamente dipendenti se e solo se sono allineati.

LEMMA 7.2.2. Sia  $V$  uno spazio vettoriale su  $\mathbb{K}$ . Dati  $v_0, \dots, v_p \in V$  le seguenti condizioni sono equivalenti:

- (1)  $i$   $p+1$  vettori  $v_0, \dots, v_p \in V$  sono affinamente dipendenti;
- (2)  $i$   $p+1$  vettori  $(v_0, 1), \dots, (v_p, 1) \in V \times \mathbb{K}$  sono linearmente dipendenti;
- (3) esiste un indice  $i = 0, \dots, p$  tale che  $i$   $p$  vettori  $v_j - v_i$ ,  $j \neq i$ , sono linearmente dipendenti;
- (4) per ogni  $i = 0, \dots, p$   $i$   $p$  vettori  $v_j - v_i$ ,  $j \neq i$ , sono linearmente dipendenti.

DIMOSTRAZIONE. L'equivalenza tra le prime due condizioni, già osservata nel caso  $p = 2$ , si generalizza immediatamente al caso  $p > 2$ , dato che l'equazione

$$\sum_{i=0}^p a_i (v_i, 1) = 0, \quad a_i \in \mathbb{K},$$

è del tutto equivalente al sistema di due equazioni

$$\sum_{i=0}^p a_i v_i = 0, \quad \sum_{i=0}^p a_i = 0, \quad a_i \in \mathbb{K}.$$

Mostriamo che (3) implica (1). Per semplicità supponiamo  $i = 0$  (per  $i \neq 0$  la dimostrazione è sostanzialmente identica). Siano  $a_1, \dots, a_p \in \mathbb{K}$  non tutti nulli e tali che  $\sum_{j=1}^p a_j (v_j - v_0) = 0$ . Se poniamo  $a_0 = -\sum_{j=1}^p a_j$  si ha

$$\sum_{j=0}^p a_j v_j = \sum_{j=1}^p a_j v_j - \sum_{j=1}^p a_j v_0 = \sum_{j=1}^p a_j (v_j - v_0) = 0.$$

Mostriamo adesso che (1) implica (4). Sia  $i$  un indice fissato e siano  $a_0, \dots, a_p \in \mathbb{K}$  non tutti nulli e tali che  $\sum a_j v_j = 0$ . Siccome  $a_i = -\sum_{j \neq i} a_j$  esiste almeno un indice  $j \neq i$  tale che  $a_j \neq 0$  e si ha la relazione di dipendenza lineare

$$\sum_{j \neq i} a_j (v_j - v_i) = \sum_{j \neq i} a_j v_j - \left( \sum_{j \neq i} a_j \right) v_i = \sum_{j=0}^p a_j v_j = 0.$$

□

Da notare che: il massimo numero di vettori affinemente indipendenti in  $\mathbb{K}^n$  è  $n+1$ ; ogni vettore (anche nullo) è affinemente indipendente; due vettori sono affinemente indipendenti se e solo se sono distinti.

Sia  $V$  uno spazio vettoriale sul campo  $\mathbb{K}$ . Una combinazione lineare  $a_0 v_0 + \dots + a_n v_n$  di vettori  $v_i \in V$  e coefficienti  $a_i \in \mathbb{K}$  si dice una **combinazione baricentrica**<sup>2</sup> se  $\sum a_i = 1$ .

LEMMA 7.2.3. *Finiti vettori in uno spazio vettoriale sono affinemente indipendenti se e solo se nessuno di essi può essere scritto come combinazione baricentrica dei rimanenti.*

DIMOSTRAZIONE. Siano  $v_0, \dots, v_n$  vettori nello spazio vettoriale  $V$ . Se sono affinemente dipendenti allora esistono  $a_0, \dots, a_n \in \mathbb{K}$  non tutti nulli tali che

$$\sum_i a_i v_i = 0, \quad \sum_i a_i = 0.$$

Se  $j$  è un indice per cui  $a_j \neq 0$  si ha

$$v_j = \sum_{i \neq j} \frac{-a_i}{a_j} v_i, \quad \sum_{i \neq j} \frac{-a_i}{a_j} = \frac{1}{a_j} \sum_{i \neq j} -a_i = \frac{a_j}{a_j} = 1,$$

e quindi  $v_j$  è combinazione baricentrica dei rimanenti vettori. Viceversa se per un qualche indice  $j$  si ha

$$v_j = \sum_{i \neq j} b_i v_i, \quad \sum_{j \neq i} b_i = 1,$$

ponendo  $b_j = -1$  si ha

$$\sum_i b_i v_i = 0, \quad \sum_i b_i = 0,$$

e quindi i vettori  $v_i$  sono affinemente dipendenti. □

Un sottoinsieme di  $V$  si dice un **sottospazio affine** se è chiuso per combinazioni baricentriche. In altri termini, un sottoinsieme  $H \subset V$  è un sottospazio affine se per ogni successione finita  $v_0, \dots, v_n \in H$  ed ogni successione  $a_0, \dots, a_n \in \mathbb{K}$  tale che  $\sum a_i = 1$  si ha  $a_0 v_0 + \dots + a_n v_n \in H$ .

- ESEMPIO 7.2.4. (1) il vuoto è un sottospazio affine;  
 (2) per ogni  $v \in V$ , il sottoinsieme  $\{v\}$  è un sottospazio affine;  
 (3) ogni sottospazio vettoriale è anche un sottospazio affine;  
 (4) intersezione di una famiglia arbitraria di sottospazi affini è ancora un sottospazio affine;

<sup>2</sup>Qui purtroppo non esiste una terminologia standard in letteratura: le combinazioni baricentriche vengono chiamate *combinazioni affini* da alcuni autori e *centroidi* da altri.

(5) Il sottoinsieme di  $\mathbb{K}^n$  formato dalle soluzioni  $(x_1, \dots, x_n)^T$  di un sistema lineare

$$\begin{cases} a_{11}x_1 + \dots + a_{1n}x_n = b_1 \\ \vdots \\ a_{m1}x_1 + \dots + a_{mn}x_n = b_m \end{cases}$$

è un sottospazio affine;

(6) Se  $H \subseteq V$  e  $K \subseteq W$  sono sottospazi affini, il loro prodotto cartesiano  $H \times K$  è un sottospazio affine di  $V \times W$ .

LEMMA 7.2.5. *Siano  $V$  uno spazio vettoriale e  $H \subset V$  un sottospazio affine che non contiene il vettore nullo. Allora  $n+1$  vettori  $v_0, \dots, v_n \in H$  sono affinementemente indipendenti se e solo se sono linearmente indipendenti in  $V$ .*

DIMOSTRAZIONE. Una implicazione è chiara: se  $v_0, \dots, v_n$  sono linearmente indipendenti, a maggior ragione sono affinementemente indipendenti.

Supponiamo viceversa che i vettori  $v_i$  siano linearmente dipendenti, ossia che si abbia una combinazione lineare  $\sum_{i=0}^n a_i v_i = 0$ , con gli  $a_i \in \mathbb{K}$  non tutti nulli e denotiamo  $a = \sum_{i=0}^n a_i$ . Se  $a \neq 0$  allora

$$\sum_{i=0}^n \frac{a_i}{a} = 1, \quad \sum_{i=0}^n \frac{a_i}{a} v_i = 0,$$

in contraddizione con l'ipotesi  $0 \notin H$ . Dunque  $a = 0$  e di conseguenza i vettori  $v_i$  sono affinementemente dipendenti.  $\square$

DEFINIZIONE 7.2.6 (Inviluppo affine). Per ogni insieme finito di vettori  $v_0, \dots, v_n$ , l'insieme

$$\langle\langle v_0, \dots, v_n \rangle\rangle = \{a_0 v_0 + \dots + a_n v_n \mid a_i \in \mathbb{K}, \sum a_i = 1\}$$

di tutte le combinazioni baricentriche viene detto **inviluppo affine** di  $v_0, \dots, v_n$ .

Ogni inviluppo affine è un sottospazio affine. Infatti dati  $w_0, \dots, w_m \in \langle\langle v_0, \dots, v_n \rangle\rangle$  per definizione esiste una matrice  $a_{ij}$ ,  $i = 0, \dots, n$ ,  $j = 0, \dots, m$  tale che

$$w_j = \sum_{i=0}^n a_{ij} v_i, \quad \sum_{i=0}^n a_{ij} = 1, \quad \text{per ogni } j = 0, \dots, m.$$

Allora per ogni  $b_0, \dots, b_m \in \mathbb{K}$  tali che  $\sum b_j = 1$  si ha

$$\sum_j b_j w_j = \sum_{i,j} a_{ij} b_j v_i = \sum_i c_i v_i, \quad c_i = \sum_j b_j a_{ij},$$

e siccome

$$\sum_i c_i = \sum_i \sum_j b_j a_{ij} = \sum_j b_j \sum_i a_{ij} = \sum_j b_j \cdot 1 = 1$$

ne consegue che  $\sum_j b_j w_j \in \langle\langle v_0, \dots, v_n \rangle\rangle$ .

Segue immediatamente dalle definizioni che se  $H$  è un sottospazio affine di uno spazio vettoriale e  $v_0, \dots, v_n \in H$ , allora  $\langle\langle v_0, \dots, v_n \rangle\rangle \subset H$ . Ne segue che l'inviluppo affine  $\langle\langle v_0, \dots, v_n \rangle\rangle$  coincide con l'intersezione dei sottospazi affini contenenti  $v_0, \dots, v_n$ .

LEMMA 7.2.7. *Siano  $v_0, \dots, v_n$  vettori affinementemente indipendenti in uno spazio vettoriale  $V$ . Per un vettore  $w \in V$  le seguenti condizioni sono equivalenti:*

- (1)  $w \in \langle\langle v_0, \dots, v_n \rangle\rangle$ ;
- (2)  $v_0, \dots, v_n, w$  sono affinementemente dipendenti.

DIMOSTRAZIONE. Una implicazione segue immediatamente dal Lemma 7.2.3: se  $w \in \langle\langle v_0, \dots, v_n \rangle\rangle$  allora  $w$  è combinazione baricentrica di  $v_0, \dots, v_n$  e quindi  $v_0, \dots, v_n, w$  sono affinementemente dipendenti.

Viceversa, se  $v_0, \dots, v_n, w$  sono affinementemente dipendenti si hanno due relazioni

$$aw + \sum_{i=0}^n a_i v_i = 0, \quad a + \sum_{i=0}^n a_i = 0,$$

con i coefficienti  $a, a_0, \dots, a_n$  non tutti nulli.

Se fosse  $a = 0$  allora anche i vettori  $v_0, \dots, v_n$  sarebbero affinementemente dipendenti, quindi  $a \neq 0$  ed allora

$$1 = \frac{a}{a} = - \sum_{i=0}^n \frac{a_i}{a}, \quad w = - \sum_{i=0}^n \frac{a_i}{a} v_i \in \langle\langle v_0, \dots, v_n \rangle\rangle.$$

□

LEMMA 7.2.8. *Sia  $K$  un sottospazio affine di uno spazio vettoriale  $V$ . Allora per ogni vettore  $u \in V$  il sottoinsieme*

$$u + K := \{u + x \mid x \in K\}$$

*è ancora un sottospazio affine detto il **traslato di  $K$  tramite  $u$** .*

DIMOSTRAZIONE. Dati  $v_0, \dots, v_n \in u + K$  e  $a_0, \dots, a_n \in \mathbb{K}$  tali che  $\sum a_i = 1$ , per definizione  $v_i = u + x_i$  con  $x_i = v_i - u \in K$  e quindi

$$\sum a_i v_i = \sum a_i (u + x_i) = (\sum a_i) u + \sum a_i x_i = u + \sum a_i x_i \in u + K.$$

□

LEMMA 7.2.9. *Sia  $K$  un sottospazio affine non vuoto di uno spazio vettoriale  $V$ . Allora il sottoinsieme  $W = \{u - v \mid u, v \in K\} \subset V$  è un sottospazio vettoriale ed è l'unico sottospazio vettoriale che risulta essere un traslato di  $K$ . In particolare  $K$  è un sottospazio vettoriale se e solo se  $0 \in K$ .*

DIMOSTRAZIONE. Siccome  $K$  è non vuoto, pure  $W$  è non vuoto. Dati  $u, v, x, y \in K$  e  $a, b \in \mathbb{K}$  si ha

$$a(u - v) + b(x - y) = u - ((1 - a)u + av - bx + by) \in W,$$

poiché  $(1 - a) + a - b + b = 1$  e quindi  $(1 - a)u + av - bx + by \in K$ . Abbiamo provato che  $W$  è chiuso per combinazioni lineari di due vettori e dunque che è un sottospazio vettoriale.

Proviamo adesso che  $K$  è un traslato di  $W$ . Sia  $u \in K$  un elemento qualsiasi e mostriamo che  $K = u + W$ ; se  $v \in K$  allora  $v - u \in W$  e quindi  $v = u + (v - u) \in u + W$ . Viceversa, se  $w \in W$  allora  $w = x - y$  con  $x, y \in K$  e quindi  $u + w = u + x - y \in K$  poiché  $1 + 1 - 1 = 1$ .

Per finire, mostriamo che se  $K$  è un traslato di un sottospazio vettoriale  $U$ , allora  $U = W$ . Se  $U = v + W$  allora  $0 \in v + W$ , ossia  $-v \in W$ , quindi  $v \in W$  e di conseguenza  $v + W = W$ . □

Secondo il Lemma 7.2.9, per ogni sottospazio affine non vuoto  $K \subset V$  esiste un unico sottospazio vettoriale  $W$  che è un traslato di  $K$ . Chiameremo  $W$  **spazio tangente** di  $K$  in  $V$  e si definisce la **dimensione di  $K$**  come la dimensione di  $W$  come spazio vettoriale. Se  $K = \emptyset$  allora si pone per convenzione  $\dim K = -1$ .

### Esercizi

ESERCIZIO 33. Sia  $E$  un sottoinsieme di uno spazio vettoriale su di un campo diverso da  $\mathbb{Z}/2$ . Provare che  $E$  è un sottospazio affine se e solo se per ogni  $u, v \in E$  e per ogni  $a \in \mathbb{K}$  vale  $au + (1 - a)v \in E$ .

ESERCIZIO 34. Sia  $E$  un sottoinsieme di uno spazio vettoriale sul campo  $\mathbb{Z}/2$ . Provare che  $E$  è un sottospazio affine se e solo se per ogni  $u, v, w \in E$  vale  $u + v + w \in E$ .

ESERCIZIO 35. Dedurre dagli esercizi precedenti che un sottoinsieme  $E$  di uno spazio vettoriale è un sottospazio affine se e solo se per ogni  $u, v, w \in E$  ed ogni  $a, b, c \in \mathbb{K}$  tali che  $a + b + c = 1$  vale  $au + bv + cw \in E$ .

ESERCIZIO 36. Sia  $V$  uno spazio vettoriale su di un campo  $F$ . Provare che se  $F$  possiede almeno  $n + 1$  elementi, allora  $V$  non può essere unione di  $n$  sottospazi affini propri. In particolare uno spazio vettoriale su di un campo infinito non può essere unione finita di sottospazi affini propri. (Sugg.: induzione su  $n$ ; sia per assurdo  $V = \cup_{i=1}^n V_i$ , allora a meno di traslazioni possiamo supporre  $0 \in V_n$ . Se  $V_n \subset V_i$  per qualche  $i < n$  abbiamo finito, altrimenti scegliamo  $v \in V_n - \cup_{i=1}^{n-1} (V_n \cap V_i)$ ,  $h \in V - V_n$  e consideriamo la retta affine

$L = \{tv + (1-t)h \mid t \in F\}$ . Esiste allora un indice  $i$  tale che  $L$  interseca  $V_i$  in almeno due punti.)

### 7.3. Spazi e applicazioni affini

Per **spazio affine** su di un campo  $\mathbb{K}$  intenderemo un sottospazio affine di uno spazio vettoriale sul medesimo campo. Per semplicità espositiva consideriamo esclusivamente spazi affini di dimensione finita, definiti come sottospazi affini di spazi vettoriali di dimensione finita.

Per rimarcare la differenza chiameremo **punti** (anziché vettori) gli elementi di uno spazio affine; al di là della questione terminologica uno spazio affine può anche essere pensato come uno spazio vettoriale in cui il vettore nullo è un vettore come tutti gli altri ed in cui le uniche combinazioni lineari consentite sono quelle baricentriche.

I punti sono tutti e soli i sottospazi affini di dimensione 0: sottospazi affini di dimensione 1 e 2 sono detti rispettivamente rette e piani affini.

Per il Lemma 7.2.3 possiamo caratterizzare la dipendenza affine di punti in uno spazio affine  $H$  esclusivamente in termini di combinazioni baricentriche. In altri termini, la seguente definizione non porta a contraddizioni con le precedenti.

**DEFINIZIONE 7.3.1.** Finiti punti in uno spazio affine si dicono **affinemente indipendenti** se nessuno di essi può essere scritto come combinazione baricentrica dei rimanenti.

Conseguentemente, possiamo caratterizzare la dimensione di uno spazio affine usando esclusivamente le combinazioni baricentriche.

**TEOREMA 7.3.2.** Sia  $n$  la dimensione di uno spazio affine  $H$ . Allora il massimo numero di punti di  $H$  affinemente indipendenti è uguale a  $n + 1$ .

**DIMOSTRAZIONE.** Rappresentiamo  $H$  come un sottospazio affine dello spazio vettoriale  $V$  e sia  $W \subset V$  il suo spazio tangente, ossia l'unico sottospazio vettoriale traslato di  $H$ . Per definizione di dimensione si ha  $\dim W = n$ .

Se  $v_0, \dots, v_m \in H$  sono affinemente indipendenti, allora i vettori  $v_i - v_0 \in W$ ,  $i = 1, \dots, m$ , sono linearmente indipendenti e quindi  $m \leq n$ . Viceversa se  $w_1, \dots, w_n \in W$  sono una base, allora per un qualunque elemento  $v_0 \in K$  i vettori  $v_0, v_0 + w_1, \dots, v_0 + w_n$  sono affinemente indipendenti.  $\square$

**DEFINIZIONE 7.3.3.** Un'applicazione  $f: H \rightarrow K$  tra spazi affini si dice **affine** se commuta con le combinazioni baricentriche, cioè se per ogni  $v_0, \dots, v_n \in H$  e per ogni  $a_0, \dots, a_n \in \mathbb{K}$  tali che  $\sum a_i = 1$  vale  $f(\sum a_i v_i) = \sum a_i f(v_i)$ . Le applicazioni affini invertibili (ossia bigettive) vengono dette **isomorfismi affini**.

È chiaro che composizione di applicazioni affini è ancora affine. Segue dal Teorema 7.3.2 che la dimensione di uno spazio affine è invariante per isomorfismi affini.

**ESEMPIO 7.3.4.** Ogni applicazione lineare tra spazi vettoriali è anche affine.

**ESEMPIO 7.3.5.** Siano  $V$  uno spazio vettoriale e  $v \in V$ . Allora la **traslazione**

$$T_v: V \rightarrow V, \quad T_v(x) = v + x,$$

è un'affinità con inversa  $T_{-v}$ . Infatti se  $\sum a_i = 1$  si ha

$$T_v(\sum a_i x_i) = v + \sum a_i x_i = (\sum a_i)v + \sum a_i x_i = \sum a_i(v + x_i) = \sum a_i T_v(x_i).$$

**LEMMA 7.3.6.** Sia  $f: V \rightarrow W$  un'applicazione affine tra spazi vettoriali. Allora esiste un'applicazione lineare  $g: V \rightarrow W$  tale che  $f = T_{f(0)}g$ . In particolare  $f$  è lineare se e solo se  $f(0) = 0$ .

**DIMOSTRAZIONE.** Già sappiamo che se  $f$  è lineare allora  $f(0) = 0$ . Viceversa, se  $f(0) = 0$  allora per ogni  $u, v \in V$  ed ogni  $a, b \in \mathbb{K}$  si ha

$$f(au + bv) = f((1-a-b)0 + au + bv) = (1-a-b)f(0) + af(u) + bf(v) = af(u) + bf(v)$$

e quindi  $f$  è lineare. Dunque l'applicazione affine  $g = T_{-f(0)}f$  è lineare in quanto  $g(0) = T_{-f(0)}(f(0)) = 0$ .  $\square$

In generale, se  $f: V \rightarrow W$  è un'applicazione affine tra spazi vettoriali non è detto che si possa scrivere  $f = gT_v$  per opportuni  $v \in V$  e  $g$  lineare. Una condizione necessaria è che  $0 = gT_v(-v)$  appartenga all'immagine di  $f$ ; tale condizione è anche sufficiente in quanto se esiste  $v \in V$  tale che  $f(-v) = 0$ , allora l'applicazione  $g = fT_{-v}$  risulta lineare in quanto  $g(0) = 0$ .

**TEOREMA 7.3.7.** *Siano  $\mathbb{K}$  un campo con almeno tre elementi (ossia  $\mathbb{K} \neq \mathbb{Z}/(2)$ ) e  $f: H \rightarrow K$  un'applicazione tra due spazi affini definiti su  $\mathbb{K}$ . Allora  $f$  è affine se e solo se per ogni  $p, q \in H$  ed ogni  $t \in \mathbb{K}$  vale*

$$f((1-t)p + tq) = (1-t)f(p) + tf(q).$$

In altri termini  $f$  è affine se e solo se preserva gli allineamenti ed i rapporti semplici.

**DIMOSTRAZIONE.** La condizione è chiaramente necessaria. Per quanto riguarda la sufficienza dimostriamo per induzione su  $n \geq 1$  che

$$(7.6) \quad f\left(\sum_{i=0}^n t_i p_i\right) = \sum_{i=0}^n t_i f(p_i), \quad p_i \in H, \quad t_i \in \mathbb{K}, \quad \sum t_i = 1.$$

Per  $n = 1$  la (7.6) è vera per ipotesi; supponiamo quindi  $n > 1$  e scegliamo un  $b \in \mathbb{K} - \{0, 1\}$ . Si può scrivere

$$\sum_{i=0}^n t_i p_i = (1-b) \left( \frac{t_0}{1-b} p_0 + \frac{1-b-t_0}{1-b} p_1 \right) + b \left( \frac{t_0+t_1+b-1}{b} p_1 + \sum_{i=2}^n \frac{t_i}{b} p_i \right)$$

e per l'ipotesi induttiva

$$\begin{aligned} f\left(\sum_{i=0}^n t_i p_i\right) &= (1-b)f\left(\frac{t_0}{1-b} p_0 + \frac{1-b-t_0}{1-b} p_1\right) + bf\left(\frac{t_0+t_1+b-1}{b} p_1 + \sum_{i=2}^n \frac{t_i}{b} p_i\right) \\ &= (1-b)\left(\frac{t_0}{1-b} f(p_0) + \frac{1-b-t_0}{1-b} f(p_1)\right) + b\left(\frac{t_0+t_1+b-1}{b} f(p_1) + \sum_{i=2}^n \frac{t_i}{b} f(p_i)\right) \\ &= \sum_{i=0}^n t_i f(p_i). \end{aligned}$$

□

**PROPOSIZIONE 7.3.8.** *Siano  $V$  uno spazio vettoriale di dimensione  $n+1$  e  $H \subset V$  un sottospazio affine di dimensione  $n$  che non contiene il vettore nullo. Allora per ogni applicazione affine  $f: H \rightarrow H$  esiste unica un'applicazione lineare  $g: V \rightarrow V$  tale che  $g|_H = f$ .*

**DIMOSTRAZIONE.** Sia  $W \subset V$  lo spazio tangente di  $H$ . Scegliamo un vettore  $v_0 \in H$ , allora  $H = v_0 + W$  e  $v_0 \notin W$ , altrimenti si avrebbe  $-v_0 \in W$  e quindi  $0 = v_0 - v_0 \in H$  contrariamente alle ipotesi. Sia  $v_1, \dots, v_n$  una base di  $W$ , allora  $v_0, v_1, \dots, v_n$  è una base di  $V$  e  $v_0, v_0 + v_1, \dots, v_0 + v_n \in H$ .

Se  $g: V \rightarrow V$  è lineare che estende  $f$ , allora

$$(7.7) \quad g(v_0) = f(v_0), \quad g(v_i) = g(v_0 + v_i) - g(v_0) = f(v_0 + v_i) - f(v_0)$$

da cui segue che  $g$  è unica. Per mostrare l'esistenza sia  $g: V \rightarrow V$  l'applicazione lineare definita sulla base  $v_0, \dots, v_n$  dalle precedenti formule (7.7). Allora per ogni  $x \in H$  si ha  $x - v_0 \in W$  ed esistono  $a_1, \dots, a_n \in \mathbb{K}$  tali che

$$x = v_0 + \sum a_i v_i = (1 - \sum a_i) v_0 + \sum a_i (v_0 + v_i).$$

Dunque

$$\begin{aligned} f(x) &= f\left((1 - \sum a_i) v_0 + \sum a_i (v_0 + v_i)\right) = (1 - \sum a_i) f(v_0) + \sum a_i f(v_0 + v_i) \\ &= (1 - \sum a_i) g(v_0) + \sum a_i g(v_0 + v_i) = g(v_0) + \sum a_i g(v_i) = g(x). \end{aligned}$$

Si noti che  $g(v_0) \in H$ , mentre  $g(v_i) = f(v_i + v_0) - f(v_0) \in W$  per ogni  $i > 0$ .

□

La precedente proposizione permette di descrivere in forma matriciale le applicazioni affini  $f: \mathbb{K}^n \rightarrow \mathbb{K}^n$ . Infatti l'applicazione

$$\mathbb{K}^n \rightarrow \mathbb{K}^{n+1}, \quad (x_1, \dots, x_n) \mapsto (1, x_1, \dots, x_n),$$

è un isomorfismo affine con il sottospazio affine  $H = \{x_0 = 1\}$ . Le applicazioni lineari  $g: \mathbb{K}^{n+1} \rightarrow \mathbb{K}^{n+1}$  tali che  $g(H) \subset H$  sono tutte e sole quelle che si rappresentano con una matrice a blocchi del tipo

$$\begin{pmatrix} 1 & 0 \\ A & B \end{pmatrix}, \quad A \in M_{n,1}(\mathbb{K}), B \in M_{n,n}(\mathbb{K}).$$

**OSSERVAZIONE 7.3.9.** La definizione di spazio affine come sottoinsieme di uno spazio vettoriale chiuso per combinazioni baricentriche è semplice e funzionale alla stragrande maggioranza delle situazioni. Tuttavia in certi casi può essere utile introdurre la nozione di **spazio affine astratto**, ad esempio nel modo seguente (che ricalca la definizione di varietà astratta).

Per ogni insieme  $X$  indichiamo con  $\mathcal{A}(X)$  la collezione delle applicazioni bigettive  $\phi: X \rightarrow H$ , con  $H$  sottospazio affine di uno spazio vettoriale. Su  $\mathcal{A}(X)$  consideriamo la relazione di equivalenza

$$(\phi: X \rightarrow H) \sim (\psi: X \rightarrow K) \text{ se } \psi\phi^{-1}: H \rightarrow K \text{ è un isomorfismo affine.}$$

Chiameremo struttura affine su  $X$  una classe di equivalenza in  $\mathcal{A}(X)$ . Uno spazio affine astratto è un insieme dotato di struttura affine.

È possibile definire le traslazioni in uno spazio affine non vuoto  $H$  usando esclusivamente le combinazioni baricentriche, rendendo quindi tale definizione indipendente dalla scelta dell'inclusione di  $H$  in uno spazio vettoriale. Infatti, dato due punti  $p, q \in H$  possiamo definire l'applicazione

$$T_{\vec{pq}}: H \rightarrow H, \quad T_{\vec{pq}}(x) = x + q - p$$

che chiaramente coincide con  $T_{q-p}$  qualora si consideri  $H$  contenuto in uno spazio vettoriale.

È utile osservare che due traslazioni  $T_{\vec{pq}}, T_{\vec{rs}}: H \rightarrow H$  coincidono ovunque se e solo se coincidono in almeno un punto. Infatti se esiste  $x \in H$  tale che  $T_{\vec{pq}}(x) = T_{\vec{rs}}(x)$ , allora per ogni  $y \in H$  vale

$$T_{\vec{pq}}(y) = y + q - p = y + q - p + x - x = y + s - r + x - x = y + s - r = T_{\vec{rs}}(y).$$

Siccome  $T_{\vec{pq}}(p) = q$  si ha quindi

$$T_{\vec{pq}} = T_{\vec{rs}} \iff q = T_{\vec{rs}}(p) = s - r + p \iff q - p = s - r,$$

dove l'uguaglianza più a destra va intesa in uno spazio vettoriale contenente  $H$  come sottospazio affine.

**LEMMA 7.3.10.** *Sia  $f: H \rightarrow K$  un'applicazione affine. Per ogni  $p, q \in H$  vale*

$$f \circ T_{\vec{pq}} = T_{\vec{f(p)f(q)}} \circ f.$$

**DIMOSTRAZIONE.** Per ogni  $x \in H$  si ha

$$f(T_{\vec{pq}}(x)) = f(x + q - p) = f(x) + f(q) - f(p) = T_{\vec{f(p)f(q)}}(f(x)).$$

□

Dato uno spazio affine  $H$ , chiameremo **affinità di  $H$**  un qualunque isomorfismo affine  $H \rightarrow H$ . L'insieme  $\text{Aff}(H)$  delle affinità di  $H$ , dotato del prodotto di composizione è un gruppo, con l'identità come elemento neutro.

**TEOREMA 7.3.11.** *L'insieme di tutte le traslazioni in uno spazio affine  $H$  è un sottogruppo normale abeliano del gruppo delle affinità  $\text{Aff}(H)$ .*

**DIMOSTRAZIONE.** Sia  $T(H) \subset \text{Aff}(H)$  il sottoinsieme delle traslazioni.  $T(H)$  contiene l'identità ed è chiuso rispetto all'inverso, poiché  $T_{\vec{pq}} = T_{\vec{qp}}^{-1}$  per ogni  $p, q \in H$ .

Date due traslazioni  $T_{\vec{pq}}$  e  $T_{\vec{rs}}$  per ogni  $x \in H$  si ha

$$T_{\vec{pq}} T_{\vec{rs}}(x) = x + s - r + q - p$$

da cui segue

$$T_{\vec{p}\vec{q}}T_{\vec{r}\vec{s}} = T_{\vec{r}\vec{s}}T_{\vec{p}\vec{q}} = T_{\vec{p}\vec{t}}, \quad t = s + q - r.$$

In particolare  $T(H)$  è un sottogruppo abeliano di  $\text{Aff}(H)$ . Data una traslazione  $T_{\vec{p}\vec{q}}$  ed una affinità  $f: H \rightarrow H$ , per il Lemma 7.3.10 vale  $f \circ T_{\vec{p}\vec{q}} = T_{\overrightarrow{f(p)f(q)}} \circ f$ . Dato che  $f$  è invertibile si ha

$$f \circ T_{\vec{p}\vec{q}} \circ f^{-1} = T_{\overrightarrow{f(p)f(q)}}$$

e questo implica che  $T(H)$  è un sottogruppo normale.  $\square$

Sia  $H$  uno spazio affine, diremo che due sottospazi affini  $A, B \subset H$  della stessa dimensione sono **paralleli**, e scriveremo  $A \sim B$ , se sono uno il traslato dell'altro, ossia se esistono  $p, q \in H$  tali che  $T_{\vec{p}\vec{q}}(A) = B$ ; si tratta evidentemente di una relazione di equivalenza nell'insieme dei sottospazi affini di dimensione fissata.

**PROPOSIZIONE 7.3.12.** *Siano  $f: H \rightarrow K$  un'applicazione affine e  $A, B \subset H$  sottospazi paralleli. Allora i sottospazi affini  $f(A), f(B)$  sono paralleli, ed in particolare della stessa dimensione.*

**DIMOSTRAZIONE.** Siano  $p, q \in H$  tali che  $T_{\vec{p}\vec{q}}(A) = B$ . Per il Lemma 7.3.10 vale  $f \circ T_{\vec{p}\vec{q}} = T_{\overrightarrow{f(p)f(q)}} \circ f$  e quindi

$$f(B) = f(T_{\vec{p}\vec{q}}(A)) = T_{\overrightarrow{f(p)f(q)}}(f(A)).$$

$\square$

Denotiamo con  $\mathcal{L}$  l'insieme di tutte le rette affini (sottospazi affini di dimensione 1) in  $H$  e con  $\sim$  la relazione di parallelismo in  $\mathcal{L}$ . Notiamo che, fissato un punto  $p \in H$ , le rette affini passanti per  $p$  formano un insieme di rappresentanti per la relazione di equivalenza  $\sim$ , e cioè per ogni retta affine in  $L \subset H$  esiste un'unica retta  $L'$  passante per  $p$  e parallela a  $L$ . Chiameremo il quoziente  $\mathcal{L}/\sim$  **iperpiano all'infinito** e l'unione

$$\hat{H} = H \cup (\mathcal{L}/\sim)$$

**completamento proiettivo di  $H$ .**

**OSSERVAZIONE 7.3.13.** Nello spazio  $\mathbb{K}^n$  con coordinate  $t_1, \dots, t_n$ , possiamo allora considerare l'applicazione affine iniettiva

$$h: \mathbb{K}^n \rightarrow \mathbb{K}^{n+1}, \quad h(t_1, \dots, t_n) = (1, t_1, \dots, t_n).$$

L'applicazione  $h$  preserva la relazione di parallelismo e la sua immagine è il sottospazio affine  $H = \{x_0 = 1\}$ . Possiamo quindi identificare il completamento proiettivo di  $\mathbb{K}^n$  con il completamento proiettivo di  $H$ .

Ogni retta affine in  $H = \{x_0 = 1\}$  è parallela ad un unico sottospazio vettoriale di dimensione 1 di  $\{x_0 = 0\}$ . Ogni punto di  $\{x_0 = 1\}$  è contenuto in un unico sottospazio vettoriale di dimensione 1 di  $\mathbb{K}^{n+1}$ . *Esiste dunque una bigezione tra il completamento proiettivo di  $\{x_0 = 1\} \simeq \mathbb{K}^n$  e l'insieme di tutte le rette per l'origine in  $\mathbb{K}^{n+1}$ .*

### Esercizi

**ESERCIZIO 37.** Sia  $f: \mathbb{K}^n \rightarrow \mathbb{K}^m$  un'applicazione affine e siano  $f(0) = (b_1, \dots, b_m)$ ,  $f(\delta^i) - f(0) = (a_{1i}, \dots, a_{mi})$ , dove  $\delta^1, \dots, \delta^n$  indica la base canonica di  $\mathbb{K}^n$ . Provare che  $f$  manda il punto  $(x_1, \dots, x_n)$  nel punto  $(y_1, \dots, y_m)$  che soddisfa la relazione

$$\begin{pmatrix} y_1 \\ \vdots \\ y_m \\ 1 \end{pmatrix} = \begin{pmatrix} a_{11} & \dots & a_{1n} & b_1 \\ \vdots & \ddots & \vdots & \vdots \\ a_{m1} & \dots & a_{mn} & b_m \\ 0 & \dots & 0 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_n \\ 1 \end{pmatrix}.$$

Caratterizzare inoltre le matrici  $(n+1) \times (n+1)$  corrispondenti alle traslazioni in  $\mathbb{K}^n$ .

**ESERCIZIO 38.** Sia  $H \subset \mathbb{K}^n$  un sottospazio affine non contenente 0 e  $f: H \rightarrow \mathbb{K}^m$  un'applicazione affine. Dimostrare che  $f$  è la restrizione ad  $H$  di un'applicazione lineare  $g: \mathbb{K}^n \rightarrow \mathbb{K}^m$ .

ESERCIZIO 39. Siano  $P_1 = (1, 2)$ ,  $P_2 = (3, 1)$ ,  $P_3 = (3, 3)$ ,  $Q_1 = (1, 8)$ ,  $Q_2 = (0, 7)$  e  $Q_3 = (7, 3)$ . Si determini l'affinità di  $\mathbb{R}^2$  in sé che trasforma  $P_i$  in  $Q_i$  per  $i = 1, 2, 3$ .

#### 7.4. Curve di Bezier

In alcuni algoritmi usati in grafica computerizzata giocano un ruolo fondamentale i **polinomi di Bernstein**  $B_i^n(t)$ ,  $n \geq 0$ ,  $i \in \mathbb{Z}$ , definiti dalla formula:

$$(7.8) \quad B_i^n(t) = \binom{n}{i} t^i (1-t)^{n-i}, \quad \text{per } 0 \leq i \leq n,$$

e  $B_i^n(t) = 0$  per  $i < 0$  e  $i > n$ . Per semplicità espositiva consideriamo i polinomi di Bernstein a coefficienti reali, sebbene gran parte delle considerazioni che seguiranno sono valide su qualsiasi campo di caratteristica 0.

Sia  $V_n \subset \mathbb{R}[t]$  il sottospazio vettoriale dei polinomi di grado  $\leq n$ ; una base naturale di  $V_n$  è data dagli  $n+1$  monomi  $t^0, t^1, \dots, t^n$ . Siccome

$$B_{n-i}^n(t) = \binom{n}{i} t^{n-i} (1-t)^i = \sum_{h=0}^i (-1)^h \binom{i}{h} \binom{n}{i} t^{n-i} t^h = \sum_{j=0}^i (-1)^{i-j} \binom{i}{j} \binom{n}{i} t^{n-j}$$

è immediato osservare che  $B_n^n(t), \dots, B_0^n(t)$  sono linearmente indipendenti e quindi sono una base di  $V_n$ . La matrice di cambio di base è uguale a

$$(B_n^n(t), \dots, B_0^n(t)) = (t^n, \dots, t^0)(m_{ji}), \quad m_{ji} = (-1)^{i-j} \binom{i}{j} \binom{n}{i}.$$

Dunque la matrice di cambio base  $(m_{ji})$  è triangolare superiore con elementi sulla diagonale uguali a  $m_{jj} = \binom{n}{j}$ . Ad esempio per  $n=2$  e  $n=3$  si ha:

$$(B_2^2(t), B_1^2(t), B_0^2(t)) = (t^2, 2t - 2t^2, 1 - 2t + t^2) = (t^2, t, 1) \begin{pmatrix} 1 & -2 & 1 \\ 0 & 2 & -2 \\ 0 & 0 & 1 \end{pmatrix},$$

$$(B_3^3(t), \dots, B_0^3(t)) = (t^3, \dots, t^0) \begin{pmatrix} 1 & -3 & 3 & -1 \\ 0 & 3 & -6 & 3 \\ 0 & 0 & 3 & -3 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Vediamo adesso alcune proprietà dei polinomi di Bernstein (le dimostrazioni sono lasciate per esercizio):

- (1) (Simmetria) Vale  $B_i^n(t) = B_{n-i}^n(1-t)$  per ogni  $n, i$ .
- (2) (Relazioni ricorsive) Si ha  $B_0^0 = 1$  e  $B_i^0 = 0$  per  $i \neq 0$ . Per ogni  $n > 0$  ed ogni  $i$  si ha

$$B_i^n(t) = t B_{i-1}^{n-1}(t) + (1-t) B_i^{n-1}(t).$$

- (3) (Partizione dell'unità, vedi Figura 4) Per ogni  $n \geq 0$  vale

$$\sum_{i=0}^n B_i^n(t) = (t + (1-t))^n = 1.$$

- (4) (Derivate) Le derivate dei polinomi di Bernstein soddisfano la formula:

$$B_i^n(t)' = n(B_{i-1}^{n-1}(t) - B_i^{n-1}(t)).$$

La proprietà  $\sum_{i=0}^n B_i^n(t) = 1$  permette di usare i polinomi di Bernstein per definire curve parametriche nello spazio affine.

DEFINIZIONE 7.4.1. Sia  $p_0, p_1, \dots, p_n$  una successione di  $n$  punti in uno spazio affine  $H$  sul campo  $\mathbb{R}$ . Chiameremo **curva di Bézier** controllata da  $p_0, p_1, \dots, p_n$  l'applicazione

$$\mathbf{b}: [0, 1] \rightarrow H, \quad \mathbf{b}(t) = \sum_{i=0}^n B_i^n(t) p_i.$$

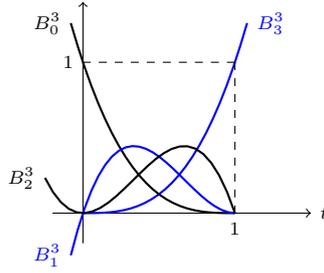


FIGURA 4. Grafici dei polinomi di Bernstein  $B_i^3(t)$  per  $0 \leq t \leq 1$  e  $0 \leq i \leq 3$ .

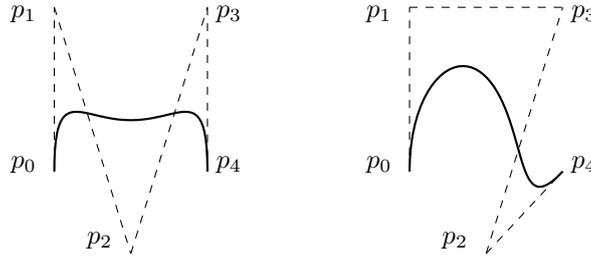


FIGURA 5. Due curve di Bézier del quarto grado; la prima controllata da  $p_0, p_1, p_2, p_3, p_4$ , la seconda da  $p_0, p_1, p_3, p_2, p_4$ .

Notiamo subito che gli estremi della curva di Bézier sono

$$\mathbf{b}(0) = p_0, \quad \mathbf{b}(1) = p_n .$$

La costruzione delle curve di Bézier commuta con le applicazioni affini: nella situazione della Definizione 7.4.1, per ogni applicazione affine  $f: H \rightarrow K$ , la curva  $f \circ \mathbf{b}$  è la curva di Bézier controllata da  $f(p_0), f(p_1), \dots, f(p_n)$ . Infatti se  $\mathbf{b}(t) = \sum_{i=0}^n B_i^n(t)p_i$  allora, siccome  $\sum_{i=0}^n B_i^n(t) = 1$  si ha

$$f(\mathbf{b}(t)) = \sum_{i=0}^n B_i^n(t)f(p_i) .$$

La proprietà di simmetria dei polinomi di Bernstein implica che se  $\mathbf{b}(t)$  è la curva di Bézier controllata da  $p_0, p_1, \dots, p_n$ , allora  $\mathbf{b}(1-t)$  è la curva di Bézier controllata da  $p_n, p_{n-1}, \dots, p_0$ . Appare invece chiaro che l'insieme  $\{\mathbf{b}(t) \mid t \in [0, 1]\}$  non è invariante per permutazioni dei punti  $p_i$  (vedi Figura 5).

Nella sostanza, la curva di Bézier controllata da una successione di punti  $p_0, \dots, p_n$  è una approssimazione algebrica della poligonale di vertici  $p_0, \dots, p_n$ . Spesso, ma non sempre, la curva di Bézier assume un aspetto “morbido”.

PROPOSIZIONE 7.4.2 (Algoritmo di de Casteljau). Sia  $p_0, p_1, \dots, p_n$  una successione di  $n$  punti in uno spazio affine  $H$  sul campo  $\mathbb{R}$ . Definiamo in maniera ricorsiva delle applicazioni

$$\mathbf{b}_i^r: [0, 1] \rightarrow H, \quad 0 \leq i, r; \quad i + r \leq n;$$

ponendo  $\mathbf{b}_i^0(t) = p_i$  per ogni  $t$  e

$$\mathbf{b}_i^r(t) = (1-t)\mathbf{b}_i^{r-1}(t) + t\mathbf{b}_{i+1}^{r-1}(t) .$$

Allora  $\mathbf{b}_0^n = \mathbf{b}$  è la curva di Bézier controllata da  $p_0, p_1, \dots, p_n$ .

DIMOSTRAZIONE. Segue dalla formula  $B_i^r(t) = tB_{i-1}^{r-1}(t) + (1-t)B_i^{r-1}(t)$  e da una semplice induzione che per ogni coppia  $i, r$  tale che  $i + r \leq n$ , si ha

$$\mathbf{b}_i^r(t) = \sum_{j=0}^r B_j^r(t)p_{i+j} .$$

□

OSSERVAZIONE 7.4.3. Il primo utilizzo delle curve di Bézier è avvenuto nell'industria automobilistica attorno<sup>3</sup> al 1960. Infatti sia P. Bézier che P. de Casteljau lavoravano al reparto carrozzeria della Renault e della Citroën, rispettivamente.

### Esercizi.

ESERCIZIO 1. Dimostrare le seguenti proprietà dei polinomi di Bernstein:

$$\begin{aligned} \sum_{j=0}^n \frac{j}{n} B_j^n(t) &= t, & B_i^n(st) &= \sum_{j=i}^n B_i^j(s) B_j^n(t), \\ t^i &= \sum_{j=i}^n \frac{\binom{j}{i}}{\binom{n}{i}} B_j^n(t), & B_i^n(t) B_j^m(t) &= \frac{\binom{n}{i} \binom{m}{j}}{\binom{n+m}{i+j}} B_{i+j}^{n+m}(t), \\ \int_0^x B_i^n(t) dt &= \frac{1}{n+1} \sum_{j=i+1}^{n+1} B_j^{n+1}(x), \\ t B_i^n(t) &= \frac{i+1}{n+1} B_{i+1}^{n+1}(t), & (1-t) B_i^n(t) &= \frac{n-i+1}{n+1} B_i^{n+1}(t), \\ B_i^n(t) &= \frac{i+1}{n+1} B_{i+1}^{n+1}(t) + \frac{n-i+1}{n+1} B_i^{n+1}(t). \end{aligned}$$

ESERCIZIO 2. Calcolare il massimo assoluto delle funzioni di variabile reale  $B_i^n: [0, 1] \rightarrow \mathbb{R}$ .

ESERCIZIO 3. Sia  $\mathbf{b}$  la curva di Bézier controllata da  $p_0, p_1, \dots, p_n \in \mathbb{R}^k$  e provare che

$$\mathbf{b}(t) = p_0 + tn(p_1 - p_0) + t^2(\dots)$$

Mostrare inoltre che se gli  $n$  vettori  $p_i - p_0$ ,  $i = 1, \dots, n$  sono linearmente indipendenti allora la derivata di  $\mathbf{b}(t)$  è sempre diversa da 0.

ESERCIZIO 4. Sia  $\mathbf{b}: [0, 1] \rightarrow \mathbb{R}^2$  la curva di Bézier di terzo grado controllata dalla poligonale  $(1, 0), (-1, 1), (1, 1), (-1, 0)$ . Mostrare che tale curva possiede una cuspidale semplice per  $t = 1/2$ , ossia che

$$\mathbf{b}\left(\frac{1}{2} + s\right) = \mathbf{b}\left(\frac{1}{2}\right) + As^2 + Bs^3,$$

con  $A, B$  vettori linearmente indipendenti.

## 7.5. Spazi proiettivi

Sia  $\mathbb{K}$  un campo e  $V$  uno spazio vettoriale su  $\mathbb{K}$ ; definiamo il **proiettivizzato** di  $V$

$$\mathbb{P}(V) = (V - \{0\}) / \sim$$

come il quoziente di  $V - \{0\}$  per la relazione di equivalenza

$$v \sim w \quad \text{se e solo se} \quad v = \lambda w \quad \text{per qualche } \lambda \in \mathbb{K} - \{0\}.$$

L'insieme  $\mathbb{P}(V)$  è in bigezione naturale con l'insieme dei sottospazi vettoriali di dimensione 1 (rette per l'origine) di  $V$ .

Dato un vettore  $v \in V - \{0\}$  si è soliti denotare con  $[v] \in \mathbb{P}(V)$  la classe di equivalenza corrispondente.

Chiameremo  $\mathbb{P}_{\mathbb{K}}^n = \mathbb{P}(\mathbb{K}^{n+1})$  **spazio proiettivo** di dimensione  $n$  sul campo  $\mathbb{K}$ . In assenza di ambiguità sul campo  $\mathbb{K}$  scriveremo più semplicemente  $\mathbb{P}^n$  in luogo di  $\mathbb{P}_{\mathbb{K}}^n$ .

Siccome  $\mathbb{P}^n$  può essere interpretato come l'insieme delle rette per l'origine in  $\mathbb{K}^{n+1}$ , per l'Osservazione 7.3.13 si ha una bigezione tra  $\mathbb{P}^n$  ed il completamento proiettivo dello spazio affine  $\mathbb{K}^n$ .

<sup>3</sup>Il segreto industriale che per anni ha coperto tali tecniche di progettazione non consente di dare una datazione precisa.

Diremo che un sottoinsieme  $M \subset V$  è un **cono** se  $0 \in M$  e se  $v \in M$  implica che  $\lambda v \in M$  per ogni  $\lambda \in \mathbb{K}$ . Se  $M \subset V$  è un cono e  $S \subset \mathbb{P}(V)$  è un sottoinsieme, si definisce

$$\mathbb{P}(M) = \{[v] \mid v \in M - \{0\}\} \subset \mathbb{P}(V) \quad \text{e} \quad C(S) = \{v \in V - \{0\} \mid [v] \in S\} \cup \{0\}.$$

Il sottoinsieme  $C(S) \subset V$  viene detto **cono affine** di  $S$ ; è immediato osservare che le applicazioni

$$\{\text{coni in } V\} \xrightarrow{\mathbb{P}} \{\text{sottoinsiemi di } \mathbb{P}(V)\} \xrightarrow{C} \{\text{coni in } V\}$$

sono bigettive ed una l'inversa dell'altra.

Se  $W \subset V$  è un sottospazio vettoriale, chiameremo  $\mathbb{P}(W)$  **sottospazio proiettivo** di  $\mathbb{P}(V)$ . Si noti che ogni punto di uno spazio proiettivo è un sottospazio:  $[v] = \mathbb{P}(\mathbb{K}v)$ .

Se  $W \subset V$  è un iperpiano diremo che  $\mathbb{P}(W)$  è un **iperpiano** di  $\mathbb{P}(V)$ . Poiché  $\mathbb{P}(\cap_i M_i) = \cap_i \mathbb{P}(M_i)$  per ogni famiglia di coni  $\{M_i\}$ , si ha in particolare che intersezione di sottospazi proiettivi è ancora un sottospazio proiettivo.

**ESEMPIO 7.5.1.** Siano  $L \subset \mathbb{P}(V)$  un sottospazio proiettivo e  $p, q \in \mathbb{P}(V)$  non appartenenti ad  $L$ . Allora esiste un iperpiano  $H \subset \mathbb{P}(V)$  tale che  $L \subset H$  e  $p, q \notin H$ .

Infatti, sia  $n = \dim V$  e  $p = [u]$ ,  $q = [v]$  e  $L = \mathbb{P}(W)$  con  $W \subset V$  sottospazio vettoriale di dimensione  $m < n$ . Se  $m = n - 1$  basta prendere  $H = L$ . Se  $m < n - 1$  si consideri una base  $v_1, \dots, v_n$  di  $V$  tale che  $v_1, \dots, v_m$  sia base di  $W$  e scriviamo

$$u = \sum_i a_i v_i, \quad v = \sum_i b_i v_i$$

L'ipotesi che  $p, q \notin L$  equivale a dire che esistono indici  $m < i, j \leq n$  tali che  $a_i, b_j \neq 0$ . Se esiste un indice  $i > m$  per cui  $a_i b_i \neq 0$  basta considerare  $H = \mathbb{P}(U)$  dove  $U$  è l'iperpiano generato da  $v_1, \dots, \hat{v}_i, \dots, v_n$ .

Se invece per ogni  $i > m$  vale  $a_i b_i = 0$  allora esistono due indici  $m < i, j \leq n$  tali che  $a_i \neq 0, b_i = 0, a_j = 0$  e  $b_j \neq 0$ . In tal caso possiamo prendere  $H = \mathbb{P}(U)$ , dove  $U$  è l'iperpiano generato da  $v_1, \dots, \hat{v}_i, \dots, \hat{v}_j, \dots, v_n, v_i + v_j$ .

**DEFINIZIONE 7.5.2** (Inviluppo di sottospazi proiettivi). Se  $W_1, W_2, \dots, W_n \subset V$  sono sottospazi vettoriali scriveremo

$$\mathbb{P}(W_1) + \mathbb{P}(W_2) + \dots + \mathbb{P}(W_n) = \mathbb{P}(W_1 + W_2 + \dots + W_n).$$

In altri termini, se  $H_1, \dots, H_n \subset \mathbb{P}(V)$  sono sottospazi proiettivi, allora  $H_1 + \dots + H_n$ , è il più piccolo sottospazio proiettivo di  $\mathbb{P}(V)$  che li contiene.

Dati due punti  $p, q \in \mathbb{P}(V)$  scriveremo anche  $\overline{pq}$  per indicare l'inviluppo proiettivo  $p + q$ . Se vale  $p_1 = [v_1], p_2 = [v_2], \dots, p_n = [v_n]$ , con  $v_1, \dots, v_n \in V - \{0\}$ , allora

$$p_1 + p_2 + \dots + p_n = \mathbb{P}(\text{Span}(v_1, \dots, v_n)).$$

Se lo spazio vettoriale  $V$  ha dimensione finita, definiamo la dimensione di  $\mathbb{P}(V)$  mediante la formula  $\dim \mathbb{P}(V) = \dim V - 1$ : in particolare l'insieme vuoto  $\emptyset = \mathbb{P}(0)$  avrà dimensione  $-1$  quando viene considerato come uno spazio proiettivo.

Spazi proiettivi di dimensione 1 e 2 si dicono rispettivamente **rette** e **piani** proiettivi. Punti contenuti in una medesima retta vengono detti **allineati**, punti (o rette) contenuti in un medesimo piano si dicono **complanari**, rette passanti per un medesimo punto si dicono **concorrenti**.

Si noti che due punti  $p = [v]$  e  $q = [w]$  in uno spazio proiettivo sono distinti se e solo se i vettori  $v, w$  sono linearmente indipendenti. Tre punti  $p = [v], q = [w]$  e  $r = [u]$  sono allineati se e solo se in tre vettori  $u, v, w$  sono linearmente dipendenti, ossia se e solo se  $\text{Span}(u, v, w)$  ha dimensione  $\leq 2$ .

Due sottospazi proiettivi  $H, K \subset \mathbb{P}(V)$  si dicono **incidenti** se  $H \cap K \neq \emptyset$ , altrimenti si dicono **sghembi**; poiché  $C(H + K) = C(H) + C(K)$  e  $\dim H = \dim C(H) - 1$  vale la **formula di Grassmann**

$$\dim(H \cap K) + \dim(H + K) = \dim H + \dim K$$

e quindi  $H$  e  $K$  sono sghembi se e solo se  $\dim(H + K) = \dim H + \dim K + 1$ .

Sia  $f: V \rightarrow W$  un isomorfismo lineare di spazi vettoriali. In particolare  $f(v) = 0$  se e solo se  $v = 0$  ed è ben definita la fattorizzazione al quoziente

$$[f]: \mathbb{P}(V) \rightarrow \mathbb{P}(W), \quad [v] \mapsto [f(v)].$$

È chiaro che  $[f]$  è bigettiva, trasforma sottospazi proiettivi in sottospazi proiettivi della stessa dimensione e preserva le relazioni di incidenza, concorrenza, allineamento, complanarità ecc.

**DEFINIZIONE 7.5.3.** Un'applicazione  $\phi: \mathbb{P}(V) \rightarrow \mathbb{P}(W)$  si dice un **isomorfismo proiettivo** o **proiettività** se è indotta per passaggio al quoziente da una applicazione lineare invertibile  $f: V \rightarrow W$  mediante la regola

$$\phi([v]) = [f(v)], \quad v \in V - \{0\},$$

e scriveremo in tal caso  $\phi = [f]$ .

Ogni proiettività è bigettiva e la sua inversa è ancora una proiettività. Più precisamente, se  $\phi = [f]$ , allora  $\phi^{-1} = [f^{-1}]$ .

La geometria proiettiva si occupa di studiare i luoghi geometrici (configurazioni, chiusi di Zariski, varietà ecc.) contenuti in uno spazio proiettivo, a meno di isomorfismi proiettivi. Per il momento ci occuperemo solamente di configurazioni, ossia di famiglie finite di sottospazi proiettivi che soddisfano alcune relazioni di incidenza, allineamento eccetera.

**ESEMPIO 7.5.4.** Siano  $V, W$  due spazi vettoriali della stessa dimensione e siano  $H \subset V$  e  $K \subset W$  due sottospazi della stessa dimensione. Allora esiste una proiettività  $\psi: \mathbb{P}(V) \rightarrow \mathbb{P}(W)$  tale che  $\psi(\mathbb{P}(H)) = \mathbb{P}(K)$ . A tal fine basta considerare  $\psi = [f]$ , con  $f: V \rightarrow W$  un qualunque isomorfismo lineare tale che  $f(H) = K$ .

In particolare, se  $V$  ha dimensione  $n+1$ , la scelta di una base di  $V$ , ossia di un isomorfismo  $\mathbb{K}^{n+1} \rightarrow V$  induce un isomorfismo proiettivo  $\mathbb{P}^n \simeq \mathbb{P}(V)$ . Lo stesso accade per qualunque scelta di un sistema di coordinate, ossia di una base di  $V^\vee$ , ossia di un isomorfismo lineare  $V \rightarrow \mathbb{K}^{n+1}$ .

**ESEMPIO 7.5.5.** Siano  $H \subset \mathbb{P}(V)$  un iperpiano e  $W \subset \mathbb{P}(V)$  un sottospazio proiettivo di dimensione  $m$ . Se  $W$  non è contenuto in  $H$  allora  $H + W = \mathbb{P}(V)$  e per la formula di Grassmann  $\dim H \cap W = m - 1$ .

Per ogni punto  $p \in W - H = \{q \in W \mid q \notin H\}$  si ha  $p + (H \cap W) = W$ . Infatti  $p + (H \cap W) \subset W$  (i due sottospazi  $p$  e  $W \cap H$  sono entrambi contenuti in  $W$ ) e per Grassmann  $\dim(p + (H \cap W)) = 1 + (m - 1) = \dim W$ .

Siano  $\mathbb{K}$  un campo finito con  $q$  elementi e  $V$  è uno spazio vettoriale di dimensione  $n+1$  su  $\mathbb{K}$ , allora  $\mathbb{P}(V)$  è isomorfo a  $\mathbb{P}_{\mathbb{K}}^n$  e quindi il numero di punti di  $\mathbb{P}(V)$ , e più in generale il numero di sottospazi proiettivi di dimensione fissata, dipende solo da  $n$  e  $\mathbb{K}$ . La prossima proposizione fornisce un metodo di calcolo di tale quantità.

**PROPOSIZIONE 7.5.6.** Siano  $\mathbb{K}$  un campo finito con  $q$  elementi,  $n$  un intero positivo e si consideri il polinomio

$$\frac{1}{t} \left( \prod_{i=0}^n (1 + tq^i) - 1 \right) = \sum_{p=0}^n a_p^n t^p \in \mathbb{Z}[t].$$

Allora per ogni  $0 \leq p \leq n$  il numero  $s_p^n$  dei sottospazi proiettivi di dimensione  $p$  contenuti in  $\mathbb{P}_{\mathbb{K}}^n$  è uguale a  $s_p^n = \frac{a_p^n}{\prod_{i=0}^p q^i}$ .

**DIMOSTRAZIONE.** È istruttivo trattare prima il caso  $p = 0$ , ossia calcolare quanti punti contiene lo spazio proiettivo di dimensione  $n$ . Siccome

$$\frac{1}{t} \left( \prod_{i=0}^n (1 + tq^i) - 1 \right) = \sum_{i=0}^n q^i + t(\dots)$$

dimostriamo per induzione su  $n$  che  $\mathbb{P}_{\mathbb{K}}^n$  contiene  $1 + q + \dots + q^n$  punti. Per l'ipotesi induttiva ogni iperpiano  $H$  di  $\mathbb{P}_{\mathbb{K}}^n$  contiene  $1 + q + \dots + q^{n-1}$  punti; basta adesso osservare che  $\mathbb{P}_{\mathbb{K}}^n - H$

è lo spazio affine  $\mathbb{K}^n$  che contiene  $q^n$  punti. Similmente la proposizione è vera per  $p = n$ : si verifica immediatamente che  $a_n^n = \prod_{i=0}^n q^i$ .

Consideriamo adesso il caso generale. Per ogni coppia di interi  $-1 \leq p \leq n$  indichiamo con  $s_p^n$  il numero di sottospazi proiettivi di  $\mathbb{P}^n$  di dimensione  $p$ . Vale allora la formula ricorsiva

$$s_{-1}^n = s_n^n = 1, \quad s_p^n = s_p^{n-1} + q^{n-p} s_{p-1}^{n-1}, \quad 0 \leq p < n.$$

Infatti se  $0 \leq p \leq n-1$  e scriviamo  $\mathbb{P}^n = \mathbb{K}^n \cup \mathbb{P}^{n-1}$  (parte affine unito iperpiano all'infinito), i sottospazi di dimensione  $p$  si dividono in due classi disgiunte: quelli contenuti nell'iperpiano all'infinito, che sono  $s_p^{n-1}$ , e quelli del tipo  $a + H$ , con  $a \in \mathbb{K}^n$  e  $H \subset \mathbb{P}^{n-1}$  di dimensione  $p-1$ . I punti  $a \in \mathbb{K}^n$  sono  $q^n$ , ma  $a + H = b + H$  se e solo se  $b \in (a + H) \cap \mathbb{K}^n$ . Basta adesso osservare che  $(a + H) \cap \mathbb{K}^n$  è il complementare di un iperpiano in  $\mathbb{P}^p$  e quindi contiene  $q^p$  punti.

D'altra parte, siccome

$$\frac{1}{t} \prod_{i=0}^n (1 + tq^i) = \frac{1}{t} + \sum_{p=0}^n a_p^n t^p = \left( \frac{1}{t} + \sum_{p=0}^{n-1} a_p^{n-1} t^p \right) (1 + tq^n)$$

si hanno le formule ricorsive

$$a_p^n = a_p^{n-1} + q^n a_{p-1}^{n-1}, \quad 0 \leq p,$$

e dividendo per  $\prod_{i=0}^p q^i$  si ottiene

$$\frac{a_p^n}{\prod_{i=0}^p q^i} = \frac{a_p^{n-1}}{\prod_{i=0}^p q^i} + q^{n-p} \frac{a_{p-1}^{n-1}}{\prod_{i=0}^{p-1} q^i}.$$

La conclusione segue dunque dal principio di definizione ricorsiva.  $\square$

Per la formula di Grassmann, due rette in  $\mathbb{P}^2$  sono sempre incidenti. Se  $p = [u] \neq q = [v]$ ,  $r = [w] \neq s = [z]$  si ha

$$\overline{pq} \cap \overline{rs} = \mathbb{P}(\text{Span}(u, v) \cap \text{Span}(w, z)),$$

e quindi bisogna trovare le soluzioni non banali del sistema lineare (3 equazioni e 4 incognite)

$$x_0 u + x_1 v = y_0 w + y_1 z.$$

Ad esempio, se  $p = [1, 0, 0]$ ,  $q = [0, 1, 0]$ ,  $r = [0, 0, 1]$  e  $s = [1, 1, 1]$ , siccome

$$(1, 1, 0) = (1, 0, 0) + (0, 1, 0) = -(0, 0, 1) + (1, 1, 1)$$

si ha che  $\overline{pq} \cap \overline{rs} = [1, 1, 0]$ .

**ESEMPIO 7.5.7.** Sia  $p$  un punto di  $\mathbb{P}^2$ . L'insieme di tutte le rette  $L \subset \mathbb{P}^2$  che contengono  $p$  viene detto **fascio di rette** passanti per  $p$ . Più raramente il termine fascio viene chiamato *pennello* o *schiera*.

Se  $H \subset \mathbb{P}^2$  è una retta che non contiene  $p$  vi è una ovvia applicazione

$$H \rightarrow \{\text{fascio di rette per } p\}, \quad q \mapsto \overline{pq},$$

che è iniettiva in quanto  $p \notin H$  ed è surgettiva in quanto due rette in  $\mathbb{P}^2$  si intersecano sempre.

La comprensione del teorema di Pappo (III secolo D.C.) e di un teorema scoperto dal matematico francese Girard Desargues nel 1639 è stata una delle principali motivazioni dello sviluppo, nel XIX secolo, della geometria proiettiva.

**TEOREMA 7.5.8 (Desargues).** *Siano dati 7 punti distinti  $o, p_1, p_2, p_3, q_1, q_2, q_3 \in \mathbb{P}^2$  tali che ciascuna delle tre terne  $(o, p_1, q_1)$ ,  $(o, p_2, q_2)$  e  $(o, p_3, q_3)$  sia formata da tre punti allineati. Allora i tre punti*

$$r_1 = \overline{p_2 p_3} \cap \overline{q_2 q_3}, \quad r_2 = \overline{p_1 p_3} \cap \overline{q_1 q_3}, \quad r_3 = \overline{p_1 p_2} \cap \overline{q_1 q_2},$$

sono allineati (Figura 6).

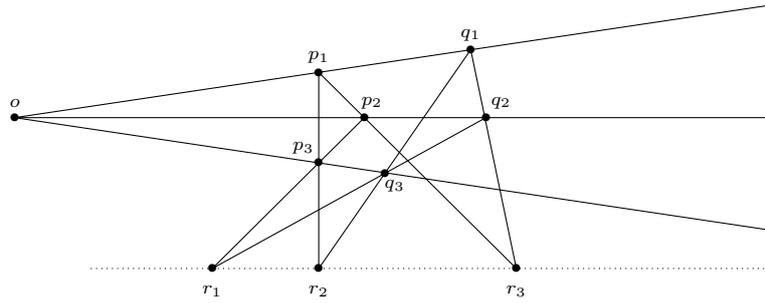


FIGURA 6. Il teorema di Desargues.

DIMOSTRAZIONE. Sia  $\mathbb{P}^2 = \mathbb{P}(V)$ , con  $V$  spazio vettoriale di dimensione 3 e scegliamo 7 vettori  $u, v_1, v_2, v_3, w_1, w_2, w_3 \in V - \{0\}$  tali che

$$o = [u], \quad p_i = [v_i], \quad q_i = [w_i].$$

Per ipotesi  $o$  appartiene alla retta  $\overline{p_1q_1}$ . Questo equivale a dire che  $u$  è una combinazione lineare di  $v_1$  e  $w_1$ : diciamo  $u = a_1v_1 + b_1w_1$ . Similmente si ha

$$u = a_1v_1 + b_1w_1 = a_2v_2 + b_2w_2 = a_3v_3 + b_3w_3.$$

Da tali uguaglianze deduciamo che

$$a_1v_1 - a_2v_2 = b_2w_2 - b_1w_1, \quad a_2v_2 - a_3v_3 = b_3w_3 - b_2w_2, \quad a_1v_1 - a_3v_3 = b_3w_3 - b_1w_1.$$

da cui segue

$$r_3 = [a_1v_1 - a_2v_2], \quad r_1 = [a_2v_2 - a_3v_3], \quad r_2 = [a_1v_1 - a_3v_3].$$

I tre punti  $r_1, r_2$  ed  $r_3$  sono allineati poiché

$$(a_1v_1 - a_2v_2) + (a_2v_2 - a_3v_3) + (a_1v_1 - a_3v_3) = 0.$$

□

OSSERVAZIONE 7.5.9. Il teorema di Desargues ha senso anche se esiste un indice  $i$  tale che  $p_i = q_i$ , ed in tal caso la sua validità è evidente perché se ad esempio  $p_1 = q_1$  allora  $r_2 = r_3 = p_1 = q_1$ , mentre l'enunciato perde di significato se  $p_i = q_i$  per almeno due indici  $i$ .

### Esercizi

ESERCIZIO 40. Se  $H, K$  sono sottospazi non vuoti di uno spazio proiettivo allora

$$H + K = \bigcup_{p \in H, q \in K} \overline{pq}.$$

ESERCIZIO 41. Siano  $p = [1, 0, \dots, 0]$  e  $q = [a_0, a_1, \dots, a_n]$  punti distinti di  $\mathbb{P}^n$ . Provare che i punti della retta  $\overline{pq}$  diversi da  $p$  sono tutti e soli quelli di coordinate

$$[a_0 + t, a_1, \dots, a_n], \quad t \in \mathbb{K}.$$

ESERCIZIO 42. Sia  $V$  uno spazio vettoriale di dimensione  $n + 1$ . Provare che ogni sottospazio proiettivo di  $\mathbb{P}(V)$  di dimensione  $k$  è intersezione di  $n - k$  iperpiani proiettivi.

ESERCIZIO 43. Nella situazione della Proposizione 7.5.6, provare che

$$s_p^n = \sum_S q^{\sum_{i=0}^p a_i}, \quad \text{dove } S = \{(a_0, \dots, a_p) \in \mathbb{N}^{p+1} \mid a_0 \leq a_1 \leq \dots \leq a_p \leq n - p\},$$

ed in particolare che il numero di rette in  $\mathbb{P}_{\mathbb{K}}^n$  è uguale a

$$s_1^n = \sum_{0 \leq i \leq j \leq n-1} q^{i+j}.$$

### 7.6. Sistemi di riferimento e coordinate omogenee

**DEFINIZIONE 7.6.1.** Diremo che  $s + 1$  punti  $p_0, \dots, p_s \in \mathbb{P}(V)$  sono **proiettivamente indipendenti** se il sottospazio  $\langle p_0, \dots, p_s \rangle$  da essi generato ha dimensione esattamente  $s$ .

Ad esempio, due punti in  $\mathbb{P}^1$  sono proiettivamente indipendenti se e solo se sono distinti; tre punti in  $\mathbb{P}^2$  sono proiettivamente indipendenti se e solo se non sono allineati.

È fondamentale osservare che, se  $v_0, \dots, v_s \in V - \{0\}$ , allora i punti  $[v_0], \dots, [v_s]$  sono proiettivamente indipendenti se e solo se i vettori  $v_0, \dots, v_s$  sono linearmente indipendenti.

**DEFINIZIONE 7.6.2.** Diremo che  $n + 2$  punti  $p_0, \dots, p_{n+1} \in \mathbb{P}(V)$  sono un **sistema di riferimento** se  $\dim V = n + 1$  e se per ogni indice  $i$  fissato, i punti  $p_j$ , per  $j \neq i$ , sono proiettivamente indipendenti.

Sono esempi di sistemi di riferimento:

- Tre punti distinti di  $\mathbb{P}^1$ .
- Quattro punti di  $\mathbb{P}^2$ , tre dei quali non siano allineati.
- Cinque punti di  $\mathbb{P}^3$ , quattro dei quali non siano complanari.

**LEMMA 7.6.3.** Sia  $V$  uno spazio vettoriale di dimensione  $n + 1$ . Allora  $n + 2$  punti  $p_0, \dots, p_{n+1} \in \mathbb{P}(V)$  sono un sistema di riferimento se e solo se esiste una base  $e_0, \dots, e_n \in V$  tale che  $p_i = [e_i]$  per  $i = 0, \dots, n$  e  $p_{n+1} = [e_0 + e_1 + \dots + e_n]$ .

**DIMOSTRAZIONE.** Se  $e_0, \dots, e_n \in V$  è una base, allora è facile osservare che i punti  $p_i = [e_i]$  per  $i = 0, \dots, n$  e  $p_{n+1} = [e_0 + e_1 + \dots + e_n]$  sono un sistema di riferimento.

Sia viceversa  $p_0, \dots, p_{n+1}$  un sistema di riferimento e scegliamo vettori  $v_0, \dots, v_n \in V$  tali che  $p_i = [v_i]$  per ogni  $i = 0, \dots, n$ . Siccome  $p_0, \dots, p_n$  sono indipendenti, ne segue che  $v_0, \dots, v_n$  è una base di  $V$  e quindi esistono  $a_0, \dots, a_n \in \mathbb{K}$  tali che  $p_{n+1} = [e_{n+1}]$ , dove  $e_{n+1} = a_0 v_0 + \dots + a_n v_n$ . Se fosse  $a_i = 0$  per qualche indice  $i$ , allora gli  $n + 1$  vettori

$$v_0, \dots, v_{i-1}, e_{n+1}, v_{i+1}, \dots, v_n$$

sarebbero linearmente dipendenti e quindi  $p_0, \dots, p_{n+1}$  non potrebbe essere un sistema di riferimento. Quindi  $a_i \neq 0$  per ogni  $i$  ed è sufficiente considerare la base  $e_i = a_i v_i$ ,  $i = 0, \dots, n$ .  $\square$

Per quadrilatero completo in  $\mathbb{P}^n$  si intende la configurazione di una quaterna di punti  $a, b, c, d$  (i vertici) e delle 6 rette  $\overline{ab}, \overline{ac}, \overline{ad}, \overline{bc}, \overline{bd}, \overline{cd}$  (i lati). Il quadrilatero si dice **non degenero** se tra i 4 punti non ne esistono 3 allineati.

Se  $n = 2$ , un quadrilatero completo è non degenero se e solo se i vertici formano un sistema di riferimento proiettivo.

**ESEMPIO 7.6.4.** Siano  $a, b, c, d \in \mathbb{P}^2$  i vertici di un quadrilatero completo non degenero. Allora i tre punti di intersezione delle coppie di lati opposti

$$p = \overline{ab} \cap \overline{cd}, \quad q = \overline{ac} \cap \overline{bd}, \quad r = \overline{ad} \cap \overline{bc}$$

sono distinti. Inoltre  $p, q, r$  sono allineati se e solo se il campo  $\mathbb{K}$  ha caratteristica 2.

Infatti possiamo trovare coordinate proiettive tali che

$$a = [1, 0, 0], \quad b = [0, 1, 0], \quad c = [0, 0, 1], \quad d = [1, 1, 1],$$

da cui segue

$$p = [1, 1, 0], \quad q = [1, 0, 1], \quad r = [0, 1, 1],$$

ed il determinante

$$\begin{vmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{vmatrix} = -2$$

si annulla se e solo se il campo è di caratteristica 2.

Chiameremo **sistema di coordinate omogenee** su  $\mathbb{P}(V)$  un qualsiasi sistema di coordinate lineari su  $V$ . Se  $\mathbb{P}(V)$  ha dimensione finita  $n$ , la scelta di un sistema di coordinate omogenee definisce un isomorfismo proiettivo  $\mathbb{P}(V) = \mathbb{P}^n$  e quindi permette di rappresentare ogni punto  $p \in \mathbb{P}(V)$  nella forma  $p = [a_0, \dots, a_n]$ , con i numeri  $a_i \in \mathbb{K}$  non tutti nulli.

Tale rappresentazione non è unica: infatti vale  $[a_0, \dots, a_n] = [b_0, \dots, b_n]$  se e solo se esiste  $\lambda \in \mathbb{K} - \{0\}$  tale che  $b_i = \lambda a_i$  per ogni  $i$ .

Le seguenti quaterne di punti di  $\mathbb{P}^2$ , descritte in coordinate omogenee, sono sistemi di riferimento:

- (1)  $[1, 0, 0], [0, 1, 0], [0, 0, 1], [1, 1, 1]$ ;  
 (2)  $[1, 0, 0], [1, 1, 0], [0, 0, 1], [0, 1, 1]$ .

La prima non è altro che la rappresentazione del Lemma 7.6.3 per la base canonica; la seconda quaterna è invece riferita alla base  $e_0 = (-1, 0, 0), e_1 = (1, 1, 0), e_2 = (0, 0, 1)$ , poiché  $[1, 0, 0] = [-1, 0, 0]$ .

LEMMA 7.6.5. *Siano  $f, g: V \rightarrow W$  due applicazioni lineari iniettive e consideriamo le applicazioni*

$$\phi, \psi: \mathbb{P}(V) \rightarrow \mathbb{P}(W), \quad \phi([v]) = [f(v)], \quad \psi([v]) = [g(v)].$$

Allora vale  $\phi = \psi$  se e solo se esiste  $\lambda \in \mathbb{K} - \{0\}$  tale che  $f = \lambda g$ .

DIMOSTRAZIONE. L'unica implicazione non banale è il "solo se". Supponiamo quindi  $\phi = \psi$  e fissiamo una base  $v_0, \dots, v_n$  di  $V$ . L'iniettività di  $g$  implica allora che i vettori  $g(v_0), \dots, g(v_n)$  sono linearmente indipendenti.

Dalle relazioni  $[f(v_i)] = [g(v_i)]$  si ricava che esistono  $n + 1$  scalari invertibili  $\lambda_i$  tali che

$$f(v_i) = \lambda_i g(v_i), \quad i = 0, \dots, n.$$

Siccome  $f, g$  sono univocamente determinate dai valori che assumono sulla base  $v_0, \dots, v_n$ , per concludere basta dimostrare che  $\lambda_i = \lambda_j$  per ogni  $i, j$ . Dalla relazione

$$[f(v_0 + \dots + v_n)] = [g(v_0 + \dots + v_n)]$$

deduciamo che esiste un  $\lambda \in \mathbb{K} - \{0\}$  tale che

$$f(v_0 + \dots + v_n) = \lambda g(v_0 + \dots + v_n) = \sum_i \lambda g(v_i).$$

D'altra parte

$$f(v_0 + \dots + v_n) = \sum_i f(v_i) = \sum_i \lambda_i g(v_i)$$

e l'indipendenza lineare dei vettori  $g(v_0), \dots, g(v_n)$  implica che  $\lambda_i = \lambda$  per ogni indice  $i$ .  $\square$

Si denota  $\text{PGL}(V)$  il gruppo delle proiettività di  $\mathbb{P}(V)$  in sé. Per definizione esiste un omomorfismo surgettivo di gruppi  $\text{GL}(V) \rightarrow \text{PGL}(V)$  che, per il lemma precedente ha come nucleo i multipli dell'identità. Si indica anche  $\text{PGL}_n(\mathbb{K}) = \text{PGL}(\mathbb{K}^n)$ , e quindi  $\text{PGL}_{n+1}(\mathbb{K})$  è il gruppo degli automorfismi proiettivi di  $\mathbb{P}_{\mathbb{K}}^n$ .

PROPOSIZIONE 7.6.6. *Dati due sistemi di riferimento  $p_0, \dots, p_{n+1}$  e  $q_0, \dots, q_{n+1}$  di  $\mathbb{P}^n$ , esiste un'unica proiettività  $\varphi \in \text{PGL}_{n+1}(\mathbb{K})$  tale che  $\varphi(p_i) = q_i$  per ogni  $i$ .*

DIMOSTRAZIONE. L'esistenza segue immediatamente dal Lemma 7.6.3, mentre per l'unicità non è restrittivo supporre  $p_i = q_i$  per ogni  $i$ . Sia  $e_0, \dots, e_n$  una base di  $\mathbb{K}^{n+1}$  tale che  $p_i = [e_i]$  con  $e_{n+1} = \sum e_i$  e  $f: \mathbb{K}^{n+1} \rightarrow \mathbb{K}^{n+1}$  lineare invertibile tale che  $[f]p_i = p_i$  per ogni  $i$ . Allora esistono costanti  $a_0, \dots, a_{n+1} \in \mathbb{K}$  tali che  $f(e_i) = a_i e_i$  per ogni  $i$ . Poiché  $e_0, \dots, e_n$  sono una base segue necessariamente che  $a_i = a_{n+1}$  per ogni  $i = 0, \dots, n$  e quindi  $f$  è un multiplo dell'identità.  $\square$

Per  $n = 1$  possiamo scrivere  $\mathbb{P}^1 = \mathbb{K} \cup \{\infty\}$ , dove  $\mathbb{K} = \{[1, t] \mid t \in \mathbb{K}\}$  e  $\infty = [0, 1]$  (intuitivamente  $[0, 1]$  è il limite per  $t \rightarrow \infty$  di  $[1/t, 1] = [1, t]$ ). Ogni proiettività  $\phi$  di  $\mathbb{P}^1$  in sé è rappresentata da  $\phi([x_0, x_1]) = [ax_0 + bx_1, cx_0 + dx_1]$ ,  $ad \neq bc$ , che, nella coordinata affine  $t = x_1/x_0$  diventa

$$\phi(t) = \frac{cx_0 + dx_1}{ax_0 + bx_1} = \frac{c + dt}{a + bt}, \quad \text{con } ad - bc \neq 0.$$

TEOREMA 7.6.7 (Pappo). *Siano  $p_1, \dots, p_6$  punti distinti e non allineati di  $\mathbb{P}^2$ , divisi in due terne allineate  $p_1, p_3, p_5$  e  $p_2, p_4, p_6$  (Figura 7).*

*Allora i tre punti*

$$\overline{p_1 p_2} \cap \overline{p_4 p_5}, \quad \overline{p_2 p_3} \cap \overline{p_5 p_6}, \quad \overline{p_3 p_4} \cap \overline{p_6 p_1},$$

*sono allineati.*

DIMOSTRAZIONE. Vediamo una prima dimostrazione che utilizza conteggi elementari ma piuttosto grezzi con le coordinate omogenee. Altre dimostrazioni più concettuali saranno date in seguito.

Siano  $L$  la retta contenente  $p_1, p_3, p_5$  e  $M$  la retta contenente  $p_2, p_4, p_6$ . A meno di permutazioni cicliche degli indici non è restrittivo supporre che nessuno dei 4 punti  $p_1, \dots, p_4$  sia uguale al punto  $o$  di intersezione di  $L$  e  $M$ .

Dunque  $p_1, \dots, p_4$  sono un sistema di riferimento proiettivo ed esiste un sistema di coordinate omogenee tali che

$$p_1 = [1, 0, 0], \quad p_3 = [1, 1, 0], \quad p_2 = [0, 0, 1], \quad p_4 = [0, 1, 1].$$

La retta passante per  $p_1, p_3$  è dunque formata dai punti di coordinate omogenee  $[x + y, y, 0]$ . Siccome  $p_5 \neq p_1, p_3$  si ha  $p_5 = [x + y, y, 0]$  con  $x, y$  entrambi non nulli; ponendo  $a = (x + y)/y$  si può scrivere  $p_5 = [a, 1, 0]$ .

Con analogo ragionamento applicato ai punti  $p_6, o$  si ha

$$o = [0, 1, 0], \quad p_5 = [a, 1, 0], \quad p_6 = [0, 1, b], \quad a, b \in \mathbb{K} - \{1\},$$

e l'ipotesi  $p_5 \neq p_6$  implica che  $a$  e  $b$  non possono essere contemporaneamente nulli. Siccome:

$$a(1, 0, 0) - (0, 0, 1) = -(0, 1, 1) + (a, 1, 0),$$

$$b(a - 1)(0, 0, 1) + a(1, 1, 0) = (a, 1, 0) + (a - 1)(0, 1, b),$$

$$(1 - b)(1, 1, 0) + b(0, 1, 1) = (0, 1, b) + (1 - b)(1, 0, 0),$$

si hanno le intersezioni

$$\overline{p_1 p_2} \cap \overline{p_4 p_5} = [a, 0, -1], \quad \overline{p_2 p_3} \cap \overline{p_5 p_6} = [a, a, b(a - 1)], \quad \overline{p_3 p_4} \cap \overline{p_6 p_1} = [1 - b, 1, b],$$

e l'allineamento dei tre punti segue, *tenendo presente la commutatività del prodotto ( $ab = ba$ )*, dalla relazione:

$$(a, a, b(a - 1)) = b(a, 0, -1) + a(1 - b, 1, b).$$

□

ESEMPIO 7.6.8 (reti di iperpiani). Sia  $H \subset \mathbb{P}^n$  un sottospazio proiettivo di dimensione  $r$ . L'insieme  $\mathcal{F}$  di tutti gli iperpiani di  $\mathbb{P}^n$  che contengono  $H$  viene detta una **rete di iperpiani**. È chiaro che se  $r = n$  allora  $\mathcal{F} = \emptyset$ , mentre se  $r = n - 1$  allora  $\mathcal{F} = \{H\}$ . Il numero  $n - r - 1$  viene detto la **dimensione della rete  $\mathcal{F}$** : una rete di iperpiani di dimensione 1 viene anche detta **fascio di iperpiani**.

Se  $x_0, \dots, x_n$  è un sistema di coordinate omogenee tali che  $H$  è definito dalle equazioni  $x_{r+1} = \dots = x_n = 0$ , allora gli elementi di  $\mathcal{F}$  sono tutti e soli gli iperpiani definiti da una equazione del tipo

$$(7.9) \quad a_{r+1}x_{r+1} + \dots + a_n x_n = 0, \quad a_i \in \mathbb{K} \text{ non tutti nulli.}$$

È chiaro che ogni iperpiano definito come in (7.9) contiene  $H$ . Viceversa, se un iperpiano  $K$  di equazione  $\sum_{i=0}^n a_i x_i = 0$  contiene  $H$ , allora contiene in particolare i punti

$$[\underbrace{0, \dots, 0}_j, 1, 0, \dots, 0], \quad 0 \leq j < r$$

$j$  zeri

e questo è possibile se e solo se  $a_i = 0$  per ogni  $i = 0, \dots, r$ . Si noti che siccome  $\{x_i = 0\} \in \mathcal{F}$  per ogni  $r < i \leq n$  si ha che  $H = \bigcap_{K \in \mathcal{F}} K$ .

### Esercizi

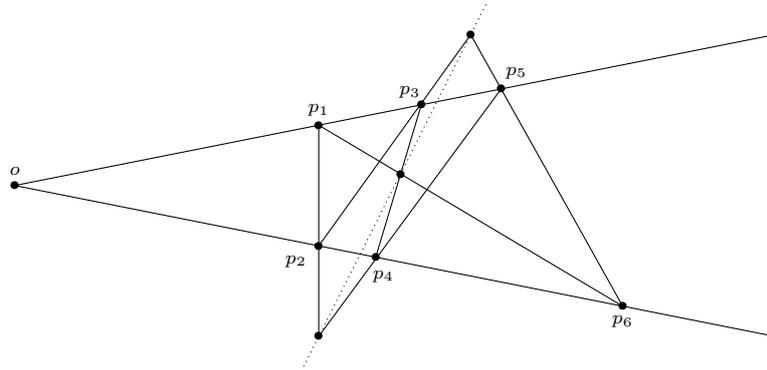


FIGURA 7. Il teorema di Pappo.

ESERCIZIO 44. Determinare le proiettività di  $\mathbb{P}^1(\mathbb{C}) = \mathbb{C} \cup \{\infty\}$  in sé che preservano i seguenti sottoinsiemi di  $\mathbb{C}$ :

$$\mathbb{R} = \{x + iy \mid y = 0\}, \quad H = \{x + iy \mid y > 0\}, \quad \bar{H} = \{x + iy \mid y \geq 0\},$$

$$\Delta = \{x + iy \mid x^2 + y^2 < 1\}, \quad \bar{\Delta} = \{x + iy \mid x^2 + y^2 \leq 1\}.$$

Provare inoltre che la proiettività  $\phi(t) = \frac{t-i}{t+i}$  trasforma il semipiano  $H$  nel disco  $\Delta$ .

### 7.7. Proiezioni

Prima di affrontare il tema proiezioni, osserviamo che per ogni proiettività  $\psi: \mathbb{P}^n \rightarrow \mathbb{P}^n$  l'insieme dei suoi punti fissi si decompone nella forma

$$\text{Fix}(\psi) = \{p \in \mathbb{P}^n \mid \psi(p) = p\} = H_1 \cup \dots \cup H_h$$

dove gli  $H_i$  sono sottospazi proiettivi disgiunti e tali che  $\sum_{i=1}^h (\dim H_i + 1) \leq n + 1$ . Infatti se  $\psi$  è indotta da un'applicazione lineare invertibile  $f: \mathbb{K}^{n+1} \rightarrow \mathbb{K}^{n+1}$ , allora i punti fissi di  $\psi$  corrispondono agli autovettori di  $f$ . Se  $\lambda_1, \dots, \lambda_h \in \mathbb{K}$  sono gli autovalori di  $f$ , allora il luogo dei punti fissi di  $\psi$  coincide con l'unione dei sottospazi  $H_i = \mathbb{P}(\ker(f - \lambda_i I))$ . Tale unione è disgiunta in quanto ad ogni autovettore corrisponde un unico autovalore. Inoltre la dimensione di  $H_i$  è uguale alla molteplicità geometrica dell'autovalore  $\lambda_i$  diminuita di 1, e la disuguaglianza  $\sum_{i=1}^h (\dim H_i + 1) \leq n + 1$  segue dai ben noti risultati di algebra lineare.

LEMMA 7.7.1. Sia  $\psi: \mathbb{P}^n \rightarrow \mathbb{P}^n$  una proiettività e siano  $H, K$  due sottospazi proiettivi contenuti nel luogo dei punti fissi  $\text{Fix}(\psi)$ . Se  $H \cap K \neq \emptyset$ , allora  $H + K \subset \text{Fix}(\psi)$ .

DIMOSTRAZIONE. Siano  $U, V \subset \mathbb{K}^{n+1}$  i due sottospazi vettoriali tali che  $H = \mathbb{P}(U)$ ,  $K = \mathbb{P}(V)$ , e sia  $f: \mathbb{K}^{n+1} \rightarrow \mathbb{K}^{n+1}$  un automorfismo lineare che induce  $\psi$ . Siccome  $\psi|_H$  è l'identità esiste uno scalare non nullo  $h \in \mathbb{K}$  tale che  $f(u) = hu$  per ogni  $u \in U$ ; similmente esiste  $k \in \mathbb{K}$  tale che  $f(v) = kv$  per ogni  $v \in V$ . Se  $H \cap K \neq \emptyset$  allora  $U \cap V$  contiene un vettore non nullo e questo implica  $h = k$  ed allora  $f(x) = hx = kx$  per ogni  $x \in U + V$ .  $\square$

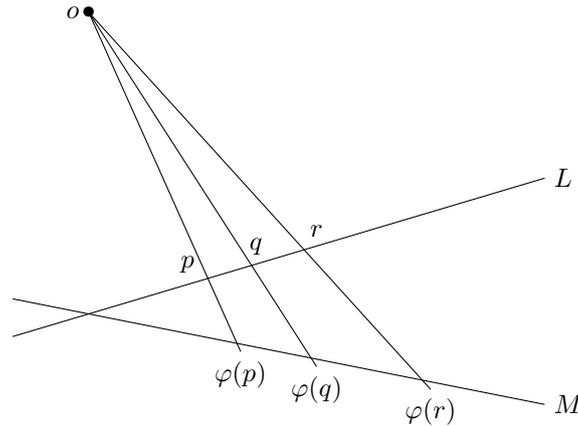
Siano  $o \in \mathbb{P}^n$  un punto e  $L, M \subset \mathbb{P}^n$  due iperpiani tali che  $o \notin M \cup L$ . Allora, per ogni  $p \in L$  si ha  $o \neq p$  e la retta  $\overline{op}$  interseca  $M$  in un unico punto, dato che  $o \notin M$ . Possiamo quindi definire un'applicazione

$$\varphi: L \rightarrow M, \quad \varphi(p) = \overline{op} \cap M,$$

detta **proiezione di centro**  $o$  (Figura 8).

È facile dimostrare che la proiezione  $\varphi$  appena definita è un isomorfismo proiettivo. Infatti, siccome  $o \notin M$  possiamo scegliere un sistema di coordinate omogenee  $x_0, \dots, x_n$  tali che  $o = [1, 0, \dots, 0]$  e  $M = \mathbb{P}(\{x_0 = 0\})$ . Siccome  $o \notin L$  l'equazione di  $L$  sarà del tipo  $x_0 = \sum_{i=1}^n a_i x_i$  e possiamo considerare l'isomorfismo proiettivo

$$\psi: \mathbb{P}^{n-1} \rightarrow L, \quad [y_1, \dots, y_n] \mapsto \left[ \sum a_i y_i, y_1, \dots, y_n \right].$$

FIGURA 8. Proiezione  $\varphi: L \rightarrow M$  di centro  $o$ .

Ma allora la composizione  $\varphi\psi$  coincide con l'isomorfismo proiettivo

$$\varphi\psi: \mathbb{P}^{n-1} \rightarrow M, \quad [y_1, \dots, y_n] \mapsto [0, y_1, \dots, y_n].$$

Segue immediatamente dalle definizioni che se  $\varphi: L \rightarrow M$  è la proiezione di centro  $o$ , allora anche  $\varphi^{-1}: M \rightarrow L$  è la proiezione di centro  $o$ .

Dati due iperpiani distinti  $L, M \subset \mathbb{P}^n$ , non tutti gli isomorfismi proiettivi  $L \rightarrow M$  sono proiezioni, come si evince dal seguente teorema.

**TEOREMA 7.7.2.** *Dati due iperpiani distinti  $L, M \subset \mathbb{P}^n$ , un isomorfismo proiettivo  $\varphi: L \rightarrow M$  è una proiezione se e solo se  $\varphi(p) = p$  per ogni  $p \in L \cap M$ .*

**DIMOSTRAZIONE.** Il risultato è ovvio se  $n = 1$ . Supponiamo  $n \geq 2$ . Una implicazione è banale: se  $\varphi$  è una proiezione di centro  $o$ , allora per ogni  $p \in L \cap M$  si ha  $\varphi(p) = \overline{op} \cap M = p$ .

Viceversa sia  $H = L \cap M$ , che per la formula di Grassmann ha dimensione  $n - 2$ , e fissiamo un sistema di riferimento proiettivo  $p_0, \dots, p_n$  di  $L$  tale che  $p_2, \dots, p_n \in H$  (Esercizio: dimostrare). Denotiamo  $q_0 = \varphi(p_0)$ ,  $q_1 = \varphi(p_1)$ ,  $r = H \cap \overline{p_0 p_1}$ .

Siccome  $\varphi(r) = r$  le due rette distinte  $\overline{p_0 p_1}$  e  $\overline{q_0 q_1} = \varphi(\overline{p_0 p_1})$  di  $\mathbb{P}^n$  hanno intersezione non vuota (entrambe contengono  $r$ ) e quindi  $P = \overline{p_0 p_1} + \overline{q_0 q_1}$  ha dimensione 2 per Grassmann. Abbiamo quindi dimostrato che i 4 punti  $p_0, p_1, q_0, q_1$  appartengono ad un piano proiettivo  $P$ , nel quale ogni coppia di rette ha intersezione non vuota. Denotiamo  $o = \overline{p_0 q_0} \cap \overline{p_1 q_1}$  e sia  $\psi: L \rightarrow M$  la proiezione di centro  $o$ . Allora  $\psi(p_0) = q_0$ ,  $\psi(p_1) = q_1$  e  $\psi(p_i) = p_i$  per ogni  $i > 1$ . Dunque  $\varphi$  e  $\psi$  coincidono in un sistema di riferimento proiettivo e dunque  $\varphi = \psi$ .  $\square$

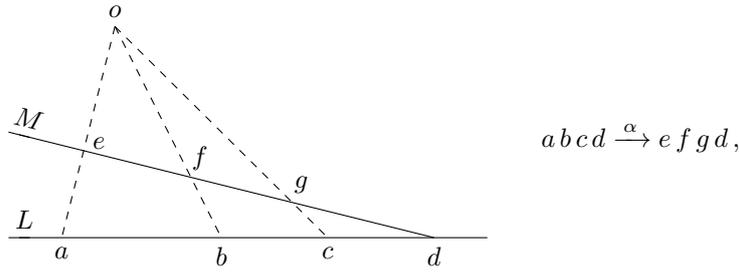
Il prossimo obiettivo è quello di dimostrare che ogni isomorfismo proiettivo tra due iperpiani si ottiene come composizione di un numero finito di proiezioni. Prima di trattare il caso generale è istruttivo considerare il caso delle rette nel piano proiettivo.

**ESEMPIO 7.7.3.** Siano  $a, b, c, d$  quattro punti distinti di una retta proiettiva  $L$ . Allora esiste una proiettività  $\varphi: L \rightarrow L$  tale che

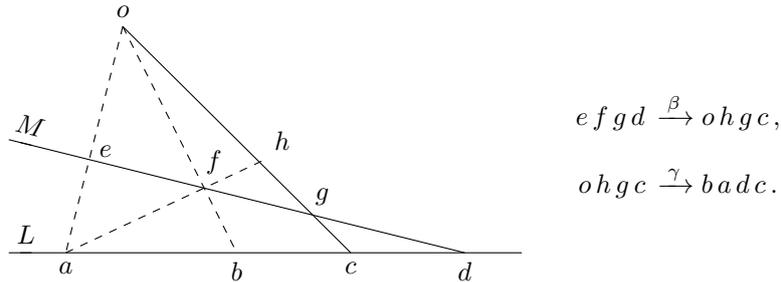
$$abcd \xrightarrow{\varphi} badc,$$

ossia  $\varphi(a) = b$ ,  $\varphi(b) = a$ ,  $\varphi(c) = d$  e  $\varphi(d) = c$ . Siccome  $a, b, c, d$  sono sistemi di riferimento proiettivi, ne segue che  $\varphi$  è unica e che  $\varphi^2$  è uguale all'identità.

Un modo particolarmente carino di dimostrare tale fatto è quello di scrivere esplicitamente  $\varphi$  come composizione di 3 proiezioni. A tal fine consideriamo  $L \subset \mathbb{P}^2$ , sia  $M \neq L$  una qualunque retta passante per  $d$  e sia  $\alpha: L \rightarrow M$  una qualunque proiezione di centro  $o \notin L \cup M$ :



Siano adesso  $\beta: M \rightarrow \overline{oc}$  la proiezione di centro  $a$  e  $\gamma: \overline{oc} \rightarrow L$  la proiezione di centro  $f$ . Allora



In conclusione la proiettività  $\varphi = \gamma\beta\alpha: L \rightarrow L$  scambia  $a$  con  $b$  e  $c$  con  $d$ . Per simmetria, esistono altresì due proiettività  $\psi, \eta: L \rightarrow L$  tali che

$$abcd \xrightarrow{\varphi} badc, \quad abcd \xrightarrow{\psi} cdab, \quad abcd \xrightarrow{\eta} dcba.$$

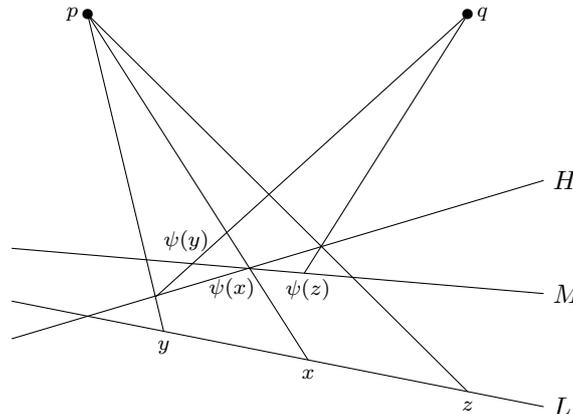
Vedremo più avanti che altre permutazioni di  $a, b, c, d$  sono ottenute per restrizione di una proiettività solamente in casi molto particolari.

**PROPOSIZIONE 7.7.4.** *Sia  $\psi: L \rightarrow M$  una proiettività tra due rette distinte di  $\mathbb{P}^2$  e sia  $o = L \cap M$  il loro punto di intersezione;*

- (1) *se  $\psi(o) = o$ , allora  $\psi$  è una proiezione;*
- (2) *se  $\psi(o) \neq o$ , allora  $\psi$  è composizione di due proiezioni.*

**DIMOSTRAZIONE.** Ridimostriamo il caso  $\psi(o) = o$  sebbene sia un caso particolare del Teorema 7.7.2. Se  $\psi(o) = o$ , estendiamo  $o$  ad un sistema di riferimento proiettivo  $o, x, y \in L$  di  $L$  e sia  $p$  il punto di intersezione delle rette  $\overline{x\psi(x)}$  e  $\overline{y\psi(y)}$ . Se  $\varphi_p: L \rightarrow M$  è la proiezione di centro  $p$ , allora  $\varphi_p(o) = o$ ,  $\varphi_p(x) = \psi(x)$ ,  $\varphi_p(y) = \psi(y)$  e questo implica che  $\varphi_p = \psi$ .

Se  $\psi(o) \neq o$  fissiamo un sistema di riferimento proiettivo  $x, y, z \in L$  tale che  $\psi(x) \notin L \cap M$  e scegliamo una qualsiasi retta  $H \subset \mathbb{P}^2$ , diversa da  $M$  che contiene  $\psi(x)$ . Sia poi  $p \notin L \cup H$  un punto allineato con  $x, \psi(x)$  e consideriamo la proiezione  $\varphi_p: L \rightarrow H$  di centro  $p$ . Allora  $\varphi_p(x) = \psi(x)$  e per quanto visto prima esiste una proiezione  $\varphi_q: H \rightarrow M$  tale che  $\varphi_q\varphi_p(x) = \psi(x)$ ,  $\varphi_q\varphi_p(y) = \psi(y)$  e  $\varphi_q\varphi_p(z) = \psi(z)$ : quindi  $\varphi_q\varphi_p = \psi$ .



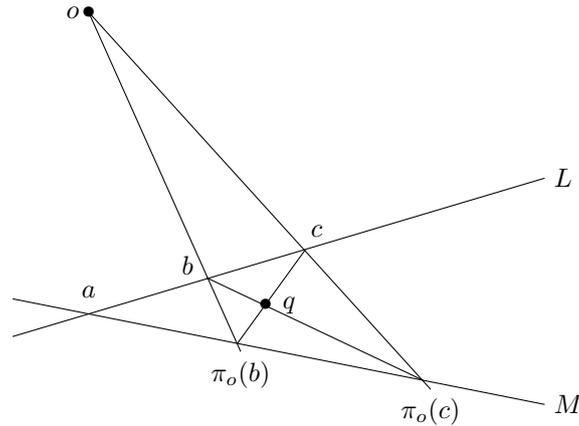


FIGURA 9. La composizione  $\pi_q \pi_o: L \rightarrow L$  scambia  $b$  con  $c$  e lascia fisso  $a$ .

□

**COROLLARIO 7.7.5.** *Sia  $L \subset \mathbb{P}^2$  una retta proiettiva. Allora ogni proiettività  $\psi: L \rightarrow L$  è composizione di al più tre proiezioni.*

**DIMOSTRAZIONE.** Sia  $\varphi: M \rightarrow L$  una qualunque proiezione, con  $M \neq L$ . Per il teorema la proiettività  $\varphi^{-1}\psi: L \rightarrow M$  è composizione di al più due proiezioni. □

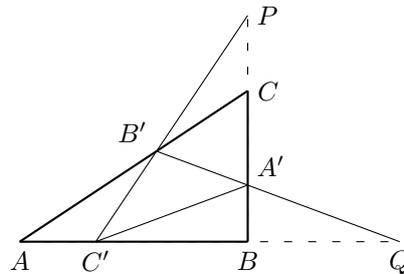
**ESEMPIO 7.7.6.** Siano  $a, b, c$  tre punti distinti di  $\mathbb{P}^1$  e costruiamo l'unica proiettività  $\psi: \mathbb{P}^1 \rightarrow \mathbb{P}^1$  tale che  $\psi(a) = a$ ,  $\psi(b) = c$  e  $\psi(c) = b$  come composizione di 2 proiezioni. A tal fine identifichiamo  $\mathbb{P}^1$  con una retta proiettiva  $L \subset \mathbb{P}^2$  e sia  $M \subset \mathbb{P}^2$  un'altra retta tale che  $L \cap M = \{a\}$ . Siano  $o \notin L \cup M$  un qualsiasi punto e  $\pi_o: L \rightarrow M$  la proiezione di centro  $o$ ; allora  $\psi = \pi_q \circ \pi_o$  dove  $\pi_q: M \rightarrow L$  è la proiezione di centro  $q = b\pi_o(c) \cap c\pi_o(b)$  (Figura 9).

**PROPOSIZIONE 7.7.7 (Steiner 1832).** *In  $\mathbb{P}^2$  si consideri un triangolo non degenere  $ABC$  ed un triangolo (non degenere)  $A'B'C'$  ad esso iscritto, ossia  $A' \in \overline{BC}$ ,  $B' \in \overline{CA}$ ,  $C' \in \overline{AB}$ . Siano:*

- (1)  $\varphi_A: \overline{C'A'} \rightarrow \overline{A'B'}$  la proiezione di centro  $A$ ;
- (2)  $\varphi_B: \overline{A'B'} \rightarrow \overline{B'C'}$  la proiezione di centro  $B$ ;
- (3)  $\varphi_C: \overline{B'C'} \rightarrow \overline{C'A'}$  la proiezione di centro  $C$ .

Allora  $\varphi_C \varphi_B \varphi_A = \text{Id}$ .

**DIMOSTRAZIONE.** Basta dimostrare che  $\psi := \varphi_C \varphi_B: \overline{A'B'} \rightarrow \overline{C'A'}$  è la proiezione di centro  $A$ . Siccome  $A' = \overline{A'B'} \cap \overline{C'A'}$  e  $A', B, C$  sono allineati, ne segue che  $\varphi_C \varphi_B(A') = \varphi_C(P) = A'$  e quindi  $\varphi_C \varphi_B$  è una proiezione.

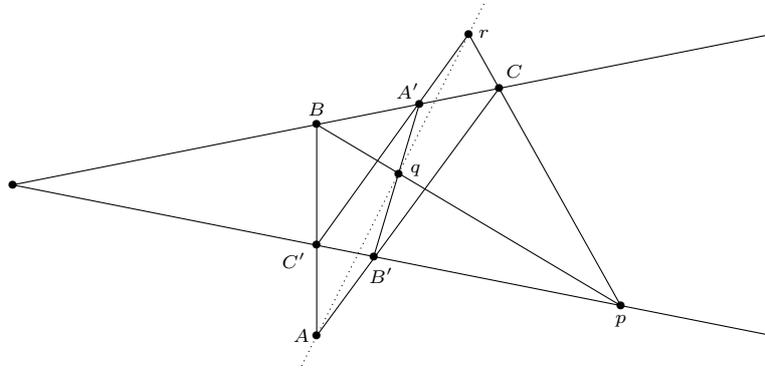


Inoltre se  $Q = \overline{AB} \cap \overline{A'B'}$  si ha

$$\begin{aligned}\psi(B') &= \varphi_C \varphi_B(B') = \varphi_C(B') \in \overline{B'C} = \overline{AB'}, \\ \psi(Q) &= \varphi_C \varphi_B(Q) = \varphi_C(C') = C' \in \overline{AB} = \overline{AQ}.\end{aligned}$$

Ma le precedenti due relazioni impongono che il centro di prospettiva di  $\psi$  deve necessariamente essere  $A$ . □

Possiamo ridimostrare il teorema di Pappo come conseguenza della Proposizione 7.7.7. A tal fine riprendiamo la Figura 7 con i punti ridenominati nel modo seguente



Allora  $\varphi_C \varphi_B(q) = \varphi_C(p) = r$ , quindi  $\varphi_A(q) = r$  ed in particolare  $A, q, r$  sono allineati.

**TEOREMA 7.7.8.** *Siano  $L \subset \mathbb{P}^n$  un iperpiano e  $\psi: L \rightarrow L$  una proiettività. Allora  $\psi$  è composizione di una successione finita di proiezioni del tipo*

$$\psi: L \xrightarrow{\varphi_1} M_1 \xrightarrow{\varphi_2} L \xrightarrow{\varphi_3} M_3 \xrightarrow{\varphi_4} L \dots \xrightarrow{\varphi_{2m}} L,$$

con  $M_i \neq L$  per ogni  $i$ .

**DIMOSTRAZIONE.** Sia  $H \subset L$  un sottospazio proiettivo di dimensione massima tra quelli contenuti nel luogo  $\text{Fix}(\psi)$  dei punti fissi di  $\psi$ . Dimostriamo il teorema per induzione su  $d = \dim L - \dim H$ . Se  $d = 0$  vuol dire che  $\psi$  è l'identità e non c'è nulla da dimostrare. Supponiamo  $d > 0$  ed il teorema vero per ogni proiettività  $\phi: L \rightarrow L$  il cui luogo fisso contiene un sottospazio di dimensione  $> \dim H$ . Trattiamo separatamente i due casi  $\text{Fix}(\psi) \neq H$  e  $\text{Fix}(\psi) = H$ .

*Primo caso,  $\text{Fix}(\psi) \neq H$ .* In particolare  $\text{Fix}(\psi) \neq \emptyset$  e di conseguenza anche  $H \neq \emptyset$ , in quanto il vuoto non ha dimensione massima tra i sottospazi proiettivi di  $\text{Fix}(\psi)$ .

Scegliamo un punto  $p \in \text{Fix}(\psi) - H$  ed un punto punto  $r \in H$ . Siccome  $p, r$  sono punti fissi di  $\psi$ , si ha  $\psi(\overline{pr}) = \overline{pr}$ . Sia  $q \in \overline{pr}$  un qualsiasi punto diverso da  $p, r$  e denotiamo con  $s = \psi(q) \in \overline{pr}$ . Adesso prendiamo un qualsiasi iperpiano  $M \subset \mathbb{P}^n$  tale che  $p \notin M$  e  $H \subset M$  ed un qualsiasi punto  $o \notin L \cup M$ . Siano  $\varphi_1: M \rightarrow L$  e  $\psi_1: L \rightarrow M$  le proiezioni di centro  $o$  e denotiamo  $q_1 = \psi_1(q)$  e dunque  $\varphi_1(q_1) = q$ . Dato che  $q_1$  appartiene al piano  $P$  generato da  $p, r, o$ , si ha che la retta  $\overline{oq_1}$  interseca la retta  $\overline{op}$  in un punto  $o'$ .

Denotiamo con  $\varphi_2: L \rightarrow M$  e  $\psi_2: M \rightarrow L$  le proiezioni di centro  $o'$ . Allora  $\varphi_2(s) = q_1$  e quindi, ponendo  $\widehat{\psi} = \varphi_1 \varphi_2 \psi: L \rightarrow L$  si ha  $\widehat{\psi}(p) = p$ ,  $\widehat{\psi}(q) = q$  e  $\widehat{\psi}(x) = x$  per ogni  $x \in H$ . Siccome  $p, q, r$  sono un sistema di riferimento di  $\overline{pr}$  ne segue che  $\overline{pr} \subset \text{Fix}(\widehat{\psi})$  e siccome  $\overline{pr} \cap H \neq \emptyset$  si ha che  $\text{Fix}(\widehat{\psi})$  contiene il sottospazio proiettivo  $\overline{pr} + H$ . Per induzione  $\widehat{\psi}$  è composizione di proiezioni. Per concludere basta allora osservare che

$$\phi = \psi_2 \psi_1 \varphi_1 \varphi_2 \psi = \psi_2 \psi_1 \widehat{\psi}.$$

*Secondo caso,  $\text{Fix}(\psi) = H$ .* Supponiamo adesso che  $H = \text{Fix}(\psi)$ . Prendiamo un qualsiasi punto  $p \in L - H$ , denotiamo  $q = \psi(p)$  e prendiamo un iperpiano  $M \subset \mathbb{P}^n$  tale che  $H \subset M$  e  $p, q \notin M$ .

Come prima sia  $o \notin L \cup M$  e  $\varphi_1: L \rightarrow M$  la proiezione di centro  $o$ . Sia poi  $\varphi_2: M \rightarrow L$  la proiezione con centro un qualsiasi punto appartenente alla retta  $\overline{q\varphi_1(p)}$ . Allora  $\varphi_2 \varphi_1(p) = q$  e dunque la proiettività  $\varphi_1^{-1} \varphi_2^{-1} \psi$  contiene sia  $H$  che  $p$  nel suo luogo fisso e ci si riconduce al caso precedentemente trattato. □

### 7.8. Prospettive

**TEOREMA 7.8.1.** *Per una proiettività  $\psi: \mathbb{P}^n \rightarrow \mathbb{P}^n$  le seguenti condizioni sono equivalenti:*

- (1) *i punti fissi di  $\psi$  contengono un iperpiano  $H$ ;*
- (2) *esiste un punto  $o \in \mathbb{P}^n$  tale che  $\psi(o) = o$  e  $\psi(p) \in \overline{op}$  per ogni  $p \neq o$ ;*
- (3) *esiste un sistema di riferimento proiettivo  $p_0, \dots, p_{n+1}$  tale che  $\psi(p_0) = p_0$  e  $\psi(p_i) \in \overline{p_0 p_i}$  per ogni  $i = 1, \dots, n+1$ .*

*Inoltre, se  $n > 1$  e  $\psi \neq \text{Id}$  soddisfa le precedenti condizioni, allora il punto  $o$  e l'iperpiano  $H$  sono unici e  $\text{Fix}(\psi) = H \cup \{o\}$ .*

**DIMOSTRAZIONE.** Possiamo chiaramente supporre  $\psi$  diversa dall'identità.

[1 implica 2]: Osserviamo innanzitutto che la condizione 2) è del tutto equivalente a dire che  $\psi(p) \in o + p$  per ogni  $p \in \mathbb{P}^n$ . Sia  $\psi = [f]$  e fissiamo una base  $v_0, \dots, v_n$  tale che  $[v_i] \in H$  per ogni  $i = 1, \dots, n$ . La restrizione di  $\psi$  ad  $H$  è l'identità, quindi a meno di moltiplicare  $f$  per uno scalare possiamo supporre  $f(v_i) = v_i$  per ogni  $i > 0$ . Se  $f(v_0) = \sum_{i=0}^n a_i v_i$  consideriamo il punto  $o = [f(v_0) - v_0]$ . Allora per ogni vettore  $w = \sum b_i v_i$  si ha

$$f(w) = b_0 f(v_0) + f(w - b_0 v_0) = b_0 f(v_0) + w - b_0 v_0 = b_0 (f(v_0) - v_0) + w,$$

ed in particolare  $f(w) \in \text{Span}(f(v_0) - v_0, w)$ .

[2 implica 3]: Basta estendere il punto  $o$  ad un sistema di riferimento proiettivo.

[3 implica 1]: Possiamo prendere una base  $v_0, \dots, v_n$  di  $\mathbb{K}^{n+1}$  tale che  $p_i = [v_i]$  per ogni  $i$  e  $p_{n+1} = [v_0 + \dots + v_n]$ . Siccome  $\psi(p_0) = p_0$  esiste un unico isomorfismo lineare  $f$  che induce  $\psi$  e tale che  $f(v_0) = v_0$ . Per ipotesi esistono  $a_i, b_i \in \mathbb{K}$ ,  $i = 1, \dots, n+1$  tali che

$$f(v_i) = a_i v_0 + b_i v_i, \quad i = 1, \dots, n$$

$$f\left(\sum v_i\right) = a_{n+1} v_0 + b_{n+1} \sum v_i.$$

Ponendo, per semplicità notazionale  $b = b_{n+1}$  si ha

$$a_{n+1} v_0 + b \sum v_i = f\left(\sum v_i\right) = \sum f(v_i) = v_0 + \sum_{i=1}^n (a_i v_0 + b_i v_i)$$

e dato che  $v_0, \dots, v_n$  sono linearmente indipendenti si ricava in particolare che  $b_i = b \neq 0$  per ogni  $i = 1, \dots, n$ . Dunque, in tale base, la proiettività  $\psi$  è indotta dall'applicazione lineare definita dalla matrice

$$A = \begin{pmatrix} a_0 & a_1 & a_2 & \cdots & a_n \\ 0 & b & 0 & \cdots & 0 \\ 0 & 0 & b & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & b \end{pmatrix}, \quad a_0, b \neq 0, \quad a_1, \dots, a_n \in \mathbb{K}.$$

Siccome  $A$  non è un multiplo dell'identità (altrimenti  $\psi = \text{Id}$ ), l'autovalore  $b$  ha molteplicità geometrica  $n$  e quindi un iperpiano di punti fissi per  $\psi$  è

$$\mathbb{P}(\ker(A - bI)) = \{[x_0, \dots, x_n] \mid (a_0 - b)x_0 + \sum_{i=1}^n a_i x_i = 0\}.$$

Per future applicazioni osserviamo che, poiché  $A$  è definita a meno di moltiplicazione per scalari non nulli, non è restrittivo assumere  $a_0 = 1$  oppure  $b = 1$ .

Mostriamo adesso che se  $n > 1$  e  $\psi \neq \text{Id}$  allora  $o$  ed  $H$  sono unici. L'unicità di  $H$  è facile: infatti se  $M$  è un altro iperpiano di punti fissi, siccome  $n > 1$  si ha  $H \cap M \neq \emptyset$  e quindi  $\mathbb{P}^n = H + M \subset \text{Fix}(\psi)$  per il Lemma 7.7.1.

Sia  $q \neq o$  un punto tale che  $\psi(q) = q$  e  $\psi(p) \in \overline{pq}$  per ogni  $p \neq q$ . Allora possiamo completare  $o, q$  ad un sistema di riferimento proiettivo  $o, q, p_1, \dots, p_n$ . Siccome  $n > 1$ , per ogni  $i = 1, \dots, n$  i punti  $o, q, p_i$  non sono allineati e quindi le due rette  $\overline{op_i}$  e  $\overline{qp_i}$  si intersecano nell'unico punto  $p_i$ . Quindi

$$\psi(p_i) \in \overline{op_i} \cap \overline{qp_i} = \{p_i\}$$

da cui segue che  $\psi$  lascia fisso un sistema di riferimento proiettivo, ma questo è possibile solo se  $\psi = \text{Id}$ .

Per finire, dimostriamo che se  $n > 1$  e  $\psi \neq \text{Id}$  allora non esistono altri punti fissi oltre  $o$  ed  $H$ , ossia  $\text{Fix}(\psi) = H \cup \{o\}$ . Sia  $q$  un punto fisso di  $\psi$ ; se  $q \notin H$  allora ogni retta  $L$  passante per  $q$  viene trasformata in se stessa da  $\psi$ . Infatti  $L \not\subset H$  e quindi  $L$  interseca  $H$  in un unico punto, diciamo  $r = L \cap H$ ,  $r \neq q$ . Allora  $L = \overline{qr}$  e  $\psi(L) = \overline{\psi(q)\psi(r)} = L$ , in contraddizione con l'unicità del punto  $o$ .  $\square$

**DEFINIZIONE 7.8.2.** Una proiettività  $\psi: \mathbb{P}^n \rightarrow \mathbb{P}^n$  che soddisfa le tre condizioni equivalenti del Teorema 7.8.1 viene detta **prospettiva**.

Qualora  $n > 2$  e  $\psi$  non sia l'identità, l'iperpiano  $H$  viene detto **asse di prospettiva** ed il punto  $o$  **centro di prospettiva**.

Osservando con un pizzico di attenzione la dimostrazione del Teorema 7.8.1 si osserva che entrambe le possibilità  $o \notin H$  e  $o \in H$  sono possibili. Più precisamente, se  $\psi$  è una prospettiva indotta da un endomorfismo lineare  $f: V \rightarrow V$ , allora vale  $o \notin H$  se e solo se  $f$  è diagonalizzabile (1 autovalore di molteplicità geometrica  $n$  ed un altro di molteplicità geometrica 1), mentre vale  $o \in H$  se e solo se  $f$  non è diagonalizzabile (1 autovalore di molteplicità algebrica  $n + 1$  e molteplicità geometrica  $n$ .)

**DEFINIZIONE 7.8.3.** Una prospettiva di centro  $o$  ed asse  $H$  viene detta: **omologia**<sup>4</sup> se  $o \notin H$ ; **trasvezione** od **omologia speciale** se  $o \in H$ .

**OSSERVAZIONE 7.8.4.** Per quanto dimostrato in precedenza le nozioni di omologia e trasvezione sono ben definite per prospettive diverse dall'identità su spazi proiettivi di dimensione maggiore di 1. Tuttavia possiamo estendere in maniera ovvia tali nozioni anche a prospettive diverse dall'identità su  $\mathbb{P}^1$ : omologia se ha due punti fissi, trasvezione se ha un solo punto fisso. Siccome tre punti distinti di  $\mathbb{P}^1$  formano un sistema di riferimento, l'unica proiettività con più di due punti fissi è l'identità.

Sia  $\psi: \mathbb{P}^n \rightarrow \mathbb{P}^n$  una prospettiva di centro  $o$  e siano  $L, M \subset \mathbb{P}^n$  due iperpiani tali che  $o \notin M$  e  $\psi(L) \subset M$ . Allora la restrizione  $\psi|_L: L \rightarrow M$  ha una evidente interpretazione geometrica. Osserviamo innanzitutto che  $o \notin L$ , altrimenti  $o = \psi(o) \in M$ , e quindi per ogni  $p \in L$  abbiamo una retta  $\overline{op}$  che interseca  $M$  in un unico punto.

Siano  $L, M \subset \mathbb{P}^n$  due iperpiani,  $p, q \notin L \cup M$  due punti e

$$\phi_p, \phi_q: L \rightarrow M$$

le proiezioni di centro  $p$  e  $q$  rispettivamente. Allora l'applicazione

$$\psi = \phi_q \phi_p^{-1}: M \rightarrow M$$

è una prospettiva di centro  $o = M \cap \overline{pq}$  ed asse  $H = L \cap M$ . Infatti  $H$  è un iperpiano di  $M$  di punti fissi di  $\psi$  e per ogni  $r \in M$  il punto  $\psi(r)$  appartiene all'intersezione di  $M$  con il piano  $p + q + r$ , ossia  $\psi(r) \in \overline{or}$  (Figura 10).

**LEMMA 7.8.5.** *Siano  $L, M \subset \mathbb{P}^n$  due iperpiani distinti ed  $o \notin L \cup M$ . Esiste allora una unica prospettiva  $\psi: \mathbb{P}^n \rightarrow \mathbb{P}^n$  di centro  $o$  e tale che  $\psi(L) = M$ ,  $\psi(M) = L$ . Inoltre:*

- (1) *la prospettiva  $\psi$  è una involuzione, ossia  $\psi^2 = \text{Id}$ , ed è una omologia se e solo se il campo ha caratteristica  $\neq 2$ .*
- (2) *le restrizioni  $\psi: L \rightarrow M$  e  $\psi: M \rightarrow L$  coincidono con le proiezioni di centro  $o$ .*

**DIMOSTRAZIONE.** Fissiamo un sistema di coordinate omogenee  $x_0, \dots, x_n$  tale che

$$o = [1, 0, \dots, 0], \quad L \cap M = \{x_0 = x_1 = 0\}.$$

Le equazioni di  $L, M$  saranno allora del tipo

$$L = \{x_0 = lx_1\}, \quad M = \{x_0 = mx_1\}, \quad l, m \in \mathbb{K}.$$

<sup>4</sup>Nulla a che vedere con l'analogo concetto in algebra omologica.

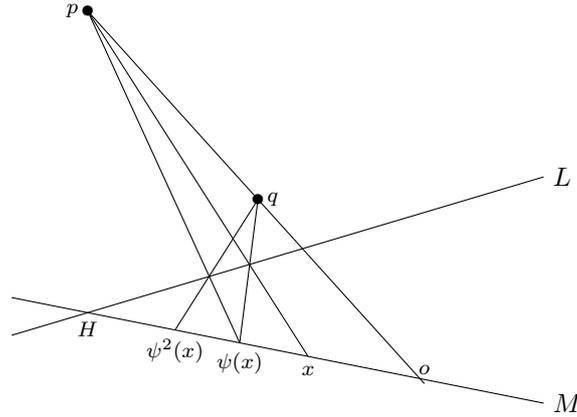


FIGURA 10. Una prospettiva  $\psi: M \rightarrow M$  di centro  $o$  ed asse  $H = L \cap M$ , composizione della proiezione  $M \rightarrow L$  di centro  $p$  e della proiezione  $L \rightarrow M$  di centro  $q$ .

Il ragionamento fatto nella dimostrazione del Teorema 7.8.1 mostra che le prospettive di centro  $o$  sono tutte e sole le proiettività rappresentate da una matrice della forma

$$A = \begin{pmatrix} 1 & a_1 & a_2 & \cdots & a_n \\ 0 & b & 0 & \cdots & 0 \\ 0 & 0 & b & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & b \end{pmatrix}, \quad b \neq 0, \quad a_1, \dots, a_n \in \mathbb{K}.$$

Si considerino i due punti  $p = [l, 1, 0, \dots, 0] \in L$  e  $q = [m, 1, 0, \dots, 0] \in M$ . Poiché

$$L = (L \cap M) + p, \quad M = (L \cap M) + q,$$

le due condizioni  $\psi(L) = M$ ,  $\psi(M) = L$  sono equivalenti alle tre condizioni

$$\psi(L \cap M) \subset L \cap M, \quad \psi(p) \in M, \quad \psi(q) \in L.$$

La condizione  $\psi(L \cap M) \subset L \cap M$  è equivalente all'annullamento  $a_2 = \dots = a_n = 0$ , mentre le condizioni  $\psi(p) \in M$  e  $\psi(q) \in L$  equivalgono al sistema lineare nelle incognite  $a_1, b$

$$l + a_1 = mb, \quad m + a_1 = lb$$

che ha come unica soluzione  $b = -1$  e  $a_1 = -l - m$ . La verifica che  $A^2 = I$  è immediata.  $\square$

**COROLLARIO 7.8.6.** *Dati tre punti distinti  $o, p, q \in \mathbb{P}^1$  esiste una prospettiva  $\psi$  di centro  $o$  tale che  $\psi(p) = q$  e  $\psi(q) = p$ .*

**LEMMA 7.8.7.** *Sia  $U \subset \mathbb{P}^n$  sottospazio proiettivo e  $\psi: U \rightarrow U$  una prospettiva di centro  $o$  ed asse  $H$ . Allora  $\psi$  si estende ad una prospettiva  $\phi: \mathbb{P}^n \rightarrow \mathbb{P}^n$  di centro  $o$  il cui asse contiene  $H$ .*

**DIMOSTRAZIONE.** Se  $U = \mathbb{P}(V)$  con  $V \subset \mathbb{K}^{n+1}$ , possiamo scegliere una base  $v_0, \dots, v_n$  tale che  $v_0, \dots, v_p$  sia una base di  $V$  e  $v_1, \dots, v_p$  base dell'asse di prospettiva. Possiamo allora rappresentare la prospettiva con  $f: V \rightarrow V$  lineare e tale che  $f(v_i) = v_i$  per  $0 < i \leq p$ . Basta allora estendere  $f$  ponendo  $f(v_i) = v_i$  per ogni  $i > 0$ .  $\square$

**TEOREMA 7.8.8.** *Sia  $\psi$  una proiettività di  $\mathbb{P}^n$  e sia  $H \subset \text{Fix}(\psi)$  un sottospazio proiettivo di dimensione  $r \leq n$ . Allora  $\psi$  è composizione di  $s \leq n - r$  prospettive i cui assi contengono  $H$ .*

**DIMOSTRAZIONE.** Se  $n - r \leq 1$  non c'è nulla da dimostrare, per induzione su  $r$  basta provare che esiste una prospettiva  $\phi$  tale che  $\phi^{-1}\psi$  contiene un sottospazio di punti fissi di dimensione  $> r$ . Scegliamo  $p \notin \text{Fix}(\psi)$  e denotiamo  $q = \psi(p) \neq p$

Se  $H = \emptyset$  per il Corollario 7.8.6 esiste una prospettiva  $\phi$  della retta  $\overline{pq}$  tale che  $\phi(p) = q$ . Possiamo estendere  $\phi$  ad una prospettiva di  $\mathbb{P}^n$  e la proiettività  $\phi^{-1}\psi$  possiede  $p$  come punto fisso.

Se  $H \neq \emptyset$  denotiamo  $L = H + p$ ,  $\dim L = r + 1$ . Se  $q \in L$ , allora  $\psi(L) = L$  e la restrizione di  $\psi$  a  $L$  è una prospettiva che si può estendere ad una prospettiva  $\phi$  di  $\mathbb{P}^n$ . Allora la proiettività  $\phi^{-1}\psi$  contiene  $L$  come luogo di punti fissi.

Se  $q \notin L$  allora  $\overline{pq} \cap H = \emptyset$  scegliamo un qualunque punto  $r \in H$ , allora  $q \notin \overline{rp}$ ,  $\psi(\overline{rp}) = \overline{rq}$ , le due rette  $\overline{rp}$  e  $\overline{rq}$  sono contenute nel piano  $P$  contenente i tre punti non allineati  $p, q, r$ . Poniamo  $M = H + q$  e  $K = H + P$ .  $L$  ed  $M$  sono iperpiani di  $K$  che si intersecano in  $H$ .

Scegliamo un punto  $s \in \overline{rp}$  diverso da  $r, p$  e poniamo  $t = \psi(s)$ . Sia  $o \in P$  il punto di intersezione delle rette  $\overline{pq}$  e  $\overline{st}$ . Sia  $\phi: K \rightarrow K$  una prospettiva di centro  $o$  e tale che  $\phi(L) = M$  ed estendiamola ad una prospettiva su  $\mathbb{P}^n$  di centro  $o$  ed asse contenente  $H$ . Necessariamente  $\phi(p) = q$ ,  $\phi(s) = t$  e quindi  $p, s, r$  sono punti fissi di  $\phi^{-1}\psi$ . Essendo  $p, s, r$  un sistema di riferimento in  $\overline{rp}$ , anche la retta  $\overline{pr}$  è contenuta nel luogo fisso di  $\phi^{-1}\psi$ . Poiché  $\overline{rp} \cap H \neq \emptyset$  ne segue che anche  $L$  è contenuto nel luogo fisso di  $\phi^{-1}\psi$ .  $\square$

### Esercizi

ESERCIZIO 45. Siano date  $n$  rette proiettive  $L_1, \dots, L_n \subset \mathbb{P}^n$ , nessuna delle quali contenuta nell'iperpiano  $H_0 = \{x_0 = 0\}$ . Scriviamo  $\mathbb{P}^n = \mathbb{K}^n \cup H_0$ , per ogni  $i = 1, \dots, n$  esiste una rappresentazione parametrica della retta affine  $L_i \cap \mathbb{K}^n$  che possiamo scrivere nella forma

$$L_i = \{[1, a_{i1}t + b_{i1}, \dots, a_{in}t + b_{in}] \mid t \in \mathbb{K}\}.$$

Provare che gli  $n$  punti di intersezione delle rette  $L_1, \dots, L_n$  con l'iperpiano  $H_0$  sono proiettivamente indipendenti se e solo se  $\det(a_{ij}) \neq 0$ .

ESERCIZIO 46 (\*). Siano date quattro rette  $L_1, \dots, L_4 \subset \mathbb{P}^3(\mathbb{C})$ . Provare che esiste almeno una retta in  $\mathbb{P}^3$  che le interseca tutte e quattro. (Sugg.: se esiste un punto  $o$  appartenente all'intersezione di due rette distinte  $L_i, L_j$  considerare la proiezione di centro  $o$ . Altrimenti si prendano coordinate omogenee tali che  $L_4 = \{x_0 = x_1 = 0\}$ ,  $L_1 = \{x_2 = x_3 = 0\}$  e si consideri l'intersezione delle rette con i piani del fascio  $F_t = \{x_1 = tx_0\}$ , per  $t \in \mathbb{K}$ . Ad un certo punto servirà il risultato dell'Esercizio 45.)

## 7.9. Il birapporto

Sia  $\mathbb{P}(V)$  uno spazio proiettivo di dimensione 1. Abbiamo visto che per ogni terna di punti distinti  $p_2, p_3, p_4$  di  $\mathbb{P}(V)$  esiste un'unica proiettività  $\phi: \mathbb{P}(V) \rightarrow \mathbb{P}^1$  tale che:

$$\phi(p_2) = 1 = [1, 1], \quad \phi(p_3) = 0 = [1, 0] \quad \text{e} \quad \phi(p_4) = \infty = [0, 1].$$

Nelle precedenti uguaglianze  $[0, 1] = \infty$  e  $[1, t] = t$ , abbiamo identificato  $\mathbb{P}^1$  con  $\mathbb{K} \cup \{\infty\}$  nel modo standard, ossia tramite il processo di disomogeneizzazione  $[x_0, x_1] \leftrightarrow x_1/x_0$ .

È allora chiaro che dati quattro punti distinti  $p_1, \dots, p_4 \in \mathbb{P}(V)$ , esistono un'unica proiettività  $\phi: \mathbb{P}(V) \rightarrow \mathbb{P}^1$  ed un elemento  $\lambda \in \mathbb{K} - \{0, 1\}$  tali che

$$\phi(p_1) = \lambda = [1, \lambda], \quad \phi(p_2) = 1 = [1, 1], \quad \phi(p_3) = 0 = [1, 0] \quad \text{e} \quad \phi(p_4) = \infty = [0, 1].$$

DEFINIZIONE 7.9.1. Nella situazione precedente, la quantità  $\lambda = [p_1, p_2; p_3, p_4]$  si dice **birapporto**<sup>5</sup> della quaterna ordinata  $p_1, \dots, p_4$ .

È immediato osservare che per ogni  $\lambda \in \mathbb{P}^1 = \mathbb{K} \cup \{\infty\}$ ,  $\lambda \neq 0, 1, \infty$ , allora  $\lambda = [\lambda, 1; 0, \infty]$ . In particolare, il birapporto può assumere qualsiasi valore in  $\mathbb{K} - \{0, 1\}$ .

PROPOSIZIONE 7.9.2. Siano  $\mathbb{P}(V)$  e  $\mathbb{P}(U)$  due rette proiettive e  $p_1, \dots, p_4 \in \mathbb{P}(V)$ ,  $q_1, \dots, q_4 \in \mathbb{P}(U)$  due quaterne di punti distinti. Allora esiste una proiettività  $\phi: \mathbb{P}(V) \rightarrow \mathbb{P}(U)$  tale che  $\phi(p_i) = q_i$  per ogni  $i$  se e solo se  $[p_1, p_2; p_3, p_4] = [q_1, q_2; q_3, q_4]$ .

<sup>5</sup>In inglese *cross ratio*; in francese *rapport anharmonique*.

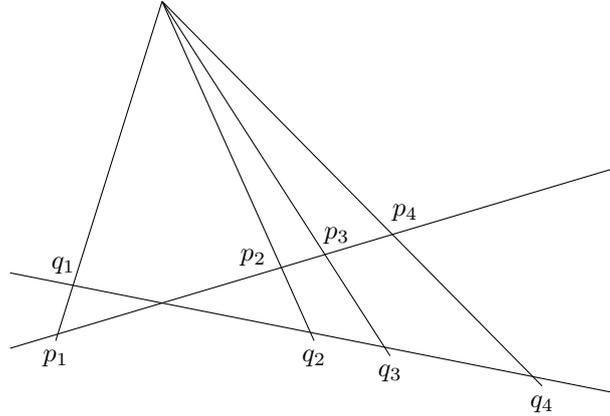


FIGURA 11. Le due quaterne  $p_1, p_2, p_3, p_4$  e  $q_1, q_2, q_3, q_4$  hanno lo stesso birapporto.

DIMOSTRAZIONE. Siano  $\eta: \mathbb{P}(V) \rightarrow \mathbb{P}^1$  e  $\mu: \mathbb{P}(U) \rightarrow \mathbb{P}^1$  le uniche proiettività tali che

$$\eta(p_2) = \mu(q_2) = 1, \quad \eta(p_3) = \mu(q_3) = 0, \quad \eta(p_4) = \mu(q_4) = \infty.$$

Allora  $\phi = \mu^{-1}\eta: \mathbb{P}(V) \rightarrow \mathbb{P}(U)$  coincide con l'unica proiettività tale che  $\phi(p_i) = q_i$ ,  $i = 2, 3, 4$ .

Ma allora  $\phi(p_1) = q_1$  se e solo se  $\eta(p_1) = \mu(q_1)$ , ossia se e solo se le due quaterne hanno lo stesso birapporto.  $\square$

Dunque il birapporto è invariante per proiettività e quindi è invariante per prospettive e proiezioni (Figura 11).

Il nome birapporto è motivato dalla formula

$$[p_1, p_2; p_3, p_4] = \frac{p_3 - p_1}{p_3 - p_2} : \frac{p_4 - p_1}{p_4 - p_2}$$

da interpretarsi come nella seguente proposizione.

PROPOSIZIONE 7.9.3. Siano  $p_1 = [x_1, y_1], \dots, p_4 = [x_4, y_4]$  punti distinti di  $\mathbb{P}^1$ . Allora vale la formula

$$(7.10) \quad [p_1, p_2; p_3, p_4] = \frac{\begin{vmatrix} x_1 & x_3 \\ y_1 & y_3 \end{vmatrix}}{\begin{vmatrix} x_2 & x_3 \\ y_2 & y_3 \end{vmatrix}} : \frac{\begin{vmatrix} x_1 & x_4 \\ y_1 & y_4 \end{vmatrix}}{\begin{vmatrix} x_2 & x_4 \\ y_2 & y_4 \end{vmatrix}} = \frac{x_1 y_3 - x_3 y_1}{x_2 y_3 - x_3 y_2} : \frac{x_1 y_4 - x_4 y_1}{x_2 y_4 - x_4 y_2},$$

che nelle coordinate affini  $t_i = \frac{y_i}{x_i} \in \mathbb{K} \cup \{\infty\}$ , diventa

$$(7.11) \quad [p_1, p_2; p_3, p_4] = \frac{t_3 - t_1}{t_3 - t_2} : \frac{t_4 - t_1}{t_4 - t_2}.$$

DIMOSTRAZIONE. Osserviamo preliminarmente che la Formula (7.10) è ben definita, ossia è invariante per moltiplicazione della coppia  $x_i, y_i$  per uno scalare non nullo, ed applicata alla quaterna

$$p_1 = [1, \lambda], \quad p_2 = [1, 1], \quad p_3 = [1, 0], \quad p_4 = [0, 1],$$

restituisce il valore  $[p_1, p_2; p_3, p_4] = \lambda$ . Basta quindi provare che la Formula (7.10) è invariante per proiettività.

Sia  $\phi: \mathbb{P}^1 \rightarrow \mathbb{P}^1$  una proiettività indotta da una matrice invertibile  $A \in \text{GL}_2(\mathbb{K})$ . Per ogni indice  $i$  si ha

$$\phi(p_i) = [z_i, w_i], \quad \text{con} \quad A \begin{pmatrix} x_i \\ y_i \end{pmatrix} = \begin{pmatrix} z_i \\ w_i \end{pmatrix}.$$

Per il teorema di Binet, per ogni coppia di indici  $i, j$  si ha:

$$A \begin{pmatrix} x_i & x_j \\ y_i & y_j \end{pmatrix} = \begin{pmatrix} z_i & z_j \\ w_i & w_j \end{pmatrix}, \quad \det(A) \begin{vmatrix} x_i & x_j \\ y_i & y_j \end{vmatrix} = \begin{vmatrix} z_i & z_j \\ w_i & w_j \end{vmatrix},$$

e di conseguenza

$$\frac{\begin{vmatrix} z_1 & z_3 \\ w_1 & w_3 \end{vmatrix}}{\begin{vmatrix} z_2 & z_3 \\ w_2 & w_3 \end{vmatrix}} : \frac{\begin{vmatrix} z_1 & z_4 \\ w_1 & w_4 \end{vmatrix}}{\begin{vmatrix} z_2 & z_4 \\ w_2 & w_4 \end{vmatrix}} = \frac{\begin{vmatrix} x_1 & x_3 \\ y_1 & y_3 \end{vmatrix}}{\begin{vmatrix} x_2 & x_3 \\ y_2 & y_3 \end{vmatrix}} : \frac{\begin{vmatrix} x_1 & x_4 \\ y_1 & y_4 \end{vmatrix}}{\begin{vmatrix} x_2 & x_4 \\ y_2 & y_4 \end{vmatrix}}.$$

□

DEFINIZIONE 7.9.4. Denotiamo con  $\Sigma_4$  il gruppo delle permutazioni dell'insieme  $\{1, 2, 3, 4\}$ . Il **gruppo trirettangolo**<sup>6</sup>  $\Gamma_4$  è il sottogruppo di  $\Sigma_4$  formato dall'identità e dalle tre permutazioni<sup>7</sup> di ordine 2

$$\sigma_1 = (2, 1, 4, 3), \quad \sigma_2 = (3, 4, 1, 2), \quad \sigma_3 = (4, 3, 2, 1).$$

Il birapporto di una quaterna dipende dall'ordine in cui vengono presi i punti. Tuttavia segue immediatamente dalle Formule (7.10) e (7.11) che per ogni quaterna di punti distinti  $p_1, \dots, p_4$  si ha:

$$[p_1, p_2; p_3, p_4] = [p_2, p_1; p_4, p_3] = [p_3, p_4; p_1, p_2] = [p_4, p_3; p_2, p_1].$$

Possiamo esprimere questo fatto dicendo che *il birapporto è invariante per l'azione del gruppo trirettangolo*.

Più in generale è naturale chiedersi come agisce  $\Sigma_4$  sul birapporto: in altri termini, data una permutazione  $\sigma \in \Sigma_4$ , siamo interessati alla relazione esistente tra i due birapporti  $[p_1, p_2; p_3, p_4]$  e  $[p_{\sigma(1)}, p_{\sigma(2)}; p_{\sigma(3)}, p_{\sigma(4)}]$ .

Siccome ogni permutazione  $\sigma$  si scrive in modo unico nella forma  $\gamma\tau$ , con  $\gamma \in \Gamma_4$ ,  $\gamma(4) = \sigma(4)$  e  $\tau(4) = 4$ , basta vedere come cambia il birapporto per effetto delle 6 permutazioni che fissano il numero 4.

LEMMA 7.9.5. Sia  $\lambda = [p_1, p_2; p_3, p_4]$  il birapporto di una quaterna di punti distinti sulla retta proiettiva. Allora si hanno le 6 uguaglianze:

$$\begin{aligned} [p_1, p_2; p_3, p_4] = \lambda & \quad [p_2, p_3; p_1, p_4] = \frac{\lambda - 1}{\lambda} & \quad [p_3, p_1; p_2, p_4] = \frac{1}{1 - \lambda} \\ [p_2, p_1; p_3, p_4] = \frac{1}{\lambda} & \quad [p_3, p_2; p_1, p_4] = \frac{\lambda}{\lambda - 1} & \quad [p_1, p_3; p_2, p_4] = 1 - \lambda \end{aligned}$$

DIMOSTRAZIONE. La dimostrazione non presenta alcuna difficoltà, anche perché possiamo sempre trovare un sistema di coordinate affini tali che

$$p_1 = \lambda, \quad p_2 = 1, \quad p_3 = 0, \quad p_4 = \infty.$$

□

Possiamo riassumere le precedenti considerazioni nel seguente risultato:

LEMMA 7.9.6. Il birapporto di una quaterna di punti distinti di  $\mathbb{P}^1$  è invariante per l'azione del gruppo trirettangolo. Se  $[p_1, p_2; p_3, p_4] = \lambda$ , allora sotto l'azione del gruppo simmetrico il birapporto assume i valori

$$(7.12) \quad \lambda, \quad \frac{1}{\lambda}, \quad 1 - \lambda, \quad 1 - \frac{1}{\lambda}, \quad \frac{1}{1 - \lambda}, \quad \frac{\lambda}{\lambda - 1}.$$

Per un generico  $\lambda \in \mathbb{K} - \{0, 1\}$  le sei espressioni in (7.12) forniscono sei birapporti distinti; si hanno tuttavia le seguenti eccezioni:

- (1) Caratteristica  $\neq 2$  e  $\lambda = -1, 2, \frac{1}{2}$ . In questo caso la quaterna è detta **armonica**.

<sup>6</sup>In inglese *Klein fourgroup*.

<sup>7</sup>Con la notazione  $\sigma = (a_1, \dots, a_n)$  si intende la permutazione tale che  $\sigma(i) = a_i$ .

- (2) Caratteristica  $\neq 3$ ,  $\xi^2 - \xi + 1 = 0$  e  $\lambda = \xi, \xi^{-1}$ . In questo caso la quaterna è detta **equianarmonica**.

Lasciamo per esercizio la verifica delle seguenti affermazioni, la prima delle quali giustifica il termine di quaterna armonica:

- (1) In caratteristica  $\neq 2$ , dati tre valori distinti  $\lambda_1, \lambda_2, \lambda_3 \in \mathbb{K} - \{0\}$  si ha  $[0, \lambda_1; \lambda_2, \lambda_3] = -1$  se e solo se  $\lambda_1$  è la media armonica di  $\lambda_2, \lambda_3$ , ossia se e solo se

$$\lambda_1 = \frac{2}{\frac{1}{\lambda_2} + \frac{1}{\lambda_3}} = \frac{2\lambda_2\lambda_3}{\lambda_2 + \lambda_3}.$$

In particolare per ogni  $x \in \mathbb{K}$  si ha

$$\left[0, \frac{1}{x}; \frac{1}{x-1}, \frac{1}{x+1}\right] = \left[\frac{1}{x+1}, \frac{1}{x-1}; \frac{1}{x}, 0\right] = \left[\frac{1}{x+1}, \frac{1}{x-1}; 0, \frac{1}{x}\right] = -1.$$

- (2) Mentre non ha senso definire le quaterne armoniche in caratteristica 2 in quanto  $-1 = 1$  e  $2 = 0$ , avrebbe senso considerare le quaterne equianarmoniche anche in caratteristica 3; tuttavia, in tal caso si ha  $\xi^2 - \xi + 1 = (1 + \xi)^2 = (1 - 2\xi)^2 = (2 - \xi)^2$  e quindi si ricade nel caso armonico. Si noti inoltre che, sempre in caratteristica 3 si hanno le uguaglianze  $-1 = 2 = 1/2$  e quindi nelle quaterne armoniche il birapporto è invariante per permutazioni.
- (3) Su  $\mathbb{C}$ , rappresentato dal piano di Gauss, la quaterna formata dai vertici di un triangolo equilatero e dal suo baricentro è equianarmonica, mentre i vertici di un quadrato formano una quaterna armonica.

**TEOREMA 7.9.7 (Quadrilatero armonico).** *Sia  $\mathbb{P}^2$  il piano proiettivo su di un campo di caratteristica  $\neq 2$ , e siano  $a, b, c, d \in \mathbb{P}^2$  i vertici di un quadrilatero completo non degenere, ossia con nessuna terna allineata. Allora i seguenti 4 punti allineati (Figura 12):*

$$p_1 = \overline{ab} \cap \overline{cd}, \quad p_2 = \overline{ac} \cap \overline{bd}, \quad p_3 = \overline{p_1p_2} \cap \overline{bc}, \quad p_4 = \overline{p_1p_2} \cap \overline{ad}.$$

*formano una quaterna armonica, e più precisamente  $[p_1, p_2; p_3, p_4] = -1$ .*

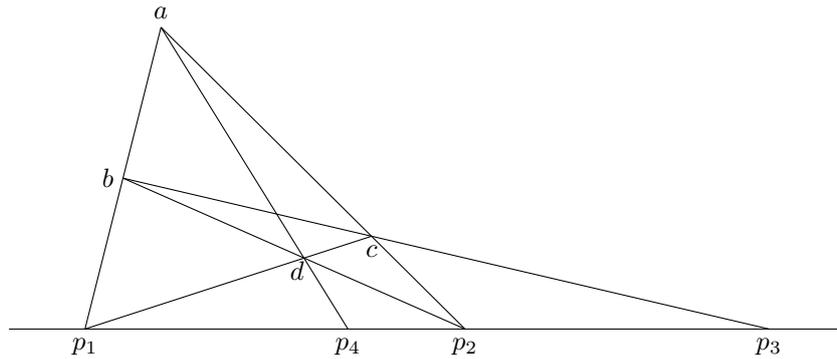
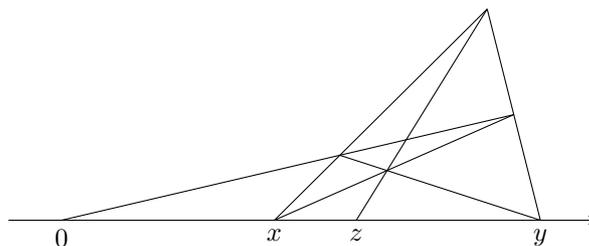


FIGURA 12. Il quadrilatero “armonico”:  $[p_1, p_2; p_3, p_4] = [p_3, p_4; p_1, p_2] = -1$ .

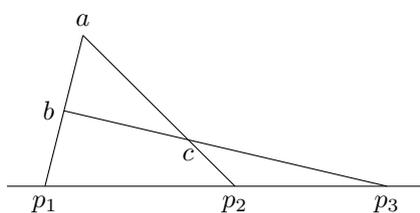
**DIMOSTRAZIONE.** Sia  $[p_1, p_2; p_3, p_4] = \lambda \neq 1, 0$  e di conseguenza  $[p_2, p_1; p_3, p_4] = \lambda^{-1}$ . Si considerino adesso le due prospettive  $\overline{p_1p_2} \rightarrow \overline{ad}$  di centro  $b$  e  $\overline{ad} \rightarrow \overline{p_1p_2}$  di centro  $c$ . Se indichiamo con  $o$  il punto di intersezione di  $\overline{ad}$  e  $\overline{bc}$ , dalla prima prospettiva ricaviamo che  $[p_1, p_2; p_3, p_4] = [a, d; o, p_4]$  e dalla seconda che  $[a, d; o, p_4] = [p_2, p_1; p_3, p_4]$ . Quindi

$$[p_1, p_2; p_3, p_4] = [a, d; o, p_4] = [p_2, p_1; p_3, p_4]$$

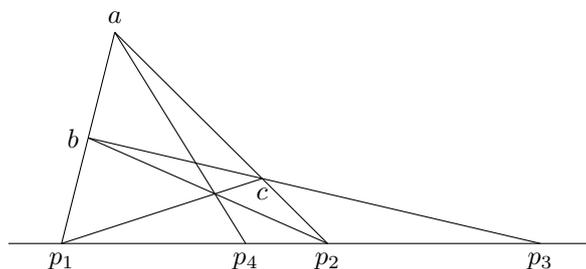
e dunque  $\lambda = \lambda^{-1}$  che ha come unica soluzione  $\lambda = -1$ .  $\square$

FIGURA 13. Il punto  $z$  è uguale alla media armonica di  $x$  e  $y$ .

Dati tre punti distinti  $p_1, p_2, p_3$  di  $\mathbb{P}^1$ , possiamo applicare il Teorema 7.9.7 per costruire “con la sola riga” l’unico punto  $p_4$  tale che  $[p_1, p_2; p_3, p_4] = -1$ . Si consideri infatti  $\mathbb{P}^1$  come una retta proiettiva  $M \subset \mathbb{P}^2$  e per ogni  $i = 1, 2, 3$  si prenda una qualunque retta proiettiva  $L_i$  tale che  $L_i \cap M = p_i$ . Denotiamo  $a = L_1 \cap L_2$ ,  $b = L_1 \cap L_3$  e  $c = L_2 \cap L_3$ :

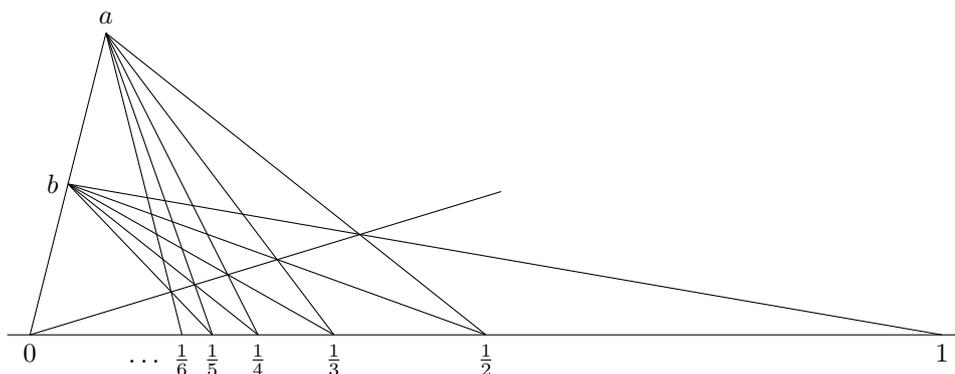


Adesso si definisca  $d$  come il punto di intersezione delle rette  $\overline{p_1c}$  e  $\overline{p_2b}$ , allora il punto cercato  $p_4$  è dato dall’intersezione di  $M$  con  $\overline{ad}$ :



La precedente costruzione si applica anche per calcolare graficamente la media armonica  $z = \frac{2xy}{x+y}$  ossia l’unico numero tal che  $[x, y; 0, z] = -1$  (Figura 13).

Siccome  $[0, \frac{1}{n}; \frac{1}{n-1}, \frac{1}{n+1}] = -1$  per ogni intero positivo  $n$ , la precedente costruzione dà un metodo “con sola riga” per costruire la serie armonica partendo da  $0, 1, \frac{1}{2}$ , e ben raffigurato dal seguente disegno,



nel quale, ribadiamo, la scelta delle tre rette  $\overline{0a}$ ,  $\overline{\frac{1}{2}a}$  e  $\overline{1b}$  è arbitraria, dopo di che tutte le altre rette seguono in maniera univoca. Inoltre il disegno illustra la proiettività  $\phi(x) = x/(x+1)$  di  $\mathbb{P}^1$  ( $x$ =coordinata affine) come composizione di due proiezioni di centri  $b$  ed  $a$  rispettivamente.

### Esercizi

ESERCIZIO 47. Sia  $\mathbb{K}$  un campo infinito. Provare che per ogni  $n \geq 5$  esiste un insieme  $S \subset \mathbb{P}^1$  di  $n$  punti tale che, se  $\phi \in \text{Aut}(\mathbb{P}^1)$  e  $\phi(S) \subset S$ , allora  $\phi = Id$ .

ESERCIZIO 48. Sia  $p \in \mathbb{P}^n$  e  $G \subset \text{Aut}(\mathbb{P}^n)$  il sottogruppo delle proiettività  $\phi$  tali che  $\phi(H) \subset H$  per ogni iperpiano  $H$  contenente  $p$ . Provare che  $G$  agisce transitivamente sull'insieme degli iperpiani di  $\mathbb{P}^n$  che non contengono  $p$ .

ESERCIZIO 49. Sia  $\lambda \in \mathbb{K} - \{0, 1\}$  fissato,  $L \subset \mathbb{P}^2$  una retta e  $\pi: \mathbb{P}^2 - \{o\} \rightarrow L$  la proiezione di centro  $o \notin L$ . Definiamo un'applicazione  $\phi: \mathbb{P}^2 \rightarrow \mathbb{P}^2$  nel modo seguente:

$\phi(o) = o$  e  $\phi(p) = p$  per ogni  $p \in L$ ; se  $p \neq o$  e  $p \notin L$ , allora si pone  $r = \pi(p)$  e  $\phi(p) = q$ , dove  $q \in o + p$  è l'unico punto tale che  $[o, r; p, q] = \lambda$ .

Provare che  $\phi$  è una proiettività. Provare inoltre  $\phi$  è un'involuzione (cioè  $\phi^2 = Id$ ) se e solo se  $\lambda = -1$ .

ESERCIZIO 50. Sia  $\mathbb{K}$  algebricamente chiuso e  $\phi \in \text{Aut}(\mathbb{P}^1)$  una proiettività di ordine finito e non divisibile per la caratteristica di  $\mathbb{K}$ . Provare che  $\phi$  ha esattamente due punti fissi.

ESERCIZIO 51. (caratteristica  $\neq 2$ ) Una quaterna ordinata  $p_1, \dots, p_4$  di punti distinti di  $\mathbb{P}^1$  definisce un omomorfismo iniettivo di gruppi  $h: \Gamma_4 \rightarrow \text{PGL}(2, \mathbb{K}) = \text{Aut}(\mathbb{P}^1)$  caratterizzato dalla proprietà che per ogni permutazione  $\sigma \in \Gamma_4$  vale  $h(\sigma)(p_i) = p_{\sigma(i)}$ . Provare che non esiste alcun sollevamento di  $h$  ad un omomorfismo  $\Gamma_4 \rightarrow \text{GL}(2, \mathbb{K})$ . (Sugg.: non è restrittivo assumere  $\mathbb{K}$  algebricamente chiuso; si prenda una coordinata affine tale che la quaterna sia  $1, -1, a, -a$  con  $a \neq \pm 1$ .)

ESERCIZIO 52. Trovare un elemento di ordine 2 di  $\text{PGL}(2, \mathbb{Q})$  che non si rappresenta con elementi di ordine finito di  $\text{GL}(2, \mathbb{Q})$ .

ESERCIZIO 53. Sia  $\mathbb{K}^* = \mathbb{K} - \{0\}$  il gruppo moltiplicativo,  $n \geq 2$  un intero e si assuma che esista un sottogruppo finito  $H \subset \mathbb{K}^*$  di ordine  $d$  tale che  $\mathbb{K}^*$  è generato da  $H$  e dalle potenze  $n$ -esime di elementi di  $\mathbb{K}^*$ . Sia inoltre  $h$  il massimo divisore di  $n$  non divisibile dalla caratteristica di  $\mathbb{K}$ .

Dimostrare che per ogni sottogruppo finito  $\Gamma \subset \text{PGL}(n, \mathbb{K})$  di ordine  $m$  esiste un sottogruppo finito  $\Gamma' \subset \text{GL}(n, \mathbb{K})$  di ordine  $\leq hdm$  che si mappa surgettivamente su  $\Gamma$  tramite la proiezione naturale  $\text{GL}(n, \mathbb{K}) \rightarrow \text{PGL}(n, \mathbb{K})$ .

ESERCIZIO 54. (caratteristica  $\neq 2, 3$ ) Sia  $p_1, \dots, p_4$  una quaterna di punti distinti di  $\mathbb{P}^1$ . Provare che:

- La quaterna è armonica se e solo se il birapporto  $[p_1, \dots, p_4]$  è invariante per l'azione di un sottogruppo di ordine 8 di  $\Sigma_4$ . Dedurre che il gruppo simmetrico  $\Sigma_4$  contiene esattamente tre sottogruppi di ordine 8 (2-Sylov) tra loro coniugati ed isomorfi al gruppo diedrale  $D_4$ .
- La quaterna è equiarmonica se e solo se il birapporto  $[p_1, \dots, p_4]$  è invariante per l'azione del gruppo alterno  $A_4$ .

ESERCIZIO 55. Si consideri l'applicazione  $v_n: \mathbb{P}^1 \rightarrow \mathbb{P}^n$ , definita in coordinate omogenee da

$$v_n([x_0, x_1]) = [x_0^n, x_0^{n-1}x_1, \dots, x_0x_1^{n-1}, x_1^n].$$

Provare che, se  $p_0, \dots, p_{n+1}$  sono  $n+2$  punti distinti di  $\mathbb{P}^1$ , allora  $v_n(p_0), \dots, v_n(p_{n+1})$  è un sistema di riferimento su  $\mathbb{P}^n$ . L'applicazione  $v_n$  è detta *applicazione di Veronese*.

ESERCIZIO 56. Si consideri il piano  $\mathbb{R}^2$  con la metrica euclidea usuale, per ogni  $p \in \mathbb{R}^2$  sia  $F_p \cong \mathbb{P}_{\mathbb{R}}^1$  il fascio di rette passanti per il punto  $p$ . Verificare che l'applicazione  $F_p \rightarrow F_p$  che manda ogni retta nella sua perpendicolare è una proiettività. Tale proiettività è chiamata *involutione degli angoli retti*.

ESERCIZIO 57. Sia  $o \in \mathbb{P}^1$  e  $G$  un insieme di  $n$  punti distinti  $p_1, \dots, p_n$  di  $\mathbb{P}^1$ , con  $n \geq 2$ . Si definisce il luogo polare di  $o$  rispetto a  $G$  come l'insieme dei punti  $q \in \mathbb{P}^1$  tali che

$$\sum_{i=1}^n [o, q; p_i, \hat{o}] = 0$$

per ogni  $\hat{o} \neq o$ . Provare che se  $o = \{\infty\}$  e  $p_1, \dots, p_n \in \mathbb{K}$  sono le radici di un polinomio monico  $f$  di grado  $n$ , allora il luogo polare di  $\{\infty\}$  rispetto a  $p_1, \dots, p_n$  è l'insieme delle radici della derivata  $f'$  di  $f$ .

ESERCIZIO 58 (\*). Con l'utilizzo della sola riga dividere un rettangolo del piano euclideo in  $n$  parti uguali, per ogni  $n \geq 2$ . (Sugg.: quadrilatero armonico.)

ESERCIZIO 59. Sia  $p \in \mathbb{P}^2$ , siano  $L, H, T$  tre rette distinte di  $\mathbb{P}^2$  passanti per il punto  $p$  e  $q, r \in T$  punti distinti da  $p$ . Si consideri le proiettività  $\phi: L \rightarrow H$  e  $\psi: H \rightarrow L$  ottenute per proiezione di centro  $q$  ed  $r$  rispettivamente. Detta  $\eta: L \rightarrow L$  la composizione di  $\phi$  e  $\psi$  calcolare il valore del birapporto  $[p, s; \eta(s), \eta^2(s)]$  al variare di  $s$  in  $L - \{p\}$ .



## Curve algebriche piane

Per evitare eccessivi tecnicismi, in questo capitolo non tutti i risultati sono dimostrati completamente: alcune dimostrazioni sono omesse, altre fatte sotto ipotesi aggiuntive ed altre ancora sostituite con argomenti euristici.

Sempre per semplicità espositiva, da questo momento in poi e salvo avviso contrario, con il simbolo  $\mathbb{K}$  denoteremo sempre un campo *algebricamente chiuso*, sebbene molti risultati esposti siano validi per una classe di campi più estesa; in alcuni casi metteremo delle condizioni sulla caratteristica di  $\mathbb{K}$ .

Giova ricordare che ogni campo algebricamente chiuso  $\mathbb{K}$  è infinito: infatti se contenesse un numero finito di elementi  $a_1, \dots, a_n$ , allora il polinomio

$$p(t) = 1 + \prod_{i=1}^n (t - a_i)$$

non avrebbe radici in  $\mathbb{K}$ , contraddicendo la chiusura algebrica.

Supporremo che il lettore abbia conoscenza delle nozioni e delle principali proprietà dei campi e degli spazi proiettivi. Il simbolo  $\mathbb{N} = \{0, 1, \dots\}$  denota l'insieme degli interi non negativi, mentre indicheremo con  $\mathbb{Q}, \mathbb{R}, \mathbb{C}$  i campi dei numeri razionali, reali e complessi, rispettivamente. Infine, se  $X$  è un insieme finito, indichiamo con  $|X| \in \mathbb{N}$  il suo numero di elementi.

### 8.1. Polinomi numerici

Dati due interi non negativi  $n, d \in \mathbb{N}$ , il coefficiente binomiale

$$\binom{n}{d}$$

può essere definito come il numero dei sottoinsiemi di cardinalità  $d$  contenuti in un insieme di  $n$  elementi e sono ben note le formule:

$$\binom{n}{0} = \binom{n}{n} = 1, \quad \binom{n}{d} = \frac{1}{d!} \prod_{i=0}^{d-1} (n - i), \quad d > 0,$$

$$\binom{n}{d} = \binom{n-1}{d-1} + \binom{n-1}{d}, \quad d, n > 0.$$

$$(x + y)^n = \sum_{d=0}^n \binom{n}{d} x^d y^{n-d}.$$

Osserviamo anche che  $\binom{n}{d} = 0$  se  $d > n$  e che per  $0 \leq d \leq n$  vale  $\binom{n}{d} = \frac{n!}{d!(n-d)!}$ .

Più in generale, se  $t$  è una indeterminata,  $n \in \mathbb{Z}$ ,  $d \in \mathbb{N}$  e consideriamo i polinomi

$$\binom{t+n}{0} = 1, \quad \binom{t+n}{d} = \frac{1}{d!} \prod_{i=0}^{d-1} (t+n-i) \in \mathbb{Q}[t], \quad d > 0,$$

allora continua a valere la formula

$$\binom{t+n}{d} = \binom{n+t-1}{d-1} + \binom{n+t-1}{d}.$$

Basta infatti osservare che

$$\binom{n+t-1}{d-1} = \binom{t+n}{d} \frac{d}{n+t}, \quad \binom{n+t-1}{d} = \binom{t+n}{d} \frac{n+t-d}{n+t}.$$

Per ogni  $a \in \mathbb{Z}$  ed ogni  $n > 0$  il polinomio

$$(8.1) \quad \binom{t+a}{n} = \frac{1}{n!} \prod_{i=0}^{n-1} (t+a-i) = \frac{1}{n!} t^n + \dots$$

ha grado  $n$ , coefficiente direttivo  $1/n!$  e  $n$  radici distinte  $-a, -a+1, \dots, -a+n-1$ .

**DEFINIZIONE 8.1.1.** Un polinomio  $p(t) \in \mathbb{Q}[t]$  si dice un **polinomio numerico** se esiste un intero  $N$  tale che  $p(n) \in \mathbb{Z}$  per ogni intero  $n \geq N$ .

Ogni polinomio a coefficienti interi è numerico, ma esistono anche polinomi numerici a coefficienti razionali: ad esempio il polinomio  $\binom{t+n}{d}$  è numerico in quanto uguale ad un coefficiente binomiale per ogni intero e  $t \geq d-n$ .

**LEMMA 8.1.2.** Se  $p(t) \in \mathbb{Q}[t]$  è un polinomio numerico, allora  $p(n) \in \mathbb{Z}$  per ogni  $n \in \mathbb{Z}$ .

**DIMOSTRAZIONE.** Induzione sul grado di  $p(t)$ . Se  $p(t)$  è una costante, allora tale costante deve essere intera. Se  $p(t)$  ha grado  $n > 0$ , allora il polinomio  $q(t) = p(t) - p(t-1)$  è numerico di grado  $n-1$  e per l'ipotesi induttiva  $q(n) \in \mathbb{Z}$  per ogni intero  $n$ . Ne consegue inevitabilmente che anche  $p(n) \in \mathbb{Z}$  per ogni  $n \in \mathbb{Z}$ .  $\square$

È chiaro che somme e differenza di polinomi numerici sono ancora polinomi numerici. Se  $p(t)$  è un polinomio numerico allora anche  $p(t-a)$  è un polinomio numerico per ogni  $a \in \mathbb{Z}$ .

**LEMMA 8.1.3.** Sia  $p(t)$  un polinomio numerico di grado  $n$ . Per ogni  $a, b \in \mathbb{Z}$  il polinomio numerico

$$p(t) + p(t-a-b) - p(t-a) - p(t-b)$$

ha grado  $\leq n-2$ .

**DIMOSTRAZIONE.** Sia  $p(t) = \sum_{i=0}^n c_i t^i$ , allora per ogni intero  $d$  si ha

$$p(t+d) = \sum_{i=0}^n c_i (t+d)^i = \sum_{i=0}^n \sum_{j=0}^i c_i \binom{i}{j} t^j d^{i-j} = \sum_{j=0}^n \left( \sum_{i=j}^n c_i d^{i-j} \binom{i}{j} \right) t^j.$$

Dunque il coefficienti di  $t^n$  e  $t^{n-1}$  in  $p(t+d)$  sono rispettivamente  $c_n$  e  $c_{n-1} + nc_n d$ . Di conseguenza, i coefficienti di  $t^n$  e  $t^{n-1}$  in  $p(t) + p(t-a-b) - p(t-a) - p(t-b)$  sono, rispettivamente  $c_n + c_n - c_n - c_n = 0$  e

$$c_{n-1} + c_{n-1} - nc_n(a+b) - c_{n-1} + nc_n a - c_{n-1} + nc_n b = 0.$$

$\square$

**TEOREMA 8.1.4.** Sia  $p(t)$  un polinomio numerico di grado  $n$ . Allora esiste un'unica successione di interi  $a_0, \dots, a_n$  tale che

$$p(t) = \sum_{i=0}^n a_i \binom{t+i}{i}.$$

**DIMOSTRAZIONE.** Sia  $V \subset \mathbb{Q}[t]$  il  $\mathbb{Q}$ -sottospazio vettoriale dei polinomi di grado  $\leq n$ . Per ogni  $i = 0, \dots, n$  il polinomio  $\binom{t+i}{i}$  ha grado  $i$ , i polinomi

$$\binom{t+0}{0}, \dots, \binom{t+n}{n},$$

sono linearmente indipendenti e siccome  $V$  ha dimensione  $n+1$  sono anche generatori. Abbiamo provato quindi che esistono unici  $a_0, \dots, a_n \in \mathbb{Q}$  tali che

$$p(t) = \sum_{i=0}^n a_i \binom{t+i}{i}.$$

Dimostriamo per induzione su  $n$  che ogni  $a_i$  è intero; a tal fine basta provare che  $a_n \in \mathbb{Z}$ . Infatti se  $a_n \in \mathbb{Z}$  allora il polinomio

$$p(t) - a_n \binom{t+n}{n} = \sum_{i=0}^{n-1} a_i \binom{t+i}{i}$$

è numerico di grado  $< n$  e per l'ipotesi induttiva  $a_i \in \mathbb{Z}$  per ogni  $i$ . Consideriamo adesso il polinomio numerico  $q(t) = p(t+1) - p(t)$ . I coefficienti direttori di  $p(t)$  e  $q(t)$  si calcolano facilmente:

$$p(t) = \frac{a_n}{n!} t^n + \dots, \quad q(t) = p(t+1) - p(t) = \frac{a_n}{n!} (nt^{n-1}) + \dots$$

Per l'ipotesi induttiva esistono  $n$  interi  $b_0, \dots, b_{n-1}$  tali che

$$q(t) = \sum_{i=0}^{n-1} b_i \binom{t+i}{i} = \frac{b_{n-1}}{(n-1)!} t^{n-1} + \dots$$

da cui segue  $a_n = b_{n-1} \in \mathbb{Z}$ . □

Per uso futuro diamo un'altra interpretazione combinatoria dei coefficienti binomiali  $\binom{d+n}{n}$  per  $d \geq 0$ .

LEMMA 8.1.5. *Siano  $x_0, \dots, x_n$  indeterminate. Per ogni  $d \geq -n$  il numero di monomi*

$$x_0^{a_0} x_1^{a_1} \dots x_n^{a_n}$$

*di grado  $a_0 + \dots + a_n = d$  è uguale al coefficiente binomiale  $\binom{d+n}{n}$ .*

DIMOSTRAZIONE. Se  $-n \leq d < 0$  si ha  $\binom{d+n}{n} = 0$  che chiaramente coincide con il numero dei monomi di grado  $d$ . Se  $d \geq 0$ , dobbiamo calcolare la cardinalità dell'insieme

$$A = \{(a_0, \dots, a_n) \in \mathbb{N}^{n+1} \mid a_0 + \dots + a_n = d\}.$$

A tal fine consideriamo gli insiemi

$$A' = \{(a_1, \dots, a_n) \in \mathbb{N}^n \mid a_1 + \dots + a_n \leq d\},$$

$$B = \{(b_1, \dots, b_n) \in \mathbb{N}^n \mid 1 \leq b_1 < b_2 < \dots < b_n \leq d+n\},$$

osservando che  $B$  è in biezione con i sottoinsiemi di cardinalità  $n$  di  $\{1, \dots, d+n\}$  e pertanto  $|B| = \binom{d+n}{n}$ . Osserviamo poi che le applicazioni  $A \xrightarrow{f} A' \xrightarrow{g} B$ :

$$f(a_0, \dots, a_n) = (a_1, \dots, a_n), \quad g(a_1, \dots, a_n) = (a_1 + 1, a_1 + a_2 + 2, \dots, a_1 + \dots + a_n + n),$$

sono bigettive con inverse

$$f^{-1}(a_1, \dots, a_n) = (d - \sum a_i, a_1, \dots, a_n),$$

$$g^{-1}(b_1, \dots, b_n) = (b_1 - 1, b_2 - b_1 - 1, \dots, b_n - b_{n-1} - 1).$$

Si noti che  $A'$  è in biezione con l'insieme dei monomi  $x_1^{a_1} \dots x_n^{a_n}$  di grado  $\leq d$ . □

### Esercizi

ESERCIZIO 5. Provare che per ogni  $n, d \geq 0$  vale la formula

$$\binom{d+n}{n} = \sum_{k \geq 0}^n \binom{n}{k} \binom{d}{k} = \sum_{k \geq 0}^n \binom{n}{n-k} \binom{d}{k}$$

considerando un insieme  $X$  formato da  $d$  palline bianche,  $n$  palline nere ed i sottoinsiemi di  $X$  formati da  $k$  palline bianche e  $n-k$  palline nere.

ESERCIZIO 6. Provare l'identità polinomiale

$$\binom{t+n}{n} = (-1)^n \binom{-t-1}{n}.$$

ESERCIZIO 7. Per ogni coppia di interi positivi  $n, m$ , denotiamo con  $M(n, m)$  l'insieme di tutte le applicazioni

$$f: \{1, 2, \dots, n\} \rightarrow \{1, 2, \dots, m\}$$

non decrescenti, ossia tali che  $f(i+1) \geq f(i)$  per ogni  $i < n$ . Calcolare le cardinalità di  $M(n, m)$ , del suo sottoinsieme delle applicazioni iniettive quando  $n \leq m$  e del suo sottoinsieme delle applicazioni surgettive quando  $n \geq m$ .

ESERCIZIO 8. Siano

$$F_0 = 0, \quad F_1 = 1, \quad F_2 = 1, \quad \dots \quad F_{n+1} = F_n + F_{n-1}, \quad \dots$$

i numeri di Fibonacci. Dimostrare che per ogni  $n \geq 0$  vale

$$F_{n+1} = \sum_{d \geq 0} \binom{n-d}{d}.$$

ESERCIZIO 9. Dimostrare il seguente risultato, generalmente noto come *Principio di inclusione-esclusione*.

Denotiamo con  $C(a, n)$  la famiglia dei sottoinsiemi di cardinalità  $a$  di  $\{1, \dots, n\}$  e siano  $A_1, \dots, A_n$  sottoinsiemi di un insieme finito  $A$ ; per ogni  $I = \{i_1, \dots, i_a\} \in C(a, n)$  denotiamo con  $\alpha(I)$  la cardinalità di  $A_{i_1} \cap \dots \cap A_{i_a}$ . Dimostrare che la cardinalità di  $A_1 \cup \dots \cup A_n$  è uguale a

$$\sum_{a=1}^n (-1)^{a-1} \sum_{I \in C(a, n)} \alpha(I).$$

(Sugg.: un punto appartenente ad  $A_i$  per esattamente  $s$  indici  $i \in \{1, \dots, n\}$  viene contato, con molteplicità,  $1 - (1-1)^s$  volte.)

ESERCIZIO 10. Dimostrare che per ogni  $s \geq 0$  vale lo sviluppo di Taylor

$$\frac{1}{(1-t)^{s+1}} = \sum_{n=0}^{+\infty} \binom{s+n}{s} t^n.$$

(Sugg.: induzione su  $s$ , derivando  $(1-t)^{-s}$ .)

ESERCIZIO 11. Provare che con la relazione di ordine,  $p \geq q$  se e solo se  $p(n) \geq q(n)$  per  $n \gg 0$ , i polinomi numerici sono un insieme totalmente ordinato.

## 8.2. Polinomi omogenei

Denotiamo con  $\mathbb{K}[x_0, \dots, x_n]$  l'anello dei polinomi a coefficienti in  $\mathbb{K}$  nelle indeterminate  $x_0, \dots, x_n$ : ogni polinomio in  $\mathbb{K}[x_0, \dots, x_n]$  è una combinazione lineare finita a coefficienti in  $\mathbb{K}$  di monomi  $x_0^{a_0} \dots x_n^{a_n}$ , il grado  $\deg(p)$  di un polinomio non nullo  $p$  è uguale al massimo grado dei monomi che vi compaiono con coefficiente diverso da 0. Con la convenzione che il grado del polinomio nullo è uguale a  $-\infty$  le seguenti formule sono di immediata verifica:

$$\deg(fg) = \deg(f) + \deg(g), \quad \deg(f+g) \leq \max(\deg(f), \deg(g)), \quad f, g \in \mathbb{K}[x_0, \dots, x_n].$$

In particolare  $fg = 0$  se e solo se  $f = 0$  oppure  $g = 0$ , ossia  $\mathbb{K}[x_0, \dots, x_n]$  è un dominio di integrità: il suo campo delle frazioni globali è detto **campo delle funzioni razionali** e viene denotato  $\mathbb{K}(x_0, \dots, x_n)$ :

$$\mathbb{K}(x_0, \dots, x_n) = \left\{ \frac{f}{g} \mid f, g \in \mathbb{K}[x_0, \dots, x_n], g \neq 0 \right\}.$$

Ad ogni polinomio  $f \in \mathbb{K}[x_0, \dots, x_n]$  è associata la corrispondente funzione polinomiale  $f: \mathbb{K}^{n+1} \rightarrow \mathbb{K}$  ottenuta sostituendo gli elementi di  $\mathbb{K}$  al posto delle indeterminate ed eseguendo le necessarie operazioni di somma e prodotto. Come nel caso di polinomi in una variabile, siccome il campo  $\mathbb{K}$  è infinito, il polinomio è univocamente determinato dalla corrispondente funzione polinomiale: ciò segue immediatamente dal seguente lemma.

LEMMA 8.2.1. *Sia  $\mathbb{K}$  un campo infinito. Allora per ogni polinomio non nullo  $0 \neq f \in \mathbb{K}[x_0, \dots, x_n]$  esistono  $a_0, \dots, a_n \in \mathbb{K}$  tali che  $f(a_0, \dots, a_n) \neq 0$ .*

DIMOSTRAZIONE. Sia  $d$  il grado di  $f$  e dimostriamo il lemma per induzione su  $n$ : se  $n = 0$  il polinomio  $f(x_0)$  ha al più  $d$  radici distinte e quindi esiste  $a_0 \in \mathbb{K}$  tale che  $f(a_0) \neq 0$ . Se  $n > 0$ , raccogliendo a fattor comune le potenze di  $x_0$  possiamo scrivere

$$f = f_0 + f_1 x_0 + f_2 x_0^2 + \cdots + f_d x_0^d,$$

con i polinomi  $f_i \in \mathbb{K}[x_1, \dots, x_n]$  non tutti nulli. Per induzione possiamo trovare  $a_1, \dots, a_n \in \mathbb{K}$  tali che i valori  $f_i(a_1, \dots, a_n) \in \mathbb{K}$  non sono tutti nulli e quindi tali che il polinomio

$$g(x_0) = f(x_0, a_1, \dots, a_n)$$

è non nullo. Come nel caso  $n = 0$  esiste  $a_0 \in \mathbb{K}$  tale che  $g(a_0) \neq 0$ .  $\square$

Un polinomio  $f \in \mathbb{K}[x_0, \dots, x_n]$  si dice **omogeneo** di grado  $d$  se è combinazione lineare di coefficienti in  $\mathbb{K}$  di monomi di grado  $d$ . Con questa definizione cadiamo nella contraddizione che il polinomio nullo è contemporaneamente di grado  $-\infty$  ed omogeneo di grado  $d$  per ogni  $d \in \mathbb{N}$ : si tratta tuttavia di una contraddizione del tutto innocua che semplifica l'esposizione rispetto ad una trattazione più formale e rigorosa.

Equivalentemente, un polinomio  $f(x_0, \dots, x_n)$  è omogeneo di grado  $d$  se, nel campo delle funzioni razionali, vale l'uguaglianza

$$f(x_0, x_1, \dots, x_n) = x_0^d f\left(1, \frac{x_1}{x_0}, \dots, \frac{x_n}{x_0}\right).$$

Notiamo infine che ogni polinomio  $f$  di grado  $n \geq 0$  si scrive in modo unico come

$$f = f_0 + f_1 + \cdots + f_n,$$

con  $f_i$  polinomio omogeneo di grado  $i$  e  $f_n \neq 0$ .

LEMMA 8.2.2. *Siano  $f, g \in \mathbb{K}[x_0, \dots, x_n]$  con  $f$  che divide  $g$  e  $g \neq 0$ . Se  $g$  è omogeneo, allora anche  $f$  è omogeneo.*

DIMOSTRAZIONE. Per ipotesi esiste un polinomio  $h$  tale che  $fh = g$  e siccome  $g \neq 0$  anche  $f, h \neq 0$ . Se  $f$  ha grado  $n$  e  $h$  ha grado  $m$  possiamo scrivere

$$f = f_0 + f_1 + \cdots + f_n, \quad h = h_0 + f_1 + \cdots + h_m, \quad n, m \geq 0,$$

con  $f_i, h_i$  omogenei di grado  $i$  e  $f_n, h_m$  non nulli. Siano

$$r = \min\{i \mid f_i \neq 0\}, \quad s = \min\{i \mid h_i \neq 0\},$$

e supponiamo per assurdo  $r < n$ ; allora

$$g = f_r h_s + \sum_{r+s < i+j < n+m} f_i h_j + f_n h_m,$$

e siccome  $f_r h_s \neq 0$  è omogeneo di grado  $r + s$ ,  $f_n h_m \neq 0$  è omogeneo di grado  $n + m$  mentre ogni monomio della sommatoria rimanente ha grado strettamente compreso tra  $r + s$  e  $n + m$ , ne segue che il polinomio  $g$  contiene sia monomi di grado  $r + s$  che monomi di grado  $n + m$ , contraddicendo l'ipotesi di omogeneità.  $\square$

Un'altra fondamentale proprietà di  $\mathbb{K}[x_0, \dots, x_n]$ , ben nota dai corsi di Algebra, è quella di essere un dominio a fattorizzazione unica: un polinomio  $f$  si dice **irriducibile** se ha grado positivo e se non è il prodotto di polinomi di grado strettamente inferiore. Ogni polinomio non nullo si scrive in maniera essenzialmente unica come prodotto di polinomi irriducibili. Più precisamente, se

$$f = p_1 \cdots p_n = q_1 \cdots q_m$$

con  $p_1, \dots, p_n, q_1, \dots, q_m$  polinomi irriducibili, allora  $n = m$  e, a meno dell'ordine, per ogni indice  $i$  vale  $p_i = c_i q_i$  per qualche  $c_i \in \mathbb{K}$ .

Due polinomi  $f, g$  si dicono senza fattori comuni, o relativamente primi, se non esiste alcun polinomio irriducibile che li divide entrambi.

Ricordiamo che un diagramma in serie di spazi vettoriali ed applicazioni lineari

$$\cdots \rightarrow V_i \xrightarrow{f_i} V_{i+1} \xrightarrow{f_{i+1}} V_{i+2} \rightarrow \cdots$$

si dice una **successione esatta** se  $\ker f_i$  è uguale all'immagine di  $f_{i-1}$ , beninteso ogni volta che  $f_i$  ed  $f_{i-1}$  fanno parte del diagramma.

Ad esempio la successione  $0 \rightarrow V \xrightarrow{f} W$  è esatta se e solo se  $f$  è iniettiva, mentre  $V \xrightarrow{f} W \rightarrow 0$  è una successione esatta se e solo se  $f$  è surgettiva. Segue dal teorema del rango che se  $0 \rightarrow V \rightarrow W \rightarrow U \rightarrow 0$  è una successione esatta di spazi vettoriali di dimensione finita, allora  $\dim W = \dim V + \dim U$ .

Il conucleo di un'applicazione lineare  $f: V \rightarrow W$  è definito come lo spazio vettoriale quoziente  $\text{coker}(f) = \frac{W}{f(V)}$ : si ha dunque una successione esatta

$$0 \rightarrow \ker(f) \xrightarrow{i} V \xrightarrow{f} W \xrightarrow{p} \text{coker}(f) \rightarrow 0$$

dove  $i$  e  $p$  sono le applicazioni di inclusione e proiezione al quoziente, rispettivamente. Similmente, ogni quadrato commutativo

$$\begin{array}{ccc} V & \xrightarrow{f} & W \\ \downarrow \alpha & & \downarrow \beta \\ A & \xrightarrow{g} & B \end{array}$$

si estende ad un diagramma commutativo con le righe esatte:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \ker(f) & \longrightarrow & V & \xrightarrow{f} & W & \longrightarrow & \text{coker}(f) & \longrightarrow & 0 \\ & & \downarrow \alpha & & \downarrow \alpha & & \downarrow \beta & & \downarrow \beta & & \\ 0 & \longrightarrow & \ker(g) & \longrightarrow & A & \xrightarrow{g} & B & \longrightarrow & \text{coker}(g) & \longrightarrow & 0. \end{array}$$

Prima di proseguire, precisiamo cosa si intende quando diciamo che “i polinomi irriducibili sono invarianti per cambio di coordinate”. Sia  $A = (a_{ij}) \in M_{n+1, m+1}(\mathbb{K})$  una matrice e denotiamo con lo stesso simbolo  $A: \mathbb{K}^{m+1} \rightarrow \mathbb{K}^{n+1}$  l'applicazione lineare associata, ossia l'applicazione che manda il punto  $y$  di coordinate  $y_0, \dots, y_m$  nel punto  $x = Ay$  di coordinate  $x_i = \sum_j a_{ij}y_j$ ,  $i = 0, \dots, n$ .

Dato un polinomio  $f(x_0, \dots, x_n)$  possiamo considerare il polinomio  $A^*f \in \mathbb{K}[y_0, \dots, y_m]$  ottenuto sostituendo alla variabile  $x_i$  l'espressione  $\sum_j a_{ij}y_j$ :

$$A^*f(y_0, \dots, y_m) = f\left(\sum_j a_{0j}y_j, \dots, \sum_j a_{nj}y_j\right).$$

Ad esempio, se  $f(x_0, x_1) = x_0^1 - x_1^2$  e l'applicazione lineare  $A$  è data dalle relazioni

$$x_0 = y_0 + y_1, \quad y_1 = x_0 - x_1$$

si ha:

$$A^*f(y_0, y_1) = (y_0 + y_1)^2 - (y_0 - y_1)^2 = 4y_0y_1.$$

Lasciamo per esercizio la verifica che l'applicazione  $A^*: \mathbb{K}[x_0, \dots, x_n] \rightarrow \mathbb{K}[y_0, \dots, y_m]$  commuta con somme e prodotti e che il grado di  $A^*f$  è minore od uguale al grado di  $f$ . La funzione polinomiale  $A^*f: \mathbb{K}^{m+1} \rightarrow \mathbb{K}$  è uguale alla composizione  $\mathbb{K}^{m+1} \xrightarrow{A} \mathbb{K}^{n+1} \xrightarrow{f} \mathbb{K}$ .

Su  $A$  è invertibile, allora  $(A^{-1})^* = (A^*)^{-1}$ . In particolare  $A^*$  è un isomorfismo di anelli e di spazi vettoriali ed il grado di  $A^*f$  è uguale al grado di  $f$ . Se  $f$  è irriducibile, allora anche  $A^*f$  è irriducibile: infatti se fosse  $A^*f = gh$  con  $g, h$  polinomi di grado positivo, allora si avrebbe  $f = ((A^{-1})^*g)((A^{-1})^*h)$  ed i due polinomi  $(A^{-1})^*g$ ,  $(A^{-1})^*h$  hanno grado positivo.

**Eliminazione semplice.** Sia  $n$  un intero positivo fissato. Per ogni intero  $d$  denotiamo con  $S_d \subset \mathbb{K}[x_0, \dots, x_n]$  il sottospazio vettoriale dei polinomi omogenei di grado  $d$ ; in particolare  $S_d = 0$  per ogni  $d < 0$ . Segue immediatamente dal Lemma 8.1.5 che per ogni  $d \geq -n$  la dimensione di  $S_d$  è uguale a

$$\dim S_d = \binom{d+n}{n} = \frac{1}{n!}d^n + \frac{n+1}{2(n-1)!}d^{n-1} + \dots, \quad d \geq -n.$$

Una dimostrazione alternativa della formula precedente si ottiene per induzione su  $d + n$  ed osservando che per ogni  $d > 0$  si ha una successione esatta

$$0 \rightarrow S_{d-1} \xrightarrow{\cdot x_0} S_d \xrightarrow{x_0 \mapsto 0} S_d \cap \mathbb{K}[x_1, \dots, x_n] \rightarrow 0,$$

da cui segue

$$\dim S_d = \binom{d+n-1}{n} + \binom{d+n-1}{n-1}.$$

**LEMMA 8.2.3.** *Siano  $f, g \in \mathbb{K}[x_0, \dots, x_n]$  polinomi omogenei non nulli e di grado  $a, b > 0$  rispettivamente. Per ogni intero  $d$  si consideri il complesso di spazi vettoriali:*

$$(8.2) \quad 0 \rightarrow S_{d-a-b} \xrightarrow{\alpha_d} S_{d-a} \oplus S_{d-b} \xrightarrow{\beta_d} S_d, \quad \alpha_d(p) = (gp, fp), \quad \beta_d(q, r) = fq - gr.$$

Allora le seguenti condizioni sono equivalenti:

- (1)  $f, g$  non hanno fattori comuni di grado positivo;
- (2) per ogni intero  $d$  il complesso (8.2) è una successione esatta;
- (3) esiste un intero  $d \geq a + b - 1$  per cui il complesso (8.2) è una successione esatta.

**DIMOSTRAZIONE.** È chiaro che  $\beta\alpha = 0$ . Inoltre, per ipotesi  $f, g$  sono entrambi non nulli quindi  $\alpha$  è iniettiva poiché  $\mathbb{K}[x_0, \dots, x_n]$  è un dominio di integrità.

Supponiamo  $f, g$  senza fattori comuni,  $d$  qualsiasi e sia  $(q, r) \in \ker \beta_d$ , ossia  $fq = gr$ . Se  $r = 0$ , siccome  $f \neq 0$  si ha  $q = 0$  ed in tal caso la coppia  $(q, r) = (0, 0)$  appartiene all'immagine di  $\alpha$ . Se  $r \neq 0$ , siccome nessun fattore di  $f$  divide  $g$  si ha  $r = fp$  con  $p \in S_{d-a-b}$ . Dunque  $gfp = fq$  da cui segue  $q = gp$  e di conseguenza  $(q, r) = \alpha_d(p)$ .

Se  $f, g$  hanno un fattore comune  $h$  di grado positivo  $c$ , dimostriamo che per ogni  $d \geq a + b - c$  il nucleo di  $\beta_d$  ha dimensione strettamente maggiore della dimensione di  $S_{d-a-b}$ . Infatti l'applicazione

$$\gamma: S_{d-a-b+c} \rightarrow \ker(\beta_d), \quad \gamma(p) = \left( p \frac{g}{h}, p \frac{f}{h} \right),$$

è ben definita ed iniettiva, quindi

$$\dim \ker(\beta_d) \geq \dim S_{d-a-b+c} > \dim S_{d-a-b}.$$

□

**TEOREMA 8.2.4 (Eliminazione semplice).** *Siano  $f, g \in \mathbb{K}[x_0, \dots, x_n]$  polinomi senza fattori comuni ed omogenei di gradi  $a, b > 0$ , rispettivamente. Allora esistono un intero  $d$  e due polinomi omogenei  $h, k \in \mathbb{K}[x_0, \dots, x_n]$  di gradi  $d - a, d - b$  rispettivamente tali che*

$$0 \neq hf - kg \in \mathbb{K}[x_1, \dots, x_n].$$

*Inoltre, se  $n = 2$  è possibile scegliere l'intero  $d$  uguale al prodotto  $ab$ .*

È chiaro l'uso del termine eliminazione nel Teorema 8.2.4 in quanto la variabile  $x_0$  viene "eliminata" mediante la combinazione  $hf - kg$ .

**DIMOSTRAZIONE.** Siccome  $a, b > 0$ , l'ipotesi che  $f, g$  non abbiano fattori comuni implica necessariamente  $n > 0$ . Per il Lemma 8.1.5 lo spazio vettoriale  $R_d = S_d \cap \mathbb{K}[x_1, \dots, x_n]$  ha dimensione uguale a

$$\binom{d+n-1}{n-1} = \frac{d^{n-1}}{(n-1)!} + \dots, \quad d \geq 1 - n.$$

Per il Lemma 8.2.3, per ogni intero  $d$  si ha una successione esatta

$$0 \rightarrow S_{d-a-b} \xrightarrow{\alpha_d} S_{d-a} \oplus S_{d-b} \xrightarrow{\beta_d} S_d \rightarrow \text{coker}(\beta_d) \rightarrow 0, \\ \alpha_d(p) = (gp, fp), \quad \beta_d(q, r) = fq - gr.$$

Per ogni  $d \geq a + b - 1$  la dimensione del conucleo di  $\beta_d$  è quindi uguale a

$$\dim \text{coker}(\beta_d) = \dim S_d - \dim S_{d-a} - \dim S_{d-b} + \dim S_{d-a-b} \\ = \binom{d+n}{n} - \binom{d-a+n}{n} - \binom{d-b+n}{n} + \binom{d-a-b+n}{n}.$$

Per il Lemma 8.1.3 la dimensione di  $\text{coker}(\beta_d)$  è un polinomio numerico in  $d$  di grado  $\leq n - 2$  e dunque per  $d$  sufficientemente grande si ha  $\dim R_d > \dim \text{coker}(\beta_d)$ . Ne segue che esiste  $d$  per cui la restrizione al sottospazio  $R_d$  della proiezione  $S_d \rightarrow \text{coker}(\beta_d)$  non è iniettiva, ossia esiste un elemento non nullo che appartiene all'intersezione di  $R_d$  con l'immagine di  $\beta_d$ , che è esattamente quello che volevamo dimostrare.

Se  $n = 2$  allora allora lo spazio vettoriale  $R_d = S_d \cap \mathbb{K}[x_1, x_2]$  ha dimensione  $d + 1$ ; si ha  $ab \geq a + b - 1$  e per ogni  $d \geq a + b - 1$  la dimensione del conucleo di  $\beta_d$  è

$$\begin{aligned} \dim \text{coker}(\beta_d) &= \binom{d+2}{2} - \binom{d-a+2}{2} - \binom{d-b+2}{2} + \binom{d-a-b+2}{2} \\ &= \frac{1}{2} ((d+2)(d+1) - (d-a+2)(d-a+1) - (d-b+2)(d-b+1) \\ &\quad + (d-a-b+2)(d-a-b+1)) \\ &= ab. \end{aligned}$$

Dunque per ogni  $d \geq ab$  l'immagine di  $\beta_d$  ha intersezione non nulla con  $R_d$ . Un conto simile mostra pure che per  $n = 1$  l'applicazione  $\beta_d$  è surgettiva per ogni  $d \geq a + b - 1$ .  $\square$

**OSSERVAZIONE 8.2.5.** I polinomi  $h, k$  nell'enunciato del Teorema 8.2.4 non sono unici, nemmeno nel caso in cui  $d$  sia il minimo intero per cui vale la proprietà. Abbiamo dato una dimostrazione non costruttiva della loro esistenza ma va segnalato che, usando tecniche più raffinate, ma sempre riconducibili all'algebra lineare, è possibile dare delle formula esplicite per  $k, h$  nel caso  $d = ab$ , in cui i coefficienti di  $h, k$  sono funzioni polinomiali dei coefficienti di  $f, g$ . Vedremo (implicitamente) tali formule (sotto l'ipotesi aggiuntiva che  $f(1, 0, \dots, 0) \neq 0$ ) nella Sezione 9.5. Questo prova anche che per ogni  $n \geq 2$  l'intero  $d$  può essere preso minore o uguale al prodotto  $ab$ .

**Derivate.** In analogia con la teoria delle derivate parziali delle funzioni di variabile reale, per ogni indice  $i = 0, \dots, n$  indichiamo con

$$\frac{\partial}{\partial x_i} : \mathbb{K}[x_0, \dots, x_n] \rightarrow \mathbb{K}[x_0, \dots, x_n]$$

l'applicazione lineare definita sui monomi mediante la formula

$$\frac{\partial}{\partial x_i} x_0^{a_0} \cdots x_n^{a_n} = \frac{a_i}{x_i} x_0^{a_0} \cdots x_n^{a_n}.$$

Lasciamo per esercizio che continua a valere la **formula di Leibniz**:

$$\frac{\partial fg}{\partial x_i} = \frac{\partial f}{\partial x_i} g + f \frac{\partial g}{\partial x_i}.$$

**LEMMA 8.2.6.** Sia  $f \in \mathbb{K}[x_0, \dots, x_n]$  tale che  $\frac{\partial f}{\partial x_i} = 0$  per ogni  $i = 0, \dots, n$ :

- (1) se il campo  $\mathbb{K}$  ha caratteristica 0, allora  $f \in \mathbb{K}$  è una costante;
- (2) se il campo  $\mathbb{K}$  è algebricamente chiuso di caratteristica positiva  $p \geq 2$ , allora esiste  $g \in \mathbb{K}[x_0, \dots, x_n]$  tale che  $f = g^p$ .

In particolare se  $f$  è irriducibile e  $\mathbb{K}$  algebricamente chiuso, allora esiste sempre un indice  $i$  tale che  $\frac{\partial f}{\partial x_i} \neq 0$ .

**DIMOSTRAZIONE.** Segue dalla formula di Leibniz che se una delle due condizioni è soddisfatta allora tutte le derivate parziali di  $f$  si annullano. Dimostriamo le implicazioni inverse per induzione su  $n$ , osservando preliminarmente che per ogni  $a \in \mathbb{K}$  ed ogni numero primo  $p$  esiste  $b$  tale che  $b^p = a$ : infatti siccome  $\mathbb{K}$  è algebricamente chiuso il polinomio  $t^p - a$  possiede radici.

Sia  $n \geq 0$  e supponiamo il lemma vero in  $\mathbb{K}[x_0, \dots, x_{n-1}]$ . Dato  $f \in \mathbb{K}[x_0, \dots, x_n]$  con  $\frac{\partial f}{\partial x_i} = 0$  per ogni  $i$ , possiamo scrivere

$$f(x_0, \dots, x_n) = \sum_{j=0}^d f_j(x_0, \dots, x_{n-1})x_n^j, \quad \frac{\partial f}{\partial x_n}(x_0, \dots, x_n) = \sum_{j=1}^d j f_j(x_0, \dots, x_{n-1})x_n^{j-1},$$

e quindi  $\frac{\partial f}{\partial x_n} = 0$  se e solo se  $j f_j = 0$  per ogni  $j$ .

Se  $\mathbb{K}$  ha caratteristica 0, e  $j f_j = 0$  per ogni  $j$ , allora  $f_j = 0$  per ogni  $j > 0$ , ossia  $f = f_0$  è un polinomio in  $x_0, \dots, x_{n-1}$  e la tesi segue dall'ipotesi induttiva.

Se  $\mathbb{K}$  ha caratteristica  $p > 0$ , e  $j f_j = 0$  per ogni  $j$ , allora  $f_j = 0$  per ogni  $j$  non divisibile per  $p$  e quindi possiamo scrivere

$$f(x_0, \dots, x_n) = \sum_{j=0}^h g_j(x_0, \dots, x_{n-1})x_n^{jp}, \quad g_j = f_{pj}.$$

Siccome, per ogni  $i < n$  si ha  $\frac{\partial f}{\partial x_i} = \sum_j \frac{\partial g_j}{\partial x_i} x_n^{jp}$  ne consegue che  $\frac{\partial g_j}{\partial x_i} = 0$  per ogni  $i, j$  e per l'ipotesi induttiva si può scrivere

$$g_j = h_j^p, \quad f = \sum_j h_j^p (x_n^j)^p.$$

Per concludere basta osservare che, poiché  $(a+b)^p = a^p + b^p$  ( $p$  divide i coefficienti binomiali  $\binom{p}{i}$  per  $0 < i < p$ ), si ha

$$\left( \sum_j h_j x_n^j \right)^p = \sum_j h_j^p (x_n^j)^p = f.$$

□

È immediato verificare la validità della seguente formula, detta **Formula di Eulero**: per ogni polinomio omogeneo  $f \in \mathbb{K}[x_0, \dots, x_n]$  di grado  $m$  vale

$$(8.3) \quad \sum_{i=0}^n x_i \frac{\partial f}{\partial x_i} = m f.$$

Infatti, per linearità non è restrittivo supporre che  $f$  sia un monomio del tipo  $x_0^{a_0} \cdots x_n^{a_n}$  con  $\sum a_i = m$ . Allora

$$\frac{\partial x_0^{a_0} \cdots x_n^{a_n}}{\partial x_i} = \begin{cases} a_i x_0^{a_0} \cdots x_i^{a_i-1} \cdots x_n^{a_n} & \text{se } a_i > 0 \\ 0 & \text{se } a_i = 0 \end{cases}$$

e quindi

$$\sum_{i=0}^n x_i \frac{\partial x_0^{a_0} \cdots x_n^{a_n}}{\partial x_i} = \sum_{\{i|a_i>0\}} a_i x_0^{a_0} \cdots x_i^{a_i} \cdots x_n^{a_n} = m x_0^{a_0} \cdots x_n^{a_n}.$$

Osserviamo che se  $f$  è omogeneo di grado  $m > 0$ , allora le sue derivate sono polinomi omogenei di grado  $m - 1$ , possibilmente nulli.

### Esercizi.

ESERCIZIO 12. Siano  $\mathbb{K}$  un campo infinito e  $f \in \mathbb{K}[x_0, \dots, x_n]$ . Provare che  $f$  è omogeneo di grado  $d \geq 0$  se e solo se per ogni  $(a_0, \dots, a_n) \in \mathbb{K}^{n+1}$  e  $t \in \mathbb{K} - \{0\}$  vale

$$f(ta_0, \dots, ta_n) = t^d f(a_0, \dots, a_n).$$

### 8.3. Ipersuperfici proiettive

Da questo punto in poi, e fino alla fine del capitolo, supporremo salvo avviso contrario che  $\mathbb{K}$  sia un campo algebricamente chiuso, e quindi infinito.

Il prossimo lemma non è altro che la reinterpretazione della chiusura algebrica di  $\mathbb{K}$  per polinomi omogenei in due variabili.

LEMMA 8.3.1. *Sia  $\mathbb{K}$  un campo algebricamente chiuso. Allora ogni polinomio omogeneo  $f \in \mathbb{K}[x_0, x_1]$  non nullo di grado  $d$  è il prodotto di  $d$  polinomi omogenei di grado 1.*

DIMOSTRAZIONE. Sia  $h \leq d$  il grado del polinomio  $f(1, t) \in \mathbb{K}[t]$ . Siccome  $\mathbb{K}$  è algebricamente chiuso si ha

$$f(1, t) = c(t - a_1)(t - a_2) \cdots (t - a_h), \quad c, a_1, \dots, a_h \in \mathbb{K},$$

e quindi

$$f(x_0, x_1) = x_0^d f\left(1, \frac{x_1}{x_0}\right) = cx_0^{d-h} \prod_{i=1}^h (x_1 - a_i x_0).$$

□

Indichiamo con  $\mathbb{P}^n$  lo spazio proiettivo di dimensione  $n$  su  $\mathbb{K}$ . Se  $f \in \mathbb{K}[x_0, \dots, x_n]$  è omogeneo di grado  $d \geq 0$ ,  $(a_0, \dots, a_n) \in \mathbb{K}^{n+1}$  e  $t \in \mathbb{K} - \{0\}$ , allora

$$f(ta_0, \dots, ta_n) = t^d f(a_0, \dots, a_n)$$

e quindi  $f(a_0, \dots, a_n) = 0$  se e solo se  $f(ta_0, \dots, ta_n) = 0$ . Tali considerazioni permettono di dare senso alle seguente definizione.

DEFINIZIONE 8.3.2. Il luogo di zeri proiettivo  $V(f)$  di un polinomio omogeneo  $f \in \mathbb{K}[x_0, \dots, x_n]$  è il sottoinsieme di  $\mathbb{P}^n$  dato da:

$$V(f) = \{p \in \mathbb{P}^n \mid f(p) = 0\} = \{(a_0, \dots, a_n) \in \mathbb{P}^n \mid f(a_0, \dots, a_n) = 0\}.$$

Quando il contesto lo consente si può scrivere, con un leggero abuso di notazione, anche  $f(x) = 0$  per indicare il luogo di zeri proiettivo  $V(f)$  di un polinomio omogeneo. Il lettore tenga sempre presente che un polinomio omogeneo  $f \in \mathbb{K}[x_0, \dots, x_n]$  non definisce alcuna funzione  $\mathbb{P}^n \rightarrow \mathbb{K}$  ma solamente il suo luogo di zeri  $V(f)$ .

In alcuni casi, motivi di chiarezza notazionale suggeriranno di usare lettere maiuscole per denotare polinomi omogenei  $F \in \mathbb{K}[x_0, \dots, x_n]$ . L'uso della lettera  $V$  (dall'inglese vanishing) per indicare il luogo di zeri è quello utilizzato nella stragrande maggioranza della letteratura in geometria algebrica, anche se non mancano rispettabilissime eccezioni.

LEMMA 8.3.3. *Se  $f \in \mathbb{K}[x_0, \dots, x_n]$  è omogeneo e non nullo, allora  $V(f)$  è un sottoinsieme proprio di  $\mathbb{P}^n$ .*

DIMOSTRAZIONE. Se  $f$  ha grado 0, ossia  $f$  è una costante non nulla, allora  $f(x) = 0$  è l'insieme vuoto. Se il grado di  $f$  è positivo allora  $f(0, \dots, 0) = 0$ , mentre per il Lemma 8.2.1 esistono  $a_0, \dots, a_n \in \mathbb{K}$  tali che  $f(a_0, \dots, a_n) \neq 0$ . Dunque gli  $a_i$  non sono tutti nulli ed il punto  $[a_0, \dots, a_n]$  non appartiene a  $V(f)$ . □

DEFINIZIONE 8.3.4. Chiameremo **ipersuperficie proiettiva** ciascun sottoinsieme del tipo  $V(f) \subset \mathbb{P}^n$ , con  $f$  polinomio omogeneo di grado positivo.

Ogni ipersuperficie in  $\mathbb{P}^1$  è un insieme finito e non vuoto di punti. Infatti, se  $f \in \mathbb{K}[x_0, x_1]$  è omogeneo di grado  $d > 0$  per il Lemma 8.3.1 esiste una scomposizione in fattori lineari

$$f(x_0, x_1) = \prod_{i=1}^d (a_i x_0 + b_i x_1)$$

e quindi  $V(f) = \{[b_i, -a_i] \mid i = 1, \dots, d\}$ . Lo stesso argomento prova che ogni sottoinsieme finito di  $\mathbb{P}^1$  è una ipersuperficie. Da tale osservazione segue in particolare che per ogni coppia di polinomi omogenei  $f, g \in \mathbb{K}[x_0, x_1]$  si ha  $V(f) \cap V(g) \neq \emptyset$  se e solo se  $f, g$  hanno un fattore comune.

LEMMA 8.3.5. *Le ipersuperfici proiettive intersecano ogni retta, ossia per ogni  $X \subset \mathbb{P}^n$  ipersuperficie ed ogni retta proiettiva  $L \subset \mathbb{P}^n$  vale  $L \cap X \neq \emptyset$ . In particolare  $X$  è infinito se  $n \geq 2$ .*

DIMOSTRAZIONE. Fissiamo un sistema di coordinate omogenee tali che  $L = \{x_2 = x_3 = \dots = x_n = 0\}$ , sia  $f$  un polinomio omogeneo tale che  $X = V(f)$  e consideriamo il polinomio  $g(x_0, x_1) = f(x_0, x_1, 0, \dots, 0)$ . Il polinomio  $g$  è nullo se e solo se  $L \subset X$ ; se  $L$  non è contenuta in  $X$  allora  $g$  è omogeneo dello stesso grado di  $f$  ed i punti di  $L \cap X$  corrispondono allora ai fattori lineari di  $g$ .

Se  $n \geq 2$  e  $o \in \mathbb{P}^n$  non appartiene ad  $X$ , allora ogni retta passante per  $o$  interseca  $X$  e l'applicazione

$$X \rightarrow \{\text{rette per } o\}, \quad p \mapsto \overline{op},$$

è surgettiva. In particolare  $X$  è un sottoinsieme infinito di  $\mathbb{P}^n$ .  $\square$

Si osserva immediatamente che più polinomi omogenei possono definire la medesima ipersuperficie, ad esempio per ogni costante  $c \neq 0$  e per ogni polinomio omogeneo  $f$  si ha  $V(cf) = V(f)$ , ed anche  $V(f) = V(f^2) = V(f^3) = \dots$ . Per ogni coppia di polinomi omogenei  $f, g$ , vale la regola  $V(fg) = V(f) \cup V(g)$ , mentre l'intersezione  $V(f) \cap V(g)$  può essere scritta convenientemente nella forma  $f(x) = g(x) = 0$ .

Fortunatamente, almeno nel caso in cui  $f$  è irriducibile, il seguente teorema permette di ricostruire  $f$  (a meno di costanti moltiplicative) dalla ipersuperficie  $f(x) = 0$ .

TEOREMA 8.3.6 (degli zeri per ipersuperfici). *Siano  $\mathbb{K}$  algebricamente chiuso e  $f, g \in \mathbb{K}[x_0, \dots, x_n]$  polinomi omogenei con  $f$  irriducibile. Allora  $V(f) \subseteq V(g)$  se e solo se  $f$  divide  $g$ .*

DIMOSTRAZIONE. Abbiamo già visto che se  $f$  divide  $g$  allora  $V(f) \subseteq V(g)$ . Viceversa se  $f$  è irriducibile e non divide  $g$ , allora ha grado positivo e per il Lemma 8.3.3 esiste un punto  $o \notin V(f)$ . A meno di un cambio lineare di coordinate, possiamo supporre che  $o = [1, 0, \dots, 0]$ .

Siano  $a$  il grado di  $f$  e  $b$  il grado di  $g$ . Se  $f$  non divide  $g$ , allora  $f$  e  $g$  non hanno fattori comuni ed abbiamo visto nel Teorema 8.2.4 che esiste un intero  $d > 0$  e due polinomi omogenei  $h$ , di grado  $d - a$ , e  $k$ , di grado  $d - b$ , tali che

$$0 \neq r = hf - kg \in \mathbb{K}[x_1, \dots, x_n].$$

Mostriamo adesso che l'ipersuperficie  $V(r)$  è una unione di rette passanti per il punto  $o$ , ossia che se  $p \in V(r) - \{o\}$ , allora  $\overline{op} \subset V(r)$ .

Siccome  $r$  contiene solo monomi in  $x_1, \dots, x_n$  si ha  $o \in V(r)$ . Se  $p \neq o$  e  $p \in V(r)$ , allora  $p = [a_0, \dots, a_n]$  con  $a_1, \dots, a_n$  non tutti nulli e tali che  $r(a_1, \dots, a_n) = 0$ . Ne segue che  $V(r)$  contiene tutti i punti della retta affine  $\overline{op} - \{o\}$ , ossia tutti i punti di coordinate omogenee  $[a_0 + t, \dots, a_n]$ ,  $t \in \mathbb{K}$ .

Supponiamo adesso per assurdo  $V(f) \subset V(g)$ , allora  $V(f) \subset V(r)$ . Infatti, se  $p \in V(f)$  e  $p = [x]$  con  $x \in \mathbb{K}^{n+1} - \{0\}$ , allora  $p \in V(g)$  e quindi  $f(x) = g(x) = 0$ ,

$$r(x) = h(x)f(x) - k(x)g(x) = 0.$$

D'altra parte ogni retta passante per  $o$  interseca  $V(f)$ , quindi interseca  $V(r)$  in un punto diverso da  $o$ , quindi è interamente contenuta in  $V(r)$ . Ma questo implicherebbe  $V(r) = \mathbb{P}^n$  in contraddizione con la condizione  $r \neq 0$ .  $\square$

COROLLARIO 8.3.7. *Siano  $\mathbb{K}$  campo algebricamente chiuso e  $f, g \in \mathbb{K}[x_0, \dots, x_n]$  polinomi omogenei irriducibili. Allora  $V(f) = V(g)$  se e solo se  $f$  e  $g$  differiscono per una costante moltiplicativa. In particolare  $f$  e  $g$  hanno lo stesso grado.*

DIMOSTRAZIONE. Per il Teorema 8.3.6, siccome  $V(f) = V(g)$  ne consegue che  $f$  divide  $g$  e  $g$  divide  $f$ .  $\square$

Notiamo che il Corollario 8.3.7 sarebbe falso senza l'ipotesi sulla chiusura algebrica del campo. Ad esempio per  $\mathbb{K} = \mathbb{R}$  i polinomi  $f = x_0^2 + x_1^2$ ,  $g = x_0^2 + 2x_1^2$  sono irriducibili e  $V(f) = V(g) = \emptyset$ .

DEFINIZIONE 8.3.8. Se il campo  $\mathbb{K}$  è algebricamente chiuso, chiameremo **ipersuperficie proiettiva irriducibile di grado  $d$**  ciascun sottoinsieme del tipo  $V(f)$ , con  $f$  polinomio omogeneo irriducibile di grado  $d$ .

Ogni ipersuperficie proiettiva è unione finita di ipersuperfici irriducibili. Infatti se  $f$  è omogeneo e  $f = f_1^{a_1} \cdots f_r^{a_r}$  è la sua decomposizione in fattori irriducibili, allora ciascun  $f_i$  è omogeneo e

$$V(f) = V(f_1^{a_1}) \cup \cdots \cup V(f_r^{a_r}) = V(f_1) \cup \cdots \cup V(f_r).$$

### Esercizi.

ESERCIZIO 13. Provare che l'applicazione

$$\mathbb{P}^1 \rightarrow \mathbb{P}^n, \quad [t_0, t_1] \mapsto [t_0^n, t_0^{n-1}t_1, \dots, t_0t_1^{n-1}, t_1^n],$$

è ben definita, iniettiva ed ha come immagine il sottoinsieme

$$X = \left\{ [x_0, \dots, x_n] \in \mathbb{P}^n \mid \text{rank} \begin{pmatrix} x_0 & x_1 & \cdots & x_{n-1} \\ x_1 & x_2 & \cdots & x_n \end{pmatrix} = 1 \right\}.$$

Scrivere inoltre  $X$  come intersezione finita di ipersuperfici.

## 8.4. Curve piane

Da questo punto, e fino alla fine del capitolo restringeremo la nostra attenzione alle ipersuperfici di  $\mathbb{P}^2$ , altrimenti dette curve piane. Salvo avviso contrario indicheremo con  $S_d \subset \mathbb{K}[x_0, x_1, x_2]$  il sottospazio vettoriale dei polinomi omogenei di grado  $d$ . Abbiamo già provato che per ogni  $d \geq -2$  la dimensione di  $S_d$  è uguale a

$$\binom{d+2}{2} = \frac{(d+2)(d+1)}{2}.$$

In prima approssimazione possiamo definire una curva algebrica piana come il luogo dei punti di  $\mathbb{P}^2$  che annullano un polinomio omogeneo nelle coordinate omogenee di  $\mathbb{P}^2$ . Questa definizione, sebbene semplice, non è sufficientemente precisa e presenta qualche difficoltà operativa.

Già nella teoria delle coniche proiettive si incontrano certi oggetti detti “rette doppie” che, insiemisticamente sono rette, ma che appartengono allo spazio delle coniche di  $\mathbb{P}^2$ .

DEFINIZIONE 8.4.1. Sia  $x_0, x_1, x_2$  un sistema di coordinate omogenee su  $\mathbb{P}^2$ . Un sottoinsieme  $C \subset \mathbb{P}^2$  si dice una **curva irriducibile** di grado  $d$  se esiste un polinomio irriducibile omogeneo  $f(x_0, x_1, x_2)$  di grado  $d$  tale che  $C = V(f)$ , cioè

$$C = \{[x_0, x_1, x_2] \in \mathbb{P}^2 \mid f(x_0, x_1, x_2) = 0\}.$$

Ad esempio le rette di  $\mathbb{P}^2$  sono curve irriducibili di grado 1. La definizione di curva irriducibile non dipende dal particolare sistema di coordinate omogenee. Sia infatti  $y_0, y_1, y_2$  un altro sistema e  $x_i = \sum a_{ij}y_j$  con la matrice  $a_{ij}$  invertibile; se  $f(x_0, x_1, x_2) = g(y_0, y_1, y_2)$ , allora vale

$$f(y_0, y_1, y_2) = 0 \quad \text{se e solo se} \quad [y_0, y_1, y_2] \in C.$$

Inoltre il grado di  $f$  è uguale al grado di  $g$  e  $f$  è irriducibile se e solo se  $g$  è irriducibile.

Fissato un sistema di coordinate omogenee  $x_i$ , una curva irriducibile  $C$  determina a meno di costante moltiplicativa il polinomio  $f$  di cui è luogo di zeri. Infatti se  $g(x_0, x_1, x_2) = 0$  per ogni  $[x] \in C$  allora, per il Teorema 8.3.6,  $f$  divide  $g$  e se  $g$  è irriducibile allora  $g = af$  per qualche  $a \in \mathbb{K}$ .

DEFINIZIONE 8.4.2. Una curva algebrica piana è una combinazione lineare formale  $C = m_1C_1 + m_2C_2 + \cdots + m_rC_r$  dove, per ogni indice  $i$ ,  $C_i$  è una curva irriducibile e  $m_i$  è un intero positivo.

- Le curve  $C_i$  si dicono le **componenti irriducibili** di  $C$ .
- Per ogni  $i = 1, \dots, r$ , il numero  $m_i$  viene detto la **molteplicità** della componente  $C_i$ .

- Il sottoinsieme  $\text{Supp}(C) = \cup C_i \subset \mathbb{P}^2$  è detto il **supporto** della curva. Con un leggero abuso di notazione, se  $C$  è una curva e  $p \in \mathbb{P}^2$ , scriveremo  $p \in C$  per indicare che  $p \in \text{Supp}(C)$ . Similmente se  $C, D$  sono due curve scriveremo  $C \cap D$  per indicare l'intersezione dei supporti  $\text{Supp}(C) \cap \text{Supp}(D)$ .
- Se  $n_1, \dots, n_r$  sono i gradi delle componenti irriducibili  $C_1, \dots, C_r$ , allora il numero  $\deg(C) = n_1 m_1 + \dots + n_r m_r$  è detto il **grado** di  $C$ .
- Una componente irriducibile  $C_i$  si dice **multipla** se la sua molteplicità  $m_i$  è maggiore di 1; la curva  $C$  si dice **ridotta** se non possiede componenti multiple, ovvero se  $m_i = 1$  per ogni  $i$ .

Se  $C$  e  $D$  sono curve, la loro "somma"  $C + D$  è la curva che ha come componenti irriducibili l'unione delle componenti di  $C$  e  $D$  e come molteplicità la somma delle stesse, dove si intende che la molteplicità di una curva irriducibile è uguale a 0 se tale curva non è una componente. Il grado della somma è uguale alla somma dei gradi.

Nel resto del capitolo, con il termine curva intenderemo sempre una curva algebrica piana. Le curve di grado 1, 2, 3, 4, 5 e 6 si possono anche chiamare rispettivamente rette, coniche, cubiche, quartiche, quintiche e sestiche.

Fissato un sistema di coordinate omogenee  $x_0, x_1, x_2$ , esiste una bigezione fra l'insieme delle curve algebriche di grado  $n$  ed il proiettivizzato dello spazio vettoriale dei polinomi omogenei di grado  $n$  nelle variabili  $x_0, x_1, x_2$ . Infatti, se  $f$  è un polinomio omogeneo di grado  $n$ , allora esiste una decomposizione in fattori irriducibili  $f = f_1^{m_1} \cdots f_r^{m_r}$ : possiamo quindi associare ad  $f$  la curva le cui componenti irriducibili  $C_i = V(f_i)$  sono i luoghi di zeri dei polinomi  $f_i$  aventi molteplicità  $m_i$ . Per l'unicità della fattorizzazione, la curva  $C = m_1 C_1 + \dots + m_r C_r$  risulta ben definita e la denoteremo spesso come la curva di equazione  $f(x) = 0$ .

Sia data viceversa una curva  $C = \sum m_i C_i$ ; per definizione di curva irriducibile possiamo scrivere  $C_i = V(f_i)$ , con  $f_i$  polinomio omogeneo irriducibile per ogni  $i$  e considerare il prodotto  $f = \prod f_i^{m_i}$ . Essendo il polinomio  $f_i$  definito a meno di costante moltiplicativa, anche  $f$  è definito a meno di costante moltiplicativa.

Si noti che in tale corrispondenza biunivoca vale la relazione  $\text{Supp}(C) = V(f)$ .

Ogni coppia di curve piane  $V(f)$  e  $V(g)$  ha intersezione non vuota: se  $f$  e  $g$  hanno un fattore comune  $f = hf'$ ,  $g = hg'$ , allora  $V(f) = V(h) \cup V(f')$ ,  $V(g) = V(h) \cup V(g')$  e di conseguenza

$$\emptyset \neq V(h) \subseteq V(f) \cap V(g).$$

Se  $f$  e  $g$  non hanno fattori comuni, il fatto che le due curve si intersecano segue dai seguenti due lemmi.

**LEMMA 8.4.3.** *Siano  $f, g \in \mathbb{K}[x_0, x_1, x_2]$  polinomi senza fattori comuni ed omogenei di gradi  $a, b > 0$ , rispettivamente a coefficienti in un campo algebricamente chiuso. Allora esistono due polinomi omogenei  $h, k \in \mathbb{K}[x_0, x_1, x_2]$  di gradi  $(b-1)a, (a-1)b$  rispettivamente tali che  $hf + kg$  è il prodotto di  $ab$  polinomi omogenei non nulli di grado 1.*

**DIMOSTRAZIONE.** Per il caso  $n = 2$  del Teorema 8.2.4 esistono due polinomi omogenei  $h, k \in \mathbb{K}[x_0, x_1, x_2]$  di gradi  $(b-1)a, (a-1)b$  rispettivamente tali che

$$0 \neq hf + kg \in \mathbb{K}[x_1, x_2],$$

mentre per il Lemma 8.3.1 ogni polinomio omogeneo in due variabili è un prodotto di fattori lineari.  $\square$

**LEMMA 8.4.4.** *Sia  $\mathbb{K}$  algebricamente chiuso. Siano  $f \in S_a$  e  $g \in S_b$ ,  $a, b > 0$ , polinomi senza fattori comuni, allora  $V(f) \cap V(g) \neq \emptyset$ . Più precisamente, se è  $d$  il minimo intero per cui esiste una relazione del tipo*

$$(8.4) \quad 0 \neq pf - qg = l_1 l_2 \cdots l_d$$

per opportuni  $l_1, \dots, l_d \in S_1$ ,  $p \in S_{d-a}$ ,  $q \in S_{d-b}$ . Allora  $V(f) \cap V(g) \cap V(l_i) \neq \emptyset$  per ogni  $i$ .

**DIMOSTRAZIONE.** Osserviamo preliminarmente che l'enunciato del lemma ha senso in virtù del Lemma 8.4.3 e che inoltre vale  $\min(a, b) \leq d \leq ab$ . Per evidenti motivi di simmetria

basta dimostrare che  $V(f) \cap V(g) \cap V(l_1) \neq \emptyset$  e fissiamo un sistema di coordinate omogenee  $x_0, x_1, x_2$  tali che  $l_1 = x_2$ . In linea teorica abbiamo la seguente dicotomia:

- (1) i due polinomi  $f(x_0, x_1, 0), g(x_0, x_1, 0)$  hanno fattori comuni, oppure
- (2) i due polinomi  $f(x_0, x_1, 0), g(x_0, x_1, 0)$  sono relativamente primi.

Nel primo caso se  $h$  è un polinomio omogeneo di grado positivo che divide  $f(x_0, x_1, 0)$  e  $g(x_0, x_1, 0)$ , allora  $V(h) \cap V(l_1)$  è non vuoto (intersezione di ipersuperficie con una retta) ed è contenuto in  $V(f) \cap V(g) \cap V(l_1)$ .

Proviamo adesso che il secondo caso conduce ad una contraddizione e quindi va escluso dalla lista delle possibilità. Supponiamo per assurdo che i polinomi  $f(x_0, x_1, 0)$  e  $g(x_0, x_1, 0)$  non abbiano fattori comuni e siano  $p, q$  come nell'enunciato.

Siccome  $x_2$  divide  $pf - qg$  si ha

$$p(x_0, x_1, 0)f(x_0, x_1, 0) - q(x_0, x_1, 0)g(x_0, x_1, 0) = 0$$

e per la fattorizzazione unica in  $\mathbb{K}[x_0, x_1, x_2]$  esiste  $r \in S_{d-a-b}$  tale che

$$(8.5) \quad p(x_0, x_1, 0) = g(x_0, x_1, 0)r(x_0, x_1, 0), \quad q(x_0, x_1, 0) = f(x_0, x_1, 0)r(x_0, x_1, 0).$$

I due polinomi omogenei  $p - gr$  e  $q - fr$  sono entrambi divisibili per  $x_2$ , ossia esistono  $h \in S_{d-a-1}$  e  $k \in S_{d-b-1}$  tali che  $x_2h = p - gr$  e  $x_2k = q - fr$ . Ma allora

$$x_2hf - x_2kg = (p - gr)f - (q - fr)g = pf - qg = x_2l_2 \cdots l_d$$

da cui segue  $hf - kg = l_2 \cdots l_d$ , in contraddizione con la minimalità di  $d$ .  $\square$

OSSERVAZIONE 8.4.5. Nella situazione del Lemma 8.4.4, le rette  $V(l_i)$  non sono univocamente determinate da  $f, g$ , anche nel caso in cui l'intero  $d$  è il minimo possibile.

Il caso limite è quando  $f, g$  hanno entrambi grado 1 ed al variare di  $(p, q) \in \mathbb{K}^2 - \{0\}$  le rette  $V(pf - qg)$  sono tutte e sole le rette passanti per il punto  $f(x) = g(x) = 0$ .

Come ulteriore esempio si considerino i polinomi di secondo grado  $f = x_0x_1, g = x_2(x_0 + x_1 + x_2)$ . Allora, oltre alle ovvie scomposizioni in fattori lineari  $1f + 0g = x_0x_1$  e  $0f + 1g = x_2(x_0 + x_1 + x_2)$  si ha:

$$f + g = (x_0 + x_2)(x_1 + x_2).$$

LEMMA 8.4.6. *Siano  $X \subset \mathbb{P}^2$  e  $d$  un intero positivo. Se per ogni punto  $q \in \mathbb{P}^2$  l'insieme  $X$  è contenuto nell'unione di  $d$  rette passanti per  $q$ , allora  $X$  contiene al più  $d$  punti distinti.*

DIMOSTRAZIONE. Supponiamo per assurdo che esistano  $p_0, \dots, p_d \in X$  punti distinti; siccome il campo  $\mathbb{K}$  è infinito possiamo trovare un punto  $p \in \mathbb{P}^2$  non appartenente all'unione delle  $d(d+1)/2$  rette  $\overline{p_i p_j}$ ,  $0 \leq i < j \leq d$ . Dunque per ogni  $i \neq j$  i tre punti  $q, p_i, p_j$  non sono allineati, ogni retta per  $q$  contiene al più un punto  $p_i$  e quindi  $X$  non è contenuto in  $d$  rette passanti per  $q$ .  $\square$

TEOREMA 8.4.7 (Bézout debole). *Siano  $f, g \in \mathbb{K}[x_0, x_1, x_2]$  polinomi omogenei senza fattori comuni di gradi  $a, b > 0$ . Allora l'intersezione  $f(x) = g(x) = 0$  delle corrispondenti ipersuperfici proiettive è non vuota e contiene al più  $ab$  punti distinti.*

DIMOSTRAZIONE. Abbiamo già dimostrato che  $V(f) \cap V(g) \neq \emptyset$ . Per il lemma precedente basta dimostrare che per ogni punto  $q \in \mathbb{P}^2$ , l'intersezione è contenuta nell'unione di  $ab$  rette passanti per  $q$ . A meno di un cambio di coordinate omogenee possiamo supporre  $q = [1, 0, 0]$  e per il Lemma 8.4.3 esistono due polinomi omogenei  $h, k$  tali che  $hf + kg$  è un polinomio omogeneo non nullo di grado  $ab$  in  $x_1, x_2$ . Dunque

$$0 \neq hf + kg = \prod_{i=1}^{ab} (a_i x_1 + b_i x_2)$$

per opportune costanti  $a_i, b_i \in \mathbb{K}$  e  $V(f) \cap V(g)$  è contenuto nell'unione delle rette di equazione  $a_i x_1 + b_i x_2 = 0$ ,  $i = 1, \dots, ab$ .  $\square$

ESEMPIO 8.4.8. Su  $\mathbb{K} = \mathbb{C}$ , per ogni  $n > 0$  consideriamo i tre di polinomi omogenei di grado  $n$ :

$$f_n = \prod_{i=1}^n (x_0 - i x_1), \quad g_n = \prod_{j=1}^n (x_2 - j x_1), \quad h_n = \prod_{i=1}^n (x_0 + i x_1).$$

Allora per ogni  $a, b > 0$  l'intersezione  $V(f_a) \cap V(h_b)$  contiene solo il punto  $[0, 0, 1]$ , mentre  $V(f_a) \cap V(g_b)$  è formata dagli  $ab$  punti distinti  $[i, 1, j]$ ,  $i = 1, \dots, a$ ,  $j = 1, \dots, b$ .

**COROLLARIO 8.4.9.** *Sia  $f$  polinomio omogeneo di grado  $n$  e sia  $L \subset \mathbb{P}^2$  una retta. Se  $L \cap V(f)$  contiene almeno  $n + 1$  punti distinti, allora l'equazione di  $L$  divide  $f$ .*

**DIMOSTRAZIONE.** L'equazione di  $L$  è un polinomio omogeneo  $l$  di grado 1. Se  $l$  non divide  $f$ , siccome  $l$  è irriducibile, i polinomi  $l, f$  non hanno fattori comuni. Per il teorema di Bézout 8.4.7 l'intersezione  $L \cap V(f)$  contiene al più  $n$  punti distinti.  $\square$

Possiamo accomunare e riscrivere in modo "geometrico" il Lemma 8.4.4 ed il Teorema 8.4.7.

**TEOREMA 8.4.10.** *Siano  $C$  e  $D$  due curve algebriche di gradi  $a$  e  $b$  rispettivamente. Allora:*

- (1)  $C \cap D \neq \emptyset$ .
- (2) *Se  $C \cap D$  contiene più di  $ab$  punti, allora  $C$  e  $D$  hanno una componente irriducibile in comune.*

**COROLLARIO 8.4.11.** *Due curve irriducibili distinte di gradi  $a, b$  hanno al più  $ab$  punti in comune.*

**DIMOSTRAZIONE.** Immediata.  $\square$

Sia  $f(x_0, x_1, x_2) = 0$  l'equazione di una curva  $C$  e sia  $p = [v_0, v_1, v_2] \in \mathbb{P}^2$ . Diremo che  $p$  è un **punto singolare** di  $C$  se

$$f(v_0, v_1, v_2) = 0 \quad \text{e} \quad \frac{\partial f}{\partial x_i}(v_0, v_1, v_2) = 0 \quad \text{per ogni } i = 0, 1, 2.$$

Si noti che:

1) La definizione di punto singolare è una buona definizione: infatti essendo  $f$  omogeneo, anche le sue derivate parziali sono omogenee. Inoltre se  $y_0, y_1, y_2$  è un diverso sistema di coordinate e  $g$  è un'equazione di  $C$  nelle coordinate  $y_i$ , allora si ha  $g(y) = af(x)$  per qualche  $a \in \mathbb{K}$  e quindi

$$\frac{\partial g}{\partial y_i} = a \sum_{j=0}^2 \frac{\partial g}{\partial x_j} \frac{\partial x_j}{\partial y_i}$$

2) Se il campo  $\mathbb{K}$  ha caratteristica 0, e più in generale se la caratteristica del campo non divide il grado di  $f$ , allora dalla formula di Eulero segue che un punto  $p$  è singolare per la curva di equazione  $f$  se e solo se  $p$  annulla tutte le derivate parziali di  $f$ .

3) Se  $C$  è irriducibile di grado  $n$  e di equazione  $f(x) = 0$  allora, essendo  $\mathbb{K}$  algebricamente chiuso, per il Lemma 8.2.6 esiste una derivata parziale di  $\frac{\partial f}{\partial x_i}$  non nulla. Il Teorema Teorema 8.4.10 applicato alle curve  $C$  e  $V(\frac{\partial f}{\partial x_i})$  implica che  $C$  ha al più  $n(n-1)$  punti singolari.<sup>1</sup>

I punti di una curva che non sono singolari si dicono **lisci**. Una curva **singolare** è una curva che contiene almeno un punto singolare. Una curva che non ha punti singolari si dice **non singolare** oppure **liscia**.

**ESEMPIO 8.4.12.** Sul campo dei numeri complessi consideriamo la curva  $C$  di equazione  $f(x_0, x_1, x_2) = x_0^3 + ax_1^3 + bx_2^3 = 0$ ,  $a, b \in \mathbb{C}$ . Allora  $C$  è singolare se e solo se  $ab = 0$ . Infatti

$$\frac{\partial f}{\partial x_0} = 3x_0^2, \quad \frac{\partial f}{\partial x_1} = 3ax_1^2, \quad \frac{\partial f}{\partial x_2} = 3bx_2^2.$$

Se  $a = 0$  allora  $[0, 1, 0]$  è un punto singolare, se  $b = 0$  allora  $[0, 0, 1]$  è un punto singolare. Se  $a, b \neq 0$  allora non esistono punti di  $\mathbb{P}^2$  che annullano tutte e tre le derivate.

**PROPOSIZIONE 8.4.13.** *Siano  $C_1, \dots, C_r$  curve algebriche (non necessariamente irriducibili e/o distinte) e sia  $C = C_1 + \dots + C_r$ . Allora:*

<sup>1</sup>In realtà una curva irriducibile di grado  $n$  ha al più  $(n-1)(n-2)/2$  punti singolari, ma la dimostrazione di questo fatto richiede alcune tecniche leggermente più sofisticate che non sono trattate in queste note, cf. [22].

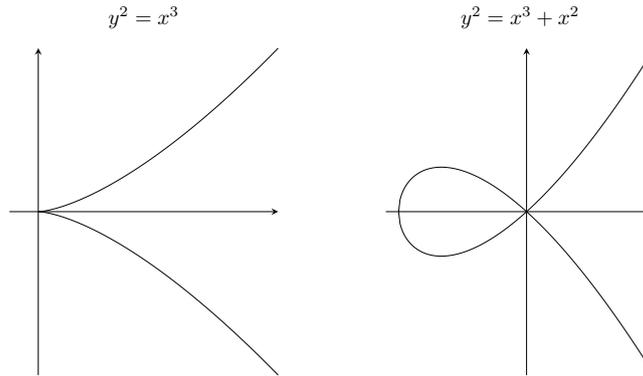


FIGURA 1. Due esempi di cubiche irriducibili singolari

- (1) Se  $p \in C_i \cap C_j$  per qualche  $i \neq j$ , allora  $p$  è un punto singolare di  $C$ . In particolare ogni curva liscia è irriducibile.
- (2) Se  $p \in C_i$  e  $p \notin C_j$  per ogni  $j \neq i$ , allora  $p$  è un punto singolare di  $C$  se e solo se è un punto singolare di  $C_i$ .
- (3) Una curva è ridotta se e solo se possiede un numero finito di punti singolari.

DIMOSTRAZIONE. Sia  $f_i$  un'equazione della curva  $C_i$ , allora  $f = f_1 \cdots f_r$  è un'equazione per  $C$ . Se  $p \in C_i \cap C_j$ , con  $i \neq j$ , allora  $f_i(p) = f_j(p) = 0$  e per la regola di Leibniz ogni derivata parziale di  $f$  si annulla in  $p$ ; questo prova 1). Se la curva  $C$  non è irriducibile, allora si può scrivere  $C = C_1 + C_2$  ed abbiamo già dimostrato che  $C_1 \cap C_2 \neq \emptyset$ .

Se invece  $f_i(p) = 0$  e  $f_j(p) \neq 0$  per ogni  $j \neq i$ , allora la regola di Leibniz implica che, per ogni  $h = 0, 1, 2$  vale  $\frac{\partial f}{\partial x_h}(p) = 0$  se e solo se  $\frac{\partial f_i}{\partial x_h}(p) = 0$ , e questo prova il punto 2).

Siccome una curva  $C = C_1 + \cdots + C_r$ , con le  $C_i$  irriducibili, è ridotta se e solo se le  $C_i$  sono distinte, il punto 3) segue dai punti precedenti e dal fatto che ogni curva irriducibile possiede un numero finito di punti singolari.  $\square$

Dunque ogni curva piana liscia è irriducibile, mentre il viceversa è falso. Ad esempio sono irriducibili e singolari nel punto  $[1, 0, 0]$  tutte le cubiche di equazione

$$x_0x_2^2 = x_1^3 + \lambda x_0x_1^2, \quad \lambda \in \mathbb{K}.$$

Osserviamo che a meno di proiettività la precedente famiglia di cubiche si riduce all'insieme delle due di equazioni  $x_0x_2^2 = x_1^3$  e  $x_0x_2^2 = x_1^3 + x_0x_1^2$ . Infatti se  $\lambda \neq 0$  e  $\xi \in \mathbb{K}$  è una radice quadrata di  $\lambda$ , la proiettività

$$[x_0, x_1, x_2] \mapsto [\xi x_0, \xi^3 x_1, \xi^4 x_2]$$

trasforma la cubica di equazione  $x_0x_2^2 = x_1^3 + \lambda x_0x_1^2$  in quella di equazione  $x_0x_2^2 = x_1^3 + x_0x_1^2$ .

ESEMPIO 8.4.14. Al variare dei parametri  $p, q \in \mathbb{K}$ , si consideri le cubica  $C \subset \mathbb{P}^2$  di equazione

$$x_0x_2^2 = x_1^3 + px_0^2x_1 + qx_0^3,$$

che nelle coordinate affini  $x = x_1/x_0$  e  $y = x_2/x_0$  diventa

$$y^2 = x^3 + px + q, \quad p, q \in \mathbb{K}.$$

Definiamo il suo *discriminante* come  $\Delta = 4p^3 + 27q^2$ . Se il campo ha caratteristica diversa da 2, allora  $C$  è singolare se e solo se  $\Delta = 0$ .

Per definizione i punti singolari di  $C$  sono le soluzioni in  $\mathbb{P}^2$  del sistema di equazioni omogenee

$$\begin{cases} x_0x_2^2 = x_1^3 + px_0^2x_1 + qx_0^3 \\ x_2^2 = 2px_0x_1 + 3qx_0^2 \\ 0 = 3x_1^2 + px_0^2 \\ 2x_0x_2 = 0 \end{cases}$$

Osserviamo preliminarmente che non esistono punti singolari sulla retta di equazione  $x_0 = 0$ . Infatti se  $x_0 = 0$  dalla prima equazione segue  $x_1^3 = 0$  e dalla seconda  $x_2^2 = 0$ , da cui  $x_0 = x_1 = x_2 = 0$  che non definisce alcun punto del piano proiettivo. Quindi ogni eventuale punto singolare sarà del tipo  $[1, x, y]$  con  $x, y \in \mathbb{K}$  soluzioni del sistema di equazioni

$$\begin{cases} y^2 = x^3 + px + q \\ y^2 = 2px + 3q \\ 0 = 3x^2 + p \\ 2y = 0 \end{cases}$$

Si noti che in caratteristica 2 tale sistema ammette l'unica soluzione  $x = \sqrt{p}$ ,  $y = \sqrt{q}$ , mentre in caratteristica  $\neq 2$  segue dall'ultima equazione che  $y = 0$  e  $x \in \mathbb{K}$  è una soluzione del sistema

$$\begin{cases} 0 = x^3 + px + q \\ 0 = 2px + 3q \\ 0 = 3x^2 + p \end{cases}$$

Consideriamo separatamente i due casi  $p = 0$  e  $p \neq 0$ . Se  $p = 0$  si ha  $\Delta = -27q^2$ ,  $q\Delta = (-3q)^3$  e quindi  $\Delta = 0$  se e solo se  $3q = 0$ . Il sistema di equazioni diventa

$$0 = x^3 + q = 3q = 3x^2$$

che ammette soluzioni se e solo se  $3q = 0$ : infatti se  $3q = 0$  e  $x$  è una soluzione di  $x^3 + q = 0$ , si ha  $(3x^2)^3 = 27x^6 = 27q^2 = 0$ .

Se  $p \neq 0$ , dalla seconda equazione segue  $x = -\frac{3q}{2p}$  ed il sistema si riduce a

$$0 = -\frac{27q^3}{8p^3} - \frac{3q}{2} + q = \frac{27q^2}{4p^2} + p \iff 0 = -q(27q^2 + 4p^3) = 27q^2 + 4p^3.$$

### Esercizi.

ESERCIZIO 14. Provare che per ogni curva algebrica  $C$ , il supporto  $\text{Supp}(C)$  è un sottoinsieme proprio e infinito di  $\mathbb{P}^2$ .

ESERCIZIO 15. Mostrare che in caratteristica 0, per ogni intero positivo  $n$  la curva di equazione  $x_0^n + x_1^n + x_2^n = 0$  è liscia.

ESERCIZIO 16. In caratteristica  $\neq 2, 3$ , determinare per quali valori del parametro  $\lambda \in \mathbb{K}$  risultano singolari le cubiche di equazioni

$$x_0x_2^2 = x_1(x_1 + x_0)(x_1 + \lambda x_0), \quad x_0^3 + x_1^3 + x_2^3 - 3\lambda x_0x_1x_2 = 0.$$

ESERCIZIO 17. Siano  $C_1, \dots, C_r$  curve piane di gradi  $n_1 \geq n_2 \geq \dots \geq n_r$  e sia  $V = C_1 \cap \dots \cap C_r$ . Dimostrare che se  $V$  è finito, allora contiene al più  $n_1 n_r$  punti.

ESERCIZIO 18. Determinare e descrivere i punti singolari (su  $\mathbb{C}$ ) delle curve di equazioni

$$y^3(4z - y)^3 - 4x^4(x + 3z)^2 = 0, \quad (8y - x - z)^3 = 216xyz, \quad (x^2 - z^2)^2y = (y^2 - z^2)^2x.$$

### 8.5. Retta tangente e punti di flesso

Sia  $C$  una curva algebrica piana di grado  $n$  ed equazione  $f(x) = 0$  e sia  $L \subset \mathbb{P}^2$  una retta. Se  $L$  è contenuta nel supporto di  $C$ , allora  $L$  è una componente irriducibile di  $C$ ; se invece  $L$  non è una componente irriducibile di  $C$ , allora presi due punti distinti  $p = [p_0, p_1, p_2]$  e  $q = [q_0, q_1, q_2]$  sulla retta  $L$ , il polinomio

$$F(t_0, t_1) = f(t_0 p_0 + t_1 q_0, t_0 p_1 + t_1 q_1, t_0 p_2 + t_1 q_2)$$

è non nullo ed omogeneo di grado  $n$ . Esistono dunque  $n$  punti di  $L$ , *contati con molteplicità* in cui  $f = 0$ : chiaramente tali punti corrispondono all'intersezione della curva  $C$  con la retta  $L$ .

Se il punto  $p$  appartiene all'intersezione  $L \cap C$ , il calcolo della molteplicità di intersezione di  $L$  con  $C$  in  $p$  è molto semplice. Basta infatti calcolare la molteplicità di  $t = 0$  come radice del polinomio (non omogeneo)

$$F(1, t) = f(p_0 + t q_0, p_1 + t q_1, p_2 + t q_2).$$

**ESEMPIO 8.5.1.** Il punto  $p = [0, 0, 1]$  appartiene all'intersezione della cubica  $C$  di equazione  $f = x_0 x_2^2 - x_1^3 - x_0^3$  con la retta  $L$  di equazione  $x_0 + x_1 = 0$ . Calcoliamo la molteplicità di intersezione di  $L$  con  $C$  in  $p$ . Siccome il punto  $q = [1, -1, 0] \neq p$  appartiene a  $L$  basta calcolare la molteplicità in  $t = 0$  del polinomio  $f(t, -t, 1)$ . Dato che  $f(t, -t, 1) = t$  la molteplicità è 1. Notiamo inoltre che anche  $q \in L \cap C$  e dato che  $f(1, -1, t) = t^2$  la molteplicità di intersezione in  $q$  è uguale a 2.

**DEFINIZIONE 8.5.2.** Siano  $L$  una retta,  $C$  una curva e  $p \in L \cap C$ . Diremo che  $L$  è **tangente** a  $C$  nel punto  $p$  se la molteplicità di intersezione di  $L$  con  $C$  in  $p$  è strettamente maggiore di 1.

Diremo che  $L$  è tangente a  $C$  se lo è in qualche punto di  $C \cap L$ ; diremo che è trasversale se non è tangente.

Notiamo che, se esiste una retta trasversale ad una curva  $C$ , allora  $C$  deve essere necessariamente ridotta.

**PROPOSIZIONE 8.5.3.** Siano dati una curva  $C$  di equazione  $f$  e due punti distinti  $p = [p_0, p_1, p_2]$  e  $q = [q_0, q_1, q_2]$ , con  $p \in C$ . Allora la retta  $L = \overline{pq}$  è tangente a  $C$  in  $p$  se e solo se

$$\sum_{i=0}^2 q_i \frac{\partial f}{\partial x_i}(p_0, p_1, p_2) = 0.$$

**DIMOSTRAZIONE.** La retta  $L$  è tangente a  $C$  in  $p$  se e solo se  $t = 0$  è una radice multipla del polinomio  $g(t) = f(x_0 + t y_0, x_1 + t y_1, x_2 + t y_2)$ , cioè se e solo se  $g'(0) = 0$ , dove  $g'$  denota la derivata di  $f$  rispetto a  $t$ . Basta adesso applicare la regola di derivazione della funzione composta.  $\square$

**COROLLARIO 8.5.4.** Sia  $p = [p_0, p_0, p_1]$  un punto di una curva  $C$  di equazione  $f$ :

- (1) Se  $p$  è singolare, allora ogni retta per  $p$  è tangente a  $C$  in  $p$ .
- (2) Se  $p$  è liscio, allora esiste unica una retta tangente a  $C$  in  $p$  la cui equazione è

$$\sum_{i=0}^2 x_i \frac{\partial f}{\partial x_i}(p_0, p_1, p_2) = 0.$$

**DIMOSTRAZIONE.** Conseguenza immediata della Proposizione 8.5.3.  $\square$

**ESEMPIO 8.5.5.** Su campi di caratteristica  $\neq 2$ , l'equazione della retta tangente alla curva di equazione  $x_0^4 - x_1^2 x_2^2 = 0$  nel punto  $[1, 1, 1]$  è  $4x_0 - 2x_1 - 2x_2 = 0$ .

Le precedenti considerazioni forniscono un metodo per il calcolo delle rette tangenti ad una curva  $C$  passanti per un punto  $q \in \mathbb{P}^2$ . Se  $f(x) = 0$  è l'equazione di  $f$  e  $q = [q_0, q_1, q_2]$  abbiamo visto che, dato un punto  $p \in C$ ,  $p \neq q$ , la retta  $\overline{pq}$  è tangente a  $C$  in  $p$  se e solo se

$\sum_i q_i f_i(p) = 0$ . Quindi se  $q \notin C$  le rette tangenti a  $C$  passanti per  $q$  sono tutte e sole quelle del tipo  $\overline{pq}$  al variare di  $p$  tra le soluzioni del sistema di due equazioni

$$(8.6) \quad f(p) = \sum_i q_i f_i(p) = 0.$$

Se invece  $q \in C$  è un punto liscio, oltre a considerare le rette  $\overline{pq}$  con  $p \neq q$  che soddisfa (8.6) bisogna ovviamente aggiungere la retta tangente a  $C$  in  $q$ . Infine, se  $q \in C$  è singolare, ogni retta passante per  $q$  è tangente a  $C$ .

ESEMPIO 8.5.6. Su di un campo di caratteristica  $\neq 3$ , calcoliamo le rette passanti per il punto  $q = [1, 0, 0]$  e tangenti alla cubica di equazione  $x_0^3 + x_1^3 + x_2^3 = 0$ . Per determinare i punti  $p \in C$  tali che la retta  $\overline{pq}$  è tangente a  $C$  nel punto  $p$  bisogna risolvere il sistema di equazioni  $x_0^3 + x_1^3 + x_2^3 = 3x_0^2 = 0$  che è equivalente a  $x_0 = x_1^3 + x_2^3 = 0$  le cui soluzioni in  $\mathbb{P}^2$  sono

$$[0, -1, \xi], \quad [0, -1, \xi^2], \quad [0, -1, 1],$$

dove  $\xi$  è una radice cubica primitiva di 1. Le tre rette passanti per  $q$  e per i tre punti suddetti sono quelle di equazioni:

$$x_2 + \xi x_1 = 0, \quad x_2 + \xi^2 x_1 = 0, \quad x_2 + x_1 = 0, .$$

DEFINIZIONE 8.5.7. Data una curva  $C$  ed un suo punto liscio  $p$  denoteremo con  $\mathbb{T}_p C$  la retta tangente a  $C$  in  $p$ . Diremo che un punto liscio  $p \in C$  è un **flesso**, o un **punto di flessione**, di  $C$  se la molteplicità di intersezione di  $\mathbb{T}_p C$  con  $C$  nel punto  $p$  è maggiore od uguale a 3

Ad esempio, in una retta tutti i punti sono di flesso. Più in generale se la curva  $C$  è unione di rette allora ogni punto liscio di  $C$  è un flesso. Per il teorema di Bezout una conica possiede punti di flesso se e solo se è unione di rette.

Dato un polinomio omogeneo  $f \in \mathbb{K}[x_0, x_1, x_2]$ , per semplicità notazionale indichiamo

$$f_i = \frac{\partial f}{\partial x_i}, \quad f_{ij} = f_{ji} = \frac{\partial^2 f}{\partial x_i \partial x_j}.$$

Si definisce la matrice Hessiana di  $f$  come:

$$H(x) = \begin{pmatrix} f_{00} & f_{01} & f_{02} \\ f_{10} & f_{11} & f_{12} \\ f_{20} & f_{21} & f_{22} \end{pmatrix}.$$

Se  $f$  ha grado  $d \geq 2$  i coefficienti di  $H(x)$  sono polinomi di grado  $d-2$  ed il suo determinante  $\det(H(x))$  è un polinomio omogeneo di grado  $3(d-2)$ .

LEMMA 8.5.8. Siano  $\mathbb{K}$  un campo algebricamente chiuso e  $H \in M_{3,3}(\mathbb{K})$  una matrice  $3 \times 3$  simmetrica. Denotando con  $\mathbb{K}^3$  lo spazio vettoriale numerico dei vettori colonna, le seguenti condizioni sono equivalenti:

- (1)  $\det(H) = 0$ ;
- (2) per ogni vettore non nullo  $v \in \mathbb{K}^3$  tale che  $v^T H v = 0$  esiste un vettore  $u \in \mathbb{K}^3$  linearmente indipendente da  $v$  tale che  $u^T H v = u^T H u = 0$ .
- (3) esistono due vettori linearmente indipendenti  $v_1, v_2 \in \mathbb{K}^3$  tali che  $v_i^T H v_j = 0$  per ogni  $i, j$ ;

DIMOSTRAZIONE. 1 implica 2. Trattiamo separatamente i due casi  $Hv = 0$  e  $Hv \neq 0$ . Se  $Hv = 0$  completiamo  $v$  ad una base  $v_1, v_2, v_3 = v$  di  $\mathbb{K}^3$  e consideriamo il polinomio omogeneo di secondo grado

$$f(t_1, t_2) = (t_1 v_1 + t_2 v_2)^T H (t_1 v_1 + t_2 v_2).$$

Per ipotesi il campo  $\mathbb{K}$  è algebricamente chiuso e quindi esiste una coppia  $(t_1, t_2)$  non nulla tale che  $f(t_1, t_2) = 0$ . Allora il vettore  $u = t_1 v_1 + t_2 v_2$  è quello cercato.

Se  $Hv \neq 0$  è sufficiente prendere  $u$  un qualsiasi vettore non nullo tale che  $Hu = 0$ .

2 implica 3. Basta provare che esiste un vettore non nullo  $v \in \mathbb{K}^3$  tale che  $v^T H v = 0$ . Questo si prova esattamente come sopra, considerando due vettori linearmente indipendenti  $v_1, v_2$  ed il polinomio omogeneo  $f(t_1, t_2) = (t_1 v_1 + t_2 v_2)^T H (t_1 v_1 + t_2 v_2)$ .

3 *implica* 1. Supponiamo per assurdo che  $H$  sia invertibile, allora i vettori  $Hv_1, Hv_2$  sono linearmente indipendenti e la matrice  $A = (Hv_1, Hv_2) \in M_{3,2}(\mathbb{K})$  ha rango massimo. D'altra parte, il nucleo dell'applicazione lineare

$$A^T: \mathbb{K}^3 \rightarrow \mathbb{K}^2$$

coincide con l'insieme dei vettori  $u$  tali che  $u^T Hv_1 = u^T Hv_2 = 0$  e quindi contiene  $v_1, v_2$ , in contraddizione con il fatto che  $A^T$  ha rango 2.

Notiamo che quest'ultima implicazione non richiede che il campo sia algebricamente chiuso. D'altra parte se  $\mathbb{K} = \mathbb{R}$ , la coppia

$$H = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \quad v = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$$

soddisfa la condizione 1 ma non le condizioni 2 e 3. Sempre su  $\mathbb{R}$ , la matrice identità soddisfa la condizione 2 ma non soddisfa 3 ed 1. □

**TEOREMA 8.5.9.** *Sia  $C$  una curva piana di grado  $d$  ed equazione  $f(x) = 0$  e sia  $h(x)$  il determinante della matrice Hessiana  $H(x)$  di  $f$ . Se il campo base ha caratteristica 0 oppure ha caratteristica positiva  $p$ , con  $p \geq \max(3, d)$ , allora un punto liscio  $p \in C$  è un flesso di  $C$  se e solo se  $h(p) = 0$ .*

**DIMOSTRAZIONE.** Il teorema è banalmente verificato per le rette, non è quindi restrittivo supporte  $d \geq 2$ ; in tal caso le ipotesi sulla caratteristica del campo ci dicono che i numeri 2 e  $d - 1$  sono non nulli e quindi invertibili.

Fissiamo  $v \in \mathbb{K}^3 - \{0\}$  tale che  $p = [v]$ . Supponiamo che la matrice  $A = H(v)$  non sia invertibile, per la formula di Eulero

$$0 = d(d-1)f(v) = (d-1) \sum_i v_i f_i(v) = \sum_{i,j} v_i v_j f_{ij}(v) = v^T A v.$$

Per il Lemma 8.5.8 esiste un punto  $q = [u] \neq p$  tale che  $u^T A v = u^T A u = 0$ . Proviamo che la retta  $\overline{pq}$  è la retta tangente a  $C$  in  $p$  e che  $p$  è un punto di flesso, ossia che  $t = 0$  è una radice di molteplicità  $> 2$  del polinomio

$$(8.7) \quad g(t) = f(v + tu) = t \sum_i f_i(v) u_i + \frac{t^2}{2} \sum_{i,j} f_{ij}(v) u_i u_j + t^3(\dots).$$

Adesso basta osservare che

$$\sum_{i,j} f_{ij}(v) u_i u_j = u^T A u = 0$$

e che per la formula di Eulero

$$\sum_i f_i(v) u_i = \frac{1}{d-1} \sum_{i,j} f_{ij}(v) v_j u_i = \frac{1}{d-1} v^T A u = 0.$$

Viceversa, supponiamo che  $p$  sia un punto di flesso e che  $\overline{pq}$  sia la retta tangente a  $C$  in  $p$ , con  $p \neq q = [u]$ . Per (8.7) questo implica che

$$0 = (d-1) \sum_i f_i(v) u_i = \sum_{i,j} f_{ij}(v) v_i u_j = v^T A u, \quad 0 = \sum_{i,j} f_{ij}(v) u_i u_j = u^T A u,$$

e per il Lemma 8.5.8 la matrice  $A$  non è invertibile. □

**COROLLARIO 8.5.10.** *In un campo algebricamente chiuso di caratteristica 0 ogni curva piana liscia di grado  $\geq 3$  possiede punti di flesso.*

**DIMOSTRAZIONE.** il determinante della matrice Hessiana definisce una curva di grado  $3(d-2) > 0$  che quindi interseca  $C$ . □

**COROLLARIO 8.5.11.** *In un campo algebricamente chiuso di caratteristica  $\neq 2$  ogni curva piana liscia di grado 3 possiede punti di flesso.*

DIMOSTRAZIONE. Per le cubiche il Teorema 8.5.9 vale su campi di caratteristica  $\neq 2$  e si ragiona come nel corollario precedente.  $\square$

### Esercizi.

ESERCIZIO 19. Sul campo dei numeri complessi, si determini il numero di rette passanti per il punto  $[1, 1, 0]$  e tangenti alla curva di Fermat  $x_0^n + x_1^n + x_2^n = 0$ .

ESERCIZIO 20. Provare che in caratteristica positiva esistono curve irriducibili  $C$  e punti  $q \notin C$  tali che ogni retta passante per  $q$  è tangente a  $C$ .

## 8.6. Le coniche

In questa sezione assumeremo, salvo avviso contrario, che  $\mathbb{K}$  sia un campo algebricamente chiuso di caratteristica diversa da 2.

Una conica è una curva algebrica piana di grado 2. Due coniche si dicono proiettivamente equivalenti se esiste una proiettività di  $\mathbb{P}^2$  che trasforma l'una nell'altra. Una conica non irriducibile è unione di due rette che possono essere distinte o coincidenti. Chiameremo **rango** di una conica di equazione  $f(x_0, x_1, x_2) = 0$ , il il rango della matrice Hessiana

$$H = \begin{pmatrix} f_{00} & f_{01} & f_{02} \\ f_{10} & f_{11} & f_{12} \\ f_{20} & f_{21} & f_{22} \end{pmatrix} \in M_{3,3}(\mathbb{K}), \quad f_{ij} = \frac{\partial^2 f}{\partial x_i \partial x_j}.$$

Il rango di una conica non dipende dalla scelta del sistema di coordinate omogenee.

TEOREMA 8.6.1. *Due coniche sono proiettivamente equivalenti se e solo se hanno lo stesso rango. In particolare ogni conica è proiettivamente equivalente ad una delle seguenti:*

- (1)  $x_0^2 = 0$ , retta doppia.
- (2)  $x_0 x_1 = 0$ , rette incidenti.
- (3)  $x_0 x_2 = x_1^2$ , conica liscia.

DIMOSTRAZIONE. Sia  $C$  una conica di equazione  $f(x_0, x_1, x_2)$  e matrice Hessiana  $H$ . Dato un punto  $p = [v_0, v_1, v_2] = [v] \in \mathbb{P}^2$  per la formula di Eulero vale

$$v^T H = (f_0(v), f_1(v), f_2(v)), \quad 2f(v) = v^T H v,$$

e quindi  $p$  è un punto singolare di  $C$  se e solo se  $v^T H = (Hv)^T = 0$ .

Se il rango di  $H$  è 1, allora esiste una retta  $L$  composta di punti singolari di  $C$  e quindi deve necessariamente essere  $C = 2L$ . Se il rango è 2, allora esiste un unico punto singolare  $p = [v]$ : proviamo che  $C$  è unione di rette passanti per  $p$ , per ragioni di grado tali rette dovranno essere esattamente due. Se  $q = [y] \in C$ , allora per ogni  $a, b \in \mathbb{K}$  vale

$$2f(av + by) = (av + by)^T H (av + by) = b^2 y^T H y = 0.$$

Infine se il rango è 3 la conica è liscia; siano  $p, q$  e  $r$  tre punti distinti di  $C$  e denotiamo con  $o = \mathbb{T}_p C \cap \mathbb{T}_q C$  il punto di intersezione delle rette tangenti a  $C$  nei punti  $p$  e  $q$  rispettivamente. La quaterna  $p, q, r, o$  è un sistema di riferimento di  $\mathbb{P}^2$ , possiamo quindi supporre a meno di proiettività che

$$p = [1, 0, 0], \quad q = [0, 0, 1], \quad r = [1, 1, 1], \quad o = [0, 1, 0].$$

Dalla condizione  $p, q \in C$  si deduce che  $f_{00} = f_{22} = 0$ . Le equazioni di  $\mathbb{T}_p C = \overline{op}$  e  $\mathbb{T}_q C = \overline{oq}$  sono rispettivamente  $x_2 = 0$  e  $x_0 = 0$ ; si deduce quindi che  $f_{01} = f_{12} = 0$  e si ha  $f = ax_0 x_2 - bx_1^2$ . La condizione  $r \in C$  impone infine che  $a = b$ .  $\square$

La dimostrazione appena terminata è costruttiva e fornisce un metodo effettivo per il calcolo della proiettività che trasforma una conica nella sua forma canonica. Tale calcolo richiede la soluzione di una equazione di secondo grado ed alcuni sistemi di equazioni lineari.

COROLLARIO 8.6.2. *Siano  $p, q, r$  tre punti distinti di una conica irriducibile  $C$ . Allora esiste un sistema di coordinate omogenee  $x_0, x_1, x_2$  tale che  $p = [1, 0, 0]$ ,  $q = [0, 0, 1]$ ,  $r = [1, 1, 1]$  e l'equazione di  $C$  è  $x_0 x_2 = x_1^2$ .*

DIMOSTRAZIONE. Basta osservare che, nella dimostrazione del Teorema 8.6.1, la scelta dei punti  $p, q$  e  $r$  è arbitraria.  $\square$

**TEOREMA 8.6.3 (Steiner, 1832).** *Siano  $p$  e  $q$  due punti di una conica liscia  $C$  e denotiamo con  $F_p$  e  $F_q$  i fasci di rette passanti per  $p$  e  $q$  rispettivamente. Allora l'applicazione  $F_p \rightarrow F_q$  definita da  $F_p \ni L \mapsto \overline{qs}$ , dove  $s$  è il punto di intersezione di  $L$  con  $C$  diverso da  $p$ , è una proiettività.*

**DIMOSTRAZIONE.** Per il Corollario 8.6.2 possiamo supporre che  $C$  sia la conica di equazione  $x_0x_2 = x_1^2$  e che  $p = [1, 0, 0]$ ,  $q = [0, 0, 1]$ .

Si consideri adesso l'applicazione  $v: \mathbb{P}^1 \rightarrow C$  descritta in coordinate omogenee da  $v([t_0, t_1]) = [t_0^2, t_0t_1, t_1^2]$ ; si vede facilmente che  $v$  è biiettiva.

Dato un punto  $[a, b] \in \mathbb{P}^1$ , la retta di  $\mathbb{P}^2$  di equazione  $bx_1 - ax_2$  interseca  $C$  nei punti  $p = [1, 0, 0]$  e  $v([a, b]) = [a^2, ab, b^2]$ , mentre la retta di equazione  $ax_1 - bx_0$  interseca  $C$  nei punti  $q = [0, 0, 1]$  e  $v([a, b]) = [a^2, ab, b^2]$ .

L'applicazione  $[a, b] \mapsto ax_1 - bx_2$  è una proiettività tra  $\mathbb{P}^1$  ed il fascio di rette passanti per  $p$ ; similmente l'applicazione  $[a, b] \mapsto ax_1 - bx_0$  è una proiettività tra  $\mathbb{P}^1$  ed il fascio di rette passanti per il punto  $q = [0, 0, 1]$ . L'applicazione descritta nel teorema è la composizione della seconda proiettività con l'inversa della prima.  $\square$

Il Teorema di Steiner 8.6.3 permette di definire sulla conica liscia  $C$  una struttura di retta proiettiva mediante l'applicazione  $v$  introdotta nella dimostrazione. In particolare è ben definito il birapporto di una quaterna ordinata di punti su  $C$ : basta fissare un punto  $p \in C$  e considerare il birapporto delle 4 rette passanti per  $p$  ed i punti della quaterna.

### Esercizi.

**ESERCIZIO 21.** Provare che il Corollario 8.6.2 è vero anche in caratteristica 2.

**ESERCIZIO 22.** Trovare le componenti irriducibili della conica di equazione

$$3x_0^2 + 5x_0x_1 + 2x_0x_2 + 2x_1^2 + x_1x_2 - x_2^2 = 0.$$

## 8.7. Sistemi lineari

Abbiamo già osservato che le curve piane di grado  $n$  sono in corrispondenza biunivoca con il proiettivizzato  $\mathbb{P}(S_n)$  dello spazio vettoriale  $S_n \subset \mathbb{K}[x_0, x_1, x_2]$  dei polinomi omogenei di grado  $n$ . Abbiamo già visto che  $S_n$  ha dimensione  $\binom{n+2}{2}$  e quindi, prendendo i monomi come base canonica di  $S_n$  si ottiene un isomorfismo di spazi proiettivi

$$\mathbb{P}(S_n) \simeq \mathbb{P}^N, \quad N = \binom{n+2}{2} - 1 = \frac{n(n+3)}{2}.$$

Alla curva di equazione  $\sum_{ijk} a_{ijk} x_0^i x_1^j x_2^k = 0$  corrisponde il punto di  $\mathbb{P}^N$  di coordinate omogenee  $[a_{ijk}]$ .

**DEFINIZIONE 8.7.1.** Un sottospazio proiettivo di  $\mathbb{P}(S_n)$  si dice un **sistema lineare** di curve di grado  $n$ . Lo stesso spazio  $\mathbb{P}(S_n)$  è un sistema lineare che viene detto **completo**.

Se  $D_0, \dots, D_r$  sono curve di grado  $n$  denotiamo con  $\langle D_0, \dots, D_r \rangle \subset \mathbb{P}(S_n)$  il sistema lineare da esse generato: se  $f_i \in S_n$  è l'equazione di  $D_i$ , allora le curve del sistema lineare  $\langle D_0, \dots, D_r \rangle$  sono esattamente quelle di equazione

$$a_0 f_0(x) + \dots + a_r f_r(x) = 0$$

dove  $a_0, \dots, a_r \in \mathbb{K}$  sono coefficienti tali che il polinomio  $a_0 f_0 + \dots + a_r f_r$  sia non nullo.

Se  $V$  è un sistema lineare, indicheremo con  $\dim V$  la sua dimensione. Ad esempio se  $D_0, D_1$  sono curve distinte, allora  $\dim \langle D_0 \rangle = \dim \langle D_1 \rangle = 0$ ,  $\dim \langle D_0, D_1 \rangle = 1$ : un sistema lineare di dimensione 1 si dice un **fascio** od anche **pennello**<sup>2</sup> o **schiera**.

<sup>2</sup>In inglese **pencil**, in francese **pinceau**.

ESEMPIO 8.7.2. Se  $V \subset \mathbb{P}(S_n)$  è un sistema lineare di curve di grado  $n$  e  $C$  è una curva di grado  $m$ , allora l'insieme

$$W = \{C + D \mid D \in V\} \subset \mathbb{P}(S_{n+m})$$

è un sistema lineare della stessa dimensione di  $V$ . Infatti se  $V = \mathbb{P}(H)$  con  $H \subset S_n$  e  $F \in S_m$  è una equazione di  $C$ , allora  $W = \mathbb{P}(K)$ , dove  $K$  è l'immagine dell'applicazione lineare iniettiva

$$S_n \rightarrow S_{n+m}, \quad G \mapsto FG.$$

Sia  $V$  un sistema lineare di curve, un punto  $p \in \mathbb{P}^2$  si dice un **punto base** di  $V$  se per ogni curva  $D \in V$  vale  $p \in D$ . Se  $V$  è un sistema lineare di dimensione  $r$  e  $f_0, \dots, f_r$  sono equazioni di un insieme di curve indipendenti di  $V$ , allora le curve di  $V$  sono tutte e sole quelle di equazione  $\sum \lambda_i f_i$  e quindi i punti base di  $V$  sono quelli determinati dal sistema di equazioni

$$f_0(x) = \dots = f_r(x) = 0.$$

L'equazione di un iperpiano in  $\mathbb{P}(S_n)$  si dice una **condizione lineare** sulle curve di grado  $n$ .

ESEMPIO 8.7.3. Sia  $p \in \mathbb{P}^2$  un punto fissato. La relazione  $p \in D$ , con  $D$  curva di grado  $n$ , viene detta **condizione di passaggio per  $p$  su  $\mathbb{P}(S_n)$** . Essa impone una condizione lineare sul sistema lineare completo: infatti se  $p = [v_0, v_1, v_2]$ , allora una curva di equazione  $\sum a_{ijk} x_0^i x_1^j x_2^k$  contiene  $p$  se e solo se vale  $\sum a_{ijk} v_0^i v_1^j v_2^k = 0$  e quest'ultima condizione è esattamente l'equazione, nelle coordinate omogenee  $\{a_{ijk}\}$ , di un iperpiano in  $\mathbb{P}(S_n)$ .

Più in generale, sia  $\mathcal{P}$  una proprietà definita sulle curve di grado  $n$  e  $V \subset \mathbb{P}(S_n)$  un sistema lineare; diremo che  $\mathcal{P}$  impone  $r$  condizioni lineari su  $V$  se l'insieme delle  $D \in V$  che soddisfano  $\mathcal{P}$  è un sottospazio proiettivo di  $V$  di codimensione  $r$ . Ad esempio la condizione di passaggio per un punto  $p$  (il termine passaggio nasce dal fatto di pensare intuitivamente un sistema lineare come una curva che si muove in  $\mathbb{P}^2$ ) induce una condizione lineare su un sistema  $V$  se e solo se  $p$  non è un punto base di  $V$ .

LEMMA 8.7.4. *Sia  $V$  un sistema lineare di curve e siano  $p_1, \dots, p_s$  punti di  $\mathbb{P}^2$ . Allora il passaggio per  $p_1, \dots, p_s$  induce  $r$  condizioni lineari su  $V$ , con  $0 \leq r \leq s$ .*

*In altri termini, l'insieme  $W$  delle curve  $D \in V$  tali che  $p_1, \dots, p_s \in D$  è un sistema lineare di dimensione  $\dim W \geq \dim V - s$ .*

DIMOSTRAZIONE. Sia  $n$  il grado delle curve del sistema lineare  $V$ . Abbiamo visto che per ogni  $i = 1, \dots, s$  l'insieme  $W_i = \{D \in \mathbb{P}(S_n) \mid p_i \in D\}$  è un iperpiano e quindi

$$W = V \cap W_1 \cap \dots \cap W_s$$

è un sottospazio proiettivo. La formula  $\dim W \geq \dim V - s$  segue immediatamente dalla formula di Grassmann.  $\square$

DEFINIZIONE 8.7.5. Diremo che un insieme di punti  $p_1, \dots, p_s$  induce **condizioni di passaggio indipendenti** su un sistema lineare  $V$  di curve se il passaggio per  $p_1, \dots, p_s$  induce  $s$  condizioni lineari su  $V$ .

Ricordiamo che l'insieme vuoto, quando considerato come spazio proiettivo, ossia  $\emptyset = \mathbb{P}(0)$  ha dimensione  $-1$ . Per il Lemma 8.7.4, affinché  $s$  punti inducano condizioni di passaggio indipendenti su un sistema lineare  $V$  è necessario che  $s \leq \dim V + 1$ .

LEMMA 8.7.6. *Sia  $V$  un sistema lineare di curve e siano  $p_1, \dots, p_s$  punti di  $\mathbb{P}^2$ . Allora  $p_1, \dots, p_s$  inducono condizioni di passaggio indipendenti su  $V$  se e solo se per ogni  $i = 1, \dots, s$  esiste una curva  $D_i \in V$  tale che*

$$p_i \notin D_i, \quad p_j \in D_i \quad \text{per ogni } j < i.$$

DIMOSTRAZIONE. Sia  $n$  il grado delle curve del sistema lineare  $V$  e per ogni  $i = 1, \dots, s$  consideriamo l'iperpiano  $W_i = \{D \in \mathbb{P}(S_n) \mid p_i \in D\}$ . Per la formula di Grassmann si ha che  $\dim(V \cap W_1 \cap \dots \cap W_s) = \dim V - s$  se e solo se per ogni indice  $i = 1, \dots, s$  vale

$$V \cap W_1 \cap \dots \cap W_i \neq V \cap W_1 \cap \dots \cap W_{i-1}$$

Gli elementi di  $V \cap W_1 \cap \dots \cap W_{i-1} - V \cap W_1 \cap \dots \cap W_i$  sono esattamente le curve  $D$  del sistema lineare tali che  $p_i \notin D_i$  e  $p_j \in D_i$  per ogni  $j < i$ .  $\square$

È utile osservare che se  $p_1, \dots, p_s$  inducono condizioni di passaggio indipendenti su  $V$  lo stesso vale per ogni sottoinsieme di  $p_1, \dots, p_s$ .

Una conseguenza immediata del Lemma 8.7.6 è il seguente corollario, che sebbene più debole ha il vantaggio di essere invariante per permutazione dei punti.

**COROLLARIO 8.7.7.** *Sia  $V$  un sistema lineare di curve e siano  $p_1, \dots, p_s$  punti di  $\mathbb{P}^2$ . Allora  $p_1, \dots, p_s$  inducono condizioni di passaggio indipendenti su  $V$  se e solo se per ogni  $i = 1, \dots, s$  esiste una curva  $D_i \in V$  tale che*

$$p_i \notin D_i, \quad p_j \in D_i \quad \text{per ogni } j \neq i.$$

**ESEMPIO 8.7.8.** Un punto  $p$  induce una condizione di passaggio indipendente, ossia non nulla, su un sistema lineare se e solo se  $p$  non è un punto base del sistema lineare. In particolare se  $V$  è un fascio di curve e  $p$  non è un punto base, allora esiste ed è unica una curva  $C \in V$  tale che  $p \in C$ .

**ESEMPIO 8.7.9.** Tre punti inducono condizioni indipendenti sulle rette, ossia sul sistema lineare completo delle curve di grado 1, se e solo se non sono allineati.

**ESEMPIO 8.7.10.** Se  $k \leq n + 1$  allora  $k$  punti distinti inducono condizioni di passaggio indipendenti sul sistema lineare completo delle curve di grado  $n$ . Per dimostrare questo fatto non è restrittivo supporre  $k = n + 1$ ; siano  $p_0, \dots, p_n \in \mathbb{P}^2$  punti distinti e scegliamo un punto  $q$  non appartenente all'unione delle rette  $\overline{p_i p_j}$ . Allora le curve  $D_i = \sum_{j \neq i} \overline{q p_j}$  soddisfano le condizioni del Lemma 8.7.6.

**ESEMPIO 8.7.11.** Quattro punti distinti inducono condizioni di passaggio indipendenti sulle coniche, ossia sul sistema lineare completo delle curve di grado 2, se e solo se non sono allineati.

Ricordiamo che il sistema lineare completo delle coniche ha dimensione 5. Se i quattro punti appartengono ad una retta  $L$ , le coniche del tipo  $L + M$ , con  $M$  retta, formano un sistema lineare di dimensione 2 che passa per i quattro punti, i quali pertanto non inducono condizioni di passaggio indipendenti.

Viceversa, dati 4 punti non allineati, per ciascuno di essi, chiamiamolo  $p$ , esiste una conica  $C$  che non contiene  $p$  e contiene gli altri tre, che chiameremo  $r, s, t$ . Infatti  $p$  può appartenere al massimo ad una delle tre rette  $\overline{rs}, \overline{st}, \overline{rt}$ . Se, per fissare le idee,  $p \notin \overline{rs} \cup \overline{st}$ , allora  $C = \overline{rs} + \overline{st}$  è la conica cercata.

**ESEMPIO 8.7.12.** Cinque punti distinti inducono condizioni di passaggio indipendenti sulle coniche se e solo se non ve ne sono quattro allineati.

Abbiamo già visto che 4 punti allineati inducono condizioni dipendenti sulle coniche; a maggior ragione 5 punti di cui 4 allineati inducono condizioni di passaggio dipendenti.

Viceversa se 5 punti inducono condizioni dipendenti, esistono almeno due coniche distinte  $C_1, C_2$  che li contengono. Per Bézout le due coniche devono avere una retta  $L$  in comune, ossia  $C_1 = L + M_1$  e  $C_2 = L + M_2$  con  $M_1, M_2$  rette distinte. Siccome  $M_1, M_2$  hanno un solo punto in comune, almeno 4 dei 5 punti devono appartenere alla retta  $L$ .

**ESEMPIO 8.7.13.** Siano dati 8 punti distinti  $p_1, \dots, p_8$  contenuti nell'unione di tre rette  $L_1, L_2, L_3$  e tali che ciascuna retta  $L_i$  contenga al più 3 punti  $p_j$ . Allora  $p_1, \dots, p_8$  inducono condizioni di passaggio indipendenti sulle cubiche.

Per simmetria basta dimostrare che esiste una cubica  $C$  che contiene  $p_2, \dots, p_8$  ma non contiene  $p_1$ . Osserviamo che  $p_1 \notin L_1 \cap L_2 \cap L_3$ , altrimenti ciascuna retta  $L_i$  potrebbe contenere al più due dei rimanenti punti  $p_2, \dots, p_8$  e quindi i punti sarebbero al massimo 7.

Dunque, a meno di permutazioni degli indici delle rette si ha uno dei seguenti due casi:

- (1)  $p_1 \in L_1 \cap L_2, p_1 \notin L_3$ ;
- (2)  $p_1 \in L_1, p_1 \notin L_2 \cup L_3$ .

Nel primo caso l'unione  $L_1 \cup L_2$  contiene esattamente 5 punti  $p_i$  e la retta  $L_3$  i rimanenti 3; nel secondo caso l'unione  $L_2 \cup L_3$  contiene almeno 5 punti  $p_i$  ed a meno di scambiare  $L_2$  con  $L_3$  si ha che  $L_3$  contiene 3 punti  $p_i$ .

A meno di permutazioni degli indici possiamo quindi supporre che  $p_1 \notin L_3$  e  $p_6, p_7, p_8 \in L_3$ .

Ma adesso tra i 5 punti  $p_1, \dots, p_5$  non ve ne sono 4 allineati e per l'esempio precedente esiste una conica  $Q$  tale che  $p_1 \notin Q$  e  $p_2, \dots, p_4 \in Q$ . Basta allora considerare la cubica  $C = L_3 + Q$ .

Prima di proseguire con lo studio dell'indipendenza delle condizioni di passaggio vediamo alcune interessanti applicazioni dei sistemi lineari.

**TEOREMA 8.7.14** (Gergonne, 1827). *Siano  $C$  e  $D$  due curve piane di grado  $n$  che si intersecano in esattamente  $n^2$  punti distinti. Se  $nm$  di questi punti appartengono ad una curva  $E$  di grado  $m \leq n$ , allora i restanti  $n(n - m)$  punti appartengono ad una curva  $H$  di grado  $n - m$ .*

**DIMOSTRAZIONE.** Siano  $p_1, \dots, p_{n^2}$  i punti di intersezione di  $C$  e  $D$ , dal teorema di Bézout segue che necessariamente  $C, D, E$  sono curve ridotte.

Infatti  $C$  e  $D$  non hanno componenti in comune e se  $C = \sum a_i C_i$  con le  $C_i$  irriducibili, allora  $C \cap D = \cup_i C_i \cap D$ ,

$$n^2 = n \left( \sum a_i \deg(C_i) \right) = |C \cap D| \leq \sum |C_i \cap D| \leq \sum n \deg(C_i)$$

e questo prova che  $a_i = 1$  per ogni  $i$ , ossia che  $C$  è ridotta. Per simmetria anche  $D$  è una curva ridotta.

Per mostrare che anche  $E$  è ridotta, scriviamo  $E = \sum a_i E_i$ ; allora con  $E_i$  irriducibile per ogni  $i$ . Siccome  $C, D$  non hanno componenti in comune si ha  $E_1 \not\subset C$  oppure  $E_1 \not\subset D$ ; supponiamo per fissare le idee che  $E_1 \not\subset C$ , allora

$$|E_1 \cap C \cap D| \leq |E_1 \cap C| \leq n \deg(E_1).$$

Similmente  $|E_i \cap C \cap D| \leq n \deg(E_i)$  per ogni  $i$  e quindi

$$nm = |E \cap C \cap D| \leq \sum_i |E_i \cap C \cap D| \leq \sum_i n \deg(E_i) \leq \sum_i n a_i \deg(E_i) = nm.$$

Dunque  $\sum_i n \deg(E_i) = \sum_i n a_i \deg(E_i)$  da cui segue  $a_i = 1$  per ogni  $i$ ; dalla condizione  $|E \cap C \cap D| = \sum_i |E_i \cap C \cap D|$  segue che  $|E_i \cap E_j \cap C \cap D| = \emptyset$  per ogni  $i \neq j$ . Infine, dalla condizione  $|E_i \cap C \cap D| \leq n \deg(E_i)$  segue che  $E_i \cap C \cap D$  contiene esattamente  $n \deg(E_i)$  punti.

Siano  $C_t$ , con  $t \in \mathbb{P}^1$ , le curve del fascio  $V$  generato da  $C$  e  $D$ ; notiamo che i punti base del fascio generato da  $C, D$  sono esattamente  $C \cap D$ . Sia  $E = E_1 + \dots + E_r$  la decomposizione in componenti irriducibili e denotiamo con  $m_i$  il grado di  $E_i$ . Siccome  $E_i \cap D \cap D \subset E_i \cap C_t$  per ogni  $t$ , dal teorema di Bezout segue che per ogni  $t \in \mathbb{P}^1$  vale una, ed una soltanto delle seguenti alternative:

- (1)  $E_i \cap C_t = E_i \cap C \cap D$ ;
- (2)  $E_i$  è una componente di  $C_t$ .

Per ogni  $i = 1, \dots, m$ , sia  $q_i \in E_i - (C \cap D)$  un punto fissato, allora esiste un unico  $t_i \in \mathbb{P}^1$  tale che  $q_i \in C_{t_i}$ ; quindi  $E_i$  è una componente di  $C_{t_i}$ . Osserviamo che se  $q = q_i = q_j \in E_i \cap E_j$ , con  $i \neq j$ , allora  $q$  non appartiene ai punti base di  $V$ , ragionando come sopra ne segue che  $t_i = t_j = t$  per ogni  $i, j$ . Dunque  $E$  è contenuta in una curva  $C_t$  del fascio, basta quindi prendere  $H = C_t - E$ .  $\square$

**COROLLARIO 8.7.15.** (Teorema di Pappo-Pascal, III sec d.C.-1640) *Le coppie di lati opposti di un esagono inscritto in una conica ridotta si intersecano in punti allineati.*

**DIMOSTRAZIONE.** (Plücker, 1828) Siano  $L_1, L_2, \dots, L_6$  i lati successivi di un esagono inscritto in una conica  $E$ . In virtù del teorema di Gergonne 8.7.14, basta osservare che le due cubiche  $C = L_1 + L_3 + L_5$  e  $D = L_2 + L_4 + L_6$  si intersecano in 9 punti e 6 di questi appartengono a  $E$ .  $\square$

È facile dimostrare che ogni fascio di coniche contiene almeno una conica riducibile. Infatti siano  $C_1, C_2$  coniche di equazioni  $f_1, f_2$  e matrici Hessiane  $H_1, H_2$  rispettivamente. Sappiamo che la conica di equazione  $af_0 + bf_1$  è riducibile se e solo se  $(a, b)$  è una radice

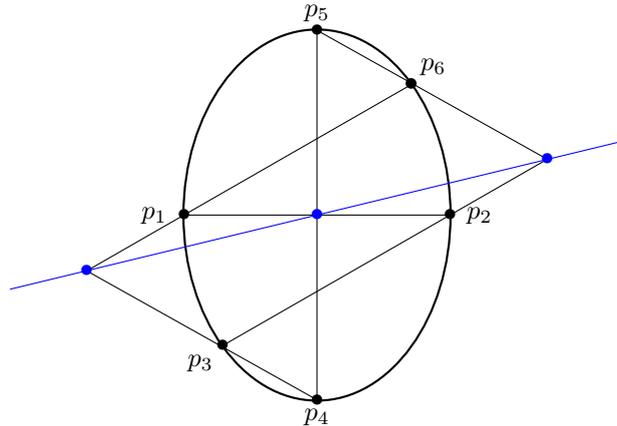


FIGURA 2. Il teorema di Pascal

del polinomio omogeneo  $p(t_1, t_2) = \det(t_1 H_1 + t_2 H_2)$ . Se vogliamo determinare i punti di intersezione di due coniche  $C_1, C_2$  si può procedere nel modo seguente.

Se  $C_2$  è riducibile, si determinano le sue componenti (sono due rette) e per ciascuna di esse si calcola l'intersezione con  $C_1$ : il procedimento richiede la soluzione di alcune equazioni di secondo grado. Se invece  $C_2$  è irriducibile si determina (risolvendo un'equazione di terzo grado) una conica riducibile  $C_0 \neq C_2$  appartenente al fascio generato da  $C_1$  e  $C_2$  e quindi ricondursi al caso precedente osservando che  $C_1 \cap C_2 = C_0 \cap C_2$ .

LEMMA 8.7.16. *Sia  $X$  un insieme finito con  $2d$  elementi e sia  $\sim$  una relazione di equivalenza su  $X$  tale che ciascuna classe di equivalenza contenga al più  $d$  elementi. Allora possiamo scrivere  $X = \{a_1, b_1, \dots, a_d, b_d\}$  con  $a_i \not\sim b_i$  per ogni  $i = 1, \dots, d$ .*

DIMOSTRAZIONE. Induzione su  $d$ , essendo il risultato evidente per  $d = 1$ . Sia dunque  $d > 1$  e scriviamo  $X$  come unione disgiunta delle sue classi di equivalenza, ordinate per cardinalità decrescente.

$$X = S_1 \cup S_2 \cup \dots, \quad d \geq |S_1| \geq |S_2| \geq \dots$$

Siccome  $S_1, S_2$  non sono vuote e  $d-1 \geq |S_3|$  possiamo scegliere  $a_1 \in S_1, b_1 \in S_2$  ed applicare l'ipotesi induttiva all'insieme  $Y = X - \{a_1, b_1\}$ .  $\square$

LEMMA 8.7.17. *Siano  $n > 0, V = \mathbb{P}(S_n)$  il sistema lineare completo delle curve di grado  $n$  e  $k \leq 2n + 1$  un intero. Allora  $k$  punti distinti di  $\mathbb{P}^2$  inducono condizioni di passaggio indipendenti su  $V$  se e solo se non ve ne sono  $n + 2$  allineati. In particolare,  $n + 2$  punti distinti inducono condizioni di passaggio indipendenti su  $V$  se e solo se non sono allineati.*

DIMOSTRAZIONE. Consideriamo  $k$  punti distinti  $p_1, \dots, p_k$  e supponiamo che ne esistano  $n + 2$  contenuti in una retta  $L$ : supponiamo per fissare le idee che  $p_1, \dots, p_{n+2} \in L$ , allora per Bezout ogni curva di grado  $n$  che contiene  $p_1, \dots, p_{n+1}$  contiene  $L$  e di conseguenza contiene anche  $p_{n+2}$ .

Supponiamo adesso che in un insieme  $S \subset \mathbb{P}^2$  di  $k$  punti non ne esistano  $n + 2$  allineati: vogliamo dimostrare che per ogni  $s \in S$  esiste una curva  $C$  di grado  $n$  che contiene  $S - \{s\}$  ma non contiene  $s$ . A meno di aggiungere ad  $S$  un numero opportuno di punti in posizione generica non è restrittivo supporre  $k = 2n + 1$ .

Considerando su  $S - \{s\}$  la relazione di equivalenza  $p \sim q$  se e solo se i punti  $s, p, q$  sono allineati, abbiamo una partizione in classi di equivalenza

$$S - \{s\} = S_1 \amalg S_2 \amalg \dots \amalg S_h.$$

Per ipotesi ciascuna classe di equivalenza contiene al massimo  $n$  punti, quindi  $h \geq 2$  e per il Lemma 8.7.16 possiamo ordinare i punti  $S - \{s\} = \{p_1, \dots, p_{2n}\}$  in modo tale che  $p_{2i}$  non sia equivalente a  $p_{2i-1}$  per ogni  $i = 1, \dots, n$ . (vedi Esercizio).

Ma allora l'unione delle  $n$  rette  $C = \overline{p_1 p_2} + \cdots + \overline{p_{2n-1} p_{2n}}$  è una curva di grado  $n$  con le proprietà richieste.  $\square$

Il passo successivo al Lemma 8.7.17, ossia determinare sotto quali condizioni  $2n + 2$  punti distinti inducono condizioni indipendenti sulle curve di grado  $n$ , inizia ad essere geometricamente non banale e precursore di importanti teoremi.

Senza entrare in dettaglio, se studiamo le condizioni di passaggio delle coniche per 6 punti distinti, osserviamo che il teorema di Steiner 8.6.3 può essere interpretato come una condizione necessaria e sufficiente sulle sestuple di punti distinti affinché siano contenute in una conica.

Anche il caso delle condizioni imposte da 8 punti sulle cubiche rimane tutto sommato abbordabile.

LEMMA 8.7.18. *Otto punti distinti  $p_1, \dots, p_8$  inducono condizioni indipendenti sulle cubiche piane se e solo se non sono contenuti in una conica e non ve ne sono 5 allineati.*

DIMOSTRAZIONE. Dire che  $p_1, \dots, p_8$  inducono condizioni indipendenti vuol dire che le cubiche passanti per tali punti sono un sistema lineare di dimensione 1. Questo esclude immediatamente che gli 8 punti possano appartenere ad una conica  $Q$ , altrimenti tutte le cubiche del tipo  $Q + L$ , con  $L$  retta, passano per  $p_1, \dots, p_8$  e formano un sistema lineare di dimensione 2. Che non vi possano essere 5 punti allineati è stato dimostrato nel Lemma 8.7.17.

Viceversa, supponiamo gli  $p_1, \dots, p_8$  non contenuti in una conica e che non ve ne sono 5 allineati: bisogna dimostrare che esiste una cubica che contiene  $p_1, \dots, p_7$  ma non  $p_8$ .

Per ogni  $i = 1, \dots, 7$  indichiamo con  $l_i$  il numero dei punti  $p_1, \dots, p_7$  che appartengono alla retta  $\overline{p_i p_8}$ . Per ipotesi ciascun  $l_i$  è minore od uguale a 3 e quindi l'insieme delle rette  $\overline{p_i p_8}$ ,  $i = 1, \dots, 7$  contiene almeno tre elementi. A meno di di permutazioni sull'insieme  $p_1, \dots, p_7$  possiamo supporre che  $\overline{p_1 p_8}$ ,  $\overline{p_2 p_8}$  e  $\overline{p_3 p_8}$  sia una terna di rette distinte che massimizza la somma  $l_1 + l_2 + l_3$ . In particolare:

- (1) le rette  $\overline{p_1 p_2}$ ,  $\overline{p_1 p_3}$  e  $\overline{p_2 p_3}$  non contengono  $p_8$ ;
- (2) per ogni  $i = 4, \dots, 7$  se  $p_i$  non appartiene a  $\overline{p_1 p_8} \cup \overline{p_2 p_8} \cup \overline{p_3 p_8}$ , allora la retta  $\overline{p_i p_8}$  non contiene alcun punto del tipo  $p_j$  con  $j \neq i, 8$ .

Se i punti  $p_4, p_5, p_6, p_7$  appartengono ad una retta  $L$ , la cubica  $L + \overline{p_1 p_2} + \overline{p_1 p_3}$  contiene  $p_1, \dots, p_7$  ma non  $p_8$ .

Se  $p_4, p_5, p_6, p_7$  non sono allineati, per ogni  $i = 1, 2, 3$  sia  $Q_i$  una conica passante per i cinque punti  $p_i, p_4, p_5, p_6, p_7$  e mostriamo che l'ipotesi  $p_8 \in Q_1 \cap Q_2 \cap Q_3$  conduce ad una contraddizione. Se  $Q_1 = Q_2 = Q_3$  allora gli 8 punti sarebbero contenuti in una conica; se invece i punti  $p_4, p_5, p_6, p_7, p_8$  sono contenuti in due coniche distinte allora 4 di essi sono contenuti in una retta  $M$ . Dato che i punti  $p_4, p_5, p_6, p_7$  non sono allineati la retta  $M$  contiene  $p_8$  e tre dei 4 punti  $p_4, p_5, p_6, p_7$ . Siccome abbiamo ordinato i punti in modo tale che la somma  $l_1 + l_2 + l_3$  sia massima deve necessariamente essere  $M = \overline{p_h p_8}$  per qualche  $h = 1, 2, 3$ , ma questo implicherebbe che in  $p_h, p_4, p_5, p_6, p_7, p_8$  vi sono 5 punti allineati.

Quindi  $p_8$  non appartiene ad almeno una delle tre coniche  $Q_1, Q_2, Q_3$ : se per fissare le idee  $p_8 \notin Q_1$ , allora la cubica  $Q_1 + \overline{p_2, p_3}$  contiene  $p_1, \dots, p_7$  ma non  $p_8$ .  $\square$

### Esercizi.

ESERCIZIO 23. Provare il risultato dell'Esempio 8.7.13 come conseguenza del Lemma 8.7.18.

ESERCIZIO 24. Sia dato un fascio di coniche generato da due rette doppie. Provare che ogni conica di tal fascio è singolare.

ESERCIZIO 25. Calcolare i punti di intersezione delle coniche di equazioni

$$x_0^2 + x_1^2 + x_2^2 = 0, \quad x_1^2 + x_2^2 - x_0 x_1 - x_0 x_2 = 0.$$

## 8.8. Curve ellittiche

Continuiamo con la convenzione che  $\mathbb{K}$  sia un campo algebricamente chiuso di caratteristica 0.

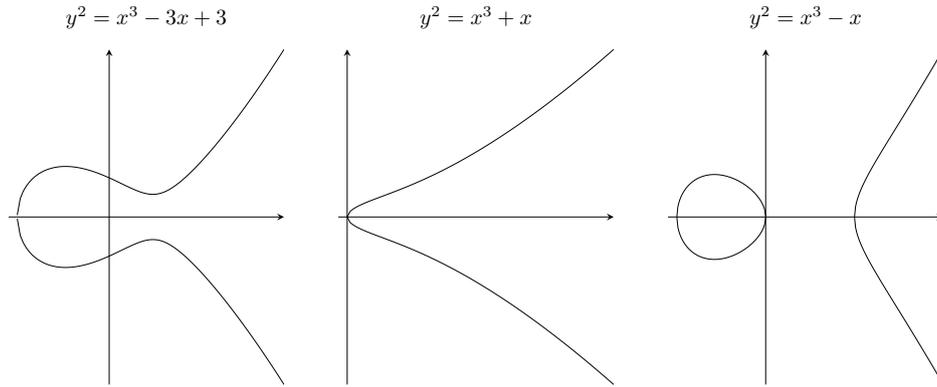


FIGURA 3. Tre esempi di cubiche lisce.

Le curve piane di grado 3 sono dette cubiche piane. Siccome  $3 = 2 + 1 = 1 + 2$  sono gli unici modi in cui possiamo scrivere 3 come somma di due interi positivi, una cubica è riducibile se e solo se contiene una retta. Ogni cubica riducibile è singolare mentre, a differenza di quanto accade per le coniche, esistono cubiche singolari irriducibili.

Abbiamo visto che ogni cubica liscia possiede punti di flesso: è possibile dimostrare che esistono esattamente 9 punti di flesso distinti, ma la dimostrazione di questo fatto va oltre gli obiettivi di questo capitolo.

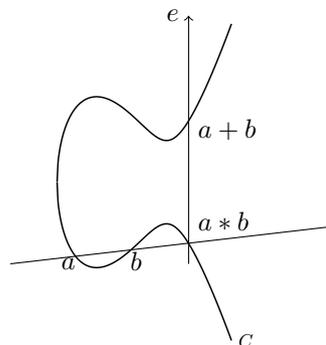
Se  $C$  è una cubica liscia ed  $e \in C$  è un suo punto di flesso, allora la retta tangente a  $C$  in  $e$  non interseca  $C$  al di fuori di  $e$ . Infatti tale retta interseca  $C$  in esattamente 3 punti contati con molteplicità  $e$ , per definizione di flesso, la molteplicità di intersezione nel punto  $e$  è almeno 3.

Chiameremo (provvisoriamente) **curva ellittica** una coppia  $(C, e)$  dove  $C$  è una cubica liscia ed  $e \in C$  è un punto di flesso. Data una curva ellittica  $(C, e)$  possiamo definire due operazioni

$$C \times C \xrightarrow{*} C, \quad C \times C \xrightarrow{+} C,$$

nel modo seguente:

- (1)  $a * b =$  terzo punto di intersezione, oltre  $a$  e  $b$ , della retta  $\overline{ab}$  con la cubica  $C$ , con la convenzione che se  $a = b$  per retta  $\overline{ab}$  si intende la tangente a  $C$  nel punto  $a = b$ .
- (2)  $a + b = (a * b) * e$ .



$$C : x_0x_2^2 = x_1^3 - 4x_0^2x_1 + 5x_0^3$$

$$e = [0, 0, 1]$$

È chiaro dalla definizione che  $a * b = b * a$ ,  $a + b = b + a$  e  $a * (a * b) = b$  per ogni coppia  $a, b \in C$ , e poichè  $e$  è un flesso si ha  $e * e = e$ . Inoltre per ogni punto  $a \in C$  vale

$$a + e = e * (e * a) = a, \quad a + (a * e) = e * (a * (a * e)) = e * e = e.$$

**TEOREMA 8.8.1.** *Sia  $(C, e)$  una curva ellittica. Allora l'operazione binaria  $+$  induce su  $C$  una struttura di gruppo abeliano su  $C$  con elemento neutro  $e$  ed inverso  $-a = a * e$ .*

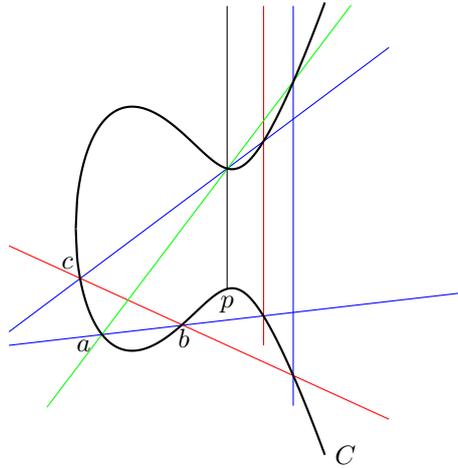


FIGURA 4. Legge associativa sulla cubica  $C$ , e cioè  $p = (a+b)+c = a+(b+c)$ . Nelle notazioni della dimostrazione le tre rette blu sono la cubica  $B$ , le due rette rosse sono la conica  $Q$  e la retta  $L$  è disegnata in verde. L'elemento neutro è il punto all'infinito corrispondente alla direzione verticale.

DIMOSTRAZIONE. Tra i vari assiomi di gruppo rimane solo da verificare la proprietà associativa della somma  $a + (b + c) = (a + b) + c$ . La dimostrazione completa di questo fatto richiede strumenti non ancora sviluppati. Tuttavia, possiamo utilizzare il teorema di Gergonne per dare una dimostrazione per triple  $a, b, c$  in posizione generica e più precisamente sotto l'ipotesi aggiuntiva che i  $9 = 3 \times 3$  punti della tabella

$$(8.8) \quad \begin{array}{ccc} a & b + c & (a + b) * c \\ b & b * c & c \\ a * b & e & a + b \end{array}$$

siano tutti distinti (Figura 4).

Dalla definizione delle operazioni  $*$  e  $+$  segue che ciascuna colonna della Tabella (8.8) è formata da tre punti allineati e quindi i nove punti coincidono con l'intersezione di  $C$  con una cubica  $B$  unione di tre rette. Similmente la seconda e terza riga della tabella sono formate da terne allineate di punti; in particolare i 6 punti delle ultime due righe coincidono con l'intersezione di  $C$  con una conica  $Q$  unione di due rette.

Per il teorema di Gergonne 8.7.14 i tre punti della prima riga appartengono ad una retta  $L$ , ossia i tre punti  $a, b + c$  e  $(a + b) * c$  sono allineati, e questo è possibile se e solo se  $(a + b) * c = a * (b + c)$ . Quindi

$$(a + b) + c = e * ((a + b) * c) = e * (a * (b + c)) = a + (b + c).$$

□

Osserviamo che un punto  $a$  in una curva ellittica  $(C, e)$  è un punto di flesso se e solo se  $a * a = a$ , o equivalentemente se e solo se  $3a = a + a + a = e$ . L'equivalenza tra flessi e punti  $a$  tali che  $a * a = a$  segue immediatamente dalle definizioni. Se  $a * a = a$ , allora

$$2a = a + a = e * (a * a) = e * a, \quad 3a = a + 2a = e * (a * (e * a)) = e * e = e.$$

Viceversa, se  $3a = e$  allora  $e * (a * a) = 2a = -a = e * a$  e quindi  $a = a * a$ .

Analogamente si osserva che tre punti  $a, b, c \in C$  sono allineati se e solo se  $a + b + c = e$ : la condizione  $a + b + c = e$  è equivalente a dire che  $e * (a * b) = a + b = -c = e * c$  che a sua volta equivale a dire che  $a * b = c$ .

COROLLARIO 8.8.2. *Dati due punti di flesso distinti  $a, b \in C$ , il terzo punto  $c$  di intersezione di  $C$  con la retta  $\overline{ab}$  è ancora un flesso.*

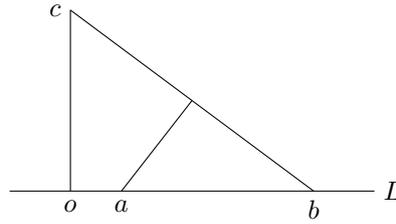


FIGURA 5. La distanza tra il punto  $a$  e la retta  $\overline{bc}$  è strettamente minore della distanza del punto  $c$  dalla retta  $L$ .

DIMOSTRAZIONE. Fissiamo un flesso  $e \in C$  (non necessariamente uguale ad  $a$  o  $b$ ), abbiamo visto che rispetto alla struttura di gruppo sulla curva ellittica  $(C, e)$  si ha  $a+b+c = e$ , ossia  $c = -a - b$ . Allora  $3c = -3a - 3b = -e - e = e$  e quindi anche  $c$  è un flesso.  $\square$

ESEMPIO 8.8.3. Sia  $\xi \in \mathbb{K} = \mathbb{C}$  una radice cubica primitiva di 1, ossia una radice del polinomio  $\xi^2 + \xi + 1$ . Allora i flessi della cubica di Fermat  $x_0^3 + x_1^3 + x_2^3$  sono le intersezioni con la Hessiana  $6^3 x_0 x_1 x_2 = 0$  e sono rappresentati nella tabella

$$\begin{array}{ccc} [0, -1, 1] & [0, 1, \xi] & [0, -1, \xi^2] \\ [-1, 0, 1] & [-1, 0, \xi^2] & [-1, 0, \xi] \\ [-1, 1, 0] & [-1, \xi, 0] & [-1, \xi^2, 0] \end{array} .$$

Senza usare il precedente corollario si verifica direttamente e facilmente che dati due punti della tabella ne esiste un terzo allineato.

Nel precedente esempio i flessi a coordinate reali sono esattamente i tre della prima colonna. Più in generale ogni cubica liscia complessa può avere al massimo tre flessi reali, come segue immediatamente dal Corollario 8.8.2 e dal seguente classico risultato di geometria proiettiva reale.

TEOREMA 8.8.4. *Sia  $S \subset \mathbb{P}_{\mathbb{R}}^n$  un insieme finito di punti che soddisfa la seguente proprietà:*

- *per ogni coppia di punti distinti  $p, q \in S$  esiste un punto  $r \in S$ , diverso da  $p, q$  e appartenente alla retta  $\overline{pq}$ . Equivalentemente, se ogni retta di  $\mathbb{P}_{\mathbb{R}}^n$  interseca  $S$  in un sottoinsieme di cardinalità diversa da 2.*

*Allora i punti di  $S$  sono tutti allineati.*

DIMOSTRAZIONE. Supponiamo per assurdo che esistano tre punti  $p, q, r \in S$  non allineati e sia  $H \subset \mathbb{P}_{\mathbb{R}}^n$  il piano che li contiene. A meno di sostituire  $\mathbb{P}_{\mathbb{R}}^n$  con  $H$  e  $S$  con  $S \cap H$  non è restrittivo supporre  $n = 2$ . Infine, prendendo come retta all'infinito una qualsiasi retta che non interseca  $S$  possiamo ridurci al caso in cui  $S \subset \mathbb{R}^2$  è un sottoinsieme finito che soddisfa la proprietà (P). Abbiamo supposto per assurdo che l'insieme  $T$  formato dalle terne ordinate  $(p, q, r) \in S^3$  di punti non allineati sia non vuoto. Scegliamo un elemento  $(u, v, c) \in T$  tale che la distanza di  $c$  dalla retta  $L = \overline{uv}$  sia la minore possibile. Detta  $M$  la retta perpendicolare ad  $L$  passante per  $c$ , la distanza di  $c$  da  $L$  è uguale alla distanza di  $c$  dal punto  $o$  di intersezione di  $L$  con  $M$ . Il punto  $o$  divide la retta  $L$  in due semirette, ed  $L$  contiene almeno tre punti di  $S$ . Possiamo quindi trovare  $a \neq b \in S \cap L$  tali che  $a$  è contenuto nel segmento di estremi  $o, b$ . Ma allora la distanza di  $a$  dalla retta  $\overline{cb}$  è strettamente minore della distanza tra  $o$  e  $c$  (Figura 5), in contraddizione con le ipotesi.  $\square$

## I teoremi della base e degli zeri di Hilbert

Con il termine anello intenderemo sempre un anello commutativo con unità  $e$ , salvo avviso contrario, ogni omomorfismo di anelli  $f: A \rightarrow B$  è unitario, cioè soddisfa la condizione  $f(1) = 1$ . Assumeremo che il lettore abbia familiarità con le nozioni di ideale, di dominio di integrità, di campo e di caratteristica di un campo.

### 9.1. Operazioni sugli ideali

Dato un anello  $A$  ed un suo sottoinsieme  $E$ , denotiamo con  $(E) \subset A$  l'ideale generato da  $E$ , ossia il più piccolo ideale di  $A$  contenente  $E$ . Si dimostra facilmente che ogni elemento di  $(E)$  si può scrivere come una combinazione lineare finita di elementi di  $E$  a coefficienti in  $A$ :

$$(E) = \left\{ \sum_{\text{finita}} a_i e_i \mid a_i \in A, e_i \in E \right\}.$$

Si noti che  $(E) = E$  se e solo se  $E$  è un ideale. Diremo che un insieme  $E$  è un **insieme di generatori** dell'ideale  $I \subset A$  se  $I = (E)$ ; un ideale si dice **finitamente generato** se ammette un insieme finito di generatori; si dice **principale** se è generato da un solo elemento.

**ESEMPIO 9.1.1.** Siano  $A$  un anello e  $a \in A$ . Allora  $(a) = A$  se e solo se  $a$  è un elemento **invertibile**, ossia se e solo se esiste  $b \in A$  tale che  $ab = 1$ . Infatti se l'ideale principale  $(a) = \{ax \mid x \in A\}$  è uguale ad  $A$ , in particolare  $1 \in (a)$  e quindi esiste  $b$  tale che  $ab = 1$ . Viceversa, se  $ab = 1$  per qualche  $b$  allora per ogni  $x \in A$  vale  $x = (ab)x = a(bx) \in (a)$  da cui segue  $(a) = A$ .

Più generalmente, per un ideale  $I \subset A$  vale  $I = A$  se e solo se  $I$  contiene un elemento invertibile: se  $I = A$  allora  $1 \in I$  e viceversa, se  $a \in I$  ed  $a$  è invertibile, allora  $A = (a) \subset I \subset A$  da cui segue  $I = A$ .

Intersezione di ideali è sempre un ideale mentre in generale l'unione di ideali non è un ideale. Se  $I, J \subset A$  sono ideali, denotiamo con  $I + J = (I \cup J)$  l'ideale generato da  $I$  e  $J$ : equivalentemente

$$I + J = \{x + y \mid x \in I, y \in J\}$$

così che, ad esempio,  $I + (x) = \{a + bx \mid a \in I, b \in A\}$ . Più in generale se  $I_\alpha$  è una famiglia arbitraria di ideali di  $A$  denotiamo con  $\sum_\alpha I_\alpha$  l'ideale generato da  $\cup_\alpha I_\alpha$ .

Un ideale  $\mathfrak{p}$  di un anello  $A$  si dice **primo** se  $\mathfrak{p} \neq A$  e se  $ab \in \mathfrak{p}$  implica che  $a \in \mathfrak{p}$  oppure  $b \in \mathfrak{p}$ . Dato un ideale  $I \subset A$  si definisce il **radicale** di  $I$  come

$$\sqrt{I} = \{a \in A \mid a^n \in I \text{ per } n \gg 0\}.$$

Il radicale di un ideale è ancora un ideale: infatti se  $a, b \in \sqrt{I}$  e  $n, m$  sono due interi positivi tali che  $a^n, b^m \in I$  si ha  $(-a)^n = \pm a^n \in I$ ,

$$\begin{aligned} (a + b)^{n+m} &= \sum_{i=0}^{n+m} \binom{n+m}{i} a^i b^{n+m-i} \\ &= b^m \sum_{i=0}^n \binom{n+m}{i} a^i b^{n-i} + a^n \sum_{i=n+1}^{n+m} \binom{n+m}{i} a^{i-n} b^{n+m-i} \in I, \end{aligned}$$

mentre per ogni  $c \in A$  vale  $(ac)^n = a^n c^n \in I$ . Si noti che per ogni ideale  $I$  vale  $I \subset \sqrt{I}$  e  $\sqrt{\sqrt{I}} = \sqrt{I}$ : infatti se  $a \in \sqrt{\sqrt{I}}$ , per definizione esistono due interi positivi  $n, m$  tali che  $a^n \in \sqrt{I}$ ,  $(a^n)^m \in I$  e quindi  $a^{nm} \in I$ .

Un **ideale radicale** è un ideale  $I$  tale che  $I = \sqrt{I}$ . Non tutti gli ideali sono radicali, ad esempio l'ideale  $(4) \subset \mathbb{Z}$  non è radicale in quanto  $\sqrt{(4)} = (2)$ .

Ogni ideale primo è radicale. Infatti se  $\mathfrak{p} \subset A$  è primo e  $a \in \sqrt{\mathfrak{p}}$ , allora  $a^n \in \mathfrak{p}$  per qualche  $n > 0$  e scrivendo  $a^n = a \cdot a^{n-1}$  si ha  $a \in \mathfrak{p}$  oppure  $a^{n-1} \in \mathfrak{p}$ ; nel secondo caso ragionando per induzione su  $n$  ricava ugualmente  $a \in \mathfrak{p}$ .

Un ideale **massimale** è un ideale proprio che è massimale rispetto all'ordinamento di inclusione. Ogni ideale massimale  $\mathfrak{m} \subset A$  è primo: infatti se  $ab \in \mathfrak{m}$  e né  $a$  né  $b$  appartengono a  $\mathfrak{m}$  allora  $\mathfrak{m} + (a) = \mathfrak{m} + (b) = (1)$  e quindi esistono  $m_1, m_2 \in \mathfrak{m}$ ,  $x_1, x_2 \in A$  tali che  $m_1 + ax_1 = m_2 + bx_2 = 1$ . Si ottiene che  $1 = m_1 m_2 + m_1 x_2 b + m_2 x_1 a + x_1 x_2 ab \in \mathfrak{m}$ , in contraddizione con il fatto che ogni ideale massimale è proprio per definizione.

La nozione di elemento massimale fa venire in mente il celebre lemma di Zorn, che richiamiamo brevemente.

**DEFINIZIONE 9.1.2.** Siano  $(X, \leq)$  un insieme parzialmente ordinato e  $S \subset X$  un sottoinsieme:

- (1)  $S$  si dice una **catena** in  $X$  se la restrizione di  $\leq$  ad  $S$  è un ordinamento totale, ossia se per ogni  $a, b \in S$  si ha  $a \leq b$  oppure  $b \leq a$ ;
- (2) un elemento  $m \in S$  si dice il **massimo** di  $S$  (e si scrive  $m = \max(S)$ ) se per ogni  $s \in S$  vale  $s \leq m$ ;
- (3) un elemento  $b \in X$  si dice un **maggiorante** di  $S$  se per ogni  $s \in S$  vale  $s \leq m$ ;
- (4) un elemento  $c \in X$  si dice l'**estremo superiore** di  $S$  se  $s \leq c \leq m$  per ogni  $s \in S$  ed ogni maggiorante  $m$  di  $S$ ;
- (5) un elemento  $m \in S$  si dice **massimale** in  $S$  se

$$\{s \in S \mid m \leq s\} = \{m\},$$

ossia se  $S$  non contiene elementi strettamente maggiori di  $m$ .

È facile vedere che massimo ed estremo superiore, se esistono sono unici, mentre in generale non c'è unicità di maggioranti ed elementi massimali.

**TEOREMA 9.1.3 (Lemma di Zorn).** *Sia  $(X, \leq)$  un insieme parzialmente ordinato e non vuoto. Se ogni catena non vuota in  $X$  possiede maggioranti, allora  $X$  possiede elementi massimali.*

Omettiamo la dimostrazione del lemma di Zorn e vediamo invece due classiche ed istruttive applicazioni.

Iniziamo osservando che le precedenti nozioni si applicano in particolare all'insieme  $\mathcal{A}$  degli ideali propri di un anello  $A$ , ordinato per inclusione. Se  $\mathcal{C} \subset \mathcal{A}$  è una catena non vuota, allora l'unione  $J = \bigcup \{I \mid I \in \mathcal{C}\}$  degli ideali nella catena è ancora un ideale. Infatti, se  $a_1, a_2 \in J$ , allora esistono due ideali  $I_1, I_2 \in \mathcal{C}$  tali che  $a_1 \in I_1$  e  $a_2 \in I_2$ . Per definizione di catena si ha  $I_1 \subseteq I_2$  oppure  $I_2 \subseteq I_1$ . Nel primo caso  $a_1, a_2 \in I_2$  e quindi  $a_1 + a_2 \in I_2 \subset J$ ; nel secondo caso  $a_1, a_2 \in I_1$  e quindi  $a_1 + a_2 \in I_1 \subset J$ . Se  $a \in A$  e  $x \in J$ , allora esiste  $I \in \mathcal{C}$  tale che  $x \in I$ ; quindi  $ax \in I \subset J$ .

**LEMMA 9.1.4.** *Ogni ideale proprio di un anello  $A$  è contenuto in un ideale massimale.*

**DIMOSTRAZIONE.** Sia  $I \subset A$  un ideale proprio e sia  $\mathcal{A}$  la famiglia degli ideali propri che contengono  $I$ . Ovviamente  $I \in \mathcal{A}$  che quindi non è vuota; se  $\{I_\alpha\}$  è una catena in  $\mathcal{A}$  allora  $\bigcup_\alpha I_\alpha = J$  è un ideale e, siccome  $1 \notin I_\alpha$  per ogni  $\alpha$ , ne segue che  $1 \notin J$ , cioè che  $J$  è un ideale proprio. Per il lemma di Zorn  $\mathcal{A}$  possiede elementi massimali.  $\square$

**LEMMA 9.1.5.** *Sia  $I \subset A$  un ideale. Allora  $\sqrt{I}$  è l'intersezione di tutti gli ideali primi che contengono  $I$ .*

**DIMOSTRAZIONE.** Se  $\mathfrak{p}$  è un ideale primo che contiene  $I$ , allora  $\sqrt{I} \subset \sqrt{\mathfrak{p}} = \mathfrak{p}$ .

Viceversa, fissiamo un elemento  $f \notin \sqrt{I}$  e denotiamo con  $\mathcal{A}$  la famiglia degli ideali radicali che contengono  $I$  e non contengono  $f$ .  $\mathcal{A}$  non è vuota perché contiene  $\sqrt{I}$ ; se  $J_\alpha$

è una catena in  $\mathcal{A}$  allora anche  $\cup J_\alpha \in \mathcal{A}$  (verifica per esercizio) e quindi per il lemma di Zorn  $\mathcal{A}$  possiede un elemento massimale  $\mathfrak{p}$ : vogliamo dimostrare che  $\mathfrak{p}$  è un ideale primo. Sia  $ab \in \mathfrak{p}$  e supponiamo per assurdo che  $a \notin \mathfrak{p}$  e  $b \notin \mathfrak{p}$ . Allora gli ideali  $\sqrt{(a) + \mathfrak{p}}$  e  $\sqrt{(b) + \mathfrak{p}}$  non appartengono ad  $\mathcal{A}$  e, poiché contengono  $I$ , dovranno contenere anche  $f$ . Esisteranno quindi interi positivi  $n, m$  tali che  $f^n \in (a) + \mathfrak{p}$  e  $f^m \in (b) + \mathfrak{p}$ . Prendendo il prodotto otteniamo  $f^{n+m} \in (ab) + \mathfrak{p} = \mathfrak{p}$  che contraddice l'appartenenza di  $\mathfrak{p}$  ad  $\mathcal{A}$ .  $\square$

**DEFINIZIONE 9.1.6.** Il **nilradicale** di un anello commutativo è l'intersezione di tutti gli ideali primi.

Per il Lemma 9.1.5 il nilradicale coincide con l'insieme degli elementi nilpotenti  $\sqrt{0}$ .

**DEFINIZIONE 9.1.7.** Un anello si dice **locale** se contiene un solo ideale massimale. L'unico campo quoziente di un anello locale si dice **campo residuo**.

Se  $f: A \rightarrow B$  è un omomorfismo di anelli e  $J \subset B$  è un ideale, allora anche  $f^{-1}(J)$  è un ideale di  $A$ ; se  $J$  è primo allora anche  $f^{-1}(J)$  è primo, mentre se  $J$  è massimale non è detto che anche  $f^{-1}(J)$  sia massimale: si consideri ad esempio l'inclusione  $\mathbb{Z} \rightarrow \mathbb{Q}$  e l'ideale nullo  $J = 0$ . Se  $I \subset A$  è un ideale e  $f$  non è surgettivo, allora in generale  $f(I)$  non è un ideale.

**PROPOSIZIONE 9.1.8.** Sia  $f: A \rightarrow B$  un omomorfismo surgettivo di anelli con nucleo  $K$ .

- (1) Se  $I \subset A$  è un ideale, allora  $f(I)$  è un ideale e  $f^{-1}(f(I)) = I + K$ . In particolare,  $f(I)$  è un ideale proprio se e solo se  $1 \notin I + K$ .
- (2)  $f^{-1}$  induce una bigezione tra l'insieme degli ideali di  $B$  e l'insieme degli ideali di  $A$  che contengono  $K$ .
- (3) Un ideale  $J \subset B$  è primo (risp.: massimale, radicale) se e solo se  $f^{-1}(J) \subset A$  è primo (risp.: massimale, radicale).

**DIMOSTRAZIONE.** Esercizio.  $\square$

Un elemento  $x$  di un anello  $A$  si dice un **divisore di 0** se esiste  $y \in A - \{0\}$  tale che  $xy = 0$ . In particolare, un anello è un dominio di integrità se e solo se 0 è l'unico divisore di 0.

Un elemento  $x$  di un anello  $A$  si dice un **nilpotente** se esiste un intero positivo  $n$  tale che  $x^n = 0$ . Un anello si dice **ridotto** se non contiene elementi nilpotenti diversi da 0; un anello è ridotto se e solo se l'ideale 0 è radicale; è chiaro che ogni dominio di integrità è ridotto, mentre il viceversa è generalmente falso (Esempio:  $\mathbb{Z}/(6)$ ).

Dato un dominio di integrità  $A$ , il **campo delle frazioni** di  $A$  è il campo  $F$  formato dalle classi di equivalenza delle frazioni  $\frac{a}{b}$ , per  $a, b \in A$  e  $b \neq 0$ . La relazione di equivalenza  $\frac{a}{b} \sim \frac{c}{d}$  è valida se e solo se  $ad = bc$ . Le operazioni di somma e prodotto in  $F$  sono definite nel modo "naturale"

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}, \quad \frac{a}{b} \frac{c}{d} = \frac{ac}{bd}.$$

La caratteristica di un dominio di integrità è, per definizione, la caratteristica del suo campo delle frazioni; se  $A$  è un dominio di caratteristica  $p > 0$ , l'applicazione  $x \mapsto x^p$  è un omomorfismo iniettivo di  $A$  in sé detto **morfismo di Frobenius**.

**DEFINIZIONE 9.1.9.** Un dominio di integrità si dice **perfetto** se ha caratteristica 0 oppure se ha caratteristica  $p > 0$  ed il morfismo di Frobenius è surgettivo.

### Esercizi

**ESERCIZIO 26.** Siano  $I, J$  ideali di un anello  $A$ . Dimostrare che se  $I \cap J$  è un ideale primo, allora  $I \subset J$  oppure  $J \subset I$ .

**ESERCIZIO 27.** Sia  $\mathfrak{m}$  un ideale massimale di un anello  $A$ . Dimostrare che  $A$  è locale se e solo se  $1 - a$  è invertibile per ogni  $a \in \mathfrak{m}$ .

**ESERCIZIO 28.** Sia  $\mathfrak{rad}$  l'intersezione di tutti gli ideali massimali di un anello commutativo  $A$ . Dimostrare che  $a \in \mathfrak{rad}$  se e solo se  $1 + ab$  è invertibile in  $A$  per ogni  $b \in A$ .

ESERCIZIO 29. Siano  $I, J$  ideali di un anello  $A$ . Provare che  $(I : J) = \{x \in A \mid xJ \subset I\}$  è un ideale. Tale ideale viene detto **ideale quoziente**.

ESERCIZIO 30. Siano  $I, J$  ideali in un anello  $A$ . Definiamo il prodotto  $IJ$  come l'ideale generato da tutti i prodotti  $xy$ , al variare di  $x \in I$  e  $y \in J$ . Provare che gli ideali  $IJ$  e  $I \cap J$  hanno lo stesso radicale.

ESERCIZIO 31. Sia  $F$  un campo infinito:

- (1) Se  $F \subset E$  è una estensione algebrica, provare che  $E$  ha, come insieme, la stessa cardinalità di  $F$ . (La dimostrazione richiede una certa conoscenza dell'aritmetica cardinale, vedi ad esempio [8]; il lettore ignaro può assumere questo punto come un dato di fatto e passare al successivo.)
- (2) Sia  $U$  un insieme di cardinalità strettamente maggiore di  $F$  e sia  $F \subset U$  una inclusione fissata. Denotiamo con  $\mathcal{A}$  l'insieme delle triple  $(E, +, \cdot)$  tali che  $F \subset E \subset U$  e  $+, \cdot: E \times E \rightarrow E$  sono operazioni binarie che inducono una struttura di campo su  $E$  che sia inoltre una estensione algebrica di  $F$ . Poniamo su  $\mathcal{A}$  la relazione di ordine  $(E, +, \cdot) \leq (E', +', \cdot')$  se e solo se  $E$  è un sottocampo di  $E'$ . Provare che  $\mathcal{A}$  possiede elementi massimali e che ogni elemento massimale è una chiusura algebrica di  $F$ .

ESERCIZIO 32. Sia  $A$  un anello commutativo con unità e siano

$$\mathfrak{rad} = \{x \in A \mid 1 + xy \text{ è invertibile per ogni } y \in A\} \quad (\text{vedi Esercizio 28}),$$

$$\mathfrak{n} = \sqrt{0} = \{x \in A \mid x \text{ è nilpotente}\}, \quad E(A) = \{x \in A \mid x^2 = x\}.$$

Provare che:

- (1) Sia  $I \subset \mathfrak{rad}$  un ideale e sia  $a \in A$ . Provare che  $a$  è invertibile in  $A$  se e solo se la sua proiezione in  $A/I$  è invertibile.
- (2) (\*) Sia  $I \subset A$  ideale e  $\alpha: E(A) \rightarrow E(A/I)$  la proiezione al quoziente. Dimostrare che se  $I \subset \mathfrak{rad}$ , allora  $\alpha$  è iniettiva e che se  $I \subset \mathfrak{n}$ , allora  $\alpha$  è bigettiva. (Sugg.: per provare la surgettività di  $\alpha$  non è restrittivo supporre  $I$  principale a quadrato nullo; può risultare utile dimostrare che  $1 - 2x$  è invertibile nell'anello  $\mathbb{Z}[x]/(x^2 - x)$ .)

ESERCIZIO 33. Sia  $D$  l'insieme dei divisori di 0 di un anello  $A$  e sia  $\mathcal{F}$  la famiglia degli ideali contenuti in  $D$ . Provare che  $\mathcal{F}$  possiede elementi massimali rispetto all'inclusione, ognuno dei quali è un ideale primo.

## 9.2. Polinomi e fattorizzazione unica

Sia  $A$  un dominio di integrità, un elemento  $a \in A$  si dice **irriducibile** se non è invertibile e se  $a = bc$ , allora uno dei due elementi  $b, c \in A$  è invertibile. Un elemento non invertibile  $a \in A$  si dice **primo** se ogniqualvolta  $a$  divide  $bc$  si ha che  $a$  divide almeno uno dei due elementi  $b, c$ . È facile dimostrare che ogni primo è irriducibile, il viceversa è generalmente falso (vedi Esercizio 52).

Un dominio di integrità si dice a **fattorizzazione unica** se:

- (1) Ogni elemento diverso da 0 è invertibile oppure si può scrivere come prodotto di un numero finito di elementi irriducibili.
- (2) Gli elementi irriducibili nominati al punto 1 sono unicamente determinati, a meno dell'ordine e di moltiplicazione per invertibili.

I campi sono domini a fattorizzazione unica. Più in generale, è ben noto che l'anello  $\mathbb{K}[t]$  e più in generale i domini di integrità a ideali principali sono domini a fattorizzazione unica (cfr. Esercizio 45).

Se  $A$  è un anello, indicheremo con  $A[x_1, \dots, x_n]$  l'anello dei polinomi a coefficienti in  $A$  nelle indeterminate  $x_1, \dots, x_n$ . La proprietà caratterizzante di  $A[x_1, \dots, x_n]$  è che per ogni omomorfismo di anelli  $\phi: A \rightarrow B$  e per ogni  $n$ -upla  $b_1, \dots, b_n \in B$  esiste una estensione di  $\phi$  ad un omomorfismo, detto di **specializzazione**,  $\hat{\phi}: A[x_1, \dots, x_n] \rightarrow B$  tale che  $\hat{\phi}(x_i) = b_i$ .

Un polinomio  $p(t) \in A[t]$  si dice **monico** se il coefficiente della potenza più alta di  $t$  è uguale a 1. Ossia,  $p(t)$  è monico di grado  $d$  se e solo se si può scrivere

$$p(t) = t^d + a_1 t^{d-1} + \cdots + a_d, \quad a_1, \dots, a_d \in A.$$

LEMMA 9.2.1. *Siano  $A$  un anello commutativo e  $a \in A$ . Allora il polinomio  $1 - ta \in A[t]$  è invertibile in  $A[t]$  se e solo se  $a$  è nilpotente in  $A$ .*

DIMOSTRAZIONE. Se  $a$  è nilpotente, diciamo  $a^{n+1} = 0$ , allora

$$(1 - ta)(1 + ta + t^2 a^2 + \cdots + t^n a^n) = 1,$$

e quindi  $1 - ta$  è invertibile. Viceversa, se  $1 - ta$  è invertibile si ha una relazione del tipo

$$(1 - ta)(b_0 + tb_1 + t^2 b_2 + \cdots + t^n b_n) = 1, \quad b_i \in A,$$

che equivale al sistema di equazioni

$$b_0 = 1, \quad tb_1 = tab_0, \quad t^2 b_2 = t^2 ab_1, \dots, t^{n+1} ab_n = 0,$$

ed una semplice induzione su  $i$  mostra che  $b_i = a^i$  per ogni  $i = 0, \dots, n$ , da cui segue  $a^{n+1} = 0$ .  $\square$

Rimandiamo all'Esercizio 34 per una estensione del Lemma 9.2.1.

DEFINIZIONE 9.2.2. Sia  $A$  un dominio a fattorizzazione unica; un polinomio  $f \in A[t]$  si dice **primitivo** se i coefficienti di  $f$  non hanno fattori comuni.

LEMMA 9.2.3 (di Gauss). *Sia  $A$  un dominio a fattorizzazione unica con campo delle frazioni  $\mathbb{K}$ . Allora il prodotto di polinomi primitivi è primitivo, ed inoltre:*

- (1) *Se  $f, g \in A[t]$ , con  $f$  primitivo che divide  $g$  in  $\mathbb{K}[t]$ , allora  $f$  divide  $g$  in  $A[t]$ .*
- (2) *Se  $f, g \in \mathbb{K}[t]$  sono polinomi monici e  $fg \in A[t]$ , allora  $f, g \in A[t]$*
- (3)  *$A[t]$  è un dominio a fattorizzazione unica.*

DIMOSTRAZIONE. Siano  $f = \sum_{i=0}^n a_i t^i$  e  $g = \sum_{j=0}^m b_j t^j$  due polinomi primitivi in  $A[t]$  e assumiamo per assurdo che esista  $c \in A$  non invertibile che divide il prodotto  $fg$ . Siano  $r \leq n$  e  $s \leq m$  due interi tali che  $c|a_i$  per  $i < r$ ,  $c \nmid a_r$ ,  $c|b_j$  per  $j < s$  e  $c \nmid b_s$ . Il coefficiente di  $t^{r+s}$  nel prodotto  $fg$  è uguale a

$$a_r b_s + \sum_{i < r} a_i b_{r+s-i} + \sum_{j < s} a_{r+s-j} b_j$$

e quindi  $c$  divide  $a_r b_s$ . Poiché  $A$  è a fattorizzazione unica, questa è una contraddizione.

[1] Sia  $f \in A[t]$  primitivo,  $g \in \mathbb{K}[t]$  e  $fg \in A[t]$ ; mettendo i coefficienti di  $g$  a denominatore comune, possiamo trovare  $a, b \in A$  senza fattori comuni tali che  $h = \frac{ag}{b}$  è un polinomio primitivo in  $A[t]$ . Dunque  $fh = \frac{agf}{b}$  è primitivo, da cui segue che  $a$  è invertibile e quindi  $g = hb/a \in A[t]$ .

[2] Se  $f, g \in \mathbb{K}[t]$  sono polinomi monici, esistono  $a, b \in A$  tali che  $af, bg \in A[t]$  sono primitivi. Quindi  $abfg \in A[t]$  è primitivo e di conseguenza  $ab$  è invertibile.

[3] La dimostrazione del terzo punto segue facilmente dai primi due e dal fatto che  $\mathbb{K}[t]$  è un dominio a fattorizzazione unica. I dettagli sono lasciati per esercizio al lettore.  $\square$

LEMMA 9.2.4 (Divisione Euclidea). *Sia  $A$  un dominio di integrità e  $p \in A[x]$  un polinomio monico di grado  $d \geq 0$ . Allora per ogni  $f \in A[x]$  esistono unici  $g, r \in A[x]$ , con  $r$  di grado minore di  $d$ , tali che  $f = gp + r$ .*

DIMOSTRAZIONE. Esistenza: sia  $\mathcal{F} \subset A[t]$  la famiglia dei polinomi  $f$  per i quali non si può scrivere  $f = gp + r$  con  $r$  di grado  $< d$ . Se per assurdo  $\mathcal{F} \neq \emptyset$  si scelga  $h \in \mathcal{F}$  di grado minimo  $s$ . Si ha  $s \geq d$  altrimenti  $h = 0g + h$ , dunque  $s > d$  e  $h = a_0 t^s + \cdots$ . Basta adesso osservare che  $h - a_0 t^{s-d} p$  ha grado  $< s$  e non appartiene a  $\mathcal{F}$ . Si può quindi scrivere  $h - a_0 t^{s-d} p = gp + r$ , da cui  $h = (a_0 t^{s-d} + g)p + r \notin \mathcal{F}$ .

Unicità: se  $f = g_1 p + r_1 = g_2 p + r_2$  allora  $r_1 - r_2 = (g_2 - g_1)p$ ; se fosse  $g_1 \neq g_2$  allora il polinomio  $(g_2 - g_1)p$  ha grado  $\geq d$ , mentre  $r_1 - r_2$  ha grado  $< d$ . Dunque  $g_1 = g_2$  e quindi  $r_2 = f - g_2 p = f - g_1 p = r_1$ .  $\square$

LEMMA 9.2.5 (regola di Ruffini). *Sia  $A$  un dominio di integrità,  $f \in A[x]$  e  $a \in A$  tale che  $f(a) = 0$ . Allora  $(x - a)$  divide  $f$ ; in particolare esistono in  $A$  al più  $\deg(f)$  radici.*

DIMOSTRAZIONE. Per la divisione Euclidea si può scrivere  $f(x) = g(x)(x - a) + f(a)$ .  $\square$

LEMMA 9.2.6. *Sia  $A$  un dominio a fattorizzazione unica con campo delle frazioni  $\mathbb{K}$  e siano  $f, g \in A[x]$  polinomi di grado positivo. Allora  $f$  e  $g$  hanno un fattore comune in  $A[x]$  di grado positivo se e solo se  $f$  e  $g$  hanno una radice comune nella chiusura algebrica di  $\mathbb{K}$ .*

DIMOSTRAZIONE. Una implicazione è evidente. Viceversa supponiamo che  $f$  e  $g$  abbiano una radice comune in  $\overline{\mathbb{K}}$  e dimostriamo, per induzione sulla somma dei gradi, che  $f$  e  $g$  hanno un fattore comune di grado positivo; non è restrittivo supporre  $f$  e  $g$  polinomi primitivi. Se  $f$  e  $g$  hanno entrambi grado 1, diciamo  $f = ax + b$  e  $g = cx + d$ , allora  $\frac{b}{a} = \frac{d}{c}$  e quindi esiste un invertibile  $e$  tale che  $a = ec$  e  $b = ed$ . Se la somma dei gradi è maggiore di 2 e, tanto per fissare le idee,  $\deg f \geq \deg g$ , allora esistono  $a \in A - \{0\}$  ed un polinomio  $h \in A[x]$  di grado  $\deg f - \deg g$  tali che

$$\deg(af - hg) < \deg f.$$

I polinomi  $g$  e  $af - hg$  hanno una radice comune e per l'ipotesi induttiva esiste un polinomio irriducibile  $q \in A[x]$  di grado positivo che divide  $g$  e  $af$ .  $\square$

Dal Lemma 9.2.5 segue il seguente criterio di cui faremo uso in seguito: *se  $A$  è un dominio di integrità infinito ed  $f \in A[t]$  allora  $f = 0$  se e solo se  $f(a) = 0$  per infiniti  $a \in A$ .*

Dato un qualsiasi anello  $A$ , per ogni  $i = 1, \dots, s$  esiste una un'applicazione

$$\frac{\partial}{\partial x_i}: A[x_1, \dots, x_s] \rightarrow A[x_1, \dots, x_s]$$

che chiameremo **derivata parziale** e che soddisfa le seguenti 4 condizioni:

- (1)  $\frac{\partial}{\partial x_i}(a) = 0$  per ogni  $a \in A$ .
- (2) (additività)  $\frac{\partial}{\partial x_i}(b_1 + b_2) = \frac{\partial}{\partial x_i}(b_1) + \frac{\partial}{\partial x_i}(b_2)$  per ogni  $b_1, b_2 \in A[x_1, \dots, x_s]$ .
- (3) (Leibniz)  $\frac{\partial}{\partial x_i}(b_1 b_2) = b_1 \frac{\partial}{\partial x_i}(b_2) + b_2 \frac{\partial}{\partial x_i}(b_1)$  per ogni  $b_1, b_2 \in A[x_1, \dots, x_s]$ .
- (4)  $\frac{\partial}{\partial x_i}(x_j) = \delta_{ij}$  (delta di Kronecker).

Si vede facilmente che  $\frac{\partial}{\partial x_i}$  è ben definita e unica. Scriveremo spesso  $\frac{\partial b}{\partial x_i}$  in luogo di  $\frac{\partial}{\partial x_i}(b)$ .

Più in generale dato un morfismo di anelli  $A \rightarrow B$ , un'applicazione  $d: B \rightarrow B$  che soddisfa le precedenti condizioni 1), 2) e 3) si dice una  **$A$ -derivazione**. Se  $A = \mathbb{R}$  le applicazioni  $\frac{\partial}{\partial x_i}$  coincidono con le usuali derivate parziali.

LEMMA 9.2.7. *Sia  $A$  un dominio perfetto a fattorizzazione unica e  $f \in A[x_1, \dots, x_s]$ . Allora  $f$  possiede un fattore multiplo di grado positivo se e solo se  $f, \frac{\partial f}{\partial x_1}, \dots, \frac{\partial f}{\partial x_s}$  hanno un fattore comune di grado positivo.*

DIMOSTRAZIONE. Se  $h^2$  divide  $f$ , segue immediatamente dalla regola di Leibniz che  $h$  divide tutte le derivate parziali. Viceversa sia  $f = f_1 f_2 \cdots f_n$  con i polinomi  $f_i$  irriducibili e senza fattori in comune; si assuma per assurdo che  $f_1$  abbia grado positivo e divida tutte le derivate parziali di  $f$ . Di nuovo per Leibniz segue che  $f_1$  divide  $\frac{\partial f_1}{\partial x_i}$  per ogni  $i$  e quindi, siccome il grado della derivata è strettamente inferiore, deve essere necessariamente  $\frac{\partial f_1}{\partial x_i} = 0$  per ogni  $i$ .

Basta quindi dimostrare che se  $f$  è irriducibile di grado positivo, allora possiede almeno una derivata parziale non nulla. L'asserzione è evidente in caratteristica 0, mentre se la caratteristica è  $p > 0$  e le tutte derivate parziali sono nulle, allora  $f \in A[x_1^p, \dots, x_s^p]$ . Siccome  $A$  è perfetto, si ha che  $f$  appartiene all'immagine del morfismo di Frobenius  $A[x_1, \dots, x_s] \rightarrow A[x_1, \dots, x_s]$  e quindi esiste  $h \in B$  tale che  $f = h^p$ .  $\square$

**Esercizi**

ESERCIZIO 34. Sia  $A$  un anello commutativo e  $f = a_0x^n + \dots + a_n \in A[x]$  un polinomio a coefficienti in  $A$ . Provare che:

- (1)  $f$  è nilpotente se e solo se  $a_i$  è nilpotente per ogni  $i$ .
- (2)  $f$  è invertibile se e solo se  $a_n$  è invertibile e  $a_0, \dots, a_{n-1}$  sono nilpotenti.

ESERCIZIO 35. Siano  $A$  un anello,  $0 \leq r < n$  interi e  $a_{r+1}, \dots, a_n \in A$ . Mostrare che l'applicazione

$$\phi: A[x_1, \dots, x_n] \rightarrow A[x_1, \dots, x_r], \quad \phi(f(x_1, \dots, x_n)) = f(x_1, \dots, x_r, a_{r+1}, \dots, a_n)$$

è un omomorfismo surgettivo di anelli e che il nucleo di  $\phi$  è l'ideale generato da  $x_{r+1} - a_{r+1}, \dots, x_n - a_n$ . (Sugg.: scrivere  $x_i = y_i + a_i$ .)

ESERCIZIO 36. Sia  $A = \mathbb{K}[t^2, t^3] \subset \mathbb{K}[t]$  il sottoanello dei polinomi con il coefficiente di  $t$  nullo. Provare che  $A$  non è un dominio a fattorizzazione unica e che il Lemma 9.2.6 non vale in  $A[x]$ .

ESERCIZIO 37. Siano  $d_1, d_2: A[x_1, \dots, x_s] \rightarrow A[x_1, \dots, x_s]$  due  $A$ -derivazioni. Dimostrare che  $d_1 = d_2$  se e solo se  $d_1(x_i) = d_2(x_i)$  per ogni  $i = 1, \dots, s$ .

ESERCIZIO 38. La **derivazione di Eulero** è l'unica  $A$ -derivazione

$$E: A[x_1, \dots, x_s] \rightarrow A[x_1, \dots, x_s]$$

tale che  $E(x_i) = x_i$  per ogni  $i$ . Dimostrare che  $E = \sum_i x_i \frac{\partial}{\partial x_i}$ .

ESERCIZIO 39. Siano  $f \in A[x_1, \dots, x_s]$  e  $g_1, \dots, g_s \in A[t]$ , provare che

$$\frac{\partial}{\partial t} f(g_1(t), \dots, g_s(t)) = \sum_{i=1}^s \frac{\partial f}{\partial x_i}(g_1(t), \dots, g_s(t)) \frac{\partial g_i}{\partial t}(t)$$

ESERCIZIO 40. Provare che in  $A[x_1, \dots, x_s]$  gli operatori  $\frac{\partial}{\partial x_i}$  commutano tra loro.

ESERCIZIO 41. Sia  $A \rightarrow B$  un morfismo di anelli e siano  $f, g, h: B \rightarrow B$  tre  $A$ -derivazioni. Provare che:

- (1)  $f + g$  e  $bf$  sono  $A$ -derivazioni per ogni  $b \in B$ .
- (2)  $[f, g] := f \circ g - g \circ f$  è una  $A$ -derivazione.
- (3)  $[f \circ g, h] = f \circ [g, h] + [f, h] \circ g$ .

ESERCIZIO 42. Sia  $R$  un dominio a fattorizzazione unica di caratteristica  $\neq 2$  e  $A = (A^{ij})$  una matrice simmetrica  $n \times n$  di rango 1 a coefficienti in  $R$ . Dimostrare che esistono, e che sono unici a meno di moltiplicazione per invertibili, elementi  $a, p_1, \dots, p_n \in R$  tali che  $\text{GCD}(p_1, \dots, p_n) = 1$  e  $A^{ij} = ap_i p_j$ .

ESERCIZIO 43. Sia  $A(t)$  una matrice quadrata a coefficienti in  $\mathbb{K}[t]$ . Se  $r$  è la dimensione su  $\mathbb{K}$  del nucleo di  $A(0)$ , allora  $t^r$  divide il determinante di  $A(t)$ .

ESERCIZIO 44 (\*). Dimostrare che un dominio di integrità è a fattorizzazione unica se e solo se sono soddisfatte entrambe le seguenti condizioni:

- (1) Ogni elemento irriducibile è primo.
- (2) Ogni famiglia non vuota di ideali principali possiede un elemento massimale.

ESERCIZIO 45. Dedurre dall'Esercizio 44 che ogni dominio ad ideali principali è a fattorizzazione unica.

ESERCIZIO 46. Dimostrare che ogni dominio di integrità finito è un campo.

ESERCIZIO 47. Dimostrare che i campi finiti sono perfetti; dimostrare inoltre che, in ogni caratteristica positiva, esistono campi non perfetti e domini perfetti che non sono campi.

ESERCIZIO 48. Provare che il polinomio  $x^3 + 2x^2 + 2x - 88$  non ha radici razionali positive.

### 9.3. Anelli graduati

Un anello  $A$  si dice **graduato** se come gruppo abeliano ammette una decomposizione in somma diretta

$$A = \bigoplus_{d=-\infty}^{+\infty} A_d$$

tale che  $A_n A_m \subset A_{n+m}$  per ogni  $n, m \in \mathbb{Z}$ . Gli elementi di  $A_d \subset A$  si dicono **omogenei** di grado  $d$ . Un ideale  $I$  di un anello graduato  $A$  si dice **omogeneo** se ogniqualvolta  $a \in I$  accade che anche tutte le componenti omogenee di  $a$  appartengono a  $I$ : in altre parole  $I$  è omogeneo se e solo se  $I = \bigoplus_{d=-\infty}^{+\infty} (I \cap A_d)$ ; si dimostra facilmente che un ideale è omogeneo se e solo se è generato da elementi omogenei.

Se  $A$  è un dominio di integrità graduato e  $f, g \in A$  sono tali che il loro prodotto  $fg$  è omogeneo, allora  $f$  e  $g$  sono necessariamente omogenei: infatti se  $f = f_n + f_{n+1} + \dots + f_N$  e  $g = g_r + g_{r+1} + \dots + g_R$  sono le decomposizioni in componenti omogenee, con  $f_n, f_N, g_r, g_R \neq 0$ , allora  $fg = f_N g_R + f_n g_r + C$ , dove  $C$  è una combinazione lineare di elementi omogenei di gradi strettamente compresi fra  $n+r$  e  $N+R$ . Siccome  $fg$  è omogeneo deve necessariamente essere  $n+r = N+R$  e quindi  $n = N, r = R$ .

Per ogni anello commutativo  $A$ , l'anello dei polinomi  $A[x_1, \dots, x_n]$  possiede una graduazione naturale

$$A[x_1, \dots, x_n] = \bigoplus_{d=0}^{+\infty} A_d,$$

dove  $A_d$  è l'insieme dei polinomi omogenei di grado  $d$ , ossia l'insieme delle combinazioni lineari a coefficienti in  $A$  di monomi  $x_1^{i_1} x_2^{i_2} \dots x_n^{i_n}$  con  $i_1 + \dots + i_n = d$ . A volte è utile associare ad ogni variabile  $x_i$  un peso  $w(x_i) \in \mathbb{N}$ ; in tal caso diremo che un polinomio è **isobaro di peso**  $m$ , rispetto ai pesi  $w(x_i)$ , se è combinazione lineare a coefficienti in  $A$  di monomi  $x_1^{i_1} x_2^{i_2} \dots x_n^{i_n}$  con  $i_1 w(x_1) + \dots + i_n w(x_n) = m$ .

Il ragionamento precedente mostra che se  $A$  è un dominio a fattorizzazione unica, allora i fattori irriducibili di un polinomio omogeneo (risp.: isobaro)  $f \in A[x_1, \dots, x_n]$  sono omogenei (risp.: isobari).

Nello studio degli anelli graduati si utilizza con una certa frequenza il determinante di Vandermonde, che richiamiamo velocemente per completezza. Dati  $n+1$  elementi  $x_0, \dots, x_n$  in un campo vale la formula

$$\begin{vmatrix} 1 & 1 & \dots & 1 \\ x_0 & x_1 & \dots & x_n \\ \vdots & \vdots & \ddots & \vdots \\ x_0^{n-1} & x_1^{n-1} & \dots & x_n^{n-1} \\ x_0^n & x_1^n & \dots & x_n^n \end{vmatrix} = \prod_{i>j} (x_i - x_j)$$

Possiamo dimostrare tale formula per induzione su  $n$ , considerando il polinomio

$$p(t) = \prod_{j=0}^{n-1} (t - x_j) = t^n + \sum_{i=0}^{n-1} a_i t^i.$$

Sommando all'ultima riga della matrice la combinazione lineare a coefficienti  $a_i$  delle rimanenti righe si ottiene

$$\begin{vmatrix} 1 & 1 & \dots & 1 \\ x_0 & x_1 & \dots & x_n \\ \vdots & \vdots & \ddots & \vdots \\ x_0^{n-1} & x_1^{n-1} & \dots & x_n^{n-1} \\ x_0^n & x_1^n & \dots & x_n^n \end{vmatrix} = \begin{vmatrix} 1 & 1 & \dots & 1 \\ x_0 & x_1 & \dots & x_n \\ \vdots & \vdots & \ddots & \vdots \\ x_0^{n-1} & x_1^{n-1} & \dots & x_n^{n-1} \\ p(x_0) & p(x_1) & \dots & p(x_n) \end{vmatrix}$$

Dato che  $p(x_i) = 0$  per ogni  $i < n$  e  $p(x_n) = \prod_{n>j}(x_n - x_j)$  si ha

$$\begin{vmatrix} 1 & 1 & \cdots & 1 \\ x_0 & x_1 & \cdots & x_n \\ \vdots & \vdots & \ddots & \vdots \\ x_0^{n-1} & x_1^{n-1} & \cdots & x_n^{n-1} \\ x_0^n & x_1^n & \cdots & x_n^n \end{vmatrix} = \begin{vmatrix} 1 & 1 & \cdots & 1 \\ x_0 & x_1 & \cdots & x_{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ x_0^{n-1} & x_1^{n-1} & \cdots & x_{n-1}^{n-1} \end{vmatrix} \cdot \prod_{n>j}(x_n - x_j).$$

LEMMA 9.3.1. *Sia  $A$  un dominio di integrità infinito e sia  $f \in A[x_1, \dots, x_s]$ . Allora  $f$  è omogeneo di grado  $n$  se e solo se*

$$f(tx_1, \dots, tx_s) = t^n f(x_1, \dots, x_s)$$

per ogni  $t \in A$ .

DIMOSTRAZIONE. Se  $f$  è omogeneo la relazione precedente è evidente. Viceversa scriviamo  $f = f_0 + f_1 + \dots + f_N$  con  $f_i$  omogeneo di grado  $i$ . Il polinomio  $P = f_0 + tf_1 + \dots + t^N f_N - t^n f \in A[x_1, \dots, x_s, t]$  si annulla per infiniti valori di  $t \in A \subset A[x_1, \dots, x_s]$  e quindi deve necessariamente essere  $f_n = f$  e  $f_i = 0$  per  $i \neq n$ .  $\square$

LEMMA 9.3.2. *Sia  $\mathbb{K}$  un campo infinito. Un ideale  $I \subset \mathbb{K}[x_1, \dots, x_n]$  è omogeneo se e solo se per ogni  $f \in I$  e per ogni  $t \in \mathbb{K}$ , il polinomio  $f_t(x_1, \dots, x_n) := f(tx_1, \dots, tx_n)$  appartiene all'ideale  $I$ .*

DIMOSTRAZIONE. Dimostriamo il lemma utilizzando il cosiddetto *argomento di Vandermonde*: tale metodo sarà usato nuovamente in seguito.

Scriviamo  $f = f_0 + f_1 + \dots + f_s$ , dove  $f_i$  è omogeneo di grado  $i$ . Per ogni scelta di  $t_0, t_1, \dots, t_s \in \mathbb{K}$  vale  $f_{t_i} = \sum_j t_j^i f_j$ . Siccome  $\mathbb{K}$  è infinito, possiamo scegliere gli scalari  $t_0, t_1, \dots, t_s$  distinti. Quindi il determinante della matrice di Vandermonde  $(t_j^i)$  è invertibile, esiste la matrice inversa  $(a_j^i) = (t_j^i)^{-1}$  e, per ogni  $j = 0, \dots, s$ , vale  $f_j = \sum_i a_j^i f_{t_i} \in I$ .  $\square$

Come ulteriore applicazione della matrice di Vandermonde diamo la seguente estensione del Lemma 8.2.6.

LEMMA 9.3.3. *Siano  $\mathbb{K}$  un campo perfetto e  $f \in \mathbb{K}[x_0, \dots, x_n]$  un polinomio di grado positivo e senza fattori multipli. Allora esistono al più un numero finito di elementi  $a \in \mathbb{K} - \{0\}$  tali che il polinomio*

$$\sum_{i=0}^n a^i \frac{\partial f}{\partial x_i}$$

ha fattori in comune con  $f$ .

DIMOSTRAZIONE. Osserviamo prima che il Lemma 8.2.6 vale, con la stessa identica dimostrazione, per ogni campo perfetto.

Sia  $f = f_1 f_2 \cdots f_r$  la decomposizione di  $f$  in fattori irriducibili: dire che  $f$  non ha fattori multipli equivale a dire che  $f_i$  non divide  $f_j$  per ogni  $i \neq j$ . Dimostriamo preliminarmente che per ogni  $i = 1, \dots, r$  esiste  $j = 0, \dots, n$  tale che  $f_i$  non divide  $\frac{\partial f}{\partial x_j}$ : per evidente simmetria basta considerare solo il caso  $i = 1$ .

Supponiamo per assurdo che  $f_1$  divida tutte le derivate parziali di  $f$ . Segue allora dalla formula di Leibniz

$$\frac{\partial f}{\partial x_j} = \frac{\partial f_1}{\partial x_j} f_2 \cdots f_r + f_1 \frac{\partial f_2 \cdots f_r}{\partial x_j},$$

che  $f_1$  divide  $\frac{\partial f_1}{\partial x_i}$  per ogni  $i$  e quindi, siccome il grado della derivata è strettamente inferiore, deve essere necessariamente  $\frac{\partial f_1}{\partial x_j} = 0$  per ogni  $j$ . Basta quindi osservare che per il Lemma 8.2.6 ogni polinomio irriducibile di grado positivo, possiede almeno una derivata parziale non nulla.

Supponiamo per assurdo che  $f$  abbia un fattore in comune con il polinomio

$$F_a := \sum_{i=0}^n a^i \frac{\partial f}{\partial x_i}$$

per ogni  $a \in S$ , con  $S$  sottoinsieme infinito di  $\mathbb{K} - \{0\}$ . Per il principio dei cassetti esistono  $n+1$  elementi distinti  $a_0, \dots, a_n \in S$  ed una componente irriducibile  $f_k$  che divide  $F_{a_0}, \dots, F_{a_n}$ . Abbiamo visto che la matrice di Vandermonde  $V = (a_i^j)$ ,  $i, j = 0, \dots, n$ , è invertibile,

$$(F(a_0), \dots, F(a_n)) = \left( \frac{\partial f}{\partial x_0}, \dots, \frac{\partial f}{\partial x_n} \right) V \iff \left( \frac{\partial f}{\partial x_0}, \dots, \frac{\partial f}{\partial x_n} \right) = (F(a_0), \dots, F(a_n)) V^{-1}$$

e questo implica che  $f_k$  divide  $\frac{\partial f}{\partial x_j}$  per ogni  $j$ , in contraddizione con quanto precedentemente dimostrato.  $\square$

LEMMA 9.3.4 (Formula di Eulero). Se  $f \in A[x_1, \dots, x_s]$  è omogeneo di grado  $n$ , allora vale

$$nf = \sum_{i=1}^s x_i \frac{\partial f}{\partial x_i}.$$

DIMOSTRAZIONE. Induzione su  $n$ . Se  $n = 0$ , allora  $f \in A$  e la formula è chiara. Sia  $n > 0$  e supponiamo la formula vera per polinomi omogenei di grado  $n-1$ ; per linearità basta provare la formula nel caso in cui  $f$  è un monomio, si può quindi scrivere  $f = x_j f'$  per qualche  $j = 1, \dots, s$  e  $f'$  omogeneo di grado  $n-1$ . Quindi per induzione

$$\sum_{i=1}^s x_i \frac{\partial f}{\partial x_i} = \sum_{i=1}^s x_j x_i \frac{\partial f'}{\partial x_i} + x_j f' = (n-1)x_j f' + x_j f' = nx_j f' = nf.$$

$\square$

### Esercizi

ESERCIZIO 49. Sia  $B = (b_{ij})$  una matrice le cui colonne sono linearmente dipendenti su  $A$ , provare che  $\det(B)$  è un divisore di 0.

ESERCIZIO 50. Sia  $B = (b_{ij})$  una matrice  $n \times (n+1)$  a coefficienti in un anello  $A$  e denotiamo con  $d_j$  il determinante minore  $n \times n$  calcolato togliendo a  $B$  la  $j$ -esima colonna. Dimostrare che

$$B \begin{pmatrix} d_1 \\ -d_2 \\ d_3 \\ \vdots \end{pmatrix} = 0.$$

(Sugg.: calcolare i determinanti delle matrici  $(n+1) \times (n+1)$  ottenute duplicando le righe di  $B$ .)

ESERCIZIO 51. Siano  $m$  e  $n$  interi positivi fissati e sia  $\mathbb{K}$  un campo di caratteristica 0 oppure maggiore di  $m$ . Dimostrare che l'insieme

$$\{p^m \mid p \in \mathbb{K}[x_1, \dots, x_n]\},$$

delle potenze  $m$ -esime dei polinomi genera  $\mathbb{K}[x_1, \dots, x_n]$  come  $\mathbb{K}$ -spazio vettoriale (Sugg.: Vandermonde).

ESERCIZIO 52. Sia  $A = \mathbb{K}[x, y, z]/(xy - z^2)$ . Provare che  $A$  è un dominio di integrità e che  $z \in A$  è irriducibile ma non è primo. (Sugg.: l'anello  $A$  è graduato).

ESERCIZIO 53. Sia  $B$  una matrice  $n \times n$  a coefficienti in un anello  $A$  e  $\tilde{B}$  la sua matrice aggiunta. Provare che per ogni vettore riga  $v$  e per ogni vettore colonna  $w$  di  $A^n$  vale

$$v\tilde{B}w + \det \begin{pmatrix} B & w \\ v & 0 \end{pmatrix} = 0$$

ESERCIZIO 54. (caratteristica 0) Dimostrare che per ogni intero  $n \geq 3$  non esistono polinomi  $p, q, r \in \mathbb{K}[x]$  relativamente primi e non costanti tali che  $p^n + q^n = r^n$ . (Sugg.: siano per assurdo  $p, q, r$  come sopra e tali che  $\deg(p) \geq \max(1, \deg(q))$ ; considerare la derivata rispetto a  $x$  e dedurne che  $p^{n-1}$  divide  $qr' - rq'$ .)

ESERCIZIO 55. Sia  $f \in \mathbb{K}[x_1, \dots, x_s]$  un polinomio omogeneo di grado  $n$ . Differenziare la relazione  $t^n f(x_1, \dots, x_s) = f(tx_1, \dots, tx_s)$  e riottenere la formula di Eulero.

ESERCIZIO 56. Provare che l'unica  $\mathbb{R}$ -derivazione su  $\mathbb{C}$  è quella nulla. Più in generale se  $A$  è un dominio perfetto e  $f \in A[t]$  è irriducibile, allora ogni  $A$ -derivazione su  $A[t]/(f)$  è nulla.

ESERCIZIO 57. Provare che un dominio a fattorizzazione unica  $A$  è perfetto se e solo se per ogni  $f \in A[t]$  irriducibile vale  $\frac{df}{dt} \neq 0$ .

ESERCIZIO 58. Sia  $A \rightarrow B$  un morfismo di anelli,  $a, b \in B$  e siano  $D, D': B \rightarrow B$  due  $A$ -derivazioni; allora vale

$$[aD, bD'] = ab[D, D'] + aD(b)D' - bD'(a)D.$$

ESERCIZIO 59. Sia  $\mathbb{Q} \rightarrow A$  un morfismo di anelli,  $D: A \rightarrow A$  una  $\mathbb{Q}$ -derivazione e sia  $x \in A$  tale che  $Dx = 1$  e  $\bigcap_{i=1}^{\infty} (x^i) = 0$ . Provare che  $x$  non è un divisore di 0.

ESERCIZIO 60. Enunciare e provare l'analogo della formula di Eulero (Lemma 9.3.4) per i polinomi isobari.

### 9.4. Anelli Noetheriani

In questa sezione dimostreremo il teorema della base di Hilbert. Per future applicazioni è conveniente inquadrare il teorema in un ambito più astratto di quello considerato precedentemente.

LEMMA 9.4.1. *Per un insieme parzialmente ordinato  $(S, \leq)$  le seguenti condizioni sono equivalenti.*

- (1) ogni sottoinsieme non vuoto di  $S$  possiede elementi massimali;
- (2) ogni successione monotona non decrescente  $x_0 \leq x_1 \leq \dots$  in  $S$  è stazionaria, ossia esiste  $m \in \mathbb{N}$  tale che  $x_n = x_m$  per ogni  $n \geq m$ .

DIMOSTRAZIONE. Data una successione monotona non decrescente  $x_0 \leq x_1 \leq \dots$ , se ogni sottoinsieme di  $S$  possiede elementi massimali, allora anche l'insieme  $\{x_0, x_1, \dots\}$  possiede un elemento massimale, diciamo  $x_m$ . Allora necessariamente  $x_n = x_m$  per ogni  $n \geq m$  e la successione è stazionaria.

Viceversa, se esiste un sottoinsieme non vuoto  $H \subset S$  senza elementi massimali, allora, per ogni  $x \in H$ , il sottoinsieme  $H_x = \{y \in H \mid y > x\}$  è non vuoto. Per l'assioma della scelta esiste un'applicazione  $f: H \rightarrow H$  tale che  $f(x) \in H_x$  per ogni  $x \in H$ . Preso comunque  $x_0 \in H$ , la successione  $x_n = f^n(x_0)$  è monotona e non è stazionaria.  $\square$

DEFINIZIONE 9.4.2. Un anello in cui ogni ideale è finitamente generato si dice **Noetheriano**.

È chiaro dalla definizione che i campi e gli anelli ad ideali principali sono tutti Noetheriani.

PROPOSIZIONE 9.4.3. *Sia  $A$  un anello Noetheriano e  $I$  un ideale. Allora l'anello quoziente  $A/I$  è Noetheriano.*

DIMOSTRAZIONE. Siano  $\pi: A \rightarrow A/I$  la proiezione al quoziente e  $J \subset A/I$  un ideale. Allora l'ideale  $\pi^{-1}(J)$  è finitamente generato, diciamo  $\pi^{-1}(J) = (a_1, \dots, a_n)$ . Ma allora, essendo  $\pi^{-1}(J) \rightarrow J$  surgettiva si ha  $J = (\pi(a_1), \dots, \pi(a_n))$ .  $\square$

È invece falso in generale che un sottoanello di un anello Noetheriano è ancora Noetheriano: ogni dominio di integrità non Noetheriano (Esempio 9.4.5) è un sottoanello del suo campo delle frazioni che è Noetheriano.

LEMMA 9.4.4. *Per un anello  $A$  le seguenti condizioni sono equivalenti:*

- (1)  $A$  è Noetheriano;
- (2) Ogni catena non vuota di ideali in  $A$  è stazionaria, ossia possiede massimo;
- (3) Ogni successione non decrescente di ideali in  $A$  è stazionaria;
- (4) Ogni famiglia non vuota di ideali di  $A$  contiene un elemento massimale.

DIMOSTRAZIONE. [1  $\Rightarrow$  2] Sia  $\{I_v \mid v \in V\}$  una catena di ideali e sia  $I = \cup\{I_v \mid v \in V\}$ . Allora  $I$  è un ideale che risulta finitamente generato, diciamo da  $a_1, \dots, a_n$ . Se  $a_i \in I_{v_i}$ , per  $i = 1, \dots, n$ , allora detto  $w$  il massimo di  $v_1, \dots, v_n$  si ha che  $I \subset I_w \subset I_v \subset I$  per ogni  $v \geq w$  e quindi  $I_w$  è il massimo della catena.

[2  $\Rightarrow$  3] è ovvio e [3  $\Rightarrow$  4] è una immediata applicazione del Lemma 9.4.1.

[4  $\Rightarrow$  1] Sia  $I$  un ideale e sia  $J \subset I$  un elemento massimale della famiglia degli ideali finitamente generati contenuti in  $I$ , dimostriamo che  $J = I$ . Sia  $a \in I$  allora l'ideale  $J + (a) \subset I$  è ancora finitamente generato e per la massimalità di  $J$  si deve avere  $a \in J$ .  $\square$

ESEMPIO 9.4.5. L'anello delle funzioni oloedre intere, ossia definite su tutto  $\mathbb{C}$  è un dominio di integrità che non è Noetheriano. Il fatto che sia un dominio di integrità segue immediatamente dal fatto che le funzioni oloedre sono sviluppabili in serie di potenze, mentre la prova che esiste un ideale che non è finitamente generato è una conseguenza del teorema di estensione di Riemann. La funzione  $e^{2\pi iz} - 1$  è oloedra e ha uno zero semplice in ciascun punto di  $\mathbb{Z} \subset \mathbb{C}$ , pertanto per ogni intero  $n$  la funzione

$$f_n(z) = \frac{e^{2\pi iz} - 1}{2\pi i(z - n)}$$

è oloedra,  $f_n(n) = 1$  e  $f_n(m) = 0$  per ogni intero  $m \neq n$ . Per ogni intero positivo  $n$ , la funzione  $f_n$  non appartiene all'ideale generato da  $f_1, \dots, f_{n-1}$  per il semplice fatto che  $f_i(n) = 0$  per ogni  $i < n$  mentre  $f_n(n) \neq 0$ . In particolare la catena di ideali

$$(f_1) \subset (f_1, f_2) \subset (f_1, f_2, f_3) \subset \dots$$

non è stazionaria.

TEOREMA 9.4.6 (Della base di Hilbert). *Se  $A$  è un anello Noetheriano, allora anche  $A[x]$  è Noetheriano.*

DIMOSTRAZIONE. Dato un polinomio  $f \in A[x]$  di grado  $r \geq 0$  chiameremo coefficiente direttore di  $f$  il coefficiente di  $x^r$  in  $f$ ; è utile osservare che i polinomi  $f, xf, x^2f, \dots$  hanno tutti lo stesso coefficiente direttore.

Sia  $I \subset A[x]$  un ideale e, per ogni  $m \geq 0$ , denotiamo con  $J_m \subset A$  l'insieme formato dallo 0 e dai coefficienti direttori dei polinomi di grado  $m$  contenuti in  $I$ . Si osserva immediatamente che  $J_m$  è un ideale e che  $J_m \subset J_{m+1}$  per ogni  $m$ . Per ipotesi l'anello  $A$  è Noetheriano, dunque gli ideali  $J_m$  sono tutti finitamente generati e la catena ascendente  $\{J_m \mid m \in \mathbb{N}\}$  è stazionaria. Sia  $N > 0$  tale che  $J_m = J_N$  per ogni  $m \geq N$  e, per ogni  $i = 0, \dots, N$ , siano  $f_1^i, \dots, f_j^i \in I$  polinomi di grado  $i$  i cui coefficienti direttori generano  $J_i$ . Sia  $H \subset I$  l'ideale generato dai polinomi  $f_j^i$ , per  $i = 0, \dots, N$ , e proviamo che  $H = I$ . Infatti, sia  $f \in I$  e scriviamo  $f = h + g$  con  $h \in H$ ,  $g$  di grado minimo e si assuma per assurdo  $g \neq 0$ . Sia  $r = \min(\deg(g), N)$ , allora il coefficiente direttore di  $g$  appartiene a  $J_r$  e quindi esistono  $a_1, \dots, a_j \in A$  tali che, detto  $s = \deg(g) - r$ , il polinomio  $g - (a_1 f_1^r + \dots + a_j f_j^r)x^s$  ha grado minore del grado di  $g$ . Dato che  $\sum a_i f_i^r \in H$  l'assurdo è servito.  $\square$

COROLLARIO 9.4.7. *Per ogni campo  $\mathbb{K}$  e per ogni ideale  $I \subset \mathbb{K}[x_1, \dots, x_n]$ , l'anello quoziente  $\mathbb{K}[x_1, \dots, x_n]/I$  è Noetheriano.*

DIMOSTRAZIONE. Il campo  $\mathbb{K}$  è Noetheriano, per il teorema della base di Hilbert e per induzione su  $n$  si ha che  $\mathbb{K}[x_1, \dots, x_n]$  è Noetheriano. Basta adesso applicare la Proposizione 9.4.3.  $\square$

### Esercizi

ESERCIZIO 61. Provare che l'anello delle funzioni continue  $f: [0, 1] \rightarrow \mathbb{R}$  non è Noetheriano.

ESERCIZIO 62. Siano  $A$  un anello Noetheriano ed  $E \subset A$  un sottoinsieme. Provare che esiste un sottoinsieme finito  $E_0 \subset E$  tale che  $(E) = (E_0)$ .

ESERCIZIO 63. Siano  $A$  un anello Noetheriano e  $f: A \rightarrow A$  un endomorfismo surgettivo di anelli. Provare che  $f$  è un isomorfismo.

ESERCIZIO 64. Sia  $A$  un anello e denotiamo con  $\mathcal{D}$  la famiglia degli ideali di  $A$  che non sono finitamente generati. Provare che se  $\mathcal{D} \neq \emptyset$ , cioè se  $A$  non è Noetheriano, allora  $\mathcal{D}$  contiene elementi massimali rispetto all'inclusione. Dimostrare inoltre gli elementi massimali di  $\mathcal{D}$  sono ideali primi di  $A$ . (Sugg.: se  $I$  è un ideale,  $xy \in I$  e  $J \subset I$  un ideale tale che  $I + (x) = J + (x)$ , allora vale  $I = J + x(I : x)$ , dove  $(I : x) = \{y \in A \mid xy \in I\}$ .)

ESERCIZIO 65. Dimostrare che la famiglia degli ideali primi di un anello commutativo possiede elementi minimali rispetto all'inclusione.

### 9.5. Il risultante

Siano  $A$  un anello commutativo. L'obiettivo di questa sezione è quello di definire esplicitamente, per ogni polinomio *monico*  $f \in A[x]$ , un'applicazione

$$A[x] \rightarrow A, \quad g \mapsto R(f, g),$$

che gode di alcune buone proprietà che saranno elencate a breve. L'elemento  $R(f, g)$  verrà detto **risultante** di  $f$  e  $g$  e sarà definito come il determinante di una opportuna matrice a coefficienti in  $A$ .

Sia  $B = (b_{ij})$  una matrice quadrata di ordine  $n$  a coefficienti in un anello  $A$ . Come per le matrici a coefficienti in un campo si definisce il determinante di  $B$  nel modo seguente

$$\det(B) = |b_{ij}| = \sum_{\sigma \in \Sigma_n} (-1)^\sigma b_{1\sigma(1)} \cdots b_{n\sigma(n)}$$

dove  $\Sigma_n$  è il gruppo simmetrico delle permutazioni di  $\{1, \dots, n\}$  e  $(-1)^\sigma$  è la segnatura di  $\sigma$ . Continuano a valere le seguenti proprietà:

- (1) (Sviluppo di Laplace.) Se  $B^{ij}$  indica il determinante minore  $(n-1) \times (n-1)$  calcolato togliendo a  $B$  la  $i$ -esima riga e la  $j$ -esima colonna, allora valgono le formule

$$\det(B) = \sum_{j=1}^n (-1)^{h+j} B^{hj} b_{hj} = \sum_{i=1}^n b_{ih} (-1)^{i+h} B^{ih}, \quad \text{per ogni } h = 1, \dots, n.$$

$$\sum_{j=1}^n b_{kj} (-1)^{h+j} B^{hj} = \sum_{i=1}^n (-1)^{i+h} B^{ih} b_{ik} = 0, \quad \text{se } h \neq k.$$

- (2) Moltiplicando una riga od una colonna di  $B$  per un elemento  $a \in A$ , anche  $\det(B)$  viene moltiplicato per  $a$ .  
 (3) Il determinante  $\det(B)$  non cambia se ad una colonna viene aggiunto un multiplo di un'altra colonna. Lo stesso per le righe.  
 (4) Se la matrice  $B$  possiede due colonne uguali, allora  $\det(B) = 0$ .  
 (5) Vale il teorema di Binet, e cioè  $\det(AB) = \det(A) \det(B)$ .  
 (6) Se  $A$  è un anello graduato e  $b_{ij}$  è omogeneo di grado  $m + i - j$ , con  $m$  intero positivo fissato, allora  $\det(B)$  è omogeneo di grado  $nm$ . Infatti ciascun addendo  $b_{1\sigma(1)} \cdots b_{n\sigma(n)}$  ha grado  $nm + \sum_i i - \sum_i \sigma(i) = nm$ .

Denotiamo con  $\tilde{B} = (\tilde{b}_{ij})$  la matrice di coefficienti  $\tilde{b}_{ij} = (-1)^{i+j} B^{ji}$ . Se  $I$  indica la matrice identità, allora segue dallo sviluppo di Laplace che

$$B \cdot \tilde{B} = \tilde{B} \cdot B = \det(B) \cdot I \quad (\text{prodotto righe per colonne}).$$

La matrice  $\tilde{B}$  viene detta **matrice aggiunta** di  $B$ .

Consideriamo un polinomio  $f(x) = x^d + a_1 x^{d-1} + \cdots + a_d \in A[x]$  monico di grado  $d \geq 0$ .

Grazie al Lemma 9.2.4, per ogni  $g \in A[x]$  esistono e sono unici dei polinomi  $h_1, \dots, h_d \in A[x]$  ed una matrice  $(r_{ij}) \in M_{d,d}(A)$  a coefficienti in  $A$  tali che

$$(9.1) \quad x^{i-1}g = h_i f + \sum_{j=1}^d r_{ij} x^{j-1}, \quad i = 1, \dots, d.$$

Definiamo il **risultante** di  $f$  e  $g$  mediante la formula

$$R(f, g) = \det(r_{ij}) \in A.$$

LEMMA 9.5.1. Per ogni  $a \in A$  vale  $R(f, a) = a^d$ .

DIMOSTRAZIONE. Nelle notazioni di (9.1) si ha  $h_i = 0$  per ogni  $i$  e  $(r_{ij}) = aI$ .  $\square$

LEMMA 9.5.2. Nelle notazioni precedenti, esistono due polinomi  $\alpha, \beta \in A[x]$ , con  $\beta$  di grado  $< d$  tali che  $R(f, g) = \alpha f + \beta g$ . In particolare il risultante  $R(f, g)$  appartiene all'intersezione di  $A$  con l'ideale  $(f, g)$  generato da  $f$  e  $g$ .

DIMOSTRAZIONE. Denotiamo con  $(R^{ij}) \in M_{n,n}(A)$  l'aggiunta classica della matrice  $(r_{ij})$ , allora si ha  $(R^{ij})(r_{ij}) = \det(r_{ij})I$  e quindi in particolare

$$\sum_{i=1}^d R^{1i} r_{i1} = R(p, q), \quad \sum_{i=1}^d R^{1i} r_{ih} = 0, \quad 2 \leq h \leq d.$$

Ma allora

$$\sum_{i=1}^d R^{1i} (x^{i-1}g - h_i f) = \sum_{i=1}^d \sum_{j=1}^d R^{1i} r_{ij} x^{j-1} = R(f, g),$$

e basta considerare  $\alpha = -\sum_{i=1}^d R^{1i} h_i$  e  $\beta = \sum_{i=1}^d R^{1i} x^{i-1}$ .  $\square$

LEMMA 9.5.3. Se esiste un polinomio  $h \in A[x]$  di grado positivo che divide  $f$  e  $g$ , allora  $R(f, g) = 0$ .

DIMOSTRAZIONE. Siccome  $h$  divide  $f$  il suo coefficiente direttore divide 1 in  $A$  ed è quindi invertibile. In particolare ogni elemento non nullo dell'ideale principale  $(h) \subset A[x]$  è un polinomio di grado positivo e siccome  $R(f, g) \in (f, g) \subset (h)$  ne consegue che  $R(f, g) = 0$ .  $\square$

LEMMA 9.5.4. Se  $A$  è un dominio a fattorizzazione unica (ad esempio un campo) e  $R(f, g) = 0$ , allora  $f$  e  $g$  possiedono un fattore comune di grado positivo.

DIMOSTRAZIONE. Se  $R(f, g) = 0$ , allora esistono due polinomi  $\alpha, \beta \in A[x]$ , con  $\beta$  di grado  $< d$  tali che  $\alpha f + \beta g = 0$ . Siccome  $\deg(\beta) < \deg(f)$  deve esistere un fattore irriducibile di  $f$  che divide  $g$ .  $\square$

LEMMA 9.5.5. Sia  $\varphi: A \rightarrow B$  un omomorfismo di anelli ed estendiamolo nel modo naturale ad un omomorfismo di anelli

$$\varphi: A[x] \rightarrow B[x], \quad \varphi\left(\sum a_i x^i\right) = \sum \varphi(a_i) x^i.$$

Allora  $R(\varphi(f), \varphi(g)) = \varphi(R(f, g))$ .

DIMOSTRAZIONE. Basta osservare che ogni omomorfismo preserva le relazioni (9.1) e commuta con i determinanti.  $\square$

I lemmi precedenti descrivono solo una piccola parte delle molte proprietà del risultante, e sono tuttavia sufficienti per caratterizzare gli ideali primi dell'anello dei polinomi in una variabile a coefficienti in un campo.

PROPOSIZIONE 9.5.6. Sia  $\mathbb{K}$  un campo. Per un ideale proprio e non nullo  $0 \neq I \subset \mathbb{K}[x]$  le seguenti condizioni sono equivalenti:

- (1)  $I$  è massimale,
- (2)  $I$  è primo,
- (3)  $I$  è generato da un polinomio irriducibile di grado positivo.

DIMOSTRAZIONE. Che ogni ideale massimale è anche un ideale primo è una proprietà generale degli ideali, ben nota dai corsi base di algebra. Siccome  $\mathbb{K}[x]$  è un anello ad ideali principali, si ha  $I = (f)$  per qualche polinomio  $f$  non nullo (poiché  $I \neq 0$ ) e di grado positivo (poiché  $I \neq \mathbb{K}[x]$ ). Se  $f = gh$  con  $h, g$  di grado positivo, allora  $h, g \notin I$ , mentre  $hg \in I$  e questo prova che  $I$  non è primo.

Per concludere, supponiamo  $f$  polinomio irriducibile di grado positivo e sia  $J$  un ideale proprio che contiene  $(f)$ . Siccome ogni elemento non nullo di  $J$  ha grado  $> 0$ , per ogni  $g \in J$  si ha  $R(f, g) \in \mathbb{K} \cap (f, g) \subset \mathbb{K} \cap J = 0$  da cui segue che  $f$  divide  $g$ , ossia  $g \in (f)$ . □

### 9.6. Il teorema degli zeri di Hilbert

Sia  $\mathbb{K}$  un campo (infinito) fissato e  $\mathbb{A}^n \cong \mathbb{K}^n$  lo spazio affine su  $\mathbb{K}$  di dimensione  $n$ .

Il **luogo di zeri** di un sottoinsieme  $E \subset \mathbb{K}[x_1, \dots, x_n]$  è definito come

$$V(E) = \{(a_1, \dots, a_n) \in \mathbb{A}^n \mid f(a_1, \dots, a_n) = 0 \text{ per ogni } f \in E\}.$$

È chiaro dalla definizione che se  $E \subset F$  allora  $V(F) \subset V(E)$ . Osserviamo inoltre che se  $(E)$  è l'ideale generato da  $E$ , allora  $E$  ed  $(E)$  hanno lo stesso luogo di zeri, cioè  $V(E) = V((E))$ . Infatti  $E \subset (E)$  e quindi  $V((E)) \subset V(E)$ ; viceversa se  $p \in V(E)$  e  $g \in (E)$  si può scrivere  $g = a_1 f_1 + \dots + a_n f_n$  con  $a_i \in \mathbb{K}[x_1, \dots, x_n]$  e  $f_i \in E$  e quindi

$$f_i(p) = 0 \text{ per ogni } i \Rightarrow g(p) = \sum_i a_i(p) f_i(p) = 0.$$

Ne segue che non è restrittivo considerare esclusivamente luoghi di zeri di ideali di  $\mathbb{K}[x_1, \dots, x_n]$ .

DEFINIZIONE 9.6.1. Un sottoinsieme  $X \subset \mathbb{K}^n$  si dice **algebrico** se è  $X = V(I)$  per qualche ideale  $I \subset \mathbb{K}[x_1, \dots, x_n]$ .

L'immagine inversa di un insieme algebrico per un'applicazione lineare è ancora algebrico: sia  $A: \mathbb{K}^n \rightarrow \mathbb{K}^m$  un'applicazione lineare, definita da una matrice  $(a_{ij})$  e sia  $f \in \mathbb{K}[y_1, \dots, y_m]$ . Un punto  $p \in \mathbb{K}^n$  appartiene a  $A^{-1}(V(f))$  se e solo se  $f(Ap) = 0$  ossia se e solo se  $p \in V(fA)$  e basta osservare che  $fA$  è la funzione polinomiale associata al polinomio

$$g(x_1, \dots, x_n) = f\left(\sum_i a_{1i} x_i, \dots, \sum_i a_{mi} x_i\right).$$

Invece, gli insiemi algebrici non sono preservati dalle immagini dirette per applicazioni lineari. Si consideri ad esempio l'iperbole  $X \subset \mathbb{K}^2$  di equazione  $x_1 x_2 - 1 = 0$  e la proiezione  $\pi: \mathbb{K}^2 \rightarrow \mathbb{K}$  sulla prima coordinata; allora  $\pi(X) = \{x_1 \neq 0\}$  che non è un sottoinsieme algebrico (l'unico polinomio che si annulla su  $\mathbb{K} - \{0\}$  è quello nullo e quindi  $V(f) \supset \mathbb{K} - \{0\}$  se e solo se  $f = 0$ ). Come illustrato nel prossimo Teorema 9.6.2 il motivo di ciò consiste nel fatto che l'ideale generato da  $x_1 x_2 - 1$  non contiene polinomi monici rispetto a  $x_2$ .

TEOREMA 9.6.2 (di proiezione generica). *Siano  $\mathbb{K}$  un campo algebricamente chiuso e  $I \subset \mathbb{K}[x_1, \dots, x_n]$  un ideale che contiene un polinomio monico di grado positivo rispetto alla variabile  $x_n$ . Siano  $J = I \cap \mathbb{K}[x_1, \dots, x_{n-1}]$  e  $\pi: \mathbb{K}^n \rightarrow \mathbb{K}^{n-1}$  la proiezione sulle prime  $n-1$  coordinate.<sup>1</sup>*

*Allora l'applicazione  $\pi: V(I) \rightarrow V(J)$  è ben definita e surgettiva.*

DIMOSTRAZIONE. Siccome  $J \subset I$  si ha  $\pi(V(I)) \subset V(J)$  e pertanto l'applicazione  $\pi: V(I) \rightarrow V(J)$  è ben definita. Sia  $(a_1, \dots, a_{n-1}) \in V(J)$  e consideriamo l'omomorfismo surgettivo di anelli

$$\epsilon: \mathbb{K}[x_1, \dots, x_n] \rightarrow \mathbb{K}[x], \quad \epsilon(p) = p(a_1, \dots, a_{n-1}, x).$$

Dato che  $\epsilon$  è surgettivo l'immagine  $\epsilon(I)$  è un ideale; dato che  $\mathbb{K}[x]$  è un dominio ad ideali principali si ha  $\epsilon(I) = (h)$  con  $h = 0$  oppure polinomio monico di grado  $d \geq 0$ .

<sup>1</sup>Stiamo considerando  $\mathbb{K}[x_1, \dots, x_{n-1}]$  come un sottoanello di  $\mathbb{K}[x_1, \dots, x_n]$ .

Mostriamo che l'ipotesi  $h$  monico di grado 0, ossia  $h = 1$  conduce ad una contraddizione. Se così fosse esisterebbe  $g \in I$  tale che  $\epsilon(g) = 1$ . Usiamo adesso l'ipotesi che  $I$  contiene un polinomio  $f$  monico di grado positivo rispetto a  $x_n$  e consideriamo il risultante  $R(f, g)$  (a tal fine si considera  $\mathbb{K}[x_1, \dots, x_n] = A[x_n]$  dove  $A = \mathbb{K}[x_1, \dots, x_{n-1}]$ ). Per le proprietà del risultante  $R(f, g) \in (f, g) \cap A \subset J$  e quindi, siccome  $(a_1, \dots, a_{n-1}) \in V(J)$  si ha  $\epsilon(R(f, g)) = 0$ . D'altra parte  $\epsilon(R(f, g)) = R(\epsilon(f), \epsilon(g)) = R(\epsilon(f), 1) = 1$  dato che anche  $\epsilon(f)$  è monico.

Dunque  $h = 0$  oppure  $h$  ha grado positivo: in entrambi i casi esiste  $a_n \in \mathbb{K}$  tale che  $h(a_n) = 0$ , da cui  $\epsilon(q)(a_n) = q(a_1, \dots, a_n) = 0$  per ogni  $q \in I$ , ossia  $(a_1, \dots, a_n) \in V(I)$ .  $\square$

LEMMA 9.6.3 (di preparazione). *Siano  $\mathbb{K}$  un campo infinito e  $f \in \mathbb{K}[x_1, \dots, x_n]$  un polinomio non nullo di grado  $d \geq 0$ . Allora esiste un cambio lineare di coordinate  $x_i = \sum a_{ij}y_j$  ed una costante  $c \in \mathbb{K}$  tale che il polinomio  $cf$  è monico di grado  $d$  rispetto alla variabile  $y_n$ .*

DIMOSTRAZIONE. Sia  $f_d$  la componente omogenea di grado  $d$  di  $f$ . Per il Lemma 8.2.1 esiste un punto  $a \in \mathbb{K}^n$  tale che  $f_d(a) \neq 0$ ; scegliamo un sistema di coordinate  $y_1, \dots, y_n$  tale che il punto  $a$  corrisponda a  $(0, 0, \dots, 0, 1)$ . Nel nuovo sistema di coordinate si ha  $f_d(0, \dots, 0, y_n) = f_d(a)y_n^d$ , dunque il polinomio  $f(0, \dots, 0, y_n)$  ha grado  $d$  e basta quindi prendere come costante  $c = 1/f_d(a)$ .  $\square$

COROLLARIO 9.6.4 (Forma debole del Teorema degli zeri di Hilbert). *Siano  $\mathbb{K}$  un campo algebricamente chiuso e  $I \subset \mathbb{K}[x_1, \dots, x_n]$  un ideale proprio. Allora  $V(I) \neq \emptyset$ .*

DIMOSTRAZIONE. Prima di procedere alla dimostrazione mostriamo che entrambe le ipotesi sul campo e sull'ideale sono necessarie. Se l'ideale  $I$  non è proprio, allora  $1 \in I$  e di conseguenza  $V(I) \subset V(1) = \emptyset$ . Se il campo  $\mathbb{K}$  non è algebricamente chiuso esiste un polinomio di grado positivo  $f \in \mathbb{K}[x]$  tale che  $V(f) = \emptyset$ , mentre l'ideale  $(f)$  è proprio.

Dimostriamo il teorema per induzione su  $n$ , essendo il caso  $n = 0$  banalmente verificato. Supponiamo quindi vero il teorema per polinomi in  $n - 1$  variabili. L'enunciato è inoltre ovvio se  $I = 0$ ; assumiamo quindi  $I \neq 0$ , allora per il lemma di preparazione, a meno di automorfismi lineari di  $\mathbb{K}^n$ , possiamo supporre che esista  $f \in I$  polinomio monico rispetto alla variabile  $x_n$ .

Consideriamo l'intersezione  $J = I \cap \mathbb{K}[x_1, \dots, x_{n-1}]$ , siccome  $1 \notin J$  per l'ipotesi induttiva  $\emptyset \neq V(J) \subset \mathbb{K}^{n-1}$  mentre per il teorema di proiezione generica esiste un'applicazione surgettiva  $V(I) \rightarrow V(J)$ .  $\square$

Riepilogando, abbiamo definito un'applicazione

$$V: \{\text{ideali di } \mathbb{K}[x_1, \dots, x_n]\} \rightarrow \{\text{sottoinsiemi algebrici di } \mathbb{K}^n\}$$

che è surgettiva per definizione ma si guarda bene dall'essere iniettiva per ogni  $n > 0$ . Ad esempio gli ideali  $(x_1)$  ed  $(x_1^2)$  sono distinti ma definiscono lo stesso luogo di zeri.

Vogliamo adesso andare nella direzione opposta e definire un'applicazione iniettiva

$$I: \{\text{sottoinsiemi algebrici di } \mathbb{K}^n\} \rightarrow \{\text{ideali di } \mathbb{K}[x_1, \dots, x_n]\}$$

con l'ulteriore proprietà di essere un'inversa destra di  $V$ , ossia  $VI = Id$ .

Più in generale, dato un qualsiasi sottoinsieme  $X \subset \mathbb{K}^n$ , si definisce

$$I(X) = \{f \in \mathbb{K}[x_1, \dots, x_n] \mid f(a) = 0 \text{ per ogni } a \in X\}.$$

Segue immediatamente dalle definizioni di  $I$  e  $V$  che per ogni sottoinsieme  $X \subset \mathbb{K}^n$  si ha  $X \subset V(I(X))$  e che per ogni ideale  $J \subset \mathbb{K}[x_1, \dots, x_n]$  vale  $J \subset I(V(J))$ .

LEMMA 9.6.5. *Nelle notazioni precedenti, per ogni sottoinsieme algebrico  $X \subset \mathbb{K}^n$  vale  $V(I(X)) = X$ .*

DIMOSTRAZIONE. Sia  $J \subset \mathbb{K}[x_1, \dots, x_n]$  un ideale tale che  $V(J) = X$ . Si hanno due ovvie inclusioni  $X \subset V(I(X))$  e  $J \subset I(X)$ , che derivano direttamente dalle definizioni degli operatori  $V$  ed  $I$ . Applicando  $V$  alla seconda inclusione si ottiene  $V(I(X)) \subset V(J) = X$  che assieme alla prima fornisce l'uguaglianza  $X = V(I(X))$ .  $\square$

L'applicazione  $I$  soddisfa inoltre le seguenti proprietà:

$$(1) \quad I(\emptyset) = \mathbb{K}[x_1, \dots, x_n] \text{ e } I(\mathbb{K}^n) = 0;$$

- (2) Se  $X \subset Y$ , allora  $I(Y) \subset I(X)$ ;  
 (3) Per ogni sottoinsieme  $X \subset \mathbb{K}^n$  l'ideale  $I(X)$  è radicale, ossia  $I(X) = \sqrt{I(X)}$ ;  
 (4) Per ogni ideale  $J \subset \mathbb{K}[x_1, \dots, x_n]$ , vale  $\sqrt{J} \subset I(V(J))$ .

L'inclusione del punto 4) è in generale propria: ad esempio, se  $\mathbb{K} = \mathbb{R}$ ,  $n = 1$  e  $J = (x^2 + 1)$ , allora  $V(J) = \emptyset$  e  $I(V(J)) = \mathbb{R}[x] \neq \sqrt{J}$ .

**COROLLARIO 9.6.6.** *Sia  $\mathbb{K}$  un campo algebricamente chiuso, allora gli ideali massimali di  $\mathbb{K}[x_1, \dots, x_n]$  sono tutti e soli gli ideali del tipo  $I(p)$ , al variare di  $p \in \mathbb{K}^n$ . Esiste dunque una bigezione naturale fra  $\mathbb{K}^n$  e l'insieme degli ideali massimali di  $\mathbb{K}[x_1, \dots, x_n]$ .*

**DIMOSTRAZIONE.** Sia  $\mathfrak{m} \subset \mathbb{K}[x_1, \dots, x_n]$  un ideale massimale e usiamo la forma debole del teorema degli zeri di Hilbert per dedurre che  $V(\mathfrak{m}) \neq \emptyset$ . Dato un qualunque punto  $p \in V(\mathfrak{m})$  vale allora  $\mathfrak{m} \subset I(p)$  da cui segue  $\mathfrak{m} = I(p)$  e quindi  $V(\mathfrak{m}) = VI(p) = \{p\}$  per il Lemma 9.6.5.

Viceversa se  $p \in \mathbb{K}^n$  e  $I(p) \subset \mathfrak{m}$ , con  $\mathfrak{m}$  massimale, allora esiste  $q \in \mathbb{K}^n$  tale che  $I(p) \subset \mathfrak{m} = I(q)$ , da cui  $\{q\} = V(I(q)) \subset V(I(p)) = \{p\}$  e quindi  $p = q$ .  $\square$

**TEOREMA 9.6.7** (degli zeri di Hilbert (1892)). *Se il campo  $\mathbb{K}$  è algebricamente chiuso, allora per ogni ideale  $J \subset \mathbb{K}[x_1, \dots, x_n]$  vale  $\sqrt{J} = I(V(J))$ .*

**DIMOSTRAZIONE.** Segue immediatamente dalle definizioni che  $\sqrt{J} \subset I(V(J))$ . Sia quindi  $f \in I(V(J))$  e denotiamo con  $F$  la classe di  $f$  nell'anello quoziente  $A = \mathbb{K}[x_1, \dots, x_n]/J$ . Vogliamo dimostrare che  $f^n \in J$ , o equivalentemente che  $F^n = 0$ , per qualche  $n > 0$ . Per il Lemma 9.2.1 tale condizione è equivalente all'invertibilità di  $1 - tF$  nell'anello  $A[t]$ . Denotiamo con  $\pi: \mathbb{K}[x_1, \dots, x_n, t] \rightarrow A[t]$  l'omomorfismo surgettivo tale che  $\pi(t) = t$  e  $\pi: \mathbb{K}[x_1, \dots, x_n] \rightarrow A$  è la proiezione al quoziente.

Si consideri adesso l'ideale  $H \subset \mathbb{K}[x_1, \dots, x_n, t]$  generato da  $J$  e  $1 - tf$  e si osservi che  $Z(H) = \emptyset$ . Infatti se per assurdo esiste  $(a_1, \dots, a_n, b) \in V(H)$ , allora  $g(a_1, \dots, a_n) = 0$  per ogni  $g \in J$  e quindi  $(a_1, \dots, a_n) \in V(J)$ ; dato che  $f \in I(V(J))$  si ha dunque  $f(a_1, \dots, a_n) = 0$  e quindi  $1 - bf(a_1, \dots, a_n) = 1$  in contraddizione con  $1 - tf \in H$ .

Dunque per la forma debole del teorema degli zeri l'ideale  $H$  non è proprio; a maggior ragione l'ideale  $\pi(H)$  nell'anello quoziente  $A[t]$  contiene 1. Siccome  $\pi(J) = 0$  si ha  $A[t] = \pi(H) = (1 - tF)$  e quindi  $1 - tF$  è invertibile.  $\square$

**COROLLARIO 9.6.8.** *Supponiamo  $\mathbb{K}$  algebricamente chiuso e siano  $f, g \in \mathbb{K}[x_1, \dots, x_n]$  con  $f$  irriducibile. Se  $V(f) \subset V(g)$ , allora  $f$  divide  $g$ .*

**DIMOSTRAZIONE.** Se  $f$  divide  $g$ , diciamo  $g = fh$ , allora  $V(f) \subset V(f) \cup V(h) = V(g)$ . Viceversa, se  $V(f) \subset V(g)$  allora  $g$  si annulla in ogni punto di  $V(f)$ , ossia  $g \in I(V(f))$ . Dunque per il teorema degli zeri vale  $g \in I(V(f)) = \sqrt{(f)}$ , ossia  $g^m \in (f)$  per qualche  $m > 0$ . Dunque  $f$  divide una potenza di  $g$  e siccome  $f$  è irriducibile ne segue che  $f$  divide  $g$ .  $\square$

L'enunciato del Corollario 9.6.8 è quasi identico al teorema degli zeri per le ipersuperfici 8.3.6, con la sottile differenza che i luoghi di zeri sono nello spazio affine, mentre in 8.3.6 sono nello spazio proiettivo. Tuttavia il Teorema 8.3.6 segue facilmente dal Corollario 9.6.8 e dalla seguente semplice osservazione: per evitare ambiguità, per ogni polinomio omogeneo  $f \in \mathbb{K}[x_0, \dots, x_n]$  denotiamo

$$V(f) = \{x \in \mathbb{K}^{n+1} \mid f(x) = 0\}, \quad [V(f)] = \{[x] \in \mathbb{P}^n \mid f(x) = 0\}.$$

Si noti che per un  $x \in \mathbb{K}^{n+1} - \{0\}$  vale  $x \in V(f)$  se e solo se  $[x] \in [V(f)]$ . Dati  $f, g \in \mathbb{K}[x_0, \dots, x_n]$  polinomi omogenei di grado positivo, allora  $0 \in V(g)$  e quindi se  $[V(f)] \subset [V(g)]$  allora  $V(f) \subset V(g)$ .

Ricordiamo che un ideale  $J \subset \mathbb{K}[x_1, \dots, x_n]$  si dice omogeneo se è generato da polinomi omogenei; se  $S_d \subset \mathbb{K}[x_1, \dots, x_n]$  denota il sottospazio vettoriale dei polinomi omogenei di grado  $d$  si verifica facilmente che  $J$  è omogeneo se e solo se  $J = \bigoplus (J \cap S_d)$ . Sia infine  $0 = (0, \dots, 0) \in \mathbb{K}^n$ ; notiamo che se  $J$  è omogeneo e  $V(J) \neq \emptyset$ , allora  $0 \in V(J)$ .

**COROLLARIO 9.6.9** (Teorema degli zeri omogeneo). *Se il campo  $\mathbb{K}$  è algebricamente chiuso e  $J \subset \mathbb{K}[x_1, \dots, x_n]$  è un ideale omogeneo proprio, allora  $V(J) = \{0\}$  se e solo se esiste  $d > 0$  tale che  $S_d \subset J$ .*

**DIMOSTRAZIONE.** Se  $S_d \subset J$ , allora per ogni  $i$  si ha  $x_i^d \in J$ , quindi  $x_i \in \sqrt{J}$  e perciò  $V(J) = V(\sqrt{J}) = \{0\}$ .

Viceversa, se  $V(J) = \{0\}$ , allora per il teorema degli zeri  $\sqrt{J} = I(\{0\}) = (x_1, \dots, x_n)$ . Esiste dunque  $d > 0$  tale che  $x_i^d \in J$  per ogni  $i$  e quindi  $S_{dn-n+1} \subset J$ .  $\square$

### Esercizi

**ESERCIZIO 66.** Sia  $Y \subset \mathbb{A}^3$  l'unione dei tre piani coordinati e  $X \subset \mathbb{A}^3$  l'unione dei tre assi coordinati. Provare che  $I(Y) = (xyz)$  e che  $I(X) = (xy, yz, zx)$ . (Sugg.: se  $f \in I(X)$  considerare  $f(x, y, z) - f(0, y, z) - f(x, 0, z) - f(x, y, 0)$ .)

**ESERCIZIO 67.** Dimostrare che ogni ideale primo di  $\mathbb{C}[x_1, \dots, x_n]$  è intersezione di ideali massimali.

**ESERCIZIO 68.** Sia  $F \subset L$  una estensione di campi e siano  $f_1, \dots, f_n \in F[x_1, \dots, x_n]$ . Usare il teorema di Rouché-Capelli per dimostrare che  $f_1, \dots, f_n$  generano un ideale proprio di  $F[x_1, \dots, x_n]$  se e solo se generano un ideale proprio di  $L[x_1, \dots, x_n]$ .

**ESERCIZIO 69.** Sia  $\mathbb{K} = \overline{F}$  una chiusura algebrica di un campo  $F$  e sia  $J \subset F[x_1, \dots, x_n]$  un ideale proprio e si denoti  $L = F[x_1, \dots, x_n]/J$ . Dimostrare che se l'anello  $L$  è un campo, allora  $L$  è isomorfo ad un sottocampo di  $\mathbb{K}$ , ossia  $L$  è una estensione algebrica di  $F$ . (Sugg.: applicare l'Esercizio 68 alla coppia  $F \subset \mathbb{K}$  ed usare la caratterizzazione degli ideali massimali di  $\mathbb{K}[x_1, \dots, x_n]$ .)

## Bibliografia

- [1] Bauer, U., Lesnick, M.: Persistence Diagrams as Diagrams: A Categorification of the Stability Theorem. arxiv:1610.10085. [110](#), [118](#)
- [2] Carlsson, G.: Topology and data. Bull. AMS Volume **46**, Number 2, 255-308 (2009). [99](#)
- [3] Deo, S.: Algebraic Topology, a Primer. Springer (2018). [78](#)
- [4] Dold, A.: Lectures on algebraic topology. Second edition, Springer, Berlin Heidelberg New York (1980). [78](#)
- [5] Edelsbrunner, H.: A short course in computational geometry and topology. [102](#)
- [6] Edelsbrunner, H., Harer, J.: Persistent Homology - a survey. Contemporary Mathematics **453**, pp. 257-282 (2008). [99](#)
- [7] Edelsbrunner, H., Morozov, D.: Persistent Homology: Theory and Practice. Proceedings of the European Congress of Mathematics, 2012, pp. 31-50. [99](#)
- [8] P.R. Halmos: Naive set theory. D. Van Nostrand Co. Princeton, N.J. (1960). [192](#)
- [9] Greenberg, M., Harper, J.: Algebraic Topology: A First Course. Addison-Wesley (1981). [78](#)
- [10] Hatcher, A.: Algebraic Topology. (2001). [78](#)
- [11] Hilton P.J., Stammbach U.: A Course in Homological Algebra. Second Edition, Springer (1997).
- [12] Nathan Jacobson: Basic Algebra, I. San Francisco (1974). [110](#)
- [13] Manetti, M.: Topologia, seconda edizione, Springer (2014) [12](#), [22](#)
- [14] Yuri I. Manin, Matilde Marcolli: Nori diagrams and persistent homology. arXiv:1901.10301. [118](#)
- [15] Müllner, D., Babu, A.: Python Mapper: An open-source toolchain for data exploration, analysis and visualization. <http://danifold.net/mapper> (2013). [97](#)
- [16] Oudot, S.Y.: Persistence Theory: From Quiver Representations to Data Analysis. Mathematical Surveys and Monographs Volume 209, American Mathematical Society Providence, Rhode Island (2015). [103](#), [120](#)
- [17] Paparozzi, V.: Omologia persistente applicata allo studio del connettoma. Tesi di Laurea in Matematica, Roma (2018). [101](#)
- [18] Singer, I.M., Thorpe, J.A.: Lecture notes on elementary topology and geometry. Scott, Foresman and Co., Glenview, Ill. (1967). [6](#)
- [19] Spanier, E.H.: Algebraic topology. McGraw-Hill (1966). [10](#), [11](#)
- [20] Ashley Suh, Mustafa Hajij, Bei Wang, Carlos Scheidegger, and Paul Rosen: Persistent Homology Guided Force-Directed Graph Layouts. arXiv:1712.05548 [101](#)
- [21] Vick, J.W.: Homology theory. Springer, Berlin Heidelberg New York (1994). [78](#)
- [22] Walker, R. J.: *Algebraic curves*. Princeton (1950). [173](#)
- [23] Weinberger, S.: What is Persistent Homology? Notices of the AMS, Volume **58**, Number 1, 36–39 (2011) [99](#)