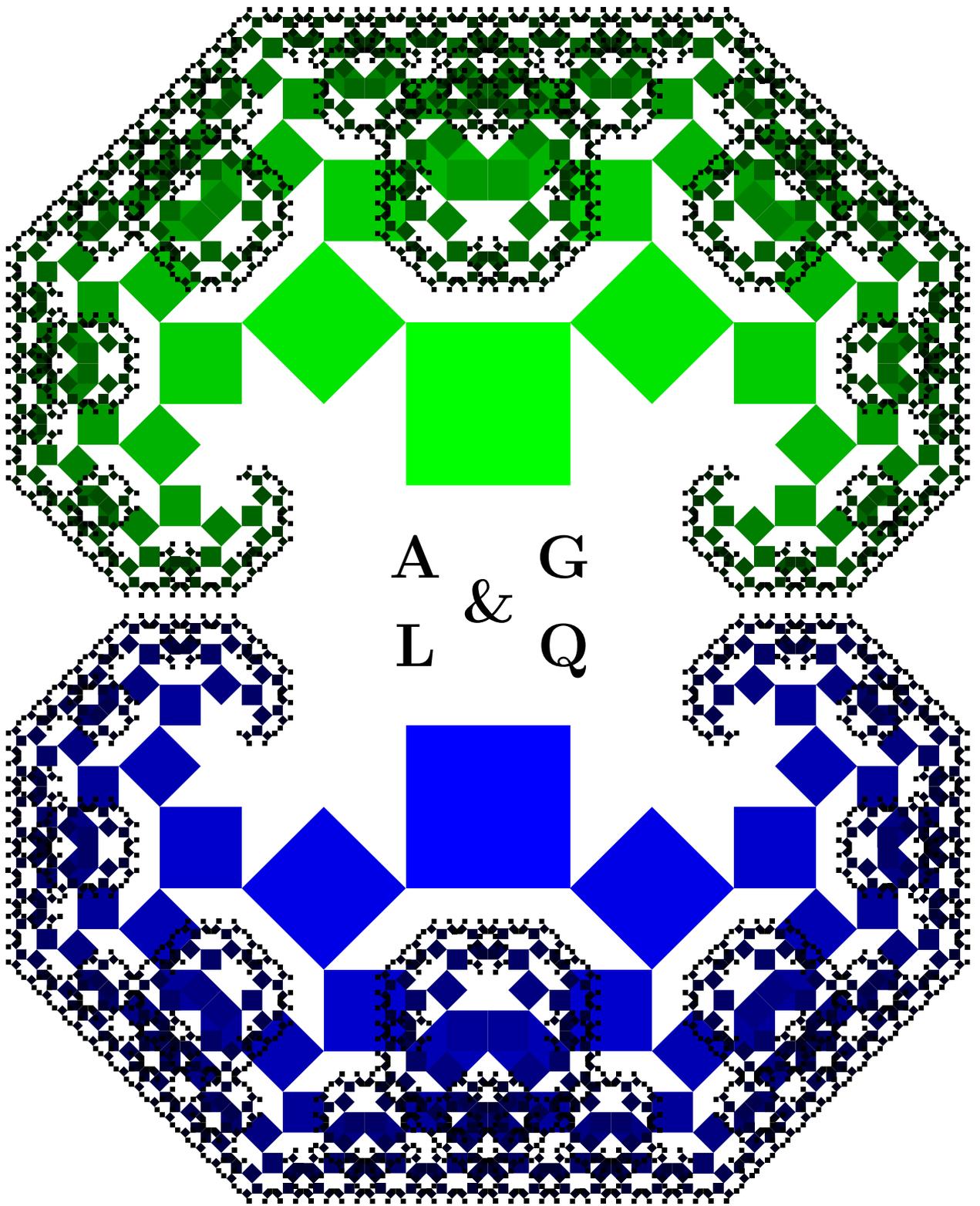


Maurizio Cailotto



*Algebra e Geometria
Lineari e Quadratiche*

Avvertenza. Questo testo è stato distribuito nel corso dell'anno accademico 2006/07 per i corsi di contenuto "geometrico" del primo anno del Corso di Laurea in Matematica dell'Università di Padova. Tuttavia il suo contenuto è notevolmente maggiore del programma effettivamente svolto, e alcuni paragrafi sono di difficile lettura per studenti del primo anno: essi sono stati indicati con ♠ e ♠♠ nel testo, a seconda del grado di difficoltà.

Al testo erano associati due Formulari (riassunto dei risultati principali) che si possono trovare nella parte didattica della mia home page <http://www.math.unipd.it/~maurizio/>.

Da dove viene e dove va questo testo. Essenzialmente non vi è nulla di originale, se non un lavoro di riordino di conoscenze classiche che deve molto a libri e appunti di I.Barsotti, F. Baldassarri, M. Candilera, G.Gerotto e a discussioni con V. Cristante e M. Candilera. Si tratta di un manuale di difficile lettura fuori del contesto di un corso universitario, e anche dentro, mi dicono.

Copyright. Tutti i diritti di questo testo sono riservati all'autore (incluse le eventuali edizioni parziali precedenti). Non ne è consentito alcun uso a scopi commerciali. Sono consentite la riproduzione e la circolazione in formato cartaceo o su supporto elettronico portatile ad esclusivo uso scientifico, didattico o documentario, purché il documento non venga alterato in alcun modo, ed in particolare mantenga le corrette indicazioni di data e fonte originale e la presente nota di copyright.

Note T_EXniche. Il testo è stato scritto in PlainT_EX, e i disegni presenti sono stati sviluppati in METAPOST. Siano ringraziati DEK e JDH. Le figure in copertina e controcopertina sono cespuglio e albero di Pitagora, frattali che si ottengono iterando semplici trasformazioni affini.

settembre 2006

Indice

Capitolo O. Strutture insiemistiche ed algebriche di base	1
1. Insiemi e funzioni.	1
2. Relazioni, equivalenze ed ordini.	6
3. Cardinalità e combinatorica.	10
4. Numeri Naturali e Induzione.	15
5. Permutazioni.	18
6. Numeri Interi.	21
7. Corpi numerici.	28
8. Polinomi.	35
9. Esercizi.	42
1. Esercizi su Insiemi, Funzioni e Relazioni.	42
2. Esercizi su Cardinali, Naturali, Combinatoria.	44
3. Esercizi su Interi, Divisione, MCD.	47
4. Esercizi su Complessi e Polinomi.	48
Capitolo I. Spazi Vettoriali	51
1. Definizione ed esempi fondamentali.	51
2. Sottospazi e quozienti.	53
3. Dipendenza e indipendenza lineari.	54
4. Basi e dimensione.	55
5. Coordinate.	58
6. Relazione di Grassmann.	60
7. Esercizi.	62
Capitolo II. Applicazioni Lineari e Matrici	65
1. Applicazioni lineari.	65
2. Matrici.	70
3. Matrici associate ad applicazioni lineari.	72
4. Dualità.	74
5. Esercizi.	77
1. Esercizi su Applicazioni Lineari.	77
2. Esercizi su Matrici.	78
Capitolo III. Sistemi Lineari	83
1. Sistemi Lineari.	83
2. Riduzione di Gauss.	86
3. Esercizi.	89
Capitolo IV. Determinanti	93
0. Motivazioni.	93
1. Determinanti e proprietà fondamentali.	94
2. Sviluppi di Laplace e matrici inverse.	96
3. Sviluppi pivotali.	98
4. Casi notevoli.	100
5. Rango e determinanti (minori).	107
6. Esercizi.	110

Capitolo V. Forme canoniche	115
1. Equivalenza di matrici.	115
2. Similitudine di matrici.	116
3. Autoteoria.	116
4. Teoria di Jordan.	122
5. Applicazioni.	127
6. Esercizi.	129
1. Esercizi su Autoteoria.	129
2. Esercizi su Jordan.	133
Capitolo VI. Geometria Affine	137
1. Spazi affini.	137
2. Calcolo baricentrico.	142
3. Trasformazioni affini e affinità.	144
4. Piano affine.	148
5. Spazio affine.	149
6. Spazi affini di dimensione quattro.	152
7. Esercizi.	152
Capitolo VII. Geometria Euclidea ed Hermitiana	157
1. Spazi Vettoriali Euclidei Reali.	157
2. Spazi Euclidei.	169
3. Trasformazioni Euclidee.	172
4. Piano euclideo.	173
5. Spazio euclideo.	174
6. Spazio euclideo di dimensione quattro.	176
7. Spazi Euclidei Complessi o Spazi Hermitiani.	176
8. Esercizi.	180
1. Esercizi su Spazi Vettoriali Euclidei.	180
2. Esercizi su Spazi Euclidei e Rigidità.	182
Capitolo VIII. Geometria Proiettiva	187
0. Motivazioni.	187
1. Spazi Proiettivi.	188
2. Alcuni modelli per gli spazi proiettivi.	192
3. Applicazioni proiettive e proiettività.	194
1. Definizioni ed esempi	195
2. Teoremi Fondamentali (della Geometria Proiettiva).	197
3. Collineazioni.	197
4. Teoria di Jordan delle proiettività.	198
4. Spazi Proiettivi, Spazi Affini e Spazi Euclidei.	203
5. Retta proiettiva e birapporti.	206
6. Piano proiettivo e costruzioni classiche.	208
7. Esercizi.	211
1. Esercizi su geometria proiettiva.	211
2. Esercizi su proiettività.	214
Capitolo IX. Forme Bilineari, Quadratiche ed Hermitiane	217
1. Forme Bilineari e Quadratiche.	217
2. Classificazioni.	221
3. Isometrie.	225
4. Forme Hermitiane e Teorema Spettrale.	225
5. Esercizi.	227

Capitolo X. Coniche e Quadriche	233
0. Introduzione.	233
1. Quadriche negli spazi proiettivi.	233
1. Definizioni.	233
2. Polarità.	235
3. Dualità.	236
4. Classificazione Proiettiva.	237
2. Quadriche negli spazi affini.	238
1. Definizioni.	238
2. Proprietà Affini.	238
3. Classificazione Affine.	238
3. Quadriche negli spazi euclidei reali.	239
1. Definizioni.	239
2. Classificazione Euclidea Reale.	240
3. Fuochi e proprietà focali.	240
4. Quadriche della retta.	241
5. Coniche (Quadriche del piano).	242
1. Proprietà proiettive.	242
2. Proprietà affini.	243
3. Proprietà Euclidee.	244
4. Sistemi lineari di Coniche.	246
6. Quadriche dello spazio.	248
1. Proprietà proiettive.	248
2. Proprietà affini.	249
3. Proprietà Euclidee.	250
7. Geometria (di Grassmann) delle rette dello spazio.	250
8. Esercizi.	254
1. Esercizi su Coniche.	254
2. Esercizi su Quadriche.	259
Capitolo XI. Geometria (dello spazio-tempo) di Minkowski	263
Capitolo XII. Geometria (piana) ellittica	271
Capitolo XIII. Geometria (piana) iperbolica	279
Appendice A. Esercizi per sviluppare l'Immaginazione.	289

Strutture insiemistiche ed algebriche di base

In questo capitolo introduttivo presenteremo alcune nozioni di base già note alla maggior parte degli studenti, ma lo faremo in una forma rigorosa che d'ora in poi deve diventare lo standard nello studio della Matematica. In effetti, la proprietà di linguaggio, la precisione delle definizioni e la chiarezza delle argomentazioni sono strumenti indispensabili per evitare errori ed ambiguità.

Vi sarà anche nel contesto l'occasione di approfondimenti o di sviluppare qualche nuovo concetto.

Nei primi due paragrafi daremo per note le nozioni di numeri interi e di operazioni tra essi; giustificheremo, almeno parzialmente, queste nozioni nei paragrafi successivi.

1. Insiemi e funzioni.

1.1. Diamo per note le nozioni di insieme e di elementi di un insieme, avendo solo cura di specificare che intenderemo fissato una volta per tutte un ambiente (detto Universo) in cui insiemi ed elementi vivono, sufficientemente grande da contenere tutte le costruzioni di cui avremo bisogno per ogni fissata teoria. Questo permette di evitare che nel linguaggio compaiano antinomie antipatiche, seppure poco significative, la più nota delle quali è la nozione dell'“insieme degli insiemi che non appartengono a se stessi” (il quale non può né appartenere, né non appartenere a se stesso). In effetti è la stessa nozione di “insieme di tutti gli insiemi” a generare tali antinomie, ed essa viene esclusa dal fatto di limitare a priori l'Universo di riferimento.

In generale indicheremo con lettere maiuscole quali A, B, C, X, Y, Z gli insiemi e con lettere minuscole quali a, b, c, x, y, z gli elementi. Talvolta le lettere saranno scritte con font diversi (e indicheranno diversi insiemi), talvolta addirittura useremo lettere greche o di altri sistemi di scrittura. Per esempio indicheremo con il simbolo \emptyset e chiameremo insieme vuoto quell'insieme che non contiene alcun elemento.

Per dire che un elemento a appartiene ad un insieme A scriveremo $a \in A$. Dunque $a \notin \emptyset$ per qualsiasi elemento a : una barra sul simbolo significa in generale la negazione del simbolo stesso; nel caso specifico: qualsiasi sia a , allora a non appartiene all'insieme vuoto.

Di solito usiamo le parentesi grafe per definire un insieme tramite la lista dei suoi elementi; per esempio scriveremo $\mathbf{3} = \{0, 1, 2\}$, e allora $1 \in \mathbf{3}$, ma $3 \notin \mathbf{3}$; si osservi che $\{\emptyset\}$ è un insieme non vuoto, contenente un unico elemento che è l'insieme vuoto: $\emptyset \in \{\emptyset\}$ (oltre che $\emptyset \subseteq \{\emptyset\}$, come vedremo subito, ma significa un'altra cosa).

1.2. DEFINIZIONE (SOTTINSIEMI). *Un insieme B si dice sottinsieme di un altro insieme A e si scrive $B \subseteq A$ se vale la seguente implicazione: per ogni elemento b , se b è elemento di B , allora b è elemento di A . Di solito si usa il simbolo \forall come quantificatore universale (“per ogni”), e il simbolo \implies per intendere l'implicazione (“allora”); quindi la frase precedente si potrà scrivere così: $\forall b, b \in B \implies b \in A$.*

1.2.1. Per esempio $\emptyset \subseteq A$ per ogni insieme A ; A stesso è sottinsieme di A per ogni A ; questi due sottinsiemi si dicono i sottinsiemi impropri di A . Se $B \subseteq A$ e $B \neq A$ (significa che esiste qualche elemento di A che non appartiene a B : usando il simbolo \exists di quantificazione esistenziale si scrive $\exists a \in A, a \notin B$), allora si scrive $B \subset A$, e si dice un sottinsieme proprio se non è vuoto.

1.2.2. Se $C \subseteq B$ e $B \subseteq A$, allora $C \subseteq A$, come si verifica subito.

1.2.3. Due insiemi si considerano uguali se e solo se sono formati dagli stessi elementi; dunque possiamo dire che $A = B$ se e solo se valgono contemporaneamente $A \subseteq B$ e $B \subseteq A$. Per dimostrare un'uguaglianza tra due insiemi converrà spesso dimostrare separatamente le due inclusioni.

1.2.4. Per ogni numero intero n , definiamo l'insieme $\mathbf{n} = \{0, 1, 2, \dots, n-1\}$ formato dai numeri naturali minori di n . Allora $\mathbf{n} \subseteq \mathbf{m}$ se e solo se $n \leq m$. Useremo spesso il simbolo \iff per intendere “se e solo se” (qualche volta abbreviato anche “sse”); quindi possiamo scrivere: $\mathbf{n} \subseteq \mathbf{m} \iff n \leq m$.

1.3. DEFINIZIONE (UNIONE). *Dati due insiemi A e B , l'insieme unione, indicato con $A \cup B$, è l'insieme formato dagli elementi che appartengono ad A oppure appartengono a B (o anche ad entrambi). In simboli:*

$$A \cup B = \{x \mid x \in A \text{ oppure } x \in B\}$$

ove il simbolo \mid si legge "tale che".

1.3.1. Si osservi che $A \subseteq A \cup B$, $B \subseteq A \cup B$ e che ogni altro insieme C contenente sia A che B contiene anche $A \cup B$; in altri termini, $A \cup B$ è il più piccolo insieme contenente sia A che B .

1.3.2. Per ogni tre insiemi A, B, C abbiamo che $(A \cup B) \cup C = A \cup (B \cup C)$, e dunque scriveremo unioni multiple senza specificare le parentesi (associatività). Inoltre abbiamo $A \cup B = B \cup A$ (commutatività), $A \cup A = A$ (idempotenza), $A \cup \emptyset = A$. Si osservi che $A \cup B = A$ se e solo se $B \subseteq A$.

1.3.3. UNIONI ARBITRARIE. Possiamo anche definire unioni di famiglie non necessariamente finite di insiemi nel modo seguente: se I è un insieme (detto spesso "di indici") e per ogni $i \in I$ è dato un insieme A_i , allora definiamo l'unione della famiglia come

$$\bigcup_{i \in I} A_i = \{x \mid \exists i \in I \text{ con } x \in A_i\} .$$

1.4. DEFINIZIONE (INTERSEZIONE). *Dati due insiemi A e B , l'insieme intersezione, indicato con $A \cap B$, è l'insieme formato dagli elementi che appartengono sia ad A sia a B . In simboli:*

$$A \cap B = \{x \mid x \in A \text{ e } x \in B\} .$$

1.4.1. Si osservi che $A \supseteq A \cap B$, $B \supseteq A \cap B$ e che ogni altro insieme C contenuto sia in A che in B è contenuto anche in $A \cap B$; in altri termini, $A \cap B$ è il più grande insieme contenuto sia in A che in B .

1.4.2. Per ogni tre insiemi A, B, C abbiamo che $(A \cap B) \cap C = A \cap (B \cap C)$, e dunque scriveremo unioni multiple senza specificare le parentesi (associatività). Inoltre abbiamo $A \cap B = B \cap A$ (commutatività), $A \cap A = A$ (idempotenza), $A \cap \emptyset = \emptyset$. Si osservi che $A \cap B = A$ se e solo se $A \subseteq B$.

1.4.3. INTERSEZIONI VUOTE. Due insiemi si dicono disgiunti se la loro intersezione è vuota; cioè se non hanno alcun elemento in comune.

1.4.4. INTERSEZIONI ARBITRARIE. Possiamo anche definire intersezioni di famiglie non necessariamente finite di insiemi nel modo seguente: se I è un insieme (detto spesso "di indici") e per ogni $i \in I$ è dato un insieme A_i , allora definiamo l'intersezione della famiglia come

$$\bigcap_{i \in I} A_i = \{x \mid \forall i \in I, x \in A_i\} .$$

Si osservi che tale intersezione risulta vuota se e solo se per ogni elemento x , esiste un indice i tale che $x \notin A_i$.

1.5. TEOREMA (LEGGI DISTRIBUTIVE). *Unioni finite ed intersezioni finite sono operazioni mutuamente distributive, cioè (espresse per il caso binario)*

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C) \quad \text{e} \quad A \cap (B \cup C) = (A \cap B) \cup (A \cap C) .$$

Più generalmente abbiamo

$$A \cup \left(\bigcap_{i \in I} A_i \right) = \bigcap_{i \in I} (A \cup A_i) \quad \text{e} \quad A \cap \left(\bigcup_{i \in I} A_i \right) = \bigcup_{i \in I} (A \cap A_i) .$$

DIMOSTRAZIONE. Dimostriamo per esempio la prima delle formule generalizzate, dimostrando separatamente le due inclusioni. Se $x \in A \cup \left(\bigcap_{i \in I} A_i \right)$ allora o $x \in A$ oppure $x \in \bigcap_{i \in I} A_i$ (cioè $x \in A_i$ per ogni i). In entrambi i casi abbiamo che $x \in A \cup A_i$ per ogni i , e dunque x appartiene all'intersezione di tutti. Viceversa, se $x \in \bigcap_{i \in I} (A \cup A_i)$, allora $x \in A \cup A_i$ per ogni i ; se $x \in A_i$ per ogni i allora $x \in \bigcap_{i \in I} A_i$, altrimenti vi è un j per cui $x \notin A_j$, ma poiché $x \in A \cup A_j$ si deve avere $x \in A$. Allora in entrambi i casi x deve appartenere all'unione di A con $\bigcap_{i \in I} A_i$ \square

1.6. DEFINIZIONE (COMPLEMENTO). *Dato un insieme A , il suo complemento (nel fissato Universo) è l'insieme degli oggetti che non appartengono ad A . Si indica con $\complement A$, oppure A^c (qualche*

volta \bar{A} , ma solo se si evitano confusioni con altre operazioni come la chiusura topologica). Dunque $x \in \complement A$ se e solo se $x \notin A$.

1.7. TEOREMA (LEGGI DI DE MORGAN). Le relazioni tra complementazione e le operazioni di unione ed intersezione sono date da

$$\complement(A \cap B) = (\complement A) \cup (\complement B) \quad \text{e} \quad \complement(A \cup B) = (\complement A) \cap (\complement B).$$

Più generalmente abbiamo

$$\complement\left(\bigcap_{i \in I} A_i\right) = \bigcup_{i \in I} \complement A_i \quad \text{e} \quad \complement\left(\bigcup_{i \in I} A_i\right) = \bigcap_{i \in I} \complement A_i.$$

DIMOSTRAZIONE. Mostriamo per esempio la prima delle formule generalizzate: $x \in \complement(\bigcap_{i \in I} A_i)$ vale se e solo se $x \notin \bigcap_{i \in I} A_i$, che vale se e solo se $x \notin A_j$ per qualche $j \in I$, dunque se solo se $x \in \complement A_j$ per qualche $j \in I$, e questo vale se e solo se $x \in \bigcup_{i \in I} \complement A_i$. Abbiamo così verificato che i due insiemi contengono esattamente gli stessi elementi. \square

1.8. DEFINIZIONE (PRODOTTO CARTESIANO). Dati due elementi x, y , diciamo coppia ordinata e scriviamo (x, y) la coppia formata dai due elementi dati nell'ordine scritto (x si dice il primo elemento della coppia, e y il secondo; potremmo formalizzare il concetto di coppia ordinata senza ricorrere a nuovi simboli dicendo che una coppia ordinata è un insieme della forma $\{x, \{x, y\}\}$); dunque $(x, y) = (a, b)$ se e solo se $x = a$ e $y = b$; in particolare $(x, y) \neq (y, x)$ (a meno che non sia $x = y$). Dati due insiemi A e B definiamo il loro prodotto cartesiano, indicato con $A \times B$ come l'insieme delle coppie ordinate il cui primo elemento sta in A , e il secondo in B . Dunque:

$$A \times B = \{(a, b) \mid a \in A, b \in B\}.$$

1.8.1. A rigor di termini, se abbiamo tre insiemi A, B e C , i prodotti $(A \times B) \times C$ e $A \times (B \times C)$ non sono proprio uguali, ma vedremo parlando di funzioni che essi sono canonicamente in biiezione, e quindi ci permetteremo di identificarli. Di conseguenza parleremo del prodotto cartesiano di più insiemi senza specificare (tramite parentesi) l'ordine in cui le operazioni sono svolte.

Scriveremo spesso A^2 invece di $A \times A$, e in generale A^n invece di $\underbrace{A \times \cdots \times A}_{n \text{ volte}}$.

1.8.2. Si osservi che $A \times \emptyset = \emptyset$, e viceversa, se $A \times B = \emptyset$, allora uno dei due insiemi tra A e B deve essere vuoto.

1.8.3. Vi sono facili relazioni tra le operazioni prima introdotte e il prodotto cartesiano: per esempio $A \times (B \cup C) = (A \times B) \cup (A \times C)$, e anche $A \times (B \cap C) = (A \times B) \cap (A \times C)$.

D'altra parte in generale vale solo che $(\complement A) \times (\complement B) \subseteq \complement(A \times B)$, l'inclusione nell'altro senso essendo in generale falsa.

1.9. DEFINIZIONE (DIFFERENZA). Dati due insiemi A e B definiamo la differenza $A \setminus B$ tra A e B come l'insieme degli elementi di A che non appartengono a B . Dunque

$$A \setminus B = \{x \in A \mid x \notin B\}$$

o equivalentemente $A \setminus B = A \cap \complement B$.

1.9.1. Evidentemente abbiamo che $A \setminus B$ è un sottinsieme di A disgiunto da B , ed è in effetti il più grande sottinsieme di A avente la proprietà di essere disgiunto da B .

Si osservi anche che $A \cup B$ è unione dei tre insiemi $A \setminus B$, $A \cap B$ e $B \setminus A$ che sono a due a due disgiunti.

1.9.2. La differenza possiede proprietà simili alla complementazione (che può essere vista come differenza tra l'Universo e un insieme); in particolare

$$A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C) = (A \setminus B) \setminus C;$$

$$(A \cup B) \setminus C = (A \setminus C) \cup (B \setminus C);$$

$$A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C);$$

$$(A \cap B) \setminus C = (A \setminus C) \cap (B \setminus C);$$

$$A \cup (B \setminus C) \supseteq (A \cup B) \setminus C \quad (\text{e vale l'uguaglianza sse } A \cap C = \emptyset);$$

$$A \cap (B \setminus C) = (A \cap B) \setminus C;$$

abbiamo l'inclusione $(A \setminus B) \times (A \setminus C) \subseteq (A \times A) \setminus (B \times C)$ (stretta in generale).

1.9.3. Vale anche che $\complement A \setminus \complement B = B \setminus A$ e $A \setminus \complement B = A \cap B$.

1.9.4. Si osservi inoltre che $A \setminus B = \emptyset$ sse $A \subseteq B$; $A \setminus B = A$ sse $A \cap B = \emptyset$; $A \setminus B = A \setminus C$ sse $A \cap B = A \cap C$; $A \setminus A = \emptyset$ e $A \setminus \emptyset = A$.

1.10. DEFINIZIONE (DIFFERENZA SIMMETRICA). *La differenza simmetrica $A \Delta B$ di A e B è definita come l'unione di $A \setminus B$ e $B \setminus A$; dalle osservazioni precedenti si vede subito che $A \Delta B = (A \cup B) \setminus (A \cap B)$*

1.10.1. Naturalmente $A \Delta B = B \Delta A$ (da cui l'aggettivo simmetrica), e $A \Delta B = \emptyset$ se e solo se $A = B$. Risultano inoltre le seguenti facili relazioni:

$$\begin{aligned} A \cap (B \Delta C) &= (A \cap B) \Delta (A \cap C), \\ A \Delta (B \Delta C) &= (A \Delta B) \Delta C, \\ A \Delta \complement B &= \complement(A \Delta B) = \complement A \Delta B; \\ \complement A \Delta \complement B &= A \Delta B. \end{aligned}$$

1.11. DEFINIZIONE (POTENZA O PARTI). *Dato un insieme A , l'insieme formato da tutti i sottinsiemi di A si dice parti di A o potenza di A e si indica con $\mathcal{P}(A)$ o $\mathbf{2}^A$; dunque*

$$\mathcal{P}(A) = \{B \mid B \subseteq A\}.$$

1.11.1. SINGOLETTI. Si osservi che $\mathcal{P}(A)$ contiene sempre \emptyset e A stesso, e dunque contiene sempre almeno due elementi se $A \neq \emptyset$; inoltre $\mathcal{P}(\emptyset) = \{\emptyset\}$.

Per ogni $a \in A$, abbiamo che $\{a\}$ (l'insieme contenente come unico elemento a) appartiene a $\mathcal{P}(A)$, $\{a\} \in \mathcal{P}(A)$, e gli insiemi di questo tipo si dicono i singoletti di A .

1.12. DEFINIZIONE (FUNZIONI). *Una funzione f di A in B , scritta $f : A \rightarrow B$ o $A \xrightarrow{f} B$, è una regola che ad ogni elemento a di A associa un unico elemento $f(a)$ di B . Si dice che A è il dominio e B il codominio di f . Vedremo in seguito che le funzioni di A in B si identificano ad opportuni sottinsiemi di $A \times B$ (il loro grafico). Se abbiamo due funzioni $f : A \rightarrow B$ e $g : B \rightarrow C$ in cui il dominio della seconda è il codominio della prima, allora possiamo definire una funzione detta composta $g \circ f : A \rightarrow C$ che manda $a \in A$ in $g(f(a)) \in C$ (spesso si indica $g \circ f$ semplicemente come gf).*

1.12.1. Talvolta l'insieme delle funzioni di A in B viene indicato con B^A .

1.12.2. (NON) COMMUTATIVITÀ. Si osservi che se abbiamo due funzioni componibili in entrambi i sensi, allora le due composizioni non sono necessariamente uguali: in generale $g \circ f \neq f \circ g$ per funzioni $f : A \rightarrow B$ e $g : B \rightarrow A$ anche se $A = B$ (farsi qualche esempio).

1.12.3. ASSOCIATIVITÀ. Se abbiamo una terza funzione $h : C \rightarrow D$ allora possiamo formare le composizioni di tre funzioni in due modi possibili, e i risultati coincidono: $h \circ (g \circ f) = (h \circ g) \circ f$ come funzione $A \rightarrow D$.

1.12.4. FUNZIONI IDENTITÀ. Per ogni insieme A esiste una funzione $A \rightarrow A$ detta identica che ad ogni elemento associa l'elemento stesso. Si scrive spesso id_A o 1_A . Per ogni funzione $f : A \rightarrow B$ abbiamo che $f \circ \text{id}_A = f$ e $\text{id}_B \circ f = f$.

1.12.5. Per ogni insieme A esiste una unica funzione $\emptyset \rightarrow A$ (infatti per definire una tale funzione non serve nulla), e per ogni singoletto $\{x\}$ esiste una unica funzione $A \rightarrow \{x\}$ (necessariamente tutti gli elementi di A sono mandati nell'unico elemento di $\{x\}$).

1.12.6. Una funzione $f : A \rightarrow B$ determina due altre funzioni, dette immagine diretta ed inversa tramite f .

L'immagine diretta è la funzione $f_* : \mathcal{P}(A) \rightarrow \mathcal{P}(B)$ (ma denotata di solito f per abuso di linguaggio) definita per ogni $X \in \mathcal{P}(A)$ (cioè $X \subseteq A$) da $f_*(X) = \{f(a) \mid a \in X\} \in \mathcal{P}(B)$ (si tratta del sottinsieme di B formato dalle immagini tramite f degli elementi di X). Si osservi che valgono le seguenti regole:

- (D1) $f_*(X \cup X') = f_*(X) \cup f_*(X')$ per ogni $X, X' \subseteq A$;
- (D2) $f_*(X \cap X') \subseteq f_*(X) \cap f_*(X')$ per ogni $X, X' \subseteq A$ (ma in generale questa inclusione è stretta);
- (D3) $f_*(\complement X)$ in generale non ha relazioni con $\complement f_*(X)$.

Di solito $f_*(A) \neq B$, e si dice l'immagine di f . Si costruiscano degli esempi per realizzare tutti i casi possibili.

L'immagine inversa tramite f è la funzione $f^* : \mathcal{P}(B) \rightarrow \mathcal{P}(A)$ definita per ogni $Y \in \mathcal{P}(B)$ (cioè $Y \subseteq B$) da $f^*(Y) = \{a \in A \mid f(a) \in Y\} \in \mathcal{P}(A)$ (si tratta del sottinsieme di A formato dagli elementi le cui immagini tramite f stanno in Y ; di solito si chiama antimagine di Y tramite f). Si osservi che valgono le seguenti regole:

- (I1) $f^*(Y \cup Y') = f^*(Y) \cup f^*(Y')$ per ogni $Y, Y' \subseteq B$;
- (I2) $f^*(Y \cap Y') = f^*(Y) \cap f^*(Y')$ per ogni $Y, Y' \subseteq B$;

(I3) $f^*(\mathbb{C}Y) = \mathbb{C}f^*(Y)$ per ogni $Y \subseteq B$.

Si osservi anche che $f^*(B) = A$. Si estendano le regole precedenti ai casi di unioni ed intersezioni arbitrarie.

Le composizioni di f_* e f^* danno luogo alle seguenti osservazioni:

(C1) $f^* \circ f_*(X) \supseteq X$ (e l'inclusione in generale è stretta);

(C2) $f_* \circ f^*(Y) \subseteq Y$ (e l'inclusione in generale è stretta, ma per un motivo ovvio: vale in generale che $f_* \circ f^*(Y) = Y \cap f(A)$).

Si consiglia ancora di costruirsi degli esempi per realizzare tutti i casi possibili.

1.12.7. Osserviamo infine le relazioni tra immagine diretta ed inversa e composizione di funzioni:

(IC) $f^*(\text{id}_A) = \text{id}_{\mathcal{P}(A)}$ e $(g \circ f)^* = f^* \circ g^*$ se $f : A \rightarrow B$ e $g : B \rightarrow C$ (si noti l'inversione nella composizione);

(DC) $f_*(\text{id}_A) = \text{id}_{\mathcal{P}(A)}$ e $(g \circ f)_* = g_* \circ f_*$ se $f : A \rightarrow B$ e $g : B \rightarrow C$.

1.12.8. DEFINIZIONE (FUNZIONI INIETTIVE, SURIETTIVE, BIETTIVE). Una funzione $f : A \rightarrow B$ si dice:

(I) iniettiva se vale la seguente implicazione: $f(a) = f(a') \implies a = a'$ per ogni $a, a' \in A$ (se due elementi di A hanno la stessa immagine in B , allora si tratta dello stesso elemento di A).

(S) suriettiva se vale la seguente condizione: per ogni $b \in B$ esiste $a \in A$ tale che $b = f(a)$ (ogni elemento di B è immagine di qualche elemento di A).

(B) biiettiva se è iniettiva e suriettiva, cioè se per ogni elemento $b \in B$ esiste un unico elemento $a \in A$ tale che $f(a) = b$.

1.12.9. In termini della funzione immagine inversa possiamo dire che una mappa è iniettiva se e solo se l'antimmagine di ogni singoletto di B contiene al più un elemento di A ; è suriettiva se e solo se l'antimmagine di ogni singoletto di B non è vuota; e dunque è biiettiva se e solo se l'antimmagine di ogni singoletto di B è un singoletto di A .

In termini della funzione immagine diretta possiamo dire che una mappa è suriettiva se e solo se la sua immagine è tutto il codominio.

1.12.10. Che relazioni vi sono tra iniettività, suriettività e biiettività per f e le analoghe condizioni per le funzioni f_* e f^* ?

1.12.11. Anticipando per il momento la nozione di insieme finito, una facile ma importante osservazione è la seguente: se A è un insieme finito, allora per le funzioni di A in sè le nozioni di essere iniettiva, suriettiva e biiettiva sono tutte tra loro equivalenti.

1.12.12. TEOREMA (INVERTIBILITÀ DELLE FUNZIONI). Valgono le seguenti equivalenze per una funzione $f : A \rightarrow B$:

(I) la funzione è iniettiva se e solo se esiste una funzione $g : B \rightarrow A$ tale che $g \circ f = \text{id}_A$ (una tale f si dice invertibile a sinistra, e g si dice una inversa sinistra per f ; dunque f è iniettiva se e solo se è invertibile a sinistra);

(S) la funzione è suriettiva se e solo se esiste una funzione $h : B \rightarrow A$ tale che $f \circ h = \text{id}_B$ (una tale f si dice invertibile a destra, e h si dice una inversa destra per f ; dunque f è suriettiva se e solo se è invertibile a destra);

(B) la funzione è biiettiva se e solo se esiste una funzione $g : B \rightarrow A$ tale che $g \circ f = \text{id}_A$ e $f \circ g = \text{id}_B$ (una tale f si dice invertibile, e g si dice una inversa per f , e si scrive di solito f^{-1} ; dunque f è biiettiva se e solo se è invertibile).

DIMOSTRAZIONE. La prima e la terza affermazione sono facilmente dimostrabili; la seconda affermazione invece non è ovvia, e una dimostrazione rigorosa richiede (e anzi è equivalente) all'assioma della scelta, che vedremo tra qualche pagina. \square

1.12.13. Si osservi che le eventuali inverse destre e sinistre per una funzione non sono uniche, a meno che la funzione stessa non sia invertibile sia a destra che a sinistra: in tal caso esiste un'unica inversa destra, un'unica inversa sinistra ed esse coincidono, come mostra la serie di uguaglianze

$$g = g \circ \text{id}_B = g \circ (f \circ h) = (g \circ f) \circ h = \text{id}_A \circ h = h$$

se $\text{id}_B = f \circ h$ e $g \circ f = \text{id}_A$.

1.12.14. Una funzione $f : A \rightarrow B$ è iniettiva se e solo se gode della seguente proprietà "di cancellazione a sinistra": per ogni coppia $g_1, g_2 : C \rightarrow A$ di funzioni tali che $f \circ g_1 = f \circ g_2$ allora $g_1 = g_2$.

Una funzione $f : A \rightarrow B$ è suriettiva se e solo se gode della seguente proprietà “di cancellazione a destra”: per ogni coppia $g_1, g_2 : B \rightarrow C$ di funzioni tali che $g_1 \circ f = g_2 \circ f$ allora $g_1 = g_2$.

1.12.15. INCLUSIONI COME FUNZIONI. Per ogni insieme A ed ogni suo sottinsieme B , la regola che ad ogni $b \in B$ associa $b \in A$ è una funzione iniettiva $i_B^A : B \rightarrow A$ che si dice l’inclusione di B in A ; essa è suriettiva (e allora una biiezione) se e solo se $A = B$. Se abbiamo $C \subseteq B \subseteq A$ allora risulta $i_B^A \circ i_C^B = i_C^A$.

1.12.16. COMPOSIZIONI E PROPRIETÀ DELLE FUNZIONI. Si verifica facilmente che la composizione di funzioni iniettive (risp. suriettive, risp. biietive) mantiene la stessa proprietà.

Valgono i seguenti risultati (converse parziali): se una composizione è iniettiva (risp. suriettiva) allora la prima funzione è iniettiva (risp. la seconda funzione è suriettiva); in particolare se una composizione è biietiva, allora la prima funzione è iniettiva e la seconda funzione è suriettiva, ma nessuna delle due è in generale biietiva.

1.12.17. GRAFICO. Una funzione $f : A \rightarrow B$ definisce un sottinsieme di $A \times B$, detto il suo grafico, dato da

$$\Gamma(f) = \{(a, f(a)) \mid a \in A\}$$

dotato della seguente proprietà: per ogni $a \in A$ esiste una ed una sola coppia in $\Gamma(f)$ il cui primo elemento sia a (tali sottinsiemi di $A \times B$ sono detti grafici). Viceversa ogni sottinsieme Γ di $A \times B$ che gode della proprietà detta è il grafico di una unica ben determinata funzione $f(\Gamma) : A \rightarrow B$.

Si verifichi che le funzioni che mandano f in $\Gamma(f)$ (dall’insieme delle funzioni di A in B nell’insieme dei grafici di $A \times B$) e Γ in $f(\Gamma)$ sopra definite sono biiezioni una inversa dell’altra.

Le proprietà di essere iniettiva, suriettiva, biietiva per una funzione si riconoscono dal suo grafico nel modo seguente: f è iniettiva se e solo se per ogni b esiste al più un a tale che $(a, b) \in \Gamma(f)$; f è suriettiva se e solo se per ogni b esiste almeno un a tale che $(a, b) \in \Gamma(f)$; f è biietiva se e solo se per ogni b esiste uno ed un solo a tale che $(a, b) \in \Gamma(f)$.

1.12.18. ALCUNE FUNZIONI CANONICHE NOTEVOLI. Spesso succede che tra due insiemi vi siano delle funzioni naturali, definite in modo intrinseco: tali funzioni si dicono canoniche; se si tratta di biiezioni, si dice che i due insiemi sono canonicamente in biiezione.

Per esempio abbiamo già accennato al caso del prodotto cartesiano: vi è una funzione naturale $A \times B \rightarrow B \times A$ che manda (a, b) in (b, a) (talvolta detta la simmetria), e che si verifica subito essere una biiezione.

Un altro esempio è dato dalla funzione $A \times (B \times C) \rightarrow (A \times B) \times C$ che manda $(a, (b, c))$ in $((a, b), c)$; anche in questo caso si vede subito che si tratta di una biiezione, che permette allora di identificare canonicamente i prodotti tripli (e perciò multipli).

Dato un insieme I e una famiglia di insiemi A_i indicata da $i \in I$, possiamo definire il prodotto della famiglia stessa, indicato come $\prod_{i \in I} A_i$, come l’insieme delle funzioni di I in $\bigcup_{i \in I} A_i$ tali che per ogni $i \in I$ la sua immagine appartenga ad A_i . Se $I = \{1, 2, \dots, n\}$ allora si scrive anche $\prod_{i \in I} A_i = \prod_{i=1}^n A_i = A_1 \times A_2 \times \dots \times A_n$. Nel caso che $I = \{1, 2\}$, questa definizione non è esattamente quella data parlando di prodotto cartesiano, ma si può facilmente vedere che si tratta di due definizioni equivalenti in modo canonico.

Dato un insieme A , vi è una biiezione naturale tra l’insieme potenza $\mathcal{P}(A)$ di A e l’insieme $\mathbf{2}^A$ delle funzioni di A in $\mathbf{2}$ che associa ad ogni sottinsieme B la cosiddetta funzione caratteristica di B che vale 1 su B e 0 su $A \setminus B$.

2. Relazioni, equivalenze ed ordini.

2.1. DEFINIZIONE (RELAZIONI). Una relazione è una terna (A, B, R) in cui A e B sono insiemi, e R è un sottinsieme del prodotto cartesiano $A \times B$; spesso si parla di relazione tra un insieme A ed un insieme B e si specifica semplicemente il terzo termine R . Se $(a, b) \in R$ si dice che a è in relazione con b secondo R , e si scrive anche aRb . Elenchiamo qualche importante definizione per relazioni tra un insieme e se stesso, insieme a delle caratterizzazioni su cui il lettore dovrebbe riflettere:

- (R) una relazione si dice riflessiva se per ogni $a \in A$ abbiamo aRa (ovvero $(a, a) \in R$, ovvero se R contiene la diagonale di $A \times A$);
- (S) una relazione si dice simmetrica se per ogni $a, b \in A$ abbiamo che aRb implica bRa (ovvero se $(a, b) \in R$, allora anche $(b, a) \in R$, ovvero se R è “simmetrico rispetto alla diagonale” come

- sottinsieme di $A \times A$);
- (A) una relazione si dice antisimmetrica se per ogni $a, b \in A$ abbiamo che aRb e bRa implicano $a = b$ (ovvero se $(a, b) \in R$ e $(b, a) \in R$, allora a e b sono lo stesso elemento, ovvero se R è “antisimmetrico rispetto alla diagonale” come sottinsieme di $A \times A$);
- (t) una relazione si dice transitiva se per ogni $a, b, c \in A$ abbiamo che aRb e bRc implicano aRc (ovvero se $(a, b) \in R$ e $(b, c) \in R$, allora anche $(a, c) \in R$; cosa significa questo in $A \times A$?);
- (T) una relazione si dice totale se per ogni $a, b \in A$ abbiamo che aRb oppure bRa sono veri (ovvero $(a, b) \in R$ oppure $(b, a) \in R$; cosa significa questo in $A \times A$?); si osservi che una relazione totale è certo riflessiva. Una relazione non totale si dice parziale.

2.1.1. Abbiamo già visto una importante classe di relazioni tra A e B costituita dai grafici di funzioni di A in B . Per abuso di linguaggio, una relazione soddisfacente alla condizione per essere un grafico (per ogni $a \in A$ esiste una ed una sola coppia nella relazione il cui primo elemento sia a) si dirà una funzione.

2.1.2. OPERAZIONI TRA RELAZIONI. Trattandosi di sottinsiemi di $A \times B$, le relazioni tra A e B sono soggette alle nozioni insiemistiche usuali; dunque possiamo parlare di inclusione tra relazioni, di unione, intersezione, differenza tra relazioni e così via.

Poiché alcune proprietà delle relazioni come la simmetria e la transitività sono stabili per intersezioni arbitrarie, ciò ci permette di parlare per ogni relazione R data della sua chiusura simmetrica o transitiva (la più piccola relazione simmetrica o transitiva contenente R , ovvero l'intersezione di tutte le relazioni simmetriche o transitive contenenti R).

2.1.3. COMPOSIZIONI TRA RELAZIONI. Analogamente alle funzioni, possiamo anche parlare di composizioni di relazioni nel modo seguente: se R è relazione di A con B e S è relazione di B con C , allora definiamo RS relazione di A con C tramite $a(RS)c$ se e solo se esiste $b \in B$ tale che aRb e bSc . La composizione tra relazioni, similmente a quella tra funzioni, è associativa ma non commutativa.

2.2. DEFINIZIONE (EQUIVALENZE). Una relazione R su un insieme A si dice di equivalenza se soddisfa alle proprietà riflessiva, simmetrica e transitiva. Di solito le relazioni di equivalenza si indicano con simboli quali \sim , \simeq , \cong , \approx . Se $a \in A$, indichiamo con $[a]_R$ oppure $[a]$ oppure \bar{a} (se R può essere sottintesa) e chiamiamo la classe di equivalenza di a modulo R il sottinsieme di A formato dagli elementi equivalenti ad a : $[a]_R = \{b \in A \mid aRb\}$.

Per ogni insieme A vi è una più piccola relazione di equivalenza (nel senso delle inclusioni in $A \times A$), ed è la relazione di identità (aRb se e solo se $a = b$; si tratta della diagonale $\{(a, a) \mid a \in A\}$ in $A \times A$). Vi è anche una massima relazione di equivalenza, quella per cui ogni elemento è in relazione con ogni altro; corrisponde a tutto l'insieme $A \times A$.

2.2.1. TEOREMA (PARTIZIONE ASSOCIATE). Data una relazione di equivalenza su un insieme A , l'insieme delle classi di equivalenza degli elementi di A formano una partizione di A (cioè le classi di equivalenza sono non vuote, a due a due disgiunte e la loro unione dà A), detta partizione associata alla relazione. Viceversa data una partizione di A esiste una unica relazione di equivalenza in A tale che la partizione associata sia quella data.

Perciò esiste una biiezione tra relazioni di equivalenza su un insieme e partizioni di quello stesso insieme.

DIMOSTRAZIONE. Che le classi di equivalenza per una relazione di equivalenza costituiscano una partizione di A si vede facilmente: ogni classe è non vuota (per la riflessività), le classi sono a due a due disgiunte (se due classi hanno un elemento in comune, allora, per la transitività e la simmetria, esse coincidono), l'unione dà tutto A (di nuovo per la riflessività). Ad ogni partizione di A associamo la relazione definita da $a \sim b$ se e solo se essi appartengono allo stesso insieme della partizione. Allora si verifica subito che si tratta di una relazione di equivalenza (la riflessività viene dal fatto che la riunione dei sottinsiemi della partizione dà tutto A , la simmetria viene dalla corrispondente proprietà dell'inclusione, e la transitività segue dalla condizione che i sottinsiemi della partizione sono a due a due disgiunti). Le due assegnazioni fatte (ad ogni equivalenza su A una partizione di A , e ad ogni partizione di A una relazione di equivalenza su A) danno luogo a due funzioni una inversa dell'altra (verificare). \square

2.2.2. DEFINIZIONE (INSIEMI QUOZIENTE). *L'insieme delle classi di equivalenza in A per una fissata relazione di equivalenza R su A si indica con A/R e si chiama l'insieme quoziente di A modulo R . Abbiamo che $[a]_R = [b]_R$ (in A/R) se e solo se aRb in A .*

2.2.3. PROIEZIONI. Esiste una funzione detta proiezione $p_R^A : A \rightarrow A/R$ che ad ogni $a \in A$ associa la sua classe di equivalenza $[a]_R \in A/R$; si tratta di una funzione suriettiva, ed è iniettiva se e solo se R è la relazione di identità. La proiezione gode della seguente proprietà di fattorizzazione: una qualsiasi funzione $f : A \rightarrow C$ si fattorizza come $f = g \circ p_R^A$ con $g : A/R \rightarrow C$ se e solo se vale l'implicazione: $aRa' \implies f(a) = f(a')$ (cioè se e solo se f è costante sulle classi di equivalenza modulo R).

2.2.4. TEOREMA (DI OMOMORFISMO PER INSIEMI). *Data una funzione $f : A \rightarrow B$, sia \sim la relazione su A definita da $a \sim a'$ se e solo se $f(a) = f(a')$. Allora \sim è una relazione di equivalenza ed esiste una unica funzione $\bar{f} : A/\sim \rightarrow B$ tale che $f = \bar{f} \circ p_{\sim}^A$. La funzione \bar{f} risulta iniettiva; inoltre risulta che f ed \bar{f} hanno la stessa immagine B' in B , e la funzione $\bar{f} : A/\sim \rightarrow B'$ è una biiezione.*

DIMOSTRAZIONE. Che \sim sia una relazione di equivalenza è facile. Per definizione la funzione f è costante sulle classi di equivalenza di \sim , dunque la fattorizzazione richiesta esiste (definita da $\bar{f}(\bar{a}) = f(a)$), ed è unica poiché la proiezione è suriettiva. La funzione \bar{f} è iniettiva poiché da $\bar{f}(\bar{a}) = \bar{f}(\bar{a}')$ segue $f(a) = f(a')$, e dunque $\bar{a} = \bar{a}'$ per definizione di \sim . Che le immagini di f ed \bar{f} coincidano è facile, e l'ultima affermazione è allora una conseguenza ovvia della iniettività di \bar{f} . \square

2.2.5. EQUIVALENZE GENERATE. L'intersezione (in $A \times A$) di una famiglia di relazioni di equivalenza è ancora una relazione di equivalenza; quindi dato un qualunque sottinsieme di $A \times A$ possiamo parlare della relazione di equivalenza su A da esso generata: si tratta della più piccola relazione di equivalenza che lo contiene, ovvero della intersezione di tutte le relazioni di equivalenza che lo contengono.

2.3. DEFINIZIONE (PREORDINI E ORDINI). *Una relazione R su un insieme A si dice un preordine se essa è transitiva; si dice un ordine se soddisfa alle proprietà riflessiva, antisimmetrica e transitiva. Di solito le relazioni di (pre)ordine si indicano con simboli quali $<, \leq, <, \preceq$. Un ordine si dice totale se lo è in quanto relazione, parziale altrimenti.*

2.3.1. Dati due insiemi ordinati A e B , una funzione $A \rightarrow B$ si dice ordinata o crescente se vale la seguente implicazione: per ogni $a, a' \in A$ da $a \leq a'$ (in A) segue che $f(a) \leq f(a')$ (in B). Viceversa la funzione si dice antiordinata o decrescente se per ogni $a, a' \in A$ da $a \leq a'$ (in A) segue che $f(a) \geq f(a')$ (in B). Una funzione si dice disordinata altrimenti, cioè se non è né crescente né decrescente.

Per ogni insieme ordinato A con relazione \leq possiamo costruire la relazione d'ordine trasposta \leq data da $a \leq a'$ se e solo se $a' \leq a$ (l'ordine viene "rovesciato"); allora una funzione antiordinata diventa una funzione ordinata dal dominio al codominio con l'ordine trasposto.

2.3.2. Ad ogni relazione R su A che sia riflessiva e transitiva (un preordine riflessivo) è associata una relazione d'equivalenza E definita da aEb se e solo se valgono aRb e bRa . Sull'insieme quoziente A/E la relazione R induce una relazione d'ordine parziale.

2.3.3. MINIMALI, MASSIMALI, MINIMO, MASSIMO. Se B è un sottinsieme di un insieme ordinato A , diciamo che $b \in B$ è elemento massimale (risp. minimale) di B se dalla relazione $b' \in B$ e $b \leq b'$ (risp. $b' \in B$ e $b' \leq b$) segue $b = b'$; si osservi che un insieme può avere più massimali (risp. minimali) distinti (necessariamente non confrontabili tra loro). Diciamo che $b \in B$ è elemento massimo (risp. minimo) di B se $b' \leq b$ (risp. $b \leq b'$) per ogni altro $b' \in B$; se b è massimo (risp. minimo) in B , allora è l'unico massimale (risp. minimale) di B ; il viceversa è falso? Se esiste il massimo (risp. il minimo) di A si dice l'ultimo (risp. il primo) elemento.

2.3.4. BUONI ORDINAMENTI. Un insieme si dice bene ordinato se ogni suo sottinsieme non vuoto ammette elemento minimo (di conseguenza l'ordine è totale).

2.3.5. MINORANTI E MAGGIORANTI. Se B è un sottinsieme di un insieme ordinato A , diciamo che $a \in A$ è maggiorante (risp. minorante) di B se vale la relazione $b \leq a$ (risp. $a \leq b$) per ogni $b \in B$.

2.3.6. ESTREMI INFERIORE E SUPERIORE. Se B è un sottinsieme di un insieme ordinato A , si dice estremo superiore (risp. inferiore) di B , se esiste, il minimo dei maggioranti (risp. il massimo dei minoranti).

♠ **2.3.7.** Vi sono altre fondamentali nozioni che riguardano gli ordinamenti: sottinsiemi limitati inferiormente e superiormente, segmenti iniziali, intervalli, catene, salti e lacune, densità, completezza e continuità ordinali, ecc. Queste nozioni sono alla base della definizione e di una possibile costruzione dei numeri reali, e saranno viste nel corso di Matematica Uno. Il lettore interessato può riferirsi per approfondimenti al testo “Appunti di Algebra” (lezioni 11-14, 26-31) di I. Barsotti, e anche all’App. B del testo “Analisi Uno” di G. De Marco.

♠ **2.3.8.** INSIEMI ORDINATI INDUTTIVI. Un insieme ordinato si dice induttivo se ogni sua catena (sottinsieme non vuoto in cui l’ordine indotto sia totale) ammette maggiorante. Si dice strettamente induttivo se ogni sua catena ammette estremo superiore. Vi è un importante e classico risultato riguardo a questo tipo di insiemi, che lega tra loro nozioni apparentemente indipendenti:

♠♠ **2.3.9.** TEOREMA. *Le seguenti asserzioni:*

- (Z) LEMMA DI ZORN: ogni insieme ordinato induttivo ammette massimali;
 - (Z') ogni insieme ordinato strettamente induttivo ammette massimali;
 - (S) ASSIOMA DELLA SCELTA: per ogni famiglia A_i , per $i \in I$, non vuota di insiemi non vuoti a due a due disgiunti, esiste un insieme S tale che $S \cap A_i$ è formato da un solo elemento per ogni i (in altri termini, possiamo scegliere un elemento in ogni insieme di una qualunque famiglia data; se la famiglia fosse finita non ci sarebbero problemi: ma se la famiglia è infinita il problema è “evidentemente” non banale);
 - (P) ASSIOMA DEL PRODOTTO: per ogni famiglia A_i , per $i \in I$, non vuota di insiemi non vuoti, il prodotto cartesiano $\prod_{i \in I} A_i$ è non vuoto, cioè esistono funzioni $f : I \rightarrow \bigcup_{i \in I} A_i$ tali che $f(i) \in A_i$ per ogni $i \in I$ (anche qui il problema è non banale per insiemi infiniti di indici);
 - (ID) la proprietà di esistenza di una inversa destra per ogni funzione suriettiva: se $f : A \rightarrow B$ è una funzione suriettiva, allora esiste una funzione $g : B \rightarrow A$ che ne è inversa a destra, cioè tale che $f \circ g = \text{id}_B$;
 - (BO) PRINCIPIO DEL BUON ORDINAMENTO: ogni insieme è bene ordinabile (cioè su ogni insieme si può definire una relazione d’ordine che sia un buon ordinamento);
- sono tutte tra loro equivalenti.

DIMOSTRAZIONE. Per vedere che (Z) e (Z') sono equivalenti, basta mostrare che (Z') implica (Z) (l'altra implicazione essendo ovvia). Sia allora A un insieme ordinato induttivo; consideriamo l'insieme A' di tutte le catene di A . Allora A' è ordinato dall'inclusione e risulta strettamente induttivo (l'estremo superiore di una catena di catene essendo l'unione delle catene stesse). Dunque in A' esistono elementi massimali, e un qualunque maggiorante in A di un massimale di A' è un massimale in A , dunque esistono massimali in A .

Che l'assioma (S) della scelta e quello (P) del prodotto siano equivalenti è facile, e lasciato al lettore. Essi implicano (ID) poiché per ogni funzione suriettiva $f : A \rightarrow B$, trovare una inversa destra si riduce a scegliere un elemento in ognuno dei sottinsiemi di A dati dalle antimmagini degli elementi di B . Viceversa, l'assioma del prodotto è dimostrato se è possibile scegliere una inversa destra della funzione $\bigcup_{i \in I} A_i \rightarrow I$ che ad ogni $a_i \in A_i$ associa i , che è ben definita perché gli insiemi sono disgiunti, ed evidentemente suriettiva poiché gli insiemi sono non vuoti. Quindi (ID) implica (P).

È anche facile dimostrare che il principio del buon ordinamento implica (S), (P) o (ID). Per dimostrare (ID) per esempio, basta infatti ben ordinare l'insieme A e per ogni $b \in B$ scegliere come $g(b)$ il minimo dell'antimmagine di b tramite f .

Vediamo che il lemma di Zorn implica (BO). Sia A un insieme qualsiasi e consideriamo l'insieme X formato dai sottinsiemi di A dotati di un buon ordine. Quest'insieme è non vuoto, poiché ogni singolo elemento di A gli appartiene (anzi ogni insieme finito di A dotato di un ordine totale gli appartiene). Ordiniamo X tramite l'ordine delle inclusioni crescenti: dunque un elemento di X è minore di un altro se il primo è incluso nel secondo e possiede l'ordine indotto dall'inclusione. Così ordinato, X è insieme induttivo (ogni catena in X ha come massimale l'unione dei suoi elementi), e quindi esiste elemento massimale in X , sia A' , dotato di un buon ordinamento, e supponiamo che sia $A' \neq A$. Allora esiste $a \in A$, ma $a \notin A'$, e il sottinsieme $A' \cup \{a\}$ ordinato usando a come minimo elemento contraddice la massimalità di A' in X . Dunque $A' = A$, e allora abbiamo un buon ordinamento su A .

Per esercizio far vedere che il lemma di Zorn implica (S), (P) e (ID) (direttamente, senza passare per (BO)).

La parte più impegnativa della dimostrazione è invece data dal fatto che il lemma di Zorn è implicato da una delle altre asserzioni (S), (P) o (ID); classicamente si dimostra che l'assioma della scelta implica (Z'), e per questo rimandiamo il lettore interessato al libro "Appunti di Algebra" (lezioni 15-16) di I. Barsotti. \square

3. Cardinalità e combinatorica.

In questo paragrafo daremo una definizione precisa della nozione intuitiva di "numerosità" di un insieme, vale a dire del "numero di elementi che lo compongono".

3.1. DEFINIZIONE (CARDINALITÀ, EQUIPOTENZA). Due insiemi A e B si dicono equipotenti (o aventi la stessa cardinalità) se esiste una biiezione di A in B . La collezione di tutti gli insiemi (dell'Universo fissato) equipotenti ad un fissato insieme A si dice una cardinalità, e si indica con $|A|$, $c(A)$, $\text{card}(A)$ o $\#A$ a seconda dei contesti.

3.2. OPERAZIONI TRA LE CARDINALITÀ. Possiamo definire tra le cardinalità alcune relazioni e operazioni analoghe a quelle ben note per i numeri naturali (che tra poco vedremo essere particolari cardinalità, quelle finite). Siano A e B due insiemi disgiunti;

(S) la somma delle due cardinalità $|A|$ e $|B|$ è la cardinalità dell'unione: $|A| + |B| = |A \cup B|$ (si presenta qui un problema generale: nella definizione abbiamo usato due specifici insiemi appartenenti a fissate cardinalità, e dobbiamo controllare che il risultato non dipenda dagli insiemi, ma solo dalla loro cardinalità; ovvero che scegliendo altri insiemi della stessa cardinalità il risultato della definizione non cambi);

(P) il prodotto delle due cardinalità $|A|$ e $|B|$ è la cardinalità del prodotto cartesiano: $|A| \cdot |B| = |A \times B|$

(E) l'elevamento a potenza della cardinalità $|A|$ alla cardinalità $|B|$ è la cardinalità dell'insieme delle funzioni di B in A : $|A|^{|B|} = |A^B|$.

Una cardinalità $|A|$ si dice minore o uguale ad una cardinalità $|B|$ e si scrive $|A| \leq |B|$ se esiste una funzione iniettiva di A in B (oppure una funzione suriettiva di B su A). Si scrive $|A| < |B|$ se $|A| \leq |B|$ e $|A| \neq |B|$.

Se $|C| = |A| + |B|$ allora scriveremo anche $|A| = |C| - |B|$ oppure $|B| = |C| - |A|$, ma si tratta di espressioni un po' pericolose, come vedremo.

3.2.1. PROPRIETÀ DELLE OPERAZIONI TRA CARDINALI. Avendo usato delle operazioni insiemistiche per definire le operazioni tra cardinali, queste ultime ereditano le proprietà delle prime; per esempio commutatività (e associatività) per somma e prodotto seguono dalla stessa proprietà per unione e prodotto cartesiano; la distributività del prodotto rispetto alla somma segue dalla analoga proprietà del prodotto cartesiano rispetto alla unione (da notare che l'altra distributività è falsa).

Useremo liberamente in futuro queste facili proprietà. Segnaliamo per esempio che da $A^{B \cup C} = A^B \times A^C$ se $B \cap C = \emptyset$ segue una ben nota formula per gli esponenti: $|A|^{|B|+|C|} = |A|^{|B|} |A|^{|C|}$.

3.2.2. FORMULA DI INCLUSIONE-ESCLUSIONE. Per ogni coppia di insiemi A e B abbiamo la relazione

$$|A \cup B| = |A| + |B| - |A \cap B|.$$

Infatti poiché A è unione disgiunta di $A \setminus B$ e $A \cap B$, B è unione disgiunta di $B \setminus A$ e $A \cap B$, e $A \cup B$ è unione disgiunta di $A \setminus B$, $A \cap B$ e $B \setminus A$, abbiamo

$$|A \cup B| + |A \cap B| = |A \setminus B| + |A \cap B| + |B \setminus A| + |A \cap B| = |A| + |B|$$

(abbiamo fatto uso implicitamente della proprietà associativa della somma).

Nel caso di tre insiemi A , B , C abbiamo una formula analoga:

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$$

che si giustifica in modo analogo.

Più in generale, abbiamo la seguente formula detta di inclusione-esclusione: data una famiglia finita A_1, A_2, \dots, A_n di insiemi, vale che

$$\left| \bigcup_{i=1}^n A_i \right| = \sum_{i=1}^n |A_i| - \sum_{i_1 < i_2=1}^n |A_{i_1} \cap A_{i_2}| + \dots + (-1)^{j+1} \sum_{i_1 < \dots < i_j=1}^n \left| \bigcap_{\ell=1}^j A_{i_\ell} \right| + \dots + (-1)^{n+1} \left| \bigcap_{i=1}^n A_i \right|$$

la cui dimostrazione diretta è laboriosa, ma che si potrà dimostrare facilmente una volta noto il principio di induzione, tra poche pagine.

3.3. TEOREMA (CARDINALITÀ POTENZA). *Per ogni insieme A , abbiamo che $|\mathcal{P}(A)| > |A|$.*

La cardinalità $|\mathcal{P}(A)|$ si indica spesso con $2^{|A|}$ poiché esiste una biiezione tra l'insieme delle parti di A e l'insieme $\mathbf{2}^A$ delle funzioni di A in $\{0, 1\}$. Dunque il teorema dice che per ogni insieme A vale che $2^{|A|} > |A|$.

DIMOSTRAZIONE. Certamente $|A| \leq |\mathcal{P}(A)|$ poiché la funzione di A in $\mathcal{P}(A)$ che porta ogni elemento a nel singoletto $\{a\}$ è iniettiva. Basta quindi mostrare che non esistono funzioni suriettive di A in $\mathcal{P}(A)$. Sia $\varphi : A \rightarrow \mathcal{P}(A)$ una qualsiasi funzione e consideriamo il sottinsieme di A dato da $A' = \{a \in A \mid a \notin \varphi(a)\}$. Allora è chiaro che A' non appartiene all'immagine di φ , poiché altrimenti sarebbe $A' = \varphi(a')$ con $a' \in A$ e risulterebbe $a' \in A'$ se e solo se $a' \notin \varphi(a') = A'$, assurdo. Quindi alcuna tale funzione può essere suriettiva; di conseguenza non esistono biiezioni tra A e la sua potenza, e quindi la cardinalità di quest'ultima è strettamente superiore. \square

♠ **3.4. TEOREMA (CANTOR-SCHRÖDER-BERNSTEIN).** *Se $|A| \leq |B|$ e $|B| \leq |A|$ allora $|A| = |B|$. In altri termini, se esistono una funzione iniettiva di A in B e una funzione iniettiva di B in A , allora esiste una biiezione tra A e B .*

DIMOSTRAZIONE. La dimostrazione è particolarmente interessante, anche se non immediata, e ne presentiamo solo le linee guida. Date due funzioni iniettive $f : A \rightarrow B$ e $g : B \rightarrow A$ garantite dalle ipotesi, per ogni elemento a di A e ogni elemento b di B diciamo che a è figlio di b se $a = g(b)$ e che b è figlio di a se $b = f(a)$. Possiamo dunque parlare di “antenati” per ogni fissato elemento nel senso genealogico. Studiando la linea genealogica di ogni elemento possiamo dividere A in tre sottinsiemi disgiunti: sia A' l'insieme degli elementi che non hanno capostipite; sia A_A l'insieme degli elementi che hanno capostipite in A ; sia A_B l'insieme degli elementi che hanno capostipite in B . Stessa cosa si può fare per B .

Ora possiamo definire una funzione biiettiva di A verso B nel modo seguente: f su A' (biiezione tra A' e B'), f su A_A (biiezione tra A_A e B_A), l'inversa di g su A_B (biiezione tra A_B e B_B). \square

♠ **3.5. TEOREMA (TOTALITÀ DELL'ORDINE).** *Dati due insiemi qualsiasi A e B , o esiste una funzione iniettiva di A in B oppure esiste una funzione iniettiva di B in A ; dunque due cardinali sono sempre confrontabili: o $|A| \leq |B|$ oppure $|B| \leq |A|$.*

DIMOSTRAZIONE. Ci si riduce al caso di insiemi ben ordinati, e in questo caso si dimostra che uno dei due è incluso ordinatamente nell'altro. Non banale: vedi Esercizi 1-10, pg. 22-23 di I. Barsotti. \square

3.6. CARDINALITÀ FINITE. Gli insiemi $\mathbf{n} = \{0, 1, \dots, n-1\}$ introdotti all'inizio si dicono insiemi finiti, e le loro cardinalità si dicono finite; potremmo definire i numeri naturali allora nel modo seguente: essi sono le cardinalità di insiemi del tipo $N_0 = \emptyset$ (e poniamo $|N_0| = 0$), $N_1 = \{\emptyset\}$ (e poniamo $|N_1| = 1$), $N_2 = \{\emptyset, \{\emptyset\}\}$ (e poniamo $|N_2| = 2$), $N_3 = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$ (e poniamo $|N_3| = 3$), e così via, definito N_n (e posto $|N_n| = n$) definiamo $N_{n+1} = N_n \cup \{N_n\}$ (che ha un elemento in più, dunque porremo $|N_{n+1}| = n + 1$).

È chiaro che in questo modo costruiamo infiniti insiemi (nel senso che non c'è un limite alla costruzione), e che le operazioni di somma e prodotto tra cardinali corrispondono esattamente alle usuali operazioni tra numeri naturali. Ci occuperemo poi di problemi di combinatorica tra insiemi finiti.

Un altro modo possibile per costruire (a partire dal vuoto \emptyset) le cardinalità finite è il seguente: $M_0 = \emptyset$, $M_1 = \{\emptyset\}$, $M_2 = \{\emptyset, \{\emptyset\}\}$, $M_3 = \{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}\}$ e così via, definito M_n definiamo $M_{n+1} = \{\emptyset\} \cup \mathcal{S}(M_n)$ ove $\mathcal{S}(M_n)$ indica l'insieme dei singoletti di M_n .

3.7. CARDINALITÀ INFINITE. Si dicono infiniti invece gli insiemi la cui cardinalità non sono finite. Per esempio la collezione di tutti gli insiemi N_n , prima usati per definire le cardinalità finite, non è finita. A rigor di termini dovremmo postulare la sua esistenza come insieme, visto che non lo possiamo esplicitamente presentare per intero. La sua cardinalità si chiama “infinito numerabile” e si indica con \aleph_0 (alef zero). Dunque abbiamo $n < \aleph_0$ per ogni cardinale finito n .

3.7.1. PROPRIETÀ DI \aleph_0 . L'infinito numerabile è particolarmente importante, e quindi ne elenchiamo alcune proprietà:

(CI1) $\aleph_0 + n = \aleph_0$ per ogni cardinale finito n ; infatti l'applicazione $(\mathbb{N} \times \{0\}) \cup (\mathbf{n} \times \{1\}) \rightarrow \mathbb{N}$ che manda $(i, 0)$ in $i + n$ e $(j, 1)$ in j è una applicazione biiettiva;

- (CI2) $\aleph_0 + \aleph_0 = \aleph_0$; infatti l'applicazione $(\mathbb{N} \times \{0\}) \cup (\mathbb{N} \times \{1\}) \rightarrow \mathbb{N}$ che manda (i, α) in $2i + \alpha$ è una applicazione biettiva;
- (CI3) $\aleph_0 \aleph_0 = \aleph_0$; infatti (primo argomento diagonale di Cantor) possiamo trovare una biiezione di \mathbb{N} su $\mathbb{N} \times \mathbb{N}$ ben ordinando quest'ultimo insieme con la regola $(a, b) \leq (a', b')$ se e solo se $a + b \leq a' + b'$ oppure $a + b = a' + b'$ e $a \leq a'$. Possiamo allora mandare $\ell \in \mathbb{N}$ nell' ℓ -esimo elemento di \mathbb{N}^2 per quest'ordine, e si tratta di una mappa suriettiva (e iniettiva: farsi un disegno).
- (CI4) $\aleph_0^{\aleph_0} = 2^{\aleph_0}$; infatti l'insieme delle funzioni di \mathbb{N} in \mathbb{N} è in biiezione con il sottinsieme delle funzioni (strettamente) crescenti di \mathbb{N} in \mathbb{N} , e queste a loro volta sono definite dall'insieme dei valori assunti, e quindi dalla funzione caratteristica dell'insieme immagine (che è una funzione di \mathbb{N} in $\mathbb{2}$). Si osservi che allora per ogni n finito si ha $\aleph_0^{\aleph_0} = n^{\aleph_0} = 2^{\aleph_0}$ per confronto.

Le stesse proprietà sono vere per ogni cardinale infinito, ma dimostrarlo è più difficile. Ricordiamo inoltre che $\mathfrak{c} = 2^{\aleph_0} > \aleph_0$ si dice la cardinalità del continuo (si vedrà essere la cardinalità dell'insieme dei numeri reali).

3.7.2. Il secondo argomento diagonale di Cantor si usa per mostrare che la cardinalità di $\mathbb{N}^{\mathbb{N}}$ è strettamente maggiore della cardinalità di \mathbb{N} (il risultato l'abbiamo già visto, ma l'argomento di Cantor si usa anche in altri contesti, per esempio per dimostrare che l'insieme dei numeri reali ha cardinalità maggiore dell'insieme dei numeri naturali). Si ragiona per assurdo nel modo seguente: supponiamo che $\mathbb{N}^{\mathbb{N}}$ sia numerabile, e sia $f : \mathbb{N} \rightarrow \mathbb{N}^{\mathbb{N}}$ una biiezione (per ogni n chiamiamo f_n la funzione corrispondente); costruiamo allora una funzione $g : \mathbb{N} \rightarrow \mathbb{N}$ che non è nessuna delle f_n , dunque contraddicendo la suriettività di f . Basta per questo definire $g(m) = f_m(m) + 1$, perché allora per ogni n abbiamo $f_n \neq g$ in quanto $f_n(n) \neq g(n)$.

♠ **3.7.3.** PROPRIETÀ DEGLI INSIEMI INFINITI. Ogni insieme infinito contiene un sottinsieme numerabile, dunque ha cardinalità maggiore o uguale ad \aleph_0 , e quindi \aleph_0 è la più piccola cardinalità infinita. Si tratta di un risultato la cui dimostrazione richiede l'uso del lemma di Zorn, o di uno degli enunciati equivalenti.

3.7.4. TEOREMA. *Un insieme è infinito se e solo se esiste una biiezione con un suo sottinsieme proprio.*

DIMOSTRAZIONE. Ogni funzione di un insieme finito in \mathbb{N} che sia iniettiva è anche suriettiva, quindi il "se" della proposizione è chiaro. Per il viceversa consideriamo prima il caso di un insieme numerabile, per esempio i numeri naturali: è chiaro allora che la funzione che manda ogni numero nel suo successore dà una biiezione di tutto l'insieme con l'insieme costituito dai numeri non nulli (sottinsieme proprio). Poiché ogni insieme infinito X contiene un insieme numerabile N , possiamo scrivere $X = N \cup (X \setminus N)$ (unione disgiunta) e definire una funzione di X in \mathbb{N} che sia l'identità su $X \setminus N$ e che identifichi N a un suo sottinsieme stretto N' ; allora la funzione costruita è una biiezione di X con $X' = N' \cup (X \setminus N) \subset X$, come si voleva. \square

♠ **3.7.5.** Ogni insieme infinito è unione disgiunta di insiemi numerabili (si deve usare il lemma di Zorn).

♠ **3.7.6.** Conseguenze: $c + n = c$, $nc = c$, $c + \aleph_0 = c$, $c\aleph_0 = c$, $c + c = c$, $cc = c$, le somme finite tra cardinali di cui almeno uno sia infinito coincidono con il massimo dei sommandi, i prodotti finiti tra cardinali di cui almeno uno sia infinito coincidono con il massimo dei fattori, $2^c = c^c > c$.

♠ **3.7.7.** Se A è infinito, e $\mathcal{P}'(A)$ indica l'insieme delle parti finite di A , allora abbiamo $|\mathcal{P}'(A)| = |A|$.

3.8. COMBINATORICA DELLE FUNZIONI. Se A e B sono insiemi finiti di cardinalità m ed n rispettivamente, possiamo chiederci qual è la cardinalità dell'insieme delle funzioni di A in B , e di certi tipi particolari di funzioni. Calcolare il numero di funzioni di A in B è facile: al fine di costruire una funzione, per ogni elemento di A dobbiamo decidere quale elemento di B è la sua immagine, ed ogni volta possiamo scegliere tra n elementi; le scelte da fare sono tutte indipendenti tra loro, e dunque in totale abbiamo n^m possibili funzioni. Quindi risulta

$$|B^A| = |B|^{|A|}$$

che giustifica la simbologia B^A per l'insieme delle applicazioni di A in B .

3.8.1. Anche l'insieme delle funzioni biettive di A in B è facilmente controllabile: è vuoto, ovvero di cardinalità zero se $|A| \neq |B|$; altrimenti è $(|A|)!$, il fattoriale della cardinalità di A (prodotto

di tutti i numeri interi da 1 a $|A|$; si pone per definizione $0! = 1$). Infatti in questo caso costruendo la funzione dobbiamo fare attenzione a non ripetere le scelte già fatte per le immagini: quindi vi sono n scelte per l'immagine del primo elemento, $n-1$ per il secondo, $n-2$ per il terzo e così via.

3.8.2. L'insieme delle funzioni iniettive di A in B è nullo se $|A| > |B|$ (principio dei cassetti: se vi sono più oggetti che cassetti, in qualche cassetto deve stare più di un oggetto; talvolta detto anche principio della piccionaia: se ci sono più piccioni che casette, in qualche casetta ci deve stare più di un piccione); altrimenti, ragionando analogamente a prima, si vede che si tratta del prodotto degli m numeri naturali in discesa partendo da n ; dunque la cardinalità è $(|B|)!/(|B|-|A|)!$.

3.8.3. Nettamente più difficile è studiare il numero di funzioni suriettive di A in B ; certamente è zero se $|A| < |B|$. Una strategia costruttiva diretta, cioè cercare tutti i modi possibili di costruire funzioni suriettive, in questo caso non è ovvia (provare per credere); conviene invece ricorrere al principio di inclusione-esclusione per conteggiare le funzioni non suriettive di A in B . In effetti se definiamo F_b l'insieme delle funzioni la cui immagine non contiene $b \in B$, abbiamo che la cardinalità dell'insieme $\bigcup_{b \in B} F_b$ delle funzioni non suriettive è dato da

$$\sum_{b \in B} |F_b| - \sum_{b, b' \in B} |F_b \cap F_{b'}| + \dots + (-1)^{i+1} \sum_{b_1, \dots, b_i \in B} |F_{b_1} \cap \dots \cap F_{b_i}| + \dots + (-1)^{|B|+1} \left| \bigcap_{b \in B} F_b \right|$$

e di conseguenza la cardinalità delle funzioni suriettive è

$$|B|^{|A|} - |B|(|B|-1)^{|A|} + \binom{|B|}{2}(|B|-2)^{|A|} + \dots + (-1)^i \binom{|B|}{i}(|B|-i)^{|A|} + \dots + (-1)^{|B|} \binom{|B|}{|B|}(|B|-|B|)^{|A|}$$

poiché il numero di addendi nella i -esima sommatoria è $\binom{|B|}{i}$ (coefficiente binomiale) e $(|B|-i)^{|A|}$ è il numero di elementi che ogni intersezione di quella sommatoria comporta (sì, è vero che l'ultimo addendo scritto è sempre zero, ma lo si è lasciato ugualmente per rispettare la simmetria della formula).

3.8.4. Nel prossimo paragrafo la formula precedente, sia

$$S_{n,k} = \sum_{i=0}^k (-1)^i \binom{k}{i} (k-i)^n$$

se $S_{n,k}$ indica il numero di funzioni suriettive da un insieme con n elementi a uno con k elementi, potrà essere dimostrata per induzione a partire dalla seguente osservazione: se fissiamo un elemento del dominio, allora possiamo distinguere le funzioni suriettive in due tipi (quali?) e di conseguenza

$$S_{n+1,k} = k(S_{n,k} + S_{n,k-1})$$

(si osserverà anche la parentela con la formula ricorsiva dei coefficienti binomiali). Problema per il (paragrafo) futuro: che tipo di formula ricorsiva si può scrivere fissando un elemento del codominio?

3.9. DISPOSIZIONI E COMBINAZIONI. Una disposizione di classe k di un insieme A è una k -upla ordinata di elementi di A ; si chiamano disposizioni con ripetizione se si permette che possano comparire più volte gli stessi elementi, senza ripetizione altrimenti. Se $|A| = n$, il numero di disposizioni di classe k con ripetizione è dato da n^k . Infatti l'insieme di tali disposizioni è in biiezione con l'insieme delle funzioni da un insieme con k elementi ad A . Il numero di disposizioni (semplici, ovvero senza ripetizioni) di classe k di un insieme con n elementi si indica con $D_{n,k}$. Poiché l'insieme di tali disposizioni è in biiezione con l'insieme delle funzioni iniettive da un insieme con k elementi ad A , abbiamo che

$$D_{n,k} = n(n-1) \dots (n-k+1) = \frac{n!}{(n-k)!}.$$

Una combinazione di classe k di un insieme A è invece una scelta non ordinata di k elementi di A ; di nuovo si distinguono le combinazioni con ripetizione se si permette che possano comparire più volte gli stessi elementi, senza ripetizione altrimenti. Per il caso delle combinazioni senza ripetizioni, la differenza rispetto alle disposizioni di classe k consiste solo nel considerare irrilevante "l'ordine di scelta" degli elementi di A ; dunque vi sono sempre $k!$ disposizioni che identificano la stessa combinazione. Da questa osservazione si deduce che le combinazioni di classe k (semplici, ovvero senza ripetizioni) di un insieme con n elementi sono in numero

$$C_{n,k} = \frac{n!}{(n-k)!k!} = \binom{n}{k}$$

(coefficiente binomiale: la tavola di questi numeri è il ben noto triangolo di Tartaglia, che ricorderemo tra poche pagine).

Poiché l'insieme delle parti di A si può vedere come unione disgiunta degli insiemi formati dai sottinsiemi di fissate cardinalità, deduciamo dalle formule precedenti che $\sum_{i=0}^n \binom{n}{i} = 2^n$ (cardinalità dell'insieme potenza, essendo in biiezione con l'insieme delle funzioni di A in $\mathbf{2}$), la ben nota formula del binomio di Newton che studieremo in generale per anelli commutativi.

Si osservi infine che l'uguaglianza evidente $\binom{n}{k} = \binom{n}{n-k}$ per ogni n e k ha una ovvia interpretazione combinatorica (passando agli insiemi complementari).

Il caso delle combinazioni con ripetizione è nettamente diverso, e può essere visto nel modo seguente. Dare una combinazione con ripetizione di classe k a partire da un insieme di n elementi è come dare una distribuzione di k palline (tutte uguali) in n scatole diverse (ogni scatola rappresenta un elemento dell'insieme, e il numero di palline nella scatola rappresenta quante volte quell'elemento viene scelto). Si tratta allora di contare in quanti modi l'insieme delle k palline (pensate allineate) può essere diviso usando $n - 1$ sbarrette. Si vede facilmente che questo numero è $\binom{n+k-1}{k}$.

3.10. PARTIZIONI DI INSIEMI. Una partizione di un insieme A è un sottinsieme di $\mathcal{P}(A)$ formato da sottinsiemi non vuoti di A a due a due disgiunti e la cui unione dà tutto A ; una partizione si dice di classe k se è formata da k sottinsiemi di A . Se $n = |A|$, allora certamente $k \leq n$. Ogni funzione suriettiva di A verso un insieme formato di k elementi dà luogo ad una partizione di A , ed evidentemente vi sono $k!$ di tali funzioni che identificano la stessa partizione (si possono scambiare comunque gli elementi dell'immagine, ovvero si può comporre la funzione data con una qualunque biiezione del codominio).

Detto $P_{n,k}$ il numero di partizioni di classe k di un insieme con n elementi, abbiamo allora che

$$P_{n,k} = \frac{1}{k!} \sum_{i=0}^k (-1)^i \binom{k}{i} (k-i)^n.$$

Si osservi per esempio che per $k = n$ vi è esattamente una partizione (quella in singoletti), che dunque ci restituisce la formula

$$n! = \sum_{i=0}^n (-1)^i \binom{n}{i} (n-i)^n$$

che non è facilmente verificabile in modo diretto. È istruttivo per il lettore farsi la tavola dei numeri $P_{n,k}$ per valori piccoli di n e di k , diciamo minori o uguali a 10.

3.11. PARTIZIONI DI NUMERI. Una partizione di un numero naturale n è una collezione formato da numeri naturali non nulli (eventualmente ripetuti) la cui somma dà n ; una partizione di n si dice di classe k se è formata da k numeri interi. Il lettore è invitato a farsi la tavola del numero di partizioni di classe k di n per valori piccoli di n e di k , diciamo minori o uguali a 10.

♠ **3.12. COMBINATORICA DELLE RELAZIONI.** Dato un insieme A di cardinalità finita n , possiamo considerare l'insieme delle possibili relazioni su A : si tratta dell'insieme delle parti di $A \times A$, e dunque di cardinalità 2^{n^2} .

3.12.1. RELAZIONI RIFLESSIVE. Le relazioni soddisfacenti alla proprietà riflessiva sono invece in numero $2^{n(n-1)}$; infatti in questo caso i termini diagonali (che sono esattamente $|A|$) di $A \times A$ devono comparire necessariamente, gli altri essendo liberi: si tratta quindi delle funzioni da un insieme con $|A \times A| - |A| = n^2 - n$ elementi in $\mathbf{2}$.

3.12.2. RELAZIONI SIMMETRICHE. Le relazioni soddisfacenti alla proprietà simmetrica sono invece in numero $2^{\frac{n(n+1)}{2}}$; infatti in questo caso i termini diagonali (che sono esattamente $|A|$) di $A \times A$ sono liberi, mentre i termini non diagonali devono essere simmetrici: si tratta quindi delle funzioni da un insieme con $\frac{|A \times A| - |A|}{2} + |A| = \frac{n^2 + n}{2}$ elementi in $\mathbf{2}$.

3.12.3. RELAZIONI SIMMETRICHE E RIFLESSIVE. Un analogo ragionamento mostra che le relazioni riflessive e simmetriche sono $2^{\frac{n(n-1)}{2}}$.

3.12.4. RELAZIONI DI EQUIVALENZE. Poiché le relazioni di equivalenza sono in biiezione con le partizioni dell'insieme A , esse sono in numero di $\sum_{k=1}^n P_{n,k}$.

3.12.5. RELAZIONI ANTISIMMETRICHE. Il numero di relazioni antisimmetriche può essere valutato tenendo conto che per ogni coppia di posizioni simmetriche non diagonali, solo tre possibilità sono compatibili con la condizione; quindi si tratta di $2^n 3^{\frac{n(n-1)}{2}}$ relazioni.

3.12.6. RELAZIONI RIFLESSIVE E ANTISIMMETRICHE. Analogamente, le relazioni che sono riflessive e antisimmetriche sono in numero di $3^{\frac{n(n-1)}{2}}$.

3.12.7. RELAZIONI D'ORDINE. Le relazioni d'ordine totale sono $n!$, come le permutazioni possibili; invece risulta difficile conteggiare le relazioni d'ordine parziale, come pure contare le relazioni soddisfacenti alla proprietà transitiva.

4. Numeri Naturali e Induzione.

La più semplice struttura algebrica è quella data da una regola per combinare due elementi di un insieme per produrne un altro.

4.1. DEFINIZIONE (MAGMA). Diciamo magma un insieme M dotato di una operazione binaria, cioè di una funzione $M \times M \rightarrow M$ che manda (m, m') in $m * m'$. Un magma si dice associativo se per ogni terna di elementi $m, m', m'' \in M$ si ha che $(m * m') * m'' = m * (m' * m'')$ (nel qual caso le operazioni si possono scrivere senza parentesi). Si dice unitario se esiste un elemento $\iota \in M$ (chiamato elemento neutro per l'operazione) tale che $\iota * m = m = m * \iota$ per ogni $m \in M$. Si dice commutativo se per ogni coppia $m, m' \in M$ si ha che $m * m' = m' * m$.

Talvolta un magma associativo ed unitario si chiama un semigruppato, e un magma commutativo, associativo ed unitario si chiama un monoide.

Una funzione tra due magma $f : M \rightarrow N$ si dice un omomorfismo di magma, oppure funzione di magma, se rispetta l'operazione e gli eventuali elementi neutri, cioè se $f(m * m') = f(m) * f(m')$ per ogni $m, m' \in M$ (si noti che il primo $*$ denota l'operazione su M , e il secondo quella su N), ed eventualmente $f(\iota_M) = \iota_N$.

Data una definizione di una struttura algebrica, si può sempre trarne una piccola messe di facili conseguenze; ne esplicitiamo alcune:

4.1.1. In un magma associativo, l'elemento neutro se esiste è unico. Siano infatti ι e ι' due elementi neutri; allora si ha $\iota = \iota * \iota' = \iota'$.

4.1.2. Se esiste l'elemento neutro ι , un simmetrico destro (risp. sinistro) di $m \in M$ è un elemento $m^* \in M$ (resp. ${}^*m \in M$) tale che $m * m^* = \iota$ (risp. ${}^*m * m = \iota$); un elemento simmetrico di $m \in M$ è un elemento m^* tale che $m * m^* = \iota = m^* * m$. Allora in un magma associativo, l'elemento simmetrico di un dato elemento se esiste è unico, e se un elemento ha simmetrico destro e sinistro, questi coincidono e sono un simmetrico per quell'elemento. Infine se m ammette simmetrico m^* , anche m^* ammette un simmetrico che è $m^{**} = m$.

4.1.3. In un magma associativo il risultato dell'applicazione ripetuta dell'operazione non dipende dalla sequenza in cui viene effettuata (fermo restando l'ordine degli elementi).

4.1.4. In un magma associativo e commutativo il risultato dell'applicazione ripetuta dell'operazione non dipende dall'ordine con cui vengono presi gli elementi.

4.1.5. MAGMA INTEGRO. Un magma M si dice intero se per ogni $a \in M$ dalla relazione $a * b = a * c$ segue che $b = c$. Data una funzione tra magma unitari, se essa rispetta la somma, allora rispetta anche l'elemento neutro sotto ipotesi che il codominio sia magma intero. Infatti in tal caso da $f(\iota_M) * f(\iota_M) = f(\iota_M * \iota_M) = f(\iota_M) = f(\iota_M) \iota_N$ deduciamo che $f(\iota_M) = \iota_N$.

4.1.6. CONGRUENZE. Una relazione di equivalenza \sim in un magma M si dice una congruenza se $a \sim b$ implica $a * c \sim b * c$ per ogni $c \in M$. Si osservi che questo è equivalente a che se $a \sim b$ e $a' \sim b'$ allora $a * a' \sim b * b'$.

In tal caso l'insieme quoziente M / \sim è dotato di una struttura di magma (ben) definita da $[a] * [b] = [a * b]$ (ben definita significa che la definizione dipende solo dalle classi $[m]$ e non dai singoli elementi di una classe).

4.1.7. NOTAZIONI ADDITIVE E MULTIPLICATIVE. Nel caso di magmi commutativi, si usa spesso indicare con $+$ (somma) l'operazione, con 0 (zero) l'elemento neutro, e con $-m$ (opposto) il simmetrico di m . Nel caso di magmi non commutativi si preferisce usare la notazione moltiplicativa cioè indicare con \cdot (prodotto, spesso muto) l'operazione, con 1 (uno o unità) l'elemento neutro, e con m^{-1} (inverso) il simmetrico di m .

4.2. Dato un qualsiasi insieme A , l'insieme A^A di tutte le funzioni di A in A , dotato della operazione di composizione di funzioni, è un magma associativo, unitario (elemento neutro è la mappa

identica) e non commutativo. Gli elementi invertibili sono le biiezioni.

Lo stesso si può dire dell'insieme $\mathcal{P}(A \times A)$ delle relazioni di A in sè, dotato della composizione di relazioni; in questo caso vi è anche un elemento ω (la relazione vuota) tale che $m * \omega = \omega = \omega * m$ per ogni $m \in M$, che si dice elemento killer.

Abbiamo già usato l'insieme dei numeri naturali nell'eccezione ingenua, e parlando di cardinalità (finite) ne abbiamo anche definito precisamente gli elementi. Diamo ora una descrizione rigorosa di questo insieme e di alcune sue importanti proprietà.

4.3. DEFINIZIONE (NUMERI NATURALI). *L'insieme \mathbb{N} dei numeri naturali ha come elementi le cardinalità finite. Esiste in \mathbb{N} una operazione somma che è commutativa ed associativa, con elemento neutro lo zero (che è anche l'unico elemento simmetrizzabile). Inoltre l'ordinamento tra i cardinali finiti dà un ordinamento totale su \mathbb{N} che è un buon ordinamento (cioè ogni sottinsieme non vuoto di \mathbb{N} ha minimo).*

4.3.1. PRODOTTO NEI NATURALI. Abbiamo anche dato una nozione di prodotto tra cardinali, e quindi tra numeri naturali; in effetti per i numeri naturali l'operazione di prodotto può essere ridotta a quella della somma nel modo seguente: il prodotto nm corrisponde a "sommare m volte il numero n con se stesso":

$$mn = \underbrace{n + \cdots + n}_{m \text{ volte}}$$

poiché $\mathbf{n} \times \mathbf{m} = (\mathbf{n} \times \{0\}) \cup \cdots \cup (\mathbf{n} \times \{m-1\})$ (si tratta di una unione di insiemi a due a due disgiunti).

Si osservi che l'insieme dei cardinali finiti con l'operazione di prodotto è anch'esso un magma associativo, commutativo e unitario (con elemento neutro 1), ma la sua struttura come ben noto, è molto più complicata; per esempio non è integro a causa della presenza di un elemento killer (lo zero).

4.4. TECNICHE DI INDUZIONE. Introduciamo ora un principio fondamentale della matematica: il principio di induzione per i numeri naturali. Si tratta di una tecnica di dimostrazione di famiglie infinite di enunciati indiciate sui numeri naturali, e che riduce a dimostrare il primo degli enunciati (base dell'induzione) e poi a dimostrare che dalla validità di un enunciato segue la validità del successivo (passo detto induttivo). Vi sono alcune variazioni possibili che esamineremo.

4.5. TEOREMA (PRINCIPIO DI INDUZIONE (PRIMA FORMA)). *Sia M un sottinsieme di \mathbb{N} soddisfacente alle due proprietà seguenti:*

- (0) $0 \in M$;
- (i) per ogni $n \in \mathbb{N}$, se $n \in M$ allora $n + 1 \in M$;

allora $M = \mathbb{N}$.

Sia ora A_n una famiglia di asserzioni indiciate da $n \in \mathbb{N}$; supponiamo soddisfatte le due proprietà seguenti:

- (0) A_0 è vera
- (i) per ogni $n \in \mathbb{N}$, se A_n è vera allora A_{n+1} è vera;

allora le affermazioni A_n sono vere per ogni $n \in \mathbb{N}$.

DIMOSTRAZIONE. La seconda asserzione del teorema segue dalla prima usando l'insieme $M = \{i \in \mathbb{N} \mid A_i \text{ è vera}\}$. La prima asserzione segue dal buon ordinamento di \mathbb{N} : supponiamo che $M \neq \mathbb{N}$; allora esiste un minimo elemento in $\mathbb{N} \setminus M \neq \emptyset$, sia i_0 ; per minimalità abbiamo che $i_0 - 1 \in M$, da cui segue che $i_0 \in M$ (per la prima condizione se $i_0 = 1$, per la seconda se $i_0 > 1$), assurdo. \square

4.5.1. Ad esempio mostriamo per induzione la formula $1 + 2 + \cdots + n = \frac{n(n+1)}{2}$. Verifichiamo il caso $n = 1$, che dà in effetti $1 = \frac{1(1+1)}{2}$. Ora supponiamo vera la formula per il valore n , e vediamo cosa succede per $n + 1$:

$$1 + 2 + \cdots + n + (n + 1) = \frac{n(n + 1)}{2} + (n + 1) = \frac{n(n + 1) + 2(n + 1)}{2} = \frac{(n + 1)(n + 2)}{2}$$

(nel primo passaggio abbiamo usato l'ipotesi induttiva) che è esattamente la stessa formula con $n + 1$ invece di n ; quindi le formule sono dimostrate per ogni n .

Questa formula può anche essere dimostrata "alla Gauss" osservando che ogni coppia di numeri "equidistanti dagli estremi" dà come somma $n + 1$, e che di tali coppie ve ne sono $n/2$ (anche se in questo c'è una imprecisione: quale?).

Un metodo ulteriore per dimostrare la formula senza induzione è la seguente osservazione:

$$\sum_{i=1}^n i^2 + (n+1)^2 - 1 = \sum_{i=1}^n (i+1)^2 = \sum_{i=1}^n i^2 + 2 \sum_{i=1}^n i + n$$

(sviluppando in due modi diversi il termine centrale), da cui, uguagliando i termini estremi, sparisce la sommatoria dei quadrati e si può ricavare la sommatoria voluta.

4.5.2. Trovare e dimostrare per induzione una formula per la sommatoria dei quadrati dei primi n numeri naturali.

4.5.3. Dimostrare per induzione che la somma dei cubi dei primi n numeri naturali è pari al quadrato della somma dei primi n numeri naturali; in formule $\sum_{i=1}^n i^3 = (\sum_{i=1}^n i)^2$, e dunque $\sum_{i=1}^n i^3 = \frac{n^2(n+1)^2}{4}$.

4.5.4. Trovare e dimostrare per induzione una formula per la sommatoria delle quarte potenze dei primi n numeri naturali.

4.5.5. Mostrare per induzione (su j) che la somma delle j -esime potenze dei primi n naturali è data da un polinomio in n di grado $j+1$?

4.5.6. Dimostrare per induzione la formula di inclusione-esclusione.

4.6. TEOREMA (PRINCIPIO DI INDUZIONE (SECONDA FORMA)). Sia M un sottinsieme di \mathbb{N} soddisfacente alle due proprietà seguenti:

- (0) $0 \in M$;
- (i) per ogni $n \in \mathbb{N}$, se $i \in M$ per ogni $i \leq n$ allora $n+1 \in M$;

allora $M = \mathbb{N}$.

Sia ora A_n una famiglia di asserzioni indiciate da $n \in \mathbb{N}$; supponiamo soddisfatte le due proprietà seguenti:

- (0) A_0 è vera
- (i) per ogni $n \in \mathbb{N}$, se A_i è vera per ogni $i \leq n$ allora A_{n+1} è vera;

allora le affermazioni A_n sono vere per ogni $n \in \mathbb{N}$.

DIMOSTRAZIONE. Analoga a quella della prima forma. □

4.6.1. (PROPRIETÀ ARCHIMEDEA DELL'ORDINE DI \mathbb{N}). Sia $n \geq 1$ un numero naturale; allora per ogni naturale m esiste un naturale p tale che $pn \geq m$. Ragioniamo per induzione su m . Se $m = 1$ allora basta usare $p = 1$ e $pn = n \geq 1 = m$. Osserviamo anche che lo stesso vale per ogni $m \leq n$. Supponiamo ora che $m > 1$, e possiamo supporlo $> n$; consideriamo $m' = m - n < m$ e per ipotesi induttiva troviamo p' tale che $p'n \geq m'$. Allora posto $p = p' + 1$ abbiamo $pn = p'n + n \geq m' + n = m$, come si voleva.

4.6.2. Altri importanti esempi di questo tipo di induzione si vedranno discutendo la “divisione con resto” tra numeri interi e tra polinomi.

4.7. ULTERIORI VARIAZIONI. Talvolta vi sono enunciati indiciati da numeri naturali che hanno significato solo da un certo valore dell'indice in poi (per esempio: l'unione di n insiemi non dipende dall'ordine in cui viene effettuata; a rigori avrebbe senso solo per $n \geq 2$); quindi può essere utile usare delle induzioni che partano da questo indice “minimo” per gli enunciati che si studiano.

Si osservi anche che, se il passo induttivo delle dimostrazioni utilizza diciamo gli m casi precedenti, indipendentemente dal livello n del passo induttivo, allora i “primi m casi” devono essere dimostrati tutti indipendentemente.

4.8. DEFINIZIONI PER INDUZIONE. Un procedimento per induzione si usa anche per definire certi oggetti matematici; noi abbiamo definito “per induzione” degli insiemi N_i che rappresentano le cardinalità finite (infatti abbiamo definito il primo, e poi abbiamo specificato come costruire “il successivo” dato uno qualunque degli elementi). Dare una definizione per induzione di oggetti F_i per $i \in \mathbb{N}$, $i \geq k$, significa:

- (0) definire il primo F_k ;
- (i) definire F_{n+1} potendo usare nella definizione gli oggetti F_i con $i \geq k$ e $i \leq n$.

Spesso risulta facile, o spontaneo dare definizioni per induzione, ma per costruirli veramente bisogna procedere “uno dopo l'altro”; è un problema non facile caratterizzare questi oggetti tramite una “definizione chiusa” che permetta di costruire ciascuno di questi senza essere passati per tutti i precedenti.

4.8.1. FATTORIALI, SEMIFATTORIALI. Un esempio facile è la definizione induttiva del fattoriale: si tratta della funzione $! : \mathbb{N} \rightarrow \mathbb{N}$ definita dalla condizione di base $0! = 1$ e dalla condizione induttiva $(n+1)! = (n+1)(n!)$. È immediato in questo caso riconoscere che si tratta della usuale definizione per cui $n!$ è il prodotto dei numeri interi da 1 a n .

Il semifattoriale $!! : \mathbb{N} \rightarrow \mathbb{N}$ è la funzione induttivamente definita da $0!! = 1$, $1!! = 1$ e dalla condizione induttiva $(n+2)!! = (n+2)(n!!)$. Anche in questo caso è facile trovare una “formula chiusa”, poiché

$$n!! = n(n-2)!! = n(n-2)(n-4)!! = \dots = n(n-2)(n-4)\dots(n-2i)\dots \begin{cases} 0!! & \text{se } n \text{ pari} \\ 1!! & \text{se } n \text{ dispari} \end{cases}$$

e dunque si tratta del prodotto dei numeri pari o dei numeri dispari minori o uguali ad n a seconda che n sia pari o dispari. Come mai abbiamo usato due “condizioni di base”?

4.8.2. NUMERI DI FIBONACCI. I numeri di Fibonacci sono definiti dalle condizioni seguenti: $F(0) = 0$, $F(1) = 1$ e ricorsivamente $F(n+2) = F(n+1) + F(n)$. Si tratta di una funzione $F : \mathbb{N} \rightarrow \mathbb{N}$ che ha la caratteristica di crescere molto velocemente (in modo immaginifico, si tratta della crescita di una popolazione di organismi immortali che ad ogni generazione aumenta di numero in modo pari alla somma delle due popolazioni precedenti). I primi numeri di Fibonacci sono i seguenti:

n	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
$F(n)$	0	1	1	2	3	5	8	13	21	34	55	89	144	233	377	610	987	1597	2584	4181	6765	10946

Esiste una formula chiusa per trovare l' n -esimo numero di Fibonacci, data da

$$F(n) = \frac{\lambda_+^n - \lambda_-^n}{\lambda_+ - \lambda_-} = \frac{1}{2^{n-1}} \sum_{\substack{i=1 \\ i \text{ dispari}}}^n \binom{n}{i} 5^{\frac{i-1}{2}}$$

ove $\lambda_{\pm} = \frac{1 \pm \sqrt{5}}{2}$ ma trovarla con metodi elementari non è facile.

4.8.3. Qual'è la funzione definita da $M(0) = 0$ ed $M(n) = n - M(n-1)$?

4.9. INDUZIONE DOPPIA. L'induzione si basa essenzialmente sulle proprietà d'ordine dell'insieme \mathbb{N} ; analogamente si possono sfruttare proprietà d'ordine sull'insieme $\mathbb{N}^2 = \mathbb{N} \times \mathbb{N}$ per ottenere tecniche di dimostrazione di enunciati o di definizione di oggetti indicati da coppie di numeri naturali.

4.9.1. COEFFICIENTI BINOMIALI. I coefficienti binomiali $\binom{n}{k}$ possono essere definiti ricorsivamente per $n \geq 0$ e $0 \leq k \leq n$ nel seguente modo: $\binom{n}{0} = \binom{n}{n} = 1$ per ogni n , e $\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1}$. Questa è la formula che permette di costruire il ben noto triangolo di Tartaglia

$k \backslash n$	0	1	2	3	4	5	6	7	8	9	10
0	1	1	1	1	1	1	1	1	1	1	1
1		1	2	3	4	5	6	7	8	9	10
2			1	3	6	10	15	21	28	36	45
3				1	4	10	20	35	56	84	110
4					1	5	15	35	70	126	210
5						1	6	21	56	126	252
6							1	7	28	84	210
7								1	8	36	120
8									1	9	45
9										1	10
10											1

e si può dimostrare per induzione che questa definizione restituisce quella combinatorica già incontrata: $\binom{n}{k} = \frac{n!}{k!(n-k)!}$. Qual'è l'interpretazione combinatorica della uguaglianza induttiva del triangolo di Tartaglia?

5. Permutazioni.

5.1. DEFINIZIONE (GRUPPO). Un gruppo G è un magma associativo con elemento neutro in cui ogni elemento è simmetrizzabile. Un gruppo si dice commutativo o abeliano se è commutativo

in quanto magma. Esplicitamente dunque un gruppo è un insieme munito di una operazione $*$: $G \times G \rightarrow G$ soddisfacente alle proprietà seguenti:

- (G1) associatività: $a * (b * c) = (a * b) * c$ per ogni $a, b, c \in G$;
 (G2) elemento neutro: esiste $\iota \in G$ tale che $a * \iota = a = \iota * a$ per ogni $a \in G$;
 (G3) esistenza dei simmetrici: per ogni $a \in G$ esiste $a^* \in G$ tale che $a * a^* = \iota = a^* * a$;
 si tratta di un gruppo abeliano se inoltre vale la
 (G4) commutatività: $a * b = b * a$ per ogni $a, b \in G$.

Una funzione $f : G \rightarrow H$ tra due gruppi si dice un omomorfismo di gruppi o funzione di gruppi se rispetta le operazioni, ovvero se $f(g * g') = f(g) * f(g')$ per ogni $g, g' \in G$ (si osservi che allora l'elemento neutro di G viene mandato nell'elemento neutro di G').

Piccole conseguenze algebriche:

5.1.1. SIMMETRICI DEI PRODOTTI. Per ogni $a, b \in G$ vale che $(a * b)^* = b^* * a^*$ (il simmetrico di un prodotto è il prodotto dei simmetrici nell'ordine inverso). Infatti $(b^* * a^*) * (a * b) = b^* * (a^* * a) * b = b^* * b = \iota$, e anche in ordine inverso.

5.1.2. SIMMETRICI DEI SIMMETRICI. Per ogni $a \in G$ vale che $(a^*)^* = a$ (il simmetrico del simmetrico è l'elemento stesso). Infatti $a^{**} * a^* = (a * a^*)^* = \iota^* = \iota$, e anche in ordine inverso.

5.1.3. GRUPPO ASSOCIATO AD UN MONOIDE INTEGRO. Ad ogni monoide integro M (magma associativo, unitario, commutativo ed integro) si può associare un gruppo (necessariamente abeliano) "aggiungendo i simmetrici di tutti gli elementi che non ce l'abbiano già". Per fare questo si considera l'insieme $M \times M$ e la relazione di equivalenza in esso definita da $(m, n) \sim (x, y)$ se e solo se $m * y = n * x$. Le classi di equivalenza formano allora un gruppo con l'operazione (ben) definita da $(m, n) * (x, y) = (m * x, n * y)$; elemento neutro è la classe di (ι, ι) , simmetrica della classe (m, n) è la classe (n, m) .

La funzione che ad ogni $m \in M$ associa la classe di (m, ι) dà un morfismo iniettivo di monoidi da M al gruppo associato ad M .

5.1.4. CONGRUENZE E SOTTOGRUPPI NORMALI. Una relazione di equivalenza R in un gruppo G si dice una congruenza se lo è nel senso dei magmi, cioè se aRb implica $(a * c)R(b * c)$ per ogni $c \in G$, o equivalentemente se aRb e $a'Rb'$ implicano che $(a * a')R(b * b')$.

Contrariamente al caso dei magmi (o anche dei monoidi), una congruenza R su un gruppo G è completamente determinata dalla classe dell'elemento neutro. Detta infatti H la classe $[\iota]_R$, si tratta di un sottinsieme di G dotato delle seguenti proprietà: esso è non vuoto, se $a, b \in H$ allora $a * b^* \in H$ (in particolare $\iota \in H$), se $a \in H$ e $b \in G$ allora $b^* * a * b \in H$. Un tale sottinsieme di G si chiama di solito un sottogruppo normale di G . Ad ogni sottogruppo normale H di G è associata una relazione di equivalenza per cui la classe di congruenza è esattamente H : essa è definita dalla condizione aRb se e solo se $a * b^* \in H$.

Le funzioni che ad ogni relazione di congruenza associa la classe dell'elemento neutro, e che ad ogni sottogruppo normale associa la corrispondente relazione di congruenza sono una l'inversa dell'altra. Anche nel caso dei magmi o dei monoidi queste funzioni potevano essere definite, ma non sarebbero state delle biiezioni una inversa dell'altra.

L'esempio fondamentale di gruppi è dato dai gruppi di permutazioni su n oggetti:

5.2. DEFINIZIONE (PERMUTAZIONI). Una permutazione su n oggetti è una applicazione biiettiva di \mathbf{n} in sè. L'insieme delle permutazioni su n oggetti si indica con \mathfrak{S}_n (e chiamato anche gruppo simmetrico) ed è un gruppo sotto l'operazione di composizione; elemento neutro è l'applicazione identica, simmetrico di un elemento dato è la funzione inversa. Si tratta di un gruppo, non commutativo se $n > 2$, di cardinalità $n!$.

5.2.1. RAPPRESENTAZIONE DELLE PERMUTAZIONI. Studiando le permutazioni è tradizione usare l'insieme $\{1, 2, \dots, n\}$ (piuttosto che \mathbf{n}). Una permutazione è in effetti una funzione biiettiva, e per facilitare i calcoli algebrici viene utile usare la seguente rappresentazione: se σ è la permutazione, la descriveremo completamente tramite la tabella

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}.$$

Quindi per esempio $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$ indica la permutazione identica di \mathfrak{S}_4 , $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$ indica la permutazione che manda 1 in 2, 2 in 3, 3 in 4, 4 in 1. Calcolare la composizione di due permutazioni in questa

forma diventa facile, ma per tradizione si calcola prima la permutazione “a sinistra” nella scrittura; così se $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$ e $\sigma' = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$ abbiamo allora

$$\sigma \circ \sigma' = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix} \text{ e } \sigma' \circ \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix} .$$

5.2.2. CICLI. Un ciclo è una permutazione in \mathfrak{S}_n che lascia fissi $n - m$ elementi e i restanti m si possono ordinare in modo tale che ognuno sia mandato nel successivo (e l'ultimo nel primo, di conseguenza). L'intero m si dice lunghezza del ciclo (un ciclo di lunghezza 1 è dunque l'identità, e non si dice). Se un ciclo σ ha lunghezza m , allora σ^m è l'identità, e nessun σ^l con $l < m$ è l'identità (per questo m si dice anche periodo del ciclo).

Si osservi che la composizione di due cicli di solito non è un ciclo.

Usualmente per rappresentare un ciclo si scrive semplicemente la sequenza nell'ordine del ciclo degli elementi che non sono fissi; per esempio $(2, 4, 1)$ rappresenta in \mathfrak{S}_n il 3-ciclo che manda 2 in 4, 4 in 1 e 1 in 2, lasciando fermi tutti gli altri elementi. Si noti che la scrittura non è unica: $(2, 4, 1) = (4, 1, 2) = (1, 2, 4)$.

Si osservi che cicli disgiunti (cioè tali che gli elementi mossi da uno siano fissi per l'altro) commutano tra di loro.

5.2.3. SCAMBI. I cicli di ordine due si dicono scambi. Gli scambi sono permutazioni idempotenti, e dunque autoinverse.

5.3. TEOREMA (DECOMPOSIZIONE IN CICLI). *Ogni permutazione si scrive unicamente come composizione dei suoi cicli, che sono a due a due disgiunti.*

DIMOSTRAZIONE. Data la permutazione $\sigma \in \mathfrak{S}_n$ consideriamo la relazione di equivalenza su $\{1, 2, \dots, n\}$ data da $a \sim_\sigma b$ se esiste $k \in \mathbb{Z}$ tale che $a = \sigma^k b$. Trattandosi di una relazione di equivalenza possiamo considerare la partizione associata: ogni elemento della partizione rappresenta un ciclo, trattandosi degli elementi della forma $a, \sigma a, \sigma^2 a, \dots, \sigma^i a$. È chiaro anche che si tratta di cicli disgiunti (sono classi diverse di una partizione), e dunque commutanti tra loro. \square

5.4. TEOREMA (DECOMPOSIZIONE IN SCAMBI). *Ogni permutazione si scrive (non unicamente) come combinazione di scambi.*

DIMOSTRAZIONE. Poiché ogni permutazione si decompone in cicli, basta mostrare che ogni ciclo di decompone in scambi, e a meno di cambiare i nomi agli elementi è sufficiente controllare che

$$(1, 2, 3, \dots, i-1, i) = (1, i) \circ (1, i-1) \circ \dots \circ (1, 3) \circ (1, 2) = (1, 2)(1, 3) \dots (1, i-1)(1, i) .$$

\square

5.5. TEOREMA (SEGNO). *La funzione, detta segno, $\text{sgn} : \mathfrak{S}_n \rightarrow \{\pm 1\}$ che manda una permutazione in 1 se essa si decompone in un numero pari di scambi, -1 altrimenti, è un morfismo di gruppi (usando l'operazione di prodotto in $\{\pm 1\}$). In particolare, il numero di cicli in due decomposizioni diverse di una data permutazione è determinato modulo 2 dalla permutazione (cioè ogni decomposizione in cicli di una fissata permutazione ha un numero pari oppure dispari di cicli).*

DIMOSTRAZIONE. Consideriamo per ogni permutazione $\sigma \in \mathfrak{S}_n$ il prodotto

$$s(\sigma) = \prod_{1 \leq i < j \leq n} (\sigma(j) - \sigma(i)) .$$

Ora è chiaro che $s(\sigma) = \pm s(\text{id})$ per ogni σ , poiché si tratta del prodotto di interi dello stesso modulo (cambiano eventualmente l'ordine e il segno); poniamo allora $\text{sgn}(\sigma) = s(\sigma)/s(\text{id}) \in \{\pm 1\}$. D'altra parte, se σ e σ' sono due permutazioni, abbiamo $\text{sgn}(\sigma\sigma') = \text{sgn}(\sigma)\text{sgn}(\sigma')$; infatti

$$\begin{aligned} \text{sgn}(\sigma\sigma') &= \frac{\prod_{i < j} (\sigma'\sigma(j) - \sigma'\sigma(i))}{\prod_{i < j} (j - i)} = \frac{\prod_{i < j} (\sigma(j) - \sigma(i)) \prod_{i < j} (\sigma'\sigma(j) - \sigma'\sigma(i))}{\prod_{i < j} (j - i) \prod_{i < j} (\sigma(j) - \sigma(i))} = \\ &= \text{sgn}(\sigma) \frac{\prod_{\sigma(i) < \sigma(j)} (\sigma'\sigma(j) - \sigma'\sigma(i))}{\prod_{\sigma(i) < \sigma(j)} (\sigma(j) - \sigma(i))} = \text{sgn}(\sigma)\text{sgn}(\sigma') . \end{aligned}$$

È facile vedere che per ogni scambio τ abbiamo $\text{sgn}(\tau) = -1$, e quindi per ogni decomposizione in scambi $\sigma = \tau_1 \dots \tau_r$ vale $\text{sgn}(\sigma) = (-1)^r$; quindi due decomposizioni in scambi di σ devono avere la

stessa parità. Questo assicura che la funzione così definita è proprio quella cercata, e anche che si tratti di un morfismo di gruppi. \square

5.5.1. Gli scambi hanno segno -1 ; in generale i cicli hanno segno opposto alla parità della loro lunghezza: i cicli dispari hanno segno 1 , quelli pari hanno segno -1 .

5.5.2. Il segno di una permutazione può anche essere caratterizzato come la parità del numero di scambi che bisogna fare per “riordinare gli oggetti”.

5.6. DEFINIZIONE (GRUPPO ALTERNO). *Il gruppo alterno su n elementi \mathfrak{A}_n è il sottinsieme di \mathfrak{S}_n formato dalle permutazioni di segno 1 ; esso è in effetti un gruppo con l'operazione indotta (e anzi un sottogruppo normale di \mathfrak{S}_n , e il quoziente $\mathfrak{S}_n/\mathfrak{A}_n$ è proprio $\{\pm 1\}$: perché?).*

5.6.1. Si osservi invece che le permutazioni di segno -1 non formano un gruppo.

6. Numeri Interi.

6.1. DEFINIZIONE (ANELLI). *Un anello A è un insieme dotato di due operazioni binarie, indicate come somma $(+)$ e prodotto (\cdot) o più spesso nulla), verificanti le seguenti proprietà:*

- (S) A con la somma è un gruppo commutativo, cioè:
- (S1) $(a + b) + c = a + (b + c)$ per ogni $a, b, c \in A$;
 - (S2) esiste un elemento nullo 0 tale che $a + 0 = a = 0 + a$ per ogni $a \in A$;
 - (S3) per ogni $a \in A$ esiste un elemento $a' \in A$ tale che $a + a' = 0 = a' + a$ (di solito a' si dice opposto di a e si indica con $-a$);
 - (S4) $a + b = b + a$ per ogni coppia $a, b \in A$;
- (P) $C \setminus \{0\}$ con il prodotto è un semigruppato, cioè:
- (P1) $(ab)c = a(bc)$ per ogni $a, b, c \in A$;
 - (P2) esiste un elemento unità 1 tale che $a1 = a = 1a$ per ogni $a \in A$;
- (D) il prodotto è distributivo rispetto alla somma: $a(b + c) = ab + ac$ per ogni $a, b, c \in A$.
- L'anello si dice commutativo se il prodotto è commutativo.

Una funzione $A \rightarrow B$ tra due anelli si dice un morfismo di anelli se rispetta somma e prodotto e manda l'unità di A nell'unità di B (questo non è garantito dalle precedenti condizioni, in generale).

Messe di piccoli risultati algebrici:

6.1.1. PRODOTTO PER ZERO. Risulta dalle definizioni che $a0 = 0 = 0a$ per ogni $a \in A$; infatti $a = 1a = (1 + 0)a = 1a + 0a = a + 0a$ (e anche nell'altro ordine).

6.1.2. OPPOSTO. Per ogni a abbiamo che l'opposto è $-a = (-1)a = a(-1)$; infatti $a + (-1)a = 1a + (-1)a = (1 + (-1))a = 0a = 0$ (e anche nell'altro ordine).

6.1.3. REGOLE DEI SEGNI. $a(-b) = -(ab) = (-a)b$, $(-a)(-b) = ab$ (segue dal punto precedente).

6.1.4. Un elemento a di un anello A si dice unipotente se una sua potenza non nulla dà l'unità, cioè se esiste un intero n non nullo per cui $a^n = 1$; in tal caso a è invertibile e $a^{-1} = a^{n-1}$.

Un elemento non nullo a di un anello A si dice nilpotente se una sua potenza dà lo zero, cioè se esiste un intero n per cui $a^n = 0$; in tal caso $1+a$ è invertibile e $(1+a)^{-1} = 1 - a + a^2 - \dots + (-1)^{n-1}a^{n-1}$.

Un elemento non nullo a di un anello A si dice divisore di zero se esiste un elemento non nullo b tale che $ab = 0$. I nilpotenti sono divisori di zero.

6.1.5. ANELLI INTEGRALI. Un anello si dice intero se $A \setminus \{0\}$ è intero in quanto semigruppato moltiplicativo, cioè se per ogni $a, b, c \in A$ non nullo, da $ac = bc$ (oppure $ca = cb$) segue $a = b$. Un anello intero non ha divisori di zero, né nilpotenti.

Un anello intero e commutativo si chiama un dominio.

6.1.6. ANELLI ORDINATI. Un anello si dice ordinato se in esso è definita una relazione d'ordine \leq soddisfacente alle seguenti proprietà:

- (AO1) se $a \geq b$ allora $a + c \geq b + c$ per ogni $c \in A$;
- (AO2) se $a \geq b$ e $c \geq 0$ allora $ac \geq bc$.

Dato un anello ordinato possiamo definire l'insieme degli elementi positivi $P \subseteq A$ come $P = \{a \in A \mid a > 0\}$; allora P gode delle seguenti proprietà:

- (P1) per ogni $c \in A$ non nullo si ha che $o \in P$ oppure $-c \in P$ (e non entrambe);
- (P2) P è chiuso rispetto alla somma dei suoi elementi;
- (P3) P è chiuso rispetto al prodotto dei suoi elementi.

Viceversa, dato un insieme P con le proprietà elencate, esiste un unico ordine su A per cui quello sia l'insieme dei positivi: basta definire $a \geq b$ se e solo se $a - b \in P$.

Si osservi che in ogni anello ordinato si ha che tutti i quadrati sono positivi e in particolare $1 > 0$. Di conseguenza un corpo ordinato ha infiniti elementi, poiché le somme iterate di 1 sono sempre tra loro diverse.

6.1.7. CONGRUENZE E IDEALI. Una relazione di equivalenza R su un anello A si dice di congruenza se essa rispetta entrambe le operazioni, cioè se aRb implica $(a+c)R(b+c)$, $acRbc$ e $caRcb$ per ogni $c \in R$ (o equivalentemente se aRb e $a'Rb'$ implicano $(a+a')R(b+b')$ e $aa'Rbb'$). Come nel caso dei gruppi, tali relazioni di equivalenza sono completamente individuate dalla classe $I = [0]_R$ dell'elemento nullo; tale classe è un sottinsieme di A dotato delle seguenti proprietà: non è vuoto, se $a, b \in I$ allora $a - b \in I$ (in particolare $0 \in I$), se $a \in I$ e $b \in A$ allora $ab, ba \in I$. Un tale sottinsieme di A si dice un ideale bilatero di A . Ad ogni ideale bilatero I resta associata una congruenza definita da aRb se e solo se $a - b \in I$ la cui classe di 0 risulta esattamente I .

6.1.8. IDEALI MASSIMALI. Un ideale bilatero si dice massimale se è diverso dall'anello e non è contenuto in nessun altro ideale bilatero proprio. Usando il lemma di Zorn possiamo dimostrare che ogni anello ammette ideali massimali (anche contenenti un fissato ideale bilatero proprio, o un fissato elemento non invertibile dell'anello).

6.1.9. DIVISIBILITÀ, RELAZIONE DI DIVISIBILITÀ. Dati due elementi a, b di un anello A si dice che a divide b e si scrive $a|b$ se esiste $c \in A$ tale che $ac = b$. La relazione di divisibilità è una relazione riflessiva e transitiva. In generale non è una relazione antisimmetrica, e quindi non è una relazione d'ordine; anche quando lo fosse, non sarebbe una relazione d'ordine per l'anello (perché?).

Se abbiamo due elementi $a, b \in A$ tali che $a|b$ e $b|a$ allora a e b si dicono associati e scriviamo $a \sim b$; si tratta di una relazione di equivalenza che non è in generale una congruenza. In un anello intero, due elementi a e b sono associati se e solo se "differiscono per un invertibile", cioè $a = ub$ con $u \in A$ elemento invertibile.

6.1.10. FORMULA DEL BINOMIO DI NEWTON. In ogni anello commutativo vale la seguente identità:

$$(a+b)^n = \sum_{i=0}^n \binom{n}{i} a^i b^{n-i}$$

per ogni $a, b \in A$ e ogni $n \in \mathbb{N}$. Questa formula si può dimostrare in almeno due modi. Il primo puramente combinatorico: ogni termine della forma $a^i b^{n-i}$ compare un certo numero di volte nello sviluppo del binomio, esattamente tante quante le combinazioni di i oggetti da un insieme contenente n oggetti. L'altra dimostrazione possibile è per induzione: la formula essendo vera per $n = 0, 1$, basta controllare il passo induttivo:

$$\begin{aligned} (a+b)^{n+1} &= (a+b)(a+b)^n = (a+b) \sum_{i=0}^n \binom{n}{i} a^i b^{n-i} = \sum_{i=0}^n \binom{n}{i} a^{i+1} b^{n-i} + \sum_{i=0}^n \binom{n}{i} a^i b^{n+1-i} = \\ &= \sum_{i=0}^{n+1} \left(\binom{n}{i} + \binom{n}{i-1} \right) a^i b^{n+1-i} = \sum_{i=0}^{n+1} \binom{n+1}{i} a^i b^{n+1-i} \end{aligned}$$

ove abbiamo usato l'ipotesi induttiva nel secondo passaggio, e la relazione ricorsiva del triangolo di Tartaglia nell'ultimo passaggio.

6.2. Per ogni insieme X , l'insieme potenza $\mathcal{P}(X)$ dotato delle operazioni di differenza simmetrica (come somma) e di intersezione (come prodotto) ha struttura di anello commutativo.

Il più semplice anello è quello dei numeri interi, che si può vedere come il gruppo associato al monoide \mathbb{N} con l'operazione $+$, e a cui viene estesa l'operazione di prodotto.

6.3. DEFINIZIONE (NUMERI INTERI). L'insieme \mathbb{Z} dei numeri interi è definito come l'insieme quoziente di \mathbb{N}^2 modulo la relazione di equivalenza definita da $(a, b) \sim (a', b')$ se e solo se $a + b' = a' + b$ (in \mathbb{N}); spesso la classe della coppia (a, b) si indica con $a - b$. Quest'insieme è dotato di due operazioni: (S) somma $(a - b) + (a' - b') = (a + a') - (b + b')$; (P) prodotto $(a - b)(a' - b') = (aa' + bb') - (ab' + a'b)$; queste due operazioni rendono \mathbb{Z} un anello commutativo con elemento nullo $0 - 0 (= a - a$ per ogni $a \in \mathbb{N})$, elemento identico $1 - 0 (= (a + 1) - a$ per ogni $a \in \mathbb{N})$, opposto di $a - b$ essendo $b - a$.

6.3.1. RAPPRESENTAZIONE USUALE. In effetti di solito si dice che i numeri interi sono l'insieme formato dai numeri naturali e "dai loro opposti"; si può riconoscere questa descrizione osservando che ogni intero nel senso della definizione può essere rappresentato da una coppia del tipo $(a, 0)$ e allora è un numero naturale, oppure da una coppia del tipo $(0, a)$ e allora è l'opposto di un numero naturale.

Identifichiamo \mathbb{N} con le coppie del tipo $(a, 0)$, cioè con le classi $a - 0$, tramite la funzione iniettiva $\mathbb{N} \rightarrow \mathbb{Z}$ che manda a in $a - 0 (= (a + b) - b$ per ogni $b \in \mathbb{N}$, e possiamo indicare con a anche l'immagine). D'altra parte possiamo chiamare $-\mathbb{N}$ l'immagine della funzione iniettiva $\mathbb{N} \rightarrow \mathbb{Z}$ che manda a in $0 - a (= b - (a + b)$ per ogni $b \in \mathbb{N}$, e possiamo indicare con $-a$ l'immagine). Allora risulta che \mathbb{Z} è unione di \mathbb{N} (detti i numeri interi positivi) e di $-\mathbb{N}$ (detti i numeri interi negativi). Risulta $\mathbb{Z} = \mathbb{N} \cup (-\mathbb{N})$ e $\mathbb{N} \cap (-\mathbb{N}) = \{0\}$.

6.3.2. PRODOTTO E REGOLE DEI SEGNI. In questa rappresentazione, si ricavano subito le usuali regole di calcolo del prodotto: $(-a)b = -(ab) = a(-b)$ e $(-a)(-b) = ab$. In effetti tutto segue dal fatto che $-a = (-1)a$, come s'è visto in generale per gli anelli.

6.3.3. L'unità e il suo opposto sono gli unici elementi invertibili di \mathbb{Z} .

6.3.4. INTEGRITÀ. Si verifica anche facilmente che \mathbb{Z} è anello integro, poiché ci si riduce al prodotto in \mathbb{N} .

6.3.5. ORDINE. Vi è un unico modo di estendere l'ordine di \mathbb{N} ad un ordine totale su \mathbb{Z} , dato dalla seguente definizione: $(a - b) \leq (a' - b')$ se e solo se $a + b' \leq a' + b$ (in \mathbb{N}). Si verifica allora immediatamente che i numeri negativi sono minori di zero, e che $a \leq b$ se e solo se $-b \leq -a$.

6.4. DEFINIZIONE (NORMA O VALORE ASSOLUTO DI NUMERI INTERI). La funzione $\mathbb{Z} \rightarrow \mathbb{N}$ definita da $|z| = \begin{cases} z & \text{se } z \geq 0 \\ -z & \text{se } z < 0 \end{cases}$ si dice norma o valore assoluto e soddisfa alle seguenti proprietà:

(N1) $|z| = 0$ se e solo se $z = 0$;

(N2) moltiplicatività: $|zz'| = |z||z'|$;

(N3) subaddittività: $|z + z'| \leq |z| + |z'|$ (e vale l'uguaglianza se sono entrambi positivi o entrambi negativi);

6.5. TEOREMA (DIVISIONE CON RESTO). Dati due numeri interi a e b con $b \neq 0$ esiste una unica coppia di numeri interi q, r tali che $a = qb + r$ con $0 \leq r < |b|$. Si dice che q è il quoziente e r il resto della divisione di a (dividendo) per b (divisore).

DIMOSTRAZIONE (ALGORITMO DI DIVISIONE). Basta mostrare il risultato quando a e b sono interi positivi (perché?). Possiamo procedere per induzione su a nel modo seguente: se $a = 0$, evidentemente $q = r = 0$ qualsiasi sia b . Se ora $a > 0$; se $a < b$ abbiamo ancora $q = 0$ e $r = a$; se invece $a \geq b$ abbiamo $a > a - b \geq 0$. Possiamo allora usare la seconda forma dell'induzione e supporre che esistano unici q_1 ed r_1 interi positivi tali che $a - b = q_1 b + r_1$ con $r_1 < b$; ma allora basta scegliere $q = q_1 + 1$ e $r = r_1$ per ottenere $a = qb + r$ come voluto.

L'unicità di quoziente e resto può essere dimostrata direttamente: se $a = qb + r$ con $0 \leq r < b$ e $a = q'b + r'$ con $0 \leq r' < b$, supponendo $r > r'$ la differenza dà $(q' - q)b = r - r'$ che è assurdo, poiché $b \leq (q' - q)b = r - r' < b$. Dunque dev'essere $r = r'$ e di conseguenza $q = q'$. \square

DIMOSTRAZIONE ALTERNATIVA (USANDO IL BUON ORDINAMENTO DI \mathbb{N}). Consideriamo l'insieme $R = \{a - qb : b \in \mathbb{Z}\}$; allora $R \cap \mathbb{N}$ (in quanto sottinsieme di \mathbb{N}) ha elemento minimo, che è il resto cercato. \square

6.5.1. IDEALI PRINCIPALI. Dall'esistenza della divisione con resto, si deduce che tutti gli ideali di \mathbb{Z} sono principali, cioè formati dai multipli di un unico elemento. Infatti ciò è ovvio per gli ideali banali (nullo e tutto, generati rispettivamente da 0 e 1); sia ora I un ideale non banale, e sia b il minimo positivo in I : allora $I = b\mathbb{Z}$. Infatti se $a \in I$, operando la divisione di a per b otteniamo $a = qb + r$ da cui si vede che $r \in I$; ora siccome b è il minimo elemento positivo di I , deve risultare $r = 0$ (nella divisione $r < b$), e allora a è multiplo di b .

6.6. DEFINIZIONE (MCD, mcm). Dati due numeri interi a e b definiamo un massimo comun divisore $\text{MCD}(a, b)$, spesso denotato semplicemente (a, b) , come un massimo (per il preordine di divisibilità) dei divisori comuni di a e b ; si tratta cioè di un intero d che divide sia a che b e tale che ogni divisore comune di a e b divida anche d . Due massimo comun divisori di a e b sono dunque tra loro associati.

Analogamente si definisce un minimo comune multiplo, denotato $\text{mcm}(a, b)$, come un minimo (per la divisibilità) dei multipli comuni di a e b .

6.6.1. È chiaro che MCD e mcm sono unici a meno del segno (se d e d' lo sono, allora ciascuno divide l'altro). Se chiediamo che siano interi positivi, allora sono unicamente definiti. Lo sottintenderemo sempre nel seguito.

6.6.2. RELAZIONE TRA MCD E mcm. Dati due numeri interi positivi risulta che

$$\text{mcm}(a, b)\text{MCD}(a, b) = ab ;$$

infatti posto $d = \text{MCD}(a, b)$ abbiamo $a = a'd$, $b = b'd$ (con $\text{MCD}(a', b') = 1$), da cui segue che $a'b'd = ab/d$ è un multiplo comune di a e di b ; se ora m è multiplo comune di a e di b (dunque $m = a''a$ e $m = b''b$), e fosse un divisore di $a'b'd = ab/d$ (dunque $mc = ab/d$ ovvero $mcd = ab$) avremmo che $mcd = a''acd = ab$ e $mcd = b''bcd = ab$, da cui si vede che cd sarebbe divisore comune di a e b , assurdo a meno che non sia $c = 1$.

6.6.3. $\text{MCD}(ac, bc) = c\text{MCD}(a, b)$, $\text{mcm}(ac, bc) = c\text{mcm}(a, b)$?

6.6.4. ESTENSIONE A n NUMERI INTERI. Definizioni analoghe di massimo comun divisore e minimo comune multiplo si possono dare per ogni insieme finito a_1, a_2, \dots, a_n di numeri interi. La facile relazione $\text{MCD}(a, b, c) = \text{MCD}(\text{MCD}(a, b), c)$ e più generalmente

$$\text{MCD}(a_1, a_2, \dots, a_n) = \text{MCD}(\text{MCD}(a_1, a_2, \dots, a_{n-1}), a_n)$$

riduce induttivamente il calcolo al caso di una coppia di numeri.

6.6.5. mcm. È facile vedere che un minimo comune multiplo tra due interi positivi a e b è il generatore (positivo) dell'ideale intersezione $a\mathbb{Z} \cap b\mathbb{Z}$; più generalmente abbiamo che $\text{mcm}(a_1, \dots, a_n)$ è il generatore (positivo) dell'ideale $\bigcap_{i=1}^n a_i\mathbb{Z}$.

6.7. TEOREMA (MCD). Il massimo comun divisore d tra due interi positivi a e b è il generatore (positivo) dell'ideale generato da $a\mathbb{Z} \cup b\mathbb{Z}$ (il più piccolo ideale contenente sia a che b); esistono due interi h, k tali che $d = ha + kb$, e d è il minimo intero positivo che si può scrivere in questa forma.

DIMOSTRAZIONE. Consideriamo l'insieme I dei numeri interi della forma $ma + nb$ al variare di $m, n \in \mathbb{Z}$. Si tratta chiaramente di un ideale di \mathbb{Z} , quindi si tratta dei multipli di un intero positivo d che è il minimo intero positivo di I . Poiché $a, b \in I$, abbiamo che d divide sia a che b , e dunque è un divisore comune. Inoltre per definizione esistono due interi h, k tali che $d = ha + kb$. Sia ora d' un divisore comune di a e b , diciamo $a = a'd'$ e $b = b'd'$; allora abbiamo $d = ha + kb = ha'd' + kb'd' = (ha' + kb')d'$, da cui si vede che d' divide d . \square

6.7.1. Nell'enunciato e nella sua dimostrazione si può evitare la nozione di ideale esprimendosi così: Il massimo comun divisore d tra due interi positivi a e b il minimo intero positivo che si può scrivere nella forma $d = ha + kb$ con $h, k \in \mathbb{Z}$. Infatti supponiamo che $d = ha + kb$ sia minimo e mostriamo che divide sia a che b ; se non dividesse a potremmo usare la divisione euclidea $d = aq + r$ con $r > 0$ e $r = d - aq = ((h - q)a + kb)$, assurdo perché sarebbe $r < d$.

6.7.2. Dal teorema segue che due numeri interi a e b sono primi tra loro se e solo se esistono interi h, k tali che $ha + kb = 1$.

6.7.3. Il teorema e l'osservazione precedente possono estendersi al caso di un numero finito di interi; il massimo comun divisore tra gli interi a_1, a_2, \dots, a_n è il minimo intero positivo che si scrive nella forma $h_1a_1 + h_2a_2 + \dots + h_na_n$ con gli h_i interi. Inoltre essi sono coprimi (cioè il loro massimo comun divisore è 1) se e solo se esistono degli interi h_i tali che $h_1a_1 + h_2a_2 + \dots + h_na_n = 1$.

6.7.4. RELAZIONE DI BÉZOUT. I combinatori interi h e k che esprimono d come $ha + kb$ non sono unici, ma se si impone loro di soddisfare certe condizioni di minimalità, allora sono ben determinati e la relazione $d = ha + kb$ si dice di Bézout. La condizione è questa: se $a \geq b$, $a = da'$, $b = db'$ allora possiamo chiedere che $|h| < |b'|$ e $|k| < |a'|$. Combinatori con questa proprietà sono forniti dall'algoritmo di Euclide.

6.8. ALGORITMO DI EUCLIDE. Dalla dimostrazione non è chiaro in effetti come procedere per calcolare il massimo comun divisore tra due numeri, né come calcolare i coefficienti h e k . Un metodo per fare ciò è l'algoritmo di Euclide che ora presentiamo. L'idea fondamentale è semplice, e può dare un'altra dimostrazione del Teorema precedente: se $a = bq + r$ è la divisione euclidea di a per b , allora

$\text{MCD}(a, b) = \text{MCD}(b, r)$, con il vantaggio che nel secondo termine dell'uguaglianza abbiamo numeri più piccoli; ripetendo questo procedimento un numero finito (perché?) di volte si ottiene il risultato voluto (perché?).

Siano a e b due numeri interi positivi di cui vogliamo calcolare il massimo comun divisore (si tratta evidentemente di trovare il generatore positivo dell'ideale generato dai due). Poniamo le seguenti definizioni ricorsive: $a_1 = a, a_2 = b, a_i = a_{i+1}q_i + a_{i+2}$ (divisione con resto di a_i per a_{i+1} , che dunque definisce il quoziente q_i e il resto a_{i+2} avente la proprietà d'essere minore di a_{i+1}). Dunque abbiamo la sequenza:

$$a_1 = a, \quad a_2 = b, \quad a_3 = a_1 - q_1 a_2, \quad \dots, \quad a_{i+2} = a_i - q_i a_{i+1}, \quad \dots$$

Ora è chiaro che ad ogni passo la sequenza a_i al variare di i diminuisce (strettamente), e dunque esiste un n tale che $a_n \neq 0$ ma $a_{n+1} = 0$; allora $d = a_n$. Infatti svolgendo a ritroso le uguaglianze $a_{i+2} = a_i - a_{i+1}q_i$ si vede che a_n si scrive come richiesto nella dimostrazione, dunque appartiene all'ideale cercato I ; e d'altra parte dal fatto che a_n divide a_{n-1} , sempre andando a ritroso si vede che a_n divide a_i per ogni $i \leq n$, ed in particolare divide sia a che b .

Per tener conto dei coefficienti senza fare i conti a ritroso, conviene ricorrere alla usuale tabellina, ricorsivamente definita in modo che ad ogni passo si abbia $a_i = h_i a_1 + k_i a_2$:

$a_1 = a$	$h_1 = 1$	$k_1 = 0$	
$a_2 = b$	$h_2 = 0$	$k_2 = 1$	
a_3	$h_3 = 1$	$k_3 = -q_1$	$[a_1 = q_1 a_2 + a_3]$
a_4	$h_4 = -q_2 h_3 = -q_2$	$k_4 = 1 - q_2 k_3 = 1 + q_1 q_2$	$[a_2 = q_2 a_3 + a_4]$
\vdots	\vdots	\vdots	\vdots
a_{i+2}	$h_{i+2} = h_i - q_i h_{i+1}$	$k_{i+2} = k_i - q_i k_{i+1}$	$[a_i = q_i a_{i+1} + a_{i+2}]$
\vdots	\vdots	\vdots	\vdots
a_n	$h_n = h_{n-2} - q_{n-2} h_{n-1}$	$k_n = k_{n-2} - q_{n-2} k_{n-1}$	$[a_{n-2} = q_{n-2} a_{n-1} + a_n]$
0			$[a_{n-1} = q_{n-1} a_n]$

6.8.1. Il lettore è invitato a farsi qualche esempio di divisione tra interi e di calcolo di MCD tra interi.

6.8.2. NOTA SULL'ALGORITMO. Probabilmente il lettore ha studiato come calcolare MCD e mcm tra numeri interi passando attraverso la fattorizzazione in primi; il punto è che fattorizzare un numero intero in primi non è facile, se non nei casi di numeri piccoli, mentre l'algoritmo di Euclide per il calcolo del MCD è un procedimento molto veloce anche in presenza di numeri grandi.

6.9. TEOREMA (FONDAMENTALE DELL'ARITMETICA: PRIMI E FATTORIZZAZIONE). *Un numero intero positivo diverso dall'unità si dice primo se è divisibile solo per 1 e per se stesso. Ogni numero intero positivo si scrive in modo essenzialmente unico come prodotto di primi (essenzialmente significa a meno dell'ordine).*

DIMOSTRAZIONE. Si può fare usando la seconda forma dell'induzione; infatti la proprietà è ovvia per 1 e per tutti i numeri primi. Se ora n è un numero maggiore di 1 e non primo, esso si esprime come prodotto $m'm''$ di due interi positivi, ciascuno minore di m ; dunque per ipotesi induttiva essi ammettono una fattorizzazione come nell'enunciato, e di conseguenza anche m (facendo il prodotto delle fattorizzazioni).

Per dimostrare l'unicità della fattorizzazione basta applicare a due distinte fattorizzazioni di uno stesso intero positivo il seguente risultato: *se p è un primo, e p divide un prodotto ab , allora p divide almeno uno dei due fattori; quindi per induzione: se p divide un prodotto di interi, allora p divide almeno uno dei fattori.* Supponiamo infatti che p divida ab , ma non divida a , e proviamo che divide b ; siccome a e p sono coprimi abbiamo $1 = ah + pk$ per opportuni interi h, k . Moltiplicando per b otteniamo $b = abh + pbk$, e poiché $ab = pl$ (per ipotesi p divide ab) risulta $b = plh + pbk = p(lh + bk)$, e dunque p divide b , come si voleva. □

Parlando di polinomi, e di particolari tipi di anelli (principali e fattoriali) vedremo che la stessa proprietà si poteva dimostrare usando solo il fatto che gli ideali di \mathbb{Z} sono principali.

6.9.1. PROBLEMA. Si generalizzi la proprietà usata nella dimostrazione di unicità della fattorizzazione nel seguente modo: *se a divide un prodotto bc e a è primo con b , allora a divide c .*

6.9.2. INFINITÀ DEI NUMERI PRIMI. È ben noto dall'antichità che i numeri primi sono infiniti. Ricordiamo una delle prime e più semplici verifiche di questo fatto: se per assurdo vi fosse solo un numero finito di primi, allora il numero intero ottenuto sommando 1 al prodotto di tutti questi primi sarebbe maggiore di ciascuno dei primi dati, e non divisibile per alcuno di essi.

6.9.3. CALCOLI DI MCD E mcm TRAMITE FATTORIZZAZIONE. Dati due numeri interi a e b e la loro fattorizzazione in primi $a = \pm p_1^{r_1} \cdots p_i^{r_i} p_{i+1}^{r_{i+1}} \cdots p_m^{r_m}$ e $b = \pm p_1^{s_1} \cdots p_i^{s_i} q_{i+1}^{s_{i+1}} \cdots q_n^{s_n}$ (ove si intende che lettere diverse indicano primi distinti) allora possiamo determinare massimo comun divisore e minimo comune multiplo nel modo seguente: $\text{MCD}(a, b) = p_1^{\min(r_1, s_1)} \cdots p_i^{\min(r_i, s_i)}$ (prodotto dei fattori comuni con il minimo esponente) e $\text{mcm}(a, b) = p_1^{\max(r_1, s_1)} \cdots p_i^{\max(r_i, s_i)} p_{i+1}^{r_{i+1}} \cdots p_m^{r_m} q_{i+1}^{s_{i+1}} \cdots q_n^{s_n}$ (prodotto di tutti i fattori con il massimo esponente).

6.10. CONGRUENZE, ANELLI MODULO. Fissato un intero m , due numeri interi a e b si dicono congrui modulo m e si scrive $a \equiv b \pmod{m}$ se $a - b$ è divisibile per m . Si tratta di una relazione di equivalenza, e anzi di congruenza poiché è definita in termini dell'ideale $m\mathbb{Z}$.

L'anello quoziente $\mathbb{Z}/m\mathbb{Z}$ delle classi resto per la relazione di congruenza modulo m ha un numero finito di elementi (esattamente m) e può essere descritto in termini delle classi degli interi da 0 a $m-1$. La classe dell'intero a è descritta come $[a]_m = \{a + im \mid i \in \mathbb{Z}\}$.

Si osservi che se m non è primo allora $\mathbb{Z}/m\mathbb{Z}$ contiene divisori di zero: infatti se $m = ab$ in \mathbb{Z} , allora $[a]_m \neq 0 \neq [b]_m$, ma $[a]_m [b]_m = [ab]_m = [m]_m = [0]_m$. Vedremo che se m è primo, allora le classi modulo m formano un anello integro, ed anzi un corpo (ogni elemento non nullo è invertibile).

6.10.1. In questo tipo di anelli bisogna fare particolare attenzione trattando di equazioni, anche lineari; per esempio può succedere che “una equazione di primo grado $aX = b$ nella incognita X ” abbia due soluzioni. Per esempio $aX = 0$ in $\mathbb{Z}/(ab)\mathbb{Z}$ ha come soluzioni sia la classe di 0, sia la classe di b (che sono diverse tra loro). Una interpretazione geometrica di questo fatto può essere la seguente: nel “piano” $(\mathbb{Z}/(ab)\mathbb{Z})^2$ (formato da $a^2 b^2$ “punti”) le due “rette” di equazioni $Y = aX$ e $Y = 0$ pur essendo distinte si incontrano in due punti distinti, l'origine $(0, 0)$ e il punto $(b, 0)$. Queste osservazioni sconsigliano dunque di fare geometria “ingenua” sugli anelli.

6.10.2. Si osservi anche che ogni anello resto, come pure ogni anello con un numero finito di elementi, non può essere ordinato.

6.10.3. RELAZIONI TRA CONGRUENZE DIVERSE. Si osservi che:

- (a) se $a \equiv b \pmod{m}$ e m' divide m allora $a \equiv b \pmod{m'}$;
- (b) se $a \equiv b \pmod{m}$ allora $ac \equiv bc \pmod{(m, c)}$ (ovvio);
- (c) se $ac \equiv bc \pmod{m}$ allora $a \equiv b \pmod{m/(m, c)}$ (questo è meno ovvio: conviene vederlo nella forma $ac \equiv 0 \pmod{m}$, e allora abbiamo $c = c'(m, c)$, $m = m'(m, c)$ con $(m', c') = 1$. Allora risulta che m divide ac , dunque m' divide ac' , e quindi m' divide a).

6.10.4. TEOREMA (SOLUZIONI DI CONGRUENZE). Consideriamo una congruenza $aX \equiv b \pmod{m}$ con $a, b \in \mathbb{Z}$ e X una incognita; allora esistono soluzioni (cioè valori $x \in \mathbb{Z}$ che soddisfano alla congruenza) se e solo se (a, m) divide b , e in tal caso tutte e sole le soluzioni sono date da $x_0 + \frac{m}{(m, a)}k$ ove $k \in \mathbb{Z}$ e x_0 è una soluzione qualsiasi (si tratta della classe laterale modulo $\frac{m}{(m, a)}$ di una qualsiasi soluzione).

DIMOSTRAZIONE. Supponiamo che esista una soluzione x_0 ; allora abbiamo $ax_0 = b + km$ per qualche $k \in \mathbb{Z}$, da cui $b = ax_0 - km$ e quindi b deve essere un multiplo del MCD tra a e m . Viceversa, supponiamo $b = c(m, a)$; poiché $(m, a) = hm + ka$, troviamo $b = c(hm + ka) = chm + cka$, e dunque $x_0 = ck$ è una soluzione cercata.

Se ora x_0 è una soluzione ($ax_0 \equiv b \pmod{m}$), e x è un'altra soluzione ($ax \equiv b \pmod{m}$), abbiamo $ax \equiv ax_0 \pmod{m}$, e quindi $a(x - x_0) \equiv 0 \pmod{m}$, da cui si deduce che $x - x_0$ è un multiplo di $\frac{m}{(m, a)}$, come si voleva. \square

♠ **6.10.5. TEOREMA (CINESE DEL RESTO).** Siano m_1, m_2, \dots, m_r numeri interi a due a due coprimi; allora il sistema di congruenze $X \equiv a_i \pmod{m_i}$ per $i = 1, 2, \dots, r$ ammette soluzioni nell'incognita X , e l'insieme delle soluzioni è dato dagli interi appartenenti ad una classe di \mathbb{Z} modulo $\prod_i m_i$.

DIMOSTRAZIONE. Osserviamo che il minimo comune multiplo tra gli m_i è esattamente il loro

prodotto (per l'ipotesi di coprimialità). Consideriamo allora la funzione di anelli

$$\mathbb{Z}/(\prod_i m_i)\mathbb{Z} \longrightarrow (\mathbb{Z}/m_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/m_r\mathbb{Z})$$

che manda $[x]_m$, se $m = \prod_i m_i$, in $([x]_{m_1}, \dots, [x]_{m_r})$. Si tratta di una funzione iniettiva tra insiemi finiti della stessa cardinalità. Essa è dunque anche suriettiva, ed è quanto afferma il teorema. \square

6.10.6. INVERTIBILI NEGLI ANELLI DI INTERI MODULO n . Un elemento non nullo \bar{x} dell'anello $\mathbb{Z}/m\mathbb{Z}$ è invertibile se e solo se esiste $y \in \mathbb{Z}$ tale che $\overline{xy} = \bar{1}$, ovvero $xy \equiv 1 \pmod{m}$, dunque se e solo se esistono $y, z \in \mathbb{Z}$ tali che $xy + zm = 1$. Questo significa esattamente che x e m sono primi tra loro: dunque la classe di $x \in \mathbb{Z}$ è invertibile modulo m (cioè in $\mathbb{Z}/m\mathbb{Z}$) se e solo se x è primo con m .

♠ 6.10.7. FUNZIONE DI EULERO. La funzione $\Phi : \mathbb{N} \rightarrow \mathbb{N}$ di Eulero è definita associando ad ogni numero naturale n il numero di elementi invertibili in $\mathbb{Z}/n\mathbb{Z}$, ovvero per $n > 1$ la cardinalità dell'insieme dei numeri minori di n ad esso coprimi. È facile calcolare i primi valori:

n	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
$\Phi(n)$	2	1	1	2	2	4	2	6	4	6	4	10	4	12	6	10	8	16	6	18	8

ed in effetti si possono determinare con le seguenti osservazioni:

- (1) caso di numeri primi p : se p è un primo, allora $\Phi(p) = p - 1$; infatti tutti i numeri naturali non nulli minori di p sono primi con p ;
- (2) proprietà moltiplicativa per numeri coprimi: se $n, n' \in \mathbb{N}$ e $(n, n') = 1$, cioè n ed n' sono primi tra loro, allora $\Phi(nn') = \Phi(n)\Phi(n')$; questo si può vedere direttamente, ma segue anche dalla dimostrazione vista del teorema cinese del resto, che dice che $\mathbb{Z}/(nn')\mathbb{Z} \cong (\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/n'\mathbb{Z})$, studiando gli invertibili dell'anello prodotto (sono le coppie formate da elementi invertibili di ciascun anello);
- (3) potenze di numeri primi: consideriamo ora p^r con p primo; i numeri naturali minori di p^r e primi con esso sono esattamente quelli non divisibili per p , dunque vale

$$\Phi(p^r) = p^r - p^{r-1} = p^{r-1}(p - 1) = p^r \left(1 - \frac{1}{p}\right).$$

Ora per un qualsiasi numero naturale n , possiamo ricorrere alla sua fattorizzazione in numeri primi $n = \prod_i p_i^{r_i}$ e di conseguenza calcolare

$$\Phi(n) = \prod_i p_i^{r_i-1}(p_i - 1) = n \prod_i \left(1 - \frac{1}{p_i}\right).$$

♠ 6.10.8. Si può provare, per esempio per induzione sul numero di primi nella fattorizzazione di n , l'uguaglianza

$$\sum_{d|n} \Phi(d) = n$$

ove la sommatoria è estesa a tutti i divisori di n (compresi 1 ed n). Si osservi che questa formula può anche essere usata come definizione induttiva (nella seconda forma) della funzione di Eulero.

♠ 6.10.9. FUNZIONE DI MOEBIUS. La funzione di Moebius $\mu : \mathbb{N} \rightarrow \{0, \pm 1\}$ è definita per ogni numero naturale nel modo seguente:

$$\mu(n) = \begin{cases} 1 & \text{se } n = 1 \text{ oppure } n \text{ si fattorizza in un numero pari di primi distinti} \\ 0 & \text{se nella fattorizzazione di } n \text{ vi sono dei primi ripetuti} \\ -1 & \text{se } n \text{ si fattorizza in un numero dispari di primi distinti} \end{cases}$$

ed è ovvio constatare che se n ed m sono coprimi allora $\mu(nm) = \mu(n)\mu(m)$ (se non sono coprimi abbiamo banalmente $\mu(nm) = 0$).

Si può esprimere la funzione di Eulero in termini della funzione di Moebius:

$$\Phi(n) = \sum_{d|n} \mu(d) \frac{n}{d}$$

per qualsiasi $n \in \mathbb{N}$.

7. Corpi numerici.

7.1. DEFINIZIONE (CORPO). Un corpo C è un anello in cui ogni elemento non nullo ammette un inverso; in dettaglio si tratta di un insieme dotato di due operazioni binarie, indicate come somma (+) e prodotto (\cdot o più spesso nulla), verificanti le seguenti proprietà:

- (S) C con la somma è un gruppo commutativo, cioè:
- (S1) $(a + b) + c = a + (b + c)$ per ogni $a, b, c \in C$;
 - (S2) esiste un elemento nullo 0 tale che $a + 0 = a = 0 + a$ per ogni $a \in C$;
 - (S3) per ogni $a \in C$ esiste un elemento $a' \in C$ (detto opposto di a e indicato con $-a$) tale che $a + a' = 0 = a' + a$;
 - (S4) $a + b = b + a$ per ogni coppia $a, b \in C$;
- (P) $C \setminus \{0\}$ con il prodotto è un gruppo, cioè:
- (P1) $(ab)c = a(bc)$ per ogni $a, b, c \in C$;
 - (P2) esiste un elemento unità 1 tale che $a1 = a = 1a$ per ogni $a \in C$;
 - (P3) per ogni $a \in C$ diverso da 0 esiste un elemento $a'' \in C$ (detto inverso di a e indicato con a^{-1}) tale che $aa'' = 1 = a''a$;
- (D) il prodotto è distributivo rispetto alla somma: $a(b + c) = ab + ac$ per ogni $a, b, c \in C$.

Il corpo si dice commutativo se il prodotto è commutativo; spesso un corpo commutativo si dice un campo.

Una funzione tra due corpi si dice un morfismo di corpi se rispetta le operazioni di somma e prodotto dei due corpi.

Messe di piccoli risultati algebrici:

7.1.1. LEGGI DI CANCELLAZIONE. In ogni corpo vale che $ac = bc$ con $c \neq 0$ implica $a = b$; infatti basta moltiplicare per l'inverso di c .

7.1.2. PRINCIPIO DI ANNULLAMENTO DEL PRODOTTO. In ogni corpo vale che $ab = 0$ implica $a = 0$ oppure $b = 0$; infatti, se $a \neq 0$ basta moltiplicare per l'inverso di a per ottenere $b = 0$.

7.1.3. Un corpo non ha divisori di zero né nilpotenti: segue dall'osservazione precedente.

7.1.4. CORPI ORDINATI. Un corpo si dice ordinato se lo è in quanto anello. Se C è un corpo ordinato e $x \in C$, da $x > 0$ segue che $x^{-1} > 0$.

7.1.5. Talvolta si accetta che anche $\{0\}$ (insieme con un solo elemento e con l'unica struttura possibile di gruppo) sia un corpo con identità uguale a zero.

7.2. NUMERI RAZIONALI. L'insieme dei numeri razionali \mathbb{Q} è il più piccolo corpo contenente l'anello \mathbb{Z} dei numeri interi (in modo che le operazioni in \mathbb{Q} estendano quelle di \mathbb{Z}). Si può costruire nel modo seguente: si consideri in $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ la relazione \sim di equivalenza definita da $(a, b) \sim (x, y)$ se e solo se $ay = bx$ (in \mathbb{Z}). Verificato per bene che si tratta di una relazione di equivalenza, costruiamo l'insieme quoziente $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\}) / \sim$, ed indichiamo con la notazione familiare $\frac{a}{b}$ la classe dell'elemento (a, b) ; allora abbiamo $\frac{a}{b} = \frac{x}{y}$ se e solo se $ay = bx$.

Definiamo ora le operazioni sull'insieme quoziente nel modo usuale: il prodotto di due classi $\frac{a}{b}$ e $\frac{a'}{b'}$ sia $\frac{aa'}{bb'}$ (verificare che il risultato non dipende dai rappresentanti usati per definirlo), e la somma sia $\frac{ab' + a'b}{bb'}$ ($= \frac{ab'}{bb'} + \frac{a'b}{bb'}$) (di nuovo il risultato dipende solo dalla classe di equivalenza, e non dai rappresentanti). Con queste operazioni l'insieme quoziente risulta un corpo ove l'elemento nullo è la classe $\frac{0}{1}$ ($= \frac{0}{a}$ per ogni $a \neq 0$), l'elemento unità è la classe di $\frac{1}{1}$ ($= \frac{a}{a}$ per ogni $a \neq 0$) e l'inverso per $\frac{a}{b}$ se $a \neq 0$ è la classe $\frac{b}{a}$.

7.2.1. ORDINE IN \mathbb{Q} . Possiamo anche rendere \mathbb{Q} un corpo ordinato definendo l'insieme degli elementi positivi come le classi $\frac{b}{a}$ con $a, b \in \mathbb{N}$ (i positivi di \mathbb{Z}).

7.2.2. PROPRIETÀ ARCHIMEDEA DI \mathbb{Q} . Il corpo ordinato dei razionali gode della seguente proprietà: per ogni coppia a, b di razionali maggiori di 0 , esiste un intero positivo n tale che $na > b$.

7.3. CORPO DEI QUOZIENTI PER DOMINI. La strategia utilizzata per costruire \mathbb{Q} a partire da \mathbb{Z} può essere generalizzata nel modo seguente: se A è un qualsiasi dominio (anello commutativo ed integro), allora l'insieme quoziente di $A \times (A \setminus \{0\})$ modulo la relazione di equivalenza definita da $(a, b) \sim (x, y)$ se e solo se $ay = bx$ (in A) ha una struttura di corpo (detto corpo dei quozienti di A) quando sia dotato delle operazioni definite da $\frac{a}{b} \frac{a'}{b'} = \frac{aa'}{bb'}$ (prodotto) e $\frac{a}{b} + \frac{a'}{b'} = \frac{ab' + a'b}{bb'}$ (somma) ove $\frac{a}{b}$ indica la classe di (a, b) .

L'ipotesi che l'anello sia integro è importante affinché la relazione definita per fare il quoziente sia in effetti una relazione di equivalenza.

7.4. NUMERI REALI. L'insieme \mathbb{R} dei numeri reali può essere definito come il completamento ordinale del corpo dei numeri razionali \mathbb{Q} ; esso verrà studiato dettagliatamente un altro corso. Ricordiamo solo che \mathbb{R} può essere definito come l'unico gruppo (per la somma) archimedeo completo (a meno di isomorfismi ordinati: vedi Barsotti), o anche l'unico corpo totalmente ordinato e completo per l'ordine (sempre a meno di isomorfismi ordinati: vedi De Marco).

7.4.1. AUTOMORFISMI DI \mathbb{R} . Per comodità ricordiamo anche che l'unico automorfismo di corpo di \mathbb{R} è l'identità; ciò si dimostra nel modo seguente: prima di tutto è facile vedere che un'automorfismo di \mathbb{R} dev'essere l'identità su \mathbb{Z} e quindi su \mathbb{Q} ; poi si verifica che manda l'insieme dei positivi nell'insieme dei positivi, e di conseguenza è crescente. Infine per un elemento $x \in \mathbb{R} \setminus \mathbb{Q}$ si consideri la sua immagine x' , e si supponga $x' \neq x$, per esempio $x' > x$; si scelga $q \in \mathbb{Q}$ tale che $x' > q > x$ (densità di \mathbb{Q} in \mathbb{R}). Allora calcolando le immagini abbiamo $q = q' > x' > q$, assurdo.

7.5. CORPI FINITI. Consideriamo ora in \mathbb{Z} la relazione di congruenza modulo p ; allora l'insieme quoziente $\mathbb{Z}/p\mathbb{Z}$, con le due operazioni ereditate da \mathbb{Z} , è un corpo se e solo se p è un numero primo. Infatti, se p è primo, per ogni $n \in \mathbb{Z}$ non multiplo di p abbiamo che $(n, p) = 1$ (sono coprimi) e dunque esistono interi x, y tali che $xn + yp = 1$; ma allora la classe di x è l'inverso della classe di n . Se invece p non è primo, nell'anello quoziente si trovano dei divisori di zero, come abbiamo già visto.

7.5.1. Indichiamo con \mathbb{F}_p il corpo $\mathbb{Z}/p\mathbb{Z}$ se p è primo; si tratta di un insieme con p elementi dotato della struttura di corpo. Invitiamo il lettore a scrivere le tabelle di somma e moltiplicazione per $p = 2, 3, 5, 7$.

I corpi finiti non sono ordinati.

7.5.2. Si osservi che per ogni $x \in \mathbb{F}_p$ si ha $x^p = x$.

7.6. CARATTERISTICA DEI CORPI. Dato un corpo C qualsiasi, possiamo considerare l'unica mappa di anelli $\mathbb{Z} \rightarrow C$ (definita dal fatto di mandare 1 di \mathbb{Z} nell'1 di C). Se si osserva l'antimmagine in \mathbb{Z} dello zero (di C), vi sono due possibilità:

- (0) tale insieme contiene solo lo zero; in tal caso la funzione è iniettiva, il corpo C contiene una copia di \mathbb{Z} e dunque di \mathbb{Q} . In questo caso il corpo C si dice di caratteristica zero.
- (p) tale insieme contiene tutti i multipli di un fissato primo p ; in tal caso la funzione si fattorizza attraverso una mappa iniettiva $\mathbb{Z}/p\mathbb{Z} \rightarrow C$, e il corpo C contiene una copia di $\mathbb{Z}/p\mathbb{Z}$. In questo caso il corpo C si dice di caratteristica (positiva) p .

Noi abbiamo visto che esistono corpi di caratteristica p che sono finiti ed hanno esattamente p elementi; in effetti per ogni intero n esiste (ed unico a meno di isomorfismi) un corpo di caratteristica p con esattamente p^n elementi (ma non è $\mathbb{Z}/p^n\mathbb{Z}$: perché?). Inoltre esistono corpi di caratteristica $p \neq 0$ aventi infiniti elementi (farsi qualche esempio). Non possiamo per il momento giustificare queste affermazioni, che diamo solo per conoscenza, e per le quali rimandiamo ad un futuro corso di Algebra.

Abbiamo visto che ogni corpo contiene una copia del corpo dei numeri razionali (se è di caratteristica nulla) oppure una copia del corpo con p elementi (se è di caratteristica p); perciò questi corpi (\mathbb{Q} ed \mathbb{F}_p al variare di p nei numeri primi) sono detti corpi fondamentali.

7.6.1. In un corpo di caratteristica p abbiamo che $(a \pm b)^p = a^p \pm b^p$, poiché per ogni $0 < i < p$ il fattoriale $\binom{p}{i}$ è divisibile per p . Dunque l'elevamento alla potenza p è un morfismo di corpo per ogni corpo di caratteristica p , ed è l'identità sul suo sottocorpo fondamentale; si chiama endomorfismo di Frobenius.

7.7. NUMERI COMPLESSI. La costruzione dei numeri complessi parte dall'osservazione che il corpo dei numeri reali non è "algebricamente chiuso": ossia esistono delle equazioni polinomiali a coefficienti in \mathbb{R} che non ammettono soluzioni in \mathbb{R} ; l'esempio più famoso è $X^2 = -1$ (infatti se un numero è un quadrato, non può essere negativo nell'ordine di \mathbb{R}). D'altra parte si può cercare di costruire un corpo contenente \mathbb{R} e in cui quell'equazione abbia soluzione; per esempio chiamando i un numero (immaginario!) tale che $i^2 = -1$, possiamo considerare l'insieme di tutte le espressioni del tipo $a + ib$ ove a e b sono elementi di \mathbb{R} . Allora se vogliamo definire una somma ed un prodotto tra scritture di questo tipo, che rispettino le regole distributiva ed associativa, siamo costretti a porre $(a + ib) + (a' + ib') = (a+a') + i(b+b')$ e anche $(a + ib)(a' + ib') = (aa' - bb') + i(ab' + a'b)$ ("infatti" $(a + ib)(a' + ib') = aa' + aib' + iba' + i^2bb' = aa' + iab' + ia'b - bb'$). Risulta allora in effetti che

l'insieme così definito è un corpo con zero dato da $0 + i0$, unità data da $1 + i0$, in cui opposto di $a + ib$ è $-a - ib = (-a) + i(-b)$. Per ogni elemento non nullo $a + ib$, un calcolo diretto mostra che l'elemento $\frac{a}{a^2+b^2} - i\frac{b}{a^2+b^2}$ è il suo inverso. La verifica delle altre proprietà è essenzialmente ovvia.

Di solito si procede in modo più formale, e meno comprensibile, dando la definizione seguente:

7.7.1. DEFINIZIONE (NUMERI COMPLESSI). *Il corpo \mathbb{C} dei numeri complessi è l'insieme \mathbb{R}^2 dotato delle seguenti operazioni:*

$$(S) (a, b) + (a', b') = (a+a', b+b');$$

$$(P) (a, b)(a', b') = (aa' - bb', ab' + a'b).$$

Queste operazioni soddisfano agli assiomi affinché \mathbb{C} sia un corpo; in particolare lo zero è $(0, 0)$, l'identità è $(1, 0)$, opposto di (a, b) è $(-a, -b)$, inverso di (a, b) è $(\frac{a}{a^2+b^2}, -\frac{b}{a^2+b^2})$. Si osserva poi che l'elemento $(0, 1)$ ha come quadrato l'opposto dell'identità (e quindi \mathbb{C} non può essere un corpo ordinato: se 1 è positivo, -1 è negativo e non può essere un quadrato).

Si osserva infine che la funzione $\mathbb{R} \rightarrow \mathbb{C}$ che manda a in $(a, 0)$ è una funzione iniettiva che identifica \mathbb{R} a un sottinsieme di \mathbb{C} (anche per le operazioni), detto parte reale di \mathbb{C} . Invece la funzione $\mathbb{R} \rightarrow \mathbb{C}$ che manda b in $(0, b)$ è una funzione iniettiva, ma rispetta solo la somma, e non il prodotto; l'immagine si chiama parte puramente immaginaria di \mathbb{C} .

7.7.2. Scrivendo $i = (0, 1)$ e per ogni numero reale $a = (a, 0)$, vediamo che $(a, b) = (a, 0) + (0, b) = (a, 0) + (0, 1)(b, 0) = a + ib$, e quindi riconosciamo la costruzione più intuitiva prima introdotta. Di solito i numeri complessi si indicano con lettere tipo z, u, v, w , e se $z = a + ib$, il numero reale a si dice la parte reale di z e si indica con $\Re(z)$, mentre il numero reale b si indica con $\Im(z)$ e si chiama la parte immaginaria di z . Quindi $z = \Re(z) + i\Im(z)$ per ogni $z \in \mathbb{C}$.

7.7.3. CONIUGAZIONE. Se z è un numero complesso, definiamo il suo coniugato \bar{z} come $\Re(z) - i\Im(z)$ (cambiamo di segno la parte immaginaria). Abbiamo allora una funzione $\mathbb{C} \rightarrow \mathbb{C}$ che è un automorfismo di corpo; cioè è una biiezione dotata delle seguenti proprietà:

(C1) rispetta le operazioni di somma $\overline{z + z'} = \bar{z} + \bar{z}'$

(C2) e di prodotto $\overline{zz'} = \bar{z}\bar{z}'$.

Notiamo inoltre che:

(C3) gli elementi fissi della coniugazione (cioè gli elementi mandati in sè stessi) sono tutti e soli i numeri reali: $z = \bar{z}$ se e solo se $z \in \mathbb{R}$;

(C4) la coniugazione è una involuzione ($\bar{\bar{z}} = z$ per ogni z), e quindi è la sua propria inversa.

7.7.4. NORMA (O MODULO) DI NUMERI COMPLESSI. Per ogni numero complesso z definiamo la sua norma (talvolta detta anche modulo) $|z|$ come la radice quadrata positiva del prodotto $z\bar{z} = \Re(z)^2 + \Im(z)^2$, che risulta un numero reale. Abbiamo allora una funzione $\mathbb{C} \rightarrow \mathbb{R}$ soddisfacente alle seguenti proprietà:

(N1) positività: $|z| \geq 0$ per ogni $z \in \mathbb{C}$ e $|z| = 0$ se e solo se $z = 0$;

(N2) moltiplicatività: $|zz'| = |z||z'|$;

(N3) subaddittività: $|z + z'| \leq |z| + |z'|$.

Si osservi anche dalla formula $|z|^2 = z\bar{z}$ segue che

$$z^{-1} = \frac{\bar{z}}{|z|^2} = \frac{\Re(z) - i\Im(z)}{\Re(z)^2 + \Im(z)^2}$$

come già prima osservato per ogni $z \neq 0$. Inoltre abbiamo anche (disuguaglianze sul quadrilatero)

(N4) $||z| - |z'|| \leq |z - z'|$;

(N5) $|z + z'|^2 + |z - z'|^2 = 2(|z|^2 + |z'|^2)$.

7.7.5. ARGOMENTO E VERSORE. I numeri complessi z di norma 1 si dicono unitari, e soddisfano alla condizione $\Re(z)^2 + \Im(z)^2 = 1$; quindi esiste un unico reale $\vartheta \in [0, 2\pi)$ tale che $\Re(z) = \cos \vartheta$ e $\Im(z) = \sin \vartheta$. In generale per ogni numero complesso z non nullo, il numero $\text{ver}(z) = z/|z|$ è unitario, si dice il versore di z , e il valore ϑ associato si dice argomento di z e si indica con $\arg(z)$. Dunque abbiamo definito una funzione $\mathbb{C} \setminus \{0\} \rightarrow [0, 2\pi)$ soddisfacente alle seguenti proprietà: $z \in \mathbb{R}$ se e solo se $\arg(z) \in \{0, \pi\}$ (se e solo se $\text{ver}(z) = \pm 1$); $\arg(zz') = \arg(z) + \arg(z')$ a meno di multipli di 2π (equivalentemente $\text{ver}(zz') = \text{ver}(z)\text{ver}(z')$).

7.7.6. FORMA TRIGONOMETRICA. Per ogni numero complesso z , se $\arg(z) = \vartheta$ e $|z| = \varrho$, abbiamo la rappresentazione parametrica di z data da

$$z = \varrho(\cos \vartheta + i \sin \vartheta)$$

che fa vedere come il numero complesso z sia identificato nel piano reale dalle sue “coordinate polari” ρ (distanza dall’origine) e ϑ (angolo di rotazione rispetto all’asse reale positivo).

In questa rappresentazione è particolarmente facile dare una interpretazione geometrica del prodotto di due numeri complessi; dati infatti $z = \rho(\cos \vartheta + i \sin \vartheta)$ e $z' = \rho'(\cos \vartheta' + i \sin \vartheta')$, abbiamo che

$$\begin{aligned} zz' &= \rho(\cos \vartheta + i \sin \vartheta)\rho'(\cos \vartheta' + i \sin \vartheta') \\ &= \rho\rho'((\cos \vartheta \cos \vartheta' - \sin \vartheta \sin \vartheta') + i(\cos \vartheta \sin \vartheta' + \sin \vartheta \cos \vartheta')) \\ &= \rho\rho'(\cos(\vartheta + \vartheta') + i \sin(\vartheta + \vartheta')) \end{aligned}$$

e dunque il prodotto è il numero complesso che ha come norma il prodotto delle norme, e come argomento la somma dei due argomenti (modulo 2π); in altri termini z viene moltiplicato per la norma di z' e ruotato dell’argomento di z' . In particolare diventa facile capire come elevare alla potenza n -esima un numero complesso: z^n è il numero complesso la cui norma è la potenza n -esima della norma di z , e il cui argomento è n volte l’argomento di z :

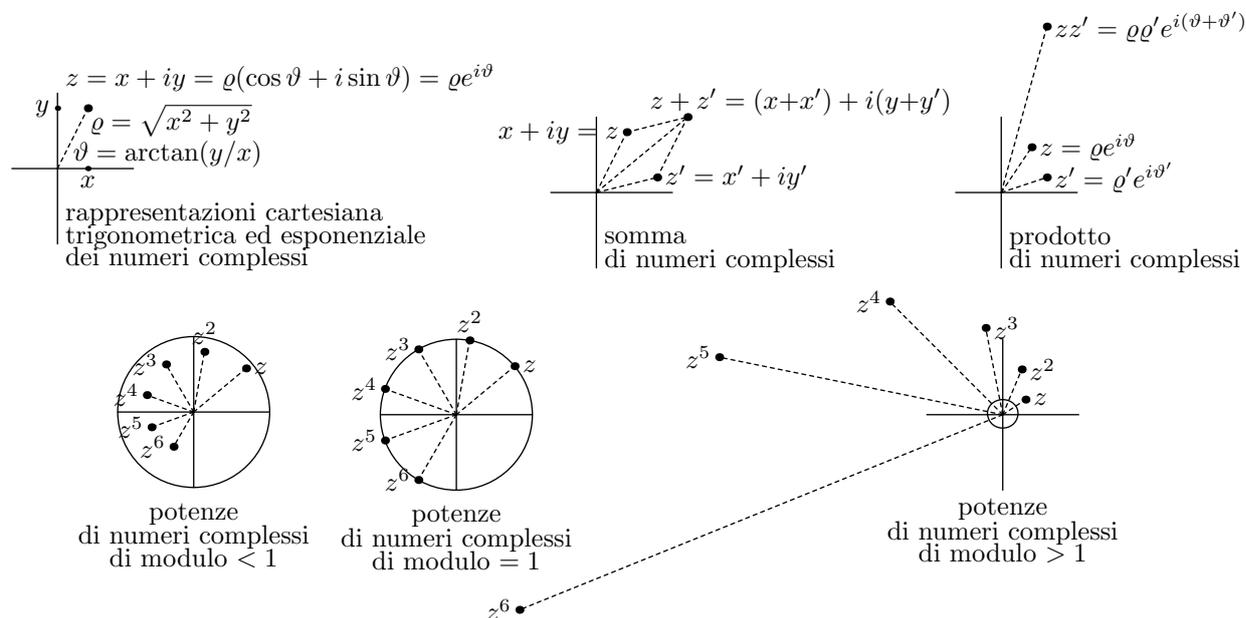
$$\text{se } z = \rho(\cos \vartheta + i \sin \vartheta) \text{ allora } z^n = \rho^n(\cos(n\vartheta) + i \sin(n\vartheta)).$$

7.7.7. FORMULE DI DE MOIVRE. Dall’osservazione precedente, si ottiene subito un metodo per il calcolo delle radici n -esime di un numero complesso z . Si tratta delle soluzioni dell’equazione $X^n = z$ in \mathbb{C} , che sono sempre n se $z \neq 0$, e si ottengono come i numeri complessi di norma la radice n -esima (reale positiva) della norma di z , e di argomento tale che moltiplicato per n dia (a meno di multipli di 2π) l’argomento di z . In formule (dette di De Moivre): le radici n -esime di $z = \rho(\cos \vartheta + i \sin \vartheta)$ sono date da

$$\sqrt[n]{\rho} \left(\cos \left(\frac{\vartheta}{n} + \frac{2\pi k}{n} \right) + i \sin \left(\frac{\vartheta}{n} + \frac{2\pi k}{n} \right) \right)$$

per i valori interi di k compresi tra 0 ed $n-1$.

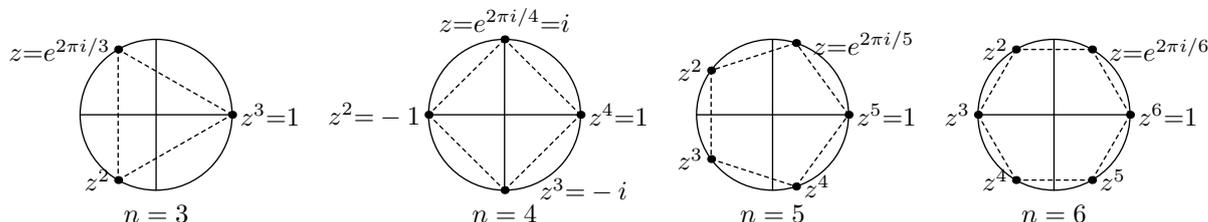
7.7.8. RAPPRESENTAZIONE GEOMETRICA: PIANO DI GAUSS. Rappresentando i numeri complessi come coppie di numeri reali è possibile dare un significato geometrico a tutte le nozioni sopra introdotte. Inseriamo qui solamente i disegni, su cui invitiamo il lettore a riflettere.



7.7.9. RADICI COMPLESSE DELL’UNITÀ. In particolare l’espressione precedente si applica per il calcolo delle radici n -esime dell’unità, ovvero per le soluzioni dell’equazione $X^n = 1$ in \mathbb{C} . Dall’interpretazione geometrica prima data dell’elevamento a potenza si capisce subito che si tratta di numeri complessi unitari che sono i vertici del poligono regolare con n lati inscritto nel cerchio unitario e un cui vertice sia 1. Esempi:

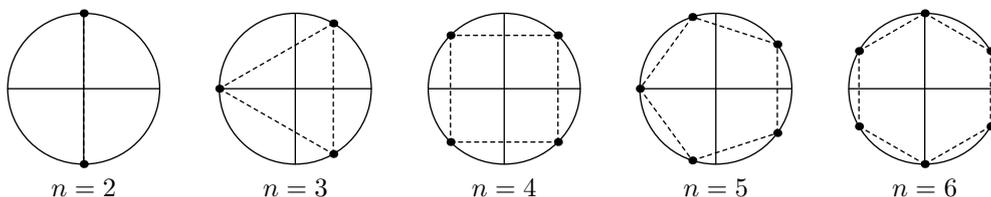
- (1) l’unica radice 1-aria di 1 è 1;
- (2) le due radici quadrate di 1 sono 1 e -1 ;
- (3) le tre radici terze di 1 sono 1 e $\cos \frac{2\pi}{3} \pm i \sin \frac{2\pi}{3}$ (vertici del triangolo equilatero);

- (4) le quattro radici quarte di 1 sono ± 1 e $\pm i$ (vertici del quadrato);
 (5) le cinque radici quinte dell'unità sono $1, \cos \frac{2\pi}{5} \pm i \sin \frac{2\pi}{5}, \cos \frac{4\pi}{5} \pm i \sin \frac{4\pi}{5}$ (vertici del pentagono regolare);
 (6) le sei radici seste dell'unità sono $\pm 1, \cos \frac{\pi}{3} \pm i \sin \frac{\pi}{3}, \cos \frac{2\pi}{3} \pm i \sin \frac{2\pi}{3}$ (vertici dell'esagono regolare).

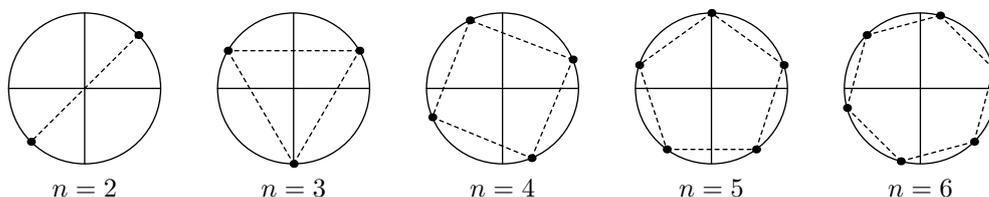


7.7.10. RADICI PRIMITIVE n -ESIME DELL'UNITÀ. Una radice n -esima z dell'unità si dice primitiva se $z^i \neq 1$ per $i < n$ (n è la minima potenza di z che dia 1). Se z è una radice primitiva n -esima dell'unità, allora una sua potenza z^i è ancora una radice primitiva n -esima dell'unità se e solo se i è primo con n (verificare). Di conseguenza per ogni n il numero di radici primitive n -esime dell'unità è uguale a $\Phi(n)$ (funzione di Eulero).

7.7.11. RADICI n -ESIME DI -1 .



7.7.12. RADICI n -ESIME DI i .



7.7.13. FORMA ESPONENZIALE. La proprietà della funzione argomento rispetto al prodotto di numeri complessi (che diventa la somma degli argomenti) suggerisce di usare una notazione esponenziale per i numeri complessi di norma uno ponendo

$$e^{i\vartheta} = \cos \vartheta + i \sin \vartheta .$$

Questa espressione sarà giustificata in un corso di Analisi (studiando gli sviluppi di Taylor delle funzioni esponenziali e circolari), ma possiamo già notare come essa renda sensibilmente semplici alcune formule viste.

Ad esempio ogni numero complesso z si scrive come $\rho e^{i\vartheta}$, e la sua potenza n -esima si scrive $z^n = (\rho e^{i\vartheta})^n = \rho^n e^{in\vartheta}$. Analogamente le radici n -esime sono $\rho^{\frac{1}{n}} e^{i\frac{\vartheta+2\pi k}{n}}$ per $k = 0, 1, \dots, n-1$.

Le radici n -esime dell'unità nel corpo complesso si scrivono in notazione esponenziale come $e^{i\frac{k\pi}{n}}$ per $k = 0, 1, \dots, n-1$.

La definizione generale di una funzione esponenziale complessa, essenzialmente decisa dalla notazione introdotta, è la seguente: se $z = a + ib$ allora $e^z = e^{a+ib} = e^a e^{ib} = e^a (\cos b + i \sin b)$. Da ciò possiamo anche dedurre la nozione di logaritmo complesso: i numeri complessi w tali che $e^w = z$ (tali w si dicono i logaritmi complessi di z) sono quelli della forma $\log \rho + i(\vartheta + 2k\pi)$ per $k \in \mathbb{Z}$ se $z = \rho e^{i\vartheta} \neq 0$. In particolare ogni numero complesso non nullo ha una famiglia numerabile di logaritmi: ciò deriva dal fatto che la funzione esponenziale complessa ha un comportamento periodico riguardo alla componente immaginaria dell'esponente: $e^z = e^{z+i2k\pi}$ per ogni k intero.

7.7.14. TEOREMA (FONDAMENTALE DELL'ALGEBRA). Ogni polinomio non costante a coefficienti complessi ammette almeno uno zero in \mathbb{C} ; e dunque ogni tale polinomio ha esattamente tante radici in \mathbb{C} quant'è il suo grado.

Una dimostrazione di questo risultato basata su metodi analitici reali si può trovare nel testo “Algebraic Structures” di S. Lang, ch. VII, §5. Esistono anche dimostrazioni di carattere algebrico, ma richiedono buone conoscenze: vedi I. Barsotti, “Appunti di Algebra”, lezione 70.

7.7.15. TEOREMA (FONDAMENTALE DELL’ALGEBRA, VERSIONE REALE). *Ogni polinomio non costante a coefficienti reali si fattorizza come prodotto di polinomi reali irriducibili che possono essere di primo grado oppure di secondo grado (e privi di radici reali, dunque con due radici complesse coniugate). In particolare ogni polinomio reale di grado dispari ha almeno una radice reale.*

DIMOSTRAZIONE. In effetti, se z è una radice complessa del polinomio $P(X)$ a coefficienti reali, allora anche il coniugato \bar{z} è radice dello stesso polinomio (se $P(z) = 0$, allora $0 = \overline{P(z)} = P(\bar{z})$, poiché $P(X)$ ha coefficienti reali). Dunque le radici complesse non reali si presentano sempre a coppie coniugate, e danno luogo a un fattore reale $(X - z)(X - \bar{z}) = X^2 - 2\Re(z)X + |z|^2$ di secondo grado del polinomio $P(X)$. L’ultima affermazione è una ovvia conseguenza. \square

7.7.16. IDENTITÀ DEI DUE QUADRATI. Dalla proprietà moltiplicativa della norma complessa si deriva la seguente regola, detta identità dei due quadrati: *il prodotto di due somme di due quadrati è ancora una somma di due quadrati.* Infatti:

$$(a^2 + b^2)(a'^2 + b'^2) = (aa' - bb')^2 + (ab' + a'b)^2$$

si ottiene esplicitando $|z|^2|z'|^2 = |zz'|^2$.

7.7.17. RETTE E CERCHI NEL PIANO COMPLESSO. Insieme, il corpo \mathbb{C} coincide con \mathbb{R}^2 , e il lettore conosce già le espressioni cartesiane di rette e cerchi nel piano reale; è interessante vedere le analoghe espressioni usando la variabile complessa.

Cominciamo dalle rette: usando le variabili reali X e Y si tratta delle espressioni del tipo $aX + bY + c = 0$ ($a, b, c \in \mathbb{R}$) in cui almeno uno tra a e b non è nullo (cioè la coppia (a, b) non è nulla). Ricordando che $2X = Z + \bar{Z}$ e $2iY = Z - \bar{Z}$, otteniamo la forma $\alpha Z + \bar{\alpha}\bar{Z} + 2c = 0$, ove $\alpha = a + ib$. Viceversa ogni tale espressione con $\alpha \in \mathbb{C}$ non nullo e $c \in \mathbb{R}$ rappresenta una retta del piano.

Per le circonferenze, è più facile impostare direttamente la condizione usando la variabile complessa: i punti Z che distano r da z_0 sono tutti e soli quelli per cui $|Z - z_0| = r$, cioè $|Z - z_0|^2 = r^2$, ovvero $(Z - z_0)(\bar{Z} - \bar{z}_0) = r^2$. Si ottiene una espressione del tipo $Z\bar{Z} - \alpha Z - \bar{\alpha}\bar{Z} + c = 0$ ove $\bar{\alpha} = z_0$ è il centro, e $\alpha\bar{\alpha} - s = r^2$ è il quadrato del raggio. Viceversa ogni tale espressione con $\alpha \in \mathbb{C}$ e $c \in \mathbb{R}$ rappresenta una circonferenza del piano (eventualmente con raggio immaginario...). L’espressione reale per le circonferenze si può ottenere ricordando che $Z = X + iY$, $\bar{Z} = X - iY$ e $Z\bar{Z} = X^2 + Y^2$, da cui si ottiene $X^2 + Y^2 - 2\Re(\alpha)X - 2\Im(\alpha)Y + c = 0$, formula usuale.

Si osservi la stretta parentela tra rette e cerchi, che è ben evidente nelle espressioni in variabile complessa: cosa descrive l’equazione $sZ\bar{Z} - \alpha Z - \bar{\alpha}\bar{Z} + c = 0$ con $s, c \in \mathbb{R}$ e $\alpha \in \mathbb{C}$?

7.7.18. TRASFORMAZIONI DI MÖBIUS DEL PIANO COMPLESSO. È di particolare interesse, e riemergerà varie volte durante il corso, la nozione di “trasformazione lineare fratta”, o trasformazione di Möbius, di \mathbb{C} . Si tratta funzioni di variabile complessa definite da $\varphi(Z) = \frac{c+dZ}{a+bZ}$ con $ad - bc \neq 0$. Si tratta di una funzione definita su \mathbb{C} tranne che per $Z = -a/b$ (se $b \neq 0$), e a valori in tutto \mathbb{C} tranne il punto d/b (sempre se $b \neq 0$). Tra tali sottinsiemi è invertibile, con inversa data da $\psi(Z) = \frac{c-aZ}{-d+bZ}$, che è una funzione dello stesso tipo.

I più semplici esempi di trasformazioni di Möbius sono le traslazioni ($\varphi(Z) = c + Z$), le omotetie o dilatazioni ($\varphi(Z) = dZ$ con $d \neq 0$), le inversioni ($\varphi(Z) = 1/Z$). Commutano tra loro?

Si dicono trasformazioni affini le composizioni di traslazioni e dilatazioni, cioè le trasformazioni non fratte, del tipo $\varphi(Z) = c + dZ$. In effetti ogni trasformazione di Möbius si può scrivere come composizione di una inversione seguita e preceduta da trasformazioni affini: la generica $\varphi(Z) = \frac{c+dZ}{a+bZ}$ si ottiene applicando prima $\varphi_1(Z) = a + bZ$, poi $\varphi_2(Z) = 1/Z$, e infine $\varphi_3(Z) = \alpha + \beta Z$ per opportuni α, β (quali?). Siccome le trasformazioni affini sono piuttosto facili da capire, per capire l’effetto delle trasformazioni di Möbius si è ricondotti a studiare l’inversione $\iota(Z) = 1/Z$. Si tratta chiaramente di una biiezione di $\mathbb{C} \setminus \{0\}$ in sè, autoinversa (cioè coincide con la sua propria inversa), che fissa il circolo unitario (ma non punto per punto), e scambia l’interno del circolo con l’esterno (e anzi scambia le circonferenze centrate in 0 di raggio r con quelle centrate in 0 e di raggio $1/r$). La cosa più interessante è il comportamento sulle rette (e di conseguenza sui cerchi): *le rette passanti per l’origine vengono trasformate in rette passanti per l’origine, mentre le altre rette vengono trasformate in cerchi passanti per l’origine; viceversa le circonferenze passanti per l’origine vengono trasformate in rette, mentre le*

altre circonferenze vengono trasformate in circonferenze. Verificare queste affermazioni usando le espressioni prima evidenziate per rette e circonferenze; farsi qualche disegno può aiutare l'intuizione.

♠♠ **7.8. QUATERNIONI DI HAMILTON.** I corpi finora visti erano tutti commutativi. Il primo esempio di corpo non commutativo è dato dai quaternioni di Hamilton, che andiamo ora ad illustrare. Vedremo in futuro che essi hanno un importante significato geometrico, poiché interpretano l'insieme delle rotazioni (attorno a rette) di uno spazio reale di dimensione tre.

7.8.1. DEFINIZIONE (QUATERNIONI). Consideriamo l'insieme \mathbb{H} formato da tutte le espressioni del tipo $a + ib + jc + kd$ ove a, b, c, d sono numeri reali, e i, j, k sono tre simboli (in particolare non appartengono ad \mathbb{R}). Definiamo le seguenti operazioni:

(S) somma: $(a + ib + jc + kd) + (a' + ib' + jc' + kd') = (a+a') + i(b+b') + j(c+c') + k(d+d')$;

(P) prodotto: pretendendo che il prodotto sia distributivo rispetto alla somma, associativo, e che tra numeri reali sia quello di \mathbb{R} , ci basta definire i prodotti tra i simboli i, j, k , cosa che facciamo nella seguente tabella:

$$\begin{array}{lll} ii = -1 & ij = k & ik = -j \\ ji = -k & jj = -1 & jk = i \\ ki = j & kj = -i & kk = -1 \end{array}$$

(per memoria: i quadrati sono tutti -1 , i prodotti di due elementi consecutivi nell'ordine ciclico i, j, k dà l'elemento successivo, i prodotti di due elementi consecutivi nell'ordine inverso dà l'opposto dell'elemento mancante).

Gli elementi di \mathbb{H} si chiamano i quaternioni, e il corpo \mathbb{H} si dice il corpo dei quaternioni di Hamilton. Invitiamo il lettore a controllare scrupolosamente che dotato delle operazioni sopra definite l'insieme \mathbb{H} ha struttura di corpo (non commutativo) di elemento nullo $0 + 0i + 0j + 0k$, di elemento unità $1 + 0i + 0j + 0k$. L'associatività del prodotto, l'esistenza degli inversi per elementi non nulli, la distributività sono le proprietà fondamentali non banali da controllare.

7.8.2. QUATERNIONI REALI ED IMMAGINARI. Diciamo quaternioni reali quelli dell'immagine della funzione $\mathbb{R} \rightarrow \mathbb{H}$ che manda x in $x + 0i + 0j + 0k$; si osservi che questa funzione rispetta le operazioni dei due corpi.

Diciamo invece immaginari i quaternioni che sono mandati a zero dalla funzione $\mathbb{H} \rightarrow \mathbb{R}$ che manda $a + ib + jc + kd$ in a (detta parte reale del quaternione); si osservi che questa funzione rispetta la somma, ma non il prodotto dei due corpi.

Ogni quaternione è dunque somma delle sue parti reale ed immaginaria.

7.8.3. CONIUGATO. Dato un quaternione $z = a + ib + jc + kd$, definiamo il suo coniugato $\bar{z} = a - ib - jc - kd = a + i(-b) + j(-c) + k(-d)$. Otteniamo così una applicazione di \mathbb{H} in sè che soddisfa alle seguenti proprietà:

(C1) rispetta la somma: $\overline{z + z'} = \bar{z} + \bar{z}'$

(C2) $\bar{z} = z$ se e solo se z è (puramente) reale; $\bar{z} = -z$ se e solo se z è (puramente) immaginario;

(C3) (anti)rispetta il prodotto: $\overline{zz'} = \bar{z}'\bar{z}$

(C4) $z\bar{z} = \bar{z}z = a^2 + b^2 + c^2 + d^2$ è puramente reale per ogni $z = a + ib + jc + kd$, e si tratta di un numero positivo (se $z \neq 0$).

(C5) $\bar{\bar{z}} = z$ per ogni z (dunque di tratta di un isomorfismo involutorio).

7.8.4. NORMA (O MODULO) DI QUATERNIONI. Definiamo la norma di un quaternione come la radice quadrata (reale positiva) del prodotto $z\bar{z}$. Si tratta allora di una funzione di \mathbb{H} in \mathbb{R} dotata delle seguenti proprietà:

(N1) positività: $|z| \geq 0$ per ogni $z \in \mathbb{C}$ e $|z| = 0$ se e solo se $z = 0$;

(N2) moltiplicatività: $|zz'| = |z||z'|$;

(N3) subaddittività: $|z + z'| \leq |z| + |z'|$.

7.8.5. INVERSI. Con le nozioni sopra introdotte, possiamo ora affermare che se z è quaternione non nullo, allora l'inverso di z è $z^{-1} = \frac{\bar{z}}{|z|^2}$.

7.8.6. Applicando l'identità $z\bar{z} = \bar{z}z$ a $z = u + v$, mostrare che per ogni coppia di quaternioni abbiamo $u\bar{v} + \bar{u}v = v\bar{u} + \bar{v}u$.

7.8.7. IDENTITÀ DEI QUATTRO QUADRATI. Analogamente a quanto visto nel caso complesso, la proprietà moltiplicativa della norma per i quaternioni dà luogo ad una formula che riguarda le somme

di quattro quadrati: *il prodotto di due somme di quattro quadrati è ancora una somma di quattro quadrati*. Precisamente:

$$\begin{aligned} & (a^2 + b^2 + c^2 + d^2)(a'^2 + b'^2 + c'^2 + d'^2) = \\ & = (aa' - bb' - cc' - dd')^2 + (ab' + ba' + cd' - dc')^2 + (ac' + ca' - db' + bd')^2 + (ad' + da' + bc' - cb')^2. \end{aligned}$$

A titolo di informazione diciamo che identità simili valgono solamente per le somme di uno, due, quattro e otto quadrati.

♠ **7.9.** I NUMERI DI GAUSS. Un esempio particolarmente significativo di anello e del suo corpo dei quozienti è dato dai numeri di Gauss che ora definiamo.

7.9.1. GLI INTERI DI GAUSS. L'anello degli interi di Gauss è l'insieme $\mathbb{Z}[i]$ delle espressioni del tipo $a + ib$ con $a, b \in \mathbb{Z}$ ove i è il "numero immaginario complesso", con le operazioni definite come nel caso del corpo complesso. Si osservi che gli unici elementi invertibili in $\mathbb{Z}[i]$ sono quelli per cui $a^2 + b^2$ è un intero invertibile, e dunque ± 1 : quindi sono ± 1 e $\pm i$.

Si noti che il numero intero primo 2 si fattorizza in $\mathbb{Z}[i]$ nel modo seguente $2 = (1 + i)(1 - i)$; come pure $5 = (2 + i)(2 - i)$.

7.9.2. IL CORPO DI GAUSS. Il corpo delle frazioni di $\mathbb{Z}[i]$ si indica con $\mathbb{Q}[i]$ ed è formato dalle espressioni del tipo $a + ib$ con $a, b \in \mathbb{Q}$ (e si tratta di un sottocorpo del corpo \mathbb{C} dei numeri complessi).

7.9.3. L'anello $\mathbb{Z}[i]$ e il corpo $\mathbb{Q}[i]$ non sono ordinabili: perché?

♠ **7.10.** ESTENSIONI REALI QUADRATICHE DEI RAZIONALI. Consideriamo le espressioni del tipo $a + b\sqrt{2}$ con $a, b \in \mathbb{Q}$; esse formano un insieme indicato con $\mathbb{Q}[\sqrt{2}]$ che si può identificare con un sottosistema di \mathbb{R} (ma è pericoloso: si può fare in due modi). Con le usuali posizioni possiamo dare a $\mathbb{Q}[\sqrt{2}]$ la struttura di corpo (in effetti sottocorpo del corpo reale); analogamente al caso di Gauss e del corpo complesso possiamo definire per ogni $a + b\sqrt{2}$ il suo coniugato $a - b\sqrt{2}$; allora il prodotto $(a + b\sqrt{2})(a - b\sqrt{2}) = a^2 - 2b^2$ è un numero razionale nullo se e solo se $a = b = 0$ (cioè solo per l'elemento nullo); questo equivale al fatto che $\sqrt{2}$ non è un numero razionale, che si dimostra per assurdo usando la proprietà di fattorizzazione unica in \mathbb{Z} : se $\sqrt{2} = a/b$ con $a, b \in \mathbb{Z}$ allora $2b^2 = a^2$ (uguaglianza di numeri interi in cui il primo 2 comparirebbe nella fattorizzazione un numero dispari di volte a sinistra, e un numero pari a destra).

7.10.1. Il corpo $\mathbb{Q}[\sqrt{2}]$ non ha un ordine canonico. Vi sono due automorfismi che sono l'identità su \mathbb{Q} (quali?).

7.10.2. Il corpo $\mathbb{Q}[\sqrt{2}]$ è corpo dei quozienti di un opportuno anello $\mathbb{Z}[\sqrt{2}]$.

7.10.3. Lo stesso tipo di costruzione si può fare "aggiungendo a \mathbb{Q} " la radice quadrata di un elemento (che non sia quadrato in \mathbb{Q}).

8. Polinomi.

I polinomi (almeno in una variabile) sono un oggetto di studio ben noto; daremo qui una definizione rigorosa, e metteremo in evidenza le tecniche più importanti legate a questa nozione.

8.1. DEFINIZIONE (POLINOMI). Dato un anello A (di solito useremo un corpo), l'anello $A[X]$ dei polinomi in una variabile a coefficienti in A è il sottosistema di $A^{\mathbb{N}}$ dato dalle funzioni quasi ovunque nulle (cioè che hanno valore 0 tranne che per un numero finito di indici) dotato delle seguenti operazioni:

(S) $(a_i) + (b_i) = (c_i)$ ove $c_i = a_i + b_i$ (somma coordinata per coordinata),

(P) $(a_i) \cdot (b_i) = (p_i)$ ove $p_i = \sum_{j+k=i} a_j b_k$ (prodotto alla kronecker),

ove abbiamo indicato con $(a_i) = (a_0, a_1, \dots, a_n, \dots)$ un polinomio generico (gli a_i sono quasi tutti nulli, e si dicono i coefficienti del polinomio). Si verifica allora che si tratta di un anello (commutativo se A è commutativo), con elemento nullo la funzione nulla, elemento unità la funzione che vale 1 (di A) in 0 e nulla altrove.

8.1.1. RAPPRESENTAZIONE USUALE. Detto e_i l'elemento di $A[X]$ che vale 1 in i e zero altrove, e scrivendo semplicemente a per l'elemento che vale $a \in A$ in posto 0 e zero altrove, allora ogni elemento di $A[X]$ si scrive come somma finita $(a_i) = \sum_{i \in \mathbb{N}} a_i e_i$ con $a_i \in A$ (finita significa che solo un numero finito degli a_i non è nullo). Ora, scrivendo X^i invece di e_i si ottiene la usuale rappresentazione dei

polinomi in una indeterminata $\sum_{i \in \mathbb{N}} a_i X^i$, che giustifica la definizione del prodotto, poiché è obbligata dalle proprietà distributiva ed associativa.

8.1.2. FUNZIONI POLINOMIALI. Poiché ogni polinomio può essere “valutato” in un qualsiasi elemento dell’anello dei coefficienti, esso determina una funzione $A \rightarrow A$, che viene detta funzione polinomiale. L’insieme $P(A)$ delle funzioni polinomiali di A in sè è definito come il sottinsieme di A^A dato dalle funzioni $f : A \rightarrow A$ per le quali esiste un polinomio P con $f(a) = P(a)$ per ogni $a \in A$. Si verifica subito che $P(A)$ è sottoanello di A^A (che si considera qui come anello con le operazioni di somma e prodotto “coordinata per coordinata”, come per A^Z per ogni insieme Z ; in particolare non usiamo, non ancora, la composizione di funzioni), e che abbiamo una funzione di anelli $A[X] \rightarrow P(A)$, che abbiamo sopra descritto; questa funzione in generale non è iniettiva.

Consideriamo infatti il caso $A = \mathbb{F}_p$ (corpo con p elementi). Allora $\mathbb{F}_p[X]$ è un insieme infinito, mentre le funzioni polinomiali (che sono un sottinsieme delle funzioni di \mathbb{F}_p in sè) sono finite. Quali sono i polinomi che sono nulli come funzioni polinomiali? Quando due polinomi danno luogo alla stessa funzione polinomiale?

8.1.3. PRINCIPIO DI IDENTITÀ DEI POLINOMI. Dalla definizione che abbiamo dato è chiaro che due polinomi sono uguali se e solo se per ogni indice i i coefficienti i -esimi coincidono (questo si dice di solito principio di identità dei polinomi, e spesso si enuncia anche dicendo che un polinomio è nullo se e solo se tutti i suoi coefficienti sono nulli).

Invece che due polinomi assumano gli stessi valori su ogni elemento dell’anello dei coefficienti garantisce solo che essi determinano la stessa funzione polinomiale, non che siano lo stesso polinomio; tuttavia nel caso di domini di cardinalità infinita vale anche che due polinomi che siano uguali come funzioni polinomiali coincidono in quanto polinomi.

8.1.4. FUNZIONI CANONICHE. Vi è un morfismo canonico di anelli $A \rightarrow A[X]$ che ad $a \in A$ associa il polinomio a di grado zero. Si tratta di un morfismo iniettivo, poiché ha un inverso sinistro dato dalla “valutazione in zero” $A[X] \rightarrow A$ che associa ad ogni polinomio $P(X)$ l’elemento $P(0) \in A$ (in effetti il termine noto).

8.1.5. INTEGRITÀ. Si verifica facilmente che $A[X]$ è integro se A è integro. Infatti basta mostrare che $PQ \neq 0$ se $P \neq 0 \neq Q$; siano a_i il coefficiente direttore di P (coefficiente non nullo con massimo indice i di P), e b_j il coefficiente direttore di Q (coefficiente non nullo con massimo indice j di Q): allora il coefficiente di indice $i + j$ di PQ è $a_i b_j \neq 0$ e dunque $PQ \neq 0$.

D’ora in poi supporremo sempre A anello integro. In questo caso è chiaro che gli unici invertibili di $A[X]$ sono gli elementi invertibili di A .

8.2. DEFINIZIONE (GRADO). Si definisce grado di un polinomio non nullo $P = (a_i)$, e si indica con $\deg(P)$, il massimo indice n tale che $a_n \neq 0$ (e tale a_n si dice coefficiente direttore di P ; il polinomio si dice monico se il coefficiente direttore è 1). Per definizione poniamo $\deg(0) = -\infty$. La funzione $\deg : A[X] \rightarrow \mathbb{N} \cup \{-\infty\}$ gode delle seguenti proprietà:

- (G1) $\deg(P) = -\infty$ se e solo se $P = 0$; $\deg(P) = 0$ se e solo se $P \in A$;
- (G2) $\deg(P + Q) \leq \max\{\deg(P), \deg(Q)\}$, e vale l’uguaglianza se e solo se $\deg(P) \neq \deg(Q)$ oppure $\deg(P) = \deg(Q)$ e i coefficienti direttori non sono uno l’opposto dell’altro; dunque vale la disuguaglianza stretta se e solo se $\deg(P) = \deg(Q)$ e i coefficienti direttori sono uno l’opposto dell’altro;
- (G3) $\deg(PQ) \leq \deg(P) + \deg(Q)$ (e vale l’uguaglianza se A è integro).

8.3. TEOREMA (DIVISIONE CON RESTO). Sia C un corpo e $C[X]$ l’anello dei polinomi su C . Per ogni coppia di polinomi $M(X)$ e $N(X) \neq 0$ esiste una unica coppia di polinomi $Q(X)$ e $R(X)$ (detti il quoziente ed il resto della divisione del dividendo $M(X)$ per il divisore $N(X)$) con $\deg R(X) < \deg N(X)$ se $R(X) \neq 0$ tale che $M(X) = Q(X)N(X) + R(X)$.

DIMOSTRAZIONE (ALGORITMO DI DIVISIONE). Si procede per induzione sul grado di $M(X)$. Se $\deg M(X) < \deg N(X)$ allora $Q(X) = 0$ e $R(X) = M(X)$ danno il risultato. Se invece $\deg M(X) \geq \deg N(X)$, siano m, n i coefficienti direttori di $M(X)$ e $N(X)$ rispettivamente; allora il polinomio $M'(X) = M(X) - mn^{-1} X^{\deg M(X) - \deg N(X)} N(X)$ ha grado strettamente minore di quello di $M(X)$, e per ipotesi induttiva esistono $Q'(X)$ ed $R'(X)$ tali che $M'(X) = Q'(X)N(X) + R'(X)$ con $\deg R'(X) < \deg N(X)$ se $R'(X) \neq 0$. Allora basta porre $Q(X) = mn^{-1} X^{\deg M(X) - \deg N(X)} N(X) + Q'(X)$ ed $R(X) = R'(X)$ per ottenere il risultato voluto. \square

Si osservi che il procedimento induttivo descritto è il ben noto algoritmo per il calcolo della divisione con resto tra polinomi.

8.3.1. Potremmo togliere l'ipotesi che i polinomi abbiano coefficienti in un corpo, imponendo che il secondo polinomio sia monico (o che il coefficiente dominante sia invertibile, che è l'unica richiesta per la dimostrazione).

8.3.2. IDEALI PRINCIPALI. Dall'esistenza della divisione possiamo dedurre che gli ideali di un anello di polinomi su un corpo sono tutti principali; infatti basta considerare di un ideale I non nullo gli elementi di grado minimo: uno qualsiasi di essi genera l'ideale. Sia infatti $P(X)$ un tale elemento di grado minimo e $F(X)$ un polinomio dell'ideale; dalla divisione $F(X) = Q(X)P(X) + R(X)$ deduciamo che $R(X)$ appartiene all'ideale, e non potendo avere grado minore di quello di $P(X)$, dev'essere $R(X) = 0$, e dunque $F(X)$ un multiplo di $P(X)$.

8.3.3. RUFFINI. Dal procedimento di divisione con resto di un polinomio $P(X)$ per un polinomio del tipo $X - c$ ci dice che $P(X)$ è divisibile per $X - c$ se e solo se il polinomio stesso si annulla in c , cioè $P(c) = 0$. Infatti $P(c)$ è il resto della divisione di $P(X)$ per $X - c$.

8.3.4. Di conseguenza il numero di zeri di un polinomio a coefficienti in un dominio non può superare il grado del polinomio stesso.

8.4. DEFINIZIONE (MCD, mcm). *Dati due polinomi P e Q in $C[X]$ definiamo massimo comun divisore $\text{MCD}(P, Q)$, spesso denotato (P, Q) semplicemente, qualsiasi polinomio D che divide sia P che Q e tale che ogni divisore comune di P e Q divida anche D . Un massimo comun divisore è definito a meno di moltiplicazione per un elemento invertibile, dunque per un elemento non nullo di C .*

Analogamente si definisce minimo comune multiplo, denotato $\text{mcm}(P, Q)$, come un minimo (per la divisibilità) dei multipli comuni di P e Q . Anche un minimo comune multiplo è definito a meno di moltiplicazione per un elemento invertibile.

8.4.1. GENERALIZZAZIONE A n POLINOMI. Definizioni analoghe di massimo comun divisore e minimo comune multiplo si possono dare per ogni insieme finito P_1, P_2, \dots, P_n di polinomi.

8.5. TEOREMA (MCD). *Un massimo comun divisore D tra due polinomi P e Q è ogni generatore dell'ideale generato da P e Q (il più piccolo ideale contenente sia P che Q); esistono due polinomi H, K tali che $D = HP + KQ$, e D è un polinomio di grado minimo che si può scrivere in questa forma.*

DIMOSTRAZIONE. Consideriamo l'insieme I dei polinomi della forma $MP + NQ$ al variare di $M, N \in C[X]$. Si tratta chiaramente di un ideale di $C[X]$, quindi si tratta dei multipli di un polinomio D che è di grado minimo in I . Poiché $P, Q \in I$, abbiamo che D divide sia P che Q , e dunque è un divisore comune. Inoltre per definizione esistono due polinomi H, K tali che $D = HP + KQ$. Sia ora D' un divisore comune di P e Q , diciamo $P = P'D'$ e $Q = Q'D'$; allora abbiamo $D = HP + KQ = D = HP'D' + KQ'D' = (HP' + KQ')D'$, da cui si vede che D' divide D . \square

8.5.1. Dal teorema segue che due polinomi P e Q sono primi tra loro se e solo se esistono polinomi H, K tali che $HP + KQ = 1$.

8.5.2. Il teorema e l'osservazione precedente possono estendersi al caso di un numero finito di polinomi; un massimo comun divisore tra i polinomi P_1, P_2, \dots, P_n è ogni polinomio di grado minimo che si scriva nella forma $H_1P_1 + H_2P_2 + \dots + H_nP_n$ con gli H_i polinomi. Inoltre essi sono coprimi (cioè il loro massimo comun divisore è 1) se e solo se esistono dei polinomi H_i tali che $H_1P_1 + H_2P_2 + \dots + H_nP_n = 1$.

8.6. ALGORITMO DI EUCLIDE. Anche per i polinomi possiamo dare un procedimento di calcolo del MCD analogamente a quanto fatto per gli interi, basandoci su un procedimento di divisioni iterate. Si riscriva per bene l'algoritmo, verificando che tutto funzioni.

8.7. TEOREMA (IRRIDUCIBILI, FATTORIZZAZIONE). *Un polinomio di grado positivo (non nullo) si dice irriducibile se non si può scrivere come prodotto di due polinomi di gradi strettamente positivi. Ogni polinomio di grado positivo si scrive in modo essenzialmente unico come prodotto di irriducibili (essenzialmente significa a meno dell'ordine dei fattori e di moltiplicazione dei fattori per invertibili).*

DIMOSTRAZIONE. Si può fare usando la seconda forma dell'induzione; infatti la proprietà è ovvia per i polinomi di grado 1, che sono tutti irriducibili. Se ora F è un polinomio di grado maggiore di 1 e

non irriducibile, esso si esprime come prodotto GH di due polinomi di gradi positivi, ciascuno minore a quello di F ; dunque per ipotesi induttiva essi ammettono una fattorizzazione come nell'enunciato, e di conseguenza anche F (facendo il prodotto delle fattorizzazioni).

Per dimostrare l'unicità della fattorizzazione basta applicare a due distinte fattorizzazioni di uno stesso polinomio il seguente risultato: *se P è un polinomio irriducibile, e P divide un prodotto FG , allora P divide almeno uno dei due fattori; quindi per induzione: se P divide un prodotto di polinomi, allora P divide almeno uno dei fattori.*

Supponiamo infatti che P non divida F , e proviamo che divide G ; siccome F e P sono comprimi abbiamo $1 = FH + PK$ per opportuni polinomi H, K . Moltiplicando per G otteniamo $G = FGH + PGK$, e poiché $FG = PL$ (per ipotesi P divide FG) risulta $G = PLH + PGK = P(LH + GK)$, e dunque P divide G , come si voleva. \square

♠ **8.8.** CORPO DELLE FUNZIONI RAZIONALI. Per ogni corpo C , indichiamo con $C(X)$ e chiamiamo corpo delle funzioni razionali (in X a coefficienti in C) il corpo delle frazioni dell'anello integro $C[X]$. Gli elementi di $C(X)$ sono allora quozienti $\frac{P(X)}{Q(X)}$ con $Q(X) \neq 0$, soggetti alle usuali operazioni di somma e prodotto.

♠♠ **8.9.** ANALOGIA POLINOMI (SU UN CORPO)-INTERI: DOMINI EUCLIDEI, PRINCIPALI, FATTORIALI. Il lettore avrà notato una certa aria di ripetizione studiando interi e polinomi. Questo è dovuto (oltre al copia-incolla-modifica fatto in $\mathbb{T}_E X$ dall'estensore di queste note) ad una analogia assai profonda tra i due casi, che cerchiamo di illustrare qui di seguito.

8.9.1. DEFINIZIONE (DOMINI EUCLIDEI). *Un dominio integro A si dice euclideo se esiste una funzione $\delta : A \setminus \{0\} \rightarrow \mathbb{N}$ detta grado dotata delle seguenti proprietà:*

(E1) $\delta(a) \leq \delta(ab)$ per ogni $a, b \in A$;

(E2) per ogni $a, b \in A$ esistono q e r tali che $a = bq + r$ e $\delta(r) < \delta(b)$ se $r \neq 0$ (algoritmo di divisione euclidea: q si dice quoziente e r resto).

8.9.2. Osserviamo subito che per ogni $a \in A$ abbiamo $\delta(1) \leq \delta(a)$ (segue da (E1)); dunque $\delta(1) \in \mathbb{N}$ è il minimo valore assunto da δ , e (eventualmente sottraendolo alla funzione stessa) possiamo supporre che sia $\delta(1) = 0$.

8.9.3. È quasi immediato osservare che un elemento $a \in A$ è invertibile se e solo se $\delta(a) = \delta(1)$. Infatti se a è invertibile abbiamo $\delta(a) \leq \delta(aa^{-1}) = \delta(1)$ (l'altra disuguaglianza vale per ogni a , come s'è già detto); viceversa, nella divisione $1 = aq + r$ non può essere $\delta(r) < \delta(a)$ se $\delta(a) = \delta(1)$, e dunque $r = 0$, e allora a è invertibile con inverso q .

8.9.4. Possiamo fare una osservazione più sottile: un elemento $a \in A$ è invertibile se e solo se esiste $b \in A$ tale che $\delta(b) = \delta(ab)$ (e allora ciò vale per ogni $b \in A$, non nullo). Infatti se a è invertibile abbiamo $\delta(b) \leq \delta(ab) \leq \delta(a^{-1}ab) = \delta(b)$; viceversa, nella divisione $b = (ab)q + r$ non può essere $\delta(r) < \delta(ab) = \delta(b)$ poiché avremmo anche $\delta(b) \leq \delta(b(1 - aq)) = \delta(r)$, e dunque $r = 0$, e allora da $b = abq$ deduciamo che a è invertibile con inverso q .

8.9.5. L'osservazione precedente si può anche scrivere nella forma: un elemento $a \in A$ non è invertibile se e solo se per ogni $b \in A$ si ha $\delta(b) < \delta(ab)$.

8.9.6. DEFINIZIONE (DOMINI PRINCIPALI). *Un dominio integro A si dice principale se ogni suo ideale è principale, cioè generato da un elemento.*

8.9.7. TEOREMA. *I domini euclidei sono principali.*

DIMOSTRAZIONE. Sia I un ideale non banale, e sia a un suo elemento tale che $\delta(a)$ sia minimo tra i valori della funzione grado sugli elementi di I (essendo \mathbb{N} ben ordinato, $\delta(I)$ ha minimo). Mostriamo che I è l'ideale generato da a . Siccome $a \in I$, basta mostrare che ogni elemento $b \in I$ è multiplo di a . Consideriamo la divisione con resto $b = qa + r$; poiché $a, b \in I$ (e dunque $qa \in I$) abbiamo $r \in I$, e poiché $\delta(r) < \delta(a)$ dev'essere $r = 0$. Dunque $b = qa$ è multiplo di a . \square

8.9.8. I domini principali hanno la proprietà che ogni catena crescente di ideali propri diventa stazionaria, cioè ad un certo punto diventa costante: basta infatti considerare un generatore dell'ideale dato dalla unione degli ideali della catena; poiché esso appartiene all'unione, deve appartenere ad uno degli ideali, e a quel punto la catena diventa stazionaria.

8.9.9. DEFINIZIONE (DOMINI FATTORIALI). *Un dominio integro A si dice fattoriale se ogni suo elemento non nullo si può scrivere in modo essenzialmente unico come prodotto di elementi irriducibili; cioè se ogni elemento a si scrive come prodotto $\prod_{i=1}^m p_i$ di elementi irriducibili, e se $\prod_{j=1}^n q_j$ è un'altra tale scrittura, allora $n = m$ e a meno di riordinare gli indici abbiamo che $p_i = u_i q_i$ con $u_i \in A$ invertibili (cioè p_i e q_i sono associati).*

8.9.10. TEOREMA. *I domini principali sono fattoriali.*

DIMOSTRAZIONE. Osserviamo che dati due elementi a e b di un dominio A , risulta che a divide b se e solo se l'ideale generato da a contiene l'ideale generato da b . Inoltre l'ideale generato da un elemento è massimale se e solo se l'elemento stesso è irriducibile.

Consideriamo allora un elemento a e l'ideale da esso generato; esiste un ideale massimale che lo contiene, e dunque un elemento irriducibile p_1 tale che $a = p_1 a_1$; ripetiamo il procedimento per a_1 ottenendo $a_1 = p_2 a_2$ con p_2 irriducibile, e così via. Gli elementi a, a_1, a_2, \dots generano degli ideali che sono via via più grandi. Poiché abbiamo visto che per i domini principali le catene di ideali propri sono stazionarie, ad un certo punto troviamo un ideale massimale, e quindi una decomposizione di a in un prodotto di irriducibili. \square

8.9.11. Nessuna delle implicazioni opposte è vera: esistono domini fattoriali ma non principali (ad esempio i domini di polinomi in più variabili su un dominio fattoriale), ed esistono domini principali ma non euclidei (un esempio è l'anello $\mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$, ma non è facile discuterlo, vedi ???).

8.9.12. I numeri interi (con la funzione del valore assoluto), i polinomi in una variabile a coefficienti in un corpo (con la funzione del grado), gli interi di Gauss (con la funzione data dalla norma come numeri complessi) sono domini euclidei, e dunque principali e fattoriali.

♠♠ 8.10. Vi sono importanti risultati che riguardano i polinomi a coefficienti in un dominio fattoriale.

8.10.1. Consideriamo il corpo dei quozienti C di A e vogliamo confrontare la fattorizzazione di polinomi in $A[X]$ e in $C[X]$. Ricordiamo che un polinomio in $A[X]$ si dice primitivo se l'insieme dei suoi coefficienti ha 1 come massimo comun divisore.

8.10.2. LEMMA (DI GAUSS). *Sia A un dominio fattoriale.*

- il prodotto di due polinomi primitivi è primitivo;*
- siano $P(X)$ e $F(X)$ polinomi in $A[X]$, e supponiamo $F(X)$ primitivo; se $P(X) = F(X)G(X)$ in $C[X]$ allora anche $G(X) \in A[X]$;*
- se $P(X)$ è polinomio irriducibile in $A[X]$ allora è irriducibile anche in $C[X]$; equivalentemente se un polinomio in $A[X]$ si fattorizza come prodotto di polinomi di grado positivo in $C[X]$, allora si fattorizza anche in $A[X]$.*

DIMOSTRAZIONE. Vedi I. Barsotti, "Appunti di Algebra", lez. 60. \square

8.10.3. POLINOMI A COEFFICIENTI INTERI. In particolare per polinomi in $\mathbb{Z}[X]$, abbiamo che se $a \in \mathbb{Z}$ è uno zero del polinomio (cioè $X - a$ divide il polinomio) allora a divide il termine noto del polinomio. Se $q \in \mathbb{Q}$ è uno zero del polinomio (cioè $X - q$ divide il polinomio) allora espresso $q = a/b$ con $a, b \in \mathbb{Z}$ coprimi, abbiamo che $bX - a$ divide il polinomio stesso, e inoltre a divide il termine noto del polinomio e b divide il termine dominante

8.10.4. CRITERIO DI EISENSTEIN. Sia $F(X) = \sum_{i=1}^n a_i X^i$ un polinomio a coefficienti interi; se un numero primo p divide tutti i coefficienti tranne a_n , ma p^2 non divide a_0 allora $F(X)$ è irriducibile.

8.10.5. Fattorizzazione di $X^p \pm 1$ con p primo. È ben noto che

$$X^p - 1 = (X - 1)(X^{p-1} + X^{p-2} + \dots + X + 1) \quad \text{e} \quad X^p + 1 = (X + 1)(X^{p-1} - X^{p-2} + \dots - X + 1)$$

e tramite il criterio di Eisenstein possiamo concludere che i fattori nelle parentesi a destra sono irriducibili: per il primo conviene osservare che un polinomio $P(X)$ è irriducibile se e solo se per qualche (e allora per ogni) elemento a dell'anello si ha che $P(X - a)$ è irriducibile (nel caso specifico conviene sostituire X con $X + 1$). Il secondo caso si può trattare similmente, oppure osservando che un polinomio $P(X)$ è irriducibile se e solo se il polinomio $P(-X)$ lo è.

8.10.6. TEOREMA. *Se A è un dominio fattoriale, anche $A[X]$ è dominio fattoriale.*

DIMOSTRAZIONE. Vedi I. Barsotti, "Appunti di Algebra", lez. 61. \square

8.10.7. Per induzione sul numero di variabili, potremmo allora dimostrare che ogni anello di polinomi con un numero finito di variabili su un anello fattoriale è esso stesso un anello fattoriale. Con un facile argomento di riduzione al caso finito potremmo allora vedere che qualunque anello di polinomi con un insieme arbitrario di variabili su un dominio fattoriale è fattoriale (uso il condizionale perché non abbiamo veramente definito questi anelli, se non nel caso di una variabile, ma il lettore può pensarci da solo).

8.11. RICERCA DELLE RADICI DEI POLINOMI. È un ben noto problema quello di “cercare le radici di un polinomio”. Si tratta per un polinomio $F(X) \in A[X]$ di trovare i valori $a \in A$ tali che $F(a) = 0$, ovvero tali che $X - a$ divide $F(X)$. Nel caso di polinomi a coefficienti reali o complessi questo problema è stato risolto per i polinomi di grado minore o uguale a quattro da alcuni matematici italiani (Del Ferro, Tartaglia, Cardano, Ferrari) del sedicesimo secolo, mostrando l'esistenza di formule o procedimenti che tramite operazioni algebriche ed estrazioni di radici producono i valori cercati. Nel diciannovesimo secolo, il matematico francese Galois mostrò che non possono esistere formule risolutive per radicali per le equazioni generali di grado superiore al quarto; questo fondamentale risultato e i metodi per dimostrarlo sono oggetto di un corso avanzato (Teoria di Galois). Questi risultati erano già in parte noti a Ruffini e Abel.

Ricorderemo qui le soluzioni classiche, e penseremo a polinomi a coefficienti nei corpi reale o complesso; si può generalizzare quello che diremo a corpi la cui caratteristica sia maggiore del grado del polinomio di cui si cercano le radici.

8.11.1. POLINOMI DI PRIMO GRADO. Un generico polinomio di primo grado è $aX + b$ con $a \neq 0$. In tal caso l'unica radice del polinomio è $x = -\frac{b}{a}$.

8.11.2. POLINOMI DI SECONDO GRADO. Un generico polinomio di secondo grado è $aX^2 + bX + c$ con $a \neq 0$. Un ben noto procedimento di “completamento del quadrato” porta alle formule risolutive già studiate; l'idea è di riscrivere il polinomio in una forma tale che la parte contenente l'incognita X sia un quadrato perfetto:

$4a(aX^2 + bX + c) = 4a^2X^2 + 4abX + 4ac = 4a^2X^2 + 4abX + b^2 - b^2 + 4ac = (2aX + b)^2 - b^2 + 4ac$
da cui si deduce che le radici del polinomio si ottengono quando $2aX + b = \pm\sqrt{b^2 - 4ac}$, e sono

$$x_{1,2} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a},$$

come ben noto. La quantità $\Delta = b^2 - 4ac$ si dice discriminante del polinomio di secondo grado; nel caso in cui questi abbia coefficienti reali, il discriminante permette di capire la configurazione delle radici: vi sono due radici reali, una sola radice (necessariamente reale, detta “radice doppia”) o due radici complesse (necessariamente una coniugata dell'altra) a seconda che il suo discriminante sia positivo, nullo o negativo.

Un metodo alternativo di procedere consiste nella “sostituzione di variabile” $X = Y - \frac{b}{2a}$ che permette di eliminare il termine di primo grado:

$$a\left(Y - \frac{b}{2a}\right)^2 + b\left(Y - \frac{b}{2a}\right) + c = a\left(Y^2 - \frac{b^2}{4a^2} + \frac{c}{a}\right)$$

che evidenzia le radici $y_{1,2} = \pm\sqrt{\frac{b^2}{4a^2} - \frac{c}{a}} = \pm\frac{\sqrt{b^2 - 4ac}}{2a}$ e da cui si arriva subito alle formule usuali.

Ricordiamo infine le ben note relazioni tra radici x_1, x_2 e coefficienti a, b, c , che si ricavano subito dalla fattorizzazione $aX^2 + bX + c = a(X - x_1)(X - x_2)$:

$$x_1 + x_2 = -\frac{b}{a} \quad \text{e} \quad x_1x_2 = \frac{c}{a}.$$

8.11.3. POLINOMI DI TERZO GRADO. Un generico polinomio di terzo grado è $aX^3 + bX^2 + cX + d$ con $a \neq 0$. Usando la “sostituzione di variabile” $X = Y - \frac{b}{3a}$ che permette di eliminare il termine di secondo grado abbiamo:

$$a\left(Y - \frac{b}{3a}\right)^3 + b\left(Y - \frac{b}{3a}\right)^2 + c\left(Y - \frac{b}{3a}\right) + d = a\left(Y^3 + \frac{3ac - b^2}{3a^2}Y + \frac{27a^2d - 9abc + 2b^3}{27a^3}\right)$$

e siamo ridotti a cercare le radici di un polinomio del tipo $Y^3 + pY + q$. Il modo più veloce di procedere ora consiste nella misteriosa sostituzione di Viète $Y = W - \frac{p}{3W}$ che dà

$$\left(W - \frac{p}{3W}\right)^3 + p\left(W - \frac{p}{3W}\right) + q = W^3 - \frac{p^3}{27W^3} + q$$

che ponendo $T = W^3$ e moltiplicando per T ci riporta ad un polinomio di secondo grado $T^2 + qT - \frac{p^3}{27}$. Dalle formule risolutive otteniamo che

$$t_{1,2} = \frac{-q \pm \sqrt{q^2 + 4\frac{p^3}{27}}}{2} = -\frac{q}{2} \pm \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}.$$

Estraendo le radici cubiche di t_1 e t_2 , potremo trovare sei valori per Y , ma ciascuno ripetuto due volte; dunque possiamo trovare i tre valori cercati per X .

Per arrivare alle classiche formule di Cardano, osserviamo che se w è una radice cubica di t_1 , allora $w' = -\frac{p}{3w}$ è radice cubica di t_2 ; infatti

$$-\frac{p^3}{27w^3} = -\frac{p^3}{27} \frac{1}{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} = -\frac{p^3}{27} \frac{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}{\frac{q^2}{4} - (\frac{q^2}{4} + \frac{p^3}{27})} = t_2.$$

Allora possiamo scrivere le radici come

$$y_{1,2,3} = w_{1,2,3} + w'_{1,2,3}$$

dove w_i sono le radici cubiche di t_1 , e w'_i è la corrispondente radice cubica di t_2 tale che $w_i w'_i = -\frac{p}{3}$ (perché?).

Il termine $\Delta = \frac{q^2}{4} + \frac{p^3}{27} = (\frac{q}{2})^2 + (\frac{p}{3})^3$ è detto discriminante della equazione di terzo grado (qualcuno chiama discriminante il termine $D = -108\Delta = -4p^3 - 27q^2$); nel caso che l'equazione abbia coefficienti reali esso permette di distinguere diverse configurazioni delle radici. Se Δ è negativo, allora vi sono tre radici reali distinte; se Δ è positivo allora vi è una radice reale e due radici complesse coniugate; se Δ è zero vi sono radici multiple (un'unica radice se $p = q = 0$ oppure due altrimenti). Non vi sono errori di stampa nelle righe precedenti: il caso di tre radici reali di trova con $\Delta < 0$, e conviene fare qualche disegno con le radici cubiche complesse per capire le asserzioni fatte; in effetti per calcolare le radici reali bisogna fare calcoli con i numeri complessi.

Terminiamo con le relazioni tra radici x_1, x_2, x_3 e coefficienti a, b, c, d , che si ricavano subito dalla fattorizzazione $aX^3 + bX^2 + cX + d = a(X - x_1)(X - x_2)(X - x_3)$:

$$x_1 + x_2 + x_3 = -\frac{b}{a}, \quad x_1x_2 + x_1x_3 + x_2x_3 = \frac{c}{a} \quad \text{e} \quad x_1x_2x_3 = -\frac{d}{a}.$$

Può essere di qualche interesse ricordare come Tartaglia comunicò a Cardano il procedimento per trovare una radice reale di una equazione di terzo grado: non avendo una simbologia algebrica moderna, utilizza dei versi (con intento mnemonico) e una terminologia "geometrica":

<i>Quando che 'l cubo con le cose appresso</i>	Se (vuoi risolvere) $x^3 + px =$
<i>Se agguaglia a qualche numero discreto:</i>	$= q$
<i>Trovami dui altri, differenti in esso;</i>	trova u, v tali che $u - v = q$
<i>Dapoi terrai, questo per consueto,</i>	e
<i>Che 'l loro prodotto, sempre sia eguale</i>	$uv =$
<i>Al terzo cubo delle cose netto;</i>	$= (p/3)^3$.
<i>El residuo poi suo generale,</i>	Allora
<i>Delli lor lati cubi, ben sottratti</i>	$\sqrt[3]{u} - \sqrt[3]{v} =$
<i>Varrà la tua cosa principale.</i>	$= x.$

(a fianco abbiamo "tradotto" in termini più moderni; quali soluzioni trova veramente Tartaglia?). I versi di Tartaglia continuavano poi per trattare altri casi (all'epoca pare che i coefficienti potessero essere solo positivi, per evitare eresie):

*In el secondo, de cotesti atti;
Quando che 'l cubo, restasse lui solo,
Tu osserverai quest'altri contratti,
Del numer farai due tal part' a volo,
Che l' una, in l' altra, si produca schietto,
El terzo cubo delle cose in stolo;
Delle quali poi, per commun precepto,*

*Terrai li lati cubi, insieme gionti,
 El cotal somma, sarà il tuo concetto;
 El terzo, poi de questi nostri conti,
 Se solve col secondo, se ben guardi
 Che per natura son quasi congiunti,
 Questi trovai, et non con passi tardi
 Nel mille cinquecent' e quattro e trenta;
 Con fondamenti ben saldi, e gagliardi;
 Nella Città del mar 'intorno centa.*

(lasciamo al lettore il compito di tradurre, nel caso fosse interessato).

8.11.4. POLINOMI DI QUARTO GRADO. Un generico polinomio di quarto grado è $aX^4 + bX^3 + cX^2 + dX + e$ con $a \neq 0$. Usando la solita “sostituzione di variabile” $X = Y - \frac{b}{4a}$ che permette di eliminare il termine di terzo grado abbiamo:

$$\begin{aligned} & a\left(Y - \frac{b}{4a}\right)^4 + b\left(Y - \frac{b}{4a}\right)^3 + c\left(Y - \frac{b}{4a}\right)^2 + d\left(Y - \frac{b}{4a}\right) + e = \\ & = a\left(Y^4 + \frac{4ac - 3b^2}{4a^2}Y + \frac{16a^2d - 8abc + 2b^3}{16a^3}Y + \frac{256a^3e - 64a^2bd + 16ab^2c - 3b^4}{256a^4}\right) \end{aligned}$$

e siamo ridotti a cercare le radici di un polinomio del tipo $Y^4 + pY^2 + qY + r$. Il metodo di Ferrari consiste ora nell'introdurre un termine U in modo tale che il polinomio si scriva come differenza di due quadrati, e di conseguenza si fattorizzi in polinomi di grado minore di cui si sanno trovare le radici; abbiamo, completando il quadrato contenente Y^4 e pY^2 che

$$Y^4 + pY^2 + qY + r = \left(Y^2 + \frac{p}{2} - \frac{U}{2}\right)^2 - \left(UY^2 - qY + \frac{U^2}{4} + \frac{pU}{2} + \frac{p^2}{4} - r\right)$$

e l'espressione nella seconda parentesi è un quadrato perfetto se il discriminante (come polinomio di secondo grado in Y) si annulla; quindi basta che u sia una radice del polinomio

$$q^2 - 4U\left(\frac{U^2}{4} + \frac{pU}{4} + \frac{p^2}{4} - r\right) = -U^3 - pU^2 - (p^2 - 4r)U + q^2$$

che è di terzo grado in U e che perciò sappiamo trattare con il metodo di Cardano. Se ora u è una radice, il polinomio nelle Y si scrive

$$Y^4 + pY^2 + qY + r = \left(Y^2 + \frac{p}{2} - \frac{u}{2}\right)^2 - u\left(Y - \frac{q}{2u}\right)^2 = \left(Y^2 + vY + \frac{p}{2} - \frac{u}{2} - \frac{q}{2v}\right)\left(Y^2 - vY + \frac{p}{2} - \frac{u}{2} + \frac{q}{2v}\right)$$

se v è una radice quadrata di u . Siamo quindi ridotti a due polinomi di secondo grado nella Y , e le quattro radici che otteniamo sono le radici volute del polinomio di quarto grado.

Terminiamo con le relazioni tra radici x_1, x_2, x_3, x_4 e coefficienti a, b, c, d, e , che si ricavano subito dalla fattorizzazione $aX^4 + bX^3 + cX^2 + dX + e = a(X - x_1)(X - x_2)(X - x_3)(X - x_4)$:

$$\begin{aligned} x_1 + x_2 + x_3 + x_4 &= -\frac{b}{a} \\ x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4 &= \frac{c}{a} \\ x_1x_2x_3 + x_1x_2x_4 + x_1x_3x_4 + x_2x_3x_4 &= -\frac{d}{a} \\ x_1x_2x_3x_4 &= \frac{e}{a}. \end{aligned}$$

9. Esercizi.

9.1. Esercizi su Insiemi, Funzioni e Relazioni.

9.1.1. Quanti insiemi distinti si possono formare usando le operazioni di unione, intersezione e complementare a partire da 2 fissati insiemi A e B ? Scriverli tutti. E a partire da 3 insiemi? E da 4?

9.1.2. Sviluppare le espressioni $(A \cup B) \cap (C \cup D)$ e $(A \cap B) \cup (C \cap D)$. Cosa succede se in particolare $B = D$?

9.1.3. Mostrare che l'insieme $\mathcal{C}(A \times B)$ (si intenda: coppie non appartenenti ad $A \times B$) è unione disgiunta dei tre insiemi $(\mathcal{C}A) \times B$, $(\mathcal{C}A) \times (\mathcal{C}B)$ e $A \times (\mathcal{C}B)$.

9.1.4. Mostrare che l'insieme $(A \times A) \setminus (B \times C)$ è unione dei due insiemi $(A \setminus B) \times A$, $A \times (A \setminus C)$, ed è unione disgiunta dei tre insiemi $(A \setminus B) \times (A \cap C)$, $(A \cap B) \times (A \setminus C)$ e $(A \setminus B) \times (A \setminus C)$. Trovare una descrizione simile per l'insieme $(A \times B) \setminus (C \times D)$.

9.1.5. Scrivere esplicitamente gli elementi dei seguenti insiemi: $\mathcal{P}(\emptyset)$, $\mathcal{P}(\mathcal{P}(\emptyset))$, $\mathcal{P}(\mathcal{P}(\mathcal{P}(\emptyset)))$, $\mathcal{P}(\mathcal{P}(\mathcal{P}(\mathcal{P}(\emptyset))))$.

9.1.6. Mostrare che $A \subseteq B$ se e solo se $\mathcal{P}(A) \subseteq \mathcal{P}(B)$.

9.1.7. Determinare le relazioni tra gli insiemi seguenti:

(a) $\mathcal{P}(A \cup B)$ e $\mathcal{P}(A) \cup \mathcal{P}(B)$; (b) $\mathcal{P}(A \cap B)$ e $\mathcal{P}(A) \cap \mathcal{P}(B)$; (c) $\mathcal{P}(\mathcal{C}A)$ e $\mathcal{C}\mathcal{P}(A)$.

9.1.8. Esplorare le relazioni tra le operazioni di differenza insiemistica e di potenza: esprimere $\mathcal{P}(A \setminus B)$ e $\mathcal{P}(A \Delta B)$.

9.1.9. Per un fissato insieme X si considerino le funzioni $\mathcal{P}(X) \rightarrow \mathcal{P}(X)$ seguenti:

- (a) $u_B : A \mapsto A \cup B$ per un fissato $B \subseteq X$;
 (b) $i_C : A \mapsto A \cap C$ per un fissato $C \subseteq X$;
 (c) le composizioni $u_B \circ i_C$ e $i_C \circ u_B$;
 (d) $A \mapsto X \setminus A$;

per ognuna si dicano le proprietà di iniettività, suriettività ecc., se ne indichino eventualmente le inverse, si studi il loro rapporto con la relazione di inclusione e con le operazioni insiemistiche.

9.1.10. Determinare le relazioni tra i seguenti insiemi (di funzioni):

- (a) $(A \cup B)^C$ e $A^C \cup B^C$; (b) $A^{(B \cup C)}$ e $A^B \times A^C$;
 (c) $(A \cap B)^C$ e $A^C \cap B^C$; (d) $A^{(B \cap C)}$ e $A^B \cup A^C$;
 (e) $(A \times B)^C$ e $A^C \times B^C$; (f) $A^{(B \times C)}$, $(A^C)^B$ e $(A^B)^C$.

9.1.11. Si determini se le funzioni $\mathbb{N} \rightarrow \mathbb{N}$ definite da $f_1(n) = n + 3$ e $f_2(n) = n^2 + 1$ sono iniettive o suriettive ed eventualmente se ne trovino delle inverse destre o sinistre. Stesso problema considerandole come funzioni $\mathbb{Z} \rightarrow \mathbb{Z}$.

9.1.12. Per le seguenti funzioni $f_i : \mathbb{N} \rightarrow \mathbb{N}$, si calcolino le due composizioni possibili e si verifichi se esse commutano tra loro oppure no; si studino inoltre le loro proprietà (iniettività, suriettività, ecc.): $f_1(n) = n + 1$, $f_2(n) = 2n$, $f_3(n) = n + 3$, $f_4(n) = n^2$, $f_5(n) = n^2 + n$.

Stesso problema, ma considerando le funzioni $f_i : \mathbb{Z} \rightarrow \mathbb{Z}$. Che cosa cambia?

9.1.13. Per le funzioni dell'esercizio precedente, descrivere le funzioni immagine inversa e diretta.

9.1.14. Determinare proprietà e composizioni della funzione $f : \mathbb{N} \rightarrow \mathbb{N}$ che manda n in $n/2$ se n è pari, e in 0 altrimenti, e della funzione $g : \mathbb{N} \rightarrow \mathbb{N}$ che manda n in $2n$.

9.1.15. Dare un esempio di funzione $f : A \rightarrow B$ tale che esistano due insiemi $X, X' \subseteq A$ con $X \cap X' = \emptyset$ ma $f(X) \cap f(X') \neq \emptyset$.

9.1.16. Per una funzione $f : A \rightarrow B$, dimostrare che f è iniettiva (risp. suriettiva, biiettiva) se e solo se f_* lo è. Dimostrare inoltre che se f è iniettiva (risp. suriettiva, biiettiva) allora f^* è suriettiva (risp. iniettiva, biiettiva). Valgono i viceversa?

9.1.17. In generale, per una funzione $f : A \rightarrow B$ e per ogni $X \subseteq A$ si è visto che $f^* f_*(X) \supseteq X$; mostrare che f è iniettiva se e solo se vale l'uguaglianza per ogni $X \subseteq A$ (basta per qualche X ?).

Analogamente per ogni $Y \subseteq B$ si è visto che $f_* f^*(Y) \subseteq Y$; mostrare che f è suriettiva se e solo se vale l'uguaglianza per ogni $Y \subseteq B$ (basta per qualche Y ?).

9.1.18. Dare esempi per illustrare che in generale per una funzione $f : A \rightarrow B$ e per $X \subseteq A$ non vi sono rapporti tra $f(A \setminus X)$ e $B \setminus f(X)$.

9.1.19. Sia $f : A \rightarrow B$ una funzione; come si comportano le immagini dirette ed inverse in relazione alle operazioni di differenza insiemistica? Descrivere $f(X \setminus X')$ e $f(X \Delta X')$ per $X, X' \subseteq A$, e $f^*(Y \setminus Y')$ e $f^*(Y \Delta Y')$ per $Y, Y' \subseteq B$.

In particolare mostrare che f è iniettiva se e solo se $f(A \setminus X) = f(A) \setminus f(X)$ per ogni X , o anche se e solo se $f(A \Delta X) = B \Delta f(X)$ per ogni X .

9.1.20. Per una funzione qualsiasi $f : A \rightarrow B$, caratterizzare gli insiemi $X \subseteq A$ tali che $f^*f_*(X) = X$ e gli insiemi $Y \subseteq B$ tali che $f_*f^*(Y) = Y$. È vero che f^* e f_* sono una inversa dell'altra se ristrette a questi sottinsiemi di $\mathcal{P}(A)$ e $\mathcal{P}(B)$?

9.1.21. Si considerino le tre applicazioni seguenti: $p_1 : A \times A \rightarrow A$ che manda (a_1, a_2) in a_1 (prima proiezione), $p_2 : A \times A \rightarrow A$ che manda (a_1, a_2) in a_2 (seconda proiezione), $d : A \rightarrow A \times A$ che manda a in (a, a) (diagonale). Si verifichino le eventuali proprietà di iniettività e suriettività; si calcolino tutte le possibili combinazioni e si dica quali proprietà è possibile dedurre da esse.

9.1.22. Proprietà delle applicazioni $p_A : A \times B \rightarrow A$ e $p_B : A \times B \rightarrow B$ che mandano (a, b) in a e b rispettivamente: per ogni insieme C e per ogni coppia di funzioni $\alpha : C \rightarrow A$ e $\beta : C \rightarrow B$ esiste una unica funzione $f : C \rightarrow A \times B$ tale che $p_A \circ f = \alpha$ e $p_B \circ f = \beta$. Questo stabilisce una biiezione canonica tra $A^C \times B^C$ e $(A \times B)^C$.

9.1.23. Dati due insiemi A e B , definiamo unione disgiunta e indichiamo con $A \sqcup B$ l'insieme $(A \times \{1\}) \cup (B \times \{2\})$. Si verifichi che c'è una biiezione canonica tra $A \sqcup B$ e $B \sqcup A$.

Le due funzioni $i_A : A \rightarrow A \sqcup B$ e $i_B : B \rightarrow A \sqcup B$ che mandano a in $(a, 1)$ e b in $(b, 2)$ rispettivamente, godono della seguente proprietà: per ogni insieme C e per ogni coppia di funzioni $\alpha : A \rightarrow C$ e $\beta : B \rightarrow C$ esiste una unica funzione $f : A \sqcup B \rightarrow C$ tale che $f \circ i_A = \alpha$ e $f \circ i_B = \beta$. Questo stabilisce una biiezione canonica tra $C^A \times C^B$ e $C^{A \sqcup B}$.

Si mostri che esiste una funzione canonica $A \sqcup B \rightarrow A \cup B$, che è sempre suriettiva ed è iniettiva se e solo se $A \cap B = \emptyset$.

9.1.24. Sia $R \subseteq A \times B$ una relazione tra A e B ; mostrare che essa è grafico di una funzione di A in B se e solo se la funzione $p_A : R \rightarrow A$ che manda (a, b) in a è biiettiva. Quando R è grafico di una funzione di B in A ?

9.1.25. Studiare la stabilità delle proprietà di una relazione (essere grafico, essere simmetrica, riflessiva, transitiva, antisimmetrica, ecc.) passando alla relazione trasposta.

9.1.26. Nel piano della geometria euclidea elementare, si consideri sull'insieme delle rette la relazione di parallelismo. Mostrare che si tratta di una relazione di equivalenza (se ogni retta viene considerata parallela a se stessa!) e se ne descrivano le classi di equivalenza.

9.1.27. Nel piano della geometria euclidea elementare, si consideri sull'insieme delle rette la relazione di incidenza (due rette sono in relazione se e solo se si intersecano). Di che proprietà gode questa relazione? Si studi la relazione di equivalenza generata e se ne descrivano le classi di equivalenza.

9.1.28. Nello spazio della geometria euclidea elementare, si consideri sull'insieme delle rette (risp. dei piani) la relazione di parallelismo (essere parallele per due rette significa stare su uno stesso piano e lì essere parallele). Mostrare che si tratta di una relazione di equivalenza (se ogni retta, risp. piano, viene considerata parallela a se stessa) e se ne descrivano le classi di equivalenza.

9.1.29. Nello spazio della geometria euclidea elementare, si consideri sull'insieme delle rette (risp. dei piani) la relazione di incidenza (due rette, risp. piani, sono in relazione se e solo se si intersecano). Di che proprietà gode questa relazione? Si studi la relazione di equivalenza generata e se ne descrivano le classi di equivalenza.

9.1.30. Nell'insieme \mathbb{Z} definiamo che $a \sim b$ se e solo se $a - b$ è un numero pari (divisibile per 2). Si tratta di una relazione di equivalenza? Eventualmente quali sono le classi di equivalenza?

9.1.31. Nell'insieme \mathbb{Z} definiamo che $a \sim b$ se e solo se $a - b$ è un numero dispari (non divisibile per 2). Si tratta di una relazione di equivalenza? Eventualmente qual'è la relazione di equivalenza generata, e quali sono le sue classi di equivalenza?

9.1.32. Nell'insieme \mathbb{N} dei numeri naturali definiamo la relazione $n|m$ (letto "n divide m") se m è un multiplo di n , ovvero se $m = pn$ per qualche $p \in \mathbb{N}$. Si tratta di una relazione d'ordine? È totale? Vi sono elementi primo e ultimo? Come sono fatti i sottinsiemi totalmente ordinati per la divisibilità?

9.1.33. Nell'insieme \mathbb{Z} dei numeri interi definiamo la relazione $n|m$ (letto "n divide m") se m è un multiplo di n , ovvero se $m = pn$ per qualche $p \in \mathbb{Z}$. Mostrare che si tratta di una relazione riflessiva e transitiva. Si tratta di una relazione d'ordine? Considerare l'equivalenza $n \sim m$ se e solo se $n|m$ e $m|n$; descrivere l'insieme \mathbb{Z}/\sim e l'ordine indotto dalla divisibilità.

9.1.34. Dire quali delle seguenti funzioni $f_i : \mathbb{N} \rightarrow \mathbb{N}$ sono ordinate, sia per l'ordine \leq , sia per il preordine di divisibilità $|$: $f_1(n) = n + 1$, $f_2(n) = 2n$, $f_3(n) = n + 3$, $f_4(n) = n^2$, $f_5(n) = n^2 + n$.

9.2. Esercizi su Cardinali, Naturali, Combinatoria.

9.2.1. Dati tre cardinali α , β e γ , mostrare che

- (a) $(\alpha\beta)^\gamma = \alpha^\gamma \beta^\gamma$;
- (b) $\alpha^{\beta\gamma} = (\alpha^\beta)^\gamma = (\alpha^\gamma)^\beta$;
- (c) se $\alpha \leq \beta$ allora $\alpha + \gamma \leq \beta + \gamma$, $\alpha\gamma \leq \beta\gamma$, $\alpha^\gamma \leq \beta^\gamma$, $\gamma^\alpha \leq \gamma^\beta$.

9.2.2. Per ogni due insiemi finiti A e B , mostrare che $|A \setminus B| + |A \cap B| = |A|$, e che se $B \subseteq A$ allora $|A \setminus B| = |A| - |B|$. E per insiemi infiniti?

9.2.3. Siano A e B due insiemi. È vero o falso che $|A| + |B| = |A|$ implica $|B| = 0$? È vero o falso che $|A| \cdot |B| = |A|$ implica $|B| = 1$? Dare esempi e controesempi.

9.2.4. Mostrare le seguenti relazioni:

- (a) $|\mathbb{Z}| = |\mathbb{N}|$;
- (b) $|\mathbb{Q}| = |\mathbb{N}|$;
- (c) $|\mathbb{R}| = |[0, 1]| = |(0, 1)|$ (con le notazioni usuali: $[0, 1]$ e $(0, 1)$ sono gli intervalli dei numeri reali compresi tra 0 e 1, inclusi gli estremi o esclusi gli estremi);
- (d) $|\mathbb{R}| > |\mathbb{N}|$;

9.2.5. Si confrontino le cardinalità dei seguenti insiemi:

- (a) $\mathbb{N}^{\mathbb{N}}$, insieme delle funzioni di \mathbb{N} in \mathbb{N} in sè;
- (a') l'insieme delle funzioni di \mathbb{N} in $\mathbb{N} \setminus \{0\}$;
- (b) insieme delle funzioni (strettamente) crescenti di \mathbb{N} in \mathbb{N} in sè
- (c) insieme delle funzioni decrescenti di \mathbb{N} in \mathbb{N} in sè
- (d) insieme delle funzioni di \mathbb{N} in \mathbb{N} in sè che siano “quasi sempre nulle”, cioè che hanno valori diversi da zero solo per un numero finito di elementi;
- (e) insieme delle funzioni di \mathbb{N} in \mathbb{N} in sè che siano additive (cioè le funzioni f tali che $f(n + n') = f(n) + f(n')$ per ogni $n, n' \in \mathbb{N}$);
- (f) insieme delle funzioni di \mathbb{N} in \mathbb{N} in sè che siano moltiplicative (cioè le funzioni f tali che $f(nn') = f(n)f(n')$ per ogni $n, n' \in \mathbb{N}$).

9.2.6. Verificare la formula di inclusione-esclusione per 3, 4, n insiemi (induzione).

9.2.7. Dimostrare le formule seguenti riguardo ai coefficienti binomiali:

- (a) $\binom{n}{k} = \sum_{i=1}^n \binom{n-i}{k-1}$
- (b) $\binom{n}{k} = \sum_{i=0}^n \binom{n-i}{k-i+1}$
- (c) $\sum_{i=0}^n \binom{n}{i} = 2^n$
- (d) $\sum_{i=0}^n (-1)^i \binom{n}{i} = 0$
- (e) $\sum_{i=0}^p \binom{n}{i} \binom{n-i}{p-i} = 2^n \binom{n}{p}$

Se possibile, se ne dia una interpretazione combinatorica.

9.2.8. Studiare la funzione ricorsivamente definita da $s(1) = 1$ e $s(n+1) = s(n) + (-1)^n n$.

9.2.9. Studiare la funzione ricorsivamente definita da $f(n, k) = f(n-1, k)f(n-1, k-1)$ e $f(n, 0) = s$, $f(n, n) = s$ per ogni $n \in \mathbb{N}$.

9.2.10. Studiare gli sviluppi del trinomio $(x+y+z)^n$ per ogni $n \in \mathbb{N}$, analogamente a quanto fatto per il binomio; in particolare definire dei coefficienti trinomiali e discutere le loro relazioni ricorsive.

9.2.11. Calcolare la somma dei primi n numeri naturali dispari e la somma dei primi n numeri naturali pari per ogni n . Dare una dimostrazione per induzione del proprio risultato.

9.2.12. Determinare, e dimostrare per induzione la correttezza del proprio risultato, le somme

- (a) $\sum_{i=1}^n (-1)^i i$ per ogni n naturale.
- (b) $\sum_{i=1}^n (-1)^i i^2$ per ogni n naturale.
- (c) $\sum_{i=1}^n 2^i$ per ogni n naturale.
- (d) $\sum_{i=1}^n (-1)^i 2^i$ per ogni n naturale.

9.2.13. Mostrare che $\sum_{i=1}^n i \cdot i! = (n+1)! - 1$ per ogni $n \in \mathbb{N}$.

9.2.14. Mostrare che $\sum_{k=1}^n (1+a^k) = n + a \frac{a^n - 1}{a - 1}$ per ogni $n \in \mathbb{N} \setminus \{0\}$ e per ogni $a \in \mathbb{R} \setminus \{1\}$.

9.2.15. DISUGUAGLIANZE DI BERNOULLI.

- (a) Dimostrare che per ogni $n \in \mathbb{N}$ e ogni $x \in \mathbb{R}$ con $x > -1$ si ha $(1+x)^n \geq 1+nx$ (e vale l'uguaglianza se e solo se $x=0$ oppure $n \in \{0,1\}$);
 (b) Dimostrare che per ogni $n \in \mathbb{N}$ e ogni $x \in \mathbb{R}$ con $\frac{1}{n} > x > -1$ si ha $\frac{1}{1-nx} \geq (1+x)^n$.

9.2.16. Dimostrare che per ogni $n \in \mathbb{N}$ abbiamo

$$(1+a_1) \cdots (1+a_n) \geq 1+a_1+\cdots+a_n$$

se $a_i \in \mathbb{R}$ hanno tutti lo stesso segno e sono tutti maggiori di -1 .

9.2.17. CONFRONTO DELLE MEDIE ARITMETICA E GEOMETRICA. Per ogni $n \in \mathbb{N}$ positivo e ogni famiglia a_1, \dots, a_n di reali positivi, la media aritmetica è $m = \frac{1}{n} \sum_{i=1}^n a_i$, mentre la media geometrica è $g = (\prod_{i=1}^n a_i)^{1/n}$. Mostrare che $m \geq g$ (e vale l'uguaglianza se e solo se tutti gli a_i sono uguali). Convieni dimostrare che

$$\prod_{i=1}^n a_i \leq \left(\frac{1}{n} \sum_{i=1}^n a_i \right)^n$$

procedendo per induzione, e ragionando nel passo induttivo nel modo seguente: se uno degli a_i , diciamo l'ultimo, coincide con la media aritmetica, allora ci si riconduce subito all'ipotesi induttiva; altrimenti vi saranno un a_i , diciamo l'ultimo, che è superiore alla media aritmetica (sia $a_{n+1} = M+c$ con c positivo), e un altro a_i , diciamo il penultimo, che è inferiore alla media aritmetica (sia $a_n = M-d$ con d positivo): si sostituisca a_{n+1} con M , e a_n con $M+c-d$.

9.2.18. Per un poligono piano, si dicono diagonali i segmenti che uniscono due vertici non adiacenti; quante diagonali ha un poligono con n vertici?

9.2.19. Dati n punti nel piano, a tre a tre non allineati, quanti triangoli distinti è possibile formare? E se fossero punti nello spazio?

9.2.20. Quante parole con meno di 5 caratteri si possono formare con alfabeti di due lettere, di tre lettere, di quattro lettere, di cinque lettere, e in generale di n lettere?

Quante di queste parole non hanno lettere consecutive uguali?

9.2.21. In quanti modi si possono distribuire 18 palline uguali in 5 cassetti diversi? E facendo in modo che nessun cassetto rimanga vuoto? E facendo in modo che due siano vuoti? E facendo in modo che due fissati siano vuoti?

9.2.22. In quanti modi si possono distribuire 5 palline uguali in 18 cassetti diversi? E facendo in modo che ogni cassetto abbia al più una pallina?

9.2.23. Nove persone cenano seduti ad un tavolo circolare; in quanti modi diversi si possono disporre? E se fossero su una panchina? Se ci fossero 3 coppie di gemelli identici, quante disposizioni potrebbe distinguere un osservatore?

9.2.24. Quanti sono i numeri di n cifre (nella notazione decimale) divisibili per cinque?

9.2.25. Quanti sono i numeri di n cifre (nella notazione decimale), ognuna non nulla, tale che ogni cifra sia non minore della seguente?

9.2.26. Quanti sono i numeri di 9 cifre (nella notazione decimale) contenenti tre volte la cifra 1, due volte ciascuna le cifre 3, 5, 7?

9.2.27. Quanti sono i numeri dispari di tre cifre distinte (nella notazione decimale)? E di quattro? E di n ?

9.2.28. Scrivere tutti gli elementi di \mathfrak{S}_2 e tutti i possibili quozienti di questo gruppo.

9.2.29. Scrivere tutti gli elementi di \mathfrak{S}_3 e tutti i possibili quozienti di questo gruppo.

9.2.30. Scrivere tutti gli elementi di \mathfrak{S}_4 e tutti i possibili quozienti di questo gruppo.

9.2.31. Studiare decomposizione in cicli, in scambi e segno delle seguenti permutazioni:

- (a) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 4 & 1 & 2 & 3 \end{pmatrix}$;
 (b) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 1 & 3 & 6 & 5 & 7 & 4 & 2 \end{pmatrix}$;
 (c) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 1 \end{pmatrix}$;

$$(d) \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 5 & 8 & 9 & 2 & 1 & 4 & 3 & 6 & 7 \end{pmatrix}.$$

9.2.32. Mostrare che per ogni $\sigma \in \mathfrak{S}_n$ esiste un intero $m \leq n!$ tale che σ^m sia la permutazione identica. È vero o falso che esiste un intero $m \leq n!$ tale che σ^m sia uno scambio? È vero o falso che esiste un intero $m \leq n!$ tale che σ^m sia una permutazione appartenente ad \mathfrak{A}_n ?

***9.2.33.** LEMMA DEI MATRIMONI. Dati due insiemi M e F , e una funzione $p : M \rightarrow \mathcal{P}(F)$, esiste una applicazione iniettiva $f : M \rightarrow F$ tale che $f(m) \in p(m)$ per ogni $m \in M$ se e solo se per ogni $H \subseteq M$ si ha $|\bigcup_{m \in H} p(m)| \geq |H|$.

9.3. Esercizi su Interi, Divisione, MCD.

9.3.1. Eseguire le divisioni con resto tra le seguenti coppie di interi:

(a) 1965 e 23; (b) 1985 e 29; (c) 2004 e 109.

9.3.2. Calcolare il MCD tra le seguenti coppie di interi, e i coefficienti della loro combinazione che lo calcolano:

(a) 300 e 325; (b) 198 e 288; (c) 576 e 840. (d) 630 e 132; (e) 285 e 126.

9.3.3. Se $a = qb + r$ è la divisione con resto di a per b con a, b positivi, scrivere quoziente e resto delle divisioni di a per $-b$, di $-a$ per b e di $-a$ per $-b$.

9.3.4. Mostrare che $\text{MCD}(ac, bc) = c\text{MCD}(a, b)$.

9.3.5. Mostrare che $\text{MCD}(a, b+za) = \text{MCD}(a, b)$ se $z \in \mathbb{Z}$. Usare questo risultato per giustificare l'algoritmo di Euclide di calcolo del massimo comun divisore.

9.3.6. Mostrare che $\text{MCD}(a, bc)$ divide, e in generale non coincide, con il prodotto $\text{MCD}(a, b)\text{MCD}(a, c)$. Mostrare che $\text{MCD}(a, bc) = \text{MCD}(a, b)\text{MCD}(a, c)$ se $\text{MCD}(b, c) = 1$ (cioè se b e c sono coprimi).

9.3.7. Siano $a = qb + r$ e $a' = q'b + r'$ le divisioni con resto di a e a' per b . Cosa possiamo dire delle divisioni con resto di aa' , $a + a'$, $a - a'$ per b ?

9.3.8. Siano $a = qb + r$ e $b = q'c + r$ le divisioni con resto di a per b e di b per c . Cosa possiamo dire della divisione con resto di a per c ?

9.3.9. Date le due divisioni con resto $a = qb + r$ di a per b e $b = q'a + r'$ di b per a , che relazioni vi sono tra q, q', r, r' ?

9.3.10. Scrivere le tavole di somma e moltiplicazione di $\mathbb{Z}/n\mathbb{Z}$ per $n = 2, 3, 4, 5, 6, 7, 8, 9$. Trovare i divisori di zero, i nilpotenti, gli unipotenti, gli invertibili.

È vero che in $\mathbb{Z}/n\mathbb{Z}$ un elemento è o invertibile o divisore di zero?

9.3.11. Studiare iniettività e suriettività della funzione che manda x in x^2 come funzione di \mathbb{Z} in sé e come funzione di $\mathbb{Z}/n\mathbb{Z}$ in sé per $n = 2, 3, 4, 5, 6$.

9.3.12. Idem per la funzione che manda x in x^3 .

9.3.13. Dati $a, b \in \mathbb{N}$, si studi la funzione $f_{(a,b)} : \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$ definita da $f_{(a,b)}(x, y) = ax + by$.

9.3.14. RAPPRESENTAZIONE POSIZIONALE IN BASE QUALSIASI. Sia b un qualunque numero intero maggiore di 1. Dato un numero intero, esso si può rappresentare come sequenza di cifre comprese tra 0 e $b-1$ nel modo seguente: la sequenza $a_n a_{n-1} \cdots a_2 a_1 a_0$ rappresenta il numero $a_n b^n + a_{n-1} b^{n-1} + \cdots + a_2 b^2 + a_1 b + a_0$ (se $b = 10$, allora si tratta della rappresentazione posizionale in base 10). Dato un numero naturale, come trovare la sua rappresentazione posizionale in base b ? [Scrivere un algoritmo, usando ripetutamente la divisione euclidea con resto, per trovare successivamente le cifre a_0, a_1, \dots, a_n].

Di solito per indicare che una sequenza $a_n a_{n-1} \cdots a_1 a_0$ di cifre rappresenta un numero in base b , si scrive la base al pedice del numero: $(a_n a_{n-1} \cdots a_1 a_0)_b$

9.3.15. Come mai noi usiamo la base 10? Che base userebbero le scimmie? E i cartoni animati?

9.3.16. Scrivere nelle basi 2, 3, 4, 8, 16 i seguenti numeri scritti in base 10: 2, 4, 8, 16, 32, 64, 256, 3, 9, 27, 81, 243 (per le basi $b > 10$ si usano come cifre successive a 9 le lettere maiuscole dell'alfabeto nell'ordine alfabetico; per esempio in base 16 le cifre sono 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F).

9.3.17. Esprimere in base 10 i seguenti numeri naturali espressi nella base indicata a pedice: $101010_2, 100_8, 101_8, 115_8, 100_{16}, 101_{16}, 11A_{16}, A1A_{16}, A2C_{16}, FAC_{16}$.

9.3.18. Dare dei criteri per decidere se un numero intero scritto in base 10 è divisibile per 2, 3, 4, 5, 6, 7, 8, 9, 11, 13.

9.3.19. Ricordare la “regola del 9” per il controllo delle moltiplicazioni (e delle somme), e giustificarla in termini di congruenza modulo 9.

9.3.20. Scrivere una regola stenoaritmica per moltiplicare tra loro numeri interi scritti in base decimale la cui ultima cifra è 5; in particolare, per fare il quadrato di un tale numero.

9.3.21. Sia p un fissato numero primo. Per ogni numero intero non nullo n , definiamo l'ordine in p nel modo seguente: $\text{ord}_p(n) = a$ se p^a divide n , e p^{a+1} non divide n (dunque è il massimo esponente a tale che p^a divide n). Abbiamo allora una funzione $\text{ord}_p : \mathbb{Z} \setminus \{0\} \rightarrow \mathbb{N}$; mostrare che soddisfa alle seguenti proprietà:

- (a) $\text{ord}_p(n) = 0$ se e solo se p non divide n ;
- (b) $\text{ord}_p(nm) = \text{ord}_p(n) + \text{ord}_p(m)$ (moltiplicatività);
- (c) $\text{ord}_p(n + m) \geq \min(\text{ord}_p(n), \text{ord}_p(m))$ (quando vale l'uguaglianza? quando la disuguaglianza stretta?);
- (d) se m divide n allora $\text{ord}_p(m) \leq \text{ord}_p(n)$ (vale il viceversa?).
 ord_p è funzione suriettiva? iniettiva?

9.3.22. Calcolare ord_3 e ord_5 dei seguenti interi: 15, 16, 27, 69, 125, 330.

9.3.23. Sia p un fissato numero primo. Per un intero positivo n , calcolare $\text{ord}_p(p^n)$, $\text{ord}_p(p!)$, $\text{ord}_p(p^{n!})$, $\text{ord}_p(n!)$ [usare le cifre in base p], $\text{ord}_p\left(\binom{p}{n}\right)$.

9.3.24. Mostrare che per ogni coppia di numeri interi x e y abbiamo che $(x+y)^p \equiv x^p + y^p \pmod{p}$ (si osservi che i coefficienti binomiali $\binom{p}{i}$ sono divisibili per p se p è primo e $i \neq 0, p$).

Derivare per induzione il piccolo teorema di Fermat: per ogni intero a , abbiamo che $a^p \equiv a \pmod{p}$.

9.3.25. In una scatola ci sono scorpioni, ragni e centopiedi; in totale si contano 282 zampe. Dire se è possibile, ed eventualmente determinare quale può essere il contenuto della scatola.

9.3.26. Dire se esistono, ed eventualmente trovarli, interi x, y, z tali che $6x + 28y + 15z = 1$.

9.3.27. Risolvere la congruenza $16x \equiv 1000 \pmod{27}$.

9.3.28. Discutere il seguente sistema di congruenze:
$$\begin{cases} x \equiv 2 \pmod{7} \\ x \equiv 3 \pmod{6} \end{cases}$$

9.3.29. Discutere il seguente sistema di congruenze:
$$\begin{cases} x \equiv 5 \pmod{28} \\ 10x \equiv 35 \pmod{125} \end{cases}$$

9.3.30. Disponendo di francobolli da 36 e da 45 centesimi, è possibile affrancare un pacco per 2 euro e 34 centesimi? Eventualmente come approssimarlo con la perdita minore? E per un pacco di 3 euro e 51 centesimi?

9.4. Esercizi su Complessi e Polinomi.

9.4.1. Calcolare z^{-1} , w^{-1} , zw , zw^{-1} , $z^{-1}w$, z^2 , z^3 , z^4 , le radici quadrate di z e le radici cubiche di z per le seguenti coppie:

- (a) $z = 1 + i$, $w = 2 - i$;
- (b) $z = 1 - i$, $w = 1 + 2i$;
- (c) $z = 2e^{i\pi/3}$, $w = 3e^{i\pi/4}$
- (d) $z = \cos \frac{\pi}{4} + i \sin \frac{\pi}{4}$, $w = i$
- (e) $z = \cos \vartheta + i \sin \vartheta$, $w = \pm i$

9.4.2. Si studino le proprietà di iniettività, suriettività, eventuali inverse destre e sinistre per le seguenti funzioni $\mathbb{C} \rightarrow \mathbb{C}$:

- (1) $f_1(z) = z^2 + i$;
- (2) $f_2(z) = (z + i)^2$;
- (3) $f_3(z) = z - \bar{z}$;
- (4) $f_4(z) = z/|z|$ se $z \neq 0$, $f_4(0) = 0$.
- (5) $f_5(z) = z/\bar{z}$ se $z \neq 0$, $f_5(0) = 0$.

Per ogni $w \in \mathbb{C}$, si determini la sua controimmagine per ciascuna delle funzioni date.

9.4.3. Si consideri l'insieme $\{z^n \mid n \in \mathbb{N}\}$ per un fissato $z \in \mathbb{C}$; trovare condizioni necessarie e sufficienti affinché:

- (a) l'insieme sia finito;
- (b) l'insieme ammetta una infinità di elementi tra loro allineati;
- (c) l'insieme sia tutto contenuto nel cerchio unitario;
- (d) l'insieme sia tutto esterno al cerchio unitario.

9.4.4. Come l'esercizio precedente per l'insieme delle radici n -esime di z al variare di n .

9.4.5. Definiamo $\mathbb{S}^1 = \{z \in \mathbb{C} \mid |z| = 1\}$ (cerchio unitario o circonferenza unitaria) e $R(1) = \{z \in \mathbb{C} \mid z^n = 1 \text{ per qualche } n \in \mathbb{N}\}$ (radici dell'unità). Mostrare che $R(1) \subseteq \mathbb{S}^1$ e che l'inclusione è stretta. Come si caratterizzano gli elementi di $R(1)$ in termini dell'argomento? Determinare le cardinalità di $R(1)$ e di \mathbb{S}^1 .

9.4.6. È vero che tra due punti di \mathbb{S}^1 si trova sempre qualche punto di $R(1)$ (nel senso della geometria di \mathbb{S}^1 nel piano di Gauss)?

9.4.7. Scrivere (e disegnare sul piano di Gauss) le radici n -esime di $-i$, $1+i$, $1-i$ per $n = 2, 3, 4, 5, 6$.

9.4.8. Determinare $\cos(5t)$, $\cos(8t)$, $\sin(6t)$, $\sin(9t)$ in termini delle funzioni trigonometriche di argomento t (e loro potenze).

9.4.9. Calcolare $\sin^3 t$, $\sin^4 t$, $\cos^5 t$, $\cos^6 t$ in termini delle funzioni trigonometriche di argomento t (e multipli di t).

9.4.10. Dimostrare le formule sul parallelogramma per i numeri complessi, e spiegarne l'interpretazione geometrica.

9.4.11. Dare l'interpretazione geometrica nel piano di Gauss della inversione dei numeri complessi: se $z = \rho e^{i\vartheta}$ allora $z^{-1} = \rho^{-1} e^{-i\vartheta}$.

9.4.12. Dare l'interpretazione geometrica nel piano di Gauss del passaggio all'opposto dei numeri complessi: se $z = \rho e^{i\vartheta}$ allora $-z = \rho e^{(i\vartheta+\pi)}$.

9.4.13. Dare rappresentazioni grafiche nel piano di Gauss per la differenza e la divisione tra numeri complessi.

9.4.14. Rappresentare nel piano di Gauss tutti i logaritmi complessi di e e di ie . Per un qualsiasi $z = \rho e^{i\vartheta}$ disegnare nel piano di Gauss la famiglia dei suoi logaritmi.

9.4.15. Se $|z| = 1$, è vero che le radici n -esime di z si ottengono ruotando opportunamente (e di quanto?) le radici n -esime dell'unità?

9.4.16. Calcolare le lunghezze dei lati dei poligoni regolari di n lati inscritti nella circonferenza unitaria.

9.4.17. Mostrare che la funzione $\mathbb{S}^1 \times \mathbb{R}_{>0} \rightarrow \mathbb{C} \setminus \{0\}$ che manda (ξ, ϱ) nel prodotto $\xi\varrho$ è una biiezione. Scrivere la funzione inversa.

9.4.18. Inversione del cerchio: studiare le funzioni di $\mathbb{C} \setminus \{0\}$ in \mathbb{S}^1 ottenute mandando z in $1/z$ e $1/\bar{z}$. È vero che entrambe rispettano il cerchio unitario (in che senso?)? È vero che invertono interno ed esterno del cerchio unitario? Determinare l'immagine delle "rette verticali".

9.4.19. Il semipiano di Poincaré è definito da $P = \{z \in \mathbb{C} \mid \Im(z) > 0\}$ (numeri complessi la cui parte immaginaria è positiva). Il disco unitarietà è $D = \{z \in \mathbb{C} \mid |z| < 1\}$ (numeri complessi di modulo strettamente inferiore a 1). Mostrare che la funzione $f(z) = \frac{z-i}{z+i}$ è una biiezione $P \rightarrow D$.

Determinare l'immagine della semicirconferenza di centro origine e raggio 1; e della semiretta verticale passante per l'origine.

Mostrare che i tratti di circonferenze di centro il punto $-i$ sono mandati in tratti di circonferenze di centro il punto 1.

9.4.20. Siano a, b, c, d numeri reali tali che $ad - bc = 1$. Consideriamo la funzione (detta trasformazione lineare fratta) $s : P \rightarrow P$ (P è il semipiano di Poincaré) data da $s(z) = \frac{az+b}{cz+d}$.

Mostrare che $\Im(s(z)) = \frac{\Im(z)}{|cz+d|^2}$, cosicché in effetti s è definita da P a P .

Mostrare che s può essere scritta come composizione di funzione dei seguenti tre tipi: traslazione reale ($z \mapsto z + u$ con $u \in \mathbb{R}$), omotetie reali ($z \mapsto vz$ con $v \in \mathbb{R}$, $v > 0$), controinversioni ($z \mapsto -\frac{1}{z}$).

Descrivere le figure formate da $s(z)$ se z descrive le semicirconferenze con centro sull'asse reale, oppure le semirette ortogonali all'asse reale.

9.4.21. Fattorizzare in $\mathbb{Q}[X]$ i seguenti polinomi:

- (a) $6X^4 - 11X^3 - X^2 - 4$;
- (b) $2X^3 + 12X^2 + 13X + 15$;
- (c) $6X^5 + 11X^4 - X^3 + 5X - 6$;
- (d) $X^6 + 3X^5 + 4X^4 + 3X^3 - 15X^2 - 16X + 20$;
- (e) $2X^6 + X^5 - 9X^4 - 6X^3 - 5X^2 - 7X + 6$;

9.4.22. Eseguire la divisione tra i seguenti polinomi:

- (a) $4X^3 + X^2$ e $X + 1 + i$
- (b) $2X^4 - 3X^3 + 4X^2 - 5X + 6$ e $X^2 - 3X + 1$
- (c) $X^4 - 2X^3 + 4X^2 - 6X + 8$ e $X - 1$

9.4.23. Determinare il MCD tra i seguenti polinomi:

- (a) $X^6 - 7X^4 + 8X^3 - 7X + 7$ e $3X^5 - 7X^3 + 3X^2 - 7$
- (b) $X^5 + X^4 - X^3 - 3X^2 - 3X - 1$ e $X^4 - 2X^3 - X^2 - 2X - 1$
- (c) X^4 e $(1 - X)^4$.

9.4.24. Mostrare che il MCD tra $X^m - 1$ e $X^n - 1$ è $X^d - 1$ ove d è il MCD tra m ed n . Cioè $(X^m - 1, X^n - 1) = X^{(m,n)} - 1$.

9.4.25. Determinare un polinomio di grado n che abbia n radici fissate; esplicitare i rapporti tra i coefficienti del polinomio e le radici assegnate (relazioni di Viète).

9.4.26. FORMULA DI INTERPOLAZIONE DI LAGRANGE. Determinare un polinomio di grado n che in $a_0, a_1, \dots, a_n \in C$ (tutti distinti) valga rispettivamente $b_0, b_1, \dots, b_n \in C$. Si tratta di

$$F(X) = \sum_{i=0}^n b_i \prod_{\substack{j \neq i \\ j=0, \dots, n}} \frac{(X - a_j)}{(a_i - a_j)}.$$

9.4.27. Discutere la fattorizzazione in $\mathbb{C}[X]$, in $\mathbb{R}[X]$ e $\mathbb{Q}[X]$ dei polinomi $X^n + 1$ per ogni $n \in \mathbb{N}$; lo stesso per $X^n - 1$.

Capitolo I

Spazi Vettoriali

Questo capitolo presenta lo strumento fondamentale per lo sviluppo dei concetti geometrici in termini moderni, che è quello di Spazio Vettoriale. Uno spazio vettoriale è un insieme dotato di alcune strutture algebriche che modellano la nostra esperienza di “muoversi tra i punti di uno spazio geometrico”. In realtà già i primi esempi che ne faremo evidenzieranno che la struttura algebrica di spazio vettoriale ha applicazioni molto più ampie, ed è attualmente usato in ogni ramo della Matematica.

1. Definizione ed esempi fondamentali.

1.1. DEFINIZIONE (SPAZIO VETTORIALE SU UN CORPO). *Uno spazio vettoriale su un corpo C (i cui elementi sono chiamati scalari, in questo contesto) è il dato di un insieme V (i cui elementi sono detti vettori) dotato di due operazioni:*

(S) *somma di vettori: $V \times V \longrightarrow V : (v, w) \mapsto v + w$;*

(P) *prodotto per gli scalari: $C \times V \longrightarrow V : (\alpha, v) \mapsto \alpha v$;*

soggette ai seguenti assiomi:

(S) *V con l'operazione di somma è un gruppo commutativo (o abeliano); cioè:*

(S1) *esiste un elemento neutro $0 \in V$ tale che $v + 0 = v = 0 + v$ ($\forall v \in V$);*

(S2) *l'operazione è associativa, $u + (v + w) = (u + v) + w$ ($\forall u, v, w \in V$);*

(S3) *l'operazione è commutativa, $v + w = w + v$ ($\forall v, w \in V$);*

(S4) *ogni elemento ha opposto, ($\forall v$)($\exists w$) $v + w = 0 = w + v$;*

(P) *l'operazione di moltiplicazione per gli scalari soddisfa alle seguenti proprietà:*

(P1) *unitaria: $1v = v$ ($\forall v \in V$);*

(P2) *associativa: $\alpha(\beta v) = (\alpha\beta)v$ ($\forall \alpha, \beta \in C, \forall v \in V$);*

(P3) *lineare sugli scalari: $(\alpha + \beta)v = \alpha v + \beta v$ ($\forall \alpha, \beta \in C, \forall v \in V$);*

(P4) *lineare sui vettori: $\alpha(v + w) = \alpha v + \alpha w$ ($\forall \alpha \in C, \forall v, w \in V$).*

Si osservi che nella definizione abbiamo usato gli stessi simboli con significati diversi: per esempio il simbolo $+$ denota sia la somma in V che la somma in C , il simbolo 0 denota sia lo zero di V (che potremmo chiamare 0_V , se ci fossero possibilità di equivoco), sia lo zero di C (che potremmo chiamare 0_C). Capiterà spesso di incorrere in questi abusi di linguaggio allo scopo di rendere meno pedante il testo; il lettore è invitato a riflettere e distinguere in ogni formula gli eventuali abusi.

A partire dalla definizione si può trarre una piccola messe di risultati algebrici, quali per esempio:

1.1.1. UNICITÀ DELLO ZERO. L'elemento 0 dello spazio vettoriale V è unico; se infatti ve ne fossero due con la proprietà (S1), diciamo 0 e $0'$, avremmo $0 = 0 + 0' = 0'$.

1.1.2. UNICITÀ DELL'OPPOSTO. Per ogni $v \in V$, l'elemento w tale che $v + w = 0$ è unico; infatti, se ce ne fossero due, w e w' , avremmo $w = w + 0 = w + (v + w') = (w + v) + w' = 0 + w' = w'$.

1.1.3. RELAZIONE TRA OPPOSTO E -1 . Per ogni $v \in V$, l'opposto è l'elemento $(-1)v$; infatti $v + (-1)v = (1 - 1)v = 0v = 0$. Di solito quindi scriveremo $-v$ per indicare l'opposto di v .

1.1.4. OPPOSTO DELL'OPPOSTO. Risulta $-(-v) = v$; infatti $(-v) + v = 0$.

1.1.5. LEGGI DI CANCELLAZIONE. Dalla uguaglianza $v + w = u + w$ si deduce $v = u$; infatti basta sommare ad entrambi i lati dell'uguaglianza l'opposto di w . Da $\alpha v = \alpha u$ con $\alpha \in C$, $\alpha \neq 0$ abbiamo $v = u$; infatti basta moltiplicare entrambi i membri per l'inverso di α in C . Da $\alpha v = \beta v$ con $\alpha, \beta \in C$ e $v \neq 0$ si ha $\alpha = \beta$ (perché?).

1.1.6. LEGGE DI ANNULLAMENTO. Dalla uguaglianza $\alpha v = 0$ si deduce che $\alpha = 0$ oppure $v = 0$.

Non insisteremo ulteriormente su questi piccoli risultati ed altri analoghi, che verranno d'ora in poi tacitamente usati.

1.2. ESEMPI FONDAMENTALI. Diamo di seguito alcuni fondamentali esempi di spazi vettoriali; sono tutti estremamente importanti e verranno costantemente usati, quindi invitiamo il lettore ad uno studio accurato di questi casi.

1.2.1. SPAZI VETTORIALI STANDARD. L'insieme delle n -uple

$$\left\{ \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} : x_i \in C \text{ per } i = 1, \dots, n \right\}$$

si indica con $V_n(C)$ o semplicemente C^n e si dice lo spazio vettoriale standard (di dimensione n) sul corpo C . La somma dei suoi elementi si definisce "componente per componente", cioè

$$\text{se } x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \text{ e } y = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} \text{ allora } x + y = \begin{pmatrix} x_1 + y_1 \\ \vdots \\ x_n + y_n \end{pmatrix}$$

e il prodotto per gli scalari si definisce analogamente

$$\text{se } x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \text{ e } \alpha \in C \text{ allora } \alpha x = \begin{pmatrix} \alpha x_1 \\ \vdots \\ \alpha x_n \end{pmatrix}.$$

Si verifica subito che le condizioni della definizione sono tutte soddisfatte; in particolare lo zero di $V_n(C)$ è la n -upla con tutte le componenti nulle (lo zero di C).

1.2.2. POLINOMI. L'insieme dei polinomi in una variabile X e coefficienti in C si indica con $C[X]$ ed è dotato dalle usuali operazioni di una struttura di spazio vettoriale su C : somma e prodotto per gli scalari sono definiti da

$$\text{se } P(X) = \sum_{i=0}^n \alpha_i X^i \text{ e } Q(X) = \sum_{i=0}^m \beta_i X^i \text{ allora } P(X) + Q(X) = \sum_{i=0}^{\max(n,m)} (\alpha_i + \beta_i) X^i$$

e

$$\text{se } P(X) = \sum_{i=0}^n \alpha_i X^i \text{ e } \alpha \in C \text{ allora } \alpha P(X) = \sum_{i=0}^n \alpha \alpha_i X^i$$

(ove si intende $\alpha_i = 0$ se $i > n$ e $\beta_i = 0$ se $i > m$). Si verificano subito le proprietà richieste. Ricordiamo che nell'insieme dei polinomi è definito anche un prodotto tra polinomi e una operazione di composizione, ma per il momento non ce ne occuperemo.

Ricordiamo anche che si dice grado di un polinomio il massimo esponente della variabile che ha coefficiente non nullo: se $P(X) = \sum_{i=0}^n \alpha_i X^i$ allora $\deg P(X) = \max\{i : \alpha_i \neq 0\}$.

Si osservi che $\deg(P(X) + Q(X)) \leq \max(\deg P(X), \deg Q(X))$ e vale l'uguale se $\deg P(X) \neq \deg Q(X)$ (oppure se i polinomi hanno lo stesso grado e coefficienti del termine direttore non opposti).

1.2.3. POLINOMI TRONCATI. Il sottinsieme di $C[X]$ formato dai polinomi di grado minore o uguale ad un fissato numero naturale n , dotato delle usuali operazioni di somma e prodotto per gli scalari, forma uno spazio vettoriale su C che verrà indicato con $C[X]_{\leq n}$.

1.2.4. SERIE FORMALI. L'insieme delle serie in una variabile X e coefficienti in C si indica con $C[[X]]$ ed è dotato dalle usuali operazioni di una struttura di spazio vettoriale su C : somma e prodotto per gli scalari sono definiti esattamente come nel caso dei polinomi (le serie formali sono espressioni del tipo $P(X) = \sum_{i=0}^{\infty} \alpha_i X^i$ con i coefficienti $\alpha_i \in C$, ma le operazioni sono definite sempre usando somma e prodotto del corpo C). I polinomi sono le serie formali per cui i coefficienti sono "quasi tutti nulli", che significa tutti nulli tranne che per un numero finito di indici.

1.2.5. FUNZIONI REALI. Consideriamo l'insieme delle funzioni reali di variabile reale. Anche in questo caso possiamo definire una struttura di spazio vettoriale nel modo seguente:

$$\text{se } f : \mathbb{R} \rightarrow \mathbb{R} \text{ e } g : \mathbb{R} \rightarrow \mathbb{R} \text{ allora } f + g : \mathbb{R} \rightarrow \mathbb{R} \text{ è data da } (f + g)(x) = f(x) + g(x)$$

e

$$\text{se } f : \mathbb{R} \rightarrow \mathbb{R} \text{ e } \alpha \in \mathbb{R} \text{ allora } \alpha f : \mathbb{R} \rightarrow \mathbb{R} \text{ è data da } (\alpha f)(x) = \alpha f(x).$$

Di nuovo notiamo che l'insieme in questione è dotato di una struttura algebrica più ricca (ha anche operazioni di prodotto di funzioni e di composizione di funzioni), ma per il momento non ce ne occuperemo.

I sottinsiemi di questo spazio vettoriale dati dalle funzioni continue, derivabili, differenziabili fino ad un fissato ordine, periodiche di un fissato periodo, sono altrettanti esempi di spazi vettoriali reali.

1.2.6. FUNZIONI A VALORI IN UN CORPO. Più generalmente, consideriamo l'insieme delle funzioni da un fissato insieme X in C (corpo). Anche in questo caso possiamo definire una struttura di spazio vettoriale, sfruttando le operazioni di C , nel modo seguente:

$$\text{se } f : X \rightarrow C \text{ e } g : X \rightarrow C \text{ allora } f + g : X \rightarrow C \text{ è data da } (f + g)(x) = f(x) + g(x)$$

e

$$\text{se } f : X \rightarrow C \text{ e } \alpha \in \mathbb{R} \text{ allora } \alpha f : X \rightarrow C \text{ è data da } (\alpha f)(x) = \alpha f(x).$$

Di nuovo notiamo che l'insieme in questione è dotato di una struttura algebrica più ricca (ha anche l'operazioni di prodotto di funzioni), ma per il momento non ce ne occuperemo.

1.2.7. NUMERI COMPLESSI COME SPAZIO VETTORIALE REALE. Il corpo \mathbb{C} dei numeri complessi può essere visto come spazio vettoriale su \mathbb{R} tramite le usuali operazioni di somma di numeri complessi e prodotto di numeri reali con numeri complessi.

1.3. SPAZI PRODOTTO. Siano V e W spazi vettoriali sullo stesso corpo C ; il prodotto cartesiano $V \times W$ (l'insieme delle coppie ordinate (v, w) con $v \in V$ e $w \in W$) viene dotato della seguente struttura di spazio vettoriale su C , definita "componente per componente": somma $(v, w) + (v', w') = (v + v', w + w')$ e prodotto per scalari $\alpha(v, w) = (\alpha v, \alpha w)$. L'elemento neutro di $V \times W$ risulta subito essere $(0, 0)$.

L'osservazione si generalizza ad un numero finito di spazi. Notare che gli spazi vettoriali standard sono esattamente il prodotto del corpo C con sé stesso n volte.

2. Sottospazi e quozienti.

2.1. DEFINIZIONE (SOTTOSPAZI). *Un sottinsieme W di uno spazio vettoriale V sul corpo C si dice un C -sottospazio vettoriale (o solo sottospazio, se non ci sono ambiguità) se le operazioni di V inducono una struttura di spazio vettoriale su W .*

2.1.1. ESEMPIO (SOTTOSPAZIO NULLO). Il più piccolo sottospazio di V è l'insieme $\{0\}$ contenente solo lo zero. Spesso scriveremo semplicemente 0 per indicare anche il sottospazio nullo $\{0\}$.

2.1.2. ESEMPIO. Il più grande sottospazio di V è l'insieme V stesso.

2.1.3. ESEMPIO. Osservando gli esempi fondamentali, si vede che $C[X]_{\leq n}$ è sottospazio di $C[X]$, che a sua volta è sottospazio di $C[[X]]$; lo spazio delle funzioni reali differenziabili è sottospazio di quello delle funzioni continue, che è sottospazio dello spazio di tutte le funzioni reali.

2.1.4. ESEMPIO. L'insieme delle funzioni $X \rightarrow C$ che valgono 0 in tutto un fissato sottinsieme $Y \subseteq X$ è un sottospazio dello spazio delle funzioni di X in C ; invece l'insieme delle funzioni che valgono costantemente 1 su Y non è un sottospazio.

2.2. PROPOSIZIONE (CRITERI PER SOTTOSPAZI). *Per un sottinsieme W di uno spazio vettoriale V , i fatti seguenti sono equivalenti:*

- (1) W è sottospazio vettoriale di V ;
- (2) valgono le seguenti asserzioni:
 - (i) $0 \in W$ (contiene lo zero);
 - (ii) se $u, v \in W$ allora $u + v \in W$ (è chiuso rispetto alla somma);
 - (iii) se $u \in W$ e $\alpha \in C$ allora $\alpha u \in W$ (è chiuso rispetto al prodotto per gli scalari);
- (3) valgono le seguenti asserzioni:
 - (i) $W \neq \emptyset$ (non è vuoto);
 - (ii) se $u, v \in W$ e $\alpha, \beta \in C$ allora $\alpha u + \beta v \in W$ (contiene tutte le combinazioni lineari di ogni coppia di elementi).

DIMOSTRAZIONE. Sembra facile, ma invitiamo il lettore a capire bene "che cosa" bisogna dimostrare, esplicitando le implicazioni (1) implica (2) e (3), e le opposte (2) implica (1) e (3) implica (1), come pure le due implicazioni dirette tra (2) e (3). \square

2.3. DEFINIZIONE-PROPOSIZIONE (SOTTOSPAZIO GENERATO). Se S è un sottinsieme qualsiasi di V , indichiamo con $\langle S \rangle$ il più piccolo sottospazio vettoriale di V contenente S . Esso ammette le due descrizioni seguenti:

- (1) $\langle S \rangle$ è l'intersezione di tutti i sottospazi vettoriali di V contenenti S ;
- (2) $\langle S \rangle$ è l'insieme di tutte le combinazioni lineari (finite) di elementi di S a coefficienti in C .

DIMOSTRAZIONE. La descrizione (1) è essenzialmente tautologica; l'unica cosa da notare è che l'intersezione di un numero arbitrario, non necessariamente finito, di sottospazi è un sottospazio. Diciamo poi S' l'insieme descritto in (2); certo S' è un sottospazio (verificarlo), e $S' \supseteq S$, da cui $S' \supseteq \langle S \rangle$. Viceversa se W è qualunque sottospazio contenente S , allora $W \supseteq S'$, e passando alla intersezione di tutti questi sottospazi abbiamo $\langle S \rangle \supseteq S'$. Da cui segue $S' = \langle S \rangle$. \square

2.3.1. ESEMPIO (SOTTOSPAZIO NULLO). $\langle \emptyset \rangle = \{0\}$, cioè l'insieme vuoto genera il sottospazio nullo di V , come pure $\langle 0 \rangle = \{0\}$.

2.3.2. ESEMPIO (RETTE). Lo spazio vettoriale generato da un vettore non nullo v è l'insieme di tutti i multipli scalari di v , cioè $\langle v \rangle = \{\lambda v : \lambda \in C\}$, e si dice una retta di V .

2.3.3. ESEMPIO (PIANI). Lo spazio vettoriale generato da due vettori non nulli v e w è l'insieme di tutte le combinazioni lineari di v e w , cioè $\langle v, w \rangle = \{\lambda v + \mu w : \lambda, \mu \in C\}$. Se i due vettori non sono proporzionali (cioè uno non è un multiplo dell'altro) si dice un piano di V . Cosa succede invece se w è multiplo di v ?

2.3.4. NOTA. In generale abbiamo le seguenti proprietà:

- (a) $S \subseteq \langle S \rangle$, e si ha uguaglianza se e solo se S è un sottospazio;
- (b) se $S_1 \subseteq S_2$ allora $\langle S_1 \rangle \subseteq \langle S_2 \rangle$;
- (c) $\langle \langle S \rangle \rangle = \langle S \rangle$;
- (d) $\langle S_1 \rangle \cap \langle S_2 \rangle \supseteq \langle S_1 \cap S_2 \rangle$ (l'uguaglianza in generale è falsa);
- (e) $\langle S_1 \rangle \cup \langle S_2 \rangle \subseteq \langle S_1 \cup S_2 \rangle$ (l'uguaglianza in generale è falsa per un motivo ovvio, vedi sotto).

2.4. INTERSEZIONE E SOMMA DI SOTTOSPAZI. Sia V uno spazio vettoriale su C e siano U_1, U_2 due suoi sottospazi. Allora:

- (1) l'intersezione insiemistica $U_1 \cap U_2$ è un sottospazio vettoriale di V ;
- (2) l'unione insiemistica $U_1 \cup U_2$ in generale *non* è un sottospazio vettoriale di V ; farsi dei controesempi, e poi caratterizzare in generale i casi "fortunati": l'unione di due sottospazi è un sottospazio se e solo se uno dei due è contenuto nell'altro;
- (3) in generale definiamo la somma $U_1 + U_2$ come il sottospazio generato dall'unione insiemistica di U_1 ed U_2 , cioè $U_1 + U_2 = \langle U_1 \cup U_2 \rangle$. Si tratta del più piccolo sottospazio di V contenente sia U_1 che U_2 .

Le considerazioni e le definizioni precedenti si possono estendere ad un numero finito di sottospazi.

2.5. SOMME DIRETTE. Se $U_1 + U_2 = V$ e $U_1 \cap U_2 = 0$ si dice che U_1 e U_2 sono complementari e si scrive $V = U_1 \oplus U_2$.

2.5.1. NOTA. In generale abbiamo $\langle S_1 \rangle + \langle S_2 \rangle = \langle S_1 \cup S_2 \rangle = \langle \langle S_1 \rangle \cup \langle S_2 \rangle \rangle$.

2.6. SPAZI QUOZIENTE. Sia W un sottospazio vettoriale di V ; allora la relazione " $u \sim v$ se e solo se $u - v \in W$ " definisce una relazione di equivalenza in V che rispetta la struttura di spazio vettoriale, di modo che l'insieme quoziente $V/W := V/\sim$ ha una struttura canonica di spazio vettoriale indotta da quella di V . Gli elementi di V/W sono indicati di solito come $[v]$ oppure $v+W$. Quindi le operazioni si scrivono $[v] + [v'] = [v + v']$ (somma di classi) e $\alpha[v] = [\alpha v]$ (prodotto di una classe per uno scalare) e sono ben definite, ovvero non dipendono dai rappresentanti v e v' usati per le classi.

3. Dipendenza e indipendenza lineari.

3.1. DEFINIZIONE (INSIEMI LINEARMENTE (IN)DIPENDENTI). Sia $S \subseteq V$ un sottinsieme di uno spazio vettoriale; S si dice linearmente indipendente (o libero) se per ogni combinazione lineare $\sum_{s \in S} \alpha_s s$ (in cui quasi tutti gli α_s siano nulli) si ha che: $\sum_{s \in S} \alpha_s s = 0$ implica $\alpha_s = 0$ per ogni s . In

caso contrario (esistono combinazioni lineari finite non banali che danno il vettore nullo) S si dice un insieme linearmente dipendente.

3.1.1. ESEMPIO. Un insieme costituito da un solo vettore è linearmente dipendente se e solo se quel vettore è il vettore nullo. Un insieme contenente il vettore nullo è sempre linearmente dipendente; ovvero un insieme linearmente indipendente non può contenere il vettore nullo.

3.1.2. ESEMPIO. Un insieme costituito da due vettori è linearmente dipendente se e solo se uno dei due è multiplo dell'altro.

3.1.3. ESEMPIO. Quando un insieme costituito da tre vettori è linearmente dipendente?

3.1.4. ESEMPIO. Un sottinsieme finito v_1, \dots, v_n è linearmente indipendente se e solo se ognuno dei vettori v_i non appartiene al sottospazio $\langle v_1, \dots, v_{i-1} \rangle$ generato dai precedenti

3.1.5. ESEMPIO. Sottinsiemi di insiemi linearmente indipendenti sono ancora linearmente indipendenti. Sovrainsiemi di insiemi linearmente dipendenti sono ancora linearmente dipendenti.

3.1.6. ESEMPIO. Un sottinsieme S è linearmente indipendente se e solo se per ogni $s \in S$ si ha $s \notin \langle S \setminus \{s\} \rangle$ (verificarlo bene).

3.2. DEFINIZIONE (INSIEMI GENERATORI). *L'insieme S si dice un insieme di generatori per V se $\langle S \rangle = V$, ovvero se ogni elemento $v \in V$ si può scrivere come combinazione lineare $v = \sum_{s \in S} \alpha_s s$ di elementi di S (con gli α_s quasi tutti nulli).*

3.2.1. ESEMPIO. Ovviamente V genera sé stesso, ma noi siamo interessati a trovare sistemi di generatori il più piccoli possibile per uno spazio vettoriale. In particolare ci interessiamo a spazi finitamente generati, cioè che ammettono un insieme finito di generatori.

3.2.2. ESEMPIO. Sovrainsiemi di insiemi generatori sono ancora generatori.

4. Basi e dimensione.

4.1. DEFINIZIONE-TEOREMA (SISTEMI DI GENERATORI INDIPENDENTI). *I fatti seguenti sono equivalenti:*

- (1) S è un sistema di generatori linearmente indipendente;
- (2) S è un insieme massimale di vettori linearmente indipendenti;
- (3) S è un insieme minimale di generatori per V ;

(qui massimale e minimale si intende rispetto all'ordine dato dalle inclusioni come sottinsiemi di V). Ogni tale insieme S si dice una base di V .

DIMOSTRAZIONE. È chiaro che (1) implica sia (2) (se si aggiunge un vettore ad un insieme di generatori, ovviamente si ottiene un insieme linearmente dipendente) che (3) (se si toglie un vettore ad un sistema linearmente indipendente, non può più essere un insieme di generatori).

Mostriamo che (2) implica (1): se S non fosse generatore, si potrebbe trovare $v \in V$ ma non in $\langle S \rangle$ e allora $S \cup \{v\}$ sarebbe linearmente indipendente contenente S , contro la massimalità di S .

Mostriamo che (3) implica (1): se S non fosse libero, si potrebbe trovare $v \in S$ con $v \in \langle S \setminus \{v\} \rangle$ e allora $S \setminus \{v\}$ sarebbe insieme generatore contenuto in S , contro la minimalità di S . \square

4.2. DEFINIZIONE-TEOREMA (BASI E DIMENSIONE). *Tutte le basi di V sono di una fissata cardinalità, dipendente solo da V e da C , che si chiama la dimensione di V su C e si indica con $\dim_C V$.*

4.3. TEOREMA (ESISTENZA DI BASI). *Ogni spazio vettoriale ammette (almeno) una base. Più precisamente:*

- (1) ogni insieme linearmente indipendente si può completare ad una base;
- (2) ogni insieme generatore contiene almeno una base dello spazio.

Questi due risultati si possono dimostrare in modo elementare per gli spazi finitamente generati, mentre si deve ricorrere al Lemma di Zorn nel caso di spazi vettoriali di dimensione arbitraria (non necessariamente finita).

4.4. DIMOSTRAZIONE PER SPAZI DI DIMENSIONE FINITA. Supponiamo che V sia finitamente generato, ovvero ammetta un sistema di generatori formato da un numero finito di vettori.

4.4.1. LEMMA (DELLO SCAMBIO). *Dati un insieme linearmente indipendente $S = \{s_1, \dots, s_k\}$ con k elementi e un insieme generatore $G = \{g_1, \dots, g_h\}$ con h elementi di V , si ha $k \leq h$.*

DIMOSTRAZIONE. La strategia della dimostrazione consiste nel sostituire opportuni elementi di G con elementi di S , ottenendo sempre insiemi di generatori. Alla fine avremo inserito tutti gli elementi di S al posto di (altrettanti) elementi di G , da cui la conclusione che la cardinalità di S doveva essere minore o uguale a quella di G . Vediamo in dettaglio.

Essendo G un insieme generatore, abbiamo che $s_1 = \sum_{j=1}^h a_j g_j$ ove i coefficienti a_j non sono tutti nulli; eventualmente cambiando la numerazione possiamo supporre $a_1 \neq 0$. Allora l'insieme $G_1 = \{s_1, g_2, \dots, g_h\}$ è ancora un sistema di generatori (perché? da notare che bisogna usare $a_1 \neq 0$, e dunque a_1 ammette un inverso in C).

Quindi possiamo procedere e scrivere $s_2 = b_1 s_1 + \sum_{j=2}^h b_j g_j$ ove i coefficienti b_j con $j \neq 1$ non sono tutti nulli (altrimenti s_1 e s_2 formerebbero un insieme dipendente) e possiamo supporre $b_2 \neq 0$. Allora l'insieme $G_2 = \{s_1, s_2, g_3, \dots, g_h\}$ è ancora un sistema di generatori (perché?).

Continuando in questo modo troviamo dopo k passi un insieme $G_k = \{s_1, s_2, \dots, s_k, g_{k+1}, \dots, g_h\}$, da cui segue che $k \leq h$. \square

4.4.2. DIMOSTRAZIONE (DEI TEOREMI). Che tutte le basi abbiano la stessa cardinalità (numero di elementi) segue subito dal lemma (le basi sono sia insiemi linearmente indipendenti, sia sistemi di generatori, quindi due basi possono svolgere sia il ruolo di S che quello di G , dimostrando le due disuguaglianze). Passiamo al teorema di esistenza:

- (1) Dimostriamo un risultato più preciso (lemma di completamento): dato un insieme linearmente indipendente S e un fissato sistema (finito) di generatori G di V , si può completare S a una base di V aggiungendovi opportuni elementi di G .

Se $\langle S \rangle \supseteq G$ abbiamo finito. Altrimenti si comincia scegliendo un elemento g_1 di G che non appartenga al sottospazio $\langle S \rangle$; allora $S_1 = S \cup \{g_1\}$ è ancora linearmente indipendente (perché?).

Di nuovo, se $\langle S_1 \rangle \supseteq G$ abbiamo finito, altrimenti si sceglie un elemento g_2 di G che non appartenga al sottospazio $\langle S_1 \rangle$; allora $S_2 = S_1 \cup \{g_2\}$ è ancora linearmente indipendente (perché?).

Procedendo così, dopo un numero finito p di passi si ha che $\langle S_p \rangle \supseteq G$, e dunque S_p è un insieme (linearmente indipendente e) generatore.

- (2) Consideriamo un insieme generatore G e procediamo scegliendo via via vari elementi da G in modo da formare insiemi linearmente indipendenti, finché è possibile; dopo un numero finito di passi dobbiamo ottenere una base dello spazio. Partiamo scegliendo $g_1 \neq 0$ in G e poniamo $S_1 = \{g_1\}$. Se $\langle S_1 \rangle \supseteq G$ abbiamo finito, altrimenti scegliamo g_2 in G ma non in $\langle S_1 \rangle$ e poniamo $S_2 = S_1 \cup \{g_2\}$ (che è un insieme linearmente indipendente, perché?). Al passo p -esimo avremo un insieme S_p linearmente indipendente con p elementi; se $\langle S_p \rangle \supseteq G$ abbiamo finito, altrimenti scegliamo $g_{p+1} \in G$ non in $\langle S_p \rangle$ e poniamo $S_{p+1} = S_p \cup \{g_{p+1}\}$ (che ancora è insieme linearmente indipendente). Dopo un numero di passi pari alla dimensione dello spazio, abbiamo estratto da G un insieme (linearmente indipendente e) generatore.

Nota che se l'insieme di generatori fosse stato finito, si sarebbe potuto procedere anche al contrario: eliminando via via gli elementi linearmente dipendenti, fino ad ottenere un insieme di generatori indipendenti: descrivere bene il procedimento. \square

4.4.3. PROBLEMA. Sia V uno spazio vettoriale di dimensione finita, e sia W un suo sottospazio. Mostrare che $\dim_C V = \dim_C W$ implica che $V = W$.

Più in generale, siano W_1 e W_2 sottospazi vettoriali di dimensione finita di uno spazio vettoriale V (di dimensione arbitraria). Se $W_1 \subseteq W_2$ e $\dim_C W_1 = \dim_C W_2$ allora $W_1 = W_2$.

♠♠ 4.5. DIMOSTRAZIONE PER SPAZI DI DIMENSIONE ARBITRARIA. Conviene dare un risultato in un contesto un po' più generale, che si applica, oltre che alla discussione per gli spazi vettoriali, anche ad altri contesti in cui una "relazione di dipendenza" con certe proprietà si presenti (ad esempio la "dipendenza algebrica": un numero reale si dice algebrico se esso è radice di un polinomio a coefficienti interi o, equivalentemente, razionali).

I risultati e i metodi qui sviluppati non saranno usati nel seguito, e sono piuttosto difficili; quindi consigliamo di saltare direttamente alla prossima sezione, almeno in prima lettura.

4.5.1. DEFINIZIONE (RELAZIONI DI DIPENDENZA). Sia A un insieme; una relazione $a \in X$ tra elementi e sottinsiemi di A si dice di dipendenza se valgono i seguenti assiomi:

- (D1) se $x \in X$ allora $x \in X$;
 (D2) se $z \in Y$ e $Y \in X$ (i.e. $y \in X$ per ogni $y \in Y$) allora $z \in X$;
 (D3) se $u \in X \cup \{v\}$ e $u \notin X$ allora $v \in X \cup \{u\}$;
 (D4) se $u \in X$ allora esiste una parte finita X' di X tale che $u \in X'$.

4.5.2. DIPENDENZA LINEARE E DIPENDENZA ALGEBRICA. Verificare che le seguenti due definizioni danno luogo a relazioni di dipendenza:

- (a) sia V uno spazio vettoriale; per ogni $v \in V$ e X sottoinsieme di V definiamo “ $v \in X$ se e solo se $v \in \langle X \rangle$ ”;
 (b) sia K un corpo ed H un corpo contenente K ; per ogni $\alpha \in H$ e ogni X sottoinsieme di H definiamo “ $\alpha \in X$ se e solo se α è zero di un polinomio a coefficienti in $K[X]$, o equivalentemente $K(X)$ (minimo sottocorpo di H contenente K e X)”.

4.5.3. DEFINIZIONE-PROPOSIZIONE (INSIEMI GENERATI, GENERATORI). Definiamo per ogni sottoinsieme X di A l'insieme degli elementi dipendenti $\langle X \rangle = \{u \in A \mid u \in X\}$. Per ogni X e Y risulta allora che:

- (1) $X \subseteq \langle X \rangle$;
- (2) se $X \subseteq Y$ allora $\langle X \rangle \subseteq \langle Y \rangle$;
- (3) $\langle \langle X \rangle \rangle = \langle X \rangle$;
- (4) $\langle X \cup Y \rangle = \langle \langle X \rangle \cup \langle Y \rangle \rangle$ (ma $\langle X \cap Y \rangle$ in generale è strettamente contenuto in $\langle \langle X \rangle \cap \langle Y \rangle \rangle = \langle X \rangle \cap \langle Y \rangle$).

Un sottoinsieme X si dice insieme di generatori, o insieme generatore, per A se $\langle X \rangle = A$.

4.5.4. DEFINIZIONE-PROPOSIZIONE (INSIEMI CHIUSI). Diciamo che un insieme è chiuso per la relazione se $\langle X \rangle = X$ (dunque se e solo se $\langle X \rangle \subseteq X$, cioè se $u \in X$ implica $u \in X$). Allora:

- (1) ogni $\langle X \rangle$ è chiuso per la relazione;
- (2) se due insiemi sono chiusi per la relazione, anche la loro intersezione lo è (ma l'unione no, in generale);
- (3) $\langle \emptyset \rangle$ è il minimo e A il massimo tra i chiusi per la relazione.
- (4) La classe dei sottoinsiemi di A chiusi per la relazione è un reticolo (non distributivo) con minimo e massimo sotto le operazioni di inf data da $X \wedge Y = X \cap Y$ e sup data da $X \vee Y = \langle X \cup Y \rangle$.

Due insiemi X e Y chiusi per la relazione si dicono sghembi se $X \wedge Y = \langle \emptyset \rangle$.

4.5.5. DIPENDENZA LINEARE E DIPENDENZA ALGEBRICA. Gli insiemi chiusi per la relazione di dipendenza lineare sono i sottospazi vettoriali di V ; gli insiemi chiusi per la relazione di dipendenza algebrica sono i sovracorpi di K contenuti in H e algebricamente chiusi in H .

4.5.6. DEFINIZIONE-PROPOSIZIONE (INSIEMI IRRIDUCIBILI). Un sottoinsieme X si dice irriducibile se per ogni $x \in X$ si ha $x \notin X \setminus \{x\}$, riducibile altrimenti. In particolare:

- (1) il sottoinsieme vuoto \emptyset è irriducibile; un singoletto $\{x\}$ è riducibile sse $x \in \emptyset$, sse $x \in \langle \emptyset \rangle$.
- (2) Se X è irriducibile, e $X \cup \{u\}$ è riducibile, allora $u \in X$.
- (3) un insieme X è irriducibile se e solo se ogni suo sottoinsieme finito lo è (equivalentemente, X è riducibile se e solo se contiene un insieme finito riducibile).
- (4) Se X è irriducibile e $u \in X$ allora la classe $\{Z \subseteq X \mid u \in Z\}$ ha elemento minimo per l'inclusione che è un sottoinsieme finito.

4.5.7. DIPENDENZA LINEARE E DIPENDENZA ALGEBRICA. Gli insiemi irriducibili per la relazione di dipendenza lineare sono i sottoinsiemi linearmente indipendenti di V ; gli insiemi irriducibili per la relazione di dipendenza algebrica sono i sottoinsiemi (formati da elementi di H) trascendenti su K .

4.5.8. DEFINIZIONE-TEOREMA (BASI). Un insieme irriducibile di generatori per A si dice una base di A (per la relazione di dipendenza). Sia Y un insieme di generatori per A ; allora

- (1) Y contiene (almeno) una base di A ;
- (2) se X è un sottoinsieme irriducibile contenuto in Y , allora X è contenuto in qualche base di A contenuta in Y .
- (3) Due qualsiasi basi di A sono equipotenti.

DIMOSTRAZIONE. Vedi Barsotti “Appunti di Algebra” lez. 36 (per questi risultati si usa il lemma di Zorn). □

4.5.9. DIPENDENZA LINEARE E DIPENDENZA ALGEBRICA. Di conseguenza esistono basi per ogni spazio vettoriale V , e la loro cardinalità è costante; ed esistono basi di trascendenza di H su K , vale a dire insiemi X di trascendenti indipendenti su K tali che H è algebrico su $K(X)$, e la loro cardinalità è costante.

5. Coordinate.

5.1. DEFINIZIONE (COORDINATE DEI VETTORI IN UNA FISSATA BASE). Sia V uno spazio vettoriale su C di dimensione n , e sia $\mathcal{V} = (v_1, \dots, v_n)$ una base ordinata di V . Allora per ogni $v \in V$ restano determinati unicamente gli scalari $\alpha_i \in C$ tali che $v = \sum_i \alpha_i v_i$; la n -upla $(\alpha_1, \dots, \alpha_n)$ si dice n -upla delle coordinate di v nella base \mathcal{V} . Di solito abuseremo della terminologia dicendo “base” invece di “base ordinata”, se sarà chiaro dal contesto.

5.1.1. ESEMPIO. Si osservi che le coordinate di un vettore dipendono dalla base scelta per lo spazio vettoriale. Esistono vettori che hanno sempre le stesse coordinate in qualunque base? Fissato un vettore v , esiste sempre una base dello spazio in cui quel vettore ha coordinate $(1, 0, \dots, 0)$?

5.1.2. PROBLEMA. Si osservi che vale una proprietà più forte di quella usata nella definizione: un insieme (v_1, \dots, v_n) è una base di V se e solo se ogni vettore $v \in V$ si può scrivere in un unico modo come combinazione lineare dei vettori di quell'insieme.

5.2. ESEMPI. Ritorniamo agli esempi fondamentali di spazi vettoriali.

5.2.1. SPAZI VETTORIALI STANDARD. Si dice base canonica di C^n l'insieme ordinato

$$\mathcal{E} = \{e_1, \dots, e_n\} \text{ ove } e_1 = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, e_2 = \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix}, \dots, e_n = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix}$$

ovvero e_i è la n -upla che ha 1 come i -sima componente e 0 altrove. In particolare lo spazio vettoriale standard C^n ha dimensione n . In questa base, le coordinate di un vettore v sono esattamente le sue componenti numeriche; infatti se $v = (v_1, \dots, v_n)$

$$v = v_1 e_1 + \dots + v_n e_n .$$

Detto $u = e_1 + \dots + e_n$ (vettore le cui coordinate in base canonica sono tutte 1), verificare che anche l'insieme

$$\mathcal{F} = \{u - e_1, \dots, u - e_n\}$$

è una base di C^n ; trovare le coordinate di u in questa base, e più generalmente trovare le coordinate nella base \mathcal{F} del vettore di coordinate (x_1, \dots, x_n) nella base \mathcal{E} .

5.2.2. POLINOMI. Il principio di uguaglianza tra polinomi (due polinomi sono uguali se e solo se i coefficienti di potenze omologhe della variabile sono uguali; ovvero un polinomio è nullo se e solo se tutti i suoi coefficienti sono nulli) dice che l'insieme

$$\mathcal{X} = \{1, X, X^2, X^3, \dots, X^n, \dots\}$$

è un insieme linearmente indipendente, ed in effetti è una base per lo spazio vettoriale $C[X]$ dei polinomi; dunque si tratta di uno spazio vettoriale di dimensione infinita (numerabile). In questa base, le coordinate di un polinomio sono esattamente i suoi coefficienti.

Si consideri l'insieme

$$\mathcal{Y} = \{1, 1+X, 1+X+X^2, 1+X+X^2+X^3, \dots, \sum_{i=0}^n X^i, \dots\}$$

e si dimostri che si tratta di una base per lo spazio dei polinomi; si esprimano in questa base le coordinate di un polinomio $P(X) = \sum_{i=0}^n \alpha_i X^i$ in funzione dei suoi coefficienti α_n .

5.2.3. POLINOMI TRONCATI. Una base per lo spazio $C[X]_{\leq n}$ dei polinomi troncati all'ordine n è l'insieme

$$\mathcal{X}_n = \{1, X, X^2, X^3, \dots, X^n\}$$

da cui si deduce che questo spazio ha dimensione $n + 1$.

Esistono basi di $C[X]_{\leq n}$ fatte di polinomi di grado (tutti) esattamente n ? Se sì, scriverne almeno due, ed esprimere in termini di quelle basi le coordinate di un generico polinomio troncato.

È vero che in ogni base deve esistere almeno un polinomio di grado n ? E di grado i per $i < n$?

5.2.4. SERIE FORMALI. Poiché le serie formali contengono un sottospazio di dimensione infinita (quello dei polinomi), si tratta di uno spazio di dimensioni infinita, e in realtà più che numerabile. Per studiare questo tipo di spazi vettoriali bisogna considerarne anche altre strutture (quelle topologiche in particolare).

5.2.5. FUNZIONI REALI. Lo spazio delle funzioni continue di \mathbb{R} in \mathbb{C} contiene il sottospazio delle funzioni polinomiali; quindi necessariamente è di dimensione infinita. In effetti la sua dimensione è più che numerabile, e scriverne una base è al di fuori delle nostre attuali possibilità.

5.2.6. FUNZIONI A VALORI IN UN CORPO. Lo spazio delle funzioni di un insieme X in C è di dimensione finita se e solo se X è un insieme finito, ed in tal caso è pari al numero di elementi di X (scrivere esplicitamente una base). Altrimenti, se X è infinito, questo spazio contiene un sottospazio (dato dalle funzioni che si annullano su “quasi ogni” elemento di X) che è di dimensione infinita, pari alla cardinalità di X .

5.2.7. SPAZI VETTORIALI REALI E COMPLESSI. Il corpo \mathbb{C} dei numeri complessi ha dimensione 2 come spazio vettoriale su \mathbb{R} ; infatti l'insieme $\{1, i\}$ è una base di \mathbb{C} su \mathbb{R} : ogni numero complesso z si scrive unicamente come somma $a + ib$ con $a, b \in \mathbb{R}$.

Anche l'insieme $\{1 + i, 1 - i\}$ è base di \mathbb{C} su \mathbb{R} ; dimostrarlo e calcolare le coordinate del numero complesso $z = a + ib$ in questa nuova base.

Consideriamo ora uno spazio vettoriale V su \mathbb{C} , di dimensione n e base $\mathcal{V} = \{v_1, \dots, v_n\}$. Allora V è uno spazio vettoriale su \mathbb{R} (restringendo il prodotto per gli scalari ai numeri reali), di base $\mathcal{V}' = \{v_1, iv_1, \dots, v_n, iv_n\}$, e dunque di dimensione $2n$ su \mathbb{R} (verificare). Dunque per ogni spazio vettoriale complesso V , si ha $\dim_{\mathbb{R}} V = 2 \dim_{\mathbb{C}} V$.

5.2.8. SPAZI PRODOTTO. Se V è spazio vettoriale su C di dimensione n con base $\mathcal{V} = \{v_1, \dots, v_n\}$, e W è spazio vettoriale su C di dimensione m con base $\mathcal{W} = \{w_1, \dots, w_m\}$, allora lo spazio prodotto $V \times W$ ha come base l'insieme delle coppie

$$\{(v_i, 0) : i = 1, \dots, n\} \cup \{(0, w_j) : j = 1, \dots, m\}$$

e dunque ha dimensione $n + m$ (verificare). In generale $\dim_C(V \times W) = \dim_C V + \dim_C W$, cioè lo spazio prodotto ha dimensione pari alla somma delle dimensioni degli spazi dati.

Generalizzare l'esempio al prodotto di un numero finito di spazi vettoriali sullo stesso corpo C .

5.2.9. SPAZI QUOZIENTE. Se V è spazio vettoriale su C di dimensione n e W è sottospazio vettoriale di V di dimensione m (necessariamente $m \leq n$), verificare che lo spazio quoziente V/W ha dimensione $n - m$ (si cominci scegliendo una base per W e completandola ad una base di V ; le classi degli elementi che si sono dovuti aggiungere costituiranno una base dello spazio quoziente). In generale $\dim_C(V/W) = \dim_C V - \dim_C W$, cioè lo spazio quoziente ha dimensione pari alla differenza delle dimensioni dello spazio ambiente e del suo sottospazio.

5.3. DESCRIZIONE DI SOTTOSPAZI. Vi sono essenzialmente tre modi per descrivere i sottospazi W di un fissato spazio vettoriale V ; l'unico visto finora essenzialmente è tramite generatori, possibilmente linearmente indipendenti:

5.3.1. DESCRIZIONE TRAMITE GENERATORI. Sia V uno spazio vettoriale di dimensione n , e W un suo sottospazio di dimensione m . Allora W ammette una base formata da esattamente m vettori, siano w_1, \dots, w_m , e si può descrivere come $W = \langle w_1, \dots, w_m \rangle$, ovvero come l'insieme di tutti i vettori w di V che si scrivono come combinazione

$$w = \alpha_1 w_1 + \alpha_2 w_2 + \dots + \alpha_m w_m$$

con i coefficienti $\alpha_1, \alpha_2, \dots, \alpha_m$ in C :

$$W = \left\{ \sum_{i=1}^m \alpha_i w_i \mid \alpha_i \in C, \forall i \right\} .$$

Nel caso di spazi vettoriali di dimensione finita, fissata una base di V e considerando le relative coordinate, abbiamo altri due possibili descrizioni del sottospazio W :

5.3.2. DESCRIZIONE TRAMITE EQUAZIONI PARAMETRICHE. Siano

$$\begin{pmatrix} w_{1,1} \\ w_{2,1} \\ \vdots \\ w_{n,1} \end{pmatrix}, \begin{pmatrix} w_{1,2} \\ w_{2,2} \\ \vdots \\ w_{n,2} \end{pmatrix}, \dots, \begin{pmatrix} w_{1,m} \\ w_{2,m} \\ \vdots \\ w_{n,m} \end{pmatrix}$$

le coordinate dei vettori w_1, \dots, w_m nella base scelta di V ; allora possiamo descrivere il sottospazio W come l'insieme dei vettori w di V le cui coordinate nella base scelta si scrivono

$$\begin{cases} x_1 = \alpha_1 w_{1,1} + \alpha_2 w_{1,2} + \dots + \alpha_m w_{1,m} \\ x_2 = \alpha_1 w_{2,1} + \alpha_2 w_{2,2} + \dots + \alpha_m w_{2,m} \\ \vdots \\ x_n = \alpha_1 w_{n,1} + \alpha_2 w_{n,2} + \dots + \alpha_m w_{n,m} \end{cases}$$

al variare dei coefficienti $\alpha_1, \alpha_2, \dots, \alpha_m \in C$. Queste espressioni si dicono equazioni parametriche per W , e gli α_i si dicono i parametri.

Dato un tale sistema di equazioni parametriche, è immediato ritrovare un sistema di generatori per W , che risulta una base se il numero di parametri era pari alla dimensione di W .

5.3.3. DESCRIZIONE TRAMITE EQUAZIONI CARTESIANE. Dalle equazioni parametriche si può procedere con il metodo di "eliminazione dei parametri": si ricava un parametro dalla prima equazione (eventualmente cambiando l'ordine delle equazioni) e lo sostituisce nelle altre; gettando via la prima equazione si ottiene un sistema con una equazione in meno e un parametro in meno. Ripetendo il processo per tutti i parametri si ottiene un sistema di $n - m$ equazioni (lineari omogenee) nelle coordinate x_1, x_2, \dots, x_n che descrive la sottovarietà W . Queste si dicono equazioni cartesiane per W .

Dato un tale sistema di equazioni cartesiane (lineari omogenee), si può risalire ad una descrizione parametrica, o tramite generatori, del sottospazio "risolvendo il sistema", ovvero esplicitando quali sono tutte e sole le n -uple di coordinate che soddisfano a quel sistema.

5.3.4. RELAZIONI TRA NUMERO DI GENERATORI INDIPENDENTI, DI PARAMETRI E DI EQUAZIONI CARTESIANE. Seguendo bene i passaggi appena fatti si vede che la dimensione di W corrisponde al numero minimo di generatori necessario per descrivere il sottospazio, e anche al minimo numero di parametri necessari per le equazioni parametriche. Lo stesso spazio W è invece descritto da equazioni cartesiane in numero minimo di $n - m$; questo numero viene spesso indicato come la codimensione di W in V (dipende da V , W e dal corpo C).

5.3.5. ESEMPI. Se V è spazio vettoriale di dimensione n , allora:

- (0) per descrivere il sottospazio nullo servono 0 generatori, 0 parametri, ovvero n equazioni (indipendenti);
- (1) per descrivere una retta serve un generatore (non nullo), un parametro, ovvero $n - 1$ equazioni (indipendenti);
- (2) per descrivere un piano servono due generatori (linearmente indipendenti), due parametri, ovvero $n - 2$ equazioni (indipendenti);
- (3) per descrivere uno spazio (tridimensionale) servono tre generatori (linearmente indipendenti), tre parametri, ovvero $n - 3$ equazioni (indipendenti).

Si dice iperpiano invece un sottospazio definito da una equazione cartesiana, per descrivere il quale servono dunque $n - 1$ generatori (indipendenti), ovvero un sistema parametrico con $n - 1$ parametri.

6. Relazione di Grassmann.

6.1. TEOREMA (FORMULA DI GRASSMANN). Siano U_1 ed U_2 sottospazi vettoriali di V ; vale la seguente relazione:

$$\dim_C U_1 + \dim_C U_2 = \dim_C (U_1 + U_2) + \dim_C (U_1 \cap U_2).$$

DIMOSTRAZIONE. Scegliamo una base $\mathcal{U} = \{w_1, \dots, w_r\}$ di $U_1 \cap U_2$, e completiamola ad una base $\mathcal{U}_1 = \{w_1, \dots, w_r, u_1, \dots, u_{s_1}\}$ di U_1 e ad una base $\mathcal{U}_2 = \{w_1, \dots, w_r, v_1, \dots, v_{s_2}\}$ di U_2 . Dunque con gli indici introdotti abbiamo che $\dim_C (U_1 \cap U_2) = r$, $\dim_C U_1 = r + s_1$ e $\dim_C U_2 = r + s_2$. Di

conseguenza basta dimostrare che $\dim_C(U_1 + U_2) = r + s_1 + s_2$, e per far questo basta trovare una base di $U_1 + U_2$ con esattamente $r + s_1 + s_2$ elementi.

Verifichiamo che l'insieme

$$\mathcal{U}_1 \cup \mathcal{U}_2 = \{w_1, \dots, w_r, u_1, \dots, u_{s_1}, v_1, \dots, v_{s_2}\}$$

(che ha esattamente quel numero di elementi) è una base di $U_1 + U_2$. Che sia un insieme di generatori è quasi ovvio, vista la relazione $U_1 + U_2 = \langle \mathcal{U}_1 \cup \mathcal{U}_2 \rangle$, poiché $U_1 = \langle \mathcal{U}_1 \rangle$ e $U_2 = \langle \mathcal{U}_2 \rangle$.

Resta da verificare che si tratta di un insieme linearmente indipendente. Supponiamo

$$\alpha_1 w_1 + \dots + \alpha_r w_r + \beta_1 u_1 + \dots + \beta_{s_1} u_{s_1} + \gamma_1 v_1 + \dots + \gamma_{s_2} v_{s_2} = 0$$

e vogliamo mostrare che tutti i coefficienti devono essere nulli. Scrivendo

$$\alpha_1 w_1 + \dots + \alpha_r w_r + \beta_1 u_1 + \dots + \beta_{s_1} u_{s_1} = -\gamma_1 v_1 - \dots - \gamma_{s_2} v_{s_2}$$

vediamo che si tratta di un vettore in $U_1 \cap U_2$ (guardando il lato sinistro dell'uguaglianza vi vede che appartiene a U_1 , e guardando il lato destro che appartiene a U_2). Allora deduciamo che esistono coefficienti $\delta_1, \dots, \delta_r$ tali che

$$\delta_1 w_1 + \dots + \delta_r w_r = -\gamma_1 v_1 - \dots - \gamma_{s_2} v_{s_2}$$

ovvero

$$\delta_1 w_1 + \dots + \delta_r w_r + \gamma_1 v_1 + \dots + \gamma_{s_2} v_{s_2} = 0$$

da cui abbiamo $\gamma_1 = \dots = \gamma_{s_2} = 0$ trattandosi di una combinazione di elementi della base \mathcal{U}_2 (anche $\delta_1 = \dots = \delta_r = 0$, ma non ci interessa). Tornando allora alla prima relazione abbiamo ora

$$\alpha_1 w_1 + \dots + \alpha_r w_r + \beta_1 u_1 + \dots + \beta_{s_1} u_{s_1} = 0$$

da cui infine $\alpha_1 = \dots = \alpha_r = \beta_1 = \dots = \beta_{s_1} = 0$ trattandosi di una combinazione di elementi della base \mathcal{U}_1 . \square

6.1.1. ESEMPIO (INTERSEZIONE DI SOTTOSPAZI). Una applicazione particolarmente interessante della formula di Grassmann è la seguente: se due sottospazi hanno dimensione “abbastanza grande”, essi devono avere una intersezione non banale (cioè diversa dal solo vettore nullo). Per esempio:

- (a) due sottospazi di dimensione 2 in uno spazio di dimensione 3 devono intersecarsi almeno in una retta;
- (b) due sottospazi di dimensione 3 in uno spazio di dimensione 4 devono intersecarsi almeno in un piano;
- (c) in generale, due sottospazi di dimensione m_1 ed m_2 in uno spazio di dimensione n devono intersecarsi in un sottospazio non banale se $m_1 + m_2 > n$, ed in tal caso la minima dimensione dello spazio intersezione è $m_1 + m_2 - n$.

6.1.2. PROBLEMA (SOMME DIRETTE). Siano U_1 ed U_2 sottospazi vettoriali di V , e sia $W = U_1 + U_2$; i seguenti fatti sono equivalenti:

- (1) $\dim_C(U_1 + U_2) = \dim_C U_1 + \dim_C U_2$
- (2) $U_1 \cap U_2 = 0$;
- (3) $W = U_1 \oplus U_2$;
- (4) ogni elemento $w \in W$ si scrive in modo unico come somma $u_1 + u_2$ con $u_1 \in U_1$ e $u_2 \in U_2$

6.1.3. PROBLEMA. Come si può generalizzare la formula di Grassmann avendo tre o più sottospazi? In particolare dare un controesempio alla seguente formula (falsa):

$$\begin{aligned} \dim_C(U_1 + U_2 + U_3) &= \dim_C U_1 + \dim_C U_2 + \dim_C U_3 + \\ &\quad - \dim_C(U_1 \cap U_2) - \dim_C(U_1 \cap U_3) - \dim_C(U_2 \cap U_3) + \\ &\quad + \dim_C(U_1 \cap U_2 \cap U_3) \end{aligned}$$

(osservare invece che la formula diventa vera sostituendo “sottospazi vettoriali di un fissato spazio, dimensione, somma di sottospazi, intersezione” con “sottinsiemi finiti di un fissato insieme, cardinalità, unione, intersezione” rispettivamente: si tratta allora di una delle formule di inclusione-esclusione).

7. Esercizi.

7.1. Nel piano \mathbb{R}^2 consideriamo i vettori $v = \begin{pmatrix} 1 \\ 2 \end{pmatrix}$ e $w = \begin{pmatrix} -1 \\ 1 \end{pmatrix}$.

- (a) mostrare che ogni vettore $x = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$ del piano si scrive in modo unico come combinazione lineare $x = \alpha v + \beta w$ (determinare α e β in funzione di x_1 ed x_2);
- (b) disegnare e caratterizzare (tramite equazioni o disequazioni) i sottoinsiemi di \mathbb{R}^2 formati dagli estremi finali dei vettori del tipo $\alpha v + \beta w$ ove α e β sono numeri reali soggetti alle seguenti condizioni:
- (C) $\alpha, \beta \in [0, \infty)$
 (R) $\alpha + \beta = 1$
 (S) $\alpha + \beta = 1$ con $\alpha, \beta \in [0, 1]$
 (P) $\alpha, \beta \in [0, 1]$
 (T) $\alpha + \beta \leq 1$ con $\alpha, \beta \in [0, 1]$
 (X) $\alpha + \beta \leq 1$.
- (c) specificare le relazioni di inclusione tra gli insiemi precedenti.

7.2. Nello spazio \mathbb{R}^3 consideriamo i vettori $v = \begin{pmatrix} 1 \\ 2 \\ 0 \end{pmatrix}$ e $w = \begin{pmatrix} -1 \\ -1 \\ 2 \end{pmatrix}$.

- (a) mostrare che un vettore $x = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}$ appartiene al piano generato da v e w se e solo se vale la relazione $4x_1 - 2x_2 + x_3 = 0$;
- (b) descrivere i sottoinsiemi analoghi a quelli dell'esercizio precedente.

7.3. Nello spazio \mathbb{R}^3 consideriamo i vettori $u = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}$, $v = \begin{pmatrix} 1 \\ 2 \\ 0 \end{pmatrix}$ e $w = \begin{pmatrix} -1 \\ 1 \\ 2 \end{pmatrix}$.

- (a) verificare che sono linearmente indipendenti e risolvere in α, β, γ la relazione $x = \alpha u + \beta v + \gamma w$ per un vettore $x = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}$ generico;
- (b) disegnare e caratterizzare (tramite equazioni o disequazioni) i sottoinsiemi di \mathbb{R}^3 formati dagli estremi finali dei vettori del tipo $\alpha u + \beta v + \gamma w$ ove α, β e γ sono numeri reali soggetti alle seguenti condizioni:
- (C) $\alpha, \beta, \gamma \in [0, \infty)$
 (Pi) $\alpha + \beta + \gamma = 1$
 (Tr) $\alpha + \beta + \gamma = 1$ con $\alpha, \beta, \gamma \in [0, 1]$
 (Pa) $\alpha, \beta, \gamma \in [0, 1]$
 (Te) $\alpha + \beta + \gamma \leq 1$ con $\alpha, \beta, \gamma \in [0, 1]$
 (X) $\alpha + \beta + \gamma \leq 1$.
- (c) specificare le relazioni di inclusione tra gli insiemi precedenti.

7.4. Verificare che l'insieme dei vettori $u = \begin{pmatrix} 1 \\ 2 \end{pmatrix}$, $v = \begin{pmatrix} 1 \\ -1 \end{pmatrix}$, $w = \begin{pmatrix} 0 \\ -1 \end{pmatrix}$ e $z = \begin{pmatrix} -2 \\ 2 \end{pmatrix}$ di \mathbb{R}^2 è generatore, ed estrarne tutte le basi possibili di \mathbb{R}^2 .

7.5. Verificare che l'insieme dei vettori $u = \begin{pmatrix} 1 \\ 2 \\ 0 \end{pmatrix}$, $v = \begin{pmatrix} 1 \\ 0 \\ -1 \end{pmatrix}$, $w = \begin{pmatrix} 0 \\ -1 \\ 1 \end{pmatrix}$, e $z = \begin{pmatrix} -1 \\ 2 \\ -2 \end{pmatrix}$ di \mathbb{R}^3 è generatore, ed estrarne tutte le basi possibili di \mathbb{R}^3 .

7.6. Descrivere tramite equazioni il sottospazio di \mathbb{R}^4 generato dai vettori $u = \begin{pmatrix} 1 \\ 0 \\ 2 \\ 0 \end{pmatrix}$, $v = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}$, $w = \begin{pmatrix} 0 \\ -1 \\ 1 \\ 1 \end{pmatrix}$ (sono linearmente indipendenti?), e poi completare quest'insieme ad una base di \mathbb{R}^4 .

7.7. Verificare che i sottoinsiemi di \mathbb{R}^4 formati dai vettori $x = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix}$ soddisfacenti alle condizioni $x_1 - x_4 = 0 = x_1 + x_2$ (sia U) e $x_3 - x_4 = 0 = x_2 + x_3$ (sia V) sono sottospazi vettoriali, trovarne la dimensione evidenziando delle basi; calcolare poi l'intersezione trovandone una base. Trovare le equazioni del più piccolo sottospazio vettoriale di \mathbb{R}^4 contenente sia U che V .

7.8. Siano v e w due vettori non nulli di uno spazio vettoriale V . Sotto quali condizioni i vettori v e $\alpha v + \beta w$ sono linearmente indipendenti?

7.9. Consideriamo lo spazio vettoriale reale delle applicazioni continue di \mathbb{R} in sè.

- (a) vero che l'insieme formato dalle tre funzioni 1 (funzione costante), \sin^2 e \cos^2 è linearmente dipendente?

- (b) si consideri l'insieme $\{\sin(nx) : n \in \mathbb{N}, n \neq 0\} \cup \{\cos(nx) : n \in \mathbb{N}\}$ e si dimostri che è un insieme linearmente indipendente;
- (c) cosa dire dell'insieme $\{\sin(\alpha + nx) : n \in \mathbb{N}, n \neq 0, \alpha \in \mathbb{R}\}$?

7.10. Sia $V = K[X]_{\leq 4}$ lo spazio vettoriale su K dei polinomi di grado minore o uguale a 4.

- (a) qual è la dimensione di V su K ?
- (b) esistono basi di V i cui elementi siano polinomi di grado 4?
- (c) esistono basi di V i cui elementi siano polinomi di grado minore o uguale a 3?
- (d) esistono basi di V i cui elementi siano polinomi privi di termine noto?

7.11. Si determini se i sottospazi di \mathbb{R}^3 formati dai vettori $x = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}$ soddisfacenti alle condizioni seguenti siano o meno sottospazi di \mathbb{R}^3 :

- (a) $x_1^2 + x_2^2 = x_3$
- (b) $|x_1| = |x_2|$
- (c) $x_1 + x_2 = x_3$
- (d) $x_1x_2 + x_2x_3 = 0$
- (e) $x_1 + x_2 - x_3 + 1 = 0$
- (f) $x_1 - x_2^2 = 0$ e $x_1 = 0$
- (g) $x_1 - x_2x_3 = 0$ e $x_1 = 0$

In ciascuno dei casi, cercare di disegnare l'insieme in questione.

7.12. Calcolare somma, intersezione (evidenziando basi e dimensioni) per i seguenti sottospazi di \mathbb{R}^4 :

- (a) $V = \left\langle \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} \right\rangle$ e $W = \left\langle \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \right\rangle$.
- (b) $V = \left\langle \begin{pmatrix} 1 \\ 1 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix} \right\rangle$ e $W = \left\langle \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} \right\rangle$.

7.13. Sia $V = K[X]_{\leq 4}$ lo spazio vettoriale su K dei polinomi di grado minore o uguale a 4. Consideriamo i seguenti sottospazi:

$$V_s = \{f \in V : f(X) = f(-X)\} \quad \text{e} \quad V_a = \{f \in V : f(X) = -f(-X)\}.$$

- (a) mostrare che V_s e V_a sono sottospazi, trovarne delle basi e le dimensioni;
- (b) è vero che $V = V_s \oplus V_a$?
- (c) generalizzare sostituendo 4 con n generico.

7.14. Come l'esercizio precedente usando i sottospazi $U = \{f \in V : f(X) = f(1 - X)\}$ e $W = \{f \in V : f(X) = -f(1 - X)\}$.

7.15. Qual è la minima dimensione di uno spazio vettoriale V tale che due suoi sottospazi di dimensione m_1 ed m_2 si intersecano solo nel vettore nullo? Dare degli esempi per $m_1, m_2 = 1, 2, 3, 4$.

7.16. Qual è la massima dimensione di uno spazio vettoriale V tale che due suoi sottospazi di dimensione m_1 ed m_2 hanno intersezione sempre non banale? Dare degli esempi per $m_1, m_2 = 1, 2, 3, 4$.

7.17. Due sottospazi vettoriali U e W di V sono complementari, cioè $V = U \oplus W$; sia v un vettore non appartenente a $U \cup W$ (cioè non appartenente né a U né a W). Calcolare la dimensione dei sottospazi $U + \langle v \rangle$, $W + \langle v \rangle$ e della loro intersezione.

7.18. Sia $Q(X) = c(X - \alpha_1)^{m_1} \cdots (X - \alpha_r)^{m_r}$ un polinomio di grado $n = \sum_{i=1}^r m_i$ in $V = K[X]$ e consideriamo l'insieme

$$V_Q = \left\{ \frac{P(X)}{Q(X)} : P(X) \in V \text{ con } \deg P(X) < n \right\}$$

- (a) mostrare che V_Q è spazio vettoriale su K di dimensione n ;
- (b) mostrare che l'insieme $\left\{ \frac{1}{(X - \alpha_i)^{j_i}} : j_i = 1, \dots, m_i \text{ e } i = 1, \dots, r \right\}$ è una base di V_Q su K .

7.19. Siano u, v, w e z quattro vettori in \mathbb{R}^n tali che i loro estremi siano i quattro punti consecutivi di un parallelogramma.

- (a) interpretare la condizione data in termini dei vettori;
- (b) mostrare che $(v - u) - (w - u) + (z - u) = 0$;
- (c) verificare che $u + \frac{1}{2}(w - u) = v + \frac{1}{2}(z - v)$ e dare l'interpretazione geometrica dell'uguaglianza.

7.20. Si consideri l'insieme $\mathbb{R}_{>0}$ dei numeri reali strettamente positivi, dotato delle seguenti operazioni: la "somma" di due numeri sia il loro prodotto, il prodotto scalare del reale $\alpha \in \mathbb{R}$ per l'elemento $r \in \mathbb{R}_{>0}$ sia r^α . Dimostrare che $\mathbb{R}_{>0}$ con queste operazioni è uno spazio vettoriale reale il cui vettore nullo è 1. Qual'è la sua dimensione?

Capitolo II

Applicazioni Lineari e Matrici

Uno dei punti fondamentali della Matematica è il fatto di considerare ogni qual volta si definisca un qualche tipo di oggetto anche le funzioni che in qualche senso rispettano la struttura di quel tipo di oggetti. Se tra due insiemi consideriamo funzioni di qualsiasi tipo, tra insiemi dotati di qualche struttura algebrica considereremo solo funzioni che rispettano in qualche senso più o meno forte quelle strutture. Così, tra gruppi consideriamo solo omomorfismi di gruppo, tra anelli solo omomorfismi di anello, tra corpi solo omomorfismi di corpi, tra spazi vettoriali (su uno stesso corpo) solo applicazioni lineari - almeno per il momento.

Il punto fondamentale è che il dato di una applicazione lineare tra spazi vettoriali di dimensione finita è completamente determinato da un insieme finito di dati (le immagini dei vettori di una base), che si possono organizzare in una “matrice” che descrive completamente l’applicazione. Il calcolo matriciale che ne risulta viene definito in modo che le operazioni tra matrici corrispondano alle operazioni tra le applicazioni lineari corrispondenti.

L’esigenza di scegliere basi degli spazi vettoriali per poter usare il calcolo matriciale comporta di dover capire come questo calcolo cambia variando la scelta delle basi; le matrici di cambiamento di base rispondono a questi problemi. Si tenga presente che la scelta di una base in uno spazio vettoriale è spesso del tutto arbitraria, mentre i problemi di tipo geometrico e le loro soluzioni devono essere intrinseci e non devono dipendere da scelte arbitrarie; d’altra parte è chiaro che ogni problema potrà avere una espressione matriciale più semplice in una base opportunamente scelta. È quindi fondamentale sapere come cambia l’espressione matriciale di un dato o di un problema variando la scelta delle basi coinvolte.

1. Applicazioni lineari.

1.1. DEFINIZIONE (APPLICAZIONI LINEARI). Siano V e W spazi vettoriali su un corpo C . Una applicazione $\varphi : V \rightarrow W$ si dice lineare se soddisfa alle seguenti condizioni:

$$(L1) \quad \varphi(u + v) = \varphi(u) + \varphi(v) \quad (\forall u, v \in V);$$

$$(L2) \quad \varphi(\alpha v) = \alpha \varphi(v) \quad (\forall v \in V, \forall \alpha \in C).$$

Queste due condizioni sono equivalenti all’unica condizione

$$(L) \quad \varphi(\alpha u + \beta v) = \alpha \varphi(u) + \beta \varphi(v) \quad (\forall u, v \in V, \forall \alpha, \beta \in C),$$

o anche alla condizione

$$(L') \quad \varphi(\alpha u + v) = \alpha \varphi(u) + \varphi(v) \quad (\forall u, v \in V, \forall \alpha \in C).$$

1.1.1. Dalla definizione segue subito che si ha $\varphi(0) = 0$ e $\varphi(-v) = -\varphi(v)$.

1.1.2. Sempre dalla definizione troviamo che $\varphi(\sum_i \alpha_i v_i) = \sum_i \alpha_i \varphi(v_i)$, cioè

$$\varphi(\alpha_1 v_1 + \alpha_2 v_2 + \dots + \alpha_m v_m) = \alpha_1 \varphi(v_1) + \alpha_2 \varphi(v_2) + \dots + \alpha_m \varphi(v_m),$$

per ogni insieme finito di vettori v_i e ogni corrispondente insieme di scalari α_i . Da questo si deduce subito che una applicazione lineare è determinata dai valori assunti su una base del dominio: infatti noti i valori di φ su una base di V , si può trovare il valore dell’applicazione su ogni vettore di V . Viceversa, una volta assegnati i valori su una base di V , esiste una (unica) applicazione lineare soddisfacente a quelle condizioni (che si ottiene con la formula sopra scritta), che si dice ottenuta “estendendo per linearità” le condizioni date.

1.1.3. COMPOSIZIONE DI MORFISMI LINEARI. Date due applicazioni lineari $\varphi : V \rightarrow W$ e $\psi : W \rightarrow U$, segue dalla definizione che la composizione $\psi \circ \varphi : V \rightarrow U$ è ancora una applicazione lineare.

1.2. DEFINIZIONE-PROPOSIZIONE (NUCLEO E IMMAGINE). Sia $\varphi : V \rightarrow W$ una applicazione lineare. Il nucleo (kernel) di φ è l'antimmagine del vettore nullo

$$\ker \varphi := \{v \in V \mid \varphi(v)=0\}$$

e l'immagine di φ è l'immagine in senso insiemistico

$$\operatorname{im} \varphi := \{w \in W \mid \text{esiste } v \in V \text{ tale che } w=\varphi(v)\}$$

Nucleo e immagine di φ sono sottospazi vettoriali di V e W rispettivamente.

DIMOSTRAZIONE. Verifica immediata. \square

1.3. TEOREMA (FORMULA DELLE DIMENSIONI PER APPLICAZIONI LINEARI). Sia $\varphi : V \rightarrow W$ una applicazione lineare, e supponiamo V di dimensione finita. Allora vale la relazione

$$\dim_C V = \dim_C \ker \varphi + \dim_C \operatorname{im} \varphi .$$

DIMOSTRAZIONE. Osserviamo prima di tutto che le tre dimensioni coinvolte nella formula sono finite (quella di V per ipotesi, quella di $\ker \varphi$ perché si tratta di un sottospazio di V , quella di $\operatorname{im} \varphi$ perché si tratta di un sottospazio vettoriale di W che è generato dall'immagine dei vettori di una qualsiasi base di V). Ora scegliamo una base di $\ker \varphi$, sia v_1, \dots, v_r , e completiamola ad una base di V , sia $v_1, \dots, v_r, v_{r+1}, \dots, v_n$. Per dimostrare la formula del teorema basta mostrare che $\varphi(v_{r+1}), \dots, \varphi(v_n)$ costituiscono una base di $\operatorname{im} \varphi$. Mostriamo che sono un sistema di generatori: se $w = \varphi v \in \operatorname{im} \varphi$, allora $v = \sum_{i=1}^n \alpha_i v_i$ e abbiamo

$$w = \varphi v = \varphi \left(\sum_{i=1}^n \alpha_i v_i \right) = \sum_{i=r+1}^n \alpha_i \varphi(v_i) ,$$

da cui la conclusione voluta. Mostriamo che formano un sistema linearmente indipendente: se $\sum_{i=r+1}^n \alpha_i \varphi v_i = 0$ allora abbiamo $\sum_{i=r+1}^n \alpha_i v_i \in \ker \varphi$, e usando che $\ker \varphi$ è generato da v_1, \dots, v_r abbiamo $\sum_{i=r+1}^n \alpha_i v_i = \sum_{i=1}^r \alpha_i v_i$, da cui deduciamo $\alpha_i = 0$ per ogni $i = r+1, \dots, n$. \square

1.4. TEOREMA (INIETTIVITÀ E SURIETTIVITÀ). I seguenti fatti sono equivalenti alla iniettività di φ :

- (1) $\ker \varphi = 0$ (ovvero $\dim \ker \varphi = 0$);
- (2) se $S \subseteq V$ è linearmente indipendente allora $\varphi S \subseteq W$ è linearmente indipendente (equivalentemente: se $\varphi S \subseteq W$ è linearmente dipendente allora $S \subseteq V$ è linearmente dipendente);
- (3) φ manda basi di V in insiemi linearmente indipendenti di W ;
- (4) φ manda basi di V in basi di $\operatorname{im} \varphi$;
- (5) φ ammette una inversa a sinistra (esiste $\psi : W \rightarrow V$ tale che $\psi \circ \varphi = \operatorname{id}_V$).

Da ciò si deduce che, se φ è iniettiva, allora $\dim_C V \leq \dim_C W$.

I seguenti fatti sono equivalenti alla suriettività di φ :

- (1) $\operatorname{im} \varphi = W$ (ovvero $\dim \operatorname{im} \varphi = \dim W$ se V o W hanno dimensione finita);
- (2) φ manda basi di V in insiemi generatori di W ;
- (3) l'immagine di una base di V contiene una base di W ;
- (4) φ ammette una inversa a destra (esiste $\psi : W \rightarrow V$ tale che $\varphi \circ \psi = \operatorname{id}_W$).

Da ciò si deduce che, se φ è suriettiva, allora $\dim_C V \geq \dim_C W$.

DIMOSTRAZIONE. Esercizio. \square

1.5. TEOREMA (ISOMORFISMI). Una applicazione lineare $\varphi : V \rightarrow W$ si dice un isomorfismo se esiste una applicazione lineare inversa $\psi : W \rightarrow V$ (cioè tale che $\psi \circ \varphi = \operatorname{id}_V$ e $\varphi \circ \psi = \operatorname{id}_W$). I seguenti fatti sono equivalenti a che φ sia isomorfismo:

- (1) φ è biiettiva (come mappa di insiemi; cioè diciamo che l'inversa insiemistica è necessariamente una applicazione lineare);
- (2) φ è iniettiva e suriettiva;
- (3) $\ker \varphi = 0$ e $\operatorname{im} \varphi = W$;
- (4) φ manda basi di V in basi di W .

In particolare, se φ è isomorfismo, allora $\dim_C V = \dim_C W$.

DIMOSTRAZIONE. È conseguenza del precedente. \square

1.6. COROLLARIO (ENDOMORFISMI). Se $\dim_C V = \dim_C W$ è finita (per esempio se $V = W$ è spazio vettoriale di dimensione finita) allora i seguenti fatti sono equivalenti:

- (1) φ è un isomorfismo;
- (2) φ è iniettiva;
- (2') $\ker \varphi = 0$;
- (3) φ è suriettiva;
- (3') $\operatorname{im} \varphi = W$.

DIMOSTRAZIONE. Basta usare la formula delle dimensioni per una applicazione lineare: $\ker \varphi = 0$ (iniettività) se e solo se $\dim_C \ker \varphi = 0$, se e solo se $\dim_C \operatorname{im} \varphi = \dim_C W$ se e solo se $\operatorname{im} \varphi = W$ (suriettività). \square

1.6.1. OSSERVAZIONI SULLA FINITEZZA. Si osservi che per il risultato precedente è essenziale l'ipotesi di finitezza delle dimensioni; trovare degli esempi di applicazioni lineari iniettive ma non suriettive, e suriettive ma non iniettive tra gli endomorfismi di uno spazio vettoriale di dimensione infinita (lo spazio dei polinomi per esempio).

La situazione va paragonata con quella che si ha considerando mappe di insiemi di un insieme finito (con un numero finito di elementi) in sé; anche in quel caso abbiamo che biiettività, iniettività, suriettività sono nozioni equivalenti. Fatto evidentemente falso per applicazioni di un insieme infinito in sé (farsi degli esempi). Nel caso di spazi vettoriali finitamente generati, abbiamo che le mappe lineari sono determinate in effetti dai loro valori su un insieme finito, anche se gli spazi stessi possono avere infiniti elementi.

1.7. Ricordiamo che lo spazio vettoriale standard $V_n(C)$ su C di dimensione n è l'insieme C^n dotato delle operazioni "componente per componente" e che la sua base canonica è data dai vettori e_i . Sia V uno spazio vettoriale su C di dimensione finita $\dim_C V = n$ e scegliamo una base $\mathcal{V} = (v_1, \dots, v_n)$ di V . Questo determina un isomorfismo $V_n(C) \rightarrow V$ mandando la base canonica di $V_n(C)$ ordinatamente nella base scelta. Dunque la scelta di una base determina un isomorfismo di un qualsiasi spazio vettoriale di dimensione finita n con lo spazio vettoriale standard $V_n(C)$ di quella dimensione. Osserviamo però che questo isomorfismo dipende dalla scelta della base di V , cioè non è intrinseco.

1.8. ESEMPI. Diamo alcuni esempi particolarmente importanti di applicazioni lineari.

1.8.1. INCLUSIONI DI SOTTOSPAZI. Se W è un sottospazio di V , allora l'inclusione insiemistica $\iota_W : W \rightarrow V$ è una applicazione lineare, con nucleo nullo e immagine esattamente W .

1.8.2. PROIEZIONI SU QUOZIENTI. Se W è un sottospazio di V , allora il morfismo canonico $\pi_W : V \rightarrow V/W$ che ad ogni vettore associa la sua classe modulo W è una applicazione lineare, con nucleo W e immagine tutto V/W .

1.8.3. PROIEZIONI. Siano U_1 e U_2 sottospazi vettoriali complementari di uno spazio vettoriale V (dunque $V = U_1 \oplus U_2$, ovvero $V = U_1 + U_2$ e $U_1 \cap U_2 = 0$). Allora l'applicazione $\pi_{U_1}^{U_2} : V \rightarrow V$ che ad ogni vettore $v = u_1 + u_2$ di V (con $u_1 \in U_1$ e $u_2 \in U_2$) associa il vettore u_1 si dice proiezione su U_1 nella direzione di U_2 . Si tratta di una applicazione lineare di immagine U_1 e di nucleo U_2 (dunque è un isomorfismo se e solo se $U_2 = 0$ e $U_1 = V$, nel qual caso si tratta dell'identità). Si osservi che la composizione della proiezione con sé stessa dà ancora la proiezione stessa.

1.8.4. PROBLEMA. Siano V uno spazio vettoriale di dimensione n sul corpo C ed p un endomorfismo di V tale che $p^2 = p$.

- (a) Si mostri che $V = \operatorname{im} p \oplus \ker p$.
- (b) Si mostri che esistono una base (v_1, \dots, v_n) di V ed un intero i , $1 \leq i \leq n+1$, tali che $p(v_j) = v_j$, se $j < i$, e $p(v_j) = 0$, se $j \geq i$.
- (c) Dedurre che si tratta della proiezione di asse $\operatorname{im} p$ e direzione $\ker p$.

Quindi una applicazione lineare di uno spazio vettoriale di dimensione finita in sé è una proiezione se e solo se coincide con il proprio quadrato.

1.8.5. SIMMETRIE. Nella stessa situazione, l'applicazione $\sigma_{U_1}^{U_2} : V \rightarrow V$ che ad ogni vettore $v = u_1 + u_2$ di V (con $u_1 \in U_1$ e $u_2 \in U_2$) associa il vettore $u_1 - u_2$ si dice simmetria di asse U_1 e di direzione U_2 . Si tratta di una applicazione lineare di immagine V e di nucleo 0 , dunque è sempre un isomorfismo; l'applicazione inversa è la stessa simmetria.

1.8.6. PROBLEMA. Siano V uno spazio vettoriale di dimensione n sul corpo C (di caratteristica diversa da due) e s un endomorfismo di V tale che $s^2 = \text{id}_V$.

- Si mostri che $\ker s = 0$, dunque s è un isomorfismo.
- Si mostri che esistono due sottospazi complementari V_+ e V_- di V tali che s agisce come l'identità su V_+ e la moltiplicazione per -1 su V_- .
- Si mostri che esistono una base (v_1, \dots, v_n) di V ed un intero i , $1 \leq i \leq n+1$, tali che $s(v_j) = v_j$, se $j < i$, e $s(v_j) = -v_j$, se $j \geq i$.
- Dedurre che si tratta della simmetria di asse V_+ e direzione V_- .

Quindi una applicazione lineare di uno spazio vettoriale di dimensione finita in sè è una simmetria se e solo se è di quadrato identico.

1.9. TEOREMA (PRIMO TEOREMA DI ISOMORFISMO). Sia $\varphi : V \rightarrow W$ una applicazione lineare. Allora φ induce un isomorfismo $\bar{\varphi} : V/\ker \varphi \rightarrow \text{im } \varphi$ che rende commutativo il seguente diagramma di applicazioni lineari:

$$\begin{array}{ccc} V & \xrightarrow{\varphi} & W \\ \pi \downarrow & & \uparrow \iota \\ V/\ker \varphi & \xrightarrow{\bar{\varphi}} & \text{im } \varphi \end{array}$$

ove π e ι sono le applicazioni canoniche (commutativo significa che $\varphi = \iota \circ \bar{\varphi} \circ \pi$).

DIMOSTRAZIONE. Più in generale, se V' è un sottospazio di V , è facile osservare che φ si fattorizza tramite il quoziente V/V' (significa che esiste una applicazione lineare $V/V' \rightarrow W$ tale che la composizione con la proiezione canonica $V \rightarrow V/V'$ sia φ) se e solo se $\varphi(V') = 0$, cioè $V' \subseteq \ker \varphi$. Da questo segue subito il teorema. \square

1.9.1. Si osservi che la formula delle dimensioni per il morfismo φ dice appunto che $\dim_C(V/\ker \varphi) = \dim \text{im } \varphi$.

♠ 1.10. TEOREMA (SECONDO TEOREMA DI ISOMORFISMO). Il morfismo di inclusione $\iota_1 : W_1 \rightarrow W_1 + W_2$ induce un isomorfismo $\bar{\iota}_1 : W_1/(W_1 \cap W_2) \rightarrow (W_1 + W_2)/W_2$ che rende commutativo il seguente diagramma di applicazioni lineari:

$$\begin{array}{ccc} W_1 & \xrightarrow{\iota_1} & W_1 + W_2 \\ \pi_1 \downarrow & & \downarrow \pi_2 \\ W_1/(W_1 \cap W_2) & \xrightarrow{\bar{\iota}_1} & (W_1 + W_2)/W_2 \end{array}$$

ove π_1 e π_2 sono le applicazioni canoniche (commutativo significa che $\pi_2 \circ \iota_1 = \bar{\iota}_1 \circ \pi_1$).

DIMOSTRAZIONE. Basta osservare che $\pi_2 \circ \iota_1 : W_1 \rightarrow (W_1 + W_2)/W_2$ è suriettivo e $\ker(\pi_2 \circ \iota_1) = W_1 \cap W_2$; si applica allora il primo teorema di isomorfismo. \square

1.10.1. Di solito si esprime questo risultato in modo più pittoresco dicendo che i quozienti dei lati opposti del seguente diagramma di inclusioni

$$\begin{array}{ccc} & W_1 + W_2 & \\ \sim / & & \backslash \approx \\ W_1 & & W_2 \\ \approx \backslash & & / \sim \\ & W_1 \cap W_2 & \end{array}$$

sono isomorfi tra loro.

♠ 1.11. TEOREMA (TERZO TEOREMA DI ISOMORFISMO). Se abbiamo $W_1 \supseteq W_2$ sottospazi di V , il morfismo canonico $\pi : V/W_2 \rightarrow V/W_1$ induce un isomorfismo $\bar{\pi} : (V/W_2)/(W_1/W_2) \rightarrow V/W_1$ che rende commutativo il seguente diagramma di applicazioni lineari:

$$\begin{array}{ccc} V & \xrightarrow{\pi_1} & V/W_1 \\ \pi_2 \downarrow & & \uparrow \bar{\pi} \\ V/W_2 & \xrightarrow{\bar{\pi}_1} & (V/W_2)/(W_1/W_2) \end{array}$$

ove π_1 e π_2 sono le applicazioni canoniche (commutativo significa che $\bar{\pi} \circ \bar{\pi}_1 \circ \pi_2 = \pi_1$; si noti anche che $\pi = \bar{\pi} \circ \bar{\pi}_1$ e $\pi \circ \pi_2 = \pi_1$).

DIMOSTRAZIONE. Il morfismo π esiste perché $W_2 \subseteq W_1 = \ker(V \rightarrow V/W_1)$; è facile vedere che π è suriettivo, e che $\ker \pi \cong W_1/W_2$ (canonicamente isomorfo); quindi per l'esistenza e le proprietà di $\bar{\pi}$ basta usare il primo teorema di isomorfismo. La commutatività affermata si può verificare direttamente. \square

1.11.1. Si osservi l'analogia con il calcolo delle frazioni: $(a/c)/(b/c) = a/b$.

1.12. DEFINIZIONE-PROPOSIZIONE (SPAZI DI MORFISMI). L'insieme di tutte le applicazioni C -lineari di V in W si indica con $\text{Hom}_C(V, W)$. Esso ha struttura di spazio vettoriale su C , come sottospazio di tutte le applicazioni (insiemistiche) di V in W . L'applicazione di composizione, come già detto, rispetta la linearità e dunque dà una mappa

$$\text{Hom}_C(V, W) \times \text{Hom}_C(W, U) \longrightarrow \text{Hom}_C(V, U)$$

che manda la coppia (φ, ψ) in $\psi \circ \varphi$. L'applicazione di composizione non è lineare, bensì bilineare, ovvero lineare in ogni variabile: valgono le formule

$$\psi \circ (\alpha_1 \varphi_1 + \alpha_2 \varphi_2) = \alpha_1 \psi \circ \varphi_1 + \alpha_2 \psi \circ \varphi_2 \quad \text{e} \quad (\beta_1 \psi_1 + \beta_2 \psi_2) \circ \varphi = \beta_1 \psi_1 \circ \varphi + \beta_2 \psi_2 \circ \varphi$$

per ogni $\varphi, \varphi_1, \varphi_2 \in \text{Hom}_C(V, W)$, $\psi, \psi_1, \psi_2 \in \text{Hom}_C(W, U)$, $\alpha_1, \alpha_2, \beta_1, \beta_2 \in C$.

DIMOSTRAZIONE. Esercizio. \square

1.13. DEFINIZIONE (ALGEBRA DEGLI ENDOMORFISMI). In particolare, definiamo $\text{End}_C(V) = \text{Hom}_C(V, V)$ che è un insieme dotato della struttura di algebra associativa (non commutativa) su C con unità, ovvero di:

(V) una struttura di spazio vettoriale su C ;

(A) una operazione di prodotto (composizione) $\text{End}_C(V) \times \text{End}_C(V) \rightarrow \text{End}_C(V)$ verificante le proprietà seguenti:

(A1) esiste un elemento neutro per il prodotto (l'applicazione identica id_V tale che $\varphi \circ \text{id}_V = \varphi = \text{id}_V \circ \varphi$ per ogni $\varphi \in \text{End}_C(V)$),

(A2) il prodotto è associativo ($(\varphi \circ \psi) \circ \vartheta = \varphi \circ (\psi \circ \vartheta)$ per ogni $\varphi, \psi, \vartheta \in \text{End}_C(V)$),

(A3) il prodotto rispetta la struttura di spazio vettoriale, nel senso che risulta bilineare, come già specificato.

Anche da questa definizione possiamo trarre molti risultati algebrici puramente formali, quali per esempio:

1.13.1. PRODOTTO CON LO ZERO. Risulta $0 \circ \varphi = 0 = \psi \circ 0$ per ogni φ e ψ .

1.13.2. ANNULLAMENTO. Se $\psi \circ \varphi = 0$ e uno tra φ e ψ è invertibile (ha inverso per la composizione) allora l'altro è zero.

1.13.3. SVILUPPO DEL BINOMIO. Per definizione si pone $\varphi^n = \varphi \circ \dots \circ \varphi$ (n volte) e $\varphi^0 = \text{id}_V$. Allora vale la formula del binomio per elementi che commutano: se $\psi \circ \varphi = \varphi \circ \psi$ allora $(\varphi + \psi)^n = \sum_{i=0}^n \binom{n}{i} \varphi^i \psi^{n-i}$.

1.13.4. In particolare vale $(\text{id}_V + \varphi)^n = \sum_{i=0}^n \binom{n}{i} \varphi^i$.

♠ **1.14. SOMME E PRODOTTI (ARBITRARI).** Data una famiglia \mathcal{I} di indici, e un insieme di spazi vettoriali V_i al variare di $i \in \mathcal{I}$, definiamo la somma diretta $\bigoplus_{i \in \mathcal{I}} V_i$ e il prodotto diretto $\prod_{i \in \mathcal{I}} V_i$ come gli insiemi formati dalle \mathcal{I} -uple $(v_i)_{i \in \mathcal{I}}$ di elementi con $v_i \in V_i$ per ogni i , e quasi tutti nulli (i.e. nulli tranne che per un numero finito di indici) nel caso della somma diretta. Si hanno strutture canoniche di spazio vettoriale su C con le operazioni "componente per componente".

In particolare la somma diretta è un sottospazio vettoriale del prodotto diretto, e se l'insieme di indici è finito, allora le due nozioni coincidono. Discutere i casi in cui le dimensioni di questi spazi risultano finite.

Abbiamo dei morfismi canonici di inclusione $\iota_j : V_j \rightarrow \bigoplus_{i \in \mathcal{I}} V_i$ (manda v_j nella \mathcal{I} -upla che ha tutte le componenti nulle tranne la j -esima che vale v_j) e di proiezione $\pi_j : \prod_{i \in \mathcal{I}} V_i \rightarrow V_j$ (manda una \mathcal{I} -upla nella sua j -sima componente) per ogni j . Si verifica subito che $\pi_j \circ \iota_j = \text{id}_{V_j}$ (da cui si vede che ι_j è iniettiva e π_j è suriettiva), $\pi_j \circ \iota_{j'} = 0$ se $j \neq j'$.

Per ogni spazio vettoriale W su C , vi sono i seguenti isomorfismi di spazi vettoriali su C :

$$\text{Hom}_C\left(\bigoplus_{i \in \mathcal{I}} V_i, W\right) \cong \prod_{i \in \mathcal{I}} \text{Hom}_C(V_i, W) \quad \text{e} \quad \text{Hom}_C\left(W, \prod_{i \in \mathcal{I}} V_i\right) \cong \prod_{i \in \mathcal{I}} \text{Hom}_C(W, V_i)$$

dati dalle composizioni con le inclusioni e le proiezioni, rispettivamente.

♠ **1.15. NUCLEO E QUOZIENTE.** Per ogni applicazione lineare $\varphi : V \rightarrow W$ abbiamo i seguenti isomorfismi di spazi vettoriali:

$$\text{Hom}_C(U, \ker \varphi) \cong \{f \in \text{Hom}_C(U, V) : \varphi \circ f = 0\}$$

per ogni spazio vettoriale U su C ; in altri termini, le applicazioni lineari da U verso $\ker \varphi$ sono in corrispondenza biunivoca con le applicazioni lineari di U verso V la cui immagine è contenuta in $\ker \varphi$.

Analogamente se W è un sottospazio vettoriale di V , allora abbiamo un isomorfismo di spazi vettoriali

$$\text{Hom}_C(V/W, U) \cong \{f \in \text{Hom}_C(V, U) : f(W) = 0\}$$

per ogni spazio vettoriale U su C ; in altri termini, le applicazioni lineari da V/W verso U sono in corrispondenza biunivoca con le applicazioni lineari di V verso U il cui nucleo contiene W .

2. Matrici.

2.1. DEFINIZIONE (SPAZIO VETTORIALE DELLE MATRICI). Per ogni naturale n , sia \mathbf{n} l'insieme $\{1, 2, \dots, n\}$. Lo spazio vettoriale $M_{n \times m}(C)$ (o $M_{n,m}(C)$) delle matrici $n \times m$ (n righe ed m colonne) a coefficienti in un corpo C è lo spazio vettoriale delle funzioni da $\mathbf{n} \times \mathbf{m}$ in C . Una matrice $n \times m$ a valori in un corpo C si rappresenta con una scrittura:

$$A = (a_{i,j})_{\substack{i=1,\dots,n \\ j=1,\dots,m}} = \begin{pmatrix} a_{1,1} & \cdots & a_{1,m} \\ \vdots & \ddots & \vdots \\ a_{n,1} & \cdots & a_{n,m} \end{pmatrix};$$

e le operazioni di spazio vettoriale si scrivono nel modo seguente:

(P) prodotto per elementi $\alpha \in C$: se $A = (a_{i,j})$, allora $\alpha A = (\alpha a_{i,j})$.

(S) somma: se $A = (a_{i,j}), B = (b_{i,j}) \in M_{n,m}(C)$, allora $A + B = (a_{i,j} + b_{i,j}) \in M_{n,m}(C)$.

Useremo anche la seguente scrittura "per colonne" e "per righe":

$$A = (A_{(1)} \cdots A_{(m)}) = \begin{pmatrix} A^{(1)} \\ \vdots \\ A^{(n)} \end{pmatrix}$$

ove $A_{(i)}$ sono matrici $n \times 1$ e si dicono le colonne di A , e $A^{(j)}$ sono matrici $1 \times m$ e si dicono le righe di A

2.2. Si osservi che lo spazio vettoriale $M_{n,m}(C)$ delle matrici $n \times m$ ha dimensione nm . La base canonica è data dalle matrici $e_{i,j}$ le cui entrate sono tutte nulle tranne quella in posizione (i,j) che vale 1.

2.3. DEFINIZIONE-TEOREMA (PRODOTTO RIGHE PER COLONNE DI MATRICI). Definiamo un prodotto di matrici nel modo seguente: se $A \in M_{n,m}(C)$ e $B \in M_{m,l}(C)$ (dunque il numero di colonne di A eguaglia il numero di righe di B) allora

$$AB = \left(\sum_{j=1}^m a_{i,j} b_{j,k} \right)_{\substack{i=1,\dots,n \\ k=1,\dots,l}} = \left(A^{(i)} B_{(k)} \right)_{\substack{i=1,\dots,n \\ k=1,\dots,l}} \in M_{n,l}(C).$$

Abbiamo così definito una applicazione bilineare

$$M_{n,m}(C) \times M_{m,l}(C) \longrightarrow M_{n,l}(C)$$

per la quale vale una proprietà di associatività $(A_1 A_2) A_3 = A_1 (A_2 A_3)$ per ogni matrice $A_1 \in M_{n,m}(C)$, $A_2 \in M_{m,l}(C)$, $A_3 \in M_{l,h}(C)$ (si osservi in particolare che tutti i prodotti scritti hanno senso).

Inoltre per ogni n la matrice quadrata “identità” $\mathbb{I}_n \in M_{n,n}(C)$ definita da $(\delta_{i,j})$ (ove i simboli di Kronecker $\delta_{i,j}$ sono uguali a 1 se $i = j$ e a 0 altrimenti) ha la proprietà $\mathbb{I}_n A = A$ per ogni $A \in M_{n,m}(C)$ e $B \mathbb{I}_n = B$ per ogni $B \in M_{m,n}(C)$.

DIMOSTRAZIONE. La bilinearità del prodotto di matrici $((\alpha_1 A_1 + \alpha_2 A_2)B = \alpha_1 A_1 B + \alpha_2 A_2 B$ e $A(\beta_1 B_1 + \beta_2 B_2) = \beta_1 A B_1 + \beta_2 A B_2$) si verifica subito in base alla definizione.

Per dimostrare l’associatività del prodotto è sufficiente mostrare che per ogni i e k si ha l’uguaglianza $(A_1^{(i)} A_2) A_{3(k)} = A_1^{(i)} (A_2 A_{3(k)})$, cioè basta mostrarlo per il prodotto del tipo “riga per matrice per colonna”, e in quel caso si tratta di un facile conto.

La verifica per le proprietà delle matrici identiche è immediata. \square

2.3.1. INVERTIBILITÀ DESTRA E SINISTRA. Una matrice $A \in M_{n,m}$ si dice invertibile a destra se esiste una matrice $B \in M_{m,n}$ tale che $AB = \mathbb{I}_n$; si dice invertibile a sinistra se esiste una matrice $B \in M_{m,n}$ tale che $BA = \mathbb{I}_m$.

2.3.2. NON COMMUTATIVITÀ. Si osservi che il prodotto di matrici non è commutativo: in primo luogo, se un prodotto è definito, non è nemmeno detto che il prodotto con l’ordine scambiato sia definito. Inoltre, se anche i due prodotti fossero entrambi definiti, i risultati potrebbero essere matrici di taglie diverse. Infine, anche se consideriamo matrici quadrate ($n = m$), in cui i prodotti sono definiti e si tratta di matrici nello stesso spazio vettoriale, i due prodotti in generale sono diversi. Farsi degli esempi.

2.4. DEFINIZIONE-PROPOSIZIONE (TRASPOSIZIONE). Sia $A \in M_{n,m}(C)$; definiamo $A^t \in M_{m,n}(C)$ tramite: $A^t := (a_{i,j})_{\substack{j=1,\dots,m \\ i=1,\dots,n}}$. Abbiamo allora per ogni n ad m una applicazione

$${}^t : M_{n,m}(C) \longrightarrow M_{m,n}(C)$$

con le seguenti proprietà:

- (1) $(A^t)^t = A$ (involutoria; di conseguenza è una biiezione inversa della omonima in senso inverso),
- (2) $(A + B)^t = A^t + B^t$ e $(\alpha A)^t = \alpha A^t$ (linearità),
- (3) inoltre, se A e B sono matrici moltiplicabili (cioè il numero di colonne di A coincide con il numero di righe di B), allora anche B^t e A^t lo sono e vale $(AB)^t = B^t A^t$ (rispetta il prodotto scambiando l’ordine dei fattori). Di solito si dice che il trasposto del prodotto è il prodotto delle trasposte nell’ordine inverso.

DIMOSTRAZIONE. Esercizio. \square

2.5. DEFINIZIONE (ALGEBRA DELLE MATRICI QUADRATE D’ORDINE n). In particolare le matrici quadrate d’ordine n , ovvero le matrici $n \times n$, a coefficienti in C , formano una algebra associativa (non commutativa in generale) con elemento neutro per il prodotto (la matrice identica \mathbb{I}_n che ha componenti i simboli di Kronecker $\delta_{i,j}$ uguali a 1 se $i = j$ e a 0 altrimenti). Quest’algebra si indica con $M_n(C)$.

2.5.1. MATRICI SCALARI. Consideriamo l’applicazione

$$scal : C \longrightarrow M_n(C)$$

che manda ogni $\alpha \in C$ nella matrice $scal(\alpha) = \alpha \mathbb{I}_n$ che ha componenti uguali ad α nelle posizioni con $i = j$ (diagonale principale) e zero altrove. Si tratta di una applicazione lineare e iniettiva che rispetta identità e prodotti. Le matrici dell’immagine di $scal$ si dicono matrici scalari, formano una sotto- C -algebra (e in effetti un sottocorpo) dell’algebra della matrici, e ne costituiscono il centro: le matrici scalari sono tutte e sole le matrici S che commutano con tutte le altre matrici, cioè tali che $AS = SA$ per ogni $A \in M_n(C)$.

2.5.2. MATRICI DIAGONALI. Consideriamo l’applicazione

$$diag : C^n \longrightarrow M_n(C)$$

che manda ogni $(a_1, \dots, a_n) \in C^n$ nella matrice $diag(a_1, \dots, a_n)$ che ha componente uguale ad a_i nelle posizioni (i, i) (diagonale principale) e zero altrove. Si tratta di una applicazione lineare e iniettiva. Le matrici dell’immagine di $diag$ si dicono matrici diagonali, e formano una sotto- C -algebra dell’algebra della matrici. Le matrici scalari sono particolari matrici diagonali (quali?).

2.5.3. MATRICI INVERTIBILI. Una matrice $A \in M_n(C)$ si dice invertibile se esiste una matrice B tale che $AB = \mathbb{I}_n = BA$, cioè se è invertibile a destra e a sinistra (in tal caso necessariamente le inverse destra e sinistra coincidono). La matrice B è allora unica e si indica con A^{-1}

2.5.4. Una matrice A si dice unipotente se esiste un naturale m tale che $A^m = \mathbb{I}_n$. Ogni matrice unipotente è invertibile.

2.5.5. Una matrice A si dice nilpotente se esiste un naturale m tale che $A^m = 0_n$. Se A è nilpotente, allora $\mathbb{I}_n + A$ è invertibile.

2.5.6. Una matrice A si dice divisore a sinistra di zero se esiste una matrice $B \neq 0_n$ tale che $AB = 0_n$ e divisore a destra di zero se esiste una matrice $B \neq 0_n$ tale che $BA = 0_n$. Una matrice è divisore a sinistra di zero se e solo se è divisore a destra di zero (e quindi si parlerà di divisori di zero senza specificare, ma notare che in generale i divisori di zero a destra e a sinistra per una fissata matrice sono diversi). Una matrice non nulla o è invertibile o è divisore di zero (e le due possibilità si escludono).

2.5.7. Una matrice A si dice simmetrica o antisimmetrica a seconda che $A^t = A$ oppure $A^t = -A$.

2.6. DEFINIZIONE (RANGO DI MATRICI). Il rango $\text{rk}(A)$ di una matrice $A \in M_{n,m}(C)$ è per definizione il massimo numero di colonne linearmente indipendenti.

2.6.1. Si potrebbe definire anche il “rango per righe” di una matrice, come il massimo numero di righe linearmente indipendenti. In realtà coincide con il rango (per colonne), come vedremo sia come conseguenza della dualità di spazi vettoriali, sia come conseguenza del metodo di riduzione di Gauss per matrici.

2.6.2. Una matrice ha rango nullo se e solo se è la matrice nulla.

2.6.3. Una matrice $A \in M_{n,m}(C)$ ha rango 1 se e solo se può essere scritta come prodotto $A = VW$ con $V \in M_{n,1}(C)$ e $W \in M_{1,m}(C)$ (non nulle).

2.7. DEFINIZIONE-TEOREMA (GRUPPO GENERALE LINEARE). Il sottinsieme di $M_n(C)$ delle matrici invertibili si indica con $\text{GL}(n, C)$, e si tratta di un gruppo (non commutativo) sotto il prodotto di matrici. In particolare abbiamo

- (1) $\text{diag}(a_1, \dots, a_n)^{-1} = \text{diag}(a_1^{-1}, \dots, a_n^{-1})$ se $a_i \neq 0$ per ogni i ; $\text{scal}(\alpha)^{-1} = \text{scal}(\alpha^{-1})$ se $\alpha \neq 0$; $\mathbb{I}_n^{-1} = \mathbb{I}_n$;
- (2) $(A^{-1})^{-1} = A$;
- (3) $(AB)^{-1} = B^{-1}A^{-1}$, cioè se le matrici A e B sono invertibili, nel qual caso anche AB è invertibile, l'inversa del prodotto è il prodotto delle inverse nell'ordine inverso;
- (4) se A è invertibile, anche A^t lo è, e $(A^t)^{-1} = (A^{-1})^t$; di solito si dice che la trasposta dell'inversa è l'inversa della trasposta (o che gli operatori di inversione e trasposizione commutano tra loro).

DIMOSTRAZIONE. Esercizio. □

3. Matrici associate ad applicazioni lineari.

3.1. DEFINIZIONE-TEOREMA (MATRICI ASSOCIATE AD APPLICAZIONI LINEARI). Siano V e W spazi vettoriali su C di dimensione finita $n := \dim_C V$ ed $m := \dim_C W$, e siano $\mathcal{V} = (v_1, \dots, v_n)$ e $\mathcal{W} = (w_1, \dots, w_m)$ basi ordinate di V e W rispettivamente. Allora ad ogni applicazione lineare $\varphi : V \rightarrow W$ possiamo associare una matrice $\alpha_{\mathcal{V}, \mathcal{W}}(\varphi) \in M_{m,n}(C)$ tramite la definizione seguente:

$$(\varphi v_1, \dots, \varphi v_n) = (w_1, \dots, w_m) \alpha_{\mathcal{V}, \mathcal{W}}(\varphi)$$

(o in modo compatto $\varphi \mathcal{V} = \mathcal{W} \alpha_{\mathcal{V}, \mathcal{W}}(\varphi)$ ove compare il prodotto tra una riga di vettori e una matrice di scalari, il cui risultato è una riga di vettori) cioè le colonne di $\alpha_{\mathcal{V}, \mathcal{W}}(\varphi)$ sono le coordinate nella base scelta di W delle immagini tramite φ dei vettori della base scelta di V . In questo modo abbiamo definito una applicazione

$$\alpha_{\mathcal{V}, \mathcal{W}} : \text{Hom}_C(V, W) \longrightarrow M_{m,n}(C)$$

che è un isomorfismo di spazi vettoriali (dipendente dalla scelta delle basi \mathcal{V} e \mathcal{W}).

Per ogni spazio vettoriale V di dimensione n , l'applicazione identica $\text{id}_V \in \text{Hom}_C(V, V)$ viene mandata da $\alpha_{\mathcal{V}, \mathcal{V}}$ nella matrice identica $\mathbb{I}_n \in M_n(C)$ (indipendentemente dalla base \mathcal{V} scelta).

DIMOSTRAZIONE. L'unica cosa da verificare è che $\alpha_{\mathcal{V}, \mathcal{W}}$ sia applicazione lineare, e che $\ker \alpha_{\mathcal{V}, \mathcal{W}} = 0$ (entrambe le cose sono facili). \square

3.1.1. Le notazioni precedenti, piuttosto compatte, sono estremamente utili, ma conviene esplicitarle completamente ogni qual volta diano luogo a problemi di comprensione; per esempio, esplicitiamo la definizione: se abbiamo $\varphi v_i = a_{1,i}w_1 + a_{2,i}w_2 + \dots + a_{m,i}w_m$ per ogni $i = 1, 2, \dots, n$, allora la matrice $\alpha_{\mathcal{V}, \mathcal{W}}(\varphi)$ ha come i -esima colonna i termini $a_{1,i}, a_{2,i}, \dots, a_{m,i}$. In effetti risulta:

$$(\varphi v_1, \dots, \varphi v_i, \dots, \varphi v_n) = (w_1, w_2, \dots, w_m) \begin{pmatrix} a_{1,1} & \cdots & a_{1,i} & \cdots & a_{1,n} \\ a_{2,1} & \cdots & a_{2,i} & \cdots & a_{2,n} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ a_{m,1} & \cdots & a_{m,i} & \cdots & a_{m,n} \end{pmatrix}$$

(prodotto righe per colonne).

3.1.2. Dal risultato precedente discende subito che lo spazio vettoriale $\text{Hom}_C(V, W)$ ha dimensione data dal prodotto delle dimensioni dei due spazi coinvolti: $\dim_V \text{Hom}_C(V, W) = \dim_C V \dim_C W$. In effetti si sta dicendo che una applicazione lineare tra V e W è unicamente e completamente determinata da nm scalari (una volta scelte delle basi nei due spazi).

3.1.3. MATRICI DI CAMBIAMENTI DI BASE. In particolare possiamo considerare uno spazio vettoriale V , due sue basi \mathcal{V} e \mathcal{V}' e l'applicazione identica di V in sè. Allora la matrice $\alpha_{\mathcal{V}, \mathcal{V}'}(\text{id}_V)$ si dice matrice di cambiamento di base da \mathcal{V} a \mathcal{V}' ; le sue colonne sono le coordinate nella base \mathcal{V}' dei vettori della base \mathcal{V} .

3.2. AZIONE SULLE COORDINATE. Se v ha coordinate $(x_1, \dots, x_n)^t$ nella base \mathcal{V} , allora le coordinate di $\varphi(v)$ nella base di W sono date da

$$\varphi \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \alpha_{\mathcal{V}, \mathcal{W}}(\varphi) \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}.$$

infatti abbiamo

$$\varphi(v) = \varphi((v_1, \dots, v_n) \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}) = \varphi(v_1, \dots, v_n) \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = (w_1, \dots, w_m) \alpha_{\mathcal{V}, \mathcal{W}}(\varphi) \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$$

da cui la conclusione.

3.3. TEOREMA (COMPOSIZIONE E PRODOTTI). Se $\psi : W \longrightarrow U$ è un'altra applicazione lineare, e $\mathcal{U} = (u_1, \dots, u_l)$ una base di U , allora vale l'identità

$$\alpha_{\mathcal{V}, \mathcal{U}}(\psi \circ \varphi) = \alpha_{\mathcal{W}, \mathcal{U}}(\psi) \alpha_{\mathcal{V}, \mathcal{W}}(\varphi)$$

(la composizione di applicazioni lineari corrisponde alla moltiplicazione di matrici).

DIMOSTRAZIONE. Segue dai seguenti calcoli:

$$\begin{aligned} \psi \circ \varphi \mathcal{V} &= \psi(\varphi \mathcal{V}) = \psi(\mathcal{W} \alpha_{\mathcal{V}, \mathcal{W}}(\varphi)) \\ &= \psi(\mathcal{W}) \alpha_{\mathcal{V}, \mathcal{W}}(\varphi) \\ &= \mathcal{U} \alpha_{\mathcal{W}, \mathcal{U}}(\psi) \alpha_{\mathcal{V}, \mathcal{W}}(\varphi). \end{aligned}$$

Nel secondo passaggio si è usata la linearità di ψ (gli elementi della matrice $\alpha_{\mathcal{V}, \mathcal{W}}(\varphi)$ sono scalari). Se il senso delle uguaglianze precedenti non fosse chiaro, si calcoli per ogni $v_i \in \mathcal{V}$ la sua immagine tramite $\psi \circ \varphi$ in termini della base \mathcal{U} :

$$\psi(\varphi(v_i)) = \psi\left(\sum_{j=1}^m a_{j,i} w_j\right) = \sum_{j=1}^m a_{j,i} \psi(w_j) = \sum_{j=1}^m a_{j,i} \left(\sum_{k=1}^l b_{k,j} u_k\right) = \sum_{k=1}^l \left(\sum_{j=1}^m b_{k,j} a_{j,i}\right) u_k$$

(ove abbiamo scelto $\alpha_{\mathcal{V}, \mathcal{W}}(\varphi) = (a_{j,i})$ e $\alpha_{\mathcal{W}, \mathcal{U}}(\psi) = (b_{k,j})$) e si riconosca il termine di posto k, i della matrice $\alpha_{\mathcal{V}, \mathcal{U}}(\psi \circ \varphi)$ come prodotto della riga k -esima di $\alpha_{\mathcal{W}, \mathcal{U}}(\psi)$ per la i -esima colonna di $\alpha_{\mathcal{V}, \mathcal{W}}(\varphi)$. \square

3.3.1. EFFETTO DEI CAMBIAMENTI DI BASE. Se \mathcal{V}' è un'altra base di V e \mathcal{W}' un'altra base di W , allora la matrice $\alpha_{\mathcal{V}', \mathcal{W}'}(\varphi)$ è legata alla precedente tramite le matrici di cambiamento di base $\alpha_{\mathcal{V}', \mathcal{V}}(\text{id}_V)$ e $\alpha_{\mathcal{W}, \mathcal{W}'}(\text{id}_W)$ dalla formula

$$\alpha_{\mathcal{V}', \mathcal{W}'}(\varphi) = \alpha_{\mathcal{W}, \mathcal{W}'}(\text{id}_W) \alpha_{\mathcal{V}, \mathcal{W}}(\varphi) \alpha_{\mathcal{V}', \mathcal{V}}(\text{id}_V)$$

Si osservi che le matrici di cambiamento di base sono invertibili e si ha $\alpha_{\mathcal{V}', \mathcal{V}}(\text{id}_V) = \alpha_{\mathcal{V}, \mathcal{V}'}(\text{id}_V)^{-1}$.

Nel caso che $V = W$ intendiamo sempre scegliere la stessa base su dominio e codominio, sicché la formula di cambiamento di base diventa

$$\alpha_{\mathcal{V}', \mathcal{V}'}(\varphi) = \alpha_{\mathcal{V}, \mathcal{V}'}(\text{id}_V) \alpha_{\mathcal{V}, \mathcal{V}}(\varphi) \alpha_{\mathcal{V}', \mathcal{V}}(\text{id}_V).$$

3.3.2. L'applicazione φ è iniettiva (rispettivamente suriettiva) se e solo se per qualunque scelta delle basi si ha che la matrice $\alpha_{\mathcal{V}, \mathcal{W}}(\varphi)$ è invertibile a sinistra (rispettivamente a destra).

3.3.3. In particolare nel caso $\dim_C V = \dim_C W$ allora φ è un isomorfismo se e solo se per qualunque scelta delle basi si ha che la matrice $\alpha_{\mathcal{V}, \mathcal{W}}(\varphi)$ è invertibile. Dal teorema 1.6 deduciamo allora che una matrice quadrata è invertibile se e solo se è invertibile a destra, ovvero se e solo se è invertibile a sinistra. Scrivere per bene la dimostrazione; riflettere sulla possibilità di dimostrazioni dirette dello stesso fatto.

3.4. DEFINIZIONE (RANGO DI APPLICAZIONI E MATRICI). Il rango $\text{rk}(\varphi)$ di una applicazione lineare φ è la dimensione della sua immagine $\text{im } \varphi$ come spazio vettoriale. Dunque il rango di una applicazione corrisponde al rango di una qualunque matrice che la rappresenti (indifferentemente alle basi scelte).

3.4.1. Si osservi che una matrice è invertibile a sinistra se e solo se il suo rango coincide con il numero di colonne, cioè se e solo se le sue colonne formano un sistema linearmente indipendente.

3.4.2. Una matrice $A \in M_n(C)$ ha rango strettamente minore di n se e solo se è divisore di zero nell'algebra $M_n(C)$.

3.5. ALGEBRE DI ENDOMORFISMI E ALGEBRE DI MATRICI QUADRATE. Nel caso di endomorfismi di uno spazio vettoriale V di dimensione n e per ogni scelta di una base \mathcal{V} abbiamo dunque un isomorfismo di C -algebre

$$\alpha_{\mathcal{V}, \mathcal{V}} : \text{End}(V) \longrightarrow M_n(C)$$

(significa un isomorfismo lineare che rispetta identità e moltiplicazione, ovvero $\alpha_{\mathcal{V}, \mathcal{V}}(\text{id}_V) = \mathbb{I}_n$ e $\alpha_{\mathcal{V}, \mathcal{V}}(\varphi \circ \psi) = \alpha_{\mathcal{V}, \mathcal{V}}(\varphi) \alpha_{\mathcal{V}, \mathcal{V}}(\psi)$).

Se inoltre \mathcal{V}' è un'altra base di V , allora i due isomorfismi $\alpha_{\mathcal{V}, \mathcal{V}}$ e $\alpha_{\mathcal{V}', \mathcal{V}'}$ differiscono per l'automorfismo interno di $M_n(C)$ legato alla matrice di cambiamento di base $H = \alpha_{\mathcal{V}, \mathcal{V}'}(\text{id}_V)$, cioè al morfismo che manda una matrice X nella matrice $H^{-1}XH$. In altri termini abbiamo un diagramma commutativo di isomorfismi di C -algebre

$$\begin{array}{ccc} \text{End}(V) & \xrightarrow{\alpha_{\mathcal{V}, \mathcal{V}}} & M_n(C) \\ \parallel & & \downarrow \iota_H \\ \text{End}(V) & \xrightarrow{\alpha_{\mathcal{V}', \mathcal{V}'}} & M_n(C) \end{array}$$

dove $\iota_H(X) = H^{-1}XH$.

L'isomorfismo $\alpha_{\mathcal{V}, \mathcal{V}}$ si restringe ad un isomorfismo di gruppi (non abeliani)

$$\alpha_{\mathcal{V}, \mathcal{V}} : \text{Aut}(V) \longrightarrow \text{GL}_n(C)$$

tra il gruppo degli automorfismi di V (mappe lineari invertibili) con l'operazione di composizione, e il gruppo generale lineare delle matrici invertibili con l'operazione di prodotto.

4. Dualità.

4.1. DEFINIZIONE (SPAZIO DUALE). Sia V uno spazio vettoriale su C di dimensione finita n . Definiamo il suo duale come $V^* := \text{Hom}_C(V, C)$ (applicazioni lineari di V in C), che ha una

struttura naturale di C -spazio vettoriale data da $(v^*+w^*)(v) := v^*(v)+w^*(v)$ e $(\alpha v^*)(v) := \alpha v^*(v)$ per $v^*, w^* \in V^*$ e $\alpha \in C$. Gli elementi di V^* si chiamano spesso forme lineari o covettori.

4.2. DEFINIZIONE-PROPOSIZIONE (BASI DUALI). Data una base $\mathcal{V} = (v_1, \dots, v_n)$ di V , gli elementi v_i^* di V^* definiti da $v_i^*(v_j) := \delta_{i,j}$ formano una base di V^* ; $\mathcal{V}^* = (v_1^*, \dots, v_n^*)$ si dice la base duale di \mathcal{V} . In particolare $\dim_C V^* = \dim_C V$ (dunque V e V^* sono isomorfi, ma non in modo canonico).

DIMOSTRAZIONE. Dimostriamo che \mathcal{V}^* è un insieme linearmente indipendente: se $\sum \alpha_i v_i^* = 0$, allora, calcolando in v_j troviamo $\alpha_j = (\sum \alpha_i v_i^*)v_j = 0$ per ogni $j = 1, \dots, n$. Dimostriamo che \mathcal{V}^* è un insieme generatore: se $\varphi \in V^*$, consideriamo $f_i = \varphi(v_i) \in C$; allora $\varphi = \sum_i f_i v_i^*$. Per verificare l'uguaglianza basta verificarla per gli elementi della base \mathcal{V} , ed è evidente. \square

4.3. DEFINIZIONE-PROPOSIZIONE (DUALE DI APPLICAZIONI LINEARI). Se $\varphi : V \rightarrow W$ è una applicazione lineare, allora definiamo $\varphi^* : W^* \rightarrow V^*$ tramite la regola $\varphi^*(w^*)(v) := w^*(\varphi(v))$ (i.e. $v \circ (\varphi^* w^*) = (\varphi v) \circ w^* (\forall v \in V, \forall w^* \in W^*)$). Abbiamo che $\text{id}_V^* = \text{id}_{V^*}$, $(\psi \circ \varphi)^* = \varphi^* \circ \psi^*$.

DIMOSTRAZIONE. Esercizio. \square

4.3.1. PROPOSIZIONE (MATRICE DELL'APPLICAZIONE DUALE). La matrice di φ^* nelle basi duali delle basi \mathcal{V} di V e \mathcal{W} di W è data dalla trasposta della matrice di φ in quelle basi: $\alpha_{\mathcal{W}^*, \mathcal{V}^*}(\varphi^*) = \alpha_{\mathcal{V}, \mathcal{W}}(\varphi)^t$.

DIMOSTRAZIONE. Si verifica con il calcolo diretto (indichiamo con $a_{i,j}$ le entrate di $\alpha_{\mathcal{V}, \mathcal{W}}(\varphi)$ e con $a_{i,j}^*$ le entrate di $\alpha_{\mathcal{W}^*, \mathcal{V}^*}(\varphi^*)$): da $\varphi^*(w_i^*) = \sum_k a_{k,i}^* v_k^*$, calcolando in v_j otteniamo per il primo termine $\varphi^*(w_i^*)v_j = w_i^*(\varphi v_j) = w_i^*(\sum_k a_{k,j} v_k) = a_{i,j}$, mentre il secondo termine dà $(\sum_k a_{k,i}^* v_k^*)(v_j) = a_{j,i}^*$; si conclude che $a_{j,i}^* = a_{i,j}$. \square

4.4. DEFINIZIONE-TEOREMA (DI (BI)DUALITÀ). Il morfismo canonico: $V \rightarrow V^{**} : v \mapsto \text{ev}(v)$ ove $\text{ev}(v)(v^*) := v^*(v) = v \circ v^*$ è un isomorfismo di spazi vettoriali (Notare che non c'è un isomorfismo canonico tra V e V^*). Sotto questa identificazione, per un morfismo $\varphi : V \rightarrow W$, risulta $\varphi^{**} = \varphi$, ovvero abbiamo un diagramma commutativo di isomorfismi

$$\begin{array}{ccc} V & \xrightarrow{\text{ev}_V} & V^{**} \\ \varphi \downarrow & & \downarrow \varphi^{**} \\ W & \xrightarrow{\text{ev}_W} & W^{**} \end{array}$$

DIMOSTRAZIONE. Trattandosi di spazi di dimensione finita, basta verificare che $\ker(\text{ev}) = 0$, e di tratta della proprietà di non degenerazione (N2) qui sotto. \square

Insistiamo sul fatto che non esista un isomorfismo canonico tra V e il suo duale V^* ; tuttavia esistono relazioni molto strette tra il reticolo dei sottospazi di V e quello dei sottospazi di V^* , che cerchiamo ora di esplicitare.

4.5. PROPOSIZIONE (DUALITÀ). Esiste una applicazione canonica:

$$V \times V^* \rightarrow C : (v, v^*) \mapsto v \circ v^* := v^*(v)$$

che gode delle seguenti proprietà:

(B) bilineare, cioè soddisfa alle condizioni:

- (B1) $v \circ (v^*+w^*) = v \circ v^* + v \circ w^*$,
- (B2) $(v+w) \circ v^* = v \circ v^* + w \circ v^*$,
- (B3) $(\lambda v) \circ v^* = \lambda(v \circ v^*) = v \circ (\lambda v^*)$;

(N) non degenerare, cioè soddisfa alle condizioni:

- (N1) se $v \circ v^* = 0$ per ogni $v \in V$ allora $v^* = 0$,
- (N2) se $v \circ v^* = 0$ per ogni $v^* \in V^*$ allora $v = 0$.

DIMOSTRAZIONE. Facile esercizio, ma si faccia bene attenzione alla proprietà (N2), che è, almeno apparentemente, molto diversa dalla (N1) (quest'ultima dice semplicemente che una applicazione è nulla se dà risultato zero su ogni vettore; invece l'altra dice che un vettore che viene annullato da ogni forma lineare dev'essere nullo...). \square

4.6. DEFINIZIONE-PROPOSIZIONE (ORTOGONALITÀ). *Nozione di ortogonale: per ogni sottinsieme S di V (risp. V^*) definiamo un sottospazio di V^* (risp. V), detto ortogonale di S ,*

$$S^\perp := \{v^* \in V^* : s \circ v^* = 0 (\forall s \in S)\} \quad (\text{risp.} \quad \{v \in V : v \circ s = 0 (\forall s \in S)\}).$$

Proprietà dell'ortogonale:

(O1) se $S \subseteq T$ allora $T^\perp \subseteq S^\perp$;

(O2) $S^{\perp\perp} = \langle S \rangle$; $W^{\perp\perp} = W$ se W è un sottospazio; $S^{\perp\perp\perp} = S^\perp$;

(O3) $(W+W')^\perp = W^\perp \cap W'^\perp$ per ogni W e W' sottospazi di V ;

(O4) $(W \cap W')^\perp = W^\perp + W'^\perp$ per ogni W e W' sottospazi di V ;

in particolare il passaggio all'ortogonale induce un antiisomorfismo involutorio tra i reticoli di sottospazi di V e V^ ; inoltre $\dim_C(W^\perp) = n - \dim_C W$.*

DIMOSTRAZIONE. Esercizio; si tenga presente che basta considerare sottinsiemi S di V (usando il teorema di (bi)dualità) e si osservi che (O4) segue da (O3) (molto più facile da verificare), passando agli ortogonali. \square

4.7. DEFINIZIONE-PROPOSIZIONE (NUCLEO E IMMAGINE DI APPLICAZIONI DUALI). *Data una applicazione lineare $\varphi : V \rightarrow W$, allora $\text{im}(\varphi^*) = \ker(\varphi)^\perp$ e $\ker(\varphi^*) = \text{im}(\varphi)^\perp$. In particolare $\text{rk}(\varphi^*) = \text{rk}\varphi$.*

DIMOSTRAZIONE. Le due asserzioni seguono una dall'altra, e la seconda è facile da verificare: $v^* \in \ker(\varphi^*)$ sse $\varphi^*(v^*) = 0$ sse $\varphi^*(v^*)(v) = 0$ per ogni $v \in V$, e questo significa $v^*(\varphi(v)) = 0$ per ogni $v \in V$, cioè $v^*(v') = 0$ per ogni $v' \in \text{im}(\varphi)$, e quindi se e solo se $v^* \in \text{im}(\varphi)^\perp$. \square

4.7.1. Dall'ultima affermazione segue che per ogni matrice, il rango (per colonne) ed il rango per righe coincidono (il primo è il rango della applicazione lineare associata a quella matrice, il secondo coincide con il rango della applicazione duale).

4.7.2. TEOREMA (DUALI DI SOTTOSPAZI E QUOZIENTI). *Dato un sottospazio W di V , l'inclusione canonica $W \rightarrow V$ induce una mappa suriettiva $V^* \rightarrow W^*$ di nucleo W^\perp , da cui deduciamo che $W^* \cong V^*/W^\perp$. Inoltre risulta $(V/W)^* \cong W^\perp$.*

DIMOSTRAZIONE. Il primo risultato è chiaro dal primo teorema di isomorfismo. Per il secondo basta applicare il primo sostituendo V con V^* e W con W^\perp , e poi passare al duale: da $(W^\perp)^* \cong (V^*)^*/(W^\perp)^\perp \cong V/W$ si ottiene $W^\perp \cong (W^\perp)^{**} \cong (V/W)^*$. \square

4.8. CONCLUSIONE. Si osservi che la scelta di una base di V dà una identificazione di V con $M_{n,1}(C)$, e anche di V^* con $M_{1,n}(C)$ (usando la base 1 di C). In questa identificazione il morfismo bilineare canonico $V^* \times V \rightarrow C$ si scrive come il prodotto di matrici

$$M_{1,n}(C) \times M_{n,1}(C) \longrightarrow M_{1,1}(C) = C.$$

In un certo senso possiamo dire che lo spazio duale di V è lo spazio vettoriale delle "equazioni di iperpiani di V " (ogni elemento di V^* , in quanto funzione lineare, identifica il suo nucleo, che è un sottospazio di V : di dimensione $n-1$ in generale), tenendo conto che il covettore nullo non descrive un iperpiano ma tutto lo spazio V , e che due covettori descrivono lo stesso iperpiano se e solo se sono non nulli e proporzionali (cioè linearmente dipendenti, condizione necessaria e sufficiente affinché abbiano lo stesso nucleo). L'ortogonale di un vettore è allora il sottospazio delle equazioni di iperpiani che contengono quel vettore; l'ortogonale di un sottospazio di V è l'insieme delle equazioni di iperpiani di V che contengono quel sottospazio.

♠♠ **4.9. PROBLEMA.** In questa sezione abbiamo parlato solo di spazi vettoriali di dimensione finita, ma le definizioni potevano esser date per spazi vettoriali arbitrari. Farsi degli esempi per vedere che quasi tutti i risultati riportati sono falsi per spazi vettoriali di dimensione infinita (si studi in particolare lo spazio vettoriale duale dello spazio dei polinomi, e lo si identifichi con lo spazio vettoriale delle serie formali).

5. Esercizi.

5.1. Esercizi su Applicazioni Lineari.

5.1.1. Si consideri l'applicazione f di \mathbb{R}^2 in \mathbb{R}^4 definita da $f\begin{pmatrix} s \\ t \end{pmatrix} = \begin{pmatrix} 2s+t \\ s-t \\ s+t \\ s+2t \end{pmatrix}$.

- (a) Si mostri che f è lineare;
- (b) si determini $\ker(f)$;
- (c) si trovi una base di $\text{im}(f)$.

5.1.2. Si consideri l'omomorfismo f di \mathbb{R}^3 in \mathbb{R}^2 definito da $f\begin{pmatrix} r \\ s \\ t \end{pmatrix} = \begin{pmatrix} r+s+t \\ 2r-s \end{pmatrix}$.

- (a) Si mostri che f è suriettivo;
- (b) si determini $\ker(f)$;
- (c) trovare $v \in \mathbb{R}^3$ tale che $f^{-1}\left(\begin{pmatrix} 1 \\ 2 \end{pmatrix}\right) = v + \ker(f)$;
- (d) mostrare che per ogni $\begin{pmatrix} a \\ b \end{pmatrix} \in \mathbb{R}^2$, esiste $v \in \mathbb{R}^3$, tale che $f^{-1}\left(\begin{pmatrix} a \\ b \end{pmatrix}\right) = v + \ker(f)$.

5.1.3. Considerare l'operazione di derivazione $D = \frac{d}{dX}$ come funzione di $\mathbb{R}[X]$ in sé, di $\mathbb{R}[X]_{\leq n}$ in sé, di $\mathbb{R}[[X]]$ in sé (per definizione abbiamo $D(\sum_i \alpha_i X^i) = \sum_i i\alpha_i X^{i-1}$). In ciascuno dei tre casi:

- (a) verificare che si tratta di una applicazione \mathbb{R} -lineare;
- (b) descrivere nucleo e immagine di D , specificando le dimensioni;
- (c) determinare se D è o meno iniettiva, suriettiva, biiettiva;
- (d) ripetere l'esercizio sostituendo \mathbb{R} con il corpo $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

5.1.4. Per ognuna delle seguenti condizioni, definire se possibile un endomorfismo di \mathbb{R}^3 (non nulli e) che la verifichi:

- (a) nucleo e immagine coincidano;
- (b) il nucleo contenga l'immagine;
- (c) il nucleo sia non nullo e contenuto nell'immagine;
- (d) nucleo e immagine siano complementari;
- (e) il nucleo sia diverso dall'immagine e la somma dei due non sia diretta.

Stesso problema nel caso di endomorfismi di \mathbb{R}^4 .

5.1.5. Sia V uno spazio vettoriale sul corpo C . Verificare che

- (a) se $\alpha : V \rightarrow V$ è una applicazione lineare, allora $\{v \in V : \alpha(v) = v\}$ è un sottospazio di V ;
- (b) se $W \leq V$, allora esiste una applicazione lineare $\beta : V \rightarrow V$ tale che $\{v \in V : \beta(v) = v\} = W$.

5.1.6. Sia V uno spazio vettoriale su \mathbb{R} di dimensione 3 e base v_1, v_2, v_3 . Sia φ_λ l'applicazione lineare definita da

$$\varphi(v_1) = (\lambda - 1)v_1 + 2v_2 - (\lambda + 1)v_3, \quad \varphi(v_2) = 2v_1 - \lambda v_3, \quad \varphi(v_3) = -\lambda v_1 - v_2 + (\lambda + 2)v_3$$

al variare di $\lambda \in \mathbb{R}$

- (a) determinare immagine e nucleo di φ_λ al variare di λ ;
- (b) per quali valori di λ l'immagine dell'applicazione φ_λ contiene il vettore $v_1 + 2v_2 + 2v_3$?
- (c) l'unione dei nuclei di φ_λ al variare di λ genera V ?

5.1.7. Scrivere le proiezioni su U nella direzione di W , e di W nella direzione di U per i seguenti due sottospazi di \mathbb{R}^3 : $U = \langle \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} \rangle$ e $W = \langle \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \rangle$.

5.1.8. Scrivere le proiezioni su U nella direzione di W , e di W nella direzione di U per i seguenti due sottospazi di \mathbb{R}^4 : $U = \langle \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \end{pmatrix} \rangle$ e W definito da $\begin{cases} x_1 + x_2 = 0 \\ x_3 - x_4 = 0 \end{cases}$

5.1.9. Si considerino gli \mathbb{R} -spazi vettoriali \mathbb{R}^m e \mathbb{R}^n .

- (a) Si mostri che una applicazione di \mathbb{R}^n in \mathbb{R} è lineare se e solo se è del tipo seguente:

$$(a_1, \dots, a_n) \mapsto (A_1 a_1 + \dots + A_n a_n),$$

ove A_1, \dots, A_n sono numeri reali fissati, cioè una funzione polinomiale omogenea di grado 1.

Un caso particolare è l'applicazione di \mathbb{R}^n in \mathbb{R} definita da $(a_1, \dots, a_n) \mapsto a_i$, ove $1 \leq i \leq n$; essa si indica con pr_i , e si dice la proiezione i -esima.

- (b) Si mostri che un'applicazione $f : \mathbb{R}^m \rightarrow \mathbb{R}^n$ è lineare se e solo se sono lineari le applicazioni $\text{pr}_i \circ f$ per ogni i , $1 \leq i \leq n$.

5.1.10. Siano U, V spazi vettoriali sul campo C . Siano W, Z sottospazi di U tali che $W \cap Z = 0$. Dimostrare che se $f : W \rightarrow V$ e $g : Z \rightarrow V$ sono applicazioni lineari, esiste una applicazione lineare $h : U \rightarrow V$ tale che $h|_W = f$ e $h|_Z = g$. Quando h è unica?

5.1.11. Sia P_n lo spazio vettoriale dei polinomi reali di grado $\leq n$, e sia $D : P_n \rightarrow P_n$ l'usuale derivazione, $D(f) = f'$. Si consideri l'applicazione $\varphi : P_n \rightarrow P_n$, $f \mapsto f + xf'$.

- (a) Verificare che effettivamente $f + xf' \in P_n$ se $f \in P_n$.
 (b) Dimostrare che φ è lineare.
 (c) Dimostrare che φ è un isomorfismo.

5.1.12. Si consideri l'endomorfismo $f_{a,b}$ di \mathbb{R}^2 determinato dalle condizioni $f_{a,b}(e_1) = 2e_1 + ae_2$ e $f_{a,b}(e_2) = be_1 + e_2$, dove $\{e_1, e_2\}$ è la base canonica di \mathbb{R}^2 , $a, b \in \mathbb{R}$. Dimostrare che il sottospazio $U = \langle e_1 - e_2 \rangle$ è $f_{a,b}$ -stabile (cioè che $f_{a,b}(U) \subseteq U$) se e solo se $a - b + 1 = 0$.

5.1.13. Si considerino i sottoinsiemi $B_t = \left\{ (0,1,1), \begin{pmatrix} 1 \\ 2t \\ 0 \end{pmatrix}, \begin{pmatrix} t \\ 3 \\ 1 \end{pmatrix} \right\}$ di \mathbb{R}^3 , per ogni $t \in \mathbb{R}$.

- (a) Per quali valori di t l'insieme B_t è una base di \mathbb{R}^3 ?
 (b) Per quali valori di t esiste un endomorfismo φ di \mathbb{R}^3 tale che $\varphi \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$, $\varphi \begin{pmatrix} 1 \\ 2t \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$,
 $\varphi \begin{pmatrix} t \\ 3 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}$?
 (c) Per quali valori di t l'endomorfismo di cui in (b) è unico?

5.1.14. Sia M il campo $\{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$, e sia $f : M \rightarrow M$ l'applicazione definita mediante $a + b\sqrt{2} \mapsto a - b\sqrt{2}$, $a, b \in \mathbb{Q}$.

- (a) Verificare che M è spazio vettoriale su \mathbb{Q} di dimensione 2.
 (b) Verificare che M è spazio vettoriale su M di dimensione 1.
 (c) Verificare che f è una applicazione \mathbb{Q} -lineare.
 (d) Verificare che f non è una applicazione M -lineare.

5.1.15. Siano V e W due spazi vettoriali su \mathbb{R} .

- (a) Siano f un'applicazione lineare di V in W e $G_f \subset V \times W$ il suo grafico. Si mostri che se f è lineare, allora G_f è un sottospazio vettoriale di $V \times W$.
 (b) Sia $G \subset V \times W$ un sottospazio; si mostri che $G = G_f$ per un qualche omomorfismo f , se e solo se l'applicazione π_V da G in V , definita da $(v, w) \mapsto v$, è un isomorfismo.
 (c) Si supponga che sia $G = G_f$ per un qualche omomorfismo f . Si mostri che esiste una applicazione lineare π_W da G in W tale che $f = \pi_W \circ \pi_V^{-1}$.

5.1.16. Siano V e W spazi vettoriali su C con basi v_1, v_2, v_3, v_4 e w_1, w_2, w_3 rispettivamente.

- (a) dire se esiste una applicazione lineare φ tale che

$$\begin{aligned} \varphi(v_1 + v_2 + v_3 + v_4) &= w_1 + w_2 + w_3 & \varphi(v_1 + v_2) &= w_1 - w_2 \\ \varphi(v_1 + v_2 + v_3) &= 2w_1 + 2w_2 + 2w_3 & \varphi(v_1 - v_2) &= w_1 - w_2 \end{aligned}$$

ed eventualmente se è unica o no; calcolare nucleo e immagine, discutere iniettività e suriettività;

- (b) mostrare che il sottinsieme $\{\psi \in \text{End}_{\mathbb{R}}(V) : \varphi \circ \psi = 0\}$ è un sottospazio vettoriale di $\text{End}_{\mathbb{R}}(V)$ e calcolarne la dimensione e una base;
 (c) mostrare che il sottinsieme $\{\vartheta \in \text{End}_{\mathbb{R}}(W) : \vartheta \circ \varphi = 0\}$ è un sottospazio vettoriale di $\text{End}_{\mathbb{R}}(W)$ e calcolarne la dimensione e una base.

5.1.17. Sia V uno spazio vettoriale di dimensione n sul corpo C , e si indichi con V^* lo spazio vettoriale $\text{Hom}_C(V, C)$.

- (a) Si mostri che $f \in V^*$ è suriettivo se e solo se $f \neq 0$.
 (b) Si mostri che se $f, g \in V^*$ hanno lo stesso nucleo, allora essi sono linearmente dipendenti; in quali casi è vera l'implicazione inversa?
 (c) Siano $f, g \in V^*$ linearmente indipendenti; si calcoli $\dim_C(\ker f \cap \ker g)$.

5.2. Esercizi su Matrici.

5.2.1. Sia $D : C[X]_{\leq 4} \rightarrow C[X]_{\leq 4}$ l'usuale derivazione tra polinomi;

- (a) scrivere la matrice associata a D nella base canonica $1, X, X^2, X^3, X^4$;
 (b) trovare una base di $C[X]_{\leq 4}$ fatta di polinomi di grado 4 e scrivere la matrice associata a D in questa base;
 (c) scrivere la matrice di cambiamento di base tra le due basi precedenti, e verificare la relazione di cambiamento di base per le due matrici associate a D ;
 (d) esistono mappe inverse a destra o a sinistra per D ? in caso affermativo, scriverne le matrici nelle due basi date e verificare la relazione con le matrici di D ;
 (e) ripetere tutto usando $D : C[X]_{\leq 4} \rightarrow C[X]_{\leq 3}$.

5.2.2. Sia $f : \mathbb{R}^3 \rightarrow \mathbb{R}^3$ l'applicazione lineare definita da $f \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} x+y \\ y+z \\ z+x \end{pmatrix}$.

- (a) Scrivere la matrice in base canonica;
 (b) scriverne la matrice nella base v_1, v_2, v_3 ove v_j è il vettore di coordinate tutte uguali a 1 tranne la j -esima uguale a 0;
 (c) scrivere la matrice di cambiamento di base e verificare la relazione tra le due matrici di f ;
 (d) discutere iniettività e suriettività di f .

5.2.3. Consideriamo la proiezione p su V nella direzione di W e la proiezione q su W nella direzione di V ove $V = \langle \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} \rangle$ e $W = \langle \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} \rangle$ sono sottospazi di \mathbb{R}^4 .

- (a) verificare che $\mathbb{R}^4 = V \oplus W$ e scrivere le matrici di p e q nella base di \mathbb{R}^4 formata giustapprendendo le basi di V e di W ;
 (b) si scrivano le matrici A e B di p e q nella base canonica di \mathbb{R}^4 ;
 (c) esplicitare le matrici di cambiamento di base e verificare le relazioni tra le matrici precedentemente trovate;
 (d) vero che $AB = BA = 0$?

Consideriamo ora la simmetria s di centro V e di asse W e la simmetria t di centro W e di asse V .

- (a') verificare che $\mathbb{R}^4 = V \oplus W$ e scrivere le matrici di s e t nella base di \mathbb{R}^4 formata giustapprendendo le basi di V e di W ;
 (b') si scrivano le matrici A e B di s e t nella base canonica di \mathbb{R}^4 ;
 (c') esplicitare le matrici di cambiamento di base e verificare le relazioni tra le matrici precedentemente trovate;
 (d') vero che $AB = BA$? vero che $A^2 = B^2 = \mathbb{I}_4$?

5.2.4. Sia $L : M_2(\mathbb{R}) \rightarrow M_2(\mathbb{R})$ l'applicazione definita da $L \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 2 & 4 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix}$.

- (a) Verificare che si tratta di una applicazione lineare e scriverne la matrice nella base canonica;
 (b) trovare una base del nucleo di L ;
 (c) L è suriettiva? Trovare la dimensione e una base dell'immagine di L .

5.2.5. Sia $\varphi : C[X]_{\leq 4} \rightarrow C[X]_{\leq 4}$ la funzione definita da $\varphi(P) = P + XD(P)$ ove D è l'usuale derivazione tra polinomi;

- (a) scrivere la matrice associata a φ nella base canonica $1, X, X^2, X^3, X^4$;
 (b) scrivere la matrice associata a φ nella base $X^4, D(X^4), D^2(X^4), D^3(X^4), D^4(X^4)$;
 (c) scrivere la matrice di cambiamento di base tra le due basi precedenti, e verificare la relazione di cambiamento di base per le due matrici associate a φ ;
 (d) esistono mappe inverse a destra o a sinistra per φ ? in caso affermativo, scriverne le matrici nelle due basi date e verificare la relazione con le matrici di φ .

5.2.6. Sia A una matrice quadrata d'ordine n nilpotente, cioè esista un intero positivo m tale che $A^m = 0$. Mostrare che $\mathbb{I}_n + A$ è una matrice invertibile. Cosa significa la nilpotenza in termini di una applicazione lineare rappresentata da quella matrice?

5.2.7. Si diano degli esempi di matrici quadrate dello stesso ordine, non nulle, A e B tali che $AB = 0$. È vero che allora necessariamente si ha $BA = 0$ (giustificare o dare controesempi)? Interpretare gli esempi in termini di applicazioni lineari rappresentate da quelle matrici.

5.2.8. Dire se è possibile che il prodotto di tre matrici A, B, C , quadrate dello stesso ordine e non nulle, si annulli ($ABC = 0$) nei seguenti casi:

- (a) A sia invertibile;

- (b) B sia invertibile;
 (c) C sia invertibile

(giustificare la risposta o dare dei controesempi).

5.2.9. Siano A e B due matrici quadrate dello stesso ordine. Dire che rapporti vi sono tra il fatto che A e B siano invertibili e il fatto che $A + B$ sia invertibile. Spiegare con degli esempi.

5.2.10. È vero che ogni matrice reale quadrata non (necessariamente) invertibile si può scrivere come somma di due matrici invertibili?

- (a) Caratterizzare gli endomorfismi di \mathbb{R}^n che vengono rappresentati sempre dalla stessa matrice in ogni base (i morfismi $\varphi : \mathbb{R}^n \rightarrow \mathbb{R}^n$ tali che $\alpha_{\mathcal{V}, \mathcal{V}}(\varphi) = \alpha_{\mathcal{W}, \mathcal{W}}(\varphi)$ per ogni coppia di basi \mathcal{V} e \mathcal{W} di \mathbb{R}^n).
- (b) Caratterizzare l'insieme di tutte le matrici quadrate d'ordine n che commutano con tutte le altre matrici (le matrici A tali che $AB = BA$ per ogni altra matrice B ; quest'insieme si dice il centro dell'algebra delle matrici).
- (c) Che relazione c'è tra i due punti precedenti?

5.2.11. Sia $A = \begin{pmatrix} 2 & 1 & 0 \\ -1 & 1 & 2 \end{pmatrix}$:

- (a) determinare, se esistono, le matrici $B \in M_{3 \times 2}(\mathbb{Q})$ tali che $AB = \mathbb{I}_2$;
 (b) determinare, se esistono, le matrici $C \in M_{3 \times 2}(\mathbb{Q})$ tali che $CA = \mathbb{I}_3$;
 (c) discutere i punti precedenti in termini di applicazioni lineari, se già non si è fatto;
 (d) descrivere l'insieme di cui al punto (a) in termini dello spazio vettoriale $M_{3 \times 2}(\mathbb{Q})$.

5.2.12. Siano $A = \begin{pmatrix} 1 & 2 & -4 \\ 2 & 4 & -8 \\ 3 & 6 & -12 \end{pmatrix}$ e $C = \begin{pmatrix} 0 & 1 & 1 & -2 \\ 2 & 0 & -2 & 2 \\ 3 & 2 & -1 & -1 \end{pmatrix}$ e sia $U = \{B \in M_3(\mathbb{R}) : ABC =$

$0\}$;

- (a) mostrare che U è un sottospazio di $M_3(\mathbb{R})$;
 (b) calcolare la dimensione di U su \mathbb{R} ;
 (c) trovare una base di U .

5.2.13. Siano $A \in M_2(\mathbb{Q})$ e $B \in M_3(\mathbb{Q})$; si consideri l'applicazione $\tau : M_{2 \times 3}(\mathbb{Q}) \rightarrow M_{2 \times 3}(\mathbb{Q})$ definita da $\tau(X) = AXB$.

- (a) Si mostri che τ è lineare;
 (b) si mostri che τ è invertibile se e solo se A e B sono invertibili;
 (c) si scriva una base di τ nella base canonica con l'ordine lessicografico;
 (d) stimare le dimensioni di nucleo e immagine di τ in funzione dei ranghi di A e B .

5.2.14. Si considerino gli spazi vettoriali V e W su \mathbb{R} con le rispettive basi $\mathcal{V} = (v_1, v_2, v_3, v_4)$ e $\mathcal{W} = (w_1, w_2, w_3)$.

- (a) Si dica se esiste un'applicazione lineare $\varphi : V \rightarrow W$ che soddisfa alle seguenti condizioni

$$\begin{aligned} \varphi(v_1 + v_2) &= 2w_1 + w_2 + 3w_3, & \varphi(v_2 + v_3) &= 2w_1 + 2w_2 + 5w_3, \\ \varphi(v_1 + v_2 + v_3) &= 4w_1 + 2w_2 + 6w_3, & \varphi(v_2 + v_3 + v_4) &= 4w_1 + w_2 + 4w_3; \end{aligned}$$

e se ne scriva la matrice rispetto alle basi date.

- (b) Si mostri che il sottoinsieme $A = \{\psi \in \text{Hom}_{\mathbb{R}}(V, V) : \varphi \circ \psi = 0\}$ è un sottospazio dello spazio vettoriale $\text{Hom}_{\mathbb{R}}(V, V)$ e se ne calcoli la dimensione. Sia $\alpha_{\mathcal{V}, \mathcal{V}} : \text{Hom}_{\mathbb{R}}(V, V) \rightarrow M_4(\mathbb{R})$ l'applicazione che ad ogni endomorfismo di V associa la sua matrice, rispetto alla base \mathcal{V} . Si determini una base per il sottospazio immagine di A .
- (c) Si mostri che il sottoinsieme $B = \{\vartheta \in \text{Hom}_{\mathbb{R}}(W, W) : \vartheta \circ \varphi = 0\}$ è un sottospazio dello spazio vettoriale $\text{Hom}_{\mathbb{R}}(W, W)$ e se ne calcoli la dimensione. Sia $\alpha_{\mathcal{W}, \mathcal{W}} : \text{Hom}_{\mathbb{R}}(W, W) \rightarrow M_3(\mathbb{R})$ l'applicazione che ad ogni endomorfismo di W associa la sua matrice, rispetto alla base \mathcal{W} . Si determini una base per il sottospazio immagine di B .
- (d) Si consideri il sottoinsieme $C = \{(\psi, \vartheta) \in \text{Hom}_{\mathbb{R}}(V, V) \times \text{Hom}_{\mathbb{R}}(W, W) : \vartheta \circ \varphi \circ \psi = 0\}$ del prodotto cartesiano $\text{Hom}_{\mathbb{R}}(V, V) \times \text{Hom}_{\mathbb{R}}(W, W)$, e si mostri che $A \times B$ è contenuto in C . È vero o falso che $A \times B = C$? È vero o falso che C sia un sottospazio di $\text{Hom}_{\mathbb{R}}(V, V) \times \text{Hom}_{\mathbb{R}}(W, W)$?

5.2.15. DISUGUAGLIANZA DI FROBENIUS. Date due applicazioni lineari $\varphi : U \rightarrow V$ e $\psi : V \rightarrow W$, mostrare che $\dim \text{im}(\psi \circ \varphi) \geq \dim \text{im} \varphi + \dim \text{im} \psi - \dim V$. Dedurre che date due matrici $A \in M_{m,n}(C)$ e $B \in M_{n,l}(C)$, si ha $\text{rg}(AB) \geq \text{rg}(A) + \text{rg}(B) - n$.

5.2.16. Si considerino gli spazi vettoriali V e W su \mathbb{R} con le rispettive basi $\mathcal{V} = (v_1, v_2, v_3, v_4)$ e $\mathcal{W} = (w_1, w_2, w_3)$.

(a) Si dica se esistono applicazioni lineari $\varphi : V \rightarrow W$ che soddisfano alle seguenti condizioni

$$\begin{aligned}\varphi(v_1 + v_2 + v_3) &= 2w_1 + 4w_2 + 2w_3, & \varphi(v_1 + v_3) &= 2w_1 + 3w_2 + w_3, \\ \varphi(v_1 + v_2) &= w_1 + 2w_2 + w_3, & \varphi(v_2 + v_3) &= w_1 + 3w_2 + 2w_3;\end{aligned}$$

ed eventualmente si descriva questo insieme come sottoinsieme dello spazio vettoriale $\text{Hom}_{\mathbb{R}}(V, W)$.

(a) Sia $\alpha_{\mathcal{V}, \mathcal{W}} : \text{Hom}_{\mathbb{R}}(V, W) \rightarrow M_{4 \times 3}(\mathbb{R})$ l'applicazione che ad ogni morfismo di V in W associa la sua matrice, rispetto alle basi \mathcal{V} e \mathcal{W} . Si descriva l'insieme precedente in termini dello spazio vettoriale $M_{4 \times 3}(\mathbb{R})$.

5.2.17. Si considerino gli spazi vettoriali V e W su \mathbb{R} con le rispettive basi $\mathcal{V} = (v_1, v_2, v_3, v_4)$ e $\mathcal{W} = (w_1, w_2, w_3)$.

(a) Si dica se esiste un'applicazione lineare $\varphi : V \rightarrow W$ che soddisfa alle seguenti condizioni

$$\begin{aligned}\varphi(v_1 + v_2 + v_3 + v_4) &= w_1 + w_2 + w_3, & \varphi(v_1 + v_2) &= w_1 - 2w_2, \\ \varphi(v_1 + v_2 + v_3) &= 2w_1 + 2w_2 + 2w_3, & \varphi(v_1 - v_2) &= w_1 - 2w_2;\end{aligned}$$

e se ne scriva la matrice rispetto alle basi date.

(b) Si dica se il sottoinsieme $A = \{\psi \in \text{Hom}_{\mathbb{R}}(V, V) : \varphi \circ \psi = \varphi\}$ è un sottospazio dello spazio vettoriale $\text{Hom}_{\mathbb{R}}(V, V)$, e in ogni caso se ne dia una descrizione esplicita.

(c) Sia $\alpha_{\mathcal{V}, \mathcal{V}} : \text{Hom}_{\mathbb{R}}(V, V) \rightarrow M_4(\mathbb{R})$ l'applicazione che ad ogni endomorfismo di V associa la sua matrice, rispetto alla base \mathcal{V} . Si descriva l'immagine di A in termini dello spazio vettoriale $M_4(\mathbb{R})$.

5.2.18. Siano A e B due matrici quadrate di ordine m ed n rispettivamente a coefficienti in C ; consideriamo i seguenti insiemi:

$$\mathcal{A} = \{X \in M_{m \times n}(C) : AX = 0\}, \quad \mathcal{B} = \{X \in M_{m \times n}(C) : XB = 0\}, \quad \mathcal{C} = \{X \in M_{m \times n}(C) : AXB = 0\}.$$

- Verificare che sono tre sottospazi di $M_{m \times n}(C)$ e stabilire le ovvie relazioni di inclusione;
- calcolare le dimensioni dei tre sottospazi in funzione dei ranghi di A e B ;
- studiare $\mathcal{A} \cap \mathcal{B}$;
- è vero che $\mathcal{A} + \mathcal{B} = \mathcal{C}$?

5.2.19. Sia $V = M_{3 \times 3}(\mathbb{R})$ con la solita struttura di spazio vettoriale su \mathbb{R} . Si consideri l'applicazione $\text{tr} : V \rightarrow \mathbb{R}$ definita da $\text{tr}(A) = a_{11} + a_{22} + a_{33}$, per ogni $A = (a_{ij}) \in V$.

- Si mostri che tr è un'applicazione \mathbb{R} -lineare, se ne scriva la matrice nelle basi canoniche, e si calcoli la dimensione del suo nucleo;
- Si mostri che per ogni $A, B \in V$ risulta $\text{tr}(AB) = \text{tr}(BA)$;
- Si indichi con $\mathcal{E} = (e_{ij} : i, j = 1, 2, 3)$ la base canonica di V ; si calcoli la dimensione del sottospazio di V generato dalle matrici $e_{ij}e_{rs} - e_{rs}e_{ij}$ al variare di e_{ij} e e_{rs} in \mathcal{E} ;
- Si calcoli la dimensione del sottospazio di V generato da tutte le matrici del tipo $AB - BA$ al variare di A, B in V .

5.2.20. Sia V uno spazio vettoriale con base (v_1, v_2, v_3, v_4) . Sia $f : V \rightarrow V$ l'endomorfismo di V di matrice $A = \begin{pmatrix} 2 & 0 & 5 & 0 \\ 0 & 2 & 1 & 0 \\ 3 & -1 & 7 & 0 \\ 1 & 2 & 3 & 1 \end{pmatrix}$ rispetto alla base data. Determinare una base di $\ker f^*$.

Capitolo III

Sistemi Lineari

In questo capitolo presentiamo le definizioni ed i risultati fondamentali della teoria dei sistemi di equazioni lineari. Pur trattandosi d'un problema puramente "algebrico", è la sua interpretazione in termini geometrici che permette la migliore comprensione dei risultati importanti, ed è in termini della geometria degli spazi vettoriali (ed affini) che le dimostrazioni risultano più chiare.

Il primo paragrafo presenta la teoria generale, che può essere riassunta nel teorema di Rouché-Capelli per i sistemi lineari generali, e nella regola di Cramer per sistemi lineari quadrati invertibili.

Il secondo paragrafo presenta il metodo di riduzione di Gauss per la risoluzione di un sistema lineare, ed ancora si enfatizzano i legami tra il calcolo algebrico (matriciale) e la geometria degli spazi vettoriali.

Nota terminologica: in questo capitolo si parlerà di "sottospazi affini" o di "sottovarietà lineari affini" di uno spazio vettoriale standard. Questi termini saranno definiti più in generale per gli spazi affini in un futuro capitolo. Per ora si deve intendere questo: un sottospazio affine (o equivalentemente una sottovarietà lineare affine) è una qualsiasi classe laterale di un sottospazio vettoriale, cioè un sottinsieme \mathbb{L} di K^n del tipo $v + W = \{v + w | w \in W\}$ con $v \in K^n$ e W un sottospazio vettoriale di K^n . Si tratta dei "traslati" di sottospazi vettoriali; talvolta il vettore v , o meglio il suo "estremo", si dice "punto di passaggio" di \mathbb{L} e il sottospazio W si dice "direzione" o "giacitura" di \mathbb{L} . In questo contesto l'insieme K^n viene indicato anche con il simbolo $\mathbb{A}(K^n)$ oppure $\mathbb{A}^n(K)$ (e si legge "spazio affine associato a K^n ").

1. Sistemi Lineari.

Sia K un corpo fissato.

1.1. DEFINIZIONE. Un sistema lineare di m equazioni ed n incognite (e a coefficienti in K) è una lista di m equazioni nelle incognite X_1, \dots, X_n ,

$$\begin{cases} a_{1,1}X_1 + a_{1,2}X_2 + \dots + a_{1,n}X_n = b_1 \\ a_{2,1}X_1 + a_{2,2}X_2 + \dots + a_{2,n}X_n = b_2 \\ \vdots \\ a_{m,1}X_1 + a_{m,2}X_2 + \dots + a_{m,n}X_n = b_m \end{cases}$$

ove $a_{i,j}, b_i \in K$ (per ogni $i = 1, \dots, m$ e $j = 1, \dots, n$) si dicono i coefficienti del sistema; in particolare i b_i (per ogni $i = 1, \dots, m$) si dicono i termini noti del sistema. Il sistema si dice omogeneo se tutti i termini noti sono nulli, e si dice quadrato se $m=n$.

1.1.1. SCRITTURA MATRICIALE. Un sistema come sopra si rappresenta in forma matriciale come

$$\begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m,1} & a_{m,2} & \cdots & a_{m,n} \end{pmatrix} \begin{pmatrix} X_1 \\ X_2 \\ \vdots \\ X_n \end{pmatrix} = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{pmatrix}$$

e in forma più compatta con

$$AX=b$$

ove $A = (a_{i,j}) \in M_{m,n}(K)$ (matrici $m \times n$ a coefficienti in K), $X = (X_1, X_2, \dots, X_n)^t$ e $b = (b_i) \in K^m$ (vettore dello spazio vettoriale standard K^m).

La matrice A si dice la matrice incompleta del sistema o matrice dei coefficienti, la matrice $(A \ b) \in M_{m,n+1}(K)$, che si ottiene aggiungendo alla matrice incompleta la colonna dei termini noti,

si dice la matrice completa del sistema. Il sistema è quadrato se la matrice incompleta è quadrata. Omogeneo se b è il vettore nullo.

1.2. DEFINIZIONE. Dato un sistema lineare $AX = b$ come sopra, si dice soluzione del sistema ogni n -pla $(x_1, \dots, x_n)^t \in K^n$ per cui valgono tutte le uguaglianze. Risolvere il sistema significa trovare tutte le soluzioni, cioè descrivere esplicitamente l'insieme

$$S_{A,b} = \{x \in K^n \text{ tali che } Ax = b\}$$

delle soluzioni. Nel caso $S_{A,b}$ sia vuoto il sistema si dice impossibile o incompatibile. In caso contrario il sistema si dice compatibile.

1.2.1. INTERPRETAZIONE VETTORIALE. La matrice incompleta A del sistema lineare può essere interpretata come la matrice di una applicazione lineare

$$\varphi_A : K^n \longrightarrow K^m$$

espressa dalla matrice A rispetto alle basi canoniche di K^n e K^m . L'insieme $S_{A,b}$ delle soluzioni si può quindi interpretare come l'immagine inversa tramite φ_A del vettore $b \in K^m$:

$$S_{A,b} = \varphi_A^{-1}(b) := \{x \in K^n \text{ tali che } \varphi_A(x) = b\}.$$

Questa interpretazione ci permette di capire qual è la struttura dell'insieme delle soluzioni.

Nel caso più semplice in cui il sistema è omogeneo, dunque $b = 0$, si tratta di calcolare il nucleo dell'applicazione lineare φ_A . Dunque $S_{A,0} = \ker \varphi_A$, e si tratta di un sottospazio vettoriale di K^n , di dimensione $\dim_K \ker \varphi_A = n - \dim_K \text{im } \varphi_A = n - \text{rg}(A)$. Risolvere il sistema equivale dunque a scrivere una base del nucleo di φ_A .

Nel caso in cui il sistema non sia omogeneo, si possono presentare due casi:

- (i) il vettore $b \in K^m$ non appartiene all'immagine $\text{im}(\varphi_A)$ dell'applicazione lineare φ_A ; in tal caso $S_{A,b} = \emptyset$, e il sistema è impossibile.
- (ii) il vettore $b \in K^m$ appartiene all'immagine $\text{im}(\varphi_A)$ dell'applicazione lineare φ_A ; in tal caso, scelta una soluzione particolare $x_0 \in K^n$ del sistema (dunque $Ax_0 = b$), ogni altra soluzione si scrive sommando a x_0 una soluzione del sistema lineare omogeneo avente la stessa matrice dei coefficienti (infatti, se $y \in K^n$ è un'altra soluzione, allora $y = x_0 + (y - x_0)$, e $y - x_0$ soddisfa a $A(y - x_0) = Ay - Ax_0 = b - b = 0$, dunque è soluzione del sistema lineare omogeneo associato; viceversa se $z \in K^n$ soddisfa $Az = 0$, allora $x_0 + z$ soddisfa a $A(x_0 + z) = Ax_0 + Az = b + 0 = b$, dunque è soluzione del sistema originario). Dunque abbiamo mostrato che $S_{A,b} = x_0 + \ker \varphi_A = x_0 + S_{A,0}$, e si conclude che $S_{A,b}$ è una sottovarietà lineare affine dello spazio affine standard $\mathbb{A}(K^n)$. Risolvere il sistema equivale quindi a descrivere la sottovarietà affine $x_0 + \ker \varphi_A$, e dunque si riduce a trovare una soluzione particolare x_0 e il sottospazio delle soluzioni del sistema lineare omogeneo associato.

1.2.2. OSSERVAZIONE SUL PROBLEMA INVERSO. La discussione precedente mostra che il problema di risolvere un sistema lineare si presenta come il problema di descrivere una sottovarietà affine di $\mathbb{A}(K^n)$ a partire da un insieme di equazioni che la definiscono; in altri termini si tratta di trovare equazioni parametriche, ovvero una descrizione in termini di punti e generatori del sottospazio direttore, per una sottovarietà lineare affine descritta da equazioni "cartesiane" (il sistema di partenza).

Sappiamo che anche il problema inverso è importante: trovare equazioni cartesiane di una sottovarietà affine lineare di $\mathbb{A}(K^n)$ che sia descritta in termini di punti, oppure di un punto di passaggio e uno spazio direttore. Si tratta in questo caso di trovare un sistema lineare di equazioni il cui insieme di soluzioni sia la sottovarietà affine lineare data.

Ricordiamo brevemente come risolvere questo problema. Sia $\mathbb{L} = P + W$, con $P \in \mathbb{A}(K^n)$ un punto dello spazio affine e $W = \langle w_1, \dots, w_r \rangle$ un sottospazio vettoriale di K^n di dimensione r , una varietà affine di dimensione r di $\mathbb{A}(K^n)$. Essa si descrive tramite equazioni parametriche: un punto X di $P + W$ si scrive come $X = P + \sum_{i=1}^r \alpha_i w_i$ ove gli $\alpha_i \in K$ sono i parametri e, se P ha coordinate (p_1, \dots, p_n) , si può esplicitare:

$$\begin{pmatrix} X_1 \\ X_2 \\ \vdots \\ X_n \end{pmatrix} = \begin{pmatrix} p_1 \\ p_2 \\ \vdots \\ p_n \end{pmatrix} + \alpha_1 \begin{pmatrix} w_{1,1} \\ w_{2,1} \\ \vdots \\ w_{n,1} \end{pmatrix} + \dots + \alpha_r \begin{pmatrix} w_{1,r} \\ w_{2,r} \\ \vdots \\ w_{n,r} \end{pmatrix} \quad \text{ovvero} \quad \begin{cases} X_1 = p_1 + \alpha_1 w_{1,1} + \dots + \alpha_r w_{1,r} \\ X_2 = p_2 + \alpha_1 w_{2,1} + \dots + \alpha_r w_{2,r} \\ \dots \\ X_n = p_n + \alpha_1 w_{n,1} + \dots + \alpha_r w_{n,r} \end{cases}$$

ove $w_j = (w_{i,j})$ sono le coordinate dei vettori w_j .

Un sistema di equazioni per \mathbb{L} si può ottenere tramite il procedimento di “eliminazione dei parametri” a partire dalle equazioni precedenti (si procede ricavando un parametro da una equazione e sostituendolo nelle rimanenti: dopo aver eliminato tutti i parametri resta un sistema lineare di $n-r$ equazioni).

Ma *conoscendo la nozione di determinante*, si può procedere in modo più sistematico per trovare subito un sistema di equazioni cartesiane: si impone la condizione

$$\operatorname{rg} \begin{pmatrix} X-P & w_1 & \cdots & w_r \end{pmatrix} \leq r$$

(matrice $n \times (r+1)$) che equivale ad annullare tutti i minori d'ordine $r+1$. Equivalentemente si può chiedere che

$$\operatorname{rg} \begin{pmatrix} 1 & 1 & 0 & \cdots & 0 \\ X & P & w_1 & \cdots & w_r \end{pmatrix} \leq r+1$$

(matrice $(n+1) \times (r+2)$) che di nuovo equivale ad annullare tutti i minori d'ordine $r+2$. Apparentemente si tratterebbe di $\binom{n+1}{r+2}$ equazioni, ma il rango del sistema sarà comunque $n-r$. Per trovare esattamente $n-r$ equazioni indipendenti si ricorre al *principio dei minori orlati*: dalle ultime $r+1$ colonne, possiamo estrarre una sottomatrice quadrata invertibile di ordine $r+1$; le equazioni richieste si ottengono annullando i determinanti di ordine $r+2$ della matrice completa contenenti la sottomatrice scelta (ovvero i minori che si ottengono “orlando” la sottomatrice invertibile scelta).

Un analogo ragionamento porta a descrivere la sottovarietà affine lineare passante per i punti P_0, P_1, \dots, P_r tramite la condizione

$$\operatorname{rg} \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ X & P_0 & P_1 & \cdots & P_r \end{pmatrix} \leq r+1$$

(matrice $(n+1) \times (r+2)$) cui di nuovo si può applicare il principio dei minori orlati per ricavare esattamente $n-r$ equazioni, se i punti dati erano in posizione generale.

Anticipiamo infine che l'interpretazione cartesiana (che verrà trattata parlando di spazi euclidei in un futuro capitolo) dei coefficienti dell'equazione di un iperpiano (essi formano un vettore ortogonale allo spazio direttore dell'iperpiano) dà un metodo pratico per trovare equazioni cartesiane. Sia $\mathbb{L} = P + W$ come usuale, con $P \in \mathbb{A}(K^n)$ un punto dello spazio affine e $W = \langle w_1, \dots, w_r \rangle$ un sottospazio vettoriale di K^n di dimensione r . Allora possiamo scrivere un sistema di equazioni per \mathbb{L} della forma $AX = AP$, ove $A \in M_{(n-r),n}$ è una matrice le cui righe sono generatori del sottospazio W^\perp ortogonale di W .

1.2.3. INTERPRETAZIONE GEOMETRICA. Insistiamo ancora sulla interpretazione geometrica di questi oggetti; abbiamo visto che le soluzioni di un sistema lineare $AX = b$ sono una sottovarietà affine lineare \mathbb{L} , e che risolvere il sistema significa descrivere la sottovarietà affine parametricamente come $\mathbb{L} = P + \langle w_1, \dots, w_r \rangle$ ($P \in \mathbb{A}(K^n)$ una soluzione particolare e $\langle w_1, \dots, w_r \rangle$ sottospazio di K^n delle soluzioni del sistema omogeneo associato). Si tratta quindi di passare dalla descrizione di \mathbb{L} come “insieme degli zeri” della funzione

$$f : \mathbb{A}(K^n) \longrightarrow \mathbb{A}(K^m) \quad X = (X_1, \dots, X_n)^t \longmapsto AX - b$$

ad una descrizione di \mathbb{L} come “immagine” della funzione

$$g : \mathbb{A}(K^r) \longrightarrow \mathbb{A}(K^n) \quad Y = (Y_1, \dots, Y_r)^t \longmapsto P + \sum_i Y_i w_i$$

(e viceversa per il problema inverso). Per rappresentare \mathbb{L} si può sempre scegliere f suriettiva (sistema minimale di equazioni) e g iniettiva (sistema minimale di generatori).

Veniamo ora al risultato fondamentale:

1.3. TEOREMA DI ROUCHÉ-CAPELLI. *Il sistema lineare $AX=b$ con $A \in M_{m,n}(K)$ e $b \in K^m$ ammette soluzioni se e solo se il rango della matrice completa è uguale al rango della matrice incompleta, ed in tal caso se x_0 è una soluzione, l'insieme $S_{A,b}$ di tutte le soluzioni si scrive come $x_0 + S_{A,0}$ dove $S_{A,0}$ è il sottospazio vettoriale di K^n delle soluzioni del sistema lineare omogeneo associato, i.e. $AX = 0$. Infine si ha che $\dim_K S_{A,0} = n - \operatorname{rg}(A)$.*

DIMOSTRAZIONE. Come abbiamo fatto sopra, interpretiamo il problema usando l'applicazione

$$\varphi_A : K^n \longrightarrow K^m$$

di matrice A nelle basi canoniche. Affinché il sistema abbia soluzione è necessario e sufficiente che il vettore $b \in K^m$ appartenga all'immagine di φ_A , ovvero per definizione che sia combinazione lineare delle colonne della matrice A , ovvero ancora che matrice completa e incompleta del sistema abbiano lo stesso rango (aggiungendo la colonna b il rango non deve aumentare). Nel caso vi siano soluzioni, abbiamo visto prima che esse si scrivano come $x_0 + S_{A,0}$ ove x_0 è una soluzione particolare e $S_{A,0} = \ker \varphi_A$. La formula delle dimensioni per l'applicazione lineare φ_A dà allora $n = \dim_K \ker \varphi_A + \dim_K \operatorname{im} \varphi_A = \dim_K S_{A,0} + \operatorname{rg}(A)$, da cui l'ultima affermazione. \square

In particolare, nel caso di sistemi quadrati in cui la matrice $n \times n$ dei coefficienti sia invertibile (cioè di rango n), abbiamo uno spazio delle soluzioni ridotto ad un punto: infatti qualunque sia il vettore dei termini noti il rango della matrice completa è comunque n (corrisponde al fatto che l'applicazione φ_A è suriettiva), e lo spazio delle soluzioni del sistema omogeneo associato è ridotto al vettore nullo (corrisponde al fatto che l'applicazione φ_A è iniettiva).

Il seguente risultato permette un calcolo esplicito dell'unico punto soluzione: vi si presuppone la conoscenza della nozione di determinante, e va quindi letto dopo che tale nozione sia stata introdotta.

1.4. REGOLA DI CRAMER. *Il sistema $AX=b$ con $A \in M_n(C)$ (sistema quadrato) ha un'unica soluzione se e solo se $\det A \neq 0$, i.e. se la matrice A è invertibile, e in tal caso l'unica soluzione è $x=A^{-1}b$. Se A_i è la matrice che si ottiene da A sostituendo la i -esima colonna con la colonna b dei termini noti, si ha che $x_i = \det A_i / \det A$.*

DIMOSTRAZIONE. Dal teorema di Rouché-Capelli sappiamo che la soluzione esiste unica se e solo se A ha rango massimo, e questo equivale a che A sia invertibile, e anche a che $\det A \neq 0$. Chiaramente la soluzione cercata è data da $x=A^{-1}b$. Ricordiamo che la matrice inversa si calcola usando i complementi algebrici della matrice A , precisamente

$$A^{-1} = \frac{1}{\det A} (c_{i,j})$$

ove $c_{i,j} = (-1)^{i+j} \det A_{j,i}$ è il determinante della matrice che si ottiene da A eliminando la j -esima riga e la i -esima colonna. Di conseguenza si ottiene

$$x_i = \frac{1}{\det A} \sum_{j=1}^n c_{i,j} b_j = \frac{1}{\det A} \sum_{j=1}^n (-1)^{i+j} b_j \det A_{j,i} = \frac{\det A_i}{\det A}$$

poiché la sommatoria scritta rappresenta lo sviluppo di Laplace del determinante di A_i rispetto alla i -esima colonna (costituita dai termini noti). \square

2. Riduzione di Gauss.

Rimane ancora da discutere come risolvere effettivamente un sistema lineare, ovvero dare un procedimento effettivo che permetta di scrivere tutte le soluzioni. Per questo definiamo la nozione di sistemi equivalenti.

2.1. DEFINIZIONE. *Due sistemi $AX=b$ e $A'X=b'$, con $A \in M_{m,n}(K)$ ed $A' \in M_{m',n}(K)$, $b \in K^m$ e $b' \in K^{m'}$ (cioè aventi lo stesso numero di incognite!), si dicono equivalenti se hanno lo stesso insieme di soluzioni. Si tratta ovviamente di una relazione di equivalenza nell'insieme dei sistemi lineari in n incognite.*

Se due sistemi sono equivalenti, allora abbiamo $\operatorname{rg}(A) = \operatorname{rg}(A')$ (il viceversa è ovviamente falso).

Osserviamo subito che, se $H \in M_m(C)$ è una matrice invertibile, allora $AX = b$ è equivalente a $(HA)X = Hb$.

La morale di questo paragrafo è la seguente: *tramite operazioni elementari sulle righe della matrice completa si può trasformare il sistema in un sistema equivalente in forma a scalini, da cui si leggono subito i ranghi delle matrici (per applicare il teorema di Rouché-Capelli), e si scrivono le eventuali soluzioni.*

Vogliamo però insistere sul significato delle operazioni elementari sia in termini di matrici (moltiplicazione per certe matrici invertibili dette "matrici elementari"), sia in termini di applicazioni lineari (cambiamenti di base).

2.2. DEFINIZIONE (MATRICI A SCALINI (PER RIGA)). Una matrice $A = (a_{i,j}) \in M_{m,n}(K)$ si dice in forma a scalini (per righe) se gode della seguente proprietà: per ogni riga, se a_{r,j_r} è il primo elemento non nullo della riga, allora $a_{i,j} = 0$ ogni volta che $i \geq r$ e $j \leq j_r$, a parte $i = r$ e $j = j_r$ (significa che tutti i termini “a sinistra e in basso” rispetto ad a_{r,j_r} sono nulli, o ancora che a_{r,j_r} è l'unico elemento non nullo della sottomatrice di A che si ottiene cancellando le righe soprastanti e le colonne a destra). I primi termini non nulli di ciascuna riga si dicono allora i pivot o i termini direttori della matrice. La matrice si dice in forma speciale a scalini (per righe) se è in forma speciale e tutti i pivot sono uguali ad 1.

2.2.1. Il tipico aspetto di una matrice in forma a scalini (per righe) è dunque il seguente:

$$A = \begin{pmatrix} 0 & \cdots & 0 & a_{1,j_1} & \cdots & * & * & \cdots & * & * & \cdots & * & * & \cdots & a_{1,n} \\ 0 & \cdots & 0 & 0 & \cdots & 0 & a_{2,j_2} & \cdots & * & * & \cdots & * & * & \cdots & a_{2,n} \\ 0 & \cdots & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & a_{3,j_3} & \cdots & * & * & \cdots & a_{3,n} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & a_{r,j_r} & \cdots & a_{r,n} \\ 0 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & 0 & \cdots & 0 \end{pmatrix},$$

ove le stelline indicano elementi non (necessariamente) nulli. La condizione della definizione si può esprimere nel modo seguente: sia a_{i,j_i} il primo elemento non nullo della i -esima riga (per $i = 1, \dots, m$) ed intendiamo $j_i = n+i+1$ se la riga è nulla; allora la matrice è in forma a scalini se e solo se $j_1 < j_2 < \dots < j_m$.

Ad esempio, una matrice quadrata triangolare superiore con tutti i termini diagonali non nulli è in forma a scalini; più generalmente è in forma a scalini una matrice rettangolare con tutti gli elementi di posto (i, i) non nulli e i termini di posto (i, j) con $i < j$ nulli.

2.2.2. RANGO DI UNA MATRICE A SCALINI. Si vede immediatamente che il rango di una matrice in forma a scalini è uguale al numero di righe non nulle, ovvero uguale al numero dei pivot, che evidentemente corrispondono al numero di colonne linearmente indipendenti.

2.2.3. SOLUZIONI DI UN SISTEMA A SCALINI. Se un sistema ha matrice incompleta in forma a scalini, allora il teorema di Rouché-Capelli si applica immediatamente per dire che il sistema è impossibile se e solo se la colonna dei termini noti contiene qualche nuovo pivot (corrisponde ad avere una equazione del tipo $0 = k$ con $k \neq 0$). Se il sistema ammette soluzioni si scrivono tutte e sole nel modo seguente: comunque si assegnino degli elementi $a_j \in K$, per ogni $j \neq j_1, \dots, j_r, 1 \leq j \leq n$, esiste un'unica soluzione del sistema, $(x_1, x_2, \dots, x_n) \in K^n$, tale che $x_j = a_j$. Dunque quegli $a_j \in K$ (in numero di $n-r$) sono i parametri che permettono di scrivere tutte le soluzioni del sistema lineare.

2.2.4. Verificare per bene le due affermazioni precedenti. Fatto questo, è chiaro che per risolvere esplicitamente un sistema, basta trasformarlo in uno equivalente la cui matrice completa sia in forma a scalini. Ciò si fa tramite le “operazioni elementari” sulle righe della matrice completa.

2.3. DEFINIZIONE (OPERAZIONI ELEMENTARI SULLE RIGHE). Le seguenti operazioni si dicono “operazioni elementari sulle righe di una matrice” A :

- (i) scambiare di posto tra di loro due righe;
- (ii) sostituire una riga con la somma di se stessa e di un multiplo scalare di un'altra riga;
- (iii) moltiplicare una riga per uno scalare non nullo.

2.3.1. INTERPRETAZIONI IN TERMINI DI SISTEMI LINEARI. È chiaro che se queste operazioni vengono effettuate sulla matrice completa di un sistema lineare, si ottiene la matrice di un sistema equivalente (le operazioni corrispondono, nell'ordine, a: scambiare di posto due equazioni, sommare ad una un multiplo di un'altra, moltiplicare una equazione per uno scalare non nullo).

2.3.2. INTERPRETAZIONE IN TERMINI DI PRODOTTO DI MATRICI. Indichiamo con $e_{i,j}$ la base canonica dello spazio delle matrici quadrate d'ordine m , cioè $e_{i,j} = (\delta_{r,i}\delta_{j,s})_{1 \leq r,s \leq m}$ (delta di Kronecker). Le operazioni elementari sulle righe corrispondono a moltiplicare a sinistra la matrice A per opportune matrici invertibili $H \in M_m(C)$, dette *matrici elementari*. Precisamente:

- (i) scambiare tra di loro la i -esima e la j -esima riga corrisponde a moltiplicare per $S(i, j) := \mathbb{I} + e_{i,j} + e_{j,i} - e_{i,i} - e_{j,j}$;
 - (ii) sostituire la i -esima riga con la somma di se stessa e di $\alpha \in K$ volte la j -esima riga corrisponde a moltiplicare per $H(i, j, \alpha) := \mathbb{I} + \alpha e_{i,j}$;
 - (iii) moltiplicare la riga i -esima per $\alpha \in K$ corrisponde a moltiplicare per $H(i, \alpha) := \mathbb{I} + (\alpha - 1)e_{i,i}$.
- Che le matrici elementari siano invertibili si può vedere direttamente, ma sarà chiaro per l'osservazione successiva.

2.3.3. INTERPRETAZIONE IN TERMINI DI CAMBIAMENTO DI BASE. Identificando la matrice A con la matrice di una applicazione lineare, le operazioni elementari sulle righe si possono interpretare come cambiamenti di base *nel codominio*. Precisamente

- (i) scambiare tra di loro la i -esima e la j -esima riga corrisponde a scambiare di posto i vettori e_i ed e_j della base canonica;
- (ii) sostituire la i -esima riga con la somma di se stessa e di $\alpha \in K$ volte la j -esima riga corrisponde a sostituire il vettore e_j della base canonica con il vettore $e_j - \alpha e_i$;
- (iii) moltiplicare la riga i -esima per $\alpha \in K$ corrisponde a sostituire il vettore e_i della base canonica con il vettore $\alpha^{-1}e_i$.

Che si tratti ancora di basi di K^m è evidente, e permette subito anche di calcolare le inverse delle matrici elementari, poiché basta identificare le operazioni (elementari) che ristabiliscono la base canonica. Abbiamo $S(i, j)^{-1} = S(i, j)$ (cioè $S(i, j)^2 = \mathbb{I}$), $H(i, j, \alpha)^{-1} = H(i, j, -\alpha)$ ed infine $H(i, \alpha)^{-1} = H(i, \alpha^{-1})$.

2.3.4. RIASSUNTO. Convieni forse riassumere la discussione precedente in una tabella:

<i>operazioni elementari sulle righe di una matrice:</i>	<i>moltiplicazione a sinistra per:</i>	<i>cambiamenti di base nel codominio:</i>
scambio tra loro le righe i -esima e j -esima	la matrice elementare $S(i, j)$	scambio tra loro i vettori i -esimo e j -esimo
sommo alla riga i -esima la j -esima moltiplicata per α	la matrice elementare $H(i, j, \alpha)$	sottraggo al j -esimo vettore l' i -esimo moltiplicato per α
moltiplico la riga i -esima per $\alpha \neq 0$	la matrice elementare $H(i, \alpha)$	divido l' i -esimo vettore per α

2.4. TEOREMA (RIDUZIONE DI GAUSS). *Tramite operazioni elementari sulle righe ogni matrice può essere ridotta in forma a scalini (per righe) usando operazioni dei tipi (i) e (ii); usando anche operazioni elementari del terzo tipo ogni matrice può essere ridotta in forma speciale a scalini (per righe).*

DIMOSTRAZIONE (METODO DI RIDUZIONE DI GAUSS). Si procede per induzione sul numero di righe. A meno di un'operazione elementare del tipo (i) (scambiare la prima riga con un'altra) possiamo supporre che la prima colonna non nulla abbia il primo termine non nullo, sia a_{1,j_1} . Allora tramite operazioni elementari del secondo tipo (sommando ad ogni riga un opportuno multiplo della prima) possiamo far sì che tutti gli altri termini di quella colonna diventino nulli. Ora si procede per induzione, sulla sottomatrice che si ottiene cancellando la prima riga e la prime j_1 colonne.

Per ottenere la forma speciale per righe è ora sufficiente moltiplicare ogni riga non nulla per l'inverso del suo termine direttore. \square

2.5. CALCOLO DELL'INVERSA D'UNA MATRICE QUADRATA INVERTIBILE. Ogni matrice quadrata invertibile A può essere ridotta (tramite il metodo di Gauss) alla matrice identica, e questa riduzione permette il calcolo dell'inversa: la matrice rettangolare $(A \mathbb{I})$ viene ridotta (per righe) a $(\mathbb{I} A^{-1})$. La riduzione fino alla forma speciale per righe di A porta ad avere a sinistra una matrice triangolare superiore con tutti i termini diagonali uguali ad 1; ora delle operazioni elementari sulle righe procedendo dal basso verso l'alto permettono di ricondursi alla matrice identica. Le operazioni elementari che vengono fatte sono via via accumulate nella parte destra della matrice rettangolare, che perciò alla fine del procedimento restituisce la matrice inversa di A .

Che cosa succederebbe in questo procedimento se la matrice A non fosse invertibile?

2.6. OPERAZIONI ELEMENTARI SULLE COLONNE. Chiudiamo questo paragrafo facendo notare che (quasi) tutto quello che si è detto si potrebbe riscrivere per le colonne di una matrice, piuttosto che per le righe. Cioè *possiamo definire la forma (eventualmente speciale) a scalini per colonne, e tramite opportune operazioni elementari sulle colonne possiamo ridurre ogni matrice in quella forma*. Le operazioni elementari sulle colonne ammettono ugualmente interpretazioni in termini di moltiplicazione a destra per matrici elementari, ed in termini di cambiamenti di base nel dominio:

- (i) scambiare di posto le colonne A_i e A_j corrisponde a moltiplicare per $S(i, j) := \mathbb{I} + e_{i,j} + e_{j,i} - e_{i,i} - e_{j,j}$;
- (ii) sostituire la i -esima colonna con la somma di quella colonna e il prodotto di $\alpha \in K$ per la j -esima colonna corrisponde a moltiplicare per $H(j, i, \alpha) := \mathbb{I} + \alpha e_{j,i}$;
- (iii) moltiplicare la colonna i -esima per $\alpha \in K$; corrisponde a moltiplicare per $H(i, \alpha) := \mathbb{I} + (\alpha - 1)e_{i,i}$.

Va osservato però che queste operazioni applicate alla matrice completa di un sistema lineare *non danno sistemi lineari equivalenti*, e dunque non possono essere usate per la risoluzione.

Convieni organizzare una tabella simile a quella vista per le operazioni elementari sulle righe.

3. Esercizi.

3.1. Risolvere il sistema lineare $Ax = b$ di matrice completa $\begin{pmatrix} 10 & 23 & 17 & 44 & 25 \\ 15 & 35 & 26 & 69 & 40 \\ 25 & 57 & 42 & 108 & 65 \\ 30 & 69 & 51 & 133 & 95 \end{pmatrix}$.

3.2. Al variare di $\ell \in \mathbb{R}$, risolvere i sistemi lineari $A_\ell x = b_\ell$ di matrice completa

$$\begin{pmatrix} 5 & -3 & 2 & 4 & 3 \\ 4 & -2 & 3 & 7 & 1 \\ 8 & -6 & -1 & -5 & 9 \\ 7 & -3 & 7 & 17 & \ell \end{pmatrix} \quad \text{e} \quad \begin{pmatrix} 2 & 5 & 1 & 3 & 2 \\ 4 & 6 & 3 & 5 & 4 \\ 4 & 14 & 1 & 7 & 4 \\ 2 & -3 & 3 & \ell & 7 \end{pmatrix}.$$

3.3. Al variare di $\ell \in \mathbb{R}$ risolvere l'equazione $XA_\ell = 0$, dove $A_\ell = \begin{pmatrix} \ell & 1 & -1 \\ 0 & 1 & 1 \end{pmatrix}$. In questo problema l'incognita è la matrice $X = \begin{pmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{pmatrix}$, quindi l'equazione $XA_\ell = 0$ diventa un sistema lineare omogeneo in $x_{11}, x_{12}, x_{21}, x_{22}$.

3.4. Sia $\Sigma : Ax = b$ un sistema lineare con $A \in M_{m \times n}(K)$. Sia $H \in M_m(K)$ e $\Pi : HAx = b$. Se Σ ha soluzioni, Π ha soluzioni? In generale che relazione c'è tra i due insiemi di soluzioni? La stessa domanda con H invertibile.

3.5. In \mathbb{R}^4 si considerino i sottospazi $U = \langle \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \end{pmatrix} \rangle$, e $V = \langle \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 1 \\ 1 \end{pmatrix} \rangle$. Determinare tre sistemi lineari tali che U , V e $U \cap V$ ne siano rispettivamente gli insiemi delle soluzioni. Risolvere lo stesso problema trovando però sistemi minimali di equazioni per ciascuno dei sottospazi U , V e $U \cap V$.

3.6. Sia S l'insieme $\left\{ \begin{pmatrix} 2\lambda-1 \\ \mu+3 \\ 3\lambda+1 \\ -\lambda+\mu \end{pmatrix} \text{ tali che } \lambda, \mu \in \mathbb{R} \right\}$. Determinare un sistema lineare il cui insieme delle soluzioni coincide con S .

3.7. Sia $A = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \in M_2(\mathbb{R})$. Dimostrare che l'insieme delle matrici che commutano con A (cioè l'insieme delle matrici $B \in M_2(\mathbb{R})$ tali che $AB = BA$) è un sottospazio di $M_2(\mathbb{R})$ e calcolarne la dimensione. Per ogni intero n calcolare A^n . Determinare, per ogni $n \in \mathbb{Z}$, la dimensione dello spazio delle matrici di $M_2(\mathbb{R})$ che commutano con A^n .

3.8. Per ogni $t \in \mathbb{R}$ si consideri il sistema lineare $\Sigma_t : \begin{cases} -tx + (t-1)y + z = -1 \\ (t-1)y + tz = 1 \\ 2x + z = 5 \end{cases}$ Sia S_t l'insieme delle soluzioni di Σ_t .

- (a) Per quali valori di t S_t è costituito da un solo punto?
 (b) Per quali valori di t S_t è vuoto?
 (c) Per quali valori di t S_t è una sottovarietà lineare affine di dimensione 1?
 (d) Per i valori di t di cui al punto (c), esibire equazioni parametriche di S_t .

3.9. Sia dato il sistema lineare reale $\Sigma_k: A_k x = b_k$ di matrice completa $C_k = \begin{pmatrix} 0 & 2k & k^2 - 1 & 0 \\ k & -1 & -k & -1 \\ 1 & -k & 1 & k \end{pmatrix}$

al variare di $k \in \mathbb{R}$. Determinare per quali valori di k Σ_k ammette un'unica soluzione e, in questi casi, determinare la soluzione di Σ_k . Risolvere lo stesso problema su \mathbb{C} .

3.10. Consideriamo il sistema lineare reale $\begin{cases} x + y = 1 \\ x + z = \lambda \\ (2 - \lambda)x + y + z = 1 \end{cases}$ al variare di $\lambda \in \mathbb{R}$.

- (a) Discutere i ranghi delle matrici completa e incompleta al variare di $\lambda \in \mathbb{R}$.
 (b) Determinare per ogni $\lambda \in \mathbb{R}$ l'insieme delle soluzioni S_λ .
 (c) Descrivere l'insieme S unione di tutti gli S_λ .
 (d) È vero che S è una sottovarietà affine lineare? Eventualmente qual'è la minima sottovarietà affine lineare contenente S ?

3.11. Come l'esercizio precedente, usando il sistema $\begin{cases} x + (1 - \lambda)y + z = 1 + \lambda \\ (2 - \lambda)x + (\lambda - 1)^2 y + \lambda z = 3 - \lambda^2 \\ x + (\lambda - 1)z = 2 + \lambda \end{cases}$

3.12. Sia $A = \begin{pmatrix} 1 & 3 & 5 & 3 \\ 1 & 4 & 7 & 3 \\ 0 & 1 & 2 & 0 \\ 1 & 2 & 3 & 2 \end{pmatrix}$. Si discuta il sistema $AX = b$ al variare di b in \mathbb{R}^4 ; in particolare

si mostri che i b per i quali il sistema ammette soluzione, sono tutte e sole le soluzioni di un'equazione lineare omogenea.

3.13. Si consideri il seguente sistema lineare $\begin{cases} lx + my - mz = m \\ mx - ly = l \\ x - y - z = 0 \end{cases}$.

Si dica per quali coppie $(l, m) \in \mathbb{R}^2$ il sistema ammette soluzioni, e per quali la soluzione è unica.

3.14. Calcolare il rango della matrice $A = \begin{pmatrix} 1 & 1 & 3 & 1 & 0 \\ 3 & 2 & 3 & 1 & 1 \\ 2 & 1 & t & 0 & 1 \\ t & t & 2t + t^2 & t^2 & 0 \end{pmatrix}$ al variare di t in \mathbb{R} .

3.15. Si calcolino le inverse delle seguenti matrici:

$$A = \begin{pmatrix} 6 & -2 & -3 \\ -2 & 1 & 1 \\ -1 & 0 & 1 \end{pmatrix} \quad B = \begin{pmatrix} 2 & 2 & 3 \\ 1 & -1 & 0 \\ -1 & 2 & 1 \end{pmatrix} \quad C = \begin{pmatrix} 1 & a & a^2 & a^3 \\ 0 & 1 & a & a^2 \\ 0 & 0 & 1 & a \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

3.16. Si indichino con A e B gli spazi delle soluzioni dei seguenti sistemi lineari omogenei:

$$\begin{cases} 2x_1 - 3x_2 - x_4 = 0 \\ 3x_2 - 2x_3 + x_4 = 0 \\ x_1 + x_4 = 0 \end{cases} \quad \text{e} \quad \begin{cases} x_1 + 2x_2 - 3\lambda x_3 = 0 \\ (\lambda + 1)x_1 + 2x_2 - 3\lambda x_3 + x_4 = 0 \\ 2\lambda x_2 - 3x_3 + 2\lambda x_4 = 0 \end{cases}$$

Si determini la funzione d definita su \mathbb{R} da $d(\lambda) = \dim(A \cap B)$.

3.17. QUADRATI MAGICI. Un quadrato magico è una matrice quadrata, con termini interi positivi o nulli, tale che le somme dei termini su ogni riga, su ogni colonna e sulle due diagonali coincidano tutte. Determinare tutti i quadrati magici d'ordine 2 (sono solo quelli banali, con tutte le entrate uguali) e 3 (mostrare in particolare che il termine centrale della matrice è necessariamente un terzo della somma).

3.18. (IL RANGO PER RIGHE COINCIDE CON IL RANGO PER COLONNE) Siano C un campo e $A \in M_{m \times n}(C)$; allora indicheremo con $(A_{(1)}, \dots, A_{(n)})$ (risp. con $(A^{(1)}, \dots, A^{(m)})$) le colonne (risp.

le righe) di A ; quindi $A = (A_{(1)} \dots A_{(n)}) = \begin{pmatrix} A^{(1)} \\ \vdots \\ A^{(m)} \end{pmatrix}$.

Definiamo $\text{rkc}(A) = \dim\langle A_{(1)}, \dots, A_{(n)} \rangle$ e $\text{rkr}(A) = \dim\langle A^{(1)}, \dots, A^{(m)} \rangle$.

- (a) Sia $Y \in M_{n \times n}(C)$; si mostri che $\text{rkc}(AY) \leq \text{rkc}(A)$ e che $\text{rkr}(AY) \leq \text{rkr}(A)$;
- (b) Sia $Y \in GL_n(C)$; si mostri che $\text{rkc}(AY) = \text{rkc}(A)$ e che $\text{rkr}(AY) = \text{rkr}(A)$;
- (c) Sia $X \in M_{n \times n}(C)$; si mostri che $\text{rkc}(XA) \leq \text{rkc}(A)$ e che $\text{rkr}(XA) \leq \text{rkr}(A)$;
- (d) Sia $X \in GL_n(C)$; si mostri che $\text{rkc}(XA) = \text{rkc}(A)$ e che $\text{rkr}(XA) = \text{rkr}(A)$;
- (e) Si mostri che $\text{rkc}(A) = \text{rkr}(A)$.

3.19. Con le notazioni dell'esercizio precedente, sia

$$A = \begin{pmatrix} 1 & -1 & 2 \\ 2 & 1 & 1 \\ 3 & 1 & 2 \end{pmatrix} \in M_{3 \times 3}(\mathbb{R}).$$

- (a) Calcolare il rango di A ;
- (b) Trovare una matrice $Y \in GL_3(\mathbb{R})$, tale che $AY = (B_{(1)} B_{(2)} 0)$;
- (c) Trovare una matrice $X \in GL_3(\mathbb{R})$, tale che $XA = \begin{pmatrix} C^{(1)} \\ C^{(2)} \\ 0 \end{pmatrix}$;
- (d) Trovare X, Y come nei punti precedenti, e tali inoltre che $XAY = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}$.

m=3

Capitolo IV

Determinanti

La nozione di determinante per endomorfismi e per matrici quadrate è forse lo strumento più basilare ed importante del corso. È nozione ubiquitaria per i suoi significati geometrici.

0. Motivazioni.

0.1. RISOLUZIONI DI SISTEMI LINEARI QUADRATI. Nella risoluzione di un sistema lineare di due equazioni in due incognite

$$\begin{cases} a_{1,1}x_1 + a_{1,2}x_2 = b_1 \\ a_{2,1}x_1 + a_{2,2}x_2 = b_2 \end{cases}$$

troviamo, tramite metodi elementari e senza preoccuparci dei passaggi, le “soluzioni”

$$\begin{cases} x_1 = \frac{b_1a_{2,2} - b_2a_{2,1}}{a_{1,1}a_{2,2} - a_{1,2}a_{2,1}} \\ x_2 = \frac{a_{1,1}b_2 - a_{1,2}b_1}{a_{1,1}a_{2,2} - a_{1,2}a_{2,1}} \end{cases}$$

e quindi siamo portati a chiamare il termine $a_{1,1}a_{2,2} - a_{1,2}a_{2,1}$ il “determinante” del sistema: se esso non è nullo, la soluzione scritta è l’unica. Se invece è nullo, nei passaggi fatti si sono commesse delle imprecisioni, e il sistema può essere impossibile o indeterminato.

Analogamente, nel caso di sistemi di tre equazioni in tre incognite, ma con molti più calcoli, si possono scrivere le soluzioni come rapporti in cui al denominatore compare sempre lo stesso termine dipendente solo dai coefficienti delle equazioni e non dai termini noti.

Il concetto di determinante per una matrice quadrata permette di estendere queste osservazioni a tutti i sistemi di n equazioni in n incognite: esiste un termine (il determinante appunto) che dipende dai coefficienti delle equazioni e determina l’unicità o meno delle soluzioni a seconda che sia diverso da zero o no.

0.2. INDIPENDENZA LINEARE DI VETTORI. Dati n vettori in uno spazio vettoriale di dimensione n , sappiamo che essi formano una base se e solo se sono linearmente indipendenti. Decidere se sono linearmente indipendenti significa esattamente capire se la soluzione nulla è l’unica soluzione di un sistema lineare omogeneo di n equazioni in n incognite (i combinatori lineari). Dunque la discussione precedente ci dice che il concetto di determinante dà un test di indipendenza lineare.

0.3. CALCOLO DI EQUAZIONI CARTESIANE DI SOTTOSPAZI. La nozione di determinante permetterà anche un modo automatico e spesso utile per la ricerca di equazioni cartesiane di sottospazi, una volta che siano noti dei generatori, senza passare per le equazioni parametriche.

0.4. STUDIO DELLE FORME CANONICHE DELLE MATRICI. Lo studio delle forme canoniche delle matrici, nel prossimo capitolo, utilizzerà in modo essenziale la nozione di determinante per il calcolo del cosiddetto polinomio caratteristico associato alla matrice.

0.5. CALCOLO DI VOLUMI IN GEOMETRIA EUCLIDEA. Vedremo parlando di Geometria Euclidea che il calcolo del determinante è anche legato al calcolo del volume di certi oggetti geometrici (parallelepipedi e semplici n -dimensionali). Vedere quali proprietà debba soddisfare la nozione di volume motiva bene la prima definizione che daremo; se vogliamo ottenere una funzione $A(v_1, v_2)$ di due vettori v_1 e v_2 che misuri l’area del parallelogramma descritto, la funzione dovrà rispettare alcune regole ovvie:

- (1) se uno dei vettori è moltiplicato per uno scalare, l’area sarà moltiplicata per quello scalare: $A(\alpha v_1, v_2) = \alpha A(v_1, v_2) = A(v_1, \alpha v_2)$;
- (2) se nella prima variabile si sommano due vettori, il risultato è la somma delle aree: $A(v_1 + v'_1, v_2) = A(v_1, v_2) + A(v'_1, v_2)$ (idem per la seconda variabile); farsi un disegno per capire: si tratta di decomporre un parallelogramma in due aventi stesse “basi” e “altezze” dei due sommati;

- (3) se i due vettori sono dipendenti il risultato è nullo;
 (4) il quadrato unitario ha volume 1: $A(e_1, e_2) = 1$.

Di solito le prime due condizioni si riassumono dicendo che la funzione è bilineare (lineare in ogni variabile) e la terza dicendo che è alternante (perché se ne deduce che $A(v_1, v_2) = -A(v_2, v_1)$). Se si trova che esiste una unica tale funzione, essa dà la “giusta definizione” di area. Andiamo a formalizzare e studiare tali condizioni.

1. Determinanti e proprietà fondamentali.

In tutto il capitolo, il corpo C ha caratteristica diversa da 2.

1.1. DEFINIZIONE (FUNZIONI MULTILINEARI ALTERNANTI). Se V è uno spazio vettoriale sul corpo C , una funzione m -lineare a valori in un altro spazio vettoriale W su C è una applicazione

$$\delta : \underbrace{V \times \cdots \times V}_{m \text{ volte}} \longrightarrow W$$

che è lineare separatamente in ogni variabile, per qualsiasi fissati valori delle altre. Inoltre si dice alternante se si annulla ogni qual volta due argomenti sono uguali.

Se $W = C$ si parla di forme m -lineari, eventualmente alternanti. Si osservi che gli insiemi delle funzioni m -lineari e m -lineari alternanti formano in modo naturale spazi vettoriali su C .

1.1.1. La condizione di m -linearità della definizione si può esprimere dicendo che per ogni i e per ogni fissata scelta di vettori $v_j \in V$ per $j \neq i$, la funzione $v \mapsto \delta(v_1, \dots, v, \dots, v_m)$ (v in posizione i -esima) è lineare. Si osservi che non basta che tutte le composizioni $\delta \circ \iota_j$ siano applicazioni lineari ove $\iota_j : V \rightarrow V \times \cdots \times V$ è la j -esima inclusione per ogni $j = 1, \dots, m$.

1.1.2. PROPOSIZIONE (PROPRIETÀ FONDAMENTALI). Sia δ una applicazione m -lineare alternante. Allora:

- (1) δ si annulla non appena si applichi ad un insieme di m vettori linearmente dipendenti;
- (2) δ cambia di segno se si scambiano di posto due qualsiasi suoi argomenti.

DIMOSTRAZIONE. Possiamo supporre $v_m = \sum_{i=1}^{n-1} a_i v_i$; allora risulta

$$\begin{aligned} \delta(v_1, v_2, \dots, v_m) &= \delta(v_1, v_2, \dots, \sum_{i=1}^{n-1} a_i v_i) \\ &= \sum_{i=1}^{n-1} a_i \delta(v_1, v_2, \dots, v_i) = \sum_{i=1}^{n-1} a_i 0 = 0. \end{aligned}$$

Per il secondo punto, possiamo supporre di scambiare di posto v_1 e v_2 , e dal calcolo

$$0 = \delta(v_1 + v_2, v_1 + v_2, v_3, \dots, v_m) = \delta(v_1, v_2, v_3, \dots, v_m) + \delta(v_2, v_1, v_3, \dots, v_m)$$

abbiamo il risultato voluto (tenendo conto che il corpo ha caratteristica diversa da due). \square

1.1.3. PROBLEMA. Indichiamo con $m\text{-Lin}_C(V, W)$ e $m\text{-LinAlt}_C(V, W)$ gli spazi vettoriali delle forme m -lineari (risp. e alternanti), e sottoindentiamo W se $W = C$. Che dimensioni hanno questi spazi, in funzione delle dimensioni di V e di W ?

1.2. DEFINIZIONE-TEOREMA (DETERMINANTE DI APPLICAZIONI LINEARI). Sia V uno spazio vettoriale di dimensione n . Allora:

- (1) lo spazio delle forme n -lineari alternanti ha dimensione 1 su C , e dunque ogni suo elemento non nullo ne costituisce una base; scelta una base ordinata \mathcal{V} di V , l'applicazione $n\text{-LinAlt}_C(V) \rightarrow C$ che manda D in $D(\mathcal{V})$ è un isomorfismo di spazi vettoriali.
- (2) una forma n -lineare alternante non identicamente nulla si annulla se e solo se l'insieme costituito dagli argomenti è un insieme linearmente dipendente.

Detta D una qualunque forma n -lineare alternante non nulla, definiamo il determinante di una applicazione lineare come il rapporto

$$\det \varphi = \frac{D(\varphi v_1, \dots, \varphi v_n)}{D(v_1, \dots, v_n)}$$

ove v_1, \dots, v_n è una qualsiasi base di V ; questa definizione non dipende dalla base scelta. In particolare si ha che $\det(\text{id}_V) = 1$.

DIMOSTRAZIONE. Osserviamo innanzitutto che una applicazione n -lineare alternante D è determinata dal valore che assume in una base qualsiasi: se infatti v_1, \dots, v_n è una qualsiasi base di V , allora

$$\begin{aligned} D\left(\sum_{i_1=1}^n \alpha_{i_1,1} v_{i_1}, \dots, \sum_{i_n=1}^n \alpha_{i_n,n} v_{i_n}\right) &= \sum_{i_1=1}^n \cdots \sum_{i_n=1}^n \alpha_{i_1,1} \cdots \alpha_{i_n,n} D(v_{i_1}, \dots, v_{i_n}) \\ &= \sum_{\sigma \in \mathfrak{S}_n} \text{sgn}(\sigma) \alpha_{\sigma(1),1} \cdots \alpha_{\sigma(n),n} D(v_1, \dots, v_n) \end{aligned}$$

ove \mathfrak{S}_n indica l'insieme delle permutazioni sull'insieme $\{1, \dots, n\}$ e $\text{sgn}(\sigma)$ è il segno della permutazione σ (uguale a 1 se σ è composizione di un numero pari di scambi, -1 se σ è composizione di un numero dispari di scambi). Si osservi che nel primo passaggio abbiamo usato la multilinearità, nel secondo abbiamo usato la proprietà di alternanza.

Da questo deduciamo subito che se D e D' sono due applicazioni n -lineari alternanti non nulle, allora $D = kD'$ ove $k = D(v_1, \dots, v_n)/D'(v_1, \dots, v_n) \in C$. Rimane da vedere che in effetti non tutte le applicazioni n -lineari alternanti sono nulle, ma questo è immediato osservando che definendo $D(v_1, \dots, v_n) = 1$ e usando la formula precedente per definire l'applicazione D , otteniamo una applicazione n -lineare alternante non nulla.

D'altra parte è chiaro che ogni forma di questo tipo si annulla su un insieme di n vettori linearmente dipendenti; viceversa, se si annulla su una base, allora per la formula precedente dev'essere l'applicazione nulla.

Dimostriamo ora che la definizione di determinante non dipende dalla base scelta: se v'_1, \dots, v'_n è un'altra base di V , abbiamo $(v'_1, \dots, v'_n) = (v_1, \dots, v_n)H$ ove H è una matrice invertibile, di conseguenza abbiamo

$$\frac{D(\varphi v'_1, \dots, \varphi v'_n)}{D(v'_1, \dots, v'_n)} = \frac{D((\varphi v_1, \dots, \varphi v_n)H)}{D((v_1, \dots, v_n)H)} = \frac{hD(\varphi v_1, \dots, \varphi v_n)}{hD(v_1, \dots, v_n)}$$

ove $h = \sum_{\sigma \in \mathfrak{S}_n} \text{sgn}(\sigma) h_{\sigma(1),1} \cdots h_{\sigma(n),n}$ è una costante non nulla. In effetti questa verifica è inutile, se si ricorda che il rapporto che definisce \det è il rapporto tra due funzioni n -lineari alternanti non nulle (D e una sua modificata tramite una trasformazione H invertibile). \square

1.2.1. Segue subito dal risultato precedente che il determinante di una applicazione φ è non nullo se e solo se φ è un isomorfismo.

1.3. DEFINIZIONE-TEOREMA (DETERMINANTE DI MATRICI). *Detta D una qualunque forma n -lineare alternante non nulla di $V_n(C)$, definiamo il determinante di una matrice $A \in M_n(C)$ come il determinante della applicazione lineare di $V_n(C)$ in sé che è rappresentata dalla matrice A nella base canonica. Il determinante di A è dunque l'elemento di C dato da*

$$\det A = |A| := \sum_{\sigma \in \mathfrak{S}_n} \text{sgn}(\sigma) \prod_{i=1}^n a_{i,\sigma(i)}$$

ove \mathfrak{S}_n indica l'insieme delle permutazioni sull'insieme $\{1, \dots, n\}$. In particolare si ha che $\det \mathbb{I}_n = 1$.

DIMOSTRAZIONE. È nascosta nella dimostrazione del precedente teorema. \square

1.3.1. Segue subito dal risultato precedente che il determinante di una matrice A è non nullo se e solo se A è invertibile. In particolare n vettori formano una base di V (ovvero sono linearmente indipendenti) se e solo se il determinante della matrice che ha come colonne le loro coordinate (in una base qualsiasi) è non nullo.

1.3.2. Si osservi che il determinante di una matrice può essere visto come un polinomio omogeneo di grado (totale) n nelle entrate della matrice, ed esso è di primo grado rispetto a ciascuna entrata.

In quanto polinomio nelle n^2 variabili $a_{i,j}$, il determinante è irriducibile, cioè non può essere scritto come prodotto di due polinomi di grado strettamente minore.

1.4. TEOREMA (DI BINET). Le applicazioni $\det : \text{End}_C(V) \rightarrow C$ e $\det : M_n(C) \rightarrow C$ rispettano identità e prodotto, cioè:

- (1) $\det(\text{id}_V) = 1$ e $\det \mathbb{I}_n = 1$;
- (2) $\det(\psi \circ \varphi) = \det(\psi) \det(\varphi)$ per ogni $\varphi, \psi \in \text{End}_C(V)$ e $\det(AB) = \det(A) \det(B)$ per ogni $A, B \in M_n(C)$.

DIMOSTRAZIONE. Il primo punto si è già visto, ed è ovvio dalla definizione. Per il secondo punto, se uno dei due determinanti è nullo, il risultato è chiaro. Altrimenti φ e ψ sono isomorfismi e possiamo calcolare, usando qualsiasi forma multilineare alternante D e qualsiasi base di V ,

$$\begin{aligned} \det(\psi \circ \varphi) &= \frac{D(\psi \circ \varphi v_1, \dots, \psi \circ \varphi v_n)}{D(v_1, \dots, v_n)} \\ &= \frac{D(\psi \circ \varphi v_1, \dots, \psi \circ \varphi v_n)}{D(\varphi v_1, \dots, \varphi v_n)} \frac{D(\varphi v_1, \dots, \varphi v_n)}{D(v_1, \dots, v_n)} \\ &= \det(\psi) \det(\varphi) \end{aligned}$$

poiché il calcolo del determinante non dipende dalla base scelta dello spazio. \square

1.4.1. PROBLEMA. Si osservi invece che la somma di matrici non è rispettata dal determinante, cioè in generale $\det(A+B) \neq \det(A) + \det(B)$ (farsi degli esempi).

Mostrare che $\det(-A) = (-1)^n \det(A)$ se $A \in M_n(C)$.

1.5. TEOREMA (DETERMINANTE DELLA TRASPOSTA). Se $\varphi \in \text{End}_C(V)$ allora abbiamo $\varphi^* \in \text{End}_C(V^*)$ e risulta $\det(\varphi^*) = \det \varphi$. Per ogni matrice $A \in M_n(C)$ si ha $\det(A^t) = \det A$.

DIMOSTRAZIONE. La prima asserzione segue dalla seconda, che è evidente:

$$\det A^t = \sum_{\sigma \in \mathfrak{S}_n} \text{sgn}(\sigma) \prod_{i=1}^n a_{\sigma(i), i} = \sum_{\sigma \in \mathfrak{S}_n} \text{sgn}(\sigma) \prod_{j=1}^n a_{j, \sigma^{-1}(j)} = \sum_{\pi \in \mathfrak{S}_n} \text{sgn}(\pi) \prod_{j=1}^n a_{j, \pi(j)} = \det A .$$

\square

2. Sviluppi di Laplace e matrici inverse.

2.1. TEOREMA (SVILUPPI DI LAPLACE). Il determinante di una matrice $A \in M_n(C)$ si calcola mediante gli sviluppi di Laplace per riga o colonna, riconducendosi a determinanti di matrici in $M_{n-1}(C)$:

$$\begin{aligned} |A| &= \sum_{j=1}^n (-1)^{i+j} a_{i,j} |A_{i,j}| \quad (\text{sviluppo secondo la } i\text{-esima riga}) \\ &= \sum_{i=1}^n (-1)^{i+j} a_{i,j} |A_{i,j}| \quad (\text{sviluppo secondo la } j\text{-esima colonna}) \end{aligned}$$

ove $A_{i,j} \in M_{n-1}$ è la matrice che si ottiene da A eliminando la i -esima riga e la j -esima colonna. I termini $(-1)^{i+j} |A_{i,j}|$ si chiamano i complementi algebrici di posto (j, i) della matrice A .

DIMOSTRAZIONE. Si tratta di vedere che le funzioni definite dalle formule di Laplace valgono 1 sulla matrice identica, e sono n -lineari alternanti sulle colonne della matrice. \square

2.1.1. ANNULLAMENTI O SVILUPPI (CON COFATTORI) ALIENI. Dal risultato precedente segue subito che

$$\sum_{j=1}^n (-1)^{i+j} a_{k,j} |A_{i,j}| = 0 \quad (\text{risp.} \quad \sum_{i=1}^n (-1)^{i+j} a_{i,k} |A_{i,j}| = 0)$$

per ogni $k \neq i$ (risp. $k \neq j$), poiché si tratta di sviluppi di Laplace di matrici con due righe (risp. colonne) uguali.

2.1.2. DEFINIZIONE-TEOREMA (MATRICE DEI COMPLEMENTI ALGEBRICI). Data una matrice quadrata A , si dice complemento algebrico o minore segnato di posto i, j e si indica con $a_{i,j}^c$ il determinante $(-1)^{i+j} |A_{j,i}|$. la matrice dei complementi algebrici A^c è la matrice $(a_{i,j}^c)$. Vale la relazione

$$AA^c = A^c A = |A| \mathbb{I}_n .$$

Inoltre abbiamo $\mathbb{I}_n^c = \mathbb{I}_n$ e $(AB)^c = B^c A^c$.

DIMOSTRAZIONE. Segue subito dagli sviluppi di Laplace (e dal fatto che matrici con due righe o due colonne uguali hanno determinante nullo). L'ultima asserzione segue dal confronto tra $(AB)(AB)^c = |AB|\mathbb{I}_n$ e $ABB^c A^c = |B|AA^c = |A||B|\mathbb{I}_n$. \square

2.2. TEOREMA (INVERSA). Una matrice è invertibile se e solo se il suo determinante è diverso da zero. Se $A \in M_n(C)$ è invertibile la sua matrice inversa si indica con A^{-1} e si calcola tramite:

$$A^{-1} = \frac{1}{|A|} A^c = \frac{1}{|A|} \left((-1)^{i+j} |A_{j,i}| \right)_{\substack{i=1,\dots,n \\ j=1,\dots,n}}.$$

DIMOSTRAZIONE. Facile conseguenza del risultato precedente. \square

2.3. TEOREMA (CAUCHY). Il determinante della matrice dei complementi algebrici di A è dato dalla potenza $n-1$ -esima del determinante di A , cioè $|A^c| = |A|^{n-1}$.

DIMOSTRAZIONE. Se $|A| = 0$ il risultato è ovvio, poiché anche $|A^c| = 0$ (si noti per inciso che il rango di A^c è $n, 1, 0$ a seconda che il rango di A sia $n, n-1$, minore di $n-1$; altrimenti basta calcolare il determinante della uguaglianza $AA^c = |A|\mathbb{I}_n$, da cui $|A||A^c| = |A|^n$). \square

2.3.1. OSSERVAZIONE. Vale che $A^{cc} = |A|^{n-2}A$. Si ottiene per esempio confrontando $AA^c = |A|\mathbb{I}_n$ con $A^c A^{cc} = |A^c|\mathbb{I}_n$.

2.4. PROPOSIZIONE (GRUPPO GENERALE LINEARE). Il gruppo generale lineare $GL(n, C)$ si caratterizza come il sottinsieme di $M_n(C)$ delle matrici di determinante non nullo. Il determinante si restringe ad un morfismo di gruppi

$$\det : GL_n(C) \longrightarrow C^\times$$

tra il gruppo delle matrici invertibili con l'operazione di prodotto e il gruppo degli elementi non nulli di C con l'operazione di prodotto.

DIMOSTRAZIONE. Ovvio dalle definizioni e dai risultati precedenti. \square

2.4.1. In particolare abbiamo $\det(A^{-1}) = \det(A)^{-1}$.

2.4.2. L'applicazione $\det : GL_n(C) \longrightarrow C^\times$ è suriettiva; è vero che esistono delle inverse a destra? Trovarne qualcuna la cui immagine sia contenuta nel sottogruppo delle matrici diagonali. È possibile trovare una inversa a destra la cui immagine sia contenuta nel sottogruppo delle matrici scalari?

2.4.3. Le matrici di determinante uguale ad 1 formano un sottogruppo normale di $GL_n(C)$. È vero che ogni matrice invertibile si può scrivere come prodotto di una matrice scalare (risp. diagonale) e di una matrice di determinante 1?

♠♠ **2.5. SVILUPPI DI LAPLACE GENERALIZZATI.** Il calcolo del determinante tramite sviluppo di Laplace può essere generalizzato nel modo seguente: fissate r righe (risp. r colonne), invece di una sola, si può calcolare il determinante come somma di prodotti dei determinanti delle sottomatrici quadrate di quelle righe (risp. colonne) per il determinante della sottomatrice "complementare" (che si ottiene sopprimendo quelle righe e quelle colonne). La parte sofisticata della formula è nel tener conto dei segni con cui tali prodotti devono essere conteggiati.

2.5.1. TEOREMA (SVILUPPI DI LAPLACE GENERALIZZATI). Sia K sottinsieme (ordinato) di $\{1, 2, \dots, n\}$ e indichiamo con $K' = \{1, 2, \dots, n\} \setminus K$ il complementare (ordinato). Sia $\varepsilon(K, K')$ il segno della permutazione che manda i nell' i -esimo elemento della lista (K, K') . Allora

$$\det A = \varepsilon(K, K') \sum_H \varepsilon(H, H') \det A_{H,K} \det A_{H',K'}$$

dove la sommatoria è estesa a tutti i sottinsiemi H di $\{1, 2, \dots, n\}$ aventi la stessa cardinalità di K , H' è l'insieme complementare, $A_{H,K}$ indica la sottomatrice quadrata che si ottiene selezionando le righe (risp. le colonne) i cui indici sono in H (risp. in K), e $A_{H',K'}$ indica la sottomatrice quadrata che si ottiene eliminando le righe (risp. le colonne) i cui indici sono in H (risp. in K).

DIMOSTRAZIONE. Si tratta di vedere che le funzioni definite dalle formule di Laplace valgono 1 sulla matrice identica, e sono n -lineari alternanti sulle colonne della matrice. \square

ESEMPLI. **2.5.2.** Se $K = \{i\}$ è di cardinalità uno, oppure $K = \{1, 2, \dots, n\} \setminus \{i\}$ è di cardinalità $n - 1$, si tratta dello sviluppo di Laplace secondo la i -esima colonna.

2.5.3. Una generalizzazione analoga può essere fatta per lo sviluppo di Laplace per righe (invece che per colonne), e si può dedurre dal teorema scritto passando alla matrice trasposta.

2.5.4. Se $K = \{1, 2\}$ e $n = 4$?

2.5.5. Se $K = \{1, 2\}$ e $n = 5$?

2.5.6. ANNULAMENTI O SVILUPPI (CON COFATTORI) ALIENI. Si osservi anche che, analogamente al caso di “sviluppi di Laplace su una riga (o una colonna) sbagliata” si ha che

$$\sum_H \varepsilon(H, H') \det A_{H,K} \det A_{H',L} = 0$$

per ogni $L \subseteq \{1, 2, \dots, n\}$ della stessa cardinalità di K' ma diverso da K' .

3. Sviluppi pivotali.

Poiché il determinante di una matrice è funzione multilineare in ogni riga o colonna, è possibile sfruttare il metodo di riduzione di Gauss per semplificare la forma della matrice di cui calcolare il determinante, per esempio portando la matrice alla forma triangolare. Questo tipo di procedimento dà luogo a formule interessanti, dette sviluppi pivotali.

3.1. DETERMINANTE DELLE OPERAZIONI ELEMENTARI. Le matrici elementari che si usano nella riduzione hanno determinanti facilmente calcolabili: abbiamo $\det S(i, j) = -1$, $\det H(i, j, \alpha) = 1$ e $\det H(i, \alpha) = \alpha$.

In particolare, sommare ad una riga un qualsiasi multiplo di un'altra riga non altera il determinante, mentre lo scambio di due righe cambia di segno il determinante.

♠ **3.2.** Le operazioni elementari sulle righe possono essere usate per esprimere un determinante $n \times n$ in termini di un determinante $(n-2) \times (n-2)$ e di un determinante 2×2 le cui entrate sono determinanti $(n-1) \times (n-1)$. Prima di dare un enunciato generale, proponiamo i casi di determinanti di ordine 3, 4 e 5 quali esempi.

3.2.1. DETERMINANTI D'ORDINE 3. Dopo aver moltiplicato la seconda e la terza riga per l'elemento a_1 di posto 1, 1, supposto diverso da zero, procediamo con la riduzione per righe:

$$\begin{pmatrix} a_1 & b_1 & c_1 \\ a_1 a_2 & a_1 b_2 & a_1 c_2 \\ a_1 a_3 & a_1 b_3 & a_1 c_3 \end{pmatrix} \xrightarrow[\text{III}-a_3 I]{\text{II}-a_2 I} \begin{pmatrix} a_1 & b_1 & c_1 \\ 0 & a_1 b_2 - a_2 b_1 & a_1 c_2 - a_2 c_1 \\ 0 & a_1 b_3 - a_3 b_1 & a_1 c_3 - a_3 c_1 \end{pmatrix}$$

da cui si ricava subito che

$$a_1 \begin{vmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{vmatrix} = \begin{vmatrix} a_1 & b_1 \\ a_2 & b_2 \end{vmatrix} \begin{vmatrix} a_1 & c_1 \\ a_2 & c_2 \end{vmatrix} - \begin{vmatrix} a_1 & b_1 \\ a_3 & b_3 \end{vmatrix} \begin{vmatrix} a_1 & c_1 \\ a_3 & c_3 \end{vmatrix}$$

(sviluppo rispetto al pivot a_1).

3.2.2. DETERMINANTI D'ORDINE 4. Dopo aver moltiplicato la seconda, la terza e la quarta riga per l'elemento a_1 di posto 1, 1, supposto diverso da zero, procediamo con la riduzione per righe:

$$\begin{pmatrix} a_1 & b_1 & c_1 & d_1 \\ a_1 a_2 & a_1 b_2 & a_1 c_2 & a_1 d_2 \\ a_1 a_3 & a_1 b_3 & a_1 c_3 & a_1 d_3 \\ a_1 a_4 & a_1 b_4 & a_1 c_4 & a_1 d_4 \end{pmatrix} \xrightarrow[\text{IV}-a_4 I]{\text{II}-a_2 I, \text{III}-a_3 I} \begin{pmatrix} a_1 & b_1 & c_1 & d_1 \\ 0 & a_1 b_2 - a_2 b_1 & a_1 c_2 - a_2 c_1 & a_1 d_2 - a_2 d_1 \\ 0 & a_1 b_3 - a_3 b_1 & a_1 c_3 - a_3 c_1 & a_1 d_3 - a_3 d_1 \\ 0 & a_1 b_4 - a_4 b_1 & a_1 c_4 - a_4 c_1 & a_1 d_4 - a_4 d_1 \end{pmatrix}$$

da cui si ricava subito che

$$a_1^2 \begin{vmatrix} a_1 & b_1 & c_1 & d_1 \\ a_2 & b_2 & c_2 & d_2 \\ a_3 & b_3 & c_3 & d_3 \\ a_4 & b_4 & c_4 & d_4 \end{vmatrix} = \begin{vmatrix} a_1 & b_1 \\ a_2 & b_2 \end{vmatrix} \begin{vmatrix} a_1 & c_1 \\ a_2 & c_2 \end{vmatrix} \begin{vmatrix} a_1 & d_1 \\ a_2 & d_2 \end{vmatrix} - \begin{vmatrix} a_1 & b_1 \\ a_3 & b_3 \end{vmatrix} \begin{vmatrix} a_1 & c_1 \\ a_3 & c_3 \end{vmatrix} \begin{vmatrix} a_1 & d_1 \\ a_3 & d_3 \end{vmatrix} + \begin{vmatrix} a_1 & b_1 \\ a_4 & b_4 \end{vmatrix} \begin{vmatrix} a_1 & c_1 \\ a_4 & c_4 \end{vmatrix} \begin{vmatrix} a_1 & d_1 \\ a_4 & d_4 \end{vmatrix}$$

(sviluppo rispetto al pivot a_1); usando poi lo sviluppo pivotale del determinante a destra rispetto al primo termine, ed interpretando il risultato in termini di uno sviluppo pivotale rispetto ad a_1 risulta che

$$\begin{vmatrix} a_1 & b_1 \\ a_2 & b_2 \end{vmatrix} \begin{vmatrix} a_1 & b_1 & c_1 & d_1 \\ a_2 & b_2 & c_2 & d_2 \\ a_3 & b_3 & c_3 & d_3 \\ a_4 & b_4 & c_4 & d_4 \end{vmatrix} = \begin{vmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \\ a_4 & b_4 & c_4 \end{vmatrix} \begin{vmatrix} a_1 & b_1 & d_1 \\ a_2 & b_2 & d_2 \\ a_3 & b_3 & d_3 \\ a_4 & b_4 & d_4 \end{vmatrix}$$

sotto ipotesi che il primo determinante scritto sia non nullo.

3.2.3. DETERMINANTI D'ORDINE 5. Un analogo procedimento (riduzione di Gauss per quattro righe, poi uso degli sviluppi pivotali nei casi d'ordine 4 e 3), porta alla formula

$$\begin{vmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{vmatrix} \begin{vmatrix} a_1 & b_1 & c_1 & d_1 & e_1 \\ a_2 & b_2 & c_2 & d_2 & e_2 \\ a_3 & b_3 & c_3 & d_3 & e_3 \\ a_4 & b_4 & c_4 & d_4 & e_4 \\ a_5 & b_5 & c_5 & d_5 & e_5 \end{vmatrix} = \begin{vmatrix} a_1 & b_1 & c_1 & d_1 \\ a_2 & b_2 & c_2 & d_2 \\ a_3 & b_3 & c_3 & d_3 \\ a_4 & b_4 & c_4 & d_4 \end{vmatrix} \begin{vmatrix} a_1 & b_1 & c_1 & e_1 \\ a_2 & b_2 & c_2 & e_2 \\ a_3 & b_3 & c_3 & e_3 \\ a_4 & b_4 & c_4 & e_4 \end{vmatrix}$$

sotto ipotesi che il primo determinante scritto sia non nullo.

♠♠ **3.3. TEOREMA (SVILUPPI PIVOTALI).** Data una matrice quadrata A d'ordine $n \geq 3$, e indici $1 \leq i_1 < \dots < i_r \leq n$ e $1 \leq j_1 < \dots < j_r \leq n$, indichiamo con $A_{(j_1, \dots, j_r)}^{(i_1, \dots, i_r)}$ la sottomatrice quadrata d'ordine r che si ottiene scegliendo gli elementi di A il cui indice di riga appartiene a $\{i_1, \dots, i_r\}$ e il cui indice di colonna appartiene a $\{j_1, \dots, j_r\}$; indichiamo con $A_{(j_1, \dots, j_r)}^{(\hat{i}_1, \dots, \hat{i}_r)}$ la sottomatrice quadrata d'ordine $n - r$ che si ottiene sopprimendo le righe il cui indice appartiene a $\{i_1, \dots, i_r\}$ e le colonne il cui indice appartiene a $\{j_1, \dots, j_r\}$. Allora risulta che

$$\left| A_{(j_1, j_2)}^{(\hat{i}_1, \hat{i}_2)} \right| |A| = \begin{vmatrix} \left| A_{(j_1)}^{(\hat{i}_1)} \right| & \left| A_{(j_2)}^{(\hat{i}_1)} \right| \\ \left| A_{(j_1)}^{(\hat{i}_2)} \right| & \left| A_{(j_2)}^{(\hat{i}_2)} \right| \end{vmatrix}$$

sotto ipotesi che il primo determinante sia non nullo.

DIMOSTRAZIONE. Induzione sull'ordine del determinante. Si può supporre, scambiando righe e colonne, che $i_1 = j_1 = n - 1$ e $i_2 = j_2 = n$. Si usa il procedimento di Gauss per eliminare i termini della prima colonna, ottenendo una espressione del tipo

$$\frac{1}{a_1^{n-1}} |A| = \begin{vmatrix} \left| A_{(1,2)}^{(1,2)} \right| & \left| A_{(1,3)}^{(1,2)} \right| & \dots & \left| A_{(1,n)}^{(1,2)} \right| \\ \left| A_{(1,2)}^{(1,3)} \right| & \left| A_{(1,3)}^{(1,3)} \right| & \dots & \left| A_{(1,n)}^{(1,3)} \right| \\ \vdots & \vdots & \ddots & \vdots \\ \left| A_{(1,2)}^{(1,n)} \right| & \left| A_{(1,3)}^{(1,n)} \right| & \dots & \left| A_{(1,n)}^{(1,n)} \right| \end{vmatrix}$$

Detta B la matrice d'ordine $n - 1$ il cui determinante sta sul lato destro, abbiamo (usando lo sviluppo pivotale dell'ordine precedente) che

$$\left| B_{(\widehat{n-2}, \widehat{n-1})}^{(\widehat{n-2}, \widehat{n-1})} \right| |B| = \begin{vmatrix} \left| B_{(\widehat{n-2})}^{(\widehat{n-2})} \right| & \left| B_{(\widehat{n-1})}^{(\widehat{n-2})} \right| \\ \left| B_{(\widehat{n-2})}^{(\widehat{n-1})} \right| & \left| B_{(\widehat{n-1})}^{(\widehat{n-1})} \right| \end{vmatrix}$$

e d'altra parte, usando le formule intermedie date dagli sviluppi pivotali rispetto al primo termine degli ordini precedenti, abbiamo che

$$\frac{1}{a_1^{n-3}} \left| A_{\widehat{(n-1, n)}}^{\widehat{(n-1, n)}} \right| = \left| B_{\widehat{(n-2, n-1)}}^{\widehat{(n-2, n-1)}} \right|$$

e

$$\frac{1}{a_1^{n-2}} \left| A_{\widehat{(j)}}^{\widehat{(i)}} \right| = \left| B_{\widehat{(j-1)}}^{\widehat{(i-1)}} \right| \quad (\text{da usare per } i, j = n-1, n).$$

Sostituendo nella prima espressione trovata otteniamo il risultato voluto. \square

4. Casi notevoli.

4.1. MATRICI TRIANGOLARI. Se la matrice A è triangolare (inferiore se $a_{i,j}=0$ per $i > j$; superiore se $a_{i,j}=0$ per $i < j$) allora il determinante è il prodotto degli elementi in diagonale: $\det A = \prod_{i=1}^n a_{i,i}$. È una conseguenza immediata del calcolo secondo Laplace, ma anche della definizione stessa. In particolare, una matrice triangolare è invertibile se e solo se i suoi elementi diagonali sono tutti non nulli. Verificare che, allora, anche la matrice inversa è triangolare.

4.2. MATRICI A BLOCCHI. Se la matrice è "a blocchi":

$$\det \begin{pmatrix} A & B \\ 0 & D \end{pmatrix} = \det(A) \det(D) = \det \begin{pmatrix} A & 0 \\ C & D \end{pmatrix},$$

con A e D matrici quadrate. Anche questo segue subito dalla definizione (ogni addendo del determinante che coinvolge un elemento di B o di C coinvolge anche un fattore nullo), come pure da un facile argomento usando la riduzione di Gauss. Si generalizzi per più blocchi.

4.3. ALTERNANTI. In generale si dicono alternanti i polinomi di più variabili che cambiano di segno quando "si scambino tra loro" due qualsiasi delle variabili. È chiaro che, dati n polinomi $f_1(x), \dots, f_n(x)$ in una variabile e n termini x_1, \dots, x_n , i determinanti di matrici del tipo $(f_i(x_j))$ sono polinomi alternanti delle variabili x_j , e per questo vengono anch'essi detti alternanti.

I più semplici alternanti, ed in effetti quelli importanti, sono quelli di Vandermonde e le loro generalizzazioni.

4.3.1. MATRICI E DETERMINANTI DI VANDERMONDE. Si dice matrice di Vandermonde di termini x_0, x_1, \dots, x_n e si indica con $VdM(x_0, x_1, \dots, x_n)$ la matrice d'ordine $n+1$ la cui i -esima colonna è formata dalle potenze (da 0 a n) del termine x_i . Per il determinante, abbiamo

$$vdm(x_0, x_1, \dots, x_n) := \det \begin{pmatrix} 1 & 1 & \dots & 1 \\ x_0 & x_1 & \dots & x_n \\ x_0^2 & x_1^2 & \dots & x_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ x_0^n & x_1^n & \dots & x_n^n \end{pmatrix} = \prod_{0 \leq i < j \leq n} (x_j - x_i);$$

il calcolo può essere fatto per induzione su n (conviene effettuare operazioni elementari sulle righe, sottraendo ad ogni riga la precedente moltiplicata per x_0 ; si ottengono dei fattori $(x_i - x_0)$ da raccogliere e rimane una matrice dello stesso tipo e di ordine diminuito).

In particolare si vede che una matrice di Vandermonde è invertibile se e solo se $x_i \neq x_j$ per ogni $i \neq j$; in questo caso, possiamo calcolarne la matrice inversa usando la seguente osservazione: il polinomio nelle X dato da

$$(X-a_1)(X-a_2) \dots (X-a_n) = X^n - p_1 X^{n-1} + p_2 X^{n-2} + \dots + (-1)^i p_i X^{n-i} + \dots + (-1)^{n-1} p_{n-1} X + (-1)^n p_n$$

si annulla per $X = a_1, a_2, \dots, a_n$ (i termini p_ℓ sono i polinomi simmetrici elementari nei valori a_1, a_2, \dots, a_n : p_ℓ è la somma di tutti i possibili prodotti di ℓ valori distinti tra gli a_i). Usando questo fatto si vede che la matrice inversa della matrice di Vandermonde ha come i -esima riga i polinomi simmetrici p_ℓ calcolati nelle variabili x_j con $j \neq i$, moltiplicata per un opportuno coefficiente (quale?).

4.3.2. Nel caso speciale in cui $x_i = x^i$ ($i = 1, \dots, n$) si ottiene che il determinante è

$$VdM(1, x, x^2, \dots, x^n) = x^{\frac{n(n^2-1)}{6}} (x-1)^n (x^2-1)^{n-1} (x^3-1)^{n-2} \dots (x^{n-1}-1)^2 (x^n-1).$$

4.3.3. Un caso particolarmente interessante sono le matrici di Vandermonde del tipo $\Omega_n = \frac{1}{\sqrt{n}} VdM(1, \omega, \omega^2, \dots, \omega^{n-1})$ nel caso che $\omega \in \mathbb{C}$ sia una radice primitiva n -esima dell'unità. In tal caso si tratta di matrici simmetriche, e la matrice inversa è la (trasposta) coniugata. I primi esempi sono:

$$\Omega_2 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad \Omega_3 = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega^4 \end{pmatrix} = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 1 & 1 \\ 1 & \omega & \bar{\omega} \\ 1 & \bar{\omega} & \omega \end{pmatrix},$$

ove $\omega = e^{\frac{2\pi i}{3}}, e^{\frac{4\pi i}{3}}$,

$$\Omega_4 = \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & \omega & \omega^2 & \omega^3 \\ 1 & \omega^2 & \omega^4 & \omega^6 \\ 1 & \omega^3 & \omega^6 & \omega^9 \end{pmatrix} = \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & \omega & -1 & \bar{\omega} \\ 1 & -1 & 1 & -1 \\ 1 & \bar{\omega} & -1 & \omega \end{pmatrix},$$

ove $\omega = \pm i$,

$$\Omega_5 = \frac{1}{\sqrt{5}} \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & \omega & \omega^2 & \omega^3 & \omega^4 \\ 1 & \omega^2 & \omega^4 & \omega^6 & \omega^8 \\ 1 & \omega^3 & \omega^6 & \omega^9 & \omega^{12} \\ 1 & \omega^4 & \omega^8 & \omega^{12} & \omega^{16} \end{pmatrix} = \frac{1}{\sqrt{5}} \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & \omega & \omega^2 & \bar{\omega}^2 & \bar{\omega} \\ 1 & \omega^2 & \bar{\omega} & \omega & \bar{\omega}^2 \\ 1 & \bar{\omega}^2 & \omega & \bar{\omega} & \omega^2 \\ 1 & \bar{\omega} & \bar{\omega}^2 & \omega^2 & \omega \end{pmatrix}$$

ove $\omega = e^{\frac{2\pi i}{5}}, e^{\frac{4\pi i}{5}}, e^{\frac{6\pi i}{5}}, e^{\frac{8\pi i}{5}}$. Quali sono i determinanti di queste matrici?

♠ **4.3.4.** APPLICAZIONE ALLE FORMULE DI CARDANO. Consideriamo l'equazione standard di terzo grado $x^3 + px + q = 0$, e sia $X = \text{diag}(x_1, x_2, x_3)$ la matrice diagonale avente in diagonale le soluzioni (si noti che $\text{tr} X = x_1 + x_2 + x_3 = 0$). Allora risulta $X^3 + pX + q\mathbb{I}_3 = \mathbb{O}_3$. Se consideriamo la matrice $\bar{\Omega}_3 X \Omega_3 = \alpha \Sigma + \beta \Sigma^2$ ove $\Sigma = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$, abbiamo che $\sqrt{3}(0, \beta, \alpha) = (x_1, x_2, x_3) \bar{\Omega}_3$ da cui $(x_1, x_2, x_3) = (0, \beta, \alpha) \Omega_3 = (\beta, \alpha) \begin{pmatrix} 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{pmatrix}$ (principio di sovrapposizione). I valori di α e β possono essere ricavati dal sistema (di grado sei, ma bicubico) che si ottiene sostituendo $\bar{\Omega}_3 X \Omega_3 = \alpha \Sigma + \beta \Sigma^2$ nell'equazione $(\bar{\Omega}_3 X \Omega_3)^3 + p(\bar{\Omega}_3 X \Omega_3) + q\mathbb{I}_3 = \mathbb{O}_3$.

♠ **4.3.5.** APPLICAZIONE ALLE FORMULE DI FERRARI. Consideriamo l'equazione standard di quarto grado $x^4 + px^2 + qx + r = 0$, e sia $X = \text{diag}(x_1, x_2, x_3, x_4)$ la matrice diagonale avente in diagonale le soluzioni (si noti che $\text{tr} X = x_1 + x_2 + x_3 + x_4 = 0$). Allora risulta $X^4 + pX^2 + qX + r\mathbb{I}_4 = \mathbb{O}_4$. Se consideriamo la matrice $\bar{\Omega}_4 X \Omega_4 = \alpha \Sigma + \beta \Sigma^2 + \gamma \Sigma^3$ ove $\Sigma = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}$, abbiamo che $2(0, \gamma, \beta, \alpha) = (x_1, x_2, x_3, x_4) \bar{\Omega}_4$ da cui $(x_1, x_2, x_3, x_4) = (0, \gamma, \beta, \alpha) \Omega_4 = (\gamma, \beta, \alpha) \begin{pmatrix} 1 & \omega & \omega^2 & \omega^3 \\ 1 & \omega^2 & 1 & \omega^2 \\ 1 & \omega^3 & \omega^2 & \omega \end{pmatrix}$ (principio di sovrapposizione). I valori di α , β e γ possono essere ricavati dal sistema (di grado alto, e di soluzione difficile, ma possibile) che si ottiene sostituendo $\bar{\Omega}_4 X \Omega_4 = \alpha \Sigma + \beta \Sigma^2 + \gamma \Sigma^3$ nell'equazione $(\bar{\Omega}_4 X \Omega_4)^4 + p(\bar{\Omega}_4 X \Omega_4)^2 + q(\bar{\Omega}_4 X \Omega_4) + r\mathbb{I}_4 = \mathbb{O}_4$.

♠♠ **4.3.6.** MATRICI E DETERMINANTI DI VANDERMONDE GENERALIZZATI. Le matrici di Vandermonde generalizzate $VdM(x, \alpha) = VdM(x_0, \dots, x_n; \alpha_0, \dots, \alpha_n)$ di variabili x_0, \dots, x_n ed esponenti $\alpha_0 \leq \dots \leq \alpha_n$ sono le matrici definite da $VdM(x, \alpha) = (x_i^{\alpha_j})$. È chiaro che il loro determinante si annulla se due valori o due esponenti coincidono. Osserviamo che $VdM(x_0, \dots, x_n) = VdM(x_0, \dots, x_n; 0, 1, \dots, n)$. Inoltre l'ovvia relazione

$$vdm(x_0, \dots, x_n; \alpha_0, \alpha_1, \dots, \alpha_n) = (\prod_i x_i^{\alpha_0}) vdm(x_0, \dots, x_n; 0, \alpha_1 - \alpha_0, \dots, \alpha_n - \alpha_0)$$

permette di ricondursi al caso $\alpha_0 = 0$. Un'altra relazione ovvia è data da

$$vdm(x_0, \dots, x_n; \alpha \alpha_0, \alpha \alpha_1, \dots, \alpha \alpha_n) = vdm(x_0^\alpha, \dots, x_n^\alpha; \alpha_0, \alpha_1, \dots, \alpha_n).$$

Per il calcolo del determinante $vdm(x, \alpha)$ conviene osservare che, poiché esso si annulla se due valori delle variabili coincidono, esso sarà divisibile per il determinante $vdm(x)$ prima calcolato, e il rapporto $vdm(x, \alpha)/vdm(x)$ è un polinomio simmetrico nelle variabili x_0, \dots, x_n . Dobbiamo perciò introdurre qualche nozione sui polinomi simmetrici delle variabili x_1, x_2, \dots, x_n . Conviene introdurre il prodotto

$$p(x_1, x_2, \dots, x_n, T) = \prod_{i=1}^n (1 - x_i T) = \sum_{j=0}^n (-)^j p_j(x_1, x_2, \dots, x_n) T^j$$

(dunque $p_0 = 1$, $p_1 = \sum_i x_i$, $p_2 = \sum_{i < j} x_i x_j$, ed in generale p_j è la somma degli $\binom{n}{j}$ prodotti degli x_i presi a j a j senza ripetizioni: si dicono i polinomi simmetrici elementari) e il prodotto inverso

$$h(x_1, x_2, \dots, x_n, T) = \prod_{i=1}^n \frac{1}{1 - x_i T} = \prod_{i=1}^n (1 + x_i T + x_i^2 T^2 + x_i^3 T^3 + \dots) = \sum_{j=0}^{\infty} h_j(x_1, x_2, \dots, x_n) T^j$$

(dunque $h_0 = 1$, $h_1 = \sum_i x_i$, $h_2 = \sum_i x_i^2 + \sum_{i < j} x_i x_j$, ed in generale h_j è la somma degli $\binom{n+j-1}{j}$ monomi di grado j negli x_i : si dicono i polinomi simmetrici elementari completi). Dalla ovvia relazione $p(x, T)h(x, T) = h(x, T)p(x, T) = 1$ otteniamo che, dette

$$P = \begin{pmatrix} p_0 & 0 & 0 & \cdots & 0 \\ -p_1 & p_0 & 0 & \cdots & 0 \\ p_2 & -p_1 & p_0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ (-)^n p_n & (-)^{n-1} p_{n-1} & (-)^{n-2} p_{n-2} & \cdots & p_0 \end{pmatrix} \quad \text{e} \quad H = \begin{pmatrix} h_0 & 0 & 0 & \cdots & 0 \\ h_1 & h_0 & 0 & \cdots & 0 \\ h_2 & h_1 & h_0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ h_n & h_{n-1} & h_{n-2} & \cdots & h_0 \end{pmatrix}$$

si ha $PH = HP = \mathbb{I}_n$, ovvero $PH_{(1)} = e_1$ che riassume le cosiddette relazioni di Wronski:

$$\begin{aligned} 1 &= p_0 h_0 \\ 0 &= -p_1 h_0 + p_0 h_1 \\ 0 &= p_2 h_0 - p_1 h_1 + p_0 h_2 \\ &\vdots \\ 0 &= (-)^n p_n h_0 + (-)^{n-1} p_{n-1} h_1 + \cdots + p_0 h_n. \end{aligned}$$

I polinomi simmetrici elementari completi ci saranno particolarmente utili poiché soddisfano a importanti relazioni ricorsive: infatti dalle ovvie relazioni

$$h_r(x_1, \dots, x_i, \dots, x_n) = h_r(x_1, \dots, \widehat{x}_i, \dots, x_n) + x_i h_{r-1}(x_1, \dots, x_i, \dots, x_n)$$

(che abbreviamo con

$$h_r = h_r(\widehat{x}_i) + x_i h_{r-1};$$

ricordiamo che l'accento circonflesso indica che il termine accentato viene tolto dall'espressione) valide per ogni r e ogni i , possiamo ottenere (per sottrazione) che

$$(x_j - x_i) h_{r-1} = h_r(\widehat{x}_i) - h_r(\widehat{x}_j).$$

♠♠ **4.3.7.** VALUTAZIONE DEI DETERMINANTI DI VANDERMONDE GENERALIZZATI IN TERMINI DEI POLINOMI SIMMETRICI ELEMENTARI COMPLETI. Consideriamo ora la matrice

$$VdM(x_0, \dots, x_n; \alpha_0, \dots, \alpha_n) = (h_{\alpha_j}(x_i))$$

(ogni riga ha sempre la stessa variabile, elevata alle diverse potenze α_j). Considerando la seguente sequenza di operazioni elementari:

- (1) togliere ad ogni riga (dalla seconda in poi) la prima, e raccogliere i fattori $x_i - x_0$, lasciando i termini $h_{\alpha_j-1}(x_0, x_i)$;
- (2) togliere ad ogni riga (dalla terza in poi) la seconda, e raccogliere i fattori $x_i - x_1$, lasciando i termini $h_{\alpha_j-2}(x_0, x_1, x_i)$; ...
- (ℓ) togliere ad ogni riga (dalla $\ell+1$ -esima in poi) la ℓ -esima, e raccogliere i fattori $x_i - x_\ell$, lasciando i termini $h_{\alpha_j-\ell}(x_0, \dots, x_\ell, x_i)$; ...
- (n) togliere all'ultima riga la penultima riga, e raccogliere il fattore $x_n - x_{n-1}$, lasciando i termini $h_{\alpha_j-n}(x_0, x_1, \dots, x_n)$;

in cui ogni volta si usa la formula induttiva dei polinomi simmetrici elementari completi, si ottiene l'uguaglianza di determinanti

$$vdm(x_0, \dots, x_n; \alpha_0, \dots, \alpha_n) = vdm(x_0, \dots, x_n) \det(h_{\alpha_j-i}(x_0, \dots, x_i)).$$

Per ottenere una espressione più omogenea nelle variabili, si possono continuare le operazioni elementari, sommando ripetutamente ad ogni riga i -esima la successiva moltiplicata per x_{i+1} , per ottenere

l'espressione di Cauchy

$$\begin{aligned} vdm(x_0, \dots, x_n; \alpha_0, \dots, \alpha_n) &= vdm(x_0, \dots, x_n) \det(h_{\alpha_j - i}(x_0, \dots, x_n)) \\ &= vdm(x_0, \dots, x_n) \det \begin{pmatrix} h_{\alpha_0} & h_{\alpha_1} & \cdots & h_{\alpha_n} \\ h_{\alpha_0 - 1} & h_{\alpha_1 - 1} & \cdots & h_{\alpha_n - 1} \\ \vdots & \vdots & \ddots & \vdots \\ h_{\alpha_0 - n} & h_{\alpha_1 - n} & \cdots & h_{\alpha_n - n} \end{pmatrix}. \end{aligned}$$

♠ **4.3.8.** CASI PARTICOLARI. Se $\alpha_i = i$ per ogni i , allora ritroviamo il determinante di Vandermonde, poiché abbiamo a destra una matrice triangolare con 1 su tutta la diagonale. Si osservino poi i casi interessanti

$$vdm(x_0, \dots, x_n; 0, 1, \dots, n-1, n+1) = (\sum_i x_i) vdm(x_0, \dots, x_n)$$

e in generale per $N > n$

$$vdm(x_0, \dots, x_n; 0, 1, \dots, n-1, N) = h_{N-n}(x_0, \dots, x_n) vdm(x_0, \dots, x_n).$$

Inoltre per $M, N > n-1$ abbiamo

$$\begin{aligned} vdm(x_0, \dots, x_n; 0, 1, \dots, n-2, M, N) &= \det \begin{pmatrix} h_{M-n+1} & h_{N-n+1} \\ h_{M-n} & h_{N-n} \end{pmatrix} vdm(x_0, \dots, x_n) \\ &= (h_{M-n+1} h_{N-n} - h_{N-n+1} h_{M-n}) vdm(x_0, \dots, x_n). \end{aligned}$$

♠♠ **4.3.9.** VALUTAZIONE DEI DETERMINANTI DI VANDERMONDE GENERALIZZATI IN TERMINI DEI POLINOMI SIMMETRICI ELEMENTARI. Il determinante che descrive il rapporto $vdm(x; \alpha)/vdm(x)$ può anche essere espresso in termini di polinomi simmetrici elementari. Detti β_1, \dots, β_m l'insieme complementare agli indici $\alpha_0, \dots, \alpha_n$ in $\{0, 1, \dots, \alpha_n\}$, il (futuro) teorema di Jacobi sui minori della matrice dei complementi algebrici dà la formula

$$\begin{aligned} vdm(x_0, \dots, x_n; \alpha_0, \dots, \alpha_n) &= vdm(x_0, \dots, x_n) \det(p_{n-\beta_j+i}(x_0, \dots, x_n)) \\ &= vdm(x_0, \dots, x_n) \det \begin{pmatrix} p_{n-\beta_0+1} & p_{n-\beta_1+1} & \cdots & p_{n-\beta_m+1} \\ p_{n-\beta_0+2} & p_{n-\beta_1+2} & \cdots & p_{n-\beta_m+2} \\ \vdots & \vdots & \ddots & \vdots \\ p_{n-\beta_0+m} & p_{n-\beta_1+m} & \cdots & p_{n-\beta_m+m} \end{pmatrix} \end{aligned}$$

(a meno di un segno?) che risulta particolarmente utile quando $m = \alpha_n - n \leq n$.

♠♠ **4.3.10.** MATRICI E DETERMINANTI DIFFERENZIATI CONFLUENTI. Per ogni $m \leq n$ consideriamo le matrici “differenziate”

$$D_{m,n}(x) := \begin{pmatrix} 1 \\ \frac{d}{dx} \\ \frac{1}{2} \frac{d^2}{dx^2} \\ \vdots \\ \frac{1}{m!} \frac{d^m}{dx^m} \end{pmatrix} (1 \ x \ x^2 \ \cdots \ x^n) = \begin{pmatrix} 1 & x & x^2 & x^3 & \cdots & \cdots & x^n \\ 0 & 1 & 2x & 3x^2 & \cdots & \cdots & nx^{n-1} \\ 0 & 0 & 1 & 3x & \cdots & \cdots & \binom{n}{2} x^{n-2} \\ \vdots & \vdots & \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & \cdots & \binom{n}{m} x^{n-m} \end{pmatrix}$$

ove il termine in posto (i, j) è $\binom{j}{i-1} x^{j-i}$.

Considerata ora una partizione n_1, n_2, \dots, n_s di n (dunque n_i sono interi positivi con somma n), consideriamo la matrice quadrata

$$D_{(n_1, \dots, n_s)}(x_1, \dots, x_s) = \begin{pmatrix} D_{n_1, n}(x_1) \\ D_{n_2, n}(x_2) \\ \cdots \\ D_{n_s, n}(x_s) \end{pmatrix}$$

di cui vogliamo calcolare il determinante. Si tratta in effetti di una forma confluyente (cioè in cui si identificano più variabili) di una matrice di Vandermonde opportunamente trasformata: se infatti ad ogni blocco di n_i righe della matrice $VdM(y_1, \dots, y_n) = (y_i^j)$ si applicano le trasformazioni elementari

usate per studiare la forma generalizzata, e poi si identificano con x_t tutte le variabili y_i ove $n_{t-1} \leq i < n_t$, otteniamo esattamente la matrice $D_{(n_1, \dots, n_s)}(x_1, \dots, x_s)$. Quindi abbiamo che

$$d_{(n_1, \dots, n_s)}(x_1, \dots, x_s) = \lim_{\substack{y_i = x_t \\ (n_{t-1} \leq i < n_t)}} \frac{vdm(y_1, \dots, y_n)}{vdm(y_1, \dots, y_{n_1}) \cdots vdm(y_{n_{s-1}+1}, \dots, y_{n_s})} = \prod_{i < j} (x_j - x_i)^{n_i n_j}.$$

4.3.11. ALTERNANTI DOPPI DI CAUCHY. Gli alternanti doppi di Cauchy sono i determinanti di matrici della forma

$$C(x_1, \dots, x_n; y_1, \dots, y_n) = \left(\frac{1}{y_i - x_j} \right).$$

La valutazione del determinante si può fare in modo ricorsivo mediante le seguenti operazioni elementari:

- (1) ad ogni colonna togliere l'ultima colonna, raccogliendo i fattori $\frac{y_n - y_i}{y_n - x_j}$;
 - (2) ad ogni riga togliere l'ultima riga, raccogliendo i fattori $\frac{x_j - x_n}{y_i - x_n}$;
- ci si è ricondotti allora alla relazione ricorsiva

$$c(x_1, \dots, x_n; y_1, \dots, y_n) = \frac{\prod_i (y_n - y_i) \prod_j (x_j - x_n)}{\prod_j (y_n - x_j) \prod_i (y_i - x_n)} c(x_1, \dots, x_{n-1}; y_1, \dots, y_{n-1})$$

che reiterato fornisce il risultato voluto:

$$c(x_1, \dots, x_n; y_1, \dots, y_n) = \frac{vdm(x_n, \dots, x_1) vdm(y_1, \dots, y_n)}{\prod_{i,j} (y_i - x_j)}.$$

Espandendo in serie nelle y_i i due membri dell'equazione, e poi equiparando i termini con potenze uguali, si riottengono le formule per i determinanti delle matrici generalizzate di Vandermonde.

4.4. MATRICI ANTISIMMETRICHE. Ricordiamo che una matrice quadrata A si dice antisimmetrica se $A^t = -A$. Supponiamo che il corpo S abbia caratteristica diversa da 2 (altrimenti le matrici sono antisimmetriche se e solo se sono simmetriche); se A è antisimmetrica di ordine dispari, allora $|A|=0$. Infatti abbiamo $\det(A) = \det(A^t) = \det(-A) = -\det(A)$, da cui la conclusione. Inoltre abbiamo

$$\begin{vmatrix} 0 & a \\ -a & 0 \end{vmatrix} = a^2 \quad \text{e} \quad \begin{vmatrix} 0 & a & b & c \\ -a & 0 & d & e \\ -b & -d & 0 & f \\ -c & -e & -f & 0 \end{vmatrix} = (af + be - cd)^2.$$

♠ **4.4.1. PFAFFIANI.** Più in generale, il determinante di una matrice antisimmetrica d'ordine pari è il quadrato di un polinomio (a coefficienti interi) nelle entrate della matrice stessa; questa affermazione (tranne la parentesi) può essere dimostrata per induzione usando le formule degli sviluppi pivotali viste nel paragrafo precedente.

Il polinomio (determinato a meno del segno) il cui quadrato dà il determinante di una matrice antisimmetrica d'ordine $2n$ si dice Pfaffiano d'ordine n e si indica con $\text{Pf}^n(x_{i,j})$ (le variabili hanno indici $1 \leq i < j \leq 2n$ e sono in numero di $n(n-1)/2$). Di nuovo per induzione sull'ordine si può dimostrare che

$$\text{Pf}^n(x_{i,j}) = \sum_{\substack{1 \leq i_1 < i_2 < \dots < i_n \leq 2n \\ (1 \leq s \leq n)}} \text{sgn} \left(\begin{matrix} 1 & 2 & 3 & 4 & \dots & 2n-1 & 2n \\ i_1 & j_1 & i_2 & j_2 & \dots & i_n & j_n \end{matrix} \right) x_{i_1, j_1} x_{i_2, j_2} \cdots x_{i_n, j_n}$$

ove la sommatoria comprende $(2n-1)!!$ termini (e sono tutti i prodotti di n termini $x_{i,j}$ ove $i < j$ e gli indici sono tutti diversi).

4.5. CIRCOLANTI. Si chiamano circolanti le matrici le cui righe si ottengono ognuna dalla precedente "circolando" i termini di un posto a destra; si tratta quindi di matrici della forma

$$C(a_1, a_2, a_3, \dots, a_{n-1}, a_n) = \begin{pmatrix} a_1 & a_2 & a_3 & \cdots & a_{n-1} & a_n \\ a_n & a_1 & a_2 & \cdots & a_{n-2} & a_{n-1} \\ a_{n-1} & a_n & a_1 & \cdots & a_{n-3} & a_{n-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ a_3 & a_4 & a_5 & \cdots & a_1 & a_2 \\ a_2 & a_3 & a_4 & \cdots & a_n & a_1 \end{pmatrix}.$$

Per calcolare il determinante $c(a_1, a_2, a_3, \dots, a_{n-1}, a_n) = |C(a_1, a_2, a_3, \dots, a_{n-1}, a_n)|$ di una matrice circolante (detto esso stesso circolante) a coefficienti complessi possiamo ricorrere al metodo di Brioschi: moltiplicando a destra la matrice circolante $C = C(a_1, a_2, \dots, a_n)$ per la matrice di Vandermonde $V = VdM(1, \omega, \omega^2, \dots, \omega^{n-1})$, ove ω è una radice primitiva n -esima dell'unità, otteniamo $CV = V \text{diag}(\vartheta_0, \dots, \vartheta_{n-1})$ ove $\vartheta_i = \sum_{j=0}^{n-1} a_{i+1} \omega^{ij}$ per $i = 0, 1, \dots, n-1$. Passando ai determinanti, otteniamo che

$$c(a_1, a_2, a_3, \dots, a_{n-1}, a_n) = \prod_{i=0}^{n-1} \vartheta_i = \prod_{i=0}^{n-1} \sum_{j=0}^{n-1} a_{i+1} \omega^{ij}.$$

Si osservi che se la matrice circolante ha coefficienti reali, anche il determinante è reale, sebbene la formula comporti calcoli con radici complesse dell'unità.

4.5.1. Matrici e determinanti anticircolanti si ottengono da una riga circolando a sinistra i termini. Che relazioni vi sono con le matrici e i determinanti circolanti?

4.5.2. Un caso particolare in cui è possibile semplificare il calcolo è la matrice circolante

$$C(a, a+d, a+2d, \dots, a+(n-1)d).$$

In tal caso sottraendo ad ogni colonna la precedente si trova una matrice della forma

$$\begin{pmatrix} a & d & d & \cdots & d \\ a+(n-1)d & -(n-1)d & d & \cdots & d \\ a+(n-2)d & d & -(n-1)d & \cdots & d \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a+d & d & d & \cdots & -(n-1)d \end{pmatrix}$$

e sostituendo la prima riga con la somma di tutte le righe si può valutare il determinante come

$$c(a, a+d, a+2d, \dots, a+(n-1)d) = n(a + \frac{n-1}{2}d)(-1)^{n-1}d^{n-1}n^{n-2} = (-nd)^{n-1} \left(a + \frac{n-1}{2}d \right)$$

(si osservi che la matrice d'ordine n avente entrate non diagonali tutte uguali ad 1 ed entrate non diagonali uguali ad $1-x$ vale $(n-x)(-x)^{n-1} = (-1)^n x^{n-1}(x-n)$; si può vedere con le riduzioni elementari consistenti nel sottrarre alla prima riga tutte le altre, poi raccogliere il termine comune, e infine sottrarre la prima riga a tutte le altre; ma sarà più facile quando si conosceranno le nozioni di polinomio caratteristico e autovalori di una matrice).

4.5.3. In particolare abbiamo che $c(1, 2, \dots, n) = \frac{n+1}{2}(-n)^{n-1}$.

4.6. RICORRENTI. Si indicano con il nome di ricorrenti i determinanti di matrici le cui entrate sono nulle per indici (i, j) con $i < j+1$, quindi del tipo

$$\begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n-1} & a_{1,n} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n-1} & a_{2,n} \\ 0 & a_{3,2} & \cdots & a_{3,n-1} & a_{3,n} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & a_{n,n-1} & a_{n,n} \end{pmatrix}.$$

Il nome è dovuto al fatto che questi determinanti soddisfano a delle uguaglianze ricorsive al variare dell'ordine n . Detto infatti R_n il determinante della matrice d'ordine n , sviluppando rispetto all'ultima riga abbiamo due termini, uno contenente R_{n-1} , e l'altro contenente il determinante di una matrice con soli due termini nell'ultima riga; sviluppando ripetutamente rispetto all'ultima riga otteniamo che

$$R_n = a_{n,n}R_{n-1} - a_{n,n-1}a_{n-1,n}R_{n-2} + a_{n,n-1}a_{n-1,n-2}a_{n-2,n}R_{n-3} - \cdots + (-1)^n \prod_j a_{j,j-1}$$

(il termine che moltiplica R_{n-i} è $a_{n,n-1}a_{n-1,n-2} \cdots a_{n-i+2,n-i+1}a_{n-i+1,n}$ con il segno $(-1)^{i+1}$).

4.6.1. Casi in cui in ogni diagonale i termini sono tutti uguali?

4.6.2. Casi in cui la diagonale sotto la principale ha termini tutti 1?

4.7. TRIDIAGONANTI. Un caso interessante è quello di ricorrenti in cui solo la diagonale principale e i termini immediatamente adiacenti sono non nulli; si parla allora di tridiagonanti. Indicato con T_n

il determinante della matrice

$$\begin{pmatrix} a_0 & b_1 & 0 & \cdots & 0 & 0 \\ c_1 & a_1 & b_2 & \cdots & 0 & 0 \\ 0 & c_2 & a_2 & \ddots & 0 & 0 \\ \vdots & \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & \ddots & a_{n-2} & b_{n-1} \\ 0 & 0 & 0 & \cdots & c_{n-1} & a_{n-1} \end{pmatrix}.$$

la relazione ricorsiva diventa semplicemente

$$T_n = a_{n-1}T_{n-1} - c_{n-1}b_{n-1}T_{n-2}.$$

Nel caso in cui $a_i = a$, $b_i = b$ e $c_i = c$ sono costanti per $i \geq 2$ da queste relazioni ricorsive si possono determinare formule chiuse per tali determinanti (come vedremo in un futuro capitolo studiando le forme canoniche delle matrici).

4.7.1. Nel caso in cui $a_i = 0$ per ogni i ?

4.7.2. Nel caso in cui $b_i = i$ e $c_i = n - i + 1$ per ogni i ?

4.7.3. Nel caso in cui $b_i = 1$ e $c_i = 1$ per ogni i ?

♠ **4.8.** CONTINUANTI. Si dicono continuanti i tridiagonanti con $c_i = -1$ per ogni i . In questo caso essi soddisfano alle formule ricorsive

$$T_n = a_{n-1}T_{n-1} + b_{n-1}T_{n-2}.$$

Il nome è dovuto al seguente fatto: una frazione continua è una espressione del tipo

$$F_n = \frac{1}{a_0 + \frac{b_1}{a_1 + \frac{b_2}{a_2 + \ddots + \frac{b_{n-2}}{a_{n-2} + \frac{b_{n-1}}{a_{n-1}}}}}}$$

ove $a_i, b_i \in \mathbb{N}$ per ogni i (queste frazioni continue sono importanti, poiché ogni numero reale compreso tra 0 e 1 si può scrivere in tali termini con frazioni continue infinite, e le approssimazioni successive che si ottengono troncando la frazione continua sono particolarmente buone). Si dimostra per induzione su n che, detto $F_n = p_n/q_n$ (numeratore e denominatore sono funzioni di a_i e b_i), valgono le relazioni ricorsive $p_n = a_{n-1}p_{n-1} + b_{n-1}p_{n-2}$ ($p_0 = 0$ e $p_1 = 1$) e $q_n = a_{n-1}q_{n-1} + b_{n-1}q_{n-2}$ ($q_{-1} = 0$ e $q_0 = 1$). Infatti possiamo calcolare facilmente i primi casi:

$$\begin{array}{lll} F_1 = \frac{1}{a_0} & p_1 = 1 & q_1 = a_0 \\ F_2 = \frac{a_1}{a_0a_1 + b_1} & p_2 = a_1 & q_2 = a_0a_1 + b_1 \\ F_3 = \frac{a_1a_2 + b_2}{a_0a_1a_2 + a_0b_2 + a_2b_1} & p_3 = a_1a_2 + b_2 & q_3 = a_0a_1a_2 + a_0b_2 + a_2b_1 \end{array}$$

e per il caso induttivo, possiamo calcolare F_n tenendo conto che $\frac{b_{n-2}}{a_{n-2} + \frac{b_{n-1}}{a_{n-1}}} = \frac{a_{n-1}b_{n-2}}{a_{n-1}a_{n-1} + b_{n-1}}$ otteniamo

$$\begin{aligned} \frac{p_n}{q_n} &= \frac{p_{n-1}(b_{n-2} = a_{n-1}b_{n-2}; a_{n-2} = a_{n-1}a_{n-2} + b_{n-1})}{q_{n-1}(b_{n-2} = a_{n-1}b_{n-2}; a_{n-2} = a_{n-1}a_{n-2} + b_{n-1})} \\ &= \frac{(a_{n-1}a_{n-2} + b_{n-1})p_{n-2} + (a_{n-1}b_{n-2})p_{n-3}}{(a_{n-1}a_{n-2} + b_{n-1})q_{n-2} + (a_{n-1}b_{n-2})q_{n-3}} \\ &= \frac{a_{n-1}(a_{n-2}p_{n-2} + b_{n-2}p_{n-3}) + b_{n-1}p_{n-2}}{a_{n-1}(a_{n-2}q_{n-2} + b_{n-2}q_{n-3}) + b_{n-1}q_{n-2}} \\ &= \frac{a_{n-1}p_{n-1} + b_{n-1}p_{n-2}}{a_{n-1}q_{n-1} + b_{n-1}q_{n-2}} \end{aligned}$$

(abbiamo usato l'ipotesi induttiva nel secondo e nel quarto passaggio).

Siccome le relazioni ricorsive che danno i continuanti t_n sono le stesse che regolano numeratore p_n e denominatore q_n della frazione continua, e tenendo conto dei valori iniziali, possiamo concludere che

$$F_n(a_0, a_1, b_1, \dots, a_{n-1}, b_{n-1}) = \frac{T_{n-1}(a_1, a_2, b_2, \dots, a_{n-1}, b_{n-1})}{T_n(a_0, a_1, b_1, \dots, a_{n-1}, b_{n-1})}$$

per ogni $n \geq 1$ (ponendo $T_0 = 1$, determinante della matrice quadrata vuota).

4.9. DETERMINANTE DI CAYLEY-MENGER (ERONE). Si osservi che

$$\begin{vmatrix} 0 & a & b & c \\ a & 0 & c & b \\ b & c & 0 & a \\ c & b & a & 0 \end{vmatrix} = \begin{vmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & c^2 & b^2 \\ 1 & c^2 & 0 & a^2 \\ 1 & b^2 & a^2 & 0 \end{vmatrix} = -16\Delta^2$$

ove $\Delta = \sqrt{s(s-a)(s-b)(s-c)}$ è il termine di Erone per il calcolo dell'area del triangolo i cui lati hanno lunghezze a, b, c .

Inoltre

$$16\Delta^2 = \begin{pmatrix} a^2 & b^2 & c^2 \end{pmatrix} \begin{pmatrix} -1 & 1 & 1 \\ 1 & -1 & 1 \\ 1 & 1 & -1 \end{pmatrix} \begin{pmatrix} a^2 \\ b^2 \\ c^2 \end{pmatrix}$$

(generalizzazioni?).

4.10. MATRICI ELEMENTARI (ED UNA ASSIOMATICA ALTERNATIVA PER IL DETERMINANTE).

Abbiamo già calcolato i determinanti delle matrici elementari; è interessante osservare che la funzione determinante è completamente definita dalle seguenti due condizioni:

(D1) è moltiplicativa: $\det(AB) = \det A \det B$;

(D2) vale α sulle matrici $H(i, \alpha) = \mathbb{I}_n + (\alpha - 1)e_{i,i}$.

Queste due proprietà possono essere prese come definizione per la funzione determinante, ed è facile allora dimostrarne l'unicità, meno facile dimostrarne l'esistenza.

Per mostrare l'unicità si procede per gradi:

- (1) certamente le matrici $H(i, j, \alpha)$ hanno determinante non nullo, poiché $H(i, j, \alpha)H(i, j, -\alpha) = \mathbb{I}$; poiché inoltre $H(i, j, \alpha) = H(i, \alpha)H(i, j, 1)H(i, 1/\alpha)$ (se $\alpha \neq 0$) abbiamo che il determinante non dipende da α ; ma allora da $H(i, j, \alpha) = H(i, j, 2\alpha) = H(i, j, \alpha)H(i, j, \alpha)$ concludiamo che tale determinante è 1.
- (2) dalla relazione $S(i, j) = H(i, -1)H(i, j, -1)H(j, i, 1)H(i, j, -1)$ si deduce allora che $S(i, j) = -1$.
- (3) usando la riduzione di Gauss per righe e per colonne, ogni matrice può essere scritta come prodotto di matrici elementari e di una matrice diagonale (eventualmente con zeri in diagonale se è degenere), e quindi il suo determinante può essere calcolato tramite questa decomposizione.

Si osservi anche che la proprietà richiesta (D2) può essere indebolita, chiedendo solo che $\det H(1, \alpha) = \alpha$ (per ogni α).

5. Rango e determinanti (minori).

5.1. DEFINIZIONE-TEOREMA (MINORI E RANGO). Sia $A \in M_{n,m}(C)$ una matrice. I minori di ordine k della matrice A sono i determinanti delle sottomatrici quadrate di ordine k di A che si ottengono cancellando $n-k$ righe ed $m-k$ colonne di A . Il rango di una matrice coincide con il massimo ordine di un minore non nullo: la matrice A ha rango k se e solo se esiste un minore non nullo d'ordine k e tutti i minori d'ordine maggiore di k sono nulli.

DIMOSTRAZIONE. Se il rango di A è k , allora vi sono k colonne indipendenti, e dunque possiamo scegliere in quella sottomatrice k righe tali che il minore d'ordine k così trovato sia non nullo. Viceversa, se vi è un minore d'ordine k non nullo, le colonne coinvolte sono k colonne linearmente indipendenti, e dunque la matrice ha rango almeno k . \square

5.1.1. Sia $A \in M_{n,m}(C)$ una matrice. I minori d'ordine k sono in numero di $\binom{n}{k} \binom{m}{k}$. Supponiamo di avere un minore non nullo d'ordine $k-1$; qual è il numero minimo di minori d'ordine k che devono essere nulli affinché la matrice abbia rango $k-1$?

5.1.2. Si noti che se tutti i minori di ordine k sono nulli, allora anche tutti i minori d'ordine maggiore di k sono nulli. Come dimostrare direttamente questo risultato?

5.2. PRINCIPIO DEI MINORI ORLATI. Sia $A \in M_{n,m}(C)$, e sia A' una sottomatrice quadrata d'ordine r il cui determinante sia non nullo. Allora il rango di A è r se e solo se tutti i minori di A di ordine $r+1$ ottenuti da sottomatrici di A contenenti A' (sono i minori orlati di A') sono nulli (osservare che la condizione è ovviamente necessaria; che sia sufficiente invece non è ovvio: sono solo $\min m, n-r$ i minori d'ordine $r+1$ nulli per ipotesi...).

5.2.1. EQUAZIONI DI SOTTOSPAZI. Dati i vettori linearmente indipendenti v_1, \dots, v_r nello spazio vettoriale standard C^n , il sottospazio da essi generato è formato dai vettori X tali che la matrice $(X \ v_1 \ \dots \ v_r)$ abbia rango r (e non $r+1$); quindi esso è descritto dall'annullamento di tutti i minori d'ordine $r+1$ della matrice detta: si tratta delle equazioni cartesiane del sottospazio. Sappiamo già che possiamo sceglierne $n-r$ per descrivere il sottospazio, e il principio dei minori orlati permette di farlo senza esplicitare tutti i minori: basta trovare un minore d'ordine r non nullo della matrice $(v_1 \ \dots \ v_r)$ (esiste per ipotesi, poiché v_1, \dots, v_r sono linearmente indipendenti) e annullare tutti i minori d'ordine $r+1$ della matrice $(X \ v_1 \ \dots \ v_r)$ che contengono il minore scelto, ovvero che si ottengono "orlando" la sottomatrice quadrata invertibile prima scelta. Si tratta esattamente di $n-r$ equazioni cartesiane indipendenti (perché? Osservare che la matrice del sistema si presenta quasi in forma a scalini).

♠ **5.3. TEOREMA (DI JACOBI SUI MINORI DELLA MATRICE DEI COMPLEMENTI ALGEBRICI).** Siano I e J due sottinsiemi di $\{1, \dots, n\}$ di cardinalità k e indichiamo con $A_{(J)}^{(I)}$ la sottomatrice di A che si ottiene selezionando gli elementi $a_{i,j}$ con $i \in I$ e $j \in J$. Siano I' e J' gli insiemi complementari. Allora abbiamo

$$|A_{(J)}^{(I)}| = \varepsilon(I, I')\varepsilon(J, J')|A|^{k-1}|A_{(J')}^{(I')}|,$$

ovvero i minori d'ordine k di A^c coincidono con i minori segnati di A^t di indici complementari, moltiplicati per la potenza $k-1$ -esima del determinante di A .

DIMOSTRAZIONE. Vedremo dopo una generalizzazione con una dimostrazione più elegante. La dimostrazione classica procede invece così: supponiamo $I = J = \{1, \dots, k\}$ e consideriamo il prodotto di matrici

$$\begin{pmatrix} A^{(1)} \\ \vdots \\ A^{(k)} \\ A^{(k+1)} \\ \vdots \\ A^{(n)} \end{pmatrix} \begin{pmatrix} A_{(1)}^c \cdots A_{(k)}^c & e_{k+1} \cdots e_n \end{pmatrix} = \begin{pmatrix} |A|e_1 \cdots |A|e_k & A_{(k+1)} \cdots A_{(n)} \end{pmatrix}$$

dove la prima matrice è A (scritta a righe), la seconda è la matrice A^c in cui le colonne con indici in J' sono state sostituite con i vettori della base canonica di indici in I' . Calcolando i determinanti si ottiene il risultato voluto. In modo analogo si può tener conto della trasposizione e dei segni dei minori, come il lettore può scoprire calcolando i determinanti di $AB = C$ ove B è la matrice tale che $B_{(j_\ell)} = A_{(j_\ell)}^c$ se $j_\ell \in J$ e $B_{(j'_\ell)} = e_{i_\ell}$ se $j'_\ell \notin J$; e quindi le colonne di C sono $C_{(j_\ell)} = |A|e_{(j_\ell)}$ se $j_\ell \in J$ e $C_{(j'_\ell)} = A_{(i'_\ell)}$ se $j'_\ell \notin J$. \square

♠♠ **5.4.** Per capire meglio la rilevanza della nozione dei minori di una matrice quadrata, conviene dare delle definizioni più generali, e costruire, per ogni matrice $A \in M_n(C)$ e per ogni $k \leq n$ la matrice formata da tutti i suoi minori d'ordine k (considerati nell'ordine lessicografico degli indici che lo formano) e una ulteriore matrice formata dai relativi cofattori (o minori complementari segnati) che entrano nelle formula generalizzate di Laplace. Si tratta di matrici quadrate d'ordine $\binom{n}{k}$.

5.4.1. DEFINIZIONE (ORDINE LESSICOGRAFICO). Dati due sottinsiemi $I = \{i_1, i_2, \dots, i_k\}$ e $J = \{j_1, j_2, \dots, j_k\}$ di $\{1, 2, \dots, n\}$, diciamo che $I \preccurlyeq J$ (I precede J) se per il primo indice ℓ tale che $i_\ell \neq j_\ell$ si ha $i_\ell < j_\ell$. Si tratta dell'ordine che si usa nei vocabolari, ed è un ordine totale.

5.4.2. DEFINIZIONE (MATRICI COMPOSTE E MATRICI COMPOSTE COMPLEMENTARI). Data $A \in M_n(C)$, per ogni $k \leq n$ definiamo $M^{(k)}(A)$ la k -esima matrice composta o matrice dei minori

d'ordine k come

$$M^{(k)}(A) := \left(\left| A_{(I,J)}^{(I)} \right| \right)_{\substack{|I|=k \\ |J|=k}}$$

con l'ordine lessicografico degli indici I e J ; e $C^{(k)}(A)$ la k -esima matrice complementare composta o matrice dei minori complementari segnati d'ordine $n-k$ come

$$C^{(k)}(A) := \left(\varepsilon(I, I') \varepsilon(J, J') \left| A_{(J', I')}^{(I')} \right| \right)_{\substack{|I|=k \\ |J|=k}}^t$$

con l'ordine lessicografico degli indici I e J (si tratta della matrice trasposta della matrice $M^{(k)}(A)$ in cui ogni minore è stato sostituito con il suo complemento segnato).

Si ha subito che $M^{(1)}(A) = A$ e $C^{(1)}(A) = A^c$.

5.4.3. TEOREMA (RANGO). Il rango di A è uguale ad r se e solo se $M^{(r)}(A) \neq \mathbb{O}$ e $M^{(r+1)}(A) = \mathbb{O}$; più in generale, il rango di $M^{(k)}(A)$ è uguale a $\binom{r}{k}$.

Dagli sviluppi generalizzati di Laplace segue subito che:

5.4.4. TEOREMA (PRODOTTO DI COMPOSTE E LORO COMPLEMENTARI). Per ogni $k \leq n$ risulta

$$M^{(k)}(A)C^{(k)}(A) = C^{(k)}(A)M^{(k)}(A) = |A| \mathbb{I}_{\binom{n}{k}}.$$

5.4.5. TEOREMA (BINET-CAUCHY). Per ogni $k \leq n$ risulta:

- (i) $M^{(k)}(\mathbb{I}_n) = \mathbb{I}_{\binom{n}{k}}$;
- (ii) $M^{(k)}(AB) = M^{(k)}(A)M^{(k)}(B)$ per ogni $A, B \in M_n(C)$;
- (iii) $M^{(k)}(\alpha A) = \alpha^k M^{(k)}(A)$ per ogni $\alpha \in C$;
- (i') $C^{(k)}(\mathbb{I}_n) = \mathbb{I}_{\binom{n}{k}}$;
- (ii') $C^{(k)}(AB) = C^{(k)}(B)C^{(k)}(A)$ per ogni $A, B \in M_n(C)$;
- (iii) $C^{(k)}(\alpha A) = \alpha^{n-k} M^{(k)}(A)$ per ogni $\alpha \in C$.

DIMOSTRAZIONE. Non sono ovvii i punti (ii) e (ii'), che seguono dal calcolo di Binet-Cauchy per il determinante del prodotto $A'B'$ di matrici rettangolari $A' \in M_{k \times n}(C)$ e $B' \in M_{n \times k}(C)$. Si consideri infatti la seguente astuzia:

$$\begin{pmatrix} \mathbb{I}_k & A' \\ \mathbb{O}_{k,n} & \mathbb{I}_n \end{pmatrix} \begin{pmatrix} A' & \mathbb{O}_k \\ -\mathbb{I}_{k,n} & B' \end{pmatrix} = \begin{pmatrix} \mathbb{O}_k & A'B' \\ -\mathbb{I}_{k,n} & B' \end{pmatrix}$$

e sfruttando gli sviluppi di Laplace secondo le prime k righe otteniamo che $|A'B'|$ è nullo ogni volta che $k > n$, mentre è la somma $\sum_H |A'_{(H)}| |B'^{(H)}|$ dei prodotti dei minori di indici corrispondenti di A' e B' se $k \leq n$.

Ora basta applicare questo principio al minore di righe I e colonne J della matrice AB , tenendo conto che

$$\begin{pmatrix} A^{(I)} \\ A^{(I')} \end{pmatrix} \begin{pmatrix} B_{(J)} & B_{(J')} \end{pmatrix} = \begin{pmatrix} A^{(I)}B_{(J)} & A^{(I)}B_{(J')} \\ A^{(I')}B_{(J)} & A^{(I')}B_{(J')} \end{pmatrix}$$

e il minore di interesse è proprio $A^{(I)}B_{(J)}$. □

5.4.6. TEOREMA (CAUCHY-SYLVESTER). Per ogni $k \leq n$ risulta $|M^{(k)}(A)C^{(k)}(A)| = |A|^{\binom{n}{k}}$; inoltre

- (i) $|M^{(k)}(A)| = |A|^{\binom{n-1}{k-1}}$;
- (i') $|C^{(k)}(A)| = |A|^{\binom{n-1}{k}}$.

DIMOSTRAZIONE. La prima formula è ovvia dal prodotto delle matrici, quindi basta dimostrare (i). Poiché $|A|$ è polinomio irriducibile nelle entrate della matrice, il determinante cercato non può che esserne una potenza, e basta allora sapere qual è il grado omogeneo dei suoi termini. Ora $|M^{(k)}(A)|$ è polinomio di grado $k \binom{n}{k}$ nelle entrate di A , mentre $|A|$ è polinomio di grado n nelle stesse variabili. Poiché $\frac{k}{n} \binom{n}{k} = \binom{n-1}{k-1}$, abbiamo il risultato voluto. □

5.4.7. TEOREMA (INVERSE DI COMPOSTE E LORO COMPLEMENTARI). Per ogni $k \leq n$ e per ogni matrice invertibile A , risulta

- (i) $M^{(k)}(A)^{-1} = M^{(k)}(A^{-1}) = |A|^{-1}C^{(k)}(A);$
 (i') $C^{(k)}(A)^{-1} = C^{(k)}(A^{-1}) = |A|^{-1}M^{(k)}(A).$

DIMOSTRAZIONE. Per dimostrare (i) basta applicare $M^{(k)}$ al prodotto $AA^{-1} = \mathbb{I}_n$, da cui $M^{(k)}(A)M^{(k)}(A^{-1}) = \mathbb{I}_{\binom{n}{k}}$, da cui la prima uguaglianza. La seconda uguaglianza segue dal confronto con la formula del prodotto $M^{(k)}(A)C^{(k)}(A) = |A|\mathbb{I}_{\binom{n}{k}}$. \square

Si osservi anche che $M^{(k)}(A)^t = M^{(k)}(A^t)$ e analogamente $C^{(k)}(A)^t = C^{(k)}(A^t)$ (infatti $|A_{(J)}^{(I)}| = |(A^t)_{(I)}^{(J)}|$).

5.4.8. TEOREMA (FRANKE). Per ogni $h, k \leq n$ risulta

- (i) $C^{(h)}(M^{(k)}(A)) = |A|^{\binom{n-1}{k-1}-h}M^{(h)}(C^{(k)}(A));$
 (i') $C^{(h)}(C^{(k)}(A)) = |A|^{\binom{n-1}{k}-h}M^{(h)}(M^{(k)}(A)).$

DIMOSTRAZIONE. Basta confrontare l'espressione

$$M^{(h)}(M^{(k)}(A))M^{(h)}(C^{(k)}(A)) = |A|^h \mathbb{I}_{\binom{n}{h}}$$

ottenuta applicando $M^{(h)}$ al prodotto $M^{(k)}(A)C^{(k)}(A) = |A|\mathbb{I}_{\binom{n}{k}}$, con l'espressione

$$M^{(h)}(M^{(k)}(A))C^{(h)}(M^{(k)}(A)) = |M^{(k)}(A)| \mathbb{I}_{\binom{n}{h}} = |A|^{\binom{n-1}{k-1}} \mathbb{I}_{\binom{n}{h}}$$

ottenuta sostituendo A con $M^{(k)}(A)$ in $M^{(h)}(A)C^{(h)}(A) = |A|\mathbb{I}_{\binom{n}{h}}$, per ottenere (i); e con l'espressione

$$C^{(h)}(C^{(k)}(A))M^{(h)}(C^{(k)}(A)) = |C^{(k)}(A)| \mathbb{I}_{\binom{n}{h}} = |A|^{\binom{n-1}{k}} \mathbb{I}_{\binom{n}{h}}$$

ottenuta sostituendo A con $C^{(k)}(A)$ in $C^{(h)}(A)M^{(h)}(A) = |A|\mathbb{I}_{\binom{n}{h}}$, per ottenere (i'). \square

In particolare usando $k = 1$ in (i) possiamo ritrovare il teorema di Jacobi sui minori di A^c , nella forma $C^{(h)}(A) = |A|^{1-h}M^{(h)}(A^c)$ (cioè $M^{(h)}(A^c) = |A|^{h-1}C^{(h)}(A)$), mentre ponendo $h = 1$ otteniamo una espressione di $C^{(k)}(A)$ come matrice dei complementi algebrici di $M^{(k)}(A)$ moltiplicata per una opportuna costante.

Analoghe osservazioni si possono fare per (i').

6. Esercizi.

6.1. Verificare che $\det \begin{pmatrix} 2 & 2 & 2 & 2 & 1 \\ 3 & 3 & 3 & 1 & 2 \\ 4 & 4 & 5 & 1 & -1 \\ -1 & -1 & 1 & 1 & 2 \\ 2 & 1 & 1 & 1 & -1 \end{pmatrix} = 42.$

6.2. Sia $X = \begin{pmatrix} A & B \\ 0 & C \end{pmatrix}$ una matrice a blocchi, ove $A \in M_{r \times r}(\mathbb{R})$ e $C \in M_{s \times s}(\mathbb{R})$. Si mostri che $\det X = \det A \det C$, usando la tecnica di riduzione di Gauss.

6.3. Sia $X = \begin{pmatrix} B & A \\ C & 0 \end{pmatrix}$ una matrice a blocchi, ove $A \in M_{r \times r}(\mathbb{R})$ e $C \in M_{s \times s}(\mathbb{R})$. Si calcoli il determinante di X .

6.4. Sia $A \in M_{(2n+1) \times (2n+1)}(\mathbb{R})$ tale che $A = -A^t$. Mostrare che $\det A = 0$.

6.5. Determinare due matrici quadrate A, B tali che $\det(A+B) \neq \det A + \det B$.

6.6. Sia \mathfrak{S}_n il gruppo simmetrico su $\{1, \dots, n\}$. Per ogni $\sigma \in \mathfrak{S}_n$ sia φ_σ l'unico automorfismo di \mathbb{R}^n tale che $\varphi_\sigma(e_i) = e_{\sigma(i)}$ per ogni $i = 1, \dots, n$, dove $\{e_1, \dots, e_n\}$ è la base canonica di \mathbb{R}^n . Verificare che $\det \varphi_\sigma = \text{sgn}(\sigma)$ per ogni $\sigma \in \mathfrak{S}_n$.

6.7. Calcolare i determinanti delle seguenti matrici $n \times n$

$$\begin{pmatrix} 1-n & 1 & 1 & \cdots & 1 \\ 1 & 1-n & 1 & \cdots & 1 \\ 1 & 1 & 1-n & \cdots & 1 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & 1 & \cdots & 1-n \end{pmatrix}, \quad \begin{pmatrix} 1 & n & n & \cdots & n \\ n & 2 & n & \cdots & n \\ n & n & 3 & \cdots & n \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ n & n & n & \cdots & n \end{pmatrix}$$

al variare di n .

6.8. Si scriva il triangolo di Tartaglia fino all'ordine n come matrice quadrata triangolare inferiore. È vero che per ogni n essa ha determinante 1? Calcolarne la matrice inversa.

6.9. Mostrare che $\det \begin{pmatrix} 1 & a & b+c \\ 1 & b & a+c \\ 1 & c & a+b \end{pmatrix} = 0$.

6.10. Mostrare che $\det \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1+x & 1 \\ 1 & 1 & 1+y \end{pmatrix} = xy$, e generalizzare.

6.11. Calcolare i determinanti delle seguenti matrici

$$\begin{pmatrix} x & a_1 & a_2 & \cdots & a_{n-1} & 1 \\ a_1 & x & a_2 & \cdots & a_{n-1} & 1 \\ a_1 & a_2 & x & \cdots & a_{n-1} & 1 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ a_1 & a_2 & a_3 & \cdots & x & 1 \\ a_1 & a_2 & a_3 & \cdots & a_n & 1 \end{pmatrix}, \quad \begin{pmatrix} a_0 & a_1 & a_2 & \cdots & a_{n-1} & a_n \\ -x & x & 0 & \cdots & 0 & 0 \\ 0 & -x & x & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \ddots & x & 0 \\ 0 & 0 & 0 & \cdots & -x & x \end{pmatrix}, \quad \begin{pmatrix} -x & 0 & 0 & \cdots & 0 & a_0 \\ 1 & -x & 0 & \cdots & 0 & a_1 \\ 0 & 1 & -x & \cdots & 0 & a_2 \\ \vdots & \vdots & \ddots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \ddots & -x & a_{n-1} \\ 0 & 0 & 0 & \cdots & 1 & -x+a_n \end{pmatrix}$$

al variare di n .

6.12. Calcolare i determinanti delle matrici $n \times n$ $\begin{pmatrix} 1 & 1 & 0 & 0 & \cdots & 0 & 0 \\ 1 & 1 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 1 & 1 & \cdots & 0 & 0 \\ 0 & 0 & 1 & 1 & \ddots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \ddots & 1 & 1 \\ 0 & 0 & 0 & 0 & \cdots & 1 & 1 \end{pmatrix}$ al variare di n .

6.13. Calcolare i determinanti delle seguenti matrici

$$\begin{pmatrix} a & 0 & b \\ 0 & c & 0 \\ d & 0 & f \end{pmatrix}, \quad \begin{pmatrix} a & 0 & 0 & b \\ 0 & c & d & 0 \\ 0 & e & f & 0 \\ g & 0 & 0 & h \end{pmatrix}, \quad \begin{pmatrix} a & 0 & 0 & 0 & b \\ 0 & c & 0 & d & 0 \\ 0 & 0 & e & 0 & 0 \\ 0 & f & 0 & g & 0 \\ h & 0 & 0 & 0 & i \end{pmatrix}.$$

6.14. Calcolare i determinanti delle seguenti matrici

$$\begin{pmatrix} a & 1 & 0 \\ 1 & b & 1 \\ 0 & 1 & c \end{pmatrix}, \quad \begin{pmatrix} a & 1 & 0 & 0 \\ 1 & b & 1 & 0 \\ 0 & 1 & c & 1 \\ 0 & 0 & 1 & d \end{pmatrix}, \quad \begin{pmatrix} a & 1 & 0 & 0 & 0 \\ 1 & b & 1 & 0 & 0 \\ 0 & 1 & c & 1 & 0 \\ 0 & 0 & 1 & d & 1 \\ 0 & 0 & 0 & 1 & e \end{pmatrix}.$$

6.15. Calcolare i determinanti delle seguenti matrici

$$\begin{pmatrix} 1 & a & 0 \\ b & 1 & b \\ 0 & a & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & a & 0 & 0 \\ c & 1 & b & 0 \\ 0 & b & 1 & c \\ 0 & 0 & a & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & a & 0 & 0 & 0 \\ d & 1 & b & 0 & 0 \\ 0 & c & 1 & c & 0 \\ 0 & 0 & b & 1 & d \\ 0 & 0 & 0 & a & 1 \end{pmatrix}.$$

6.16. Calcolare i determinanti delle seguenti matrici

$$\begin{pmatrix} 1 & 1 & 1 \\ a & b & c \\ a^n & b^n & c^n \end{pmatrix}, \begin{pmatrix} 1 & 1 & 1 \\ a^m & b^m & c^m \\ a^n & b^n & c^n \end{pmatrix}, \begin{pmatrix} 1 & 1 & 1 & 1 \\ a & b & c & d \\ a^m & b^m & c^m & d^m \\ a^n & b^n & c^n & d^n \end{pmatrix}.$$

6.17. Calcolare i determinanti delle seguenti matrici

$$\begin{pmatrix} 0 & a \\ b & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & a \\ 0 & b & 0 \\ c & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 0 & a \\ 0 & 0 & b & 0 \\ 0 & c & 0 & 0 \\ d & 0 & 0 & 0 \end{pmatrix}.$$

e in generale calcolare il determinante di matrici che hanno entrate non nulle solo sulla antidiagonale principale (cioè nelle posizioni $(i, n+1-i)$ se n è l'ordine della matrice).

6.18. Calcolare i determinanti delle seguenti matrici

$$\begin{pmatrix} 0 & a \\ b & 0 \end{pmatrix}, \begin{pmatrix} 0 & a & b \\ c & 0 & d \\ e & f & 0 \end{pmatrix}, \begin{pmatrix} 0 & a & b & c \\ d & 0 & e & f \\ g & h & 0 & i \\ l & m & n & 0 \end{pmatrix}, \begin{pmatrix} 0 & a & b & c \\ 1 & 0 & d & e \\ 1 & 1 & 0 & f \\ 1 & 1 & 1 & 0 \end{pmatrix}.$$

6.19. Calcolare i determinanti delle seguenti matrici

$$\begin{pmatrix} a & b \\ c & a \end{pmatrix}, \begin{pmatrix} a & b & c \\ d & e & b \\ f & d & a \end{pmatrix}, \begin{pmatrix} a & b & c & d \\ e & f & g & c \\ h & i & f & b \\ l & h & e & a \end{pmatrix}.$$

6.20. Calcolare i determinanti delle seguenti matrici

$$\begin{pmatrix} a & 0 \\ 0 & -a \end{pmatrix}, \begin{pmatrix} a & b & 0 \\ c & 0 & -b \\ 0 & -c & -a \end{pmatrix}, \begin{pmatrix} a & b & c & 0 \\ d & e & 0 & -c \\ f & 0 & -e & -b \\ 0 & -f & -d & -a \end{pmatrix}.$$

e in generale discutere il determinante di matrici che sono “antisimmetriche” rispetto alla antidiagonale (cioè tali che $a_{i,j} = -a_{n+1-j,n+1-i}$ se n è l'ordine della matrice).

6.21. Calcolare i determinanti delle seguenti matrici

$$\begin{pmatrix} a & b \\ b & a \end{pmatrix}, \begin{pmatrix} a & b & c \\ c & a & b \\ b & c & a \end{pmatrix}, \begin{pmatrix} a & b & c & d \\ d & a & b & c \\ c & d & a & b \\ b & c & d & a \end{pmatrix}.$$

6.22. Sia $A \in M_n(C)$ una matrice tale che $A^t A = \mathbb{I}_n$; dimostrare che $\det A = \pm 1$. È vero il viceversa?

Sia $A \in M_n(C)$ una matrice tale che $A^t P A = P$ con $P \in GL_n(C)$; dimostrare che $\det A = \pm 1$.

6.23. Siano $A, B \in M_n(C)$; mostrare che AB è invertibile se e solo se A e B sono invertibili. Generalizzare ad un numero finito di matrici.

Interpretare e ridimostrare il risultato in termini di applicazioni lineari.

6.24. Supponiamo $A \in M_n(C)$ matrice invertibile. Mostrare che $A + A^{-1}$ è invertibile se e solo se $\mathbb{I}_n + A^2$ è invertibile. È sempre vero che $A + A^{-1}$ è invertibile?

6.25. Usando la formula di Vandermonde, calcolare il determinante

$$\det \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & x & x^2 & \cdots & x^k \\ 1 & x^2 & x^4 & \cdots & x^{2k} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x^k & x^{2k} & \cdots & x^{k^2} \end{pmatrix}$$

e dire quando la matrice è degenere. Provare a calcolare l'inversa di questa matrice, se essa è invertibile.

6.26. Calcolare il determinante

$$\det \begin{pmatrix} 1 & \binom{x_1}{1} & \binom{x_1}{2} & \cdots & \binom{x_1}{n-1} \\ 1 & \binom{x_2}{1} & \binom{x_2}{2} & \cdots & \binom{x_2}{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \binom{x_n}{1} & \binom{x_n}{2} & \cdots & \binom{x_n}{n-1} \end{pmatrix}$$

(le entrate della matrice sono i "coefficienti binomiali" $\binom{x}{i} = \frac{x(x-1)\cdots(x-i+1)}{i!}$, che sono polinomi in x).

6.27. Calcolare il determinante

$$\det \begin{pmatrix} 1 & f_1(x_1) & f_2(x_1) & \cdots & f_{n-1}(x_1) \\ 1 & f_1(x_2) & f_2(x_2) & \cdots & f_{n-1}(x_2) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & f_1(x_n) & f_2(x_n) & \cdots & f_{n-1}(x_n) \end{pmatrix}$$

ove $f_i(x)$ sono polinomi nella variabile x .

6.28. Dimostrare che ogni matrice di rango r si può scrivere come somma di r matrici di rango 1; viceversa, è vero che la somma di r matrici di rango 1 dà una matrice di rango r ?

6.29. PRINCIPIO DEI MINORI ORLATI. Sia $A \in M_n(C)$ una matrice avente un minore non nullo di ordine k , e sia $B \in M_k(C)$ la sottomatrice di A che dà quel minore. Dimostrare che se tutti i minori di ordine $k+1$ ottenuti da sottomatrici di A contenenti B sono nulli, allora la matrice A ha rango esattamente k (principio dei minori orlati).

6.30. PRINCIPIO DEI MINORI ORLATI ED EQUAZIONI DI SOTTOSPAZI. Mostrare che il sottospazio W di $V_n(C)$ generato dai vettori linearmente indipendenti v_1, v_2, \dots, v_m ha equazioni cartesiane ottenute annullando i minori d'ordine $m+1$ della matrice

$$A = \begin{pmatrix} X_1 & & & \\ \vdots & v_1 & \cdots & v_m \\ X_n & & & \end{pmatrix}$$

in $M_{n,m+1}(C[X_1, \dots, X_n])$. Si mostri inoltre che, detta B la matrice in $M_{n,m}(C)$ le cui colonne siano i vettori dati e scelto un minore non nullo d'ordine m di B , per descrivere W è sufficiente (e necessario) annullare i minori d'ordine $m+1$ di A che contengono la sottomatrice di B relativa al minore scelto (principio dei minori orlati).

Usando il principio di cui sopra, si diano equazioni cartesiane per i seguenti sottospazi di $V_3(C)$ o $V_4(C)$:

$$\langle \begin{pmatrix} 1 \\ 2 \\ 1 \end{pmatrix} \rangle, \langle \begin{pmatrix} 1 \\ 2 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \rangle, \langle \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}, \begin{pmatrix} 3 \\ 2 \\ 1 \end{pmatrix} \rangle, \langle \begin{pmatrix} 1 \\ 0 \\ 1 \\ 2 \end{pmatrix} \rangle, \langle \begin{pmatrix} 1 \\ 0 \\ 1 \\ 2 \end{pmatrix}, \begin{pmatrix} 1 \\ -1 \\ 1 \end{pmatrix} \rangle, \langle \begin{pmatrix} 1 \\ 0 \\ 1 \\ 2 \end{pmatrix}, \begin{pmatrix} 1 \\ -1 \\ 1 \\ 2 \end{pmatrix}, \begin{pmatrix} 1 \\ -1 \\ 0 \\ 0 \end{pmatrix} \rangle.$$

6.31. Sviluppando il prodotto di determinanti

$$\det \begin{pmatrix} a & -b & -c & -d \\ b & a & -d & c \\ c & d & a & -b \\ d & -c & b & a \end{pmatrix} \det \begin{pmatrix} x & -y & -z & -t \\ y & x & -t & z \\ z & t & x & -y \\ t & -z & y & x \end{pmatrix}$$

discutere dell'identità dei quattro quadrati di Eulero (il prodotto di due somme di quattro quadrati è una somma di quattro quadrati; per la somma di uno o di due quadrati è facile).

6.32. Discutere il rango delle matrici in funzioni dei parametri:

$$\begin{pmatrix} 1 & 1 & x-y & 1+x \\ 1 & 2+x & 1+x & 1+x \\ 1 & x+1 & y & 1 \\ -1 & -1 & x-y & x-1 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 3 & 1 & xy-y \\ 2 & 2 & xy-x & x+2 \\ 2 & 4 & 1 & xy-y+1 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 0 & x^2-x \\ 1 & 1 & 1 & 1 \\ 1 & xy-x & xy-x+1 & x \\ -1+x-x^2 & x-x^2 & -1+x-x^2 & 0 \end{pmatrix}.$$

6.33. Calcolare i determinanti delle seguenti matrici:

$$\begin{pmatrix} 1 & 1 & 3 & 4 \\ 2 & 0 & 0 & 8 \\ 3 & 0 & 0 & 2 \\ 4 & 4 & 7 & 5 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 1 & 2 & 3 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 \\ 0 & a & b & c & d \\ 0 & a^2 & b^2 & c^2 & d^2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 3 \\ 6 & 5 & 7 & 8 & 4 & 2 \\ 9 & 8 & 6 & 7 & 0 & 0 \\ 3 & 2 & 4 & 5 & 0 & 0 \\ 3 & 4 & 0 & 0 & 0 & 0 \\ 5 & 6 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

6.34. Calcolare i determinanti delle matrici:

$$\begin{pmatrix} 1 & 2 \\ 2 & 3 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 4 \\ 3 & 4 & 5 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 6 \\ 4 & 5 & 6 & 7 \end{pmatrix},$$

e generalizzare.

6.35. Calcolare i determinanti delle matrici:

$$\begin{pmatrix} 1 & 4 \\ 4 & 9 \end{pmatrix}, \quad \begin{pmatrix} 1 & 4 & 9 \\ 4 & 9 & 16 \\ 9 & 16 & 25 \end{pmatrix}, \quad \begin{pmatrix} 1 & 4 & 9 & 16 \\ 4 & 9 & 16 & 25 \\ 9 & 16 & 25 & 36 \\ 16 & 25 & 36 & 49 \end{pmatrix}.$$

6.36. Discutere i sistemi lineari di matrici complete:

$$\begin{pmatrix} 1 & b & 1 & 1 \\ 1 & ab & 1 & b \\ 1 & b & a & 1 \end{pmatrix}, \quad \begin{pmatrix} a & b & 2 & 1 \\ a & 2b-1 & 3 & 1 \\ a & b & b+3 & 2b-1 \end{pmatrix}, \quad \begin{pmatrix} 2a+2 & 3 & a & a+4 \\ 4a-1 & a+1 & 2a-1 & 2a+2 \\ 5a-4 & a+1 & 3a-4 & a-1 \end{pmatrix}.$$

6.37. Quante somme e prodotti è necessario fare in linea di principio per calcolare un determinante d'ordine n (tramite la formula delle permutazioni)? E tramite le formule di Laplace? E tramite riduzione di Gauss?

6.38. Scrivere il determinante della matrice $A + B$, ove A e B sono matrici d'ordine n e B ha rango 1, come la somma di $n + 1$ determinanti di matrici d'ordine n .

6.39. Si consideri l'applicazione φ di $M_3(\mathbb{R})$ in sè che manda la generica matrice $\begin{pmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{pmatrix}$

nella matrice $\begin{pmatrix} a_1b_2 - a_2b_1 & a_1c_2 - a_2c_1 & b_1c_2 - b_2c_1 \\ a_1b_3 - a_3b_1 & a_1c_3 - a_3c_1 & b_1c_3 - b_3c_1 \\ a_2b_3 - a_3b_2 & a_2c_3 - a_3c_2 & b_2c_3 - b_3c_2 \end{pmatrix}$.

Verificare che $\varphi(\mathbb{I}_3) = \mathbb{I}_3$, $\varphi(\alpha A) = \alpha^2 \varphi(A)$ e che $\varphi(AB) = \varphi(A)\varphi(B)$.

Dimostrare che:

- (a) $\text{rk}\varphi(A) = 0$ se e solo se $\text{rk}(A) \leq 1$;
- (b) $\text{rk}\varphi(A) = 1$ se e solo se $\text{rk}(A) = 2$;
- (c) $\text{rk}\varphi(A) = 3$ se e solo se $\text{rk}(A) = 3$.

Capitolo V

Forme canoniche

Come ormai dovrebbe essere chiaro al lettore, noi intendiamo occuparci di proprietà intrinseche degli spazi vettoriali e delle applicazioni lineari, mentre per svolgere dei calcoli espliciti abbiamo bisogno di fare alcune scelte arbitrarie (generalmente scelte di basi per gli spazi vettoriali e tradurre i problemi in forma matriciale). D'altra parte, siccome queste scelte sono arbitrarie, conviene farle in modo che il problema in questione ottenga una forma matriciale semplice. Per esempio se si vuole studiare una applicazione lineare, converrebbe scegliere una base in cui la matrice associata sia il più semplice possibile, per esempio triangolare o diagonale. In questo capitolo ci occuperemo in modo sistematico di questo tipo di problemi.

In tutto questo capitolo C sarà un corpo arbitrario, a meno che non sia specificato altrimenti.

1. Equivalenza di matrici.

1.1. DEFINIZIONE (EQUIVALENZA DI MATRICI). Due matrici $A, B \in M_{m,n}(C)$ si dicono equivalenti (in C) se esistono due matrici invertibili $P \in \text{GL}(n, C)$ e $Q \in \text{GL}(m, C)$ tali che $B = QAP$. Due matrici sono equivalenti se e solo se rappresentano la stessa applicazione lineare di $V_n(C)$ in $V_m(C)$ con la scelta di diverse basi nei due spazi (legate dai cambiamenti di base dati da P su $V_n(C)$ e Q su $V_m(C)$).

La relazione di equivalenza è una relazione di equivalenza tra matrici, come si verifica subito (sic).

1.2. PROBLEMA. Fare una classificazione per equivalenza delle matrici significa identificare le classi di equivalenza delle matrici secondo la relazione di equivalenza, e possibilmente per ogni classe identificare un rappresentante (il più semplice possibile).

Dal punto di vista delle applicazioni lineari di $V_n(C)$ in $V_m(C)$, si tratta di rappresentare un morfismo tramite una matrice semplice, scegliendo opportunamente le basi dei due spazi.

1.3. TEOREMA (IL RANGO CLASSIFICA LE MATRICI PER EQUIVALENZA). Due matrici a coefficienti in un corpo sono equivalenti se e solo se hanno lo stesso rango r , e in tal caso sono equivalenti alla matrice le cui entrate sono tutte nulle, tranne le entrate nelle posizioni $(1, 1), (2, 2), \dots, (r, r)$ tutte uguali ad 1, ovvero la matrice a blocchi

$$\begin{pmatrix} \mathbb{I}_r & \mathbb{O}_{r,n-r} \\ \mathbb{O}_{m-r,r} & \mathbb{O}_{m-r,n-r} \end{pmatrix}$$

(detta rappresentante canonico di quella classe di equivalenza).

DIMOSTRAZIONE. Si possono pensare due dimostrazioni del risultato.

La prima consiste nell'usare la tecnica di riduzione di Gauss, operando prima sulle righe e successivamente sulle colonne della matrice (oppure in ordine inverso), ed è chiaro che la matrice può essere ridotta come affermato; inoltre un opportuno prodotto di matrici elementari dà le matrici P e Q invertibili che rendono la matrice equivalente alla forma canonica.

La seconda consiste nella scelta opportuna di basi in $V_n(C)$ e $V_m(C)$ adattate al morfismo $\varphi : V_n(C) \rightarrow V_m(C)$ rappresentato, nelle basi canoniche, dalla matrice data. Dapprima si sceglie una base di $\ker \varphi$ e la si estende ad una base di $V_n(C)$; poi come base su $V_m(C)$ si sceglie quella formata dalle immagini dei vettori scelti come base in $V_n(C)$ che non appartenevano a $\ker \varphi$, eventualmente completandola arbitrariamente. Allora è chiaro che la matrice di φ in queste nuove basi (opportunamente ordinate) diventa quella canonica detta. \square

2. Similitudine di matrici.

Nel caso di matrici quadrate, interpretate in termini di applicazioni lineari da $V_n(C)$ in sé stesso, siamo interessati ad usare la stessa base nel dominio e nel codominio; quindi diamo la seguente definizione.

2.1. DEFINIZIONE (SIMILITUDINE DI MATRICI.). Due matrici quadrate $A, B \in M_n(C)$ si dicono simili (in C) se esiste una matrice invertibile $P \in GL(n, C)$ tale che $B = P^{-1}AP$. Due matrici sono simili se e solo se rappresentano la stessa applicazione lineare di $V_n(C)$ in sé in due basi diverse (legate dal cambiamento di base dato da P).

La relazione di similitudine è una relazione di equivalenza tra matrici, come si verifica subito.

2.1.1. La matrice identica e la matrice nulla sono simili solamente a sé stesse. Quali sono le matrici che hanno questa proprietà (la loro classe di similitudine è ridotta ad un elemento)?

2.1.2. Due matrici diagonali non sono necessariamente simili tra di loro; caratterizzare i casi in cui lo sono, e farsi degli esempi.

2.1.3. Se due matrici sono simili, allora sono anche equivalenti, mentre il viceversa è falso; dunque la relazione di similitudine è più fine (o meno grossolana) della relazione di equivalenza tra matrici.

2.1.4. La similitudine dipende dal corpo C , nel senso che le classi di similitudine dipendono dal corpo C , ma solo perché estendendo il corpo le classi di similitudine possono avere più elementi (e anche elementi più semplici), ma non capita mai che due matrici in C possano diventare simili in $C' \supseteq C$ senza che lo fossero già in C . Questo risultato è però di difficile dimostrazione, e non verrà qui né dimostrato, né utilizzato.

2.2. PROBLEMA. Fare una classificazione per similitudine delle matrici significa identificare le classi di equivalenza delle matrici secondo la relazione di similitudine, e possibilmente per ogni classe identificare un rappresentante (il più semplice possibile).

Dal punto di vista delle applicazioni lineari di $V_n(C)$ in sé, si tratta di rappresentare un morfismo tramite una matrice semplice, scegliendo opportunamente una base dello spazio.

2.3. DEFINIZIONE (DIAGONALIZZABILITÀ E TRIANGOLARIZZABILITÀ). Una matrice $A \in M_n(C)$ si dice diagonalizzabile (risp. triangolarizzabile) in C se è simile (in C) ad una matrice diagonale (risp. triangolare), cioè se esistono $P \in GL(n, C)$ e $\Delta \in M_n(C)$ diagonale tale che $A = P^{-1}\Delta P$ (risp. e $T \in M_n(C)$ triangolare tale che $A = P^{-1}TP$).

Una applicazione lineare φ di V in sé si dice diagonalizzabile (risp. triangolarizzabile) in C se esiste una base di V tale che la matrice di φ in quella base sia diagonale (risp. triangolare).

3. Autoteoria.

3.1. DEFINIZIONE (AUTOVALORI E AUTOVETTORI). Sia $\varphi : V \rightarrow V$ un endomorfismo di uno spazio vettoriale V . Un vettore non nullo $v \in V$ si dice un autovettore di φ di autovalore $\lambda \in C$ se $\varphi(v) = \lambda v$, e $\lambda \in C$ si dice un autovalore di φ se esiste un vettore $v \in V$ non nullo tale che $\varphi(v) = \lambda v$.

Sia $A \in M_n(C)$ una matrice; autovalori e autovettori di A per definizione sono quelli della applicazione lineare di $V = V_n(C)$ in sé a cui è associata la matrice A nella base canonica. Dunque $v \in V_n(C)$ non nullo (che confonderemo con le sue coordinate in base canonica) si dice autovettore di A di autovalore $\lambda \in C$ se $Av = \lambda v$, e $\lambda \in C$ si dice un autovalore di A se esiste un vettore $v \in V_n(C)$ non nullo tale che $Av = \lambda v$.

L'insieme degli autovalori di A (o di φ) si chiama spettro di A (o di φ).

Per un fissato autovalore λ , l'insieme di tutti gli autovettori di autovalore λ forma un sottospazio vettoriale di V , detto autospazio di λ e che si indica con $V_\lambda(A)$ (o $V_\lambda(\varphi)$).

3.1.1. Lo spettro di una matrice diagonale è formato dagli elementi che compaiono nella diagonale. I vettori della base canonica di $V_n(C)$ sono autovettori.

3.1.2. Gli autovettori di autovalore 0 sono gli elementi di $\ker \varphi$. Gli autovettori di autovalore 1 sono gli elementi mandati da φ in sé stessi; dunque l'autospazio di 1 è il più grande sottospazio di V in cui φ si restringe all'identità. Gli autovettori di autovalore -1 ?

3.1.3. CRITERIO BANALE DI DIAGONALIZZABILITÀ. È un fatto evidente che una matrice è diagonalizzabile se e solo se $V_n(C)$ ammette una base fatta di autovettori per la matrice. Equivalentemente, un endomorfismo di V è diagonalizzabile se e solo se V ammette una base di autovettori per quell'endomorfismo.

3.2. PROPOSIZIONE (INTERSEZIONE DI AUTOSPAZI). *Autospazi relativi ad autovalori distinti hanno intersezione nulla. In particolare autovettori relativi ad autovalori distinti sono linearmente indipendenti.*

DIMOSTRAZIONE. Sia $v \in V_\lambda(\varphi) \cap V_\mu(\varphi)$ con $\lambda \neq \mu$. Allora abbiamo $\lambda v = \varphi(v) = \mu v$ da cui $(\lambda - \mu)v = 0$, e poiché $\lambda - \mu \neq 0$ abbiamo $v = 0$.

La seconda affermazione è allora chiara (per esempio dalla formula di Grassmann). \square

3.3. TEOREMA (CRITERIO PER AUTOVALORI). *Uno scalare $\lambda \in C$ è un autovalore di $A \in M_n(C)$ (risp. di $\varphi \in \text{End}(V)$) se e solo se $\det(A - \lambda \mathbb{I}_n) = 0$ (risp. $\ker(\varphi - \text{id}_V) \neq 0$).*

DIMOSTRAZIONE. Per definizione $\lambda \in C$ è un autovalore di $A \in M_n(C)$ se e solo se esiste $v \in V_n(C)$ non nullo con $Av = \lambda v$, cioè $(A - \lambda \mathbb{I}_n)v = 0$ e questo significa che il sistema omogeneo di matrice $A - \lambda \mathbb{I}_n$ ha una soluzione non nulla, e ciò equivale a che la matrice abbia determinante nullo. \square

3.4. DEFINIZIONE-TEOREMA (POLINOMIO CARATTERISTICO). *Il polinomio caratteristico di $A \in \mathcal{M}_n(C)$ è*

$$p_A(X) := \det(X\mathbb{I}_n - A) .$$

Si tratta di un polinomio monico di grado n , è invariante per similitudine, e dunque si può chiamare anche polinomio caratteristico $p_\varphi(X)$ di φ . Uno scalare $\lambda \in C$ è un autovalore di A (o di φ) se e solo se è zero del polinomio $p_A(x)$.

Si dice che A (o φ) ha tutti i suoi autovalori in C se il polinomio caratteristico $p_A(X)$ si fattorizza in fattori lineari in $C[X]$.

DIMOSTRAZIONE. Mostriamo l'invarianza per similitudine: se $B = P^{-1}AP$ allora

$$\begin{aligned} p_B(X) &= \det(X\mathbb{I}_n - B) \\ &= \det(X\mathbb{I}_n - P^{-1}AP) \\ &= \det(P^{-1}(X\mathbb{I}_n - A)P) \\ &= \det(P)^{-1} \det(X\mathbb{I}_n - A) \det(P) \\ &= p_A(X) . \end{aligned}$$

L'altra affermazione è chiara in base al criterio precedente. \square

3.4.1. In particolare, tutti i coefficienti del polinomio caratteristico di una matrice sono invarianti per similitudine; il primo e l'ultimo sono particolarmente importanti:

$$p_A(X) = X^n - \text{tr}(A)X^{n-1} + \dots + (-1)^n \det(A)$$

ove $\text{tr}(A)$ per definizione è la somma dei termini nella diagonale principale di A .

3.4.2. Conseguenza fondamentale del teorema precedente è che lo spettro di ogni matrice (e di ogni automorfismo) è finito: si tratta degli zeri di un polinomio di grado n a coefficienti in C , e dunque un insieme con al più n elementi.

3.4.3. Gli autovalori di una matrice triangolare sono tutti e soli i suoi elementi diagonali. Dunque una matrice triangolare ha tutti i suoi autovalori in C .

3.4.4. TRACCIA. Dal teorema sappiamo ancora che la traccia $\text{tr}(A)$ di una matrice è un invariante per similitudine (dunque possiamo anche parlare di traccia di una applicazione lineare), e di tratta di una applicazione lineare $\text{tr} : M_n(C) \rightarrow C$, cioè $\text{tr}(A + B) = \text{tr}(A) + \text{tr}(B)$, e $\text{tr}(\alpha A) = \alpha \text{tr}(A)$. In generale non è moltiplicativa, ovvero $\text{tr}(AB) \neq \text{tr}(A)\text{tr}(B)$ (farsi degli esempi).

3.5. TEOREMA (CRITERIO DI TRIANGOLARIZZABILITÀ). Una matrice $A \in M_n(C)$ è simile (in C) a una matrice in forma triangolare se e solo se ha tutti i suoi autovalori in C .

Una applicazione lineare è triangolarizzabile se e solo se ha tutti i suoi autovalori in C .

DIMOSTRAZIONE. Il “solo se” è già stato osservato prima. Resta da dimostrare il “se”; supponiamo dunque che A abbia tutti i suoi autovalori in C e procediamo per induzione su n .

Se $n = 1$ tutte le matrici sono triangolari (e anzi diagonali), e non c'è nulla da dimostrare. Supponiamo allora $n > 1$, e il teorema vero per matrici di ordine $n-1$. Sia λ un autovalore, e $v \in V_n(C)$ un autovettore relativo a λ . Scelta una base di $V_n(C)$ il cui primo vettore è v , abbiamo che, posto P la matrice invertibile di cambiamento di base dalla base canonica alla nuove, risulta

$$P^{-1}AP = \begin{pmatrix} \lambda & b \\ 0 & B \end{pmatrix}$$

ove $B \in M_{n-1}(C)$. Per l'invarianza del polinomio caratteristico abbiamo $p_A(X) = (X - \lambda)p_B(X)$, e dunque la matrice B ha tutti i suoi autovalori nel corpo C (sono esattamente quelli di A , tranne una occorrenza di λ). Dunque per ipotesi induttiva, esiste $Q \in \text{GL}_{n-1}(C)$ tale che $Q^{-1}BQ = T$ è matrice triangolare superiore. Di conseguenza abbiamo:

$$\begin{pmatrix} 1 & 0 \\ 0 & Q \end{pmatrix}^{-1} P^{-1}AP \begin{pmatrix} 1 & 0 \\ 0 & Q \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & Q^{-1} \end{pmatrix} \begin{pmatrix} \lambda & b \\ 0 & B \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & Q \end{pmatrix} = \begin{pmatrix} \lambda & b' \\ 0 & T \end{pmatrix}$$

e il risultato è una matrice triangolare superiore. \square

3.5.1. In particolare quindi, se C è un corpo algebricamente chiuso (ogni polinomio in $C[X]$ ha tutte le sue radici nel corpo) allora ogni matrice in $M_n(C)$ è triangolarizzabile in C . D'altra parte, se il corpo non è algebricamente chiuso esistono matrici che non sono triangolarizzabili su quel corpo (ma lo sono in una chiusura algebrica): farsi qualche esempio usando come corpi \mathbb{Q} (suggerimento: studiare la matrice $\begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix}$) e \mathbb{R} (suggerimento: studiare la matrice $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$).

3.6. DEFINIZIONE-TEOREMA (MOLTEPLICITÀ E NULLITÀ). Ad ogni autovalore λ (di una matrice $A \in M_n(C)$ o di una applicazione lineare $\varphi \in \text{End}_C(V)$) restano associati due numeri interi positivi $M(\lambda)$ e $N(\lambda)$ così definiti:

- (1) $M(\lambda)$ si dice la molteplicità (o molteplicità algebrica) di λ , ed è la molteplicità di λ in quanto radice del polinomio caratteristico.
- (2) $N(\lambda)$ si dice la nullità (o molteplicità geometrica) di λ , ed è la dimensione del sottospazio degli autovettori associati a λ ; dunque $N(\lambda) := \dim_C \ker(\varphi - \lambda \text{id}_V) = n - \text{rk}(A - \lambda \mathbb{I}_n)$.

In generale, per ogni autovalore λ si ha $M(\lambda) \geq N(\lambda)$.

DIMOSTRAZIONE. Sia $m = N(\lambda)$; allora possiamo trovare un sistema di m autovettori per φ di autovalore λ linearmente indipendenti, diciamo v_1, \dots, v_m . Completando ad una base v_1, \dots, v_n di V , vediamo che la matrice di φ in questa base si scrive a blocchi:

$$A' = \begin{pmatrix} \lambda \mathbb{I}_m & B \\ 0 & C \end{pmatrix}$$

e calcolando il polinomio caratteristico si ha

$$p_{A'}(X) = \det(X\mathbb{I}_n - A') = \det(X\mathbb{I}_m - \lambda\mathbb{I}_m) \det(X\mathbb{I}_{n-m} - C) = (X - \lambda)^m \det(X\mathbb{I}_{n-m} - C)$$

da cui si vede che $M(\lambda) \geq m$. \square

3.7. TEOREMA (PRIMO CRITERIO DI DIAGONALIZZABILITÀ). Una matrice $A \in M_n(C)$ (risp. un endomorfismo $\varphi \in \text{End}_C(V)$ di uno spazio vettoriale V di dimensione n su C) è simile (in C) a una matrice in forma diagonale (risp. è diagonalizzabile in C) se e solo se ha tutti i suoi autovalori in C e ogni autovalore ha molteplicità e nullità uguali.

DIMOSTRAZIONE. Il “solo se” è chiaro: se una matrice è diagonalizzabile il polinomio caratteristico è uguale a quello di una matrice diagonale, e gli autovalori sono esattamente i termini nella diagonale. Inoltre, per ogni autovalore, l'autospazio corrispondente è generato dai vettori della base diagonalizzante corrispondenti alle occorrenze dell'autovalore nella diagonale, quindi in numero uguale alla nullità dell'autovalore.

Viceversa, si scelga su $V = V_n(C)$ l'insieme costituito giustappo-
nendo le basi degli autospazi relativi agli autovalori dati: per l'ipotesi fatta, si tratta di esattamente n elementi, ed è un insieme linearmente indipendente (si ricordi che autospazi relativi ad autovalori distinti hanno intersezione nulla), e dunque di una base. Sia P la matrice di cambiamento di base (dalla base di autovettori a quella iniziale); allora è chiaro che $P^{-1}AP$ è una matrice diagonale. \square

3.7.1. In particolare quindi, anche se C è un corpo algebricamente chiuso non è detto che allora ogni matrice in $M_n(C)$ sia diagonalizzabile in C . Farsi degli esempi usando il corpo complesso \mathbb{C} (si consideri per esempio la matrice $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$).

3.8. TEOREMA (HAMILTON-CAYLEY). Consideriamo le applicazioni di C -algebre

$$ev_A : C[X] \longrightarrow M_n(C) \quad e \quad ev_\varphi : C[X] \longrightarrow \text{End}_C(V)$$

(“valutazione in A ” e “valutazione in φ ”) definita mandando ogni polinomio $P(X)$ nella matrice $P(A)$ ottenuta sostituendo X con A e nell'endomorfismo $P(\varphi)$ ottenuta sostituendo X con φ .

Abbiamo allora $p_A(A) = 0$, e $p_\varphi(\varphi) = 0$. In altri termini, il polinomio caratteristico annulla la corrispondente matrice (o il corrispondente endomorfismo).

DIMOSTRAZIONE. Vi sono varie dimostrazioni possibili per questo risultato. Cominciamo da una *dimostrazione sbagliata*:

$$p_A(A) = \det(A\mathbb{I}_n - A) = \det(\mathbb{O}_n) = 0 ;$$

dov'è lo sbaglio?

Dimostrazione usando la *triangolarizzabilità*. Si osservi che possiamo sostituire il corpo C con una sua estensione C' senza che siano alterati la matrice ed il polinomio caratteristico. Dunque possiamo supporre che C contenga tutte le radici di $p_A(X)$, e di conseguenza che A sia triangolarizzabile. Siano allora $p_A(X) = \prod_i (X - \alpha_i)$ il polinomio caratteristico di A , e P una matrice invertibile tale che $P^{-1}AP = T$ matrice triangolare superiore avente sulla diagonale ordinatamente gli elementi $\alpha_1, \dots, \alpha_n$. Definiamo $V_i = \langle e_1, \dots, e_i \rangle$ i sottospazi di $V = V_n(C)$ generati dai primi i vettori della base canonica (dunque $V_0 = 0$ e $V_n = V$). Notiamo allora che si ha $(T - \alpha_i)V_i \subseteq V_{i-1}$ per ogni $i = 1, \dots, n$. Abbiamo allora

$$\begin{aligned} p_T(T)V &= (T - \alpha_1) \cdots (T - \alpha_{n-1})(T - \alpha_n)V_n \\ &\subseteq (T - \alpha_1) \cdots (T - \alpha_{n-1})V_{n-1} \\ &\subseteq \cdots \\ &\subseteq (T - \alpha_1) \cdots (T - \alpha_i)V_i \\ &\subseteq \cdots \\ &\subseteq (T - \alpha_1)V_1 = 0 \end{aligned}$$

da cui concludiamo che $p_T(T) = 0$. Di conseguenza $p_A(A) = p_A(PTP^{-1}) = Pp_T(T)P^{-1} = 0$, come si voleva.

Dimostrazione usando il *calcolo con matrici polinomiali*. Osserviamo prima che se $p_A(X) = \sum_i p_i X^i$ allora

$$\begin{aligned} p_A(X)\mathbb{I}_n - p_A(A) &= \sum_i p_i (X^i \mathbb{I}_n - A^i) \\ &= \sum_i p_i (X\mathbb{I}_n - A)(X^{i-1}\mathbb{I}_n + X^{i-2}\mathbb{I}_n A + \cdots + X\mathbb{I}_n A^{i-2} + A^{i-1}) \\ &= (X\mathbb{I}_n - A) \sum_i p_i (X^{i-1}\mathbb{I}_n + X^{i-2}\mathbb{I}_n A + \cdots + X\mathbb{I}_n A^{i-2} + A^{i-1}) \\ &= (X\mathbb{I}_n - A)Q(X) \end{aligned}$$

ove $Q(X)$ è un polinomio a coefficienti in $M_n(C)$. Ora usando la matrice dei complementi algebrici di $(X\mathbb{I}_n - A)$ abbiamo

$$\begin{aligned} p_A(A) &= p_A(X)\mathbb{I}_n - (X\mathbb{I}_n - A)Q(X) \\ &= (X\mathbb{I}_n - A)(X\mathbb{I}_n - A)^c - (X\mathbb{I}_n - A)Q(X) \\ &= (X\mathbb{I}_n - A)((X\mathbb{I}_n - A)^c - Q(X)) \\ &= (X\mathbb{I}_n - A)R(X) \end{aligned}$$

ove $R(X)$ è un polinomio a coefficienti in $M_n(C)$. Siccome sul lato sinistro abbiamo una matrice a coefficienti in C , si deduce che $R(X) = 0$ (perché?), e dunque anche $p_A(A) = 0$. \square

3.8.1. Si osservi per inciso che l'immagine dell'algebra dei polinomi tramite ev_A dà luogo ad una sottoalgebra commutativa dell'algebra delle matrici.

3.8.2. Inoltre, che l'applicazione lineare ev_A debba avere un nucleo non banale discende a priori da una pura considerazione sulle dimensioni: $\dim_C C[X] = \aleph_0 > n^2 = \dim_C \text{End}_C(V)$: esplicitare l'argomento.

3.8.3. Una piccola applicazione del teorema di Hamilton-Cayley è la seguente: se la matrice A è invertibile, allora la matrice inversa si scrive come polinomialmente in A , ovvero esiste un polinomio $F(X)$ tale che $A^{-1} = F(A)$.

3.9. DEFINIZIONE (POLINOMIO MINIMO). *Il polinomio minimo di A (o di φ) è il generatore monico dell'ideale $\ker(ev_A)$ di $C[X]$ formato dai polinomi che annullano A (o φ). Il teorema di Hamilton-Cayley dice allora che il polinomio minimo divide il polinomio caratteristico.*

3.9.1. Si può subito dimostrare in effetti che polinomio caratteristico e polinomio minimo hanno le stesse radici in (una chiusura algebrica di) C , e il teorema di Hamilton-Cayley dice che le molteplicità algebriche sono minori o uguali per il polinomio minimo rispetto a quello caratteristico.

3.10. PROBLEMA: DIAGONALIZZAZIONE SIMULTANEA. Due matrici A e B sono simultaneamente diagonalizzabili (i.e. esiste $P \in \text{GL}(n, C)$ tale che $P^{-1}AP$ e $P^{-1}BP$ sono entrambe diagonali) se e solo se sono (separatamente) diagonalizzabili e commutano tra loro (i.e. $AB = BA$, nel qual caso ciascuna delle due matrici è stabile sugli autospazi dell'altra).

Generalizzare ad un numero finito di matrici.

3.11. PROBLEMA CURIOSO. Consideriamo $\mathbf{A} \in M_n(M_m(C))$; cioè \mathbf{A} è una matrice d'ordine n le cui entrate sono matrici $A_{i,j} \in M_m(C)$ d'ordine m , e supponiamo che tutte queste matrici commutino tra loro (a due a due): diciamo che \mathbf{A} è una matrice a blocchi quadrati commutanti. Sia $A \in M_{mn}(C)$ la matrice che si ottiene da \mathbf{A} "dimenticando la divisione in blocchi". Allora vale che $\det(\det(\mathbf{A})) = \det(A)$ (a sinistra, si noti che $\det(\mathbf{A}) \in M_m(C)$, cioè è una matrice).

3.12. PROBLEMA: PRODOTTO DI MATRICI. Se almeno una tra due matrici A e B (quadrate dello stesso ordine) è invertibile, allora AB è simile a BA (dunque AB hanno BA gli stessi polinomi caratteristico e minimo). In generale (senza alcuna ipotesi) resta vero che AB e BA hanno gli stessi autovalori. Questi hanno le stesse molteplicità? E le stesse nullità? Si consideri l'esempio $A = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$ e $B = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$.

3.13. PROBLEMA. Siano A e B matrici quadrate dello stesso ordine n ; consideriamo l'applicazione $\psi_{A,B}: M_n(C) \rightarrow M_n(C)$ data da $\psi_{A,B}(X) = AX - XB$. Si verifichi che si tratta di una applicazione lineare, i cui autovalori sono le differenze tra gli autovalori di A e quelli di B . Precisamente, se v è un autovettore di A relativo all'autovalore α e w è un autovettore di B^t relativo all'autovalore β , allora vw^t è automatrice di $\psi_{A,B}$ di autovalore $\alpha - \beta$. Viceversa, se N è automatrice di $\psi_{A,B}$ di autovalore γ , si consideri un autovettore v di B di autovalore β con $Nv \neq 0$, e si concluda che Nv è autovettore di A di autovalore $\beta + \gamma$. Se invece gli autospazi di B sono contenuti nel nucleo di N , si ripete il ragionamento trovando un vettore v non appartenente al nucleo di N e tale che $Bv = \beta v + w$ con $Nw = 0$ (vedi teoria di Jordan).

3.14. DEFINIZIONE (SOTTOSPAZI STABILI). *Sia φ un endomorfismo di V , e sia W un sottospazio di V ; W si dice stabile per φ o φ -stabile se $\varphi(W) \subseteq W$.*

3.15. TEOREMA (DI DECOMPOSIZIONE). *Sia φ un endomorfismo di V , e sia $F(X) \in C[X]$ un polinomio tale che $F(\varphi) = 0$. Se $F = F_1 \cdots F_r$ con $F_1, \dots, F_r \in C[X]$ non costanti a due a due coprimi, allora posto $V_{F_i} = \ker F_i(\varphi)$ per ogni i risulta*

$$V = V_{F_1} \oplus \cdots \oplus V_{F_r}$$

e ogni V_{F_i} è spazio φ -stabile (decomposizione dello spazio in sottospazi φ -stabili).

DIMOSTRAZIONE. Per induzione su r ; il caso importante da trattare è evidentemente $r = 2$, che permette facilmente anche il passo induttivo. Sia allora $F(X) = F_1(X)F_2(X)$, ed essendo

$F_1(X)$ ed $F_2(X)$ polinomi in $C[X]$ coprimi, troviamo polinomi $G_1(X)$ e $G_2(X)$ in $C[X]$ tali che $F_1(X)G_1(X) + F_2(X)G_2(X) = 1$. Calcolando in φ si ottiene

$$F_1(\varphi)G_1(\varphi) + F_2(\varphi)G_2(\varphi) = \text{id}_V = G_1(\varphi)F_1(\varphi) + G_2(\varphi)F_2(\varphi).$$

Dimostriamo allora che V_{F_1} e V_{F_2} hanno intersezione nulla: se $v \in V$ appartiene all'intersezione allora $v = \text{id}_V(v) = G_1(\varphi)F_1(\varphi)(v) + G_2(\varphi)F_2(\varphi)(v) = 0 + 0 = 0$.

Mostriamo che $V = V_{F_1} + V_{F_2}$: ogni $v \in V$ si scrive come somma

$$v = \text{id}_V(v) = F_1(\varphi)G_1(\varphi)(v) + F_2(\varphi)G_2(\varphi)(v)$$

e posto $v_1 = F_2(\varphi)G_2(\varphi)(v)$ e $v_2 = F_1(\varphi)G_1(\varphi)(v)$ vediamo subito (poiché $0 = F(\varphi) = F_1(\varphi)F_2(\varphi) = F_2(\varphi)F_1(\varphi)$) che $v_1 \in V_{F_1}$ e $v_2 \in V_{F_2}$. \square

3.15.1. Si osservi che anche un ragionamento diretto, non induttivo, poteva dare lo stesso risultato. Lo si espliciti secondo queste linee: Sia $Q_i = \prod_{j \neq i} F_j$; allora i Q_i sono un insieme coprimo ed esistono polinomi H_i tali che $\sum_i Q_i H_i = 1$. Applicando a φ e ad un vettore v troviamo che $v = \text{id}_V(v) = \sum_i Q_i(\varphi)H_i(\varphi)v$ e ponendo $v_i = Q_i(\varphi)H_i(\varphi)v$ abbiamo che $v = \sum_i v_i$ e $v_i \in V_{F_i}$ ($F_i(\varphi)v_i = F_i(\varphi)Q_i(\varphi)H_i(\varphi)v = F(\varphi)H_i(\varphi)v = 0$). D'altra parte, come prima sappiamo che $V_{F_i} \cap V_{F_j} = 0$ se $i \neq j$.

3.15.2. Applicando in particolare il teorema al polinomio caratteristico otteniamo che se $P_\varphi(X) = \prod_i P_i(X)$ è una sua fattorizzazione in fattori a due a due coprimi, allora V è la somma diretta dei sottospazi $V_{P_i} = \ker P_i(\varphi)$, ciascuno dei quali ha dimensione $\dim_C V_{P_i} = \deg P_i(X)$ pari al grado (come polinomio in X) del fattore $P_i(X)$ (perché? si osservi che il polinomio caratteristico di φ ristretto a V_{P_i} non può contenere altri fattori che quelli di $P_i(X)$, essendone annullata, e d'altra parte il prodotto di tali polinomi caratteristici deve ricostruire il polinomio caratteristico di φ). In particolare, per ogni autovalore λ di molteplicità m si deduce che esso compare nel polinomio minimo con un esponente l che è il minimo intero positivo per cui $\dim_C \ker(\varphi - \lambda \text{id})^l = m$ (al massimo è proprio m).

3.16. TEOREMA (SECONDO CRITERIO DI DIAGONALIZZABILITÀ). Una matrice A è simile (in C) a una matrice in forma diagonale se e solo se ha tutti i suoi autovalori in C e il polinomio minimo si fattorizza in fattori lineari distinti (cioè non ha radici multiple).

DIMOSTRAZIONE. Il "solo se" è facile: se A è diagonalizzabile su C , allora sappiamo già che ha tutti i suoi autovalori in C , ed è chiaro (guardando per esempio alla matrice diagonalizzata, che nella diagonale principale ha esattamente gli autovalori distinti $\lambda_1, \dots, \lambda_r$, ripetuti ciascuno con la rispettiva nullità) che il prodotto $\prod_i (A - \lambda_i \mathbb{I}_n) = 0$, e dunque il polinomio minimo ha fattori al più lineari.

Viceversa, supponiamo che il polinomio minimo si fattorizzi con fattori lineari $m_A(X) = \prod_i (X - \lambda_i)$ con $\lambda_i \neq \lambda_j$ se $i \neq j$; per il teorema di decomposizione abbiamo che $V_n(C) = \bigoplus_i V_{\lambda_i}(A)$, ove ricordiamo che $V_{\lambda_i}(A) = \ker(A - \lambda_i \mathbb{I}_n)$ sono gli autospazi di A , e dunque di dimensioni rispettive $N(\lambda_i)$. Dalla decomposizione abbiamo allora

$$\sum_i M(\lambda_i) = n = \dim_C V_n(C) = \sum_i \dim_C V_{\lambda_i}(A) = \sum_i N(\lambda_i)$$

e poiché $M(\lambda_i) \geq N(\lambda_i)$ per ogni i , trattandosi di quantità positive, concludiamo che $M(\lambda_i) = N(\lambda_i)$ per ogni i , e dunque la matrice è diagonalizzabile per il primo criterio (si poteva usare anche il criterio banale di diagonalizzazione, una volta che lo spazio era decomposto in somma diretta dei vari autospazi). \square

♠ **3.17.** Il seguito del paragrafo è dedicato ad uno studio preciso dei sottospazi stabili, e delle loro relazioni con i polinomi divisori del polinomio minimo; si tratta di argomenti che possono essere saltati in prima lettura, e anche nelle eventuali successive.

3.17.1. PROPOSIZIONE (POLINOMI E SOTTOSPACI STABILI). Sia $F = F(X) \in C[X]$ un polinomio non costante; allora il sottospazio $V_F = \ker F(\varphi)$ è un sottospazio di V stabile per φ ; inoltre se abbiamo due polinomi $F, F' \in C[X]$ e $F|F'$ (F divide F') allora $V_F \subseteq V_{F'}$.

Viceversa, se W è un sottospazio φ -stabile, possiamo associargli il polinomio minimo della restrizione di φ a W , sia m_W (che è un divisore del polinomio minimo di φ); se $W \subseteq W'$ allora $m_W | m_{W'}$ (m_W divide $m_{W'}$ in $C[X]$).

DIMOSTRAZIONE. Formale. □

3.17.2. TEOREMA (STRUTTURA DEI SOTTOSPAZI STABILI?). Per ogni polinomio $F = F(X) \in C[X]$ risulta che $m_{W_F} | F$ (il polinomio minimo di φ ristretto a $\ker F(\varphi)$ divide F) e per ogni sottospazio stabile W risulta che $V_{m_W} \supseteq W$ (W è contenuto nello spazio φ -stabile associato al polinomio minimo di φ ristretto a W).

Ne segue che abbiamo una biiezione tra i seguenti due insiemi:

- (1) polinomi della forma m_W ove W è un sottospazio φ -stabile;
- (2) sottospazi di V della forma W_F ove F è un polinomio non costante (che si può supporre un divisore monico del polinomio minimo di φ).

DIMOSTRAZIONE. La seconda parte segue formalmente dalle prime due osservazioni e dal seguente risultato generale:

Siano A e B due insiemi ordinati (significa per A che è data una relazione, scritta di solito \leq , che è riflessiva ($a \leq a$ per ogni $a \in A$), transitiva (se $a \leq a'$ e $a' \leq a''$ allora $a \leq a''$ per ogni $a, a', a'' \in A$) e antisimmetrica (se $a \leq a'$ e $a' \leq a$ allora $a = a'$ per ogni $a, a' \in A$) e similmente per B). Siano date due funzioni ordinate $f: A \rightarrow B$ e $g: B \rightarrow A$ (significa che da $a \leq a'$ segue $f(a) \leq f(a')$, e similmente per g) tali che $gf(a) \leq a$ per ogni $a \in A$ e $b \leq fg(b)$ per ogni $b \in B$. Allora f e g inducono biiezioni una inversa dell'altra tra gli insiemi $\text{im}(g) \subseteq A$ e $\text{im}(f) \subseteq B$.

Si tratta in effetti di una conseguenza delle seguenti due facili osservazioni: $fgf(a) = f(a)$ per ogni $a \in A$ (perché da $gf(a) \leq a$ segue che $fgf(a) \leq f(a)$, mentre da $b \leq fg(b)$ per $b = f(a)$ segue $f(a) \leq fgf(a)$, da cui l'uguaglianza per antisimmetria) e $gfg(b) = g(b)$ per ogni $b \in B$ (argomento simile). Dunque f e g sono inverse l'una dell'altra quando applicate ad elementi della forma $g(b)$ e $f(a)$ rispettivamente. □

3.17.3. NOTA. Si osservi che gli insiemi identificati dal teorema sono finiti (sono finiti i divisori monici possibili di un polinomio), ma non tutti i sottospazi stabili per φ compaiono necessariamente nella forma V_F per qualche F (infatti i sottospazi stabili potrebbero anche essere in numero infinito: quelli in biiezione con i divisori monici del polinomio minimo di φ sono quelli in qualche modo “massimali” tra i sottospazi stabili). Farsi degli esempi.

3.17.4. PROBLEMA. Ad ogni sottospazio φ -stabile W si può associare anche il polinomio caratteristico di φ ristretto a quel sottospazio, sia p_W ; è ancora vero che se $W \subseteq W'$ allora $p_W | p_{W'}$. Perché non lo abbiamo usato?

3.17.5. ESEMPIO. Al polinomio minimo di φ corrisponde tutto lo spazio V . In effetti $V_F = V$ se e solo se $F(\varphi) = 0$, dunque se e solo se F è un multiplo del polinomio minimo.

4. Teoria di Jordan.

4.1. DEFINIZIONE-TEOREMA (NILPOTENZA). L'applicazione φ è nilpotente se esiste $N \in \mathbb{N}$ tale che $\varphi^N = 0$; l'indice di nilpotenza è il minimo intero per cui ciò succede, si indica con $\text{nilp}(A)$. L'applicazione φ è nilpotente se e solo se una (e allora ogni) sua matrice associata è nilpotente (e gli ordini di nilpotenza sono uguali). L'applicazione φ è nilpotente se e solo se il polinomio caratteristico è X^n , dunque se e solo se ha l'unico autovalore 0 con molteplicità n .

DIMOSTRAZIONE. Facile. □

4.2. DEFINIZIONE (MATRICI NILPOTENTI STANDARD). La matrice nilpotente standard di ordine m è la matrice $N_m := \sum_{i=1}^{m-1} e_{i,i+1} \in M_m(C)$, cioè la matrice triangolare superiore

$$\begin{pmatrix} 0 & & & & \\ \vdots & \mathbb{I}_{m-1} & & & \\ 0 & \cdots & 0 & & \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & \ddots & 1 \\ 0 & 0 & 0 & \cdots & 0 \end{pmatrix}.$$

4.2.1. Si calcolino le potenze $i = 1, \dots, m$ della matrice M_m (è particolarmente simpatico ragionando in termini di applicazioni lineari) e in particolare si verifichi che $(N_m)^m = \mathbb{O}_m$, ma $(N_m)^i \neq \mathbb{O}_m$ se $i < m$ e dunque il polinomio minimo di M_m è X^m (uguale al polinomio caratteristico).

♠♠ 4.3. TEOREMA (STRUTTURA DEGLI ENDOMORFISMI NILPOTENTI). *Una matrice A è nilpotente se e solo se è simile a una matrice a blocchi diagonali formati da matrici nilpotenti standard. Dunque un morfismo è nilpotente se e solo se esiste una base dello spazio tale che la matrice in quella base è una matrice a blocchi diagonali formati da matrici nilpotenti standard.*

DIMOSTRAZIONE. Il “se” è ovvio, visto che le matrici nilpotenti standard sono nilpotenti. Per dimostrare il “solo se” procederemo alla costruzione di una base dello spazio $V_n(C)$ tale che la matrice associata all’endomorfismo φ che ha la matrice data in base canonica, sia del tipo detto. Questa è la costruzione fondamentale per la teoria di Jordan, e va capita bene per proseguire nella lettura. Sia N l’ordine di nilpotenza di φ , dunque $\varphi^N = 0$ (e nessuna potenza minore di φ è nulla). Consideriamo le inclusioni di sottospazi di $V_n(C)$ dati dai nuclei delle potenze successive di φ

$$\ker \varphi \subset \ker \varphi^2 \subset \ker \varphi^3 \subset \dots \subset \ker \varphi^{N-1} \subset \ker \varphi^N = V_n(C)$$

dove si può verificare in effetti che tutte le inclusioni sono strette (tra parentesi: $N \leq n$, nonostante sia maiuscola). Consideriamo una decomposizione $V_n(C) = \ker \varphi^{N-1} \oplus V_{N-1}$ (ovvero V_{N-1} è un complementare in $\ker \varphi^N$ di $\ker \varphi^{N-1}$), e sia

$$\mathcal{V}_{N-1} = (v_{N-1,1}, \dots, v_{N-1,s_{N-1}})$$

una base di V_{N-1} . Allora l’insieme $\varphi(\mathcal{V}_{N-1})$ è contenuto in $\ker \varphi^{N-1}$ (ma non in $\ker \varphi^{N-2}$) e l’insieme $\mathcal{V}_{N-1} \cup \varphi(\mathcal{V}_{N-1})$ è linearmente indipendente.

Consideriamo ora una decomposizione $\ker \varphi^{N-1} = \ker \varphi^{N-2} \oplus V_{N-2}$ (ovvero V_{N-2} è un complementare in $\ker \varphi^{N-1}$ di $\ker \varphi^{N-2}$), e sia

$$\mathcal{V}_{N-2} = (v_{N-2,1}, \dots, v_{N-2,s_{N-2}})$$

un completamento di $\varphi(\mathcal{V}_{N-1})$ a una base di V_{N-2} . Allora gli insiemi $\varphi^2(\mathcal{V}_{N-1})$ e $\varphi(\mathcal{V}_{N-2})$ sono contenuti in $\ker \varphi^{N-2}$ (ma non in $\ker \varphi^{N-3}$) e l’insieme $\mathcal{V}_{N-1} \cup \varphi(\mathcal{V}_{N-1}) \cup \varphi^2(\mathcal{V}_{N-1}) \cup \mathcal{V}_{N-2} \cup \varphi(\mathcal{V}_{N-2})$ è linearmente indipendente.

Procedendo per induzione (discendente) su N , per ogni $i = 1, \dots, N$ si decompone $\ker \varphi^{N-i+1} = \ker \varphi^{N-i} \oplus V_{N-i}$ (ovvero V_{N-i} è un complementare in $\ker \varphi^{N-i+1}$ di $\ker \varphi^{N-i}$), e sia

$$\mathcal{V}_{N-i} = (v_{N-i,1}, \dots, v_{N-i,s_{N-i}})$$

un completamento di $\bigcup_{j < i} \varphi^{i-j}(\mathcal{V}_{N-j})$ a una base di V_{N-i} .

Alla fine del procedimento abbiamo decomposto lo spazio $V_n(C)$ nella somma diretta

$$\begin{aligned} V_n(C) &= \ker \varphi^{N-1} \oplus V_{N-1} \\ &= \ker \varphi^{N-2} \oplus V_{N-2} \oplus V_{N-1} \\ &= \dots \\ &= \ker \varphi^{N-i} \oplus V_{N-i} \oplus \dots \oplus V_{N-2} \oplus V_{N-1} \\ &= \dots \\ &= V_0 \oplus V_1 \oplus V_2 \oplus \dots \oplus V_{N-2} \oplus V_{N-1} \end{aligned}$$

ove $V_0 = \ker \varphi$ e per ognuno dei sottospazi V_{N-i} abbiamo una base del tipo $\bigcup_{j \leq i} \varphi^{i-j}(\mathcal{V}_{N-j})$. Possiamo riassumere schematicamente il dato nella seguente tabella, dove sotto ad ogni sottospazio viene evidenziata la base costruita:

V_0	V_1	V_2	V_3	\dots	V_{N-3}	V_{N-2}	V_{N-1}
\mathcal{V}_0							
$\varphi \mathcal{V}_1$	\mathcal{V}_1						
$\varphi^2 \mathcal{V}_2$	$\varphi \mathcal{V}_2$	\mathcal{V}_2					
$\varphi^3 \mathcal{V}_3$	$\varphi^2 \mathcal{V}_3$	$\varphi \mathcal{V}_3$	\mathcal{V}_3				
\vdots	\vdots	\vdots	\vdots	\ddots			
$\varphi^{N-3} \mathcal{V}_{N-3}$	$\varphi^{N-4} \mathcal{V}_{N-5}$	$\varphi^{N-5} \mathcal{V}_{N-3}$	$\varphi^{N-6} \mathcal{V}_{N-3}$	\dots	\mathcal{V}_{N-3}		
$\varphi^{N-2} \mathcal{V}_{N-2}$	$\varphi^{N-3} \mathcal{V}_{N-2}$	$\varphi^{N-4} \mathcal{V}_{N-2}$	$\varphi^{N-5} \mathcal{V}_{N-2}$	\dots	$\varphi \mathcal{V}_{N-2}$	\mathcal{V}_{N-2}	
$\varphi^{N-1} \mathcal{V}_{N-1}$	$\varphi^{N-2} \mathcal{V}_{N-1}$	$\varphi^{N-3} \mathcal{V}_{N-1}$	$\varphi^{N-4} \mathcal{V}_{N-1}$	\dots	$\varphi^2 \mathcal{V}_{N-1}$	$\varphi \mathcal{V}_{N-1}$	\mathcal{V}_{N-1}

Scegliendo ora come base di $V_n(C)$ la base ottenuta leggendo la tabella (dall'alto in basso, da sinistra a destra) nel modo seguente

$$\begin{aligned} & (v_{0,1}, v_{0,2}, \dots, v_{0,s_0}, \\ & \varphi v_{1,1}, v_{1,1}, \varphi v_{1,2}, v_{1,2}, \dots, \varphi v_{1,s_1}, v_{1,s_1}, \\ & \varphi^2 v_{2,1}, \varphi v_{2,1}, v_{2,1}, \varphi^2 v_{2,2}, \varphi v_{2,2}, v_{2,2}, \dots, \varphi^2 v_{2,s_2}, \varphi v_{2,s_2}, v_{2,s_2}, \\ & \dots, \\ & \varphi^{N-1} v_{N-1,1}, \varphi^{N-2} v_{N-1,1}, \dots, \varphi v_{N-1,1}, v_{N-1,1}, \varphi^{N-1} v_{N-1,2}, \varphi^{N-2} v_{N-1,2}, \dots, \varphi v_{N-1,2}, v_{N-1,2}, \dots, \\ & \varphi^{N-1} v_{N-1,s_{N-1}}, \varphi^{N-2} v_{N-1,s_{N-1}}, \dots, \varphi v_{N-1,s_{N-1}}, v_{N-1,s_{N-1}}) \end{aligned}$$

abbiamo esattamente la matrice cercata, cioè della forma

$$\begin{pmatrix} A_0 & \mathbb{O} & \mathbb{O} & \cdots & \mathbb{O} \\ \mathbb{O} & A_1 & \mathbb{O} & \cdots & \mathbb{O} \\ \mathbb{O} & \mathbb{O} & A_2 & \cdots & \mathbb{O} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \mathbb{O} & \mathbb{O} & \mathbb{O} & \cdots & A_{N-1} \end{pmatrix}$$

ove i blocchi diagonali A_i sono formati a loro volta da s_i blocchi diagonali del tipo nilpotente standard N_{i+1} ; ovvero

$$A_0 = \mathbb{O}_{s_0}, \quad A_1 = \underbrace{\begin{pmatrix} N_2 & & \\ & \ddots & \\ & & N_2 \end{pmatrix}}_{s_1 \text{ blocchi}}, \quad A_2 = \underbrace{\begin{pmatrix} N_3 & & \\ & \ddots & \\ & & N_3 \end{pmatrix}}_{s_2 \text{ blocchi}}, \dots, \quad A_{N-1} = \underbrace{\begin{pmatrix} N_N & & \\ & \ddots & \\ & & N_N \end{pmatrix}}_{s_{N-1} \text{ blocchi}}$$

□

4.3.1. Se invece scegliessimo la base giustapponendo le basi trovate nell'ordine scritto dalla tabella avremmo

$$(v_{0,j}, \varphi v_{1,j}, v_{1,j}, \varphi^2 v_{2,j}, \varphi v_{2,j}, v_{2,j}, \dots, \varphi^{N-1} v_{N-1,j}, \varphi^{N-2} v_{N-1,j}, \dots, \varphi v_{N-1,j}, v_{N-1,j})$$

(variando per primo l'indice j) e la matrice dell'applicazione risulterebbe della forma

$$\begin{pmatrix} B_0 & \mathbb{O} & \mathbb{O} & \cdots & \mathbb{O} \\ \mathbb{O} & B_1 & \mathbb{O} & \cdots & \mathbb{O} \\ \mathbb{O} & \mathbb{O} & B_2 & \cdots & \mathbb{O} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \mathbb{O} & \mathbb{O} & \mathbb{O} & \cdots & B_{N-1} \end{pmatrix}$$

ove i blocchi diagonali sono del tipo

$$B_0 = \mathbb{O}_{s_0}, \quad B_1 = \begin{pmatrix} \mathbb{O} & \mathbb{I}_{s_1} \\ \mathbb{O} & \mathbb{O} \end{pmatrix}, \quad B_2 = \begin{pmatrix} \mathbb{O} & \mathbb{I}_{s_2} & \mathbb{O} \\ \mathbb{O} & \mathbb{O} & \mathbb{I}_{s_2} \\ \mathbb{O} & \mathbb{O} & \mathbb{O} \end{pmatrix}, \dots, \quad B_{N-1} = \begin{pmatrix} \mathbb{O} & \mathbb{I}_{s_{N-1}} & & & \\ & \mathbb{O} & \mathbb{I}_{s_{N-1}} & & \\ & & \ddots & \ddots & \\ & & & \mathbb{O} & \mathbb{I}_{s_{N-1}} \\ & & & & \mathbb{O} \end{pmatrix}$$

(ogni matrice B_i ha i blocchi).

♠ **4.4.** DEFINIZIONE-TEOREMA (TIPO DI NILPOTENZA). *Il tipo di nilpotenza di una matrice nilpotente $A \in M_n(C)$ è la n -pla di naturali (i_1, \dots, i_n) ove i_l è il numero di blocchi nilpotenti standard di ordine l della forma ridotta di A (dunque $\sum_j j i_j = n$). Due matrici nilpotenti sono simili se e solo se hanno lo stesso tipo di nilpotenza.*

DIMOSTRAZIONE. Il “se” è di nuovo ovvio. Per il “solo se” è sufficiente riguardare la dimostrazione precedente: se le matrici sono simili, gli spazi V_i della decomposizione hanno le stesse dimensioni, e dunque otteniamo lo stesso numero di blocchi nilpotenti standard per ogni fissato ordine di nilpotenza. □

4.5. ESEMPLI. Elenchiamo le matrici nilpotenti canoniche a meno di equivalenza per $n \leq 5$; notare che il polinomio caratteristico è in ogni caso X^n , mentre il polinomio minimo è dato da $X^{\text{nilp}(A)}$. Si

osservi che per $n \leq 3$ la nilpotenza caratterizza le matrici nilpotenti canoniche a meno di similitudine; per $n \leq 6$ nilpotenza e rango determinano le matrici nilpotente canoniche a meno di similitudine; per $n \geq 7$ vi sono matrici nilpotenti aventi stesso rango e stessa nilpotenza, ma non simili.

4.5.1. Per $n = 1$ l'unica matrice nilpotente è la matrice nulla.

4.5.2. Per $n = 2$ le matrici nilpotenti canoniche sono di due tipi: la matrice nulla di tipo $(2, 0)$ e la nilpotente standard $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ di tipo $(0, 1)$.

4.5.3. Per $n = 3$ abbiamo tre tipi di matrici nilpotenti canoniche:

la matrice nulla di tipo $(3, 0, 0)$;

la matrice $\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$ di tipo $(1, 1, 0)$ (sse $\text{nilp}(A) = 2$ e $\text{rk}(A) = 1$);

la matrice $\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}$ di tipo $(0, 0, 1)$ (sse $\text{nilp}(A) = 3$ e $\text{rk}(A) = 2$);

4.5.4. Per $n = 4$ abbiamo cinque tipi di matrici nilpotenti canoniche:

la matrice nulla di tipo $(4, 0, 0, 0)$;

la matrice $\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$ di tipo $(2, 1, 0, 0)$ (sse $\text{nilp}(A) = 2$ e $\text{rk}(A) = 1$);

la matrice $\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$ di tipo $(1, 0, 1, 0)$ (sse $\text{nilp}(A) = 3$ e $\text{rk}(A) = 2$);

la matrice $\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}$ di tipo $(0, 2, 0, 0)$ (sse $\text{nilp}(A) = 2$ e $\text{rk}(A) = 2$);

la matrice standard $\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}$ di tipo $(0, 0, 0, 1)$ (sse $\text{nilp}(A) = 4$ e $\text{rk}(A) = 3$).

4.5.5. Per $n = 5$ abbiamo sette tipi di matrici nilpotenti canoniche:

la matrice nulla di tipo $(5, 0, 0, 0, 0)$;

la matrice $\begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$ di tipo $(3, 1, 0, 0, 0)$ (sse $\text{nilp}(A) = 2$ e $\text{rk}(A) = 1$);

la matrice $\begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$ di tipo $(1, 2, 0, 0, 0)$ (sse $\text{nilp}(A) = 2$ e $\text{rk}(A) = 2$);

la matrice $\begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$ di tipo $(2, 0, 1, 0, 0)$ (sse $\text{nilp}(A) = 3$ e $\text{rk}(A) = 2$);

la matrice $\begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$ di tipo $(1, 0, 0, 1, 0)$ (sse $\text{nilp}(A) = 4$ e $\text{rk}(A) = 3$);

la matrice $\begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$ di tipo $(0, 1, 1, 0, 0)$ (sse $\text{nilp}(A) = 3$ e $\text{rk}(A) = 3$);

la matrice $\begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$ di tipo $(0, 0, 0, 0, 1)$ (sse $\text{nilp}(A) = 5$ e $\text{rk}(A) = 4$).

4.5.6. Elencare le matrici nilpotenti canoniche per $n = 6$ (sono 11).

4.5.7. Elencare le matrici nilpotenti canoniche per $n = 7$ (sono 14).

♠ **4.6.** DEFINIZIONE (MATRICI DI JORDAN). Si dice matrice standard di Jordan di ordine m e autovalore λ la matrice $J_m(\lambda) := \lambda \mathbb{I} + N_m$. Si dice matrice di Jordan una matrice quadrata a blocchi diagonali formati da matrici standard di Jordan.

♠♠ **4.7.** TEOREMA (DI JORDAN). Una matrice $A \in M_n(C)$ ha tutti i suoi autovalori in C se e solo se è simile (in C) a una matrice di Jordan, ovvero una matrice a blocchi diagonali formati da matrici standard di Jordan.

DIMOSTRAZIONE. Come al solito il “se” è ovvio (una matrice di Jordan è triangolare). Vediamo il “solo se”. La dimostrazione procede decomponendo lo spazio negli autospazi generalizzati, che sono stabili per l'applicazione e tali che la restrizione dell'applicazione a ciascuno di essi sia una applicazione lineare con un solo autovalore. In questo modo ci si riconduce al caso di matrici nilpotenti (studiando le varie applicazioni meno il loro autovalore) e poi è sufficiente giustapporre le matrici di Jordan trovate.

4.7.1. AUTOSPACI GENERALIZZATI. Sia $p_\varphi(x) = \prod_i (x - \lambda_i)^{r_i}$ ($r_i = m(\lambda_i)$); gli autospazi generalizzati di φ sono $V_i := \ker((\varphi - \lambda_i \text{id}_V)^{r_i})$. Allora $V = \bigoplus_i V_i$, e ogni V_i è sottospazio stabile per φ .

Ora l'applicazione $\varphi_i = \varphi|_{V_i}$ (uguale a φ ristretta a V_i) è applicazione lineare di V_i in sé con un solo autovalore λ_i ; perciò la differenza $\varphi_i - \lambda_i \text{id}_{V_i}$ è una applicazione lineare nilpotente a cui si può

applicare il teorema di struttura per applicazioni nilpotenti. Giustapponendo le basi dei sottospazi V_i si trova una base rispetto a cui la matrice di φ è nella forma dichiarata. \square

♠ 4.8. INVARIANTI. La molteplicità di un autovalore λ_i di A come radice del polinomio minimo è la dimensione del più grande blocco di Jordan relativo a quell'autovalore. La nullità di un autovalore λ_i di A è il numero di blocchi di Jordan relativi a quell'autovalore. La molteplicità di un autovalore λ_i di A come radice del polinomio caratteristico è la dimensione dell'autospazio generalizzato relativo a quell'autovalore. Come contare il numero di blocchi di Jordan di un autovalore e di un fissato ordine?

Questi sono degli invarianti della matrice A per similitudine, quindi invarianti di ogni endomorfismo. Invarianti completi per la classificazione per similitudine?

4.9. ESEMPI. Scriviamo le forme canoniche di Jordan non equivalenti tra loro, e per ognuna specifichiamo i polinomi caratteristico p e minimo m .

4.9.1. Per $n = 1$ ogni matrice è diagonale.

4.9.2. Per $n = 2$ abbiamo tre forme canoniche non equivalenti di Jordan:

la matrice diagonale $\begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix}$ con $p = m = (X - \alpha)(X - \beta)$;

la matrice diagonale $\begin{pmatrix} \alpha & 0 \\ 0 & \alpha \end{pmatrix}$ con $p = (X - \alpha)^2$ e $m = (X - \alpha)$;

la matrice non diagonalizzabile $\begin{pmatrix} \alpha & 1 \\ 0 & \alpha \end{pmatrix}$ con $p = m = (X - \alpha)^2$.

4.9.3. Per $n = 3$ abbiamo sei forme canoniche non equivalenti di Jordan:

la matrice diagonale $\begin{pmatrix} \alpha & 0 & 0 \\ 0 & \beta & 0 \\ 0 & 0 & \gamma \end{pmatrix}$ con $p = m = (X - \alpha)(X - \beta)(X - \gamma)$;

la matrice diagonale $\begin{pmatrix} \alpha & 0 & 0 \\ 0 & \alpha & 0 \\ 0 & 0 & \beta \end{pmatrix}$ con $p = (X - \alpha)^2(X - \beta)$ e $m = (X - \alpha)(X - \beta)$;

la matrice non diagonalizzabile $\begin{pmatrix} \alpha & 1 & 0 \\ 0 & \alpha & 0 \\ 0 & 0 & \beta \end{pmatrix}$ con $p = m = (X - \alpha)^2(X - \beta)$;

la matrice diagonale $\begin{pmatrix} \alpha & 0 & 0 \\ 0 & \alpha & 0 \\ 0 & 0 & \alpha \end{pmatrix}$ con $p = (X - \alpha)^3$ e $m = (X - \alpha)$;

la matrice non diagonalizzabile $\begin{pmatrix} \alpha & 1 & 0 \\ 0 & \alpha & 0 \\ 0 & 0 & \alpha \end{pmatrix}$ con $p = (X - \alpha)^3$ e $m = (X - \alpha)^2$;

la matrice non diagonalizzabile $\begin{pmatrix} \alpha & 1 & 0 \\ 0 & \alpha & 1 \\ 0 & 0 & \alpha \end{pmatrix}$ con $p = m = (X - \alpha)^3$.

4.9.4. Per $n = 4$ abbiamo 14 forme canoniche non equivalenti di Jordan:

$\begin{pmatrix} \alpha & 0 & 0 & 0 \\ 0 & \beta & 0 & 0 \\ 0 & 0 & \gamma & 0 \\ 0 & 0 & 0 & \delta \end{pmatrix}$ con $p = m = (X - \alpha)(X - \beta)(X - \gamma)(X - \delta)$;

$\begin{pmatrix} \alpha & 0 & 0 & 0 \\ 0 & \alpha & 0 & 0 \\ 0 & 0 & \beta & 0 \\ 0 & 0 & 0 & \gamma \end{pmatrix}$ con $p = (X - \alpha)^2(X - \beta)(X - \gamma)$ e $m = (X - \alpha)(X - \beta)(X - \gamma)$;

$\begin{pmatrix} \alpha & 1 & 0 & 0 \\ 0 & \alpha & 0 & 0 \\ 0 & 0 & \beta & 0 \\ 0 & 0 & 0 & \gamma \end{pmatrix}$ con $p = m = (X - \alpha)^2(X - \beta)(X - \gamma)$;

$\begin{pmatrix} \alpha & 0 & 0 & 0 \\ 0 & \alpha & 0 & 0 \\ 0 & 0 & \beta & 0 \\ 0 & 0 & 0 & \beta \end{pmatrix}$ con $p = (X - \alpha)^2(X - \beta)^2$ e $m = (X - \alpha)(X - \beta)$;

$\begin{pmatrix} \alpha & 1 & 0 & 0 \\ 0 & \alpha & 0 & 0 \\ 0 & 0 & \beta & 0 \\ 0 & 0 & 0 & \beta \end{pmatrix}$ con $p = (X - \alpha)^2(X - \beta)^2$ e $m = (X - \alpha)^2(X - \beta)$;

$\begin{pmatrix} \alpha & 1 & 0 & 0 \\ 0 & \alpha & 0 & 0 \\ 0 & 0 & \beta & 1 \\ 0 & 0 & 0 & \beta \end{pmatrix}$ con $p = m = (X - \alpha)^2(X - \beta)^2$;

$\begin{pmatrix} \alpha & 0 & 0 & 0 \\ 0 & \alpha & 0 & 0 \\ 0 & 0 & \alpha & 0 \\ 0 & 0 & 0 & \beta \end{pmatrix}$ con $p = (X - \alpha)^3(X - \beta)$ e $m = (X - \alpha)(X - \beta)$;

$\begin{pmatrix} \alpha & 1 & 0 & 0 \\ 0 & \alpha & 0 & 0 \\ 0 & 0 & \alpha & 0 \\ 0 & 0 & 0 & \beta \end{pmatrix}$ con $p = (X - \alpha)^3(X - \beta)$ e $m = (X - \alpha)^2(X - \beta)$;

$\begin{pmatrix} \alpha & 1 & 0 & 0 \\ 0 & \alpha & 1 & 0 \\ 0 & 0 & \alpha & 0 \\ 0 & 0 & 0 & \beta \end{pmatrix}$ con $p = (X - \alpha)^3(X - \beta)$ e $m = (X - \alpha)^3(X - \beta)$;

$\begin{pmatrix} \alpha & 0 & 0 & 0 \\ 0 & \alpha & 0 & 0 \\ 0 & 0 & \alpha & 0 \\ 0 & 0 & 0 & \alpha \end{pmatrix}$ con $p = (X - \alpha)^4$ e $m = (X - \alpha)$;

$\begin{pmatrix} \alpha & 1 & 0 & 0 \\ 0 & \alpha & 0 & 0 \\ 0 & 0 & \alpha & 0 \\ 0 & 0 & 0 & \alpha \end{pmatrix}$ con $p = (X - \alpha)^4$ e $m = (X - \alpha)^2$;

$$\begin{pmatrix} \alpha & 1 & 0 & 0 \\ 0 & \alpha & 0 & 0 \\ 0 & 0 & \alpha & 1 \\ 0 & 0 & 0 & \alpha \end{pmatrix} \text{ con } p = (X - \alpha)^4 \text{ e } m = (X - \alpha)^2;$$

$$\begin{pmatrix} \alpha & 1 & 0 & 0 \\ 0 & \alpha & 1 & 0 \\ 0 & 0 & \alpha & 0 \\ 0 & 0 & 0 & \alpha \end{pmatrix} \text{ con } p = (X - \alpha)^4 \text{ e } m = (X - \alpha)^3;$$

$$\begin{pmatrix} \alpha & 1 & 0 & 0 \\ 0 & \alpha & 1 & 0 \\ 0 & 0 & \alpha & 1 \\ 0 & 0 & 0 & \alpha \end{pmatrix} \text{ con } p = (X - \alpha)^4 \text{ e } m = (X - \alpha)^4.$$

4.9.5. Scriversi tutte le forme canoniche non equivalenti di Jordan con $n = 5$ (sono 27).

4.9.6. Si noti che fino ad $n = 3$ la coppia dei polinomi caratteristico e minimo determina la forma canonica di Jordan; per $n > 3$ ciò in generale è falso. Cosa serve per la classificazione?

♠♠ **4.10.** DEFINIZIONE (SEMISEMPlicitÀ). Una matrice $A \in M_n(C)$ si dice semisemplice se essa è diagonalizzabile in una chiusura algebrica di C . Un endomorfismo di uno spazio vettoriale V di dimensione finita su C si dice semisemplice se una matrice associata lo è (e allora tutte lo sono).

4.10.1. ESEMPLI. Matrici trigonometriche in $M_2(\mathbb{R})$, matrici in $M_2(\mathbb{Q})$ diagonalizzabili in $\mathbb{Q}[\sqrt{2}]$.

4.10.2. DECOMPOSIZIONE ASTRATTA DI JORDAN. Sia A un endomorfismo di uno spazio vettoriale V di dimensione finita (rispettivamente: sia A una matrice quadrata) con tutti i suoi autovalori nel corpo di base C . Allora esistono due endomorfismi (risp. matrici) A_s, A_n tali che

- (i) A_s è semisemplice e A_n è nilpotente;
- (ii) $A_s A_n = A_n A_s$ e $A = A_s + A_n$;
- (iii) esistono polinomi $p(X), q(X) \in C[X]$ privi di termine noto e tali che $A_s = p(A)$, $A_n = q(A)$; in particolare A_s ed A_n commutano con ogni endomorfismo (risp. ogni matrice) che commuti con A ;
- (iv) sottospazi stabili per A sono stabili sia per A_s che per A_n ;
- (v) se $AB = BA$ con A e B soddisfacenti all'ipotesi detta, allora $(A + B)_s = A_s + B_s$ e $(A + B)_n = A_n + B_n$.

4.10.3. DECOMPOSIZIONE ASTRATTA MULTIPLICATIVA DI JORDAN. Sia A un automorfismo di uno spazio vettoriale V di dimensione finita (rispettivamente: sia A una matrice quadrata invertibile) con tutti i suoi autovalori nel corpo di base C . Allora i suoi autovalori sono tutti non nulli, ed esistono due endomorfismi (risp. matrici) A_s, A_u tali che

- (i) A_s è semisemplice e A_u è unipotente (significa che ha 1 come unico autovalore);
- (ii) $A_s A_u = A_u A_s = A$;
- (iii) sottospazi stabili per A sono stabili sia per A_s che per A_u ;
- (iv) se $AB = BA$ con A e B soddisfacenti all'ipotesi detta, allora $(AB)_s = A_s B_s$ e $(AB)_u = A_u B_u$.

5. Applicazioni.

5.1. CALCOLO DI POTENZE DELLE MATRICI. Data una matrice A , calcolarne le potenze A^m richiede normalmente molti conti, a meno che A non sia di una forma particolare. Due casi particolarmente semplici sono i seguenti:

(5.1.1) se $D = \text{diag}(a_1, \dots, a_n)$ è matrice diagonale, allora $D^m = \text{diag}(a_1^m, \dots, a_n^m)$;

(5.1.2) se $J = D + N$ è in forma di Jordan, poiché $DN = ND$, possiamo applicare la formula del binomio di Newton: $J^m = (D + N)^m = \sum_{i=0}^m \binom{m}{i} D^i N^{m-i}$ (si ricordi che D ed N commutano tra loro; le potenze delle matrici nilpotenti standard sono di calcolo immediato).

5.1.3. Se una matrice A ammette forma canonica diagonale o di Jordan, allora esiste una matrice invertibile P tale che $A = P^{-1}JP$. In tal caso abbiamo $A^m = P^{-1}J^mP$, il che semplifica notevolmente il calcolo.

5.2. SOLUZIONE DI EQUAZIONI RICORSIVE. Supponiamo che una sequenza di numeri $a_i \in C$ per $i \in \mathbb{N}$ sia definita ricorsivamente dalle seguenti posizioni: $a_0 = \alpha_0$, $a_1 = \alpha_1$, ..., $a_{n-1} = \alpha_{n-1}$ e $a_k = \beta_1 a_{k-1} + \beta_2 a_{k-2} + \dots + \beta_n a_{k-n}$ per ogni $k \geq n$, ove $\alpha_i, \beta_i \in C$. Come trovare una formula chiusa che calcoli a_k , senza dover calcolare tutti i precedenti?

Se consideriamo i vettori le cui componenti sono $a_k, a_{k-1}, \dots, a_{k-n+1}$, possiamo riassumere la relazione ricorsiva come

$$\begin{pmatrix} a_k \\ a_{k-1} \\ \dots \\ a_{k-n+1} \end{pmatrix} = \begin{pmatrix} \beta_1 & \beta_2 & \dots & \beta_n \\ & \mathbb{I}_{n-1} & & 0 \\ & & & \vdots \\ & & & 0 \end{pmatrix} \begin{pmatrix} a_{k-1} \\ \dots \\ a_{k-n+1} \\ a_{k-n} \end{pmatrix}$$

da cui si vede che

$$\begin{pmatrix} a_k \\ a_{k-1} \\ \vdots \\ a_{k-n+1} \end{pmatrix} = \begin{pmatrix} \beta_1 & \beta_2 & \dots & \beta_n \\ & \mathbb{I}_{n-1} & & 0 \\ & & & \vdots \\ & & & 0 \end{pmatrix}^{k-n+1} \begin{pmatrix} \alpha_{n-1} \\ \vdots \\ \alpha_1 \\ \alpha_0 \end{pmatrix}$$

e quindi il problema è ricondotto a calcolare la (prima riga della) potenza $(k-n+1)$ -esima della matrice scritta. Tale calcolo può essere effettuato cercando la forma canonica (diagonale o di Jordan), come prima spiegato.

♠ **5.3.** SOLUZIONE DI EQUAZIONI ALLE DIFFERENZE. Più in generale, possiamo porre il seguente problema: trovare le successioni $v_m \in C^n$ (per $m \in \mathbb{N}$) tali che $v_{m+1} = Av_m$ per una fissata matrice $A \in M_n(C)$. Chiaramente per ogni scelta del vettore iniziale v_0 , vi è una unica tale successione definita da $v_n = A^n v_0$, e una descrizione esplicita può essere ottenuta se la matrice A ammette una forma canonica diagonale o di Jordan.

5.3.1. Supponiamo per esempio che A sia diagonalizzabile, che $A = P^{-1}\Delta P$ con Δ matrice diagonale avente in diagonale gli autovalori di A , e P matrice invertibile la cui inversa ha come colonne una base di autovettori per A . Allora $A^m = P^{-1}\Delta^m P$ e, scelta la “condizione iniziale” $v_0 = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ e

posto $\begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = P \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$, abbiamo che $v_m = \sum_{i=1}^n y_i \lambda_i^m u_i$ ove λ_i sono gli autovalori di A (diagonale di Δ) e u_i sono i rispettivi autovettori (colonne di P^{-1}).

5.3.2. Se invece A ammette forma canonica di Jordan J non diagonale, compaiono nelle soluzioni ulteriori termini dovuti alla parte nilpotente di J . Studiamo per esempio il caso di un blocco di Jordan d'autovalore α e d'ordine n . Sia $A = P^{-1}JP$ con $J = \alpha\mathbb{I}_n + N_n$ tale blocco.

Allora $v_m = A^m v_0 = P^{-1}J^m P \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = P^{-1}J^m \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}$ (con le notazioni precedenti). Poiché $J^m = (\alpha\mathbb{I}_n + N_n)^m = \sum_{j=0}^{m-1} \binom{m}{j} \alpha^{m-j} N_n^j$ (esplicitare bene questa formula), abbiamo che

$$v_m = \sum_{i=1}^n \left(\sum_{j=i}^m \binom{m}{j-i} \alpha^{m-j+i} y_j \right) u_i = \sum_{j=1}^n y_j \left(\sum_{i=1}^j \binom{m}{j-i} \alpha^{m-j+i} u_i \right).$$

5.3.3. PROCESSI DISCRETI DI MARKOV. Un caso interessante di equazioni alle differenze è descritto dalle matrici reali con entrate comprese tra 0 e 1, e tali che in ogni colonna la somma delle entrate sia 1. Vengono così descritti dei fenomeni (demografici, statistici, ecc.) in cui ad ogni “passo” certe quantità, rappresentate dalle componenti dei vettori, sono redistribuite secondo una certa regola fissata dalla matrice (detta di transizione).

È facile in questo caso verificare che la matrice ammette sempre l'autovalore 1, e che tutti gli altri autovalori (eventualmente complessi) hanno valore assoluto minore o uguale ad 1. Supponiamo che il blocco relativo all'autovalore 1 di A sia diagonalizzabile. Allora, se gli autovalori diversi da 1 hanno tutti valore assoluto strettamente minore di 1, la sequenza A^n tende, per n grande (“limite per n che va all'infinito”) alla matrice $P^{-1}\Delta'P$ ove Δ' è la matrice diagonale avente nella diagonale solo l'autovalore 1 (con la sua molteplicità). Che conseguenze vi sono per la successione dei v_n ?

♠ **5.4.** ESPONENZIALI DI MATRICI. Nel caso di matrici reali o complesse, possiamo definire una nozione di esponenziale di base e per una matrice qualsiasi A usando quale definizione la formula di Taylor:

$$e^A := \sum_{i=0}^{\infty} \frac{A^i}{i!} = \mathbb{I}_n + A + \frac{A^2}{2} + \frac{A^3}{6} + \dots + \frac{A^i}{i!} + \dots$$

Si pone subito un problema di convergenza: abbiamo usato una sommatoria infinita di matrici, e quindi bisogna controllare che esista il limite delle somme parziali.

5.4.1. Per questo occorre introdurre una nozione di norma nell'insieme delle matrici, e ciò può essere fatto in questo modo: per $A = (a_{i,j})$ definiamo $|A| := \max_{i,j} |a_{i,j}|$ (valore assoluto di numeri reali o complessi). Si verifica allora che la definizione data è corretta per ogni matrice A . Si mostra infatti per induzione che $|A^i| \leq n^i |A|^i = (n|A|)^i$, e dunque la serie scritta è maggiorata, termine a termine, dalla serie numerica convergente a $e^{n|A|}$.

5.4.2. Abbiamo dunque una applicazione $M_n(\mathbb{R}) \rightarrow \text{GL}_n(\mathbb{R})$ che soddisfa alle usuali proprietà: $e^{\mathbb{O}_n} = \mathbb{I}_n$, $e^{A+B} = e^A e^B$ sotto ipotesi che A e B commutino tra loro (quindi $e^A e^{-A} = \mathbb{I}_n$, per cui e^{-A} è matrice inversa della matrice e^A , e tutte le esponenziali sono matrici invertibili).

5.4.3. Il calcolo della matrice esponenziale è particolarmente facile per matrici diagonali ($e^{\text{diag}(a_1, \dots, a_n)} = \text{diag}(e^{a_1}, \dots, e^{a_n})$ come si vede subito) e per matrici nilpotenti (si tratta di una somma finita, in questo caso).

Per una matrice A che sia diagonalizzabile si può allora calcolarne l'esponenziale nel modo seguente: se $A = P^{-1} \Delta P$ con Δ diagonale, si ha $e^A = P^{-1} e^\Delta P$, che è di calcolo immediato.

Per una matrice che ammetta forma di Jordan $J = \Delta + N$ (quindi per tutte se usiamo il corpo complesso) abbiamo $A = P^{-1} J P$ con $J = \Delta + N$, da cui $e^A = P^{-1} e^J P = P^{-1} e^\Delta e^N P$.

5.4.4. Si osservi che se λ è autovalore di A , allora e^λ è autovalore di e^A . Da questo si deduce subito che $\det(e^A) = e^{\text{tr} A}$ (infatti $\Pi e^\lambda = e^{\Sigma \lambda}$). In particolare le matrici di traccia nulla hanno esponenziali di determinante 1.

5.4.5. Che proprietà hanno le matrici esponenziali di matrici antisimmetriche?

5.4.6. SISTEMI DI EQUAZIONI DIFFERENZIALI LINEARI A COEFFICIENTI COSTANTI. Una equazione differenziale lineare a coefficienti costanti (reali o complessi) è una espressione del tipo $\frac{dv}{dx} = Av$ ove $v = v(x)$ è un vettore di funzioni (reali o complesse) della variabile x e A è una matrice quadrata con coefficienti nel corpo reale o complesso. Soluzioni di questa equazione sono tutti i vettori di funzioni che soddisfano all'uguaglianza.

Si studierà in Analisi che per ogni "condizione iniziale" $v(0) = v_0$ (vettore reale o complesso) esiste una unica soluzione $v(x)$ all'equazione posta che soddisfi anche alla condizione iniziale. Vediamo qui come determinare tale soluzione usando l'esponenziazione di matrici.

Si consideri la matrice e^{Ax} come funzione della variabile x (e si trascurino per il momento problemi di convergenza in x); si verifica quasi subito che $\frac{d(e^{Ax})}{dx} = A e^{Ax}$ e che abbiamo $e^{Ax}|_{x=0} = \mathbb{I}_n$.

Quindi il vettore $v(x) = e^{Ax} v_0$ soddisfa alla equazione differenziale e anche alla condizione iniziale; in altri termini, le soluzioni della equazione differenziale data si ottengono mediante combinazioni lineari delle colonne della matrice e^{Ax} secondo dei combinatori che dipendono dalle condizioni iniziali poste.

6. Esercizi.

6.1. Esercizi su Autoteoria.

6.1.1. Verificare che 0, 1 e -1 sono autovalori della matrice reale $A = \begin{pmatrix} -3 & 5 & 1 & 1 \\ -1 & 0 & -1 & 1 \\ 0 & 3 & 2 & -1 \\ -3 & 6 & 1 & 1 \end{pmatrix}$.

Determinare gli autospazi relativi. La matrice A è simile ad una matrice diagonale?

6.1.2. Sia A una matrice quadrata $n \times n$. Verificare che A è non singolare (cioè invertibile) se e solo se 0 non è un autovalore di A .

A si dice nilpotente se e solo se esiste k tale che $A^k = 0$. Verificare che A è nilpotente se e solo se il polinomio caratteristico di A è X^n (sugg.: come risulta il polinomio minimo?).

6.1.3. Sia A una matrice quadrata in $M_n(C)$ e α un autovalore di A . Allora α^k è autovalore di A^k (per ogni $k \in \mathbb{N}$). È vero il "viceversa" (se α^k è autovalore di A^k per qualche $k \dots$)?

6.1.4. Sia A una matrice quadrata in $M_n(C)$ e α un autovalore di A . Se $f(x)$ è un polinomio in $C[x]$, allora $f(\alpha)$ è un autovalore di $f(A)$.

Se A è invertibile, allora α^{-1} è un autovalore di A^{-1} . Mostrare che gli autovalori di A^{-1} sono gli inversi degli autovalori di A , esattamente con la stessa molteplicità.

6.1.5. Sia A una matrice quadrata in $M_n(C)$. Mostrare che se A è diagonalizzabile (risp. triangolarizzabile) allora A^k è diagonalizzabile (risp. triangolarizzabile) (per ogni $k \in \mathbb{N}$). È vero il “viceversa” (se A^k è diagonalizzabile per qualche k ...)?

6.1.6. Sia \mathfrak{S}_n il gruppo simmetrico su $\{1, \dots, n\}$. Per ogni $\sigma \in \mathfrak{S}_n$ sia φ_σ l'unico automorfismo di \mathbb{R}^n tale che $\varphi_\sigma(e_i) = e_{\sigma(i)}$ per ogni $i = 1, \dots, n$, dove $\{e_1, \dots, e_n\}$ è la base canonica di \mathbb{R}^n . Si tratta di morfismi diagonalizzabili su \mathbb{R} ? E su \mathbb{C} ? (*Sugg.: decomporre σ in cicli*).

Se invece K è corpo di caratteristica p , ed usiamo $n = p$, allora un ciclo σ induce un morfismo φ_σ che non è diagonalizzabile.

6.1.7. Sia A una matrice quadrata in $M_n(C)$. Determinare la relazione tra il polinomio caratteristico $p_A(X)$ di A e il polinomio caratteristico $p_{\alpha A}(X)$ di αA ove $\alpha \in C$ e $\alpha \neq 0$.

6.1.8. Sia A una matrice quadrata in $M_n(\mathbb{C})$. Mostrare che $p_{A^k}(X^k) = \prod_{\omega} p_{\omega A}(X)$ ove il prodotto è indiciato dalle radici k -esime di 1.

In particolare $p_{A^2}(X^2) = p_A(X)p_{-A}(X)$.

6.1.9. Discutere la diagonalizzabilità su \mathbb{R} e su \mathbb{C} di matrici reali A d'ordine 2. In particolare, distinguere i seguenti casi:

(a) $\text{tr}(A)^2 - 4 \det(A) > 0$,

(b) $\text{tr}(A)^2 - 4 \det(A) = 0$,

(c) $\text{tr}(A)^2 - 4 \det(A) < 0$.

($\text{tr}(A)$ indica la traccia di A , ovvero la somma degli elementi diagonali).

6.1.10. Calcolare autovalori, molteplicità e nullità, autospazi per le seguenti matrici:

$$\begin{pmatrix} 5 & -3 & 2 \\ 6 & -4 & 4 \\ 4 & -4 & 5 \end{pmatrix}, \quad \begin{pmatrix} 7 & -12 & 6 \\ 10 & -19 & 10 \\ 12 & -24 & 13 \end{pmatrix}, \quad \begin{pmatrix} 4 & -5 & 7 \\ 1 & -4 & 9 \\ -4 & 0 & 5 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 & 0 \\ -4 & 4 & 0 \\ -2 & 1 & 2 \end{pmatrix}.$$

Quali sono diagonalizzabili? Quali triangolarizzabili?

6.1.11. Calcolare autovalori, molteplicità e nullità, autospazi per le seguenti matrici:

$$\begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} 2 & 2 & 0 & 2 \\ -2 & 0 & 0 & -2 \\ 0 & 0 & 2 & 0 \\ -2 & -2 & 0 & -4 \end{pmatrix}, \quad \begin{pmatrix} 2 & 0 & -3 & 0 \\ 0 & 5 & 0 & 3 \\ 3 & 0 & -4 & 0 \\ 2 & 0 & 2 & 1 \end{pmatrix},$$

$$\begin{pmatrix} 2 & 0 & -1 & 0 \\ 2 & 3 & 1 & 1 \\ 1 & 0 & 4 & 0 \\ -1 & 0 & 0 & 2 \end{pmatrix}, \quad \begin{pmatrix} 3 & 0 & 1 & 0 \\ 0 & 2 & 0 & 0 \\ 1 & 0 & 3 & 0 \\ 0 & 0 & 0 & 4 \end{pmatrix}, \quad \begin{pmatrix} 1 & -2 & 0 & 0 \\ 0 & -3 & 0 & 0 \\ -4 & -4 & 1 & -4 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Quali sono diagonalizzabili? Quali triangolarizzabili?

6.1.12. Studiare per quali valori dei parametri le seguenti matrici sono diagonalizzabili:

$$\begin{pmatrix} 1 & 0 & 0 \\ a & 2 & 0 \\ a & 0 & 1-a \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 & 0 \\ 2 & 3 & 0 \\ 1 & a & b \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & a \\ a & 0 & -1 \end{pmatrix}, \quad \begin{pmatrix} 1 & a^2 & -1 \\ 0 & 1 & 0 \\ 0 & 2 & -1 \end{pmatrix}, \quad \begin{pmatrix} a & b & c \\ ab & b^2 & bc \\ ac & bc & c^2 \end{pmatrix}.$$

6.1.13. Studiare per quali valori del parametro la matrice $\begin{pmatrix} 1 & 2 & a^2-a & a \\ 2 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 3 \end{pmatrix}$ è diagonalizzabile.

6.1.14. Calcolare il polinomio caratteristico delle seguenti matrici

$$\begin{pmatrix} 0 & a \\ 1 & b \end{pmatrix}, \quad \begin{pmatrix} 0 & 0 & a \\ 1 & 0 & b \\ 0 & 1 & c \end{pmatrix}, \quad \begin{pmatrix} 0 & 0 & 0 & a \\ 1 & 0 & 0 & b \\ 0 & 1 & 0 & c \\ 0 & 0 & 1 & d \end{pmatrix}, \quad \begin{pmatrix} 0 \cdots 0 & a_0 \\ & a_1 \\ & \vdots \\ \mathbb{I}_{n-1} & \\ & a_{n-1} \end{pmatrix}.$$

Dedurre che ogni polinomio monico è polinomio caratteristico di qualche matrice.

6.1.15. Una matrice reale d'ordine 2 ha un solo autovalore (di molteplicità 2). Dire quali sono le possibili nullità, e per ciascun caso dare un esempio di matrice di tale tipo.

6.1.16. Una matrice reale d'ordine 3 ha un solo autovalore (di molteplicità 3). Dire quali sono le possibili nullità, e per ciascun caso dare un esempio di matrice di tale tipo.

6.1.17. Una matrice reale d'ordine 3 ha due autovalori distinti (uno dei quali di molteplicità 2). Dire quali sono le possibili nullità, e per ciascun caso dare un esempio di matrice di tale tipo.

6.1.18. Una matrice reale d'ordine 4 ha un solo autovalore (di molteplicità 4). Dire quali sono le possibili nullità, e per ciascun caso dare un esempio di matrice di tale tipo.

6.1.19. Una matrice reale d'ordine 4 ha due autovalori distinti (uno dei quali di molteplicità 3). Dire quali sono le possibili nullità, e per ciascun caso dare un esempio di matrice di tale tipo.

6.1.20. Una matrice reale d'ordine 4 ha due autovalori distinti (ciascuno dei quali di molteplicità 2). Dire quali sono le possibili nullità, e per ciascun caso dare un esempio di matrice di tale tipo.

* **6.1.21.** Che relazioni vi sono tra polinomio caratteristico, autovalori, loro molteplicità e nullità per una matrice e per la matrice trasposta?

6.1.22. Calcolare polinomio caratteristico e diagonalizzabilità per le matrici

$$\begin{pmatrix} 0 & c & 0 & \cdots & 0 \\ 0 & 0 & c & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & \ddots & c \\ c & 0 & 0 & \cdots & 0 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 1 & 2 & 0 & \cdots & 0 \\ 1 & 2 & 3 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 2 & 3 & \cdots & n \end{pmatrix}$$

d'ordine n .

6.1.23. Si diano se possibile esempi di matrici reali d'ordine 2 tali che:

- (a) siano prive di autovalori reali;
- (b) abbiano un solo autovalore reale.

Se ne discuta eventualmente la diagonalizzabilità.

6.1.24. Si diano se possibile esempi di matrici reali d'ordine 3 tali che:

- (a) siano prive di autovalori reali;
- (b) abbiano un solo autovalore reale;
- (c) abbiano due soli autovalori reali.

Se ne discuta eventualmente la diagonalizzabilità.

6.1.25. Si diano se possibile esempi di matrici reali d'ordine 4 tali che:

- (a) siano prive di autovalori reali;
- (b) abbiano un solo autovalore reale;
- (c) abbiano due soli autovalori reali.
- (d) abbiano tre soli autovalori reali.

Se ne discuta eventualmente la diagonalizzabilità.

6.1.26. Sia A una matrice quadrata tale che $A^2 = \mathbb{I}$. Dimostrare che A è diagonalizzabile e che i suoi autovalori sono solo 1 oppure -1 . Se B è una matrice quadrata della stessa dimensione di A e se $B^2 = \mathbb{I}$, allora A e B sono simili se e solo se hanno la stessa molteplicità dell'autovalore 1.

6.1.27. Sia A una matrice quadrata tale che $A^2 = A$. Dimostrare che A è diagonalizzabile e che i suoi autovalori sono solo 0 oppure 1. Se B è una matrice quadrata della stessa dimensione di A e se $B^2 = B$, allora A e B sono simili se e solo se hanno lo stesso rango.

6.1.28. Sia A una matrice quadrata tale che $A^3 = A$.

- (a) Dimostrare che A è diagonalizzabile e che i suoi autovalori sono solo 0, 1 oppure -1 .
- (b) Sia B una matrice quadrata della stessa dimensione di A e $B^3 = B$; scrivere e dimostrare un criterio, basato sul rango e sulle molteplicità degli autovalori, affinché A e B siano simili.
- (c) Dire quante matrici diagonali non equivalenti tra loro esistono per le matrici $n \times n$ soddisfacenti all'ipotesi dell'esercizio.

- (d) Per i casi $n = 2, 3$ controllare il risultato precedente elencando tutte le possibili matrici in questione.

6.1.29. Sia A una matrice quadrata $n \times n$ a coefficienti reali tale che $A^3 = \mathbb{I}_n$.

- (a) Dire se A è necessariamente diagonalizzabile nel corpo \mathbb{C} dei numeri complessi;
 (b) Dire se A è necessariamente diagonalizzabile nel corpo \mathbb{R} dei numeri reali; è vero che ha 1 come unico autovalore reale?

- (c) Discutere il caso della matrice reale $A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & -1 & -1 \end{pmatrix}$; è diagonalizzabile su \mathbb{C} ? Lo è su \mathbb{R} ?

6.1.30. Sia A una matrice quadrata a coefficienti nel campo \mathbb{R} dei numeri reali e tale che $A^3 = 2A$.

- (a) Dire se A è necessariamente diagonalizzabile su \mathbb{R} .
 (b) Elencare tutti i possibili autovalori di A in \mathbb{R} .
 (c) Dimostrare che se A è a coefficienti in \mathbb{Q} dei numeri razionali, essa è diagonalizzabile su \mathbb{Q} se e solo se A è la matrice nulla.

6.1.31. Sia A una matrice quadrata a coefficienti nel campo \mathbb{C} dei numeri complessi e tale che $A^3 = -A$.

- (a) Dire se A è necessariamente diagonalizzabile su \mathbb{C} .
 (b) Elencare tutti i possibili autovalori di A in \mathbb{R} , il campo dei numeri reali.
 (c) Dimostrare che se A è a coefficienti in \mathbb{R} , essa è diagonalizzabile su \mathbb{R} se e solo se A è la matrice nulla.

6.1.32. Sia A una matrice quadrata tale che $A^3 = A^2$.

- (a) Dire se A è necessariamente diagonalizzabile; se no, dare un esempio di matrice non diagonalizzabile soddisfacente all'ipotesi detta.
 (b) In ogni caso dimostrare che gli autovalori di A sono solo 0 oppure 1.
 (c) È vero o falso che A è diagonalizzabile se e solo se il suo rango coincide con la molteplicità geometrica dell'autovalore 1? Sia B una matrice quadrata della stessa dimensione di A e $B^3 = B^2$; scrivere e dimostrare un criterio, basato sul rango e sulle molteplicità degli autovalori, affinché A e B siano simili.

6.1.33. Diagonalizzare simultaneamente, se possibile, le due matrici

$$A = \begin{pmatrix} 2 & -1 & -1 \\ 0 & 3 & 1 \\ 0 & 1 & 3 \end{pmatrix} \quad B = \begin{pmatrix} 3 & 0 & 1 \\ -1 & 2 & -1 \\ 1 & 0 & 3 \end{pmatrix}$$

e trovare la trasformazione lineare che le diagonalizza.

6.1.34. Se due endomorfismi φ e ψ sono diagonalizzabili e commutano tra loro, allora $\psi \circ \varphi$ è diagonalizzabile. È vero in generale che il composto di due morfismi diagonalizzabili è diagonalizzabile? E per la somma di due endomorfismi?

6.1.35. Sia f l'endomorfismo di \mathbb{R}^4 di matrice $A = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 2 & -2 & -1 & 2 \\ 1 & 0 & 2 & -1 \\ -3 & -3 & 0 & 2 \end{pmatrix}$ rispetto alla base

canonica. Determinare il sottospazio massimo X di \mathbb{R}^4 ove f coincide con l'applicazione identica. Il sottospazio X ha un complemento f -invariante?

Sia $W = \ker(f - 1)^2$. Verificare che W ha un complemento f -invariante Z , e determinare Z . Il sottospazio Z è unico?

6.1.36. Sia f l'endomorfismo di \mathbb{R}^4 di matrice $A = \begin{pmatrix} 2 & 0 & 0 & 0 \\ \sqrt{2} & -\sqrt{2} & 0 & -\sqrt{2} \\ 0 & 0 & 2 & 0 \\ 2 + \sqrt{2} & \sqrt{2} & 0 & -\sqrt{2} \end{pmatrix}$ rispetto alla

base canonica. Verificare che esistono sottospazi f -invarianti di \mathbb{R}^4 di dimensione 2 e determinarli tutti.

6.1.37. Se A e B sono matrici quadrate dello stesso ordine, e $B = H^{-1}AH$ (con H invertibile), allora si ha che $B^n = H^{-1}A^nH$. Questo può essere utile per semplificare il calcolo delle potenze di una matrice: studiare il caso di matrice diagonalizzabile.

6.1.38. La successione di Fibonacci è definita da $x_0 = 1$, $x_1 = 1$ e poi ricorsivamente da $x_{n+1} = x_n + x_{n-1}$ (si tratta della crescita di una popolazione di conigli immortali, che ogni anno cresce di un numero di individui pari al numero di individui della popolazione dell'anno precedente). Scrivere i primi numeri della successione. Determinare una formula chiusa, cioè non ricorsiva, che dia x_n in funzione di n .

Suggerimento: il processo di generazione dei numeri si può rappresentare tramite la trasformazione lineare $\begin{pmatrix} x_n \\ x_{n-1} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} x_{n-1} \\ x_{n-2} \end{pmatrix}$ e iterando il procedimento: $\begin{pmatrix} x_n \\ x_{n-1} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^{n-1} \begin{pmatrix} x_1 \\ x_0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^n \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ per cui si tratta di calcolare la potenza n -sima di una matrice, che risulta diagonalizzabile: detti $\alpha_{\pm} = \frac{1 \pm \sqrt{5}}{2}$ le radici del polinomio caratteristico, risulta che $\begin{pmatrix} \alpha_{\pm} \\ 1 \end{pmatrix}$ sono gli autovettori, e $x_n = \frac{\alpha_+^{n+1} - \alpha_-^{n+1}}{\alpha_+ - \alpha_-}$ (ma $\sqrt{5}$ deve sparire dalle formule: gli x_n sono interi).

Più in generale, discutere la diagonalizzabilità su \mathbb{R} della matrice della forma $\begin{pmatrix} b & a \\ 1 & 0 \end{pmatrix}$, e la sua relazione con formule esplicite per un problema analogo a quello di Fibonacci.

6.1.39. Idem per le matrici $\begin{pmatrix} c & b & a \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$ e $\begin{pmatrix} d & c & b & a \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$.

6.1.40. Sia d_n il determinante della matrice d'ordine n avente entrate non nulle solo sulla diagonale principale (tutte uguali a b), immediatamente sopra la diagonale principale (tutte uguali ad a) e immediatamente sotto (tutte uguali a c); queste matrici e i loro determinanti si dicono trigonanti. Si proceda scoprendo d_1 , d_2 e la relazione ricorsiva $d_n = bd_{n-1} - acd_{n-2}$, ragionando poi come nel caso di Fibonacci. I numeri di Fibonacci sono un caso particolare di d_n ? Sperimentare con $a = 1$, $b = 3$, $c = 2$.

6.1.41. Studiare i processi di Markov associati alle seguenti matrici, determinando in particolare il comportamento al limite (cioè il limite per n infinito delle potenze n -sime):

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \begin{pmatrix} 1/2 & 1/3 \\ 1/2 & 2/3 \end{pmatrix}, \quad \begin{pmatrix} 1/3 & 2/3 \\ 2/3 & 1/3 \end{pmatrix}, \\ \begin{pmatrix} 1/2 & 1/2 & 0 \\ 0 & 1/2 & 1/2 \\ 1/2 & 0 & 1/2 \end{pmatrix}, \quad \begin{pmatrix} 1/2 & 1/4 & 1/4 \\ 1/3 & 1/3 & 1/3 \\ 1/4 & 1/4 & 1/2 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1/4 & 1/2 \\ 1/2 & 1/2 & 1/2 \\ 1/2 & 1/4 & 0 \end{pmatrix}.$$

6.1.42. Sia $G = \text{SL}(2, \mathbb{R}) := \{X \in M_2(\mathbb{R}) : \det(X) = 1\}$. Mostrare che:

- se $|\text{tr}(X)| > 2$ allora esiste $U \in G$ tale che $UXU^{-1} = \begin{pmatrix} t & 0 \\ 0 & 1/t \end{pmatrix}$ con $t \in \mathbb{R} \setminus \{-1, 0, 1\}$ (caso iperbolico);
- se $|\text{tr}(X)| < 2$ allora esiste $U \in G$ tale che $UXU^{-1} = \begin{pmatrix} \cos t & -\sin t \\ \sin t & \cos t \end{pmatrix}$ con $t \in \mathbb{R}$ (caso ellittico);
- se $X \neq \pm \mathbb{I}_2$ e $|\text{tr}(X)| = 2$ allora esiste $V \in G$ tale che $VXV^{-1} \in \{\pm \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \pm \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}\}$ (caso parabolico);
- per ogni $X \in G$ esistono uniche due matrici $U \in K$ e $V \in T$ tali che $X = UV$ ove

$$K := \left\{ \begin{pmatrix} \cos t & -\sin t \\ \sin t & \cos t \end{pmatrix} : t \in \mathbb{R} \right\} \quad \text{e} \quad T := \left\{ \begin{pmatrix} u & v \\ 0 & 1/u \end{pmatrix} : u, v \in \mathbb{R}, u > 0 \right\}$$

sono sottogruppi di G . Dedurre che allora possiamo supporre $U \in K$ in (b), e $V \in T$ in (c).

6.1.43. Sia $G = \text{SL}(2, \mathbb{C}) := \{X \in M_2(\mathbb{C}) : \det(X) = 1\}$. Mostrare che:

- se $\text{tr}(X) \neq \pm 2$ allora esiste $U \in G$ tale che $UXU^{-1} = \begin{pmatrix} t & 0 \\ 0 & 1/t \end{pmatrix}$ con $t \in \mathbb{C} \setminus \{-1, 0, 1\}$;
- se $X \neq \pm \mathbb{I}_2$ e $\text{tr}(X) = 2$ (risp. $= -2$) allora esiste $V \in G$ tale che $VXV^{-1} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ (risp. $= \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$);
- per ogni $X \in G$ esistono uniche due matrici $U \in K$ e $V \in T$ tali che $X = UV$ ove

$$K := \left\{ \begin{pmatrix} u & \bar{v} \\ v & \bar{u} \end{pmatrix} : u, v \in \mathbb{C}, |u|^2 + |v|^2 = 1 \right\} \quad \text{e} \quad T := \left\{ \begin{pmatrix} a & b \\ 0 & 1/a \end{pmatrix} : a, b \in \mathbb{R}, a, b > 0 \right\}$$

sono sottogruppi di G .

6.2. Esercizi su Jordan.

6.2.1. Sia f l'endomorfismo di \mathbb{R}^4 che, con riferimento alla base canonica (e_1, e_2, e_3, e_4) , ha matrice

$$A = \begin{pmatrix} 2 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

- Determinare il polinomio caratteristico ed il polinomio minimo di f .
- Determinare una matrice di Jordan J per f e trovare una base di \mathbb{R}^4 rispetto cui f è rappresentata da J .
- È vero che esistono vettori u, v, w di \mathbb{R}^4 , tali che $(u, v, w, f(v) - v)$ sia una base di \mathbb{R}^4 ? Nel caso affermativo si espliciti una tale base e si scriva la matrice di f rispetto ad essa. Si tratta di una matrice di Jordan?

6.2.2. Per ognuna delle seguenti matrici, sia f l'endomorfismo di \mathbb{R}^4 che, con riferimento alla base canonica (e_1, e_2, e_3, e_4) , ha quella matrice:

$$A_1 = \begin{pmatrix} 4 & 0 & 6 & 12 \\ 1 & 0 & 0 & 3 \\ 0 & 0 & -2 & 0 \\ 2 & 0 & 0 & 6 \end{pmatrix}, \quad A_2 = \begin{pmatrix} 1 & 0 & 0 & 5 \\ 0 & 4 & 0 & 0 \\ 3 & 8 & 0 & 15 \\ -2 & 0 & 0 & -10 \end{pmatrix}.$$

- Determinare il polinomio caratteristico ed il polinomio minimo di f .
- Determinare una matrice di Jordan J per f .
- Trovare una base di \mathbb{R}^4 rispetto cui f è rappresentata da J .

6.2.3. Sia φ l'endomorfismo di \mathbb{C}^4 di matrice $A = \begin{pmatrix} 2 & 0 & 0 & 0 \\ -4 & 2 & -4 & -3 \\ 4 & 0 & 5 & 3 \\ -3 & 0 & -2 & 0 \end{pmatrix}$ rispetto alla base

canonica di \mathbb{C}^4 .

- Determinare il polinomio minimo e la forma di Jordan di φ .
- Trovare una base di \mathbb{C}^4 rispetto cui la matrice di φ è in forma di Jordan.
- Determinare la forma di Jordan dell'endomorfismo $(\varphi - a)^2$, al variare di a in \mathbb{C} .

6.2.4. Sia φ l'endomorfismo di \mathbb{R}^4 rappresentato dalla matrice $A = \begin{pmatrix} 4 & 0 & -1 & 1 \\ 0 & 4 & -1 & 1 \\ 0 & 1 & 6 & -2 \\ 0 & 1 & 2 & 2 \end{pmatrix}$ rispetto

alla base canonica.

- Calcolare il polinomio minimo e il polinomio caratteristico di φ .
- Determinare la forma di Jordan di φ .
- Trovare una base di \mathbb{R}^4 rispetto cui la matrice di φ assume la forma di Jordan.
- Rispondere ai punti a, b e c relativamente all'endomorfismo $\eta = (\varphi - 4)^2$ di \mathbb{R}^4 .

6.2.5. Sia φ l'endomorfismo di \mathbb{C}^4 di matrice $A = \begin{pmatrix} 0 & 0 & 0 & 1 \\ -1 & 2 & 0 & 0 \\ -1 & 1 & 1 & 0 \\ -1 & 1 & 0 & 1 \end{pmatrix}$ rispetto alla base canonica

(e_1, \dots, e_4) .

- Si scriva il polinomio minimo di φ ed una matrice di Jordan J per φ .
- Trovare una base di \mathbb{C}^4 rispetto cui la matrice di φ è J .
- Mostrare tutte le matrici B di $M_4(\mathbb{C})$ tali che $\text{rk}(B) = 4$, $\text{rk}(B - 1) = 2$, $\text{rk}(B - 1)^2 = 1$, $\text{rk}(B - 1)^3 = 0$, sono simili ad A .

6.2.6. Sia φ l'endomorfismo di \mathbb{C}^4 che, con riferimento alla base canonica (e_1, e_2, e_3, e_4) di \mathbb{C}^4 , ha matrice $A = \begin{pmatrix} -2 & 0 & -1 & 0 \\ 6 & -2 & 2 & -1 \\ 0 & 0 & -2 & 0 \\ -4 & 0 & 3 & -2 \end{pmatrix}$.

- Determinare il polinomio caratteristico ed il polinomio minimo di φ .

- (b) Determinare una matrice di Jordan J per φ e trovare una base di \mathbb{C}^4 rispetto cui φ è rappresentata da J .
- (c) Esistono una matrice B in $M_3(\mathbb{C})$ ed uno scalare α in \mathbb{C} tale che B e $(A - \alpha)^2$ hanno lo stesso polinomio minimo?

6.2.7. Sia φ l'endomorfismo di \mathbb{C}^4 la cui matrice rispetto alla base canonica è $A = \begin{pmatrix} 5 & -1 & 0 & 0 \\ 0 & 3 & 0 & 1 \\ 8 & -4 & 3 & 1 \\ 2 & -1 & 0 & 3 \end{pmatrix}$.

- (a) Determinare il polinomio minimo di φ .
- (b) Trovare una base di \mathbb{C}^4 rispetto cui φ assume la forma di Jordan.
- (c) Trovare tutte le matrici di Jordan che hanno lo stesso polinomio caratteristico di A .
- (d) Dire se esistono almeno 5 sottospazi φ -invarianti distinti di dimensione 2 di \mathbb{C}^4 .

6.2.8. Sia φ l'endomorfismo di \mathbb{C}^4 di matrice $A = \begin{pmatrix} 3 & 3 & 0 & -4 \\ 0 & 3 & 0 & 0 \\ -1 & 2 & 3 & 6 \\ 0 & -1 & 0 & 3 \end{pmatrix}$ rispetto alla base canonica.

- (a) Determinare il polinomio caratteristico, il polinomio minimo e la forma di Jordan di φ .
- (b) Trovare una base di \mathbb{C}^4 rispetto cui la matrice di φ è in forma di Jordan.
- (c) Dire se nella \mathbb{C} -algebra $\mathbb{C}[A]$ generata da A esistono divisori di zero non nilpotenti.

6.2.9. Sia φ l'endomorfismo di \mathbb{C}^4 di matrice $A = \begin{pmatrix} -2 & 0 & 8 & 2 \\ -1 & -4 & -4 & -1 \\ 0 & 0 & -4 & 0 \\ 0 & 1 & 1 & -4 \end{pmatrix}$ rispetto alla base canonica.

- (a) Determinare il polinomio minimo e la forma di Jordan di φ .
- (b) Trovare una base di \mathbb{C}^4 rispetto cui φ assume la forma di Jordan.
- (c) Trovare tutte le matrici di Jordan che hanno lo stesso polinomio caratteristico di A .
- (d) Trovare, se esiste, una matrice B di $M_3(\mathbb{C})$ con lo stesso polinomio minimo di A .

6.2.10. Sia φ l'endomorfismo di \mathbb{R}^4 di matrice $A = \begin{pmatrix} 2 & 0 & -2 & 2 \\ 0 & 2 & -2 & 2 \\ 0 & 2 & 5 & -3 \\ 0 & 2 & 3 & -1 \end{pmatrix}$ rispetto alla base canonica.

- (a) Calcolare il polinomio minimo e il polinomio caratteristico di φ .
- (b) Determinare la forma di Jordan di φ .
- (c) Trovare una base di \mathbb{R}^4 rispetto cui la matrice di φ assume la forma di Jordan.
- (d) La \mathbb{R} -algebra $\mathbb{R}[A]$ generata da A contiene divisori di zero non nulli? ed elementi nilpotenti non nulli?

6.2.11. Sia φ l'endomorfismo di \mathbb{R}^4 rappresentato dalla matrice $A = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 6 & -5 & -5 & 5 \end{pmatrix}$ rispetto alla base canonica.

- (a) Calcolare il polinomio minimo e il polinomio caratteristico di φ .
- (b) Determinare la forma di Jordan di φ .
- (c) Trovare una base di \mathbb{R}^4 rispetto cui la matrice di φ assume la forma di Jordan.
- (d) Sia $(s_n)_{n \in \mathbb{N}}$ la successione definita mediante $s_0 = 0$, $s_1 = 3$, $s_2 = 3$, $s_3 = 9$, $s_{n+4} = 6s_n - 5s_{n+1} - 5s_{n+2} + 5s_{n+3}$ per ogni n in \mathbb{N} . Calcolare esplicitamente s_n per ogni n in \mathbb{N} .

6.2.12. Sia φ l'endomorfismo di \mathbb{R}^4 di matrice $A = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}$ rispetto alla base canonica

(e_1, \dots, e_4) .

- (a) Verificare che -1 è un autovalore di φ , calcolare $\dim \ker(\varphi + 1)$ e verificare che $e_1 + e_2 + e_3 + e_4$ è un autovettore di φ .
- (b) Determinare il polinomio caratteristico ed il polinomio minimo di φ (suggerimento: usare (a)).
- (c) Determinare una matrice di Jordan J per φ e trovare una base di \mathbb{R}^4 rispetto cui φ è rappresentata da J .
- (d) Esiste una matrice Y tale che $Y^tAY = J$?

6.2.13. Studiare la forma di Jordan della derivazione e delle sue potenze come endomorfismi dello spazio dei polinomi di grado minore o uguale ad n .

6.2.14. Un endomorfismo nilpotente φ d'indice 4 di uno spazio vettoriale V soddisfa alle condizioni $\dim \ker \varphi = 5$, $\dim \ker \varphi^2 = 9$, $\dim \ker \varphi^3 = 12$, $\dim \ker \varphi^4 = 14$. Determinare $\dim V$, il numero e la dimensione dei blocchi di Jordan di φ e scrivere la forma canonica di Jordan per φ .

6.2.15. La forma canonica di Jordan di un endomorfismo nilpotente φ di uno spazio vettoriale V comporta 2 blocchi d'ordine 1, 1 blocco d'ordine 2, 3 blocchi d'ordine 3. Determinare $\dim V$, l'indice di nilpotenza di φ , e $\dim \ker \varphi^j$ per ogni j .

Capitolo VI

Geometria Affine

La nozione di Spazio Affine vuole modellare la nostra esperienza di “spazio geometrico” (senza ancora le nozioni metriche di distanze ed angoli); in uno spazio geometrico vi sono dei punti, e ci si può spostare da un punto ad un altro tramite “vettori-spostamento”. D’altra parte in uno spazio geometrico non vi sono riferimenti privilegiati (non esiste una origine, un punto migliore di altri), né ha senso a priori fare operazioni tra punti.

Perciò definiremo uno Spazio Affine come un insieme su cui uno Spazio Vettoriale agisce spostando da un punto ad un altro (e la struttura di spazio vettoriale conviene, poiché siamo interessati a parlare di “spostamento nullo”, “somma di spostamenti”, “spostamento contrario”, ecc.). Un Fisico direbbe che uno spazio vettoriale dà le “velocità” e uno spazio affine dà le “posizioni” per delle particelle.

Per gli Spazi Affini studieremo il calcolo baricentrico, una sorta di “operazione tra punti”, e la nozione di trasformazioni affini, cioè di trasformazioni tra Spazi Affini (“deformazioni lineari dello spazio”).

1. Spazi affini.

1.1. DEFINIZIONE (SPAZIO AFFINE). *Uno spazio affine di dimensione n su un corpo C con spazio delle traslazioni V (spazio vettoriale di dimensione n su C) è un insieme \mathbb{A} (i cui elementi vengono detti punti) dotato di una azione di V :*

$$\mathbb{A} \times V \longrightarrow \mathbb{A} : (P, v) \mapsto P+v$$

soggetti ai seguenti assiomi:

- (A1) nullitarità: $P + 0 = P$ (per ogni $P \in \mathbb{A}$);
- (A2) associatività: $(P + v) + w = P + (v + w)$ (per ogni $P \in \mathbb{A}$ e per ogni $v, w \in V$);
- (A3) differenza di punti: per ogni coppia di punti $P, Q \in \mathbb{A}$ esiste un unico vettore $v \in V$ tale che $P + v = Q$. (l’unico vettore v si scrive $v = Q - P$, sicché possiamo parlare di “differenza tra punti”).

1.1.1. Si osservi che (A3) chiede esistenza ed unicità del vettore v ; in particolare da (A3) e (A1) segue che $P + v = P$ (per qualche P) implica $v = 0$. Dunque per ogni P vale che: $P + v = P$ se e solo se $v = 0$.

1.1.2. Di solito si riassume la definizione dicendo che \mathbb{A} è un insieme dotato di una azione fedele e transitiva di uno spazio vettoriale V , ove:

azione significa la funzione $+: \mathbb{A} \times V \rightarrow \mathbb{A}$ nullitaria ed associativa;

fedele significa: $P + v = P$ (se e) solo se $v = 0$;

transitiva significa: per ogni coppia di punti $P, Q \in \mathbb{A}$ esiste un vettore $v \in V$ tale che $P + v = Q$ (la fedeltà fa sì che v sia unico).

1.1.3. In modo equivalente si può definire uno spazio affine di dimensione n su un corpo C con spazio delle traslazioni V come un insieme dotato di una mappa “differenza di punti”

$$\mathbb{A} \times \mathbb{A} \longrightarrow V : (P, Q) \mapsto Q - P$$

ove V è uno spazio vettoriale di dimensione n su C , soddisfacente alle seguenti proprietà:

- (A’1) $P - P = 0$ (per ogni $P \in \mathbb{A}$);
- (A’2) $(Q - P) + (P - R) = Q - R$ (per ogni $P, Q, R \in \mathbb{A}$);
- (A’3) per ogni punto $P \in \mathbb{A}$ e per ogni vettore $v \in V$ esiste un unico punto $Q \in \mathbb{A}$ tale che $v = Q - P$.

1.1.4. Si noti che fissato arbitrariamente un punto P di \mathbb{A} , l’applicazione insiemistica $V \rightarrow \mathbb{A}$ che manda v in $P + v$ è una biiezione, la cui inversa $\mathbb{A} \rightarrow V$ è l’applicazione che manda Q in $Q - P$.

1.1.5. Ogni spazio vettoriale V è uno spazio affine su sé stesso (cioè con spazio delle traslazioni V) sotto l'operazione di somma. In particolare, quando lo spazio vettoriale standard $V_n(C)$ viene visto come spazio affine su sé stesso, si indica con il simbolo $\mathbb{A}^n(C)$ (o anche \mathbb{A}_C^n).

1.2. UN ESEMPIO IMPORTANTE. Inseriamo qui un esempio che giustifica la generalità della definizione data di spazio affine. Dato uno spazio vettoriale V di dimensione n e un suo sottospazio vettoriale di dimensione $m \leq n$, consideriamo l'insieme \mathbb{A} formato da tutti i sottospazi complementari di W , cioè $\mathbb{A} = \{U \leq V : U \cap W = 0 \text{ e } U + W = V\}$. Che struttura ha l'insieme \mathbb{A} ?

Questo insieme è uno spazio affine di dimensione $m(n-m)$, e possiamo descrivere in due modi lo spazio delle traslazioni di \mathbb{A} . La prima descrizione è la seguente: lo spazio delle traslazioni è lo spazio vettoriale $\text{Hom}_C(V/W, W)$, e l'azione sugli elementi di \mathbb{A} si ottiene così: dato $U \in \mathbb{A}$ abbiamo un isomorfismo canonico $U \cong V/W$, e quindi per ogni $\psi : V/W \rightarrow W$ abbiamo un'applicazione lineare $\psi : U \rightarrow W$; poniamo allora $U + \psi = \{u + \psi(u) : u \in U\}$, che si verifica facilmente essere un sottospazio di V complementare di W , e dunque un elemento di \mathbb{A} .

La seconda descrizione permette di identificare uno strano sottospazio di $\text{Aut}(V)$. Consideriamo $\mathbb{T} = \{\varphi \in \text{Aut}(V) : \varphi|_W = \text{id}_W \text{ e } \varphi/V = \text{id}_{V/W}\}$ cioè l'insieme degli automorfismi di V che si restringono alla identità su W e che inducono il morfismo identico su V/W . La struttura di spazio vettoriale di \mathbb{T} è data usando la composizione di applicazioni (si noti che essa risulta commutativa) e la moltiplicazione per gli scalari definita da $\alpha \cdot \varphi = \text{id}_V + \alpha(\varphi - \text{id}_V)$. Può essere più facile vedere la struttura di \mathbb{T} osservando che con una opportuna scelta dalla base di V , gli elementi di \mathbb{T} sono rappresentati da matrici a blocchi del tipo $\begin{pmatrix} \mathbb{I}_m & F \\ 0_{n-m, m} & \mathbb{I}_{n-m} \end{pmatrix}$ ove $F \in M_{m, n-m}(C)$ (quest'ultima rappresenta un elemento $\psi \in \text{Hom}_C(V/W, W)$) e osservando come si comporta il prodotto tra matrici di questo tipo. Ora l'azione di $\varphi \in \mathbb{T}$ su $U \in \mathbb{A}$ è data da $U + \varphi = \varphi(U)$.

1.3. DEFINIZIONE (POSIZIONE GENERALE DI PUNTI). Siano P_0, P_1, \dots, P_m punti di uno spazio affine \mathbb{A} con spazio delle traslazioni V di dimensione n . Essi si dicono "in posizione generale" o "indipendenti" se i vettori $P_1 - P_0, \dots, P_m - P_0$ di V sono linearmente indipendenti (dunque in particolare $m \leq n$).

1.4. DEFINIZIONE (RIFERIMENTI AFFINI E COORDINATE). Sia \mathbb{A} uno spazio affine su C con spazio delle traslazioni V di dimensione n . Un sistema di riferimento di \mathbb{A} è equivalentemente:

(R) un insieme di $n+1$ punti P_0, P_1, \dots, P_n di \mathbb{A} in posizione generale;

(R') un punto O di \mathbb{A} e una base v_1, \dots, v_n di V .

Scelto un sistema di riferimento, ad ogni punto P di \mathbb{A} restano associate le sue coordinate $(x_1, \dots, x_n)^t$ (in quel sistema di riferimento) definite equivalentemente da

(R) $P = P_0 + \sum_i x_i (P_i - P_0)$;

(R') $P = O + \sum_i x_i v_i$.

Il passaggio da (R) a (R') si ottiene definendo $O = P_0$ e $v_i = P_i - P_0$ per $i = 1, \dots, n$. Il viceversa si ottiene definendo $P_0 = O$ e $P_i = P_0 + v_i$ per $i = 1, \dots, n$.

1.4.1. Utilizzando le coordinate in un fissato riferimento affine, possiamo allora dire che i punti P_0, P_1, \dots, P_m sono in posizione generale se e solo se la matrice $(P_1 - P_0 \ \dots \ P_m - P_0) \in M_{n, m}(C)$ ha rango m , o anche se e solo se la matrice

$$\begin{pmatrix} 1 & 1 & \dots & 1 \\ P_0 & P_1 & \dots & P_m \end{pmatrix} \in M_{n+1, m+1}(C)$$

ha rango $m+1$.

1.5. DEFINIZIONE (SOTTOSPAZI AFFINI). Un sottinsieme del tipo

$$P + W = \{P + w : w \in W\}$$

con $P \in \mathbb{A}$ e W un sottospazio vettoriale di V di dimensione m si dice una varietà lineare affine (o sottospazio affine) di dimensione m di \mathbb{A} ; W si chiama lo spazio direttore.

1.5.1. Si noti che $P + W = Q + W$ se e solo se $Q - P \in W$.

1.5.2. I punti di \mathbb{A} sono sottospazi affini con spazio direttore nullo.

1.5.3. Le rette (risp. i piani) di \mathbb{A} sono i sottospazi affini con spazio direttore di dimensione 1 (risp. 2).

1.5.4. EQUAZIONI PARAMETRICHE E CARTESIANE. Una varietà affine si descrive tramite equazioni parametriche: se w_1, \dots, w_m sono una base di W , allora ogni punto X di $P + W$ si scrive come $X = P + \sum_i \alpha_i w_i$ ove gli $\alpha_i \in C$ sono i parametri.

Fissato un riferimento affine, se P ha coordinate $(x_1, \dots, x_n)^t$, si può esplicitare:

$$\begin{cases} X_1 = x_1 + \sum_i \alpha_i w_{i,1} \\ \dots \\ X_n = x_n + \sum_i \alpha_i w_{i,n} \end{cases}$$

Il sottospazio affine $P + W$ si può descrivere anche tramite un sistema di $n-m$ equazioni lineari (rappresentazione cartesiana) che si ottengono dalla condizione

$$\text{rk} \begin{pmatrix} X-x & w_1 & \dots & w_m \end{pmatrix} \leq m$$

(esiste una sottomatrice quadrata invertibile di ordine m : e allora basta annullare i determinanti di ordine $m+1$ contenenti quella sottomatrice). Equivalentemente si può chiedere che

$$\text{rk} \begin{pmatrix} 1 & 1 & 0 & \dots & 0 \\ X & x & w_1 & \dots & w_m \end{pmatrix} \leq m + 1.$$

Viceversa un sistema lineare di m equazioni nelle incognite $X = (X_1, \dots, X_n)$ (che abbia soluzioni) determina un sottospazio affine di dimensione $n - r$ ove r è il rango comune delle matrici completa e incompleta. Il sistema di equazioni si dice minimale se è composto esattamente da r equazioni. Risolvere il sistema equivale a trovare una rappresentazione parametrica per la varietà lineare.

1.5.5. Una collezione di $m+1$ punti P_0, P_1, \dots, P_m di \mathbb{A} in posizione generale determina una varietà affine di dimensione m : la più piccola varietà affine contenente quei punti. Ha equazioni parametriche $X = P_0 + \sum_i \alpha_i (P_i - P_0)$ ed equazioni cartesiane date dalla condizione:

$$\text{rk} \begin{pmatrix} X-P_0 & P_1-P_0 & \dots & P_m-P_0 \end{pmatrix} \leq m$$

ovvero che

$$\text{rk} \begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ X & P_0 & P_1 & \dots & P_m \end{pmatrix} \leq m + 1.$$

Si ricordi il principio dei minori orlati al fine di ricavare un sistema minimo di equazioni lineari, a partire dalle condizioni di rango.

1.5.6. Una collezione di $m+1$ punti P_0, P_1, \dots, P_m di \mathbb{A} è in posizione generale se e solo se ogni punto non appartiene al sottospazio affine generato dagli altri. Per esempio due punti distinti sono in posizione generale; tre punti non allineati sono in posizione generale; quattro punti non complanari sono in posizione generale.

1.6. DEFINIZIONE (POSIZIONI RECIPROCHE DI SOTTOSPAZI AFFINI). Siano $L = P + W$ e $L' = P' + W'$; i due sottospazi si dicono

- (1) incidenti se $L \cap L' \neq \emptyset$ (e l'intersezione è un sottospazio affine); disgiunti in caso contrario;
- (2) paralleli se $W \subseteq W'$ o $W' \subseteq W$; in tal caso possono appartenersi ($L \subseteq L'$ risp. $L' \subseteq L$) oppure essere disgiunti;
- (3) sghembi se sono disgiunti e $W \cap W' = 0$.

1.6.1. Secondo la definizione, due punti sono sempre paralleli, ma non si dice.

1.6.2. Secondo la definizione, un punto è parallelo a qualunque sottospazio affine, ma non si dice nemmeno questo.

1.6.3. Due rette sono parallele se e solo se i vettori generatori degli spazi direttori sono proporzionali. Questo si dice.

1.6.4. Una retta $P + \langle v \rangle$ è parallela ad un piano $Q + \langle w_1, w_2 \rangle$ se e solo se $v \in \langle w_1, w_2 \rangle$. Essa è contenuta nel piano se inoltre $P - Q \in \langle w_1, w_2 \rangle$.

1.6.5. Esistono coppie di sottospazi affini che non sono né incidenti, né parallele, né sghembi: per esempio in \mathbb{A}_C^4 sia L definito da $X_1 = X_2 = 0$ e M definito da $X_1 - 1 = X_3 = 0$. In \mathbb{A}_C^3 la situazione è più semplice: due sottospazi affini sono o incidenti o paralleli o sghembi.

1.6.6. È quasi ovvio osservare che per ogni sottospazio affine $\mathbb{L} = P + W$ di \mathbb{A} , e per ogni punto $Q \notin \mathbb{L}$ esiste un unico sottospazio affine passante per Q , parallelo e della stessa dimensione con \mathbb{L} (si

tratta di $Q + W$). Quindi nei nostri Spazi Affini vale sempre il celebre “quinto postulato” di Euclide: per ogni punto esterno ad una retta data passa una ed una unica retta parallela alla data”.

Facciamo solo notare che noi, nel prossimo capitolo e seguendo la terminologia moderna, useremo il termine “geometria euclidea” non per indicare la validità del postulato, ma per indicare Spazi Affini reali in cui si introduca una nozione di metrica (distanza tra punti, angoli, ortogonalità, tutte nozioni indotte arricchendo la struttura dello spazio vettoriale delle traslazioni).

1.7. DEFINIZIONE (INF E SUP DI SOTTOSPAZI AFFINI). Siano $L = P + W$ e $L' = P' + W'$ sottospazi affini di \mathbb{A} ; poniamo

(1) *inf* (o *meet*, o *intersezione*) di L e L' : $L \wedge L' := L \cap L'$,

(2) *sup* (o *join*, o *congiungente*) di L e L' : $L \vee L' :=$ la minima sottovarietà contenente L e L' .

Quest'ultima si scrive come $P + \langle P' - P, W, W' \rangle$ (ovvero $P' + \langle P - P', W + W' \rangle$) in generale (in particolare se le varietà sono disgiunte); per varietà con intersezione non vuota, possiamo supporre $P = P'$ e allora il sup è dato da $P' + (W + W')$.

1.8. TEOREMA (GRASSMANN AFFINE). Risulta che:

$$\dim_C(L \vee L') + \dim_C(L \wedge L') \leq \dim_C L + \dim_C L'$$

e vale l'uguaglianza se L e L' sono incidenti (oppure sghembe se poniamo $\dim_C \emptyset := -1$); se le varietà sono disgiunte (in particolare se sono parallele) è

$$\dim_C(L \vee L') + \dim_C(W \cap W') = \dim_C L + \dim_C L' + 1.$$

DIMOSTRAZIONE. Evidente dalla descrizione precedente e dalla formula di Grassmann per spazi vettoriali. \square

1.8.1. Si osservi che la seconda formula è particolarmente sgradevole, poiché abbiamo dovuto ricorrere ad un termine, la dimensione dello spazio vettoriale $W \cap W'$ che non ha apparentemente corrispondente nello spazio affine. Si tratta di un termine che tiene conto delle “direzioni in comune” tra L ed L' , ma non corrisponde ad alcun punto dello spazio affine. Studiando la Geometria Proiettiva, questi termini saranno interpretati come “punti all'infinito” in comune alle varietà date, e la formula assumerà un aspetto molto più intrinseco.

1.8.2. Comunque, sotto l'ipotesi che due sottospazi affini non siano paralleli, le formule di Grassmann possono essere usate per dedurre che se le loro dimensioni sono abbastanza grande, allora devono essere incidenti. Scrivere un enunciato preciso di questo tipo.

1.9. SOTTOSPAZI COMPLEMENTARI. Due sottospazi affini L ed L' si dicono complementari se sono sghembi ($L \wedge L' = \emptyset$ e l'intersezione degli spazi direttori è nulla) e generano tutto lo spazio affine ($L \vee L' = \mathbb{A}$). In tal caso $\dim_C L + \dim_C L' = n - 1$ se n è la dimensione di \mathbb{A} (si noti che gli spazi direttori non generano tutto lo spazio vettoriale delle traslazioni).

1.9.1. Per esempio una retta ed un punto non appartenente ad essa sono complementari in un piano affine.

1.9.2. In uno spazio affine tridimensionale due rette sono complementari se e solo se sono sghembe. Un piano è complementare ad un punto se e solo se il punto non appartiene al piano.

1.9.3. In uno spazio affine quadridimensionale una retta è complementare ad un piano se e solo se retta e piano sono sghembi tra loro.

1.10. COLLEZIONI DI IPERPIANI AFFINI (SOTTOSPAZI AFFINI DI CODIMENSIONE UNO). Dati r iperpiani π_1, \dots, π_r in uno spazio affine \mathbb{A} di dimensione n tali che $\pi_1 \cap \dots \cap \pi_r$ abbia dimensione $n - r$ (equivalentemente: scelto qualsiasi riferimento, il sistema delle equazioni $L_1(\frac{1}{X}) = 0, \dots, L_r(\frac{1}{X}) = 0$ degli iperpiani risulta compatibile di rango r ; si noti che $L_1, \dots, L_r \in M_{1,n+1}(C)$), allora: un iperpiano di \mathbb{A} contiene $\pi_1 \cap \dots \cap \pi_r$ se e solo se la sua equazione è una combinazione lineare a coefficienti non tutti nulli delle equazioni di π_1, \dots, π_r (nel riferimento dato dev'essere quindi del tipo $(\alpha_1 L_1 + \dots + \alpha_r L_r)(\frac{1}{X}) = 0$ ove $\alpha_1, \dots, \alpha_r \in C$ non tutti nulli).

Si tratta di una applicazione immediata del teorema di Rouché-Capelli: aggiungendo l'equazione del nuovo iperpiano il sistema ha esattamente le stesse soluzioni...

L'insieme di tutti gli iperpiani contenenti l'intersezione di π_1, \dots, π_r si chiama collezione di iperpiani di centro $\pi_1 \cap \dots \cap \pi_r$.

1.10.1. Nel piano affine si dice *fascio di rette di centro un punto* P l'insieme formato da tutte le rette contenenti quel punto; se P ha coordinate $\begin{pmatrix} x \\ y \end{pmatrix}$, ovvero equazioni $X - x = 0 = Y - y$, allora le rette del fascio hanno equazioni $\alpha(X - x) + \beta(Y - y) = 0$ con α, β non entrambi nulli.

Date due rette distinte nel piano affine, se la loro intersezione è un punto siamo esattamente nel caso descritto e le rette del fascio hanno equazioni date dalle combinazioni non nulle delle equazioni date; se invece le due rette sono parallele, le rette che si descrivono tramite combinazioni non nulle sono tutte e sole le rette parallele alle due date (segue ancora da Rouché-Capelli) e la loro collezione si dice un fascio di rette improprio; si dice ancora che queste rette hanno in comune “un punto all'infinito”.

1.10.2. Nello spazio affine di dimensione 3 si dice *fascio di piani di asse una retta* r l'insieme formato da tutti i piani contenenti quella retta; se r ha equazioni $L = 0 = M$, allora i piani del fascio hanno equazioni $\alpha L + \beta M = 0$ con α, β non entrambi nulli.

Dati due piani distinti nello spazio affine, se la loro intersezione è una retta siamo esattamente nel caso descritto e i piani del fascio hanno equazioni date dalle combinazioni non nulle delle equazioni date; se invece i due piani sono paralleli, i piani che si descrivono tramite combinazioni non nulle sono tutti e soli i piani paralleli ai due dati e l'insieme si dice un fascio di piani improprio; si dice ancora che questi piani hanno in comune “una retta all'infinito”.

1.10.3. Nello spazio affine di dimensione 3 si dice *stella di piani di centro un punto* P l'insieme formato da tutti i piani contenenti quel punto; se P ha coordinate $\begin{pmatrix} x \\ y \\ z \end{pmatrix}$, ovvero equazioni $X - x = Y - y = Z - z = 0$, allora le rette del fascio hanno equazioni $\alpha(X - x) + \beta(Y - y) + \gamma(Z - z) = 0$ con α, β, γ non tutti nulli.

Dati tre piani distinti nello spazio affine, se la loro intersezione è un punto siamo esattamente nel caso descritto e i piani della stella hanno equazioni date dalle combinazioni non nulle delle equazioni date; se invece i tre piani hanno intersezione vuota, i piani che si descrivono tramite combinazioni non nulle sono tutti e soli i piani paralleli alla direzione comune ai tre dati e l'insieme si dice una stella di piani impropria; si dice ancora che questi piani hanno in comune “un punto all'infinito”.

1.10.4. In uno spazio affine di dimensione 4 si possono definire fasci, stelle, reti di iperpiani, che sono collezioni di iperpiani di centri rispettivamente un piano, una retta, un punto e sono descritti usando rispettivamente due, tre e quattro parametri non tutti nulli.

Dati due, tre, quattro iperpiani, essi definiscono rispettivamente un fascio, una stella, una rete di iperpiani se la loro intersezione è rispettivamente un piano, una retta, un punto. Se invece le intersezioni hanno dimensioni minori, si parla di fasci, stelle, reti impropri di iperpiani.

1.11. PROBLEMA. *Siano r ed s due rette sghembe in uno spazio affine; si mostri che per ogni punto P appartenente a $r \vee s$ ma non a $r \cup s$ (attenzione!) esiste una unica retta t passante per P e complanare sia con r che con s (ovviamente, in due piani distinti...). Quando tale retta è incidente o parallela con le due date? Per affrontare il problema, conviene ragionare identificando le condizioni a cui deve soddisfare t : dovendo passare per P e dovendo essere complanare con r , deve stare sul piano $P \vee r$ (un piano?); per lo stesso motivo deve stare su $P \vee s$; ma allora deve essere l'intersezione di questi due piani, se l'intersezione è una retta... Si noti che il ragionamento fatto dà anche un procedimento facile per calcolare delle equazioni per la retta cercata: basta trovare le equazioni dei due piani, e per questi basta imporre al generico piano del fascio di asse r (risp. s) la condizione di passare per P .*

Generalizzare il problema per sottospazi di dimensioni superiori.

1.12. INTERPRETAZIONE GEOMETRICA DI ROUCHÉ-CAPELLI (COSTELLAZIONI DI SOTTOSPAZI AFFINI). Il teorema di Rouché-Capelli ci permette di discutere completamente tutte le possibili relazioni reciproche di sottospazi affini. Si osservi però che diverse disposizioni geometriche possono comparire aventi gli stessi ranghi completi e incompleti del sistema che descrive i sottospazi coinvolti. Discutiamo solo una paio di casi, invitando il lettore a svilupparne altri.

1.12.1. La costellazione di tre piani in \mathbb{A}^3 è descritta da un sistema lineare di matrice incompleta $A \in M_3(C)$ e completa $(A \ b) \in M_{3,4}(C)$; distinguiamo i casi delle coppie $(\text{rg} A, \text{rg}(A \ b))$:

- (3, 3) sono tre piani che si incontrano in un punto: piani generici di una stella;
- (2, 3) i tre piani hanno intersezione vuota, ma è necessario distinguere due casi:

- il rango di A è 2 perché una riga è multipla di un'altra: allora si hanno due piani paralleli e distinti, e un terzo che li interseca in due rette parallele;

- il rango di A è 2 ma nessuna riga è multipla di un'altra: allora si tratta di tre piani aventi una direzione comune delle giaciture, e a due a due si intersecano in (tre) rette tra loro parallele;
- (2, 2) si tratta di tre piani di un fascio di centro una retta (l'intersezione comune);
- (1, 2) si tratta di tre piani paralleli di cui almeno due distinti;
- (1, 1) si tratta di tre piani coincidenti.
 - 1.12.2. La costellazione di due piani in \mathbb{A}^3 ?
 - 1.12.3. La costellazione di un piano e una retta in \mathbb{A}^3 ?
 - 1.12.4. La costellazione di tre rette in \mathbb{A}^3 ?
 - 1.12.5. La costellazione di due piani in \mathbb{A}^4 è descritta da un sistema lineare di matrice incompleta $A \in M_4(C)$ e completa $(A \ b) \in M_{4,5}(C)$; distinguiamo i casi delle coppie $(\text{rg} A, \text{rg}(A \ b))$:
 - (4, 4) sono due piani che si intersecano in un punto: il sottospazio congiungente è tutto \mathbb{A}^4 ;
 - (3, 4) sono due piani con intersezione vuota, ma le cui giaciture hanno una direzione comune: il sottospazio congiungente è tutto \mathbb{A}^4 ; esistono due iperpiani paralleli contenenti ciascuno uno dei due piani;
 - (3, 3) sono due piani che si intersecano in una retta: il sottospazio congiungente è un iperpiano;
 - (2, 3) sono due piani paralleli e distinti contenuti in uno stesso iperpiano;
 - (2, 2) sono due piani coincidenti.
 - 1.12.6. La costellazione di tre iperpiani in \mathbb{A}^4 ?
 - 1.12.7. La costellazione di tre piani in \mathbb{A}^4 ?

2. Calcolo baricentrico.

2.1. DEFINIZIONE-TEOREMA (SOMME PESATE O BARICENTRICHE DI PUNTI). *Dati $m+1$ punti $P_0, P_1, \dots, P_m \in \mathbb{A}$ e m coefficienti $\alpha_1, \dots, \alpha_m \in C$ tali che $\sum_i \alpha_i = 1$, il punto definito dalla formula $P := P_0 + \sum_i \alpha_i (P_i - P_0)$ risulta indipendente dal punto di base P_0 e si può dunque scrivere come $P := \sum_i \alpha_i P_i$ ("somma pesata di punti" o "somma baricentrica di punti": la somma dei punti è definita solo se i coefficienti hanno somma 1). Il punto P si dice il baricentro del sistema dei punti $P_1, \dots, P_m \in \mathbb{A}$ con i pesi rispettivi $\alpha_1, \dots, \alpha_m \in C$.*

DIMOSTRAZIONE. Se P'_0 è qualsiasi altro punto, e $P' := P'_0 + \sum_i \alpha_i (P_i - P'_0)$, allora la differenza $P - P'$ è $(P_0 - P'_0) + \sum_i \alpha_i (P'_0 - P_0) = 0$. \square

2.1.1. Le combinazioni pesate di m punti descrivono il sottospazio affine generato da quei punti; si tratta di un sottospazio di dimensione $m - 1$ se i punti sono in posizione generale. In particolare: le combinazioni pesate di due punti distinti descrivono la retta congiungente i due punti; le combinazioni pesate di tre punti non allineati descrivono il piano congiungente i tre punti.

2.1.2. PROPRIETÀ DISTRIBUTIVA DEI BARICENTRI. Data una famiglia di punti $P_{i,j}$ con $i = 0, \dots, m$ e $j = 0, \dots, r$, una famiglia di pesi $\alpha_{i,j}$ con $i = 0, \dots, m$ e $j = 0, \dots, r$ tali che $\sum_j \alpha_{i,j} = 1$ per ogni i , ed una ulteriore famiglia di pesi β_k con $k = 0, \dots, m$ tali che $\sum_k \beta_k = 1$ allora risulta

$$\sum_i \beta_i \left(\sum_j \alpha_{i,j} P_{i,j} \right) = \sum_{i,j} (\beta_i \alpha_{i,j}) P_{i,j}$$

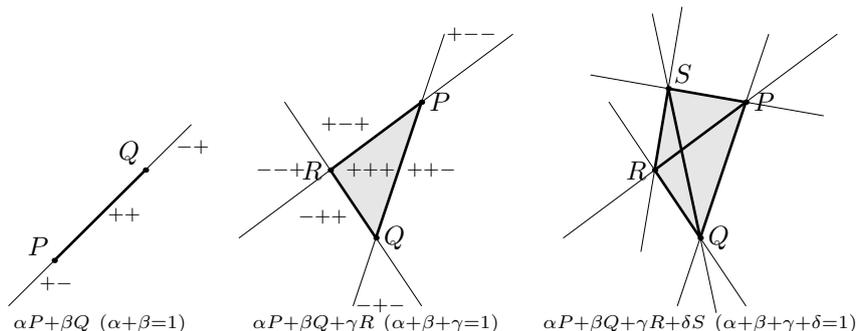
(nel senso che entrambe le espressioni hanno senso, in particolare $\sum_{i,j} \beta_i \alpha_{i,j} = 1$, e i due punti coincidono).

2.2. PROPOSIZIONE (CARATTERIZZAZIONE BARICENTRICA DEI SOTTOSPAZI AFFINI). *Un sottospazio L di \mathbb{A} è un sottospazio affine se e solo se è stabile per somme pesate di punti, ovvero se e solo se contiene due punti contiene la retta generata (combinazioni pesate di due punti).*

DIMOSTRAZIONE. Facile esercizio. \square

2.3. DEFINIZIONE (COMBINAZIONI CONVESSE REALI DI PUNTI: m -EDRI). *Nel caso $C = \mathbb{R}$, possiamo descrivere il segmento tra P_1 e P_2 come le combinazioni pesate dei due punti con i combinatori $\alpha_1, \alpha_2 \in [0, 1]$; il triangolo di vertici P_1, P_2 e P_3 tramite le combinazioni pesate con $\alpha_1, \alpha_2, \alpha_3 \in [0, 1]$; in generale l'involuppo convesso di m punti si rappresenta tramite le combinazioni $\sum_i \alpha_i P_i$ con $\sum_i \alpha_i = 1$*

e $0 \leq \alpha_i \leq 1$ per ogni i . L'involuppo convesso di m punti in posizione generale si dice un m -edro (segmento per $m = 2$, triangolo per $m = 3$, tetraedro per $m = 4$).



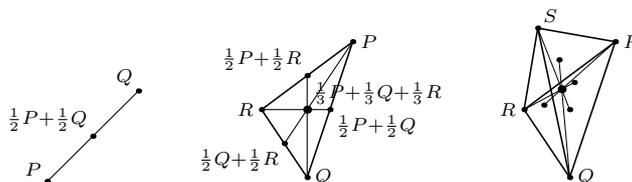
2.4. DEFINIZIONE-TEOREMA (BARICENTRI). Il punto medio del segmento tra P_1 e P_2 è il punto $\frac{1}{2}P_1 + \frac{1}{2}P_2$.

Il baricentro del triangolo di vertici P_1, P_2 e P_3 (punti non allineati) è il punto $\frac{1}{3}P_1 + \frac{1}{3}P_2 + \frac{1}{3}P_3$ e appartiene alle rette congiungenti ogni vertice col punto medio del lato opposto.

Il baricentro del tetraedro di vertici P_1, P_2, P_3 e P_4 (punti non complanari) è il punto $\frac{1}{4}P_1 + \frac{1}{4}P_2 + \frac{1}{4}P_3 + \frac{1}{4}P_4$ e appartiene alle rette congiungenti ogni vertice col baricentro del triangolo opposto.

Dati m punti P_1, \dots, P_m in posizione generale, il baricentro dell' m -edro costituito da quei punti è il punto $\frac{1}{m}P_1 + \dots + \frac{1}{m}P_m$, e appartiene alle rette congiungenti ogni vertice col baricentro dell' $(m-1)$ -edro opposto (quello generato dagli altri vertici).

DIMOSTRAZIONE. Facile esercizio. □



2.4.1. OSSERVAZIONE. Si osservi che la nozione di punto medio e in generale di baricentro non ha, a priori, a che fare con le distanze; noi non abbiamo ancora definito cosa siano le distanze tra punti. La definizione di baricentro dipende solo dalla struttura affine, vale a dire dall'azione dello spazio vettoriale, e dal fatto che i vettori possono essere moltiplicati per gli scalari $\frac{1}{2}, \frac{1}{3}, \dots, \frac{1}{n}, \dots$ (siamo in \mathbb{R} , o comunque in corpi di caratteristica 0, in cui ogni intero è invertibile; cosa succede di queste nozioni in corpi di caratteristica positiva, o in corpi non ordinabili?).

2.4.2. PROBLEMA. Dati quattro punti P_1, P_2, P_3, P_4 in $\mathbb{A}^n(\mathbb{R})$, si consideri un quadrilatero (non necessariamente piano) formato dai quattro punti (basta scegliere un ordine tra i quattro punti); allora i baricentri dei quattro lati formano un parallelogramma, quindi in particolare sono complanari. Quanti di questi piani si possono ottenere a partire da quattro fissati punti?

♠ **2.5. DEFINIZIONE (RAPPORTO SEMPLICE).** Dati tre punti allineati $X, A, B \in \mathbb{A}$, se $X = \lambda A + \mu B$ con $\lambda + \mu = 1$, definiamo

$$(X \ A \ B) := -\frac{\mu}{\lambda}.$$

Se $\xi, \alpha, \beta \in C$ sono le coordinate di X, A, B in un riferimento sulla retta che li contiene, allora

$$(X \ A \ B) = \frac{\xi - \beta}{\xi - \alpha}$$

(“rapporto tra le distanze”, anche se la terminologia è abusiva, visto che non abbiamo ancora definito una nozione di distanza: è tuttavia interessante notare che in Geometria Affine abbiamo un termine che tiene conto del rapporto tra termini che saranno definiti solo in Geometria Euclidea).

Verifichiamo la seconda formula: siano P_0 e P_1 il riferimento scelto. Allora $X = P_0 + \xi(P_1 - P_0)$, $A = P_0 + \alpha(P_1 - P_0)$, $B = P_0 + \beta(P_1 - P_0)$, e da $X = \lambda A + \mu B = P_0 + (\lambda\alpha + \mu\beta)(P_1 - P_0)$. Quindi

dall'uguaglianza $\xi = \lambda\alpha + \mu\beta$ insieme alla condizione $\lambda + \mu = 1$, troviamo $\lambda = \frac{\xi - \beta}{\alpha - \beta}$ e $\mu = \frac{\alpha - \xi}{\alpha - \beta}$, da cui la formula voluta.

2.5.1. X è il punto medio tra A e B sse $(X A B) = -1$.

2.5.2. AZIONE DELLE PERMUTAZIONI. Dati tre punti allineati $A, B, C \in \mathbb{A}$, se $(A B C) = \varrho$, allora:

$$\begin{aligned} (A B C) &= \varrho & (B A C) &= \frac{\varrho}{\varrho - 1} \\ (B C A) &= \frac{\varrho - 1}{\varrho} & (C B A) &= 1 - \varrho \\ (C A B) &= \frac{1}{1 - \varrho} & (A C B) &= \frac{1}{\varrho} \end{aligned}$$

(si lasciano le verifiche per esercizio).

2.5.3. Dati quattro punti allineati $A, B, C, D \in \mathbb{A}$ Abbiamo che $(A B C) = (A B D)(A D C)$.

♠ **2.6.** TEOREMA (CEVA E MENELAO). Sia dato un triangolo di vertici i punti A, B, C (non allineati); siano A', B', C' tre punti rispettivamente sulle rette $B \vee C, A \vee C, A \vee B$; allora:

(MENELAO) A', B', C' sono allineati se e solo se $(A' B C)(B' C A)(C' A B) = 1$;

(CEVA) $A \vee A', B \vee B', C \vee C'$ si incontrano in un punto sse $(A' B C)(B' C A)(C' A B) = -1$.

DIMOSTRAZIONE. Siano $A' = \alpha B + \alpha' C, B' = \beta A + \beta' C, C' = \gamma A + \gamma' B$ (con $\alpha + \alpha' = \beta + \beta' = \gamma + \gamma' = 1$), da cui $(A' B C) = -\alpha'/\alpha, (B' C A) = -\beta'/\beta, (C' A B) = -\gamma'/\gamma$.

Sappiamo ora che A', B', C' sono allineati se e solo se $A' = \lambda B' + \mu C'$ (con $\lambda + \mu = 1$), e questo equivale a

$$\alpha B + \alpha' C = \lambda B' + \mu C' = \lambda(\beta A + \beta' C) + \mu(\gamma A + \gamma' B) = (\lambda\beta + \mu\gamma)A + \mu\gamma' B + \lambda\beta' C$$

e dunque al sistema in λ e μ

$$\begin{cases} \lambda\beta + \mu\gamma = 0 \\ \mu\gamma' = \alpha \\ \lambda\beta' = \alpha' \end{cases}$$

che ha soluzioni se e solo se $\lambda = \alpha'/\beta'$ e $\mu = \alpha/\gamma'$ soddisfano alla prima equazione, ovvero se e solo se $\frac{\alpha'}{\beta'} \frac{\beta}{\gamma'} = -1$, che dà la condizione cercata.

D'altro lato sappiamo che $A \vee A', B \vee B', C \vee C'$ si incontrano in un punto se e solo se esiste un punto X che si scrive al contempo

$$X = \lambda A + \lambda' A' = \lambda A + \lambda' \alpha B + \lambda' \alpha' C$$

$$X = \mu B + \mu' B' = \mu' \beta A + \mu B + \mu' \beta' C$$

$$X = \nu C + \nu' C' = \nu' \gamma A + \nu' \gamma' B + \nu C$$

(con $\lambda + \lambda' = \mu + \mu' = \nu + \nu' = 1$), dunque se e solo se il sistema in λ', μ', ν'

$$\begin{cases} \mu' \beta = \nu' \gamma \\ \lambda' \alpha = \nu' \gamma' \\ \lambda' \alpha' = \mu' \beta' \end{cases}$$

ammette soluzione. Questo si vede facilmente essere equivalente alla condizione $\frac{\alpha'}{\beta'} \frac{\beta}{\gamma'} = 1$, che dà la condizione cercata. \square

3. Trasformazioni affini e affinità.

3.1. DEFINIZIONE (TRASFORMAZIONI AFFINI). Siano \mathbb{A} e \mathbb{B} spazi affini di spazi direttori V e W rispettivamente. Una trasformazione affine è una applicazione insiemistica $F : \mathbb{A} \rightarrow \mathbb{B}$ tale che "rispetta il calcolo baricentrico", i.e. per ogni insieme finito di punti P_1, \dots, P_n e per ogni insieme di numeri reali $\alpha_1, \dots, \alpha_n$ tali che $\sum_{i=1}^n \alpha_i = 1$ si ha $F(\sum_{i=1}^n \alpha_i P_i) = \sum_{i=1}^n \alpha_i F(P_i)$.

L'insieme delle trasformazioni affini di \mathbb{A} in \mathbb{B} si indica con $\text{Trasf}(\mathbb{A}, \mathbb{B})$.

3.1.1. Nella definizione bastava chiedere che per ogni coppia di punti fossero rispettate le somme baricentriche, e poi estendere la proprietà per induzione ad ogni insieme finito di punti, tenendo conto della distributività del calcolo baricentrico.

3.1.2. La composizione di trasformazioni affini è ancora una trasformazione affine; se $F \in \text{Trasf}(\mathbb{A}, \mathbb{B})$ e $G \in \text{Trasf}(\mathbb{B}, \mathbb{C})$ allora $G \circ F \in \text{Trasf}(\mathbb{A}, \mathbb{C})$.

3.1.3. Dalla definizione segue subito che una trasformazione affine manda sottospazi affini in sottospazi affini (ricordare che i sottospazi affini si descrivono come “somme pesate di punti”).

3.2. TEOREMA (APPLICAZIONI LINEARI SOGGIACENTI). Sia $F : \mathbb{A} \rightarrow \mathbb{B}$ una applicazione insiemistica tra spazi affini di spazi direttori V e W rispettivamente. I seguenti fatti sono equivalenti:

- (1) F è trasformazione affine;
- (2) esiste una applicazione lineare $\varphi : V \rightarrow W$ con la proprietà che $F(P + v) = F(P) + \varphi(v)$ per ogni $P \in \mathbb{A}$ e ogni $v \in V$.
- (3) esiste una applicazione lineare $\varphi : V \rightarrow W$ tale che $F(P') - F(P) = \varphi(P' - P)$ per ogni coppia $P, P' \in \mathbb{A}$.

DIMOSTRAZIONE. Le condizioni (2) e (3) sono evidentemente equivalenti, basta porre $v = P' - P$.

Supponiamo vero (1), e per ogni vettore v , definiamo $\varphi(v) = F(P') - F(P)$ se $v = P' - P$; questa definizione non dipende dalla rappresentazione di v (se $v = Q' - Q$ allora $Q' = Q + P - P'$, e per ipotesi $F(Q') = F(Q) + F(P) - F(P')$), e definisce una applicazione lineare di V in W con le proprietà richieste in (3). Viceversa, è facile verificare che una funzione F come in (3) rispetta il calcolo baricentrico, e dunque è una trasformazione affine. \square

3.3. PROPOSIZIONE (RAPPRESENTAZIONE VETTORIALE). La scelta di un punto $P \in \mathbb{A}$ e un punto $Q \in \mathbb{B}$ permette di descrivere le trasformazioni affini tramite coppie (w, φ) con $w \in W$ e $\varphi : V \rightarrow W$ applicazione lineare. Precisamente abbiamo una biiezione

$$\text{Trasf}(\mathbb{A}, \mathbb{B}) \longrightarrow W \times \text{Hom}_C(V, W)$$

che manda F nella coppia $(F(P) - Q, \varphi)$ se φ è l'applicazione lineare sottostante a F .

In questi termini, la composizione di due trasformazioni affini $F : \mathbb{A} \rightarrow \mathbb{B}$ e $G : \mathbb{B} \rightarrow \mathbb{C}$ (scelti $P \in \mathbb{A}$, $Q \in \mathbb{B}$, $R \in \mathbb{C}$) corrispondenti a (w, φ) e (z, ψ) è la coppia $(z + \psi w, \psi \circ \varphi)$.

DIMOSTRAZIONE. Fissato $P \in \mathbb{A}$, ogni trasformazione affine è determinata dal vettore $w = F(P) - Q$ e dalla applicazione lineare associata φ , tramite:

$$F(X) = F(P + (X - P)) = F(P) + \varphi(X - P) = Q + w + \varphi(X - P).$$

Viceversa è chiaro che ogni tale formula determina una trasformazione affine, e che due trasformazioni affini coincidono se e solo se sono rappresentate dalla stessa coppia in $W \times \text{Hom}_C(V, W)$.

L'affermazione per le composizioni segue dal calcolo

$$G \circ F(X) = G(Q + w + \varphi(X - P)) = R + z + \psi(w + \varphi(X - P)) = R + (z + \psi w) + \psi \circ \varphi(X - P)$$

da cui segue che $G \circ F$ è rappresentata come detto. \square

3.3.1. Poiché la scelta di una base di V e una base di W permette di identificare $\text{Hom}_C(V, W)$ con lo spazio delle matrici $M_{n,m}(C)$ (se \mathbb{A} ha dimensione m e \mathbb{B} dimensione n), e W con $M_{n,1}(C)$ la scelta di riferimenti affini su \mathbb{A} e \mathbb{B} permette di avere una identificazione $\text{Trasf}(\mathbb{A}, \mathbb{B}) \cong M_{n,1}(C) \times M_{n,m}(C)$. Inoltre la composizione di due trasformazioni affini F e G come sopra rappresentate da (w, A) e (z, B) è rappresentata da $(z + Bw, BA)$.

3.4. PROPOSIZIONE (RAPPRESENTAZIONE MATRICIALE). La scelta di un riferimento affine su \mathbb{A} e di un riferimento affine su \mathbb{B} permette di definire una mappa

$$\text{Trasf}(\mathbb{A}, \mathbb{B}) \longrightarrow M_{n+1,m+1}(C)$$

che manda φ nella matrice $\begin{pmatrix} 1 & 0 \\ w & A \end{pmatrix}$ se la coppia $(w, A) \in M_{n,1}(C) \times M_{n,m}(C)$ rappresentava la trasformazione affine φ come sopra. Si tratta di una mappa iniettiva, e ogni matrice della forma detta (la prima riga è $(1, 0, \dots, 0) \in M_{1,m+1}(C)$) corrisponde ad una trasformazione affine.

In questi termini, la composizione di due trasformazioni affini $F : \mathbb{A} \rightarrow \mathbb{B}$ e $G : \mathbb{B} \rightarrow \mathbb{C}$ (scelti riferimenti affini in $\mathbb{A}, \mathbb{B}, \mathbb{C}$) è rappresentata dal prodotto delle due matrici.

DIMOSTRAZIONE. Si tratta di mostrare che la mappa

$$M_{n,1}(C) \times M_{n,m}(C) \longrightarrow M_{n+1,m+1}(C)$$

che manda (w, A) in $\begin{pmatrix} 1 & 0 \\ w & A \end{pmatrix}$ è iniettiva e che l'immagine è quella descritta. Entrambe le cose sono facili. Per vedere che la composizione a sinistra corrisponde alla moltiplicazione di matrici a destra, basta osservare che

$$\begin{pmatrix} 1 & 0 \\ z & B \end{pmatrix} \begin{pmatrix} 1 & 0 \\ w & A \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ z+Bw & BA \end{pmatrix}$$

(facendo il prodotto a blocchi). \square

3.4.1. Studiare l'effetto sulle matrici di cambiamenti di riferimento affine ("punto dello spazio affine e base dello spazio direttore") su dominio e codominio.

3.5. RIASSUNTO. Abbiamo quindi visto le seguenti biezioni:

$$\begin{array}{l} \text{Trasf}(\mathbb{A}, \mathbb{B}) \cong W \times \text{Hom}_C(V, W) \cong M_{n,1}(C) \times M_{n,m}(C) \cong \left\{ \begin{pmatrix} 1 & 0 \\ w & A \end{pmatrix} \in M_{n+1,m+1}(C) \right\} \\ \text{(scelti } P \in \mathbb{A}, Q \in \mathbb{B}) \quad \text{(scelte basi di } V, W) \\ F \mapsto (w = F(P) - Q, \varphi) \mapsto (w, A = \alpha_{\mathcal{V}} \varphi) \mapsto \begin{pmatrix} 1 & 0 \\ w & A \end{pmatrix} \end{array}$$

che rispettano le composizioni definite da:

$$GF \leftrightarrow (z, \psi)(w, \varphi) = (z + \psi w, \psi \varphi) \leftrightarrow (z, B)(w, A) = (z + Bw, BA) \leftrightarrow \begin{pmatrix} 1 & 0 \\ z & B \end{pmatrix} \begin{pmatrix} 1 & 0 \\ w & A \end{pmatrix} .$$

3.6. TEOREMA. Fissato un riferimento nello spazio affine \mathbb{A} e un insieme ordinato di punti della stessa cardinalità nello spazio affine \mathbb{B} , esiste una unica trasformazione affine che manda ordinatamente i punti del riferimento nei punti scelti.

DIMOSTRAZIONE. Ovvio, dall'analogo risultato per gli spazi vettoriali. \square

3.7. DEFINIZIONE-TEOREMA (AFFINITÀ). Le affinità di uno spazio affine \mathbb{A} sono le trasformazioni affini biettive di \mathbb{A} in sè. L'insieme delle affinità di \mathbb{A} è un gruppo sotto la composizione e si indica con $\text{Aff}(\mathbb{A})$. Fissati due riferimenti affini su \mathbb{A} , esiste una unica affinità che manda ordinatamente i punti del primo riferimento nei punti del secondo.

3.7.1. Dalla definizione segue subito che le affinità rispettano il rapporto semplice di tre punti allineati. Dunque, anticipando la nozione di "distanza tra punti" possiamo dire che le affinità non rispettano in generale le distanze, ma mantengono costanti opportuni rapporti tra le distanze.

3.7.2. La scelta di $P \in \mathbb{A}$ determina un isomorfismo del gruppo delle affinità di \mathbb{A} in sè con il gruppo $V \times \text{Aut}_C(V)$ dotato di una opportuna composizione dato dalla regola $(v, \varphi) \circ (w, \psi) = (v + \varphi w, \varphi \circ \psi)$.

L'affinità identica è rappresentata dalla matrice identica. L'inversa dell'affinità rappresentata da (v, φ) è dunque $(\varphi^{-1}v, \varphi^{-1})$.

3.7.3. La scelta di un riferimento affine in \mathbb{A} determina un isomorfismo del gruppo delle affinità di \mathbb{A} in sè con il sottogruppo del gruppo $GL_{n+1}(C)$ formato dalle matrici del tipo $\begin{pmatrix} 1 & 0 \\ v & A \end{pmatrix}$ con $A \in GL_n(C)$.

L'affinità identica è rappresentata dalla matrice identica. L'inversa dell'affinità rappresentata da $\begin{pmatrix} 1 & 0 \\ v & A \end{pmatrix}$ è dunque rappresentata dalla matrice inversa $\begin{pmatrix} 1 & 0 \\ A^{-1}v & A^{-1} \end{pmatrix}$.

3.7.4. RIASSUNTO. Abbiamo quindi visto le seguenti biezioni:

$$\begin{array}{l} \text{Aff}(\mathbb{A}) \cong V \times \text{Aut}_C(V) \cong M_{n,1}(C) \times GL_n(C) \cong \left\{ \begin{pmatrix} 1 & 0 \\ w & A \end{pmatrix} : A \in GL_n(C) \right\} \\ \text{(scelto } P \in \mathbb{A}) \quad \text{(scelta base di } V) \\ F \mapsto (w = F(P) - P, \varphi) \mapsto (w, A = \alpha_{\mathcal{V}} \varphi) \mapsto \begin{pmatrix} 1 & 0 \\ w & A \end{pmatrix} . \end{array}$$

3.7.5. DEFINIZIONE-TEOREMA (TRASLAZIONI). Le traslazioni di \mathbb{A} sono le affinità con applicazione lineare associata l'identità; osservare che $\text{Trasl}(\mathbb{A})$ è sottogruppo delle affinità di \mathbb{A} isomorfo a V , dunque in particolare commutativo.

In un riferimento affine le traslazioni si riconoscono dall'aver matrice associata del tipo $\begin{pmatrix} 1 & 0 \\ v & I_n \end{pmatrix}$ con $v \in M_{n,1}(C)$; quindi la composizione di traslazioni corrisponde alla somma di vettori, poiché $\begin{pmatrix} 1 & 0 \\ v & I_n \end{pmatrix} \begin{pmatrix} 1 & 0 \\ w & I_n \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ v+w & I_n \end{pmatrix}$.

3.7.6. DEFINIZIONE-TEOREMA (AFFINITÀ CENTRALI). *Le affinità centrali di centro $P \in \mathbb{A}$ sono le affinità F di \mathbb{A} con $F(P) = P$; osservare che $\text{Centr}_P(\mathbb{A})$ è sottogruppo delle affinità di \mathbb{A} isomorfo a $\text{Aut}_C(V)$ (quindi non commutativo).*

In un riferimento affine con origine in P le affinità centrali di centro P si riconoscono dall'averne matrice associata del tipo $\begin{pmatrix} 1 & 0 \\ 0 & A \end{pmatrix}$ con $A \in \text{GL}_n(C)$; quindi la composizione di traslazioni corrisponde al prodotto di matrici, poiché $\begin{pmatrix} 1 & 0 \\ 0 & A \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & B \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & AB \end{pmatrix}$.

3.7.7. Si osservi che le traslazioni non commutano in generale con le affinità centrali di centro assegnato, poiché

$$\begin{pmatrix} 1 & 0 \\ v & \mathbb{I}_n \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & A \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ v & A \end{pmatrix} \neq \begin{pmatrix} 1 & 0 \\ Av & A \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & A \end{pmatrix} \begin{pmatrix} 1 & 0 \\ v & \mathbb{I}_n \end{pmatrix};$$

capire il significato geometrico (si pensi al piano) e caratterizzare i casi in cui le due affinità commutano.

3.7.8. DECOMPOSIZIONI. Ogni affinità si può scrivere come composizione di una affinità centrale di centro assegnato seguita da una traslazione, o anche in ordine inverso, poiché

$$\begin{pmatrix} 1 & 0 \\ v & \mathbb{I}_n \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & A \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ v & A \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & A \end{pmatrix} \begin{pmatrix} 1 & 0 \\ A^{-1}v & \mathbb{I}_n \end{pmatrix}.$$

3.7.9. SIMMETRIE. Siano U e V sottospazi complementari di $V_n(C)$ (i.e. $V_n(C) = U \oplus V$). La simmetria di $\mathbb{A}^n(C)$ di asse la varietà affine $P + U$ e direzione il sottospazio V è l'affinità definita dall'averne P come punto unito e applicazione lineare associata la simmetria di $V_n(C)$ di asse U e direzione V (i.e. l'applicazione che al vettore $u + v$ con $u \in U$ e $v \in V$ associa $u - v$). Si osservi che i punti uniti della simmetria sono tutti e soli i punti di $P + U$. Inoltre il quadrato di una simmetria è sempre l'identità.

Si osservi che in un opportuno riferimento di $\mathbb{A}^n(C)$ la simmetria viene rappresentata da una matrice $\begin{pmatrix} 1 & 0 & 0 \\ 0 & \mathbb{I}_u & 0 \\ 0 & 0 & -\mathbb{I}_v \end{pmatrix}$.

Cos'è la composizione di due simmetrie di direzione V comune?

3.7.10. PROIEZIONI (PARALLELE, O DALL'INFINITO). Siano U e V sottospazi complementari di $V_n(C)$ (i.e. $V_n(C) = U \oplus V$). La proiezione di $\mathbb{A}^n(C)$ sulla varietà affine $P + U$ nella direzione del sottospazio V è la trasformazione affine definita dall'averne P come punto unito e applicazione lineare associata la proiezione di $V_n(C)$ su U con direzione V (i.e. l'applicazione che al vettore $u + v$ con $u \in U$ e $v \in V$ associa u). Si osservi che i punti uniti della proiezione sono tutti e soli i punti di $P + U$. Inoltre il quadrato di una proiezione è sempre la proiezione stessa. Una proiezione può essere una affinità?

Si osservi che in un opportuno riferimento di $\mathbb{A}^n(C)$ la proiezione viene rappresentata da una matrice $\begin{pmatrix} 1 & 0 & 0 \\ 0 & \mathbb{I}_u & 0 \\ 0 & 0 & \mathbb{O}_v \end{pmatrix}$.

Cos'è la composizione di due proiezioni di direzione V comune?

3.7.11. PROIEZIONI DI CENTRO AFFINE. Siano L e L' sottospazi affini complementari di $\mathbb{A}^n(C)$ (i.e. sghembi e $\mathbb{A}^n(C) = L \vee L'$). La proiezione di $\mathbb{A}^n(C)$ su L e di centro L' è la funzione $\pi : \mathbb{A}^n(C) \setminus L' \rightarrow \mathbb{A}^n(C)$ definita da $\pi(P) = (P \vee L') \cap L$ (verificare usando le formule di Grassmann affini che il risultato in effetti è un punto).

Si tratta di una funzione suriettiva $\pi : \mathbb{A}^n(C) \setminus L' \rightarrow L$ i cui punti fissi sono esattamente gli elementi di L . Per ogni sottospazio affine M complementare con L' (dunque della stessa dimensione di L), π si restringe a una affinità $\pi : M \rightarrow L$ che si dice proiezione da M a L di centro L' .

3.8. TEOREMA (AZIONE SU SOTTOSPACI AFFINI). *Siano $\varphi \in \text{Aff}(\mathbb{A})$ e \mathbb{L} un sottinsieme di \mathbb{A} ; allora \mathbb{L} è sottovarietà affine se e solo se $\varphi(\mathbb{L})$ lo è, e in tal caso hanno la stessa dimensione.*

Se \mathbb{L} è definita dalle equazioni $BX = b$ con $B \in M_{m,n}(C)$ e $b \in M_{m,1}(C)$ e φ è rappresentata dalla matrice $A = \begin{pmatrix} 1 & 0 \\ v & A' \end{pmatrix}$ allora $\varphi(\mathbb{L})$ è definita dalle equazioni $BA'^{-1}X = b + BA'^{-1}v$. In forma compatta: se \mathbb{L} è dato da $(-bB)\begin{pmatrix} 1 \\ X \end{pmatrix} = 0$, allora $\varphi(\mathbb{L})$ è dato da $(-bB)A^{-1}\begin{pmatrix} 1 \\ X \end{pmatrix} = 0$.

Invece l'antimmagine di \mathbb{L} tramite φ ha equazioni date da $(-bB)A\begin{pmatrix} 1 \\ X \end{pmatrix} = 0$.

DIMOSTRAZIONE. La prima asserzione dipende dal fatto che una affinità è una biezione che rispetta il calcolo baricentrico.

D'altra parte, se \mathbb{L} è definita da $(-bB)\begin{pmatrix} 1 \\ X \end{pmatrix} = 0$, allora

$$\begin{aligned} \varphi(\mathbb{L}) &= \left\{ \varphi(X) | (-bB)\begin{pmatrix} 1 \\ X \end{pmatrix} = 0 \right\} \\ &= \left\{ Y | \begin{pmatrix} 1 \\ Y \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ v & A' \end{pmatrix} \begin{pmatrix} 1 \\ X \end{pmatrix} \text{ con } (-bB)\begin{pmatrix} 1 \\ X \end{pmatrix} = 0 \right\} \\ &= \left\{ Y | (-bB)\begin{pmatrix} 1 & 0 \\ v & A' \end{pmatrix}^{-1} \begin{pmatrix} 1 \\ Y \end{pmatrix} = 0 \right\} \end{aligned}$$

che giustifica la seconda asserzione; per l'ultima basta considerare che $\varphi^*(\mathbb{L}) = (\varphi^{-1})(\mathbb{L})$ (e che φ^{-1} è affinità di matrice la matrice inversa di quella di φ). \square

♠♠ 3.9. FUNZIONI AFFINI. In particolare abbiamo le trasformazioni affini di \mathbb{A} sulla retta affine: $\mathbb{A} \rightarrow \mathbb{A}_C^1$. Queste trasformazioni si dicono “funzioni (affini) su \mathbb{A} ”, e il loro insieme si indica con $\mathcal{O}(\mathbb{A})$. Ogni trasformazione affine $F: \mathbb{A} \rightarrow \mathbb{B}$ determina una applicazione $F^*: \mathcal{O}(\mathbb{B}) \rightarrow \mathcal{O}(\mathbb{A})$ (per composizione). Per una applicazione insiemistica $F: \mathbb{A} \rightarrow \mathbb{B}$, i seguenti fatti sono equivalenti:

- (i) $F: \mathbb{A} \rightarrow \mathbb{B}$ è una trasformazione affine;
- (ii) per ogni $f \in \mathcal{O}(\mathbb{B})$ si ha $f \circ F \in \mathcal{O}(\mathbb{A})$;
- (iii) scelti un punto $Q \in \mathbb{B}$ e una base w_1, \dots, w_n di W , si ha $f_i \circ F \in \mathcal{O}(\mathbb{A})$ per $i = 1, \dots, n$ ove $f_i \in \mathcal{O}(\mathbb{B})$ sono definite da $f_i(Q+v) = w_i^*(v)$. [riconoscere che le f_i sono delle “proiezioni” per il riferimento scelto: si tratta delle composizioni $\mathbb{B} \xrightarrow{\cong} \mathbb{A}_C^n \rightarrow \mathbb{A}_C^1$ ove il primo isomorfismo è dato dalla scelta del riferimento in \mathbb{B} .]

Dunque le trasformazioni affini tra \mathbb{A} e \mathbb{B} si possono definire come “le applicazioni insiemistiche F il cui pull-back F^* manda $\mathcal{O}(\mathbb{B})$ in $\mathcal{O}(\mathbb{A})$ ”, ovvero rispetta le funzioni (affini) definite sugli spazi.

Ricordare l'analogo risultato per le applicazioni lineari tra due spazi vettoriali. Riflettere sulla opportunità di definire le “trasformazioni tra spazi geometrici” come le applicazioni insiemistiche che “rispettano un prefissato tipo di funzioni” su quegli spazi.

4. Piano affine.

Siano $P_i = \begin{pmatrix} x_i \\ y_i \end{pmatrix} \in \mathbb{A}^2(C)$ punti del piano e $v_i = \begin{pmatrix} l_i \\ m_i \end{pmatrix} \in V_2(C)$ vettori dello spazio direttore.

4.1. CONDIZIONE DI ALLINEAMENTO DI TRE PUNTI. Tre punti P_0, P_1, P_2 sono allineati se e solo se

$$\begin{vmatrix} x_1-x_0 & x_2-x_0 \\ y_1-y_0 & y_2-y_0 \end{vmatrix} = 0 \quad \text{ovvero} \quad \begin{vmatrix} 1 & 1 & 1 \\ x_0 & x_1 & x_2 \\ y_0 & y_1 & y_2 \end{vmatrix} = 0.$$

4.2. RETTE.

4.2.1. RETTA PER DUE PUNTI. La retta per i punti distinti P_0 e P_1 si scrive $P_0 + \langle P_1 - P_0 \rangle$; ha equazioni parametriche

$$\begin{cases} X = x_0 + \alpha(x_1 - x_0) \\ Y = y_0 + \alpha(y_1 - y_0) \end{cases}$$

ed equazione cartesiana:

$$\begin{vmatrix} X-x_0 & x_1-x_0 \\ Y-y_0 & y_1-y_0 \end{vmatrix} = 0 \quad \text{ovvero,} \quad \begin{vmatrix} 1 & 1 & 1 \\ X & x_0 & x_1 \\ Y & y_0 & y_1 \end{vmatrix} = 0.$$

4.2.2. RETTA PER UN PUNTO E DIREZIONE UN VETTORE. La retta per il punto P_0 e di direzione il vettore non nullo v si scrive $P_0 + \langle v \rangle$; ha equazioni parametriche

$$\begin{cases} X = x_0 + \alpha l_0 \\ Y = y_0 + \alpha m_0 \end{cases}$$

ed equazione cartesiana:

$$\begin{vmatrix} X-x_0 & l_0 \\ Y-y_0 & m_0 \end{vmatrix} = 0 \quad \text{ovvero} \quad \begin{vmatrix} 1 & 1 & 0 \\ X & x_0 & l_0 \\ Y & y_0 & m_0 \end{vmatrix} = 0.$$

4.2.3. POSIZIONE RECIPROCHE DI DUE RETTE. Date due rette $r_0 = P_0 + \langle v_0 \rangle$ e $r_1 = P_1 + \langle v_1 \rangle$ di equazioni cartesiane rispettivamente $a_0X + b_0Y + c_0 = 0$ e $a_1X + b_1Y + c_1 = 0$, esse risultano:

- (1) incidenti se v_0 e v_1 sono linearmente indipendenti; ovvero se e solo se la matrice $\begin{pmatrix} a_0 & b_0 \\ a_1 & b_1 \end{pmatrix}$ ha rango due. In tal caso il punto di incidenza ha coordinate date dalla regola di Cramer applicata al sistema delle due equazioni.
- (2) parallele e distinte se v_0 e v_1 sono linearmente dipendenti e $P_0 \notin r_1$; ovvero se e solo se la matrice incompleta $\begin{pmatrix} a_0 & b_0 \\ a_1 & b_1 \end{pmatrix}$ ha rango uno e la matrice completa $\begin{pmatrix} a_0 & b_0 & c_0 \\ a_1 & b_1 & c_1 \end{pmatrix}$ ha rango due.
- (3) coincidenti se v_0 e v_1 sono linearmente dipendenti e $P_0 \in r_1$; ovvero se e solo se le matrici incompleta e completa hanno rango uno.

4.2.4. FASCI DI RETTE. Le rette passanti per un fissato punto P_0 si scrivono come $P_0 + \langle \begin{pmatrix} l \\ m \end{pmatrix} \rangle$, ovvero $m(X - x_0) - l(Y - y_0) = 0$ con $(l, m) \neq (0, 0)$.

Le rette parallele ad un fissato vettore direzione v_0 si scrivono come $P + \langle v_0 \rangle$ con P punto qualsiasi, ovvero $m_0X - l_0Y + c = 0$ con $c \in C$.

Due rette distinte r_0 e r_1 determinano un fascio di rette che si descrive tramite

$$\lambda(a_0X + b_0Y + c_0) + \mu(a_1X + b_1Y + c_1) = 0, \quad \text{ovvero} \quad (\lambda a_0 + \mu a_1)X + (\lambda b_0 + \mu b_1)Y + (\lambda c_0 + \mu c_1) = 0$$

al variare di $(\lambda, \mu) \neq (0, 0)$.

Una retta r_2 appartiene al fascio determinato da r_0 e r_1 se e solo se la matrice completa del sistema delle tre rette ha determinante nullo.

4.3. AFFINITÀ DEL PIANO. La scelta di un riferimento affine sul piano $\mathbb{A}^2(C)$ determina un isomorfismo del gruppo $\text{Aff}(\mathbb{A}^2(C))$ delle affinità del piano con il sottogruppo

$$\left\{ \begin{pmatrix} 1 & 0 & 0 \\ a & b & A \end{pmatrix} \mid a, b \in C; A \in \text{GL}_2(C) \right\}$$

di $\text{GL}_3(C)$.

4.3.1. AZIONE SULLE RETTE. L'immagine di una retta $r = P \vee Q$ (risp. $r = P + \langle v \rangle$) tramite una affinità F (di applicazione lineare associata φ) si calcola più facilmente come $F(r) = F(P) \vee F(Q)$ (risp. $F(r) = F(P) + \langle \varphi(v) \rangle$). Se la retta r è data tramite equazione cartesiana, per calcolare $F(r)$ bisogna usare la matrice inversa di F in quel riferimento.

4.3.2. SIMMETRIE RISPETTO A PUNTI E RETTE. La matrice associata alla simmetria del piano rispetto al punto $P = \begin{pmatrix} x_0 \\ y_0 \end{pmatrix}$ è tale che $A = -\mathbb{I}_2$, e $\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} 2x_0 \\ 2y_0 \end{pmatrix}$.

La matrice associata alla simmetria del piano di asse la retta $P + \langle v \rangle$ e di direzione w , ove $P = \begin{pmatrix} x_0 \\ y_0 \end{pmatrix}$, è tale che, posto $B = (vw)$ (matrice invertibile d'ordine due), $A = B \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} B^{-1}$, e $\begin{pmatrix} a \\ b \end{pmatrix} = B \begin{pmatrix} 0 & 0 \\ 0 & 2 \end{pmatrix} B^{-1} \begin{pmatrix} x_0 \\ y_0 \end{pmatrix}$.

5. Spazio affine.

Siano $P_i = \begin{pmatrix} x_i \\ y_i \\ z_i \end{pmatrix} \in \mathbb{A}^3$ punti dello spazio e $v_i = \begin{pmatrix} l_i \\ m_i \\ n_i \end{pmatrix} \in V$ vettori dello spazio delle traslazioni.

5.1. RELAZIONI TRA PUNTI.

5.1.1. CONDIZIONE DI COMPLANARITÀ DI QUATTRO PUNTI. quattro punti P_0, P_1, P_2, P_3 sono complanari se e solo se

$$\begin{vmatrix} x_1 - x_0 & x_2 - x_0 & x_3 - x_0 \\ y_1 - y_0 & y_2 - y_0 & y_3 - y_0 \\ z_1 - z_0 & z_2 - z_0 & z_3 - z_0 \end{vmatrix} = 0, \quad \text{ovvero} \quad \begin{vmatrix} 1 & 1 & 1 & 1 \\ x_0 & x_1 & x_2 & x_3 \\ y_0 & y_1 & y_2 & y_3 \\ z_0 & z_1 & z_2 & z_3 \end{vmatrix} = 0.$$

5.1.2. CONDIZIONE DI ALLINEAMENTO DI TRE PUNTI. Tre punti P_0, P_1, P_2 sono allineati se e solo se

$$\text{rk} \begin{pmatrix} x_1 - x_0 & x_2 - x_0 \\ y_1 - y_0 & y_2 - y_0 \\ z_1 - z_0 & z_2 - z_0 \end{pmatrix} = 1, \quad \text{ovvero} \quad \text{rk} \begin{pmatrix} 1 & 1 & 1 \\ x_0 & x_1 & x_2 \\ y_0 & y_1 & y_2 \\ z_0 & z_1 & z_2 \end{pmatrix} = 2.$$

5.2. PIANI.

5.2.1. PIANO PER TRE PUNTI NON ALLINEATI. Il piano per tre punti non allineati P_0, P_1, P_2 si scrive $P_0 + \langle P_1 - P_0, P_2 - P_0 \rangle$; ha equazioni parametriche

$$\begin{cases} X = x_0 + \alpha_1(x_1 - x_0) + \alpha_2(x_2 - x_0) \\ Y = y_0 + \alpha_1(y_1 - y_0) + \alpha_2(y_2 - y_0) \\ Z = z_0 + \alpha_1(z_1 - z_0) + \alpha_2(z_2 - z_0) \end{cases}$$

ed equazione cartesiana:

$$\begin{vmatrix} X - x_0 & x_1 - x_0 & x_2 - x_0 \\ Y - y_0 & y_1 - y_0 & y_2 - y_0 \\ Z - z_0 & z_1 - z_0 & z_2 - z_0 \end{vmatrix} = 0, \quad \text{ovvero} \quad \begin{vmatrix} 1 & 1 & 1 & 1 \\ X & x_0 & x_1 & x_2 \\ Y & y_0 & y_1 & y_2 \\ Z & z_0 & z_1 & z_2 \end{vmatrix} = 0.$$

5.2.2. PIANO PER UN PUNTO E DIREZIONE DUE VETTORI LINEARMENTE INDIPENDENTI. Il piano passante per P_0 e di giacitura lo spazio generato da due vettori linearmente indipendenti v_0, v_1 si scrive $P_0 + \langle v_0, v_1 \rangle$; ha equazioni parametriche

$$\begin{cases} X = x_0 + \alpha l_0 + \beta l_1 \\ Y = y_0 + \alpha m_0 + \beta m_1 \\ Z = z_0 + \alpha n_0 + \beta n_1 \end{cases}$$

ed equazione cartesiana:

$$\begin{vmatrix} X - x_0 & l_0 & l_1 \\ Y - y_0 & m_0 & m_1 \\ Z - z_0 & n_0 & n_1 \end{vmatrix} = 0 \quad \text{ovvero} \quad \begin{vmatrix} 1 & 1 & 0 & 0 \\ X & x_0 & l_0 & l_1 \\ Y & y_0 & m_0 & m_1 \\ Z & z_0 & n_0 & n_1 \end{vmatrix} = 0.$$

5.2.3. POSIZIONI RECIPROCHE DI DUE PIANI. Dati due piani $\pi_0 = P_0 + \langle v_0, v'_0 \rangle$ e $\pi_1 = P_1 + \langle v_1, v'_1 \rangle$ di equazioni cartesiane rispettivamente $a_0X + b_0Y + c_0Z + d_0 = 0$ e $a_1X + b_1Y + c_1Z + d_1 = 0$, essi risultano:

- (1) incidenti se $\text{rk}(v_0 \ v'_0 \ v_1 \ v'_1) = 3$; ovvero sse la matrice $\begin{pmatrix} a_0 & b_0 & c_0 \\ a_1 & b_1 & c_1 \end{pmatrix}$ ha rango due. In tal caso la retta di incidenza ha equazioni cartesiane date dal sistema delle due equazioni.
- (2) paralleli e distinti se $\text{rk}(v_0 \ v'_0 \ v_1 \ v'_1) = 2$; (i.e. gli spazi direttori coincidono: $\langle v_0, v'_0 \rangle = \langle v_1, v'_1 \rangle$) e $P_0 \notin \pi_1$ (i.e. $\pi_0 \cap \pi_1 = \emptyset$); ovvero sse la matrice incompleta $\begin{pmatrix} a_0 & b_0 & c_0 \\ a_1 & b_1 & c_1 \end{pmatrix}$ ha rango uno e la matrice completa $\begin{pmatrix} a_0 & b_0 & c_0 & d_0 \\ a_1 & b_1 & c_1 & d_1 \end{pmatrix}$ ha rango due.
- (3) coincidenti se gli spazi direttori coincidono e $P_0 \in \pi_1$; ovvero sse le matrici incompleta e completa hanno rango uno.

5.2.4. FASCI DI PIANI. I piani contenenti una fissata retta $r_0 = P_0 + \langle v_0 \rangle$ (asse del fascio) di equazioni cartesiane $\begin{cases} a_0X + b_0Y + c_0Z + d_0 = 0 \\ a'_0X + b'_0Y + c'_0Z + d'_0 = 0 \end{cases}$ si scrivono come $P_0 + \langle v_0, \begin{pmatrix} l \\ m \\ n \end{pmatrix} \rangle$ con $\begin{pmatrix} l \\ m \\ n \end{pmatrix}$ vettore linearmente indipendente con v_0 , ovvero

$$\lambda(a_0X + b_0Y + c_0Z + d_0) + \mu(a'_0X + b'_0Y + c'_0Z + d'_0) = 0$$

cioè

$$(\lambda a_0 + \mu a'_0)X + (\lambda b_0 + \mu b'_0)Y + (\lambda c_0 + \mu c'_0)Z + (\lambda d_0 + \mu d'_0) = 0$$

al variare di $(\lambda, \mu) \neq (0, 0)$.

I piani paralleli ad un fissato spazio direttore $\langle v_0, v_1 \rangle$ si scrivono come $P + \langle v_0, v_1 \rangle$ con P punto qualsiasi, ovvero

$$(m_0n_1 - n_0m_1)X + (-l_0n_1 + n_0l_1)Y + (l_0m_1 - m_0l_1)Z + c = 0$$

con $c \in \mathbb{C}$ (i coefficienti sono i minori d'ordine due di $(v_0 \ v_1)$).

Due piani distinti π_0 e π_1 determinano un fascio di piani descritto da

$$\lambda(a_0X + b_0Y + c_0Z + d_0) + \mu(a_1X + b_1Y + c_1Z + d_1) = 0,$$

ovvero

$$(\lambda a_0 + \mu a_1)X + (\lambda b_0 + \mu b_1)Y + (\lambda c_0 + \mu c_1)Z + (\lambda d_0 + \mu d_1) = 0$$

per $(\lambda, \mu) \neq (0, 0)$.

Un piano π_2 appartiene al fascio di piani determinato da π_0 e π_1 se e solo se la matrice completa del sistema dei tre piani ha rango due.

5.2.5. STELLE DI PIANI. I piani passanti per un fissato punto P_0 si scrivono come $P_0 + \langle v, w \rangle$ con v e w vettori linearmente indipendenti, ovvero $m(X-x_0) + l(Y-y_0) + n(Z-z_0) = 0$ con $(l, m, n) \neq (0, 0, 0)$.

I piani paralleli ad un fissato vettore direzione v_0 (ovvero a una qualsiasi retta r_0 di direzione v_0) si scrivono come $P + \langle v_0, v \rangle$ con P punto qualsiasi e v vettore linearmente indipendente con v_0 , ovvero $aX + bY + cZ + d = 0$ con $d \in C$, $(a, b, c) \neq (0, 0, 0)$ tale che $al_0 + bm_0 + cn_0 = 0$.

Tre piani distinti π_0, π_1 e π_2 che non appartengano ad un fascio determinano una stella di piani che si descrive tramite

$$\lambda(a_0X + b_0Y + c_0Z + d_0) + \mu(a_1X + b_1Y + c_1Z + d_1) + \nu(a_2X + b_2Y + c_2Z + d_2) = 0$$

ovvero

$$(\lambda a_0 + \mu a_1 + \nu a_2)X + (\lambda b_0 + \mu b_1 + \nu b_2)Y + (\lambda c_0 + \mu c_1 + \nu c_2)Z + (\lambda d_0 + \mu d_1 + \nu d_2) = 0$$

per $(\lambda, \mu, \nu) \neq (0, 0, 0)$.

5.3. RETTE.

5.3.1. RETTA PER DUE PUNTI DISTINTI. La retta per due punti distinti P_0, P_1 si scrive $P_0 + \langle P_1 - P_0 \rangle$; ha equazioni parametriche

$$\begin{cases} X = x_0 + \alpha(x_1 - x_0) \\ Y = y_0 + \alpha(y_1 - y_0) \\ Z = z_0 + \alpha(z_1 - z_0) \end{cases}$$

ed equazioni cartesiane date dalla condizione:

$$\text{rk} \begin{pmatrix} X-x_0 & x_1-x_0 \\ Y-y_0 & y_1-y_0 \\ Z-z_0 & z_1-z_0 \end{pmatrix} = 1, \quad \text{ovvero} \quad \text{rk} \begin{pmatrix} 1 & 1 & 1 \\ X & x_0 & x_1 \\ Y & y_0 & y_1 \\ Z & z_0 & z_1 \end{pmatrix} = 2.$$

5.3.2. RETTA PER UN PUNTO E DI DIREZIONE UN VETTORE. La retta per un punto P_0 e di direzione un vettore non nullo v_0 si scrive $P_0 + \langle v_0 \rangle$; ha equazioni parametriche

$$\begin{cases} X = x_0 + \alpha l_0 \\ Y = y_0 + \alpha m_0 \\ Z = z_0 + \alpha n_0 \end{cases}$$

ed equazioni cartesiane date da:

$$\text{rk} \begin{pmatrix} X-x_0 & l_0 \\ Y-y_0 & m_0 \\ Z-z_0 & n_0 \end{pmatrix} = 1, \quad \text{ovvero} \quad \text{rk} \begin{pmatrix} 1 & 1 & 0 \\ X & x_0 & l_0 \\ Y & y_0 & m_0 \\ Z & z_0 & n_0 \end{pmatrix} = 2.$$

5.3.3. POSIZIONE RECIPROCHE DI DUE RETTE. Date due rette $r_0 = P_0 + \langle v_0 \rangle$ e $r_1 = P_1 + \langle v_1 \rangle$ di equazioni cartesiane rispettivamente $\begin{cases} a_0X + b_0Y + c_0Z + d_0 = 0 \\ a'_0X + b'_0Y + c'_0Z + d'_0 = 0 \end{cases}$ e $\begin{cases} a_1X + b_1Y + c_1Z + d_1 = 0 \\ a'_1X + b'_1Y + c'_1Z + d'_1 = 0 \end{cases}$, esse risultano:

- (1) sghembe se v_0 e v_1 sono linearmente indipendenti e $r_0 \cap r_1 = \emptyset$, ovvero sse la matrice incompleta del sistema delle due rette ha rango tre, e la matrice completa rango quattro;
- (2) incidenti e distinte se v_0 e v_1 sono linearmente indipendenti e $r_0 \cap r_1 \neq \emptyset$; ovvero sse le matrici incompleta e completa hanno rango tre. In tal caso il piano di appartenenza è dato da $P_0 + \langle v_0, v_1 \rangle$ ed è l'unico piano appartenente a entrambi i fasci di asse le due rette. Il punto di incidenza ha coordinate date dalla soluzione del sistema delle quattro equazioni.
- (3) parallele e distinte se v_0 e v_1 sono linearmente dipendenti e $r_0 \cap r_1 = \emptyset$; ovvero sse la matrice incompleta ha rango due e la matrice completa ha rango tre. Il piano di appartenenza è $P_0 + \langle P_1 - P_0, v_0 \rangle$ ed è l'unico piano appartenente a entrambi i fasci di asse le due rette.
- (4) coincidenti se v_0 e v_1 sono linearmente dipendenti e $r_0 \cap r_1 \neq \emptyset$; ovvero sse la matrice incompleta e la matrice completa hanno rango due.

5.3.4. FASCI DI RETTE IN UN PIANO. Usando equazioni cartesiane, si tratta di intersecare il piano dato con la stella dei piani che soddisfano alle condizioni poste (passaggio per un punto o contenente una fissata direzione).

Se $\pi_0 = P_0 + \langle v_0, v'_0 \rangle$ è il piano di giacenza, e si tratta del fascio per $P_1 \in \pi_0$, il fascio di rette si scrive come $P_1 + \langle \alpha v_0 + \beta v'_0 \rangle$ con $(\alpha, \beta) \neq (0, 0)$; se si tratta del fascio di rette di direzione $v_1 \in \langle v_0, v'_0 \rangle$ allora si scrive come $(P_0 + \alpha v_0 + \beta v'_0) + \langle v_1 \rangle$ con (α, β) qualsiasi.

5.3.5. STELLE DI RETTE. Le rette passanti per un fissato punto P_0 si scrivono come $P_0 + \langle \begin{pmatrix} l \\ m \\ n \end{pmatrix} \rangle$ con $\begin{pmatrix} l \\ m \\ n \end{pmatrix} \neq \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$, ovvero scegliendo due equazioni indipendenti tra le seguenti:
 $m(X-x_0) - l(Y-y_0) = 0$, $n(X-x_0) - l(Z-z_0) = 0$ e $n(Y-y_0) - m(Z-z_0) = 0$.

Le rette parallele ad un fissato vettore direzione v_0 si scrivono come $P + \langle v_0 \rangle$ con $P = \begin{pmatrix} x \\ y \\ z \end{pmatrix}$ punto qualsiasi, ovvero scegliendo due equazioni indipendenti tra le seguenti:

$$m_0(X-x) - l_0(Y-y) = 0, n_0(X-x) - l_0(Z-z) = 0 \text{ e } n_0(Y-y) - m_0(Z-z) = 0.$$

5.4. POSIZIONI RECIPROCHE DI RETTE E PIANI: dati un piano $\pi_0 = P_0 + \langle v_0, v'_0 \rangle$ e una retta $r_1 = P_1 + \langle v_1 \rangle$, di equazioni cartesiane rispettivamente $a_0X + b_0Y + c_0Z + d_0 = 0$ e $\begin{cases} a_1X + b_1Y + c_1Z + d_1 = 0 \\ a'_1X + b'_1Y + c'_1Z + d'_1 = 0 \end{cases}$, essi risultano:

- (1) incidenti se v_0, v'_0 e v_1 sono linearmente indipendenti; ciò accade sse le matrici completa e incompleta del sistema piano-retta hanno rango comune tre; le coordinate del punto di intersezione si ottengono applicando la regola di Cramer a tale sistema;
- (2) paralleli e disgiunti se $v_1 \in \langle v_0, v'_0 \rangle$ (i.e. se v_0, v'_0 e v_1 sono linearmente dipendenti) e $\pi_0 \cap r_1 = \emptyset$; ovvero sse la matrice incompleta ha rango due e la matrice completa ha rango tre.
- (3) appartenersi se $v_1 \in \langle v_0, v'_0 \rangle$ (i.e. se v_0, v'_0 e v_1 sono linearmente dipendenti) e $\pi_0 \cap r_1 \neq \emptyset$; ovvero sse le matrici incompleta e completa hanno rango due. In tal caso $r_1 \subseteq \pi_0$.

5.5. AFFINITÀ DELLO SPAZIO. La scelta di un riferimento affine sullo spazio $\mathbb{A}^3(C)$ determina un isomorfismo del gruppo $\text{Aff}(\mathbb{A}^3(C))$ delle affinità dello spazio con il sottogruppo

$$\left\{ \left(\begin{array}{cccc} 1 & 0 & 0 & 0 \\ a & b & c & A \end{array} \right) \mid a, b, c \in C; A \in \text{GL}_3(C) \right\}$$

di $\text{GL}_4(C)$.

5.5.1. AZIONE SULLE RETTE E SUI PIANI. L'immagine di una retta $r = P \vee Q$ (risp. $r = P + \langle v \rangle$) tramite una affinità F (di applicazione lineare associata φ) si calcola più facilmente come $F(r) = F(P) \vee F(Q)$ (risp. $F(r) = F(P) + \langle \varphi(v) \rangle$).

L'immagine di un piano $\pi = P \vee Q \vee R$ (risp. $\pi = P + \langle v, w \rangle$) tramite una affinità F (di applicazione lineare associata φ) si calcola più facilmente come $F(\pi) = F(P) \vee F(Q) \vee F(R)$ (risp. $F(\pi) = F(P) + \langle \varphi(v), \varphi(w) \rangle$).

Se la retta r o il piano π sono dati tramite equazioni cartesiane, per calcolare $F(r)$ o $F(\pi)$ bisogna usare la matrice inversa di F in quel riferimento.

5.5.2. SIMMETRIE RISPETTO A PUNTI, RETTE E PIANI. La matrice associata alla simmetria dello spazio rispetto al punto $P = \begin{pmatrix} x_0 \\ y_0 \\ z_0 \end{pmatrix}$ è tale che $A = -\mathbb{I}_3$, e $\begin{pmatrix} a \\ b \\ c \end{pmatrix} = \begin{pmatrix} 2x_0 \\ 2y_0 \\ 2z_0 \end{pmatrix}$.

La matrice associata alla simmetria dello spazio di asse la retta $P + \langle u \rangle$ e di direzione $\langle v, w \rangle$, ove $P = \begin{pmatrix} x_0 \\ y_0 \\ z_0 \end{pmatrix}$, è tale che, posto $B = (u \ v \ w)$ (matrice invertibile d'ordine tre), $A = B \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix} B^{-1}$, e $\begin{pmatrix} a \\ b \\ c \end{pmatrix} = B \begin{pmatrix} 0 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix} B^{-1} \begin{pmatrix} x_0 \\ y_0 \\ z_0 \end{pmatrix}$.

La matrice associata alla simmetria dello spazio di asse il piano $P + \langle u, v \rangle$ e di direzione $\langle w \rangle$, ove $P = \begin{pmatrix} x_0 \\ y_0 \\ z_0 \end{pmatrix}$, è tale che, posto $B = (u \ v \ w)$ (matrice invertibile d'ordine tre), $A = B \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix} B^{-1}$, e $\begin{pmatrix} a \\ b \\ c \end{pmatrix} = B \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 2 \end{pmatrix} B^{-1} \begin{pmatrix} x_0 \\ y_0 \\ z_0 \end{pmatrix}$.

6. Spazi affini di dimensione quattro.

La stesura di questa sezione, sulla falsariga delle precedenti, è un esercizio per il lettore.

7. Esercizi.

7.1. In ciascuno dei seguenti casi determinare un'equazione cartesiana della retta di $\mathbb{A}^2(\mathbb{C})$ contenente i punti:

- (a) $(-1, -1), (3, 2i)$, (b) $(-1, i), (-i, -i)$, (c) $(1, 2i), (1, -2i)$.

7.2. Verificare se le seguenti rette di $\mathbb{A}^2(\mathbb{C})$ sono in un fascio: $r : 3i + iX_1 - X_2 = 0$, $s : 5 + X_1 + 3iX_2 = 0$, $t : 1 + X_1 - iX_2 = 0$.

7.3. Verificare se le rette $r : \begin{cases} 1 - X_1 + X_2 = 0 \\ X_1 - 2X_2 + X_3 = 0 \end{cases}$, $s : \begin{cases} 1 + X_2 - 3X_3 = 0 \\ 1 - 2X_1 - 2X_2 = 0 \end{cases}$ di $\mathbb{A}^3(\mathbb{R})$ sono sghembe oppure incidenti.

7.4. Per ogni $t \in \mathbb{R}$ si consideri il sistema lineare $\Sigma_t : \begin{cases} -tx + (t-1)y + z = -1 \\ (t-1)y + tz = 1 \\ 2x + z = 5 \end{cases}$. Sia S_t l'insieme delle soluzioni di Σ_t .

- (a) Per quali valori di t S_t è costituito da un solo punto?
 (b) Per quali valori di t S_t è vuoto?
 (c) Per quali valori di t S_t è una sottovarietà lineare affine di dimensione 1?
 (d) Per i valori di t di cui al punto (c), esibire equazioni parametriche di S_t .

7.5. Nello spazio affine tridimensionale, sono date tre famiglie di piani di equazioni

$$a_\lambda : X + \lambda Z = \lambda \quad b_\lambda : \lambda X + Y + (1 + \lambda^2)Z = \lambda^2 \quad c_\lambda : (1 - \lambda)X - Y - Z = 1 - \lambda^2$$

al variare del parametro $\lambda \in \mathbb{R}$.

- (a) determinare per quali valori di λ i tre piani si intersecano esattamente in un punto, e per tali valori determinare il punto di intersezione P_λ .
 (b) determinare se esistono valori di λ per i quali i tre piani si intersecano in una retta, ed eventualmente dare una espressione parametrica per questa retta.
 (c) determinare se esistono valori di λ per i quali i tre piani non hanno punti in comune.
 (d) è vero che le soluzioni del sistema formato dai tre piani al variare del parametro $\lambda \in \mathbb{R}$ giacciono tutte su uno stesso piano?

7.6. Discutere (usando il teorema di Rouché-Capelli) tutte le posizioni reciproche possibili delle seguenti costellazioni di sottovarietà affini lineari:

- (1) tre piani in $\mathbb{A}^3(\mathbb{R})$; (2) quattro piani in $\mathbb{A}^3(\mathbb{R})$; (3) un piano ed una retta in $\mathbb{A}^3(\mathbb{R})$;
 (4) due piani in $\mathbb{A}^4(\mathbb{R})$; (5) tre piani in $\mathbb{A}^4(\mathbb{R})$;
 (6) tre iperpiani in $\mathbb{A}^4(\mathbb{R})$; (7) quattro iperpiani in $\mathbb{A}^4(\mathbb{R})$.

7.7. Siano r_1, r_2 ed r_3 tre fissate rette a due a due sghembe nello spazio affine tridimensionale reale. Sia L l'insieme di tutte le rette che si appoggiano a tutte e tre le rette date (cioè che intersecano sia r_1 che r_2 che r_3), e sia C il sottinsieme dello spazio affine dato dall'unione di tutte le rette in L . Descrivere L e C .

In particolare, se r_1, r_2 ed r_3 hanno equazioni rispettivamente $\begin{cases} X = 0 \\ Y = 0 \end{cases}$, $\begin{cases} X = 1 \\ Z = 0 \end{cases}$ e $\begin{cases} Y = 1 \\ Z = 1 \end{cases}$ dare delle equazioni per la generica retta in L , e scrivere una equazione che descriva l'insieme C .

7.8. Un *quadrilatero piano completo* \mathcal{Q} del piano affine $\mathbb{A}^2(\mathbb{C})$ è la figura costituita da quattro rette $r_i, i = 1, 2, 3, 4$ a due a due non parallele, e a tre a tre non appartenenti ad uno stesso fascio. Le rette $r_i, i = 1, 2, 3, 4$ sono dette i *lati* di \mathcal{Q} ; i sei punti d'intersezione $P_{ij} = r_i \cap r_j$, ove $1 \leq i < j \leq 4$ sono detti i *vertici*; due vertici si dicono *opposti* se non appartengono ad uno stesso lato; le rette che congiungono una coppia di vertici opposti si dicono *diagonali*. Si faccia il disegno della figura seguendo la descrizione, e si mostri che i punti medi delle tre diagonali (cioè dei segmenti delimitati dalle coppie di vertici opposti) sono allineati.

7.9. Si scriva l'equazione del piano di $\mathbb{A}^3(C)$ passate per il punto $P = \begin{pmatrix} 1 \\ 0 \\ -2 \end{pmatrix}$ e parallelo alle rette r, s di equazioni rispettive $X = Y = Z$ e $X + 3Y = 0 = X - Y + Z - 1$.

7.10. Si scriva l'equazione della retta t di $\mathbb{A}^3(C)$ passate per il punto $P = \begin{pmatrix} 1 \\ 0 \\ -2 \end{pmatrix}$ e complanare alle rette r, s di equazioni rispettive $X = Y = Z$ e $X + 3Y = 0 = X - Y + Z - 1$. Si verifichi poi se t è incidente o parallela a r ed s .

7.11. Nel piano affine $\mathbb{A}^2(C)$ si considerino due rette r, s distinte, tre punti distinti P_1, P_2, P_3 di r , ed altri tre punti Q_1, Q_2, Q_3 di s distinti tra di loro e dai precedenti. Si indichi con u_{ij} la retta passante per P_i e Q_j , e si mostri che i tre punti $u_{12} \cap u_{21}, u_{13} \cap u_{31}, u_{23} \cap u_{32}$ sono allineati.

7.12. Si considerino le tre rette r, s, t di $\mathbb{A}^3(C)$ di equazioni rispettive

$$X + 3Y = 0 = X - Y + Z - 1, \quad X = Y = Z, \quad X = -Y = 1;$$

- (i) Si mostri che per ogni punto P di t passa una ed una sola retta u_P complanare con r ed s .
- (ii) Si mostri che se $P \neq Q$ sono due punti di t , allora u_P ed u_Q sono sghembe;
- (iii) Si trovino le coordinate del punto P di t per cui passa una retta parallela ad r ed incidente s .

7.13. Si considerino le tre rette r, s, t di $\mathbb{A}^3(C)$ di equazioni rispettive

$$X = 2Y - 1, Z = 1; \quad X = Y + 1, Z = -1; \quad X = Y = Z - 1.$$

- (i) Si trovino un punto P di r ed un punto Q di s tali che il punto medio del segmento PQ appartenga a t .
- (ii) Si trovi il luogo dei punti medi dei segmenti con un estremo in r e l'altro in s .

7.14. Nello spazio affine $\mathbb{A}^3(\mathbb{R})$ si considerino i piani $\gamma : 3x - y = 3$, $\pi : x + y - 4z = -1$, e la famiglia di coppie di piani (α_k, β_k) di equazioni $\alpha_k : kx + y + 2z = 1$, $\beta_k : x - 2y - kz = 2$, al variare di k in \mathbb{R} .

- (a) Dimostrare che i piani α_k, β_k si intersecano in una retta r_k e dare equazioni parametriche di questa retta per ogni valore di k in \mathbb{R} .
- (b) Studiare la posizione reciproca tra la retta r_k ed il piano γ al variare di k in \mathbb{R} .
- (c) Esiste k in \mathbb{R} tale che la retta r_k sia parallela alla retta $\gamma \cap \pi$?

7.15. Nello spazio affine $\mathbb{A}^3(\mathbb{R})$ si consideri la famiglia di terne di piani $(\alpha_s, \beta_s, \gamma_s)$ di equazioni

$$-(2s + 1)x + 2sy + z = -1, \quad 2x + z = 5, \quad 2sy + (2s + 1)z = 1,$$

al variare di s in \mathbb{R} .

- (a) Per quali valori di s l'intersezione dei piani $\alpha_s, \beta_s, \gamma_s$ è costituita da un punto?
- (b) Per quali valori di s l'intersezione dei piani $\alpha_s, \beta_s, \gamma_s$ è vuota?
- (c) Per quali valori di s l'intersezione dei piani $\alpha_s, \beta_s, \gamma_s$ è una retta?
- (d) Per i valori di s di cui al punto (c), esibire equazioni parametriche della retta $r_s = \alpha_s \cap \beta_s \cap \gamma_s$.

7.16. Si considerino, al variare di λ tra i numeri reali, i piani $\alpha_\lambda, \beta_\lambda, \gamma_\lambda$ di $\mathbb{A}^3(\mathbb{R})$ di equazioni

$$(\lambda + 1)x + 2y - (\lambda + 1)z = 1 - \lambda, \quad (-\lambda + 1)x - \lambda y + (\lambda + 1)z = \lambda, \quad 2x - z = 0.$$

Senza risolvere il sistema formato dalle tre equazioni si risponda ai seguenti quesiti:

- (a) Per quali valori di λ l'insieme $\alpha_\lambda \cap \beta_\lambda \cap \gamma_\lambda$ è un punto?
- (b) Per quali valori di λ l'insieme $\alpha_\lambda \cap \beta_\lambda \cap \gamma_\lambda$ è una retta?
- (c) Per quali valori di λ l'insieme $\alpha_\lambda \cap \beta_\lambda \cap \gamma_\lambda$ è vuoto?

7.17. Nello spazio affine standard $\mathbb{A}^3(\mathbb{R})$ si considerino le tre rette r, s, t , le cui equazioni sono:

$$r : \begin{cases} x - y + z = 1 \\ 2x + 3y = 0 \end{cases}, \quad s : \begin{cases} 2x + y - z = 1 \\ x + y + z = 2 \end{cases}, \quad t : x = y = -z.$$

- (i) Si verifichi che le rette r ed s sono sghembe.
- (ii) Si scrivano le equazioni cartesiane di tutte le rette incidenti t e complanari con r ed s .
- (iii) Si dica se tra le rette di cui in (ii) ve ne sono di parallele ad s .

7.18. Consideriamo i quattro punti $P_0 = \begin{pmatrix} -1 \\ -1 \\ -1 \end{pmatrix}$, $P_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$, $P_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$, $P_3 = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$, e le quattro rette $r_0 : X - Y = 0 = Z - 1$, $r_1 : X + Y - Z = 0 = 2Z - 1$, $r_2 : X - Y = 0 = Z - 2$, $r_3 : X + Y = 0 = Z$. Dire quali rette attraversano il tetraedro formato dai quattro punti, eventualmente specificando le facce o gli spigoli che esse toccano.

7.19. Dati tre punti non allineati di un piano affine reale, le tre rette che essi determinano dividono il piano stesso in sette zone. Descrivere queste zone tramite disequazioni a partire dai punti $P_0 = \begin{pmatrix} 1 \\ 2 \end{pmatrix}$, $P_1 = \begin{pmatrix} 2 \\ 1 \end{pmatrix}$, $P_3 = \begin{pmatrix} -1 \\ -1 \end{pmatrix}$.

Analogamente, dati quattro punti non complanari in uno spazio affine reale tridimensionale, i quattro piani che essi determinano dividono lo spazio stesso in nove zone. Descrivere queste zone tramite disequazioni a partire dai punti $P_0 = \begin{pmatrix} 1 \\ 0 \\ 2 \end{pmatrix}$, $P_0 = \begin{pmatrix} 0 \\ 1 \\ 2 \end{pmatrix}$, $P_0 = \begin{pmatrix} 2 \\ 1 \\ 0 \end{pmatrix}$, $P_0 = \begin{pmatrix} -1 \\ -1 \\ -1 \end{pmatrix}$.

Generalizzare le affermazioni precedenti per spazi affini reali n -dimensionali (dati $n+1$ punti non appartenenti allo stesso iperpiano,...).

7.20. Si considerino le due famiglie di piani in $\mathbb{A}^4(\mathbb{R})$ di equazioni cartesiane:

$$\pi_\lambda : \begin{cases} (4 + \lambda)X_1 + \lambda X_2 + X_3 - \lambda X_4 = 1 \\ (1 + \lambda)X_2 + \lambda X_3 = \lambda \end{cases} \quad \sigma_\lambda : \begin{cases} (4 + \lambda)X_1 + (1 - \lambda)X_3 - \lambda X_4 = -\lambda \\ X_2 + \lambda X_4 = 8\lambda \end{cases}$$

al variare di $\lambda \in \mathbb{R}$.

- Dire per quali valori di λ i due piani si incontrano in un punto e determinare il punto in funzione di λ .
- Per quali valori di λ i due piani hanno intersezione vuota? In tali casi sono paralleli?
- Per quali valori di λ i due piani si intersecano in una retta?
- Dire per quali valori di λ i due piani sono contenuti in una varietà lineare affine di dimensione 3, e determinare equazioni cartesiane per tali spazi.

7.21. Sono dati i piani dello spazio affine $\mathbb{A}^4(\mathbb{R})$:

$$\pi_1 : \begin{cases} -3X_1 - X_2 + 4X_4 = -5 \\ -X_3 + X_4 = 4 \end{cases} \quad \pi_2 : \begin{cases} 4X_1 - 4X_3 + X_4 = 20 \\ 5X_1 - 4X_3 = 20 \end{cases}.$$

- Determinare $\pi_1 \wedge \pi_2$ e $\pi_1 \vee \pi_2$. Esistono sottospazi di dimensione 3 contenenti entrambi i piani?
- Si mostri che per ogni punto P non appartenente a $\pi_1 \cup \pi_2$ passa un unico piano σ_P “conspaziale con π_1 e π_2 ” (cioè tale che le congiungenti $\pi_1 \vee \sigma_P$ e $\pi_2 \vee \sigma_P$ abbiano dimensione 3).
- Sia r la retta per l’origine e direzione e_1 ; descrivere tramite equazione cartesiana l’insieme $\bigcup_{P \in r} \sigma_P$. Si tratta di un sottospazio affine?
- (d*) Generalizzare l’esercizio ad $\mathbb{A}^n(\mathbb{R})$: dati due sottospazi affini \mathbb{L}_1 ed \mathbb{L}_2 di dimensione $n - 2$ tali che ..., per ogni punto P non appartenente alla loro unione, esiste unico ...

7.22. Dare caratterizzazioni geometrica ed algebrica ed espressione esplicita delle simmetrie di $\mathbb{A}_{\mathbb{R}}^3$:

- di asse un punto P e direzione \mathbb{R}^3 ;
- di asse una retta $r = P + \langle u \rangle$ e direzione $\langle v, w \rangle$;
- di asse un piano $\pi = P + \langle u, v \rangle$ e direzione $\langle w \rangle$;
- di asse tutto $\mathbb{A}_{\mathbb{R}}^3$ e direzione 0.

[Esempio per (2): geometricamente è una applicazione F tale che per ogni punto Q si ha $F(Q) - Q \in \langle v, w \rangle$ e $\frac{1}{2}F(Q) + \frac{1}{2}Q \in r$ (cioè con punto medio tra Q e $F(Q)$ in r); nel riferimento affine dato da P, u, v, w è l’applicazione $F(x, y, z) = (x, -y, -z)$; algebricamente si tratta di affinità aventi (almeno) un punto unito e applicazione lineare associata diagonalizzabile di polinomio caratteristico $(x - 1)(x + 1)^2$.]

Generalizzare le descrizioni al caso di simmetrie di $\mathbb{A}_{\mathbb{R}}^n$. Esplicitare il caso $n = 2$.

7.23. Determinare il simmetrici di $s : \begin{cases} z = 5 \\ 4x + y = 8 \end{cases}$ e $\pi : z = 5$ rispetto alla retta r di equazioni

parametriche $\begin{cases} x = 1 + 2t \\ y = 2 - t \\ z = 3 + t \end{cases}$ secondo la direzione $\langle v, w \rangle$ con $v = (1, 0, 0)$ e $w = (0, 1, 1)$. Scrivere

esplicitamente l’espressione della simmetria in questione nel riferimento dato.

7.24. Dare caratterizzazioni geometrica ed algebrica ed espressione esplicita delle proiezioni di $\mathbb{A}_{\mathbb{R}}^3$:

- su un punto P e direzione \mathbb{R}^3 ;
- su una retta $r = P + \langle u \rangle$ e direzione $\langle v, w \rangle$;
- su un piano $\pi = P + \langle u, v \rangle$ e direzione $\langle w \rangle$;
- su tutto $\mathbb{A}_{\mathbb{R}}^3$ e direzione 0.

[Esempio per (3): geometricamente è una applicazione F tale che per ogni punto Q si ha $F(Q) - Q \in \langle w \rangle$ e $F(Q) \in \pi$; nel riferimento affine dato da P , u, v, w è l'applicazione $F(x, y, z) = (x, y, 0)$; algebricamente si tratta di trasformazioni affini aventi (almeno) un punto unito e applicazione lineare associata diagonalizzabile di polinomio caratteristico $x(x-1)^2$.]

Generalizzare le descrizioni al caso di proiezioni di $\mathbb{A}_{\mathbb{R}}^n$. Esplicitare il caso $n = 2$.

7.25. Scrivere le proiezioni di $r : \begin{cases} y - 1 = 0 \\ x - z = 0 \end{cases}$, $s : \begin{cases} x = 1 + t \\ y = 2 - t \\ z = 3 + 2t \end{cases}$ e $\sigma : x - z = 6$ sul piano π di

equazione $x + y = 5$ secondo la direzione $\langle w \rangle$ con $w = (1, 0, 1)$. Spiegare i risultati con un disegno. Scrivere l'espressione della proiezione nel riferimento dato.

7.26. Nello spazio affine $\mathbb{A}^3(\mathbb{R})$ si consideri l'affinità f di matrice

$$A = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 2 & -2 & -1 & 2 \\ 1 & 0 & 2 & -1 \\ 3 & -3 & 0 & 2 \end{pmatrix}$$

rispetto al sistema di riferimento canonico. Determinare le equazioni cartesiane di tutti i piani uniti sotto f . I piani uniti sono in un fascio?

7.27. Nello spazio affine $\mathbb{A}^3(\mathbb{R})$ si consideri l'affinità f di matrice

$$X = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 2 & -2 & -1 & 2 \\ 1 & 0 & 2 & -1 \\ 3 & -3 & 0 & 2 \end{pmatrix}.$$

- Si mostri che esiste un fascio \mathcal{F} costituito tutto di piani uniti per f .
- Si scrivano le equazioni di tutte le rette r di $\mathbb{A}^3(\mathbb{R})$ tali che $f(r)$ sia parallela ad r .

Capitolo VII

Geometria Euclidea ed Hermitiana

In questo capitolo introdurremo una nuova struttura nello spazio vettoriale standard su \mathbb{R} di dimensione n ; si tratta della operazione di “prodotto scalare” tra vettori (il risultato è un numero reale) che vedremo essere la base comune per due nozioni ben note: quella di norma (o lunghezza) di vettori e quella di (misura del coseno dell’) angolo tra due vettori (la “trigonometria” lega queste due nozioni). In particolare avremo una nozione di ortogonalità tra vettori, ed una riscrittura di risultati classici (Pitagora, Euclide, Carnot). Studieremo le trasformazioni che rispettano l’operazione di prodotto scalare, dette isometrie o trasformazioni ortogonali. E vedremo le nozioni di base per il calcolo di volumi (di parallelepipedi e tetraedri r -dimensionali), e il loro legame con il calcolo di determinanti.

Studieremo poi gli spazi euclidei, cioè gli spazi affini reali il cui spazio direttore sia dotato del prodotto scalare.

Estenderemo infine questi argomenti al caso di spazi vettoriali ed affini sul corpo complesso, dando le definizioni fondamentali di Geometria Hermitiana.

Le definizioni verranno date solo per spazi vettoriali standard ed useranno in modo esplicito la base canonica; quindi non sono propriamente “intrinseche”: dare le stesse definizioni usando una base qualsiasi porta a risultati non confrontabili. Per una teoria intrinseca dei “prodotti scalari” bisognerà studiare più in generale le forme bilineari e quadratiche, cosa che si farà in futuro, e sarà molto facilitata dall’averne una conoscenza, seppure non intrinseca, degli spazi euclidei.

1. Spazi Vettoriali Euclidei Reali.

1.1. DEFINIZIONE-TEOREMA (PRODOTTO SCALARE). Sia $V_n(\mathbb{R})$ lo spazio vettoriale standard su \mathbb{R} di dimensione n . Definiamo il prodotto scalare di due vettori $v = (x_i)^t$ e $w = (y_i)^t$ come $v \cdot w := v^t w = \sum_i x_i y_i$, ove si sono usate le coordinate nella base canonica.

Il prodotto scalare dà una funzione $V_n(\mathbb{R}) \times V_n(\mathbb{R}) \rightarrow \mathbb{R}$ che gode delle seguenti proprietà:

- (PS1) simmetria: $v \cdot w = w \cdot v$ (per ogni $v, w \in V_n(\mathbb{R})$);
(PS2) bilinearità: $v \cdot (\alpha_1 w_1 + \alpha_2 w_2) = \alpha_1 (v \cdot w_1) + \alpha_2 (v \cdot w_2)$ e $(\alpha_1 v_1 + \alpha_2 v_2) \cdot w = \alpha_1 (v_1 \cdot w) + \alpha_2 (v_2 \cdot w)$ (per ogni $v, v_1, v_2, w, w_1, w_2 \in V_n(\mathbb{R})$, ed ogni $\alpha_1, \alpha_2 \in \mathbb{R}$);
(PS3) positività: $v \cdot v \geq 0$ (per ogni $v \in V_n(\mathbb{R})$); $v \cdot v = 0$ se e solo se $v = 0$.

Lo spazio vettoriale $V_n(\mathbb{R})$ dotato del prodotto scalare si dice lo spazio euclideo (reale) standard di dimensione n .

DIMOSTRAZIONE. Facili conti. □

1.2. DEFINIZIONE (NORMA). La norma di un vettore $v \in V_n(\mathbb{R})$ è definita come

$$\|v\| := \sqrt{v \cdot v}$$

(si usa la positività). Un vettore di norma 1 si dice un versore.

1.3. TEOREMA (DISUGUAGLIANZA DI CAUCHY-SCHWARZ). Per ogni $v, w \in V_n(\mathbb{R})$ vale che

$$(v \cdot w)^2 \leq (v \cdot v)(w \cdot w)$$

e dunque

$$|v \cdot w| \leq \|v\| \|w\|.$$

Inoltre vale l’uguaglianza se e solo se v e w sono linearmente dipendenti.

DIMOSTRAZIONE. Supponiamo v e w non nulli (altrimenti è ovvio) e usiamo la disuguaglianza $(v + \lambda w) \cdot (v + \lambda w) \geq 0$ per ogni $\lambda \in \mathbb{R}$. Svolgendo il prodotto per bilinearità otteniamo

$$v \cdot v + 2\lambda v \cdot w + \lambda^2 w \cdot w \geq 0$$

per ogni $\lambda \in \mathbb{R}$; da questo segue che il discriminante dell'equazione di secondo grado in λ dev'essere negativo o nullo: $(v \cdot w)^2 - (v \cdot v)(w \cdot w) \leq 0$, da cui la disuguaglianza. Se poi vale l'uguaglianza allora per $\lambda = -\frac{v \cdot w}{w \cdot w}$ abbiamo $v + \lambda w = 0$; viceversa se v e w sono linearmente dipendenti possiamo supporre $v = \alpha w$ e i due lati della disequazione sono entrambi uguali ad $\alpha^2(v \cdot v)$.

Una dimostrazione alternativa si può ottenere sostituendo direttamente $\lambda = w \cdot w$ e $\mu = -v \cdot w$ nella disuguaglianza $(\lambda v + \mu w) \cdot (\lambda v + \mu w) \geq 0$. \square

1.3.1. Si osservi che per x_1, \dots, x_n e y_1, \dots, y_n n -uple in \mathbb{R} abbiamo $(\sum_i x_i y_i)^2 \leq (\sum_i x_i^2)(\sum_i y_i^2)$. Per quali termini differiscono i due membri della disuguaglianza? Si può dimostrare questa disuguaglianza in modo più elementare?

1.4. TEOREMA (PROPRIETÀ DELLA NORMA).

- (N1) $\|v\| = 0$ se e solo se $v = 0$;
 (N2) $\|\alpha v\| = |\alpha| \|v\|$;
 (N3) $\|v + w\| \leq \|v\| + \|w\|$ (disuguaglianza triangolare);
 (N4) $\|v \pm w\|^2 = \|v\|^2 \pm 2(v \cdot w) + \|w\|^2$ (teorema di Carnot);
 (N5) $\|v + w\|^2 + \|v - w\|^2 = 2(\|v\|^2 + \|w\|^2)$.

DIMOSTRAZIONE. I primi due e gli ultimi due punti sono facili a partire dalle definizioni; per esempio l'ultimo si ottiene così:

$$\begin{aligned} \|v + w\|^2 + \|v - w\|^2 &= (v + w) \cdot (v + w) + (v - w) \cdot (v - w) \\ &= (v \cdot v + 2v \cdot w + w \cdot w) + (v \cdot v - 2v \cdot w + w \cdot w) = 2v \cdot v + 2w \cdot w. \end{aligned}$$

La disuguaglianza triangolare segue da quella di Cauchy-Schwarz: considerando infatti i quadrati si ha

$$\|v + w\|^2 = (v + w) \cdot (v + w) = v \cdot v + 2v \cdot w + w \cdot w \leq \|v\|^2 + 2\|v\| \|w\| + \|w\|^2 = (\|v\| + \|w\|)^2. \quad \square$$

1.5. DEFINIZIONE (MISURA DI ANGOLI). *Nozione di misura (del coseno) dell'angolo $\vartheta(v, w)$ tra due vettori non nulli $v, w \in V_n(\mathbb{R})$:*

$$\cos \vartheta(v, w) := \frac{v \cdot w}{\|v\| \|w\|}$$

(ha senso per la disuguaglianza di Cauchy-Schwarz).

1.5.1. Usando la funzione arcocoseno (arccos dell'Analisi) possiamo anche definire la misura dell'angolo propriamente detta. In effetti tale funzione è definita da

$$\arccos(x) = \int_x^1 \frac{1}{\sqrt{1-t^2}} dt \quad \text{e} \quad \arccos(-1) = \pi$$

(in cui si riconoscerà un integrale che dà una "lunghezza d'arco" della circonferenza unitaria), in maniera del tutto indipendente dalla geometria.

1.6. DEFINIZIONE (ORTOGONALITÀ). *Due vettori $v, w \in V_n(\mathbb{R})$ si dicono ortogonali e si scrive $v \perp w$ se vale $v \cdot w = 0$ (il loro prodotto scalare è zero).*

1.6.1. Si noti che 0 è l'unico vettore ortogonale a tutti i vettori dello spazio. In particolare si mostri che se $v \cdot w = 0$ per ogni $w \in V_n(\mathbb{R})$, allora $v = 0$ (basta che la condizione valga per i vettori w appartenenti ad una base qualsiasi di $V_n(\mathbb{R})$?).

1.6.2. Due vettori ortogonali e non nulli sono linearmente indipendenti; più in generale un insieme di vettori non nulli a due a due ortogonali è linearmente indipendente; infatti da $\sum_i \alpha_i v_i = 0$, usando il prodotto scalare con v_j si deduce $\alpha_j v_j \cdot v_j = 0$, da cui $\alpha_j = 0$, per ogni j .

1.7. TEOREMA (PITAGORA). *Abbiamo che $v \perp w$ se e solo se $\|v + w\|^2 = \|v\|^2 + \|w\|^2$. In generale vale il teorema del coseno: $\|v \pm w\|^2 = \|v\|^2 + \|w\|^2 \pm 2\|v\| \|w\| \cos \vartheta(v, w)$.*

DIMOSTRAZIONE. Segue immediatamente dalle definizioni poste e dalle proprietà già viste della norma. Si osservi che la definizione di misura del coseno dell'angolo che abbiamo dato è "giustificata" da questi risultati, nel senso che risulta compatibile con le nozioni della geometria elementare. \square

1.8. DEFINIZIONE (PROIEZIONE ORTOGONALE). *Proiezione ortogonale di un vettore v nella direzione di w :*

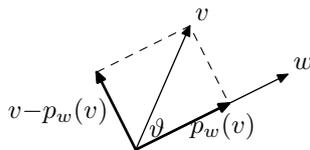
$$p_w(v) = \frac{v \cdot w}{\|w\|^2} w = \frac{v \cdot w}{w \cdot w} w .$$

Risulta che $p_w(v) \perp (v - p_w(v))$.

1.8.1. INTERPRETAZIONE ELEMENTARE. La definizione precedente si giustifica in questo modo: la proiezione ortogonale di v nella direzione di w dev'essere un vettore di direzione quella di w (dunque di versore $w/\|w\|$) e di lunghezza la proiezione della lunghezza di v lungo w , dunque $\|v\| \cos \vartheta(v, w)$; in conclusione:

$$\|v\| \cos \vartheta(v, w) \frac{w}{\|w\|} = \|v\| \frac{v \cdot w}{\|v\| \|w\|} \frac{w}{\|w\|} = \frac{v \cdot w}{\|w\|^2} w$$

come si vede dal disegno:



1.8.2. Si ha che $v + w = p_{v+w}(v) + p_{v+w}(w)$, i.e. $v - p_{v+w}(v) = -(w - p_{v+w}(w))$ (farsi un buon disegno può aiutare ad identificare un'altezza del triangolo di lati v , w e $v + w$).

1.9. TEOREMA (EUCLIDE). *Siano $v, w \in V_n(\mathbb{R})$; allora:*

- (1) $v \perp w$ se e solo se $\|v\|^2 = \|v + w\| \|p_{v+w}(v)\|$ (riconoscere il quadrato di un cateto e il rettangolo costruito sull'ipotenusa con la proiezione del cateto);
- (2) $v \perp w$ se e solo se $\|v - p_{v+w}(v)\|^2 = \|p_{v+w}(v)\| \|p_{v+w}(w)\|$ (riconoscere il quadrato dell'altezza relativa all'ipotenusa e il rettangolo costruito dalle proiezioni dei cateti).

DIMOSTRAZIONE. Si osservi che $\|p_{v+w}(v)\| = |v \cdot (v + w)| / \|v + w\|$, da cui (1) segue quasi immediatamente confrontando $\|v\|$ con $v \cdot (v + w)$.

Per (2) si osservi che $\|v - p_{v+w}(v)\|^2 = \|v\|^2 - \|p_{v+w}(v)\|^2 = (\|v\|^2 \|w\|^2 - (v \cdot w)^2) / \|v + w\|^2$, da cui si conclude confrontando $\|v\|^2 \|w\|^2 - (v \cdot w)^2$ con $|v \cdot (v + w)| |w \cdot (v + w)|$. \square

1.10. BASI ORTOGONALI E ORTONORMALI. Una base di $V_n(\mathbb{R})$ si dice ortogonale se essa è formata di vettori a due a due ortogonali; si dice ortonormale se inoltre i suoi vettori hanno tutti norma 1. Se (v_1, \dots, v_n) è una base ortonormale di $V_n(\mathbb{R})$, allora le coordinate di un vettore $v \in V_n(\mathbb{R})$ in quella base sono date da $\begin{pmatrix} v \cdot v_1 \\ \vdots \\ v \cdot v_n \end{pmatrix}$. Infatti da $v = \sum_i \alpha_i v_i$, usando il prodotto scalare con v_j si deduce $v \cdot v_j = \alpha_j v_j \cdot v_j = \alpha_j$. In altri termini, per ogni vettore v risulta

$$v = \sum_{i=1}^n (v \cdot v_i) v_i = (v \cdot v_1) v_1 + (v \cdot v_2) v_2 + \dots + (v \cdot v_n) v_n .$$

1.10.1. RICERCA DI BASI ORTOGONALI E ORTONORMALI: PROCEDIMENTO DI GRAM-SCHMIDT. Data una base qualsiasi v_1, \dots, v_n di $V_n(\mathbb{R})$ è sempre possibile ricavarne una base ortogonale u_1, \dots, u_n tale che $\langle v_1, \dots, v_i \rangle = \langle u_1, \dots, u_i \rangle$ (per ogni $i = 1, \dots, n$) nel modo seguente: ad ogni passo si aggiunge il vettore u_i ottenuto togliendo a v_i tutte le sue proiezioni ortogonali sui precedenti vettori u_1, \dots, u_{i-1} . Dunque si ha:

$$\begin{aligned} u_1 &= v_1 \\ u_2 &= v_2 - \frac{u_1 \cdot v_2}{u_1 \cdot u_1} u_1 \\ u_3 &= v_3 - \frac{u_1 \cdot v_3}{u_1 \cdot u_1} u_1 - \frac{u_2 \cdot v_3}{u_2 \cdot u_2} u_2 \\ &\dots \\ u_n &= v_n - \sum_{i=1}^{n-1} \frac{u_i \cdot v_n}{u_i \cdot u_i} u_i . \end{aligned}$$

Per ottenere una base ortonormale, basta poi dividere ogni vettore u_i per la sua norma.

Si osservi che il procedimento funziona (cioè fornisce una base ortogonale) anche a partire da un qualsiasi insieme di generatori di $V_n(\mathbb{R})$, eliminando naturalmente i vettori nulli generati dal procedimento stesso.

- 1.11. DEFINIZIONE-TEOREMA (ORTOGONALI DI SOTTOSPACI).** Per S sottinsieme di $V_n(\mathbb{R})$ definiamo l'ortogonale $S^\perp = \{v \in V_n(\mathbb{R}) | v \perp s (\forall s \in S)\}$, che risulta un sottospazio vettoriale. Si ha:
- (O0) $\{0\}^\perp = V_n(\mathbb{R})$, $V_n(\mathbb{R})^\perp = 0$,
 - (O1) Se $S \subseteq T$ allora $T^\perp \subseteq S^\perp$;
 - (O2) $\langle S \rangle = (S^\perp)^\perp$; dunque per W sottospazio: $(W^\perp)^\perp = W$. Inoltre $((S^\perp)^\perp)^\perp = S^\perp$.
 - (O3) Se W e W' sono sottospazi vettoriali di $V_n(\mathbb{R})$: $(W + W')^\perp = W^\perp \cap W'^\perp$
 - (O4) Se W e W' sono sottospazi vettoriali di $V_n(\mathbb{R})$: $(W \cap W')^\perp = W^\perp + W'^\perp$.

DIMOSTRAZIONE. I primi tre punti sono facili. L'ultimo segue dal penultimo applicato agli spazi ortogonali e poi prendendo l'ortogonale. Il penultimo si dimostra così: affinché un vettore sia ortogonale a tutti i vettori di $W + W'$ è necessario che sia ortogonale sia ai vettori di W che a quelli di W' ; dalla bilinearità del prodotto scalare segue che queste due condizioni sono anche sufficienti. \square

1.11.1. RELAZIONI CON GLI ORTOGONALI SUL DUALE. La definizione di prodotto scalare permette di identificare lo spazio duale di $V_n(\mathbb{R})$ con lo spazio $V_n(\mathbb{R})$ stesso nel modo seguente: ad ogni applicazione lineare $\alpha : V_n(\mathbb{R}) \rightarrow \mathbb{R}$ resta associato il vettore dato dalla trasposta della sua matrice nella base canonica, sia v_α . Allora abbiamo $\alpha(v) = v_\alpha \cdot v$ per ogni $v \in V_n(\mathbb{R})$. Da questo isomorfismo $V_n(\mathbb{R})^* \cong V_n(\mathbb{R})$ abbiamo che la nozione di ortogonale qui definita corrisponde a quella definita per gli spazi duali.

1.11.2. TEOREMA (DECOMPOSIZIONI ORTOGONALI). Per ogni sottospazio W di $V_n(\mathbb{R})$ si ha che $W \oplus W^\perp = V_n(\mathbb{R})$, cioè W e W^\perp sono sottospazi complementari (talvolta si scrive $W \boxplus W^\perp$ per indicare la mutua ortogonalità).

DIMOSTRAZIONE. Per il teorema precedente, basta dimostrare che l'intersezione tra W e W^\perp è nulla, e questo discende dal fatto che vettori ortogonali tra loro sono linearmente indipendenti. \square

1.11.3. SOLUZIONI AI MINIMI QUADRATI PER SISTEMI INCOMPATIBILI. Dato un sistema lineare $AX = b$ privo di soluzioni, ci si può chiedere quali siano i vettori x tali che la norma di $Ax - b$ sia minima possibile (quelli dunque che meglio approssimano una soluzione nel senso della distanza euclidea). Ora questa condizione è realizzata se e solo se $Ax - b$ è ortogonale allo spazio generato dalle colonne di A , dunque se e solo se $A^t(Ax - b) = 0$, e dunque se e solo se x risolve il sistema lineare $A^tAX = A^tb$ (la matrice A^tA è simmetrica, e il suo rango è uguale al rango di A : perché?).

Equivalentemente, se decomponiamo $b = a + a'$ con a appartenente al sottospazio generato dalle colonne di A , e a' ortogonale allo stesso sottospazio, si tratta delle soluzioni del sistema lineare $AX = a$ (un lato dell'equivalenza è ovvio: se $Ax = a$ allora $A^tAx = A^ta = A^tb$, poiché $A^ta' = 0$ per ipotesi; d'altro lato, se $A^tAx = A^tb = A^ta$ abbiamo che $Ax - a$ appartiene sia allo spazio delle colonne di A , sia al suo ortogonale, e dunque è nullo).

1.12. DEFINIZIONE-TEOREMA (TRASFORMAZIONI ORTOGONALI O ISOMETRIE). Sia φ un automorfismo di $V_n(\mathbb{R})$ in sé; le due proprietà seguenti sono equivalenti:

- (1) φ rispetta la struttura euclidea, i.e. $\varphi(v) \cdot \varphi(w) = v \cdot w$ per ogni $v, w \in V_n(\mathbb{R})$;
- (2) φ rispetta la norma dei vettori, i.e. $\|\varphi(v)\| = \|v\|$ per ogni $v \in V_n(\mathbb{R})$.

Tali automorfismi si dicono trasformazioni ortogonali o isometrie di $V_n(\mathbb{R})$.

DIMOSTRAZIONE. È ovvio che (1) implica (2) (basta usare $v = w$). Viceversa per vedere che (2) implica (1) basta notare che applicando l'ipotesi a $v + w$ otteniamo $\|\varphi(v) + \varphi(w)\| = \|v + w\|$, da cui $\|\varphi(v)\|^2 + 2\varphi(v) \cdot \varphi(w) + \|\varphi(w)\|^2 = \|v\|^2 + 2v \cdot w + \|w\|^2$, e si conclude che $\varphi(v) \cdot \varphi(w) = v \cdot w$ (per ogni v e w). \square

1.12.1. Una applicazione insiemistica di $V_n(\mathbb{R})$ in sé che soddisfi alla proprietà (1) è necessariamente un morfismo lineare; infatti si tratta di verificare che $\varphi(v + \alpha w) - \varphi(v) - \alpha\varphi(w) = 0$, ovvero che il suo prodotto scalare con sé stesso è nullo.

D'altra parte un morfismo lineare che rispetti la proprietà (2) è necessariamente biiettivo, e dunque un automorfismo. Infatti da $\varphi v = 0$ segue $\|v\| = \|\varphi v\| = 0$, e dunque $v = 0$.

Quindi il teorema poteva essere enunciato così: *una applicazione insiemistica di $V_n(\mathbb{R})$ in sé rispetta il prodotto scalare se e solo se è una applicazione lineare che rispetta la norma; e in tal caso si tratta di una applicazione biiettiva, dunque di un automorfismo.*

1.12.2. Si osservi anche che la proprietà (1) è equivalente alla condizione che $\|\varphi(v) - \varphi(w)\| = \|v - w\|$ per ogni $v, w \in V_n(\mathbb{R})$, unito alla condizione $\varphi(0) = 0$; per questo tali funzioni vengono chiamate isometrie dello spazio vettoriale euclideo (in cui 0 sia un “punto fisso”): rispettano (lo zero e) le distanze tra i punti dello spazio affine associato allo spazio vettoriale euclideo $V_n(\mathbb{R})$.

1.13. TEOREMA (GRUPPO ORTOGONALE). *Sia φ una trasformazione ortogonale. Ogni matrice A associata a φ usando una base di vettori ortonormali (tali che $v_i \cdot v_j = \delta_{i,j}$) risulta una matrice ortogonale, i.e. tale che $A^t A = \mathbb{I}$, ovvero $A^{-1} = A^t$. Le matrici ortogonali formano un sottogruppo (non normale, se $n > 1$) di $GL(n, \mathbb{R})$ che si indica con $O(n, \mathbb{R})$ o $O_n(\mathbb{R})$ e si dice il Gruppo Ortogonale. Se $A \in O(n, \mathbb{R})$, allora $\det A = \pm 1$ e gli autovalori complessi di A hanno tutti modulo 1 (dunque se sono reali sono ± 1).*

DIMOSTRAZIONE. Le colonne $A_{(i)}$ della matrice A sono le immagini dei vettori di una base ortonormale, quindi risulta $A_{(i)} \cdot A_{(j)} = \delta_{i,j}$, da cui segue subito che $A^t A = \mathbb{I}$. Da questo segue che $1 = \det \mathbb{I} = \det(A^t A) = \det(A)^2$, da cui l’asserzione sul determinante.

Se poi α è un autovalore (eventualmente complesso di A) e v autovettore, allora anche il coniugato $\bar{\alpha}$ è autovalore con autovettore \bar{v} (perché la matrice ha coefficienti reali), e allora abbiamo $v^t \bar{v} = (Av)^t \bar{Av} = \alpha \bar{\alpha} v^t \bar{v}$ da cui risulta $|\alpha| = \alpha \bar{\alpha} = 1$ poiché $v^t \bar{v} \neq 0$ (somma di quadrati). \square

1.13.1. GRUPPO ORTOGONALE SPECIALE. Il sottinsieme di $O_n(\mathbb{R})$ formato dalle matrici di determinante 1 si indica con $SO(n, \mathbb{R})$ o $SO_n(\mathbb{R})$ e si dice il Gruppo Ortogonale Speciale. Si tratta di un sottogruppo normale di indice 2 di $O_n(\mathbb{R})$, cioè il quoziente $O_n(\mathbb{R})/SO_n(\mathbb{R})$ è isomorfo a $\{\pm 1\}$ (gruppo moltiplicativo con due elementi).

Si osservi che scelta $S \in O_n(\mathbb{R}) \setminus SO_n(\mathbb{R})$, la moltiplicazione per S induce una biiezione insiemistica $SO_n(\mathbb{R}) \rightarrow O_n(\mathbb{R}) \setminus SO_n(\mathbb{R})$ (qual’è l’applicazione inversa? perché non si parla di morfismo di gruppi?).

1.13.2. FORMULA DI PARSEVAL REALE. Se v_1, \dots, v_n è base ortonormale di $V_n(\mathbb{R})$, allora sappiamo che le coordinate di $v \in V_n(\mathbb{R})$ in questa base sono date da Ax ove x è la colonna delle componenti di v (coordinate di v nella base canonica) e A è matrice ortogonale del cambiamento di base dalla base canonica alla base data. Dunque risulta $v \cdot w = x^t y = x^t A^t A y = (Ax)^t (Ay)$, ovvero il prodotto scalare tra v e w si può calcolare facendo la somma dei prodotti delle coordinate omonime in una qualsiasi base ortonormale di $V_n(\mathbb{R})$.

Ricordando poi che la coordinata i -esima di v nella base ortonormale v_1, \dots, v_n è data da $v \cdot v_i$ otteniamo la cosiddetta formula di Parseval (reale): se v_1, \dots, v_n è base ortonormale di $V_n(\mathbb{R})$ e $v, w \in V_n(\mathbb{R})$ allora $v \cdot w = \sum_{i=1}^n (v \cdot v_i)(w \cdot v_i)$.

1.13.3. MATRICI DI SIMMETRIE ASSIALI. Consideriamo un vettore non nullo $v \in V_n(\mathbb{R})$ e scriviamo la matrice della simmetria di direzione v e asse l’iperpiano ortogonale v^\perp . Si tratta dell’applicazione s che manda un generico vettore x in $s(x) = x - 2p_v(x) = x - 2\frac{x \cdot v}{v \cdot v} v = (\text{id} - 2\frac{v v^t}{v \cdot v})x$ da cui si legge direttamente la matrice. Se supponiamo $v \cdot v = v^t v = 1$, allora la matrice di s è data da $\mathbb{I}_n - 2v v^t$. Si noti che $v v^t$ è la matrice della proiezione su v con direzione v^\perp (quindi matrice di rango 1), mentre $\mathbb{I}_n - v v^t$ è matrice della proiezione su v^\perp con direzione v (quindi di rango $n-1$).

Più generalmente, se W è un sottospazio di $v \in V_n(\mathbb{R})$ di dimensione m possiamo scrivere la matrice della simmetria ortogonale su W (cioè di direzione W^\perp nel modo seguente. Sia w_1, \dots, w_r una base ortonormale di W^\perp ; allora la simmetria s_W in questione ha matrice $\mathbb{I}_n - 2\sum_{i=1}^r w_i w_i^t$. Si osservi che $\sum_{i=1}^r w_i w_i^t$ è la matrice della proiezione ortogonale su W^\perp (dunque di rango $r = n-m$), mentre $\mathbb{I}_n - \sum_{i=1}^r w_i w_i^t$ è la matrice della proiezione ortogonale su W (dunque di rango m).

1.13.4. Supponiamo ora che il sottospazio W sia generato dalle colonne della matrice A (matrice $n \times m$ di rango m); allora:

- (1) se $A^t A = \mathbb{I}_m$ allora AA^t è la matrice della proiezione ortogonale su W , $\mathbb{I}_n - AA^t$ è la matrice della proiezione ortogonale su W^\perp , e $\mathbb{I}_n - 2AA^t$ è la matrice della simmetria ortogonale su asse W ;
- (2) in generale, la matrice della proiezione ortogonale su W è data da $A(A^t A)^{-1} A^t$ (infatti si vede subito che le colonne di A sono autovettori d’autovalore 1, e che i vettori ortogonali alle colonne

di A sono annullati), e dunque la simmetria ortogonale di asse W ha matrice data da $\mathbb{I}_n - 2A(A^t A)^{-1}A^t$. Si osservi la similitudine con il caso di un vettore, e si tenga presente che A non è quadrata (la formula non è stupida).

1.14. TEOREMA (TEOREMA SPETTRALE REALE (VERSIONE MATRICIALE)). *Le matrici reali simmetriche sono ortogonalmente diagonalizzabili, cioè se $A \in M_n(\mathbb{R})$ e $A^t = A$ (simmetrica) allora esiste una matrice ortogonale $P \in O_n(\mathbb{R})$ tale che $P^{-1}AP = P^tAP$ è matrice diagonale (reale).*

DIMOSTRAZIONE. Si procede in tre passi:

(1) dimostriamo che tutti gli autovalori di A sono reali: certamente troviamo tutti gli autovalori in \mathbb{C} , e sia $\alpha \in \mathbb{C}$ un autovalore con autovettore v ; allora dalle uguaglianze

$$\bar{\alpha}(\bar{v}^t v) = (A\bar{v})^t v = \bar{v}^t Av = \bar{v}^t \alpha v = \alpha(\bar{v}^t v)$$

(la seconda uguaglianza è quella fondamentale e usa la simmetria di A , le altre usano il fatto che A è matrice reale: se v è autovettore per α allora \bar{v} è autovettore per $\bar{\alpha}$) e si deduce che $\alpha = \bar{\alpha}$ poiché $\bar{v}^t v \neq 0$. Dunque $\alpha \in \mathbb{R}$.

(2) dimostriamo che gli autospazi sono tra loro ortogonali: se v, w sono autovettori per A relativi agli autovalori α, β diversi tra loro, allora dalle uguaglianze

$$\beta(w^t v) = (Aw)^t v = w^t Av = w^t \alpha v = \alpha(w^t v)$$

(nella seconda uguaglianza si usa la simmetria di A) deduciamo che $(\alpha - \beta)w^t v = 0$ e siccome $\alpha - \beta \neq 0$ otteniamo $w^t v = 0$, cioè che autovettori relativi ad autovalori distinti sono tra loro ortogonale, come si voleva.

(3) dimostriamo ora che esiste una base di autovettori: sia v_1, \dots, v_r un insieme linearmente indipendente massimale di autovettori per A ; allora lo spazio $U = \langle v_1, \dots, v_r \rangle$ è stabile per A , ma anche U^\perp lo è, poiché se $v \in V_n(\mathbb{R})$ è ortogonale ai v_i , anche Av lo è, essendo

$$(Av) \cdot v_i = (Av)^t v_i = v^t Av_i = \alpha_i v^t v_i = 0.$$

Ora, se fosse $U^\perp \neq 0$ troveremmo almeno un altro autovalore e un autovettore relativo, indipendente dai precedenti, il che è assurdo per la massimalità ipotizzata. Dunque $U = V_n(\mathbb{R})$ e abbiamo trovato una base di autovettori. \square

1.14.1. Si osservi che il teorema si può enunciare come una equivalenza: una matrice quadrata reale è simmetrica se e solo se è ortogonalmente diagonalizzabile (il Teorema Spettrale dà l'implicazione difficile, l'altra è quasi ovvia).

1.14.2. PROBLEMA. Per capire bene le relazioni tra matrici ortogonali e matrici (reali) simmetriche, si osservi che: vi sono matrici ortogonali non simmetriche, vi sono matrici simmetriche non ortogonali (farsi degli esempi), e infine che *una matrice reale è ortogonale e simmetrica (ovvero ortogonale e ortogonalmente diagonalizzabile) se e solo se è la matrice di una simmetria ortogonale (cioè di una simmetria in cui asse e direzione sono tra loro ortogonali).*

1.15. TRASFORMAZIONI ORTOGONALI DEL PIANO. Si consideri lo spazio vettoriale reale $V_2(\mathbb{R})$ munito del prodotto scalare e si indichi con $O_2(\mathbb{R})$ il gruppo delle matrici delle isometrie di $V_2(\mathbb{R})$. Si osservi che tali matrici possono avere autovalori reali ± 1 , oppure due autovalori complessi di modulo uno (uno inverso dell'altro, cioè uno coniugato dell'altro).

1.15.1. $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in O_2(\mathbb{R})$ se e solo se le due colonne formano una base ortonormale di $V_2(\mathbb{R})$: se la prima si scrive $\begin{pmatrix} \cos \vartheta \\ \sin \vartheta \end{pmatrix}$, la seconda dev'essere $\pm \begin{pmatrix} -\sin \vartheta \\ \cos \vartheta \end{pmatrix}$; dunque esiste un unico numero reale ϑ , $0 \leq \vartheta < 2\pi$, tale che

$$A = \begin{pmatrix} \cos \vartheta & \mp \sin \vartheta \\ \sin \vartheta & \pm \cos \vartheta \end{pmatrix}$$

ove si prendono o entrambi i segni superiori, o entrambi gli inferiori.

1.15.2. Il sottoinsieme $SO_2(\mathbb{R}) = \left\{ \begin{pmatrix} \cos \vartheta & -\sin \vartheta \\ \sin \vartheta & \cos \vartheta \end{pmatrix} \mid 0 \leq \vartheta < 2\pi \right\}$ di $O_2(\mathbb{R})$ è il gruppo speciale ortogonale del piano $SO_2(\mathbb{R})$ e si dice anche il gruppo delle rotazioni del piano euclideo.

1.15.3. Se $A \in O_2(\mathbb{R}) \setminus SO_2(\mathbb{R})$ allora $A^2 = \mathbb{I}_2$, cioè le matrici ortogonali non speciali sono tutte matrici di riflessioni (ortogonali); è vero il viceversa? Si interpreti tramite un disegno la seguente relazione:

$$\begin{pmatrix} \cos \vartheta & \sin \vartheta \\ \sin \vartheta & -\cos \vartheta \end{pmatrix} = \begin{pmatrix} \cos \frac{\vartheta}{2} & -\sin \frac{\vartheta}{2} \\ \sin \frac{\vartheta}{2} & \cos \frac{\vartheta}{2} \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} \cos \frac{\vartheta}{2} & \sin \frac{\vartheta}{2} \\ -\sin \frac{\vartheta}{2} & \cos \frac{\vartheta}{2} \end{pmatrix}.$$

1.15.4. Invece, in $\text{SO}_2(\mathbb{R})$ vi sono elementi di periodo n , per ogni intero $n \geq 1$, ed elementi di periodo infinito (i.e. $A^n \neq \mathbb{I}_2$ se $n > 0$).

1.15.5. L'applicazione $x \mapsto \begin{pmatrix} \cos 2\pi x & -\sin 2\pi x \\ \sin 2\pi x & \cos 2\pi x \end{pmatrix}$ induce un isomorfismo di gruppi $\varphi: (\mathbb{R}/\mathbb{Z}, +) \rightarrow \text{SO}_2(\mathbb{R})$ (che trasforma la somma in \mathbb{R}/\mathbb{Z} nel prodotto di matrici. Usando la legge di composizione di $\text{SO}_2(\mathbb{R})$ (prodotto di matrici) possiamo riscrivere le formule di addizione per il seno ed il coseno.

1.15.6. L'applicazione $z = a + ic \mapsto A_z = \begin{pmatrix} a & -c \\ c & a \end{pmatrix}$ induce un isomorfismo di gruppi (moltiplicativi) $\mathbb{S}^1 \rightarrow \text{SO}_2(\mathbb{R})$ dei complessi di modulo 1 sul gruppo ortogonale speciale.

1.15.7. Riassumendo, abbiamo i seguenti isomorfismi di gruppi:

$$\begin{aligned} \text{SO}_2(\mathbb{R}) &\cong \mathbb{S}^1 \cong \mathbb{R}/2\pi\mathbb{Z} \\ \begin{pmatrix} \cos \vartheta & -\sin \vartheta \\ \sin \vartheta & \cos \vartheta \end{pmatrix} &\mapsto \cos \vartheta + i \sin \vartheta \mapsto \vartheta \end{aligned}$$

1.15.8. Siano $A, B \in \text{O}_2(\mathbb{R}) \setminus \text{SO}_2(\mathbb{R})$; si mostri che $AB \in \text{SO}_2(\mathbb{R})$ (che rotazione è?); è vero che ogni elemento di $\text{SO}_2(\mathbb{R})$ si può scrivere come prodotto di al più due elementi di $\text{O}_2(\mathbb{R})$ di periodo 2 (due riflessioni fanno una rotazione, e di che angolo?); Di solito si dice che piegando un foglio di carta (ogni punto si scambia con quello sovrapposto dalla piegatura) si possono ottenere tutte le rotazioni del piano.

1.16. TRASFORMAZIONI ORTOGONALI DELLO SPAZIO. Si consideri lo spazio vettoriale reale $V_3(\mathbb{R})$ munito del prodotto scalare; si indichi con $\text{O}_3(\mathbb{R})$ il gruppo delle matrici delle isometrie di $V_3(\mathbb{R})$.

1.16.1. Allora $A \in \text{O}_3(\mathbb{R})$ se e solo se le sue colonne (risp. righe) sono una base ortonormale di \mathbb{R}^3 ; oppure se e solo se $A^t A = \mathbb{I}_3$. Se ne deduca che, se $A \in \text{O}_3(\mathbb{R})$, allora $\det A = \pm 1$, e che $\text{O}_3(\mathbb{R})$ contiene un sottogruppo isomorfo al gruppo \mathfrak{S}_3 delle permutazioni su 3 oggetti (permutazioni dei tre vettori della base canonica).

1.16.2. Il sottoinsieme $\text{SO}_3(\mathbb{R})$ di $\text{O}_3(\mathbb{R})$, costituito dalle matrici di determinante 1, è un sottogruppo normale di $\text{O}_3(\mathbb{R})$ di indice 2.

1.16.3. Per ogni $A \in \text{O}_3(\mathbb{R})$ si ha $\det[(A - \mathbb{I}_3)(A^t + \mathbb{I}_3)] = 0$ (ricordare che il determinante di matrici antisimmetriche d'ordine dispari è nullo), e quindi A possiede l'autovalore 1 oppure -1 . Si arriva allo stesso risultato ricordando che una matrice reale d'ordine dispari deve avere almeno una autovalore reale, e dovendo essere di norma unitaria (come numero complesso) dev'essere uno tra ± 1 .

1.16.4. Per ogni isometria φ esiste una base ortonormale (v_1, v_2, v_3) di \mathbb{R}^3 rispetto alla quale la matrice di φ assume la forma seguente: $B = \begin{pmatrix} \pm 1 & 0 \\ 0 & B' \end{pmatrix}$, ove $B' \in \text{O}_2(\mathbb{R})$.

In particolare se $\det \varphi = 1$ allora possiamo scegliere la base in modo che $B = \begin{pmatrix} 1 & 0 \\ 0 & B' \end{pmatrix}$, ove $B' \in \text{SO}_2(\mathbb{R})$. e si tratta di una rotazione attorno ad un asse

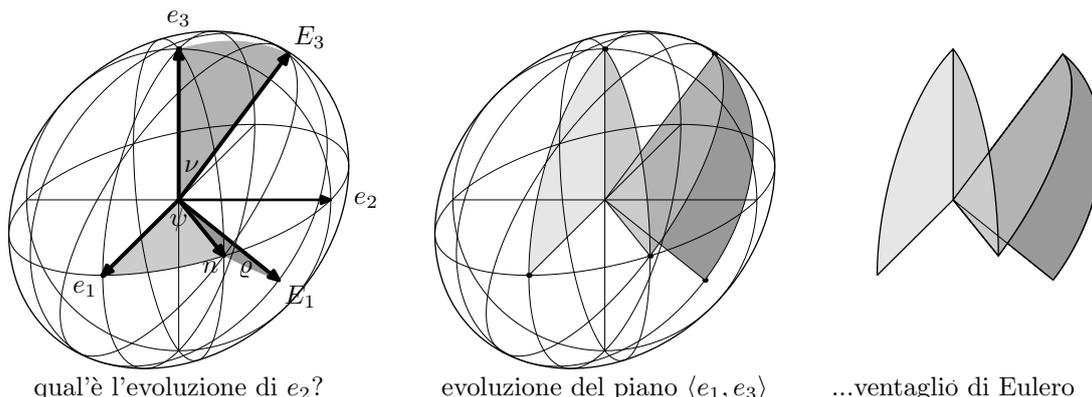
Se invece $\det \varphi = -1$ allora possiamo scegliere la base in modo che $B = \begin{pmatrix} -1 & 0 \\ 0 & B' \end{pmatrix}$, con $B' \in \text{SO}_2(\mathbb{R})$ e si tratta una rotazione seguita da una riflessione di direzione l'asse di rotazione. Come si riduce il caso di $B = \begin{pmatrix} 1 & 0 \\ 0 & B' \end{pmatrix}$, con $B' \in \text{O}_2(\mathbb{R}) \setminus \text{SO}_2(\mathbb{R})$ (rotazione seguita da una riflessione sul piano di rotazione)?

1.16.5. Si mostri che ogni elemento di $\text{O}_3(\mathbb{R})$ si può scrivere come prodotto di al più 3 elementi di periodo 2 (al più 2 se si tratta di elementi di $\text{SO}_3(\mathbb{R})$?).

1.16.6. ANGOLI DI EULERO. Fissate due basi ortonormali e_1, e_2, e_3 ed E_1, E_2, E_3 esiste un unico elemento φ di $\text{SO}_3(\mathbb{R})$ tale che $\varphi e_i = E_i$ ($i = 1, 2, 3$) e si può scrivere come composizione di al più tre rotazioni di angoli opportuni intorno a rette. Possiamo considerare i due piani $\langle e_1, e_2 \rangle$ e $\langle E_1, E_2 \rangle$. Se essi coincidono, allora φ è una rotazione attorno alla retta $\langle e_3 \rangle = \langle E_3 \rangle$, altrimenti la loro intersezione determina una retta, detta retta dei nodi, di versore diciamo n . Si considerino allora le seguenti rotazioni: rotazione di asse e_3 ed angolo $\psi = \vartheta(e_1, n)$ (precessione), rotazione di asse n ed angolo $\nu = \vartheta(e_3, E_3)$ (nutazione), rotazione di asse E_3 ed angolo $\varrho = \vartheta(n, E_1)$ (rotazione propria). La composizione nell'ordine delle tre rotazioni dà φ .

Si può quindi scrivere la matrice della trasformazione φ in termini dei tre angoli di precessione ψ , di nutazione ν e di rotazione propria ϱ tramite la composizione:

$$\begin{aligned} &\begin{pmatrix} \cos \varrho & -\sin \varrho & 0 \\ \sin \varrho & \cos \varrho & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos \nu & -\sin \nu \\ 0 & \sin \nu & \cos \nu \end{pmatrix} \begin{pmatrix} \cos \psi & -\sin \psi & 0 \\ \sin \psi & \cos \psi & 0 \\ 0 & 0 & 1 \end{pmatrix} = \\ &= \begin{pmatrix} \cos \varrho \cos \psi - \sin \varrho \cos \nu \sin \psi & -\cos \varrho \sin \psi + \sin \varrho \cos \nu \cos \psi & \sin \varrho \sin \nu \\ \sin \varrho \cos \psi - \cos \varrho \cos \nu \sin \psi & -\sin \varrho \sin \psi + \cos \varrho \cos \nu \cos \psi & -\cos \varrho \sin \nu \\ \sin \nu \sin \psi & \sin \nu \cos \psi & \cos \nu \end{pmatrix}. \end{aligned}$$



qual'è l'evoluzione di e_2 ?

evoluzione del piano $\langle e_1, e_3 \rangle$

...ventaglio di Eulero

♠♠ **1.16.7.** RELAZIONE CON IL CORPO \mathbb{H} DEI QUATERNIONI. Usiamo in questo numero la nozione di prodotto vettore \times in $V_3(\mathbb{R})$, che sarà introdotta tra poche pagine; preferiamo lasciar qui il paragrafo per non spezzare la discussione sulla struttura del gruppo ortogonale d'ordine 3. Ricordiamo innanzitutto che il sottocorpo dei quaternioni puramente reali, indichiamolo con \mathbb{H}_0 , è isomorfo al corpo dei numeri reali; e osserviamo subito che il sottinsieme, diciamo \mathbb{H}' dei quaternioni speciali o puramente immaginari, cioè la cui parte reale sia nulla, è uno spazio vettoriale reale di dimensione 3 (generato da i, j, k) e in cui l'operazione di prodotto corrisponde all'operazione di prodotto vettoriale tra vettori di \mathbb{R}^3 .

Ancora più precisamente, se indichiamo con $z = (a, v)$ e $z' = (a', v')$ due quaternioni, con $a, a' \in \mathbb{R}$ e $v, v' \in \mathbb{R}^3$ (dunque $z = a + (i, j, k)v$ e $z' = a' + (i, j, k)v'$) abbiamo che $z + z' = (a + a', v + v')$, $zz' = (aa' - v \cdot v', av' + a'v + v \times v')$, da cui si vede che il corpo dei quaternioni già "contiene" le due operazioni di prodotto (scalare e vettoriale) tra vettori: infatti il prodotto di due quaternioni speciali è dato da $(0, v)(0, v') = (-v \cdot v', v \times v')$.

Consideriamo ora il sottinsieme dei quaternioni di norma unitaria, sia $\mathbb{H}^1 = \{q \in \mathbb{H} \mid \|q\| = 1\}$. Essi si scrivono unicamente tramite un angolo ϑ (compreso tra 0 e π escluso) e un vettore $u \in \mathbb{S}^2$ di norma 1 nel modo seguente: $q = (\cos(\vartheta), \sin(\vartheta)u)$. Vogliamo vedere che ogni tale quaternionione rappresenta un elemento di $SO_3(\mathbb{R})$, e anche determinare quando due quaternioni determinano la stessa rotazione dello spazio euclideo. Consideriamo allo scopo il prodotto, per ogni $r = (0, v)$:

$$\begin{aligned} qr\bar{q} &= (\cos(\vartheta), \sin(\vartheta)u)(0, v)(\cos(\vartheta), -\sin(\vartheta)u) = \\ &= (\cos(\vartheta), \sin(\vartheta)u)(\sin(\vartheta)v \cdot u, \cos(\vartheta)v - \sin(\vartheta)v \times u) = \\ &= (0, \cos^2(\vartheta)v + 2\sin(\vartheta)\cos(\vartheta)u \times v + \sin^2(\vartheta)(v \cdot u)u - \sin^2(\vartheta)u \times (v \times u)) . \end{aligned}$$

Ora, se supponiamo che v sia multiplo di u allora, poiché $u \times v = 0$ e $(v \cdot u)u = v$, otteniamo $qr\bar{q} = r$; mentre se supponiamo che v sia ortogonale a u , poiché allora $u \cdot v = 0$ e $u \times (v \times u) = v$, otteniamo $qr\bar{q} = (0, \cos(2\vartheta)v + \sin(2\vartheta)u \times v) = (0, w)$, ove w è il vettore che si ottiene ruotando v di un angolo pari a 2ϑ attorno all'asse individuato da u .

Mettendo insieme i due risultati, possiamo quindi concludere che per ogni quaternionione unitario q la funzione $\varphi_q : \mathbb{H}' \rightarrow \mathbb{H}'$ che manda r in $qr\bar{q}$ è una rotazione di \mathbb{H}' (visto come spazio vettoriale euclideo \mathbb{R}^3). Abbiamo dunque una funzione $\varphi : \mathbb{H}^1 \rightarrow SO_3(\mathbb{R})$ (che manda q in φ_q tale che $(0, \varphi_q(v)) = q(0, v)\bar{q}$) che si controlla essere un omomorfismo di gruppi per le strutture moltiplicative date: $\varphi_1 = \mathbb{I}_3$ e $\varphi_{qq'} = \varphi_q\varphi_{q'}$. Si osservi che la seconda formula per quanto facile dà conseguenze importanti, e in particolare dà un modo quasi immediato per capire che la composizione di due rotazioni è ancora una rotazione, e di determinarne angolo e asse (geometricamente non evidente!).

È chiaro che l'omomorfismo φ è suriettivo, poiché ogni elemento di $SO_3(\mathbb{R})$ è una rotazione attorno ad un fissato asse, e quindi si rappresenta tramite (l'applicazione associata ad) un quaternionione. Resta da controllare quali quaternioni determinano la stessa rotazione, e per questo basta vedere quali quaternioni determinano la trasformazione identica: si vede facilmente che sono solo $(\pm 1, 0)$, corrispondenti a rotazioni di angoli 0 e 2π attorno a qualsiasi vettore.

Descrizione esplicita della matrice associata ad un quaternionione unitario: dall'espressione prima trovata

$$\varphi_q(v) = \cos^2(\vartheta)v + 2\sin(\vartheta)\cos(\vartheta)u \times v + \sin^2(\vartheta)(v \cdot u)u - \sin^2(\vartheta)u \times (v \times u)$$

possiamo esplicitare la matrice di φ_q in una base data in cui le coordinate di u siano $(u_1, u_2, u_3)^t$. In

effetti abbiamo

$$\varphi_q(v) = (\cos^2(\vartheta) + 2 \sin(\vartheta) \cos(\vartheta)u \times + \sin^2(\vartheta)uu^t + \sin^2(\vartheta)u \times (u \times))v$$

da cui otteniamo che la matrice cercata è la somma

$$\cos^2(\vartheta)\mathbb{I}_2 + 2 \sin(\vartheta) \cos(\vartheta) \begin{pmatrix} 0 & -u_3 & u_2 \\ u_3 & 0 & u_1 \\ u_2 & -u_1 & 0 \end{pmatrix} + \sin^2(\vartheta) \begin{pmatrix} u_1^2 & u_1u_2 & u_1u_3 \\ u_1u_2 & u_2^2 & u_2u_3 \\ u_1u_3 & u_2u_3 & u_3^2 \end{pmatrix} + \sin^2(\vartheta) \begin{pmatrix} 0 & -u_3 & u_2 \\ u_3 & 0 & u_1 \\ u_2 & -u_1 & 0 \end{pmatrix}^2.$$

Usando invece coordinate reali $q = (x_0, x_1, x_2, x_3) = (x_0, x)$ per il quaternion unitario, allora la matrice di φ_q si ottiene facilmente da calcoli diretti:

$$\begin{aligned} \varphi_q(v) &= (x \cdot v)x + x_0v \times x + x \times (v \times x) = \\ &= \begin{pmatrix} x_0^2 + x_1^2 - x_2^2 - x_3^2 & 2(x_1x_2 - x_0x_3) & 2(x_1x_3 + x_0x_2) \\ 2(x_1x_2 + x_0x_3) & x_0^2 - x_1^2 + x_2^2 - x_3^2 & 2(-x_0x_1 + x_2x_3) \\ 2(x_1x_3 - x_0x_2) & 2(x_0x_1 + x_2x_3) & x_0^2 - x_1^2 - x_2^2 + x_3^2 \end{pmatrix} \begin{pmatrix} v_1 \\ v_2 \\ v_3 \end{pmatrix} \\ &= \begin{pmatrix} 1 - 2(x_2^2 + x_3^2) & 2(x_1x_2 - x_0x_3) & 2(x_1x_3 + x_0x_2) \\ 2(x_1x_2 + x_0x_3) & 1 - 2(x_1^2 + x_3^2) & 2(-x_0x_1 + x_2x_3) \\ 2(x_1x_3 - x_0x_2) & 2(x_0x_1 + x_2x_3) & 1 - 2(x_1^2 + x_2^2) \end{pmatrix} \begin{pmatrix} v_1 \\ v_2 \\ v_3 \end{pmatrix}. \end{aligned}$$

(ricordando che $x_0^2 + x_1^2 + x_2^2 + x_3^2 = 1$).

♠ **1.17.** STRUTTURA DI $O_n(\mathbb{R})$. Naturalmente una matrice ortogonale non è necessariamente diagonalizzabile su \mathbb{R} ; però una strategia simile a quella usata per il teorema spettrale permette di dimostrare che lo è su \mathbb{C} , e anche di verificare il risultato seguente. In generale, data una matrice $A \in O_n(\mathbb{R})$, esiste una base ortonormale di $V_n(\mathbb{R})$ tale che la matrice in quella base assume la forma

$$\begin{pmatrix} \mathbb{I}_r & 0 & 0 & \cdots & 0 \\ 0 & -\mathbb{I}_s & 0 & \cdots & 0 \\ 0 & 0 & \Theta_1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & \Theta_t \end{pmatrix}$$

ove $\Theta_i \in SO_2(\mathbb{R})$. La trasformazione è diretta o inversa a seconda che il blocco $-\mathbb{I}_s$ abbia ordine pari o dispari.

Si procede osservando che gli autovalori complessi sono tutti di modulo 1, e che se ϑ è un autovalore non reale, anche $\bar{\vartheta}$ lo è, con uguali molteplicità e nullità. Se poi α, β sono autovalori distinti (non necessariamente reali), e $v, w \in \mathbb{C}^n$ sono autovettori rispettivi, allora $\bar{v}^t w = 0$ (in particolare, se sono in $V_n(\mathbb{R})$ risultano ortogonali tra loro): calcolando $(\bar{A}v)^t Aw$ si ottiene che $(1 - \bar{\alpha}\beta)\bar{v}^t w = 0$. Infine si dimostra la diagonalizzabilità (su \mathbb{C}) osservando che se U è sottospazio generato da autovettori, allora $U' = \{w \in \mathbb{C}^n | \bar{w}^t u = 0 \forall u \in U\}$ è stabile per A , e quindi contiene altri autovettori.

Il passaggio alla forma reale si ottiene “accoppiando” autovettori tra loro coniugati in senso complesso (e quindi relativi ad autovalori coniugati) per formare i blocchi di rotazioni euclidee.

1.18. DEFINIZIONE-TEOREMA (CONFORMITÀ). Sia φ un automorfismo di $V_n(\mathbb{R})$; le proprietà seguenti sono equivalenti:

- (1) φ rispetta gli angoli, i.e. $\vartheta(\varphi(v), \varphi(w)) = \vartheta(v, w)$ per ogni $v, w \in V_n(\mathbb{R})$;
- (2) φ rispetta gli angoli retti, i.e. $\varphi(v) \perp \varphi(w)$ se e solo se $v \perp w$ per ogni $v, w \in V_n(\mathbb{R})$.
- (3) esiste un numero reale $\alpha > 0$ tale che $\varphi(v) \cdot \varphi(w) = \alpha^2(v \cdot w)$ per ogni $v, w \in V_n(\mathbb{R})$;
- (4) esiste un numero reale $\alpha > 0$ tale che $\|\varphi(v)\| = \alpha \|v\|$ per ogni $v \in V_n(\mathbb{R})$.

Tali automorfismi si dicono conformità di $V_n(\mathbb{R})$, e il numero α si dice rapporto della conformità.

DIMOSTRAZIONE. Simile a quella fatta per le rigidità. □

1.18.1. Osservazioni analoghe a quelle fatte per le trasformazioni ortogonali. Una applicazione insiemistica di $V_n(\mathbb{R})$ in sè che soddisfi alla proprietà...

1.18.2. MATRICI CONFORMI. Sia φ una conformità. Ogni matrice A associata usando una base di vettori ortonormali (tali che $v_i \cdot v_j = \delta_{i,j}$) è tale che $A^t A = \alpha^2 \mathbb{I}$ per qualche reale $\alpha > 0$. Tali matrici si dicono matrici conformi, e il valore α si dice parametro o rapporto di conformità. Se A è

matrice conforme di parametro α , allora $\det A = \pm\alpha^n$. Se $\det A > 0$ la conformità si dice diretta; inversa altrimenti.

Le matrici conformi formano un sottogruppo di $GL(n, \mathbb{R})$ contenente il gruppo ortogonale.

AVVERTENZA TERMINOLOGICA. *Nel seguito scriveremo dei determinanti "misti", ovvero determinanti di matrici quadrate in cui alcune entrate della matrice saranno occupate da vettori. Intendiamo queste scritture come una semplice stenografia, e quei determinanti calcolati secondo le usuali regole usando il prodotto tra scalari, il prodotto tra scalari e vettori, e il prodotto scalare tra vettori: trattandosi di operazioni commutative e la terza bilineare, nessuna ambiguità ne dovrebbe risultare. Il lettore è sempre invitato a capire bene qual è il risultato dei calcoli (un vettore o uno scalare?).*

Segnaliamo infine che tutte le formule di questo tipo qui scritte possono essere rigorosamente interpretate in una opportuna algebra tensoriale sullo spazio vettoriale che si usa, o in un opportuno suo quoziente.

1.19. DEFINIZIONE (CROSS PRODUCT O PRODOTTO VETTORE). Sia $V_n(\mathbb{R})$ lo spazio vettoriale standard su \mathbb{R} di dimensione n e sia $\mathcal{E} = (e_1, \dots, e_n)$ la base canonica. Definiamo una applicazione $\text{cross} : V_n(\mathbb{R})^{n-1} \rightarrow V_n(\mathbb{R})$ tramite la formula:

$$\text{cross}(v_1, \dots, v_{n-1}) := \det \begin{pmatrix} \mathcal{E}^t & v_1 & \dots & v_{n-1} \end{pmatrix} = \begin{vmatrix} e_1 & v_{1,1} & \dots & v_{n-1,1} \\ e_2 & v_{1,2} & \dots & v_{n-1,2} \\ \vdots & \vdots & \ddots & \vdots \\ e_n & v_{1,n} & \dots & v_{n-1,n} \end{vmatrix}$$

In particolare:

1.19.1. per $n = 1$ si ha $\text{cross}(\emptyset) = 1$;

1.19.2. per $n = 2$ si ha $\text{cross}(v) = \begin{pmatrix} v_1 \\ -v_2 \end{pmatrix}$ se $v = \begin{pmatrix} v_1 \\ v_2 \end{pmatrix}$;

1.19.3. per $n = 3$ scriviamo $v \times w = \text{cross}(v, w) = \begin{pmatrix} v_2 w_3 - v_3 w_2 \\ -v_1 w_3 + v_3 w_1 \\ v_1 w_2 - v_2 w_1 \end{pmatrix}$ se $v = \begin{pmatrix} v_1 \\ v_2 \\ v_3 \end{pmatrix}$ e $w = \begin{pmatrix} w_1 \\ w_2 \\ w_3 \end{pmatrix}$.

In generale le componenti di $\text{cross}(v_1, \dots, v_{n-1})$ sono i minori segnati d'ordine $n-1$ della matrice che ha come colonne le componenti dei vettori v_1, \dots, v_{n-1} .

1.20. TEOREMA (PROPRIETÀ DEL CROSS PRODUCT).

- (C1) $\text{cross}(v_1, \dots, v_{n-1}) = 0$ se e solo se v_1, \dots, v_{n-1} sono linearmente dipendenti;
- (C2) $\text{cross}(v_{\sigma(1)}, \dots, v_{\sigma(n-1)}) = \text{sgn}(\sigma) \text{cross}(v_1, \dots, v_{n-1})$ (per ogni permutazione $\sigma \in \mathfrak{S}_{n-1}$);
- (C3) $v_i \cdot \text{cross}(v_1, \dots, v_{n-1}) = 0$ (cioè parlando in termini di spazi vettoriali euclidei, $\text{cross}(v_1, \dots, v_{n-1})$ è ortogonale a v_i) per ogni i ;
- (C4) multilinearità: $\text{cross}(v_1, \dots, \sum_j \alpha_j w_j, \dots, v_{n-1}) = \sum_j \alpha_j \text{cross}(v_1, \dots, w_j, \dots, v_{n-1})$ per ogni posizione delle variabili;
- (C5) Se v_1, \dots, v_{n-1} sono linearmente indipendenti, allora $v_1, \dots, v_{n-1}, \text{cross}(v_1, \dots, v_{n-1})$ sono una base di $V_n(\mathbb{R})$.

DIMOSTRAZIONE. Tutte le proprietà seguono immediatamente dalla definizione e dalle proprietà del determinante. Per l'ultimo punto basta calcolare il determinante della matrice che ha come colonne i vettori $\text{cross}(v_1, \dots, v_{n-1}), v_1, \dots, v_{n-1}$, sviluppando rispetto alla prima colonna: ne risulta una somma di quadrati non tutti nulli. \square

1.21. TEOREMA (LAGRANGE). Consideriamo ora lo spazio euclideo $V_n(\mathbb{R})$; allora la norma del cross-product si può calcolare tramite il determinante:

$$\|\text{cross}(v_1, \dots, v_{n-1})\|^2 = \left| (v_i \cdot v_j)_{i,j} \right| = \begin{vmatrix} \|v_1\|^2 & v_1 \cdot v_2 & \dots & v_1 \cdot v_{n-1} \\ v_2 \cdot v_1 & \|v_2\|^2 & \dots & v_2 \cdot v_{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ v_{n-1} \cdot v_1 & v_{n-1} \cdot v_2 & \dots & \|v_{n-1}\|^2 \end{vmatrix}.$$

In particolare:

1.21.1. per $n = 1$ si ha $\|\text{cross}(\emptyset)\| = 1$;

1.21.2. nel caso $n = 2$ l'identità di Lagrange si riduce a $\|\text{cross}(v)\| = \|v\|$;

1.21.3. nel caso $n = 3$, $v \times w = \text{cross}(v, w)$, l'identità di Lagrange è

$$\|v \times w\|^2 = \begin{vmatrix} \|v\|^2 & v \cdot w \\ w \cdot v & \|w\|^2 \end{vmatrix} = \|v\|^2 \|w\|^2 - (v \cdot w)^2 = \|v\|^2 \|w\|^2 \sin^2 \vartheta(v, w)$$

e si generalizza in

$$\sum_{i < j} (x_i y_j - x_j y_i)^2 = \left(\sum_{i=1}^n x_i^2 \right) \left(\sum_{i=1}^n y_i^2 \right) - \left(\sum_{i=1}^n x_i y_i \right)^2$$

ovvero

$$\|(x \ y)\|^2 = \|x\|^2 \|y\|^2 - (x \cdot y)^2$$

ove $x, y \in V_n(C)$ e $\|(x \ y)\|$ è la radice quadrata della somma dei quadrati dei minori 2×2 della matrice formata dai due vettori.

DIMOSTRAZIONE. Si sviluppano i calcoli:

$$\begin{aligned} \|\text{cross}(v_1, \dots, v_{n-1})\|^2 &= \text{cross}(v_1, \dots, v_{n-1}) \cdot \text{cross}(v_1, \dots, v_{n-1}) \\ &= \det \begin{pmatrix} \mathcal{E}^t & v_1 & \dots & v_{n-1} \end{pmatrix}^t \det \begin{pmatrix} \mathcal{E}^t & v_1 & \dots & v_{n-1} \end{pmatrix} \\ &= \det \left(\begin{pmatrix} \mathcal{E}^t & v_1 & \dots & v_{n-1} \end{pmatrix}^t \begin{pmatrix} \mathcal{E}^t & v_1 & \dots & v_{n-1} \end{pmatrix} \right) \\ &= \det \begin{pmatrix} \mathcal{E} & \\ v_1^t & \\ \vdots & \\ v_{n-1}^t & \end{pmatrix} \begin{pmatrix} \mathcal{E}^t & v_1 & \dots & v_{n-1} \end{pmatrix} \\ &= \begin{vmatrix} n & v_1 & v_2 & \dots & v_{n-1} \\ v_1 & \|v_1\|^2 & v_1 \cdot v_2 & \dots & v_1 \cdot v_{n-1} \\ v_2 & v_2 \cdot v_1 & \|v_2\|^2 & \dots & v_2 \cdot v_{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ v_{n-1} & v_{n-1} \cdot v_1 & v_{n-1} \cdot v_2 & \dots & \|v_{n-1}\|^2 \end{vmatrix} \end{aligned}$$

e poi si sviluppa rispetto alla prima riga. □

1.21.4. GENERALIZZAZIONE. Dati r vettori v_1, \dots, v_r in $V_n(\mathbb{R})$ con $r \leq n$, sia $W \in M_{n,r}(C)$ la matrice che ha quei vettori come colonne. Allora, definito $\|W\|$ ("norma della matrice W ") come la radice quadrata della somma dei quadrati dei minori di ordine r della matrice stessa (si tratta di $\binom{n}{r}$ termini), la formula di Lagrange si generalizza in

$$\|W\|^2 = \left| (v_i \cdot v_j)_{i,j} \right|.$$

La dimostrazione di questo fatto non è facile.

1.21.5. NOTA SULLA MATRICE TRIGONOMETRICA. La formula del teorema di Lagrange si può riscrivere usando la definizione di coseno nel modo seguente:

$$\begin{aligned} \|\text{cross}(v_1, \dots, v_{n-1})\|^2 &= \|v_1\|^2 \|v_2\|^2 \dots \|v_{n-1}\|^2 \left| (\cos \vartheta(v_i, v_j))_{i,j} \right| \\ &= \|v_1\|^2 \|v_2\|^2 \dots \|v_{n-1}\|^2 \begin{vmatrix} 1 & \cos \vartheta_{1,2} & \dots & \cos \vartheta_{1,n-1} \\ \cos \vartheta_{1,2} & 1 & \dots & \cos \vartheta_{2,n-1} \\ \vdots & \vdots & \ddots & \vdots \\ \cos \vartheta_{1,n-1} & \cos \vartheta_{2,n-1} & \dots & 1 \end{vmatrix} \end{aligned}$$

ove $\vartheta_{i,j} = \vartheta(v_i, v_j)$. Si osservi che il determinante della matrice dei coseni è sempre positivo, e ha una facile interpretazione nel caso $n = 2$ (e nel caso $n = 3$?).

1.21.6. PROBLEMA. Usando gli stessi metodi che per il teorema di Lagrange, si dimostri la seguente generalizzazione:

$$\text{cross}(u_1, \dots, u_{n-1}) \cdot \text{cross}(v_1, \dots, v_{n-1}) = \det(u_i \cdot v_j).$$

In particolare:

per $n = 2$ si ha che $\text{cross}(u) \cdot \text{cross}(v) = u \cdot v$

per $n = 3$ si ha che $(u_1 \times u_2) \cdot (v_1 \times v_2) = (u_1 \cdot v_1)(u_2 \cdot v_2) - (u_1 \cdot v_2)(u_2 \cdot v_1)$.

1.21.7. PROBLEMA. Provare che risulta:

$$\text{cross}(u_2, \dots, u_{n-1}, \text{cross}(v_1, \dots, v_{n-1})) = \sum_{i=1}^{n-1} (-1)^{i+1} |u_a \cdot v_b|_{\substack{a \neq i \\ b \neq i}} v_i.$$

Suggerimento: conviene utilizzare il punto precedente osservando che il vettore cercato appartiene allo spazio $\text{cross}(v_1, \dots, v_{n-1})^\perp = \langle v_1, \dots, v_{n-1} \rangle$, cioè è del tipo $\sum_i \alpha_i v_i$ e dunque basta trovare i coefficienti α_i . Tali coefficienti si possono determinare a partire dal sistema lineare delle equazioni che impongono l'ortogonalità di $\sum_i \alpha_i v_i$ ai vettori u_j per $j = 2, \dots, n-1$, aggiungendo una equazione corrispondente al prodotto scalare con un vettore u_1 indipendente dagli altri...

In particolare:

per $n = 2$ si ha che $\text{cross}(\text{cross}(u)) = -u$

per $n = 3$ si ha che $u \times (v \times w) = (u \cdot w)v - (u \cdot v)w$; di conseguenza abbiamo $v \times (v \times w) = (v \cdot w)v - \|v\|^2 w$ e $w \times (v \times w) = \|w\|^2 v - (w \cdot v)w$.

1.21.8. PROBLEMA. Se $v_1, v_2 \in C^3$, allora $v_1 \times v_2$ ha come componenti i coefficienti di una equazione del piano generato da v_1, v_2 . Poi, se $u_1, u_2 \in C^3$ sono altri vettori, l'intersezione tra i piani generati (se ha dimensione 1) ha come generatore $(v_1 \times v_2) \times (u_1 \times u_2)$. Provare che

$$(v_1 \times v_2) \times (u_1 \times u_2) = \det(v_1 v_2 u_2)u_1 - \det(v_1 v_2 u_1)u_2 = -\det(u_1 u_2 v_2)v_1 + \det(u_1 u_2 v_1)v_2.$$

1.22. DEFINIZIONE (PRODOTTO MISTO). $|w v_1 \dots v_{n-1}| := w \cdot \text{cross}(v_1, \dots, v_{n-1})$ è il determinante della matrice che ha come colonne gli n vettori, e si dice il prodotto misto dei vettori w e v_1, \dots, v_{n-1} ; è un elemento di C che si annulla se e solo se gli n vettori coinvolti sono linearmente dipendenti. Si ha $|v_{\sigma 1} \dots v_{\sigma n}| = \text{sgn}(\sigma)|v_1 \dots v_n|$ per ogni permutazione σ .

1.22.1. Nel caso $n = 2$ la formula delle permutazioni si riduce a $|v w| = -|w v|$.

1.22.2. Nel caso $n = 3$ la formula delle permutazioni dà luogo a sei termini:

$$|u v w| = |v w u| = |w u v| = -|u w v| = -|v w u| = -|v u w|$$

(i 3-cicli mantengono il prodotto misto, gli scambi ne cambiano il segno).

1.23. DEFINIZIONE (VOLUMI). Nel caso di spazi vettoriali euclidei, definiamo il volume orientato (risp. volume assoluto o volume) n -dimensionale dell' n -poliparallelepipedo generato da n vettori come il valore del prodotto misto (risp. il modulo del prodotto misto) di quegli n vettori. Dunque si tratta del determinante (risp. del valore assoluto del determinante) della matrice che ha quei vettori come colonne. Si scrive $\text{Vol}_n \Pi(v_1, \dots, v_n)$ se v_1, \dots, v_n sono i lati del parallelepipedo.

1.23.1. Giustificazione della definizione discende dal fatto che le proprietà del determinante (valere 1 sui vettori della base canonica e la multilinearità alternante sulle colonne) fissano quella funzione e sono le proprietà corrette per un calcolo di volumi (orientati): l'ipercubo unitario abbia n -volume 1; se si moltiplica un lato per un certo valore il volume sia moltiplicato per quel valore; se si accostano due parallelepipedi di "basi uguali" allora la somma dei volumi corrisponda al volume del parallelepipedo che ha come ultimo lato la somma dei due ultimi vettori dei solidi dati (riflettere su questo fatto facendo qualche disegno); se i lati non sono indipendenti il volume sia nullo.

1.23.2. AUTOMORFISMI E VOLUMI. Dalla definizione segue subito che gli automorfismi moltiplicano i volumi orientati per il loro determinante (e i volumi per il valore assoluto del loro determinante): se Π indica un poliparallelepipedo determinato da v_1, \dots, v_n e $\varphi \Pi$ indica il poliparallelepipedo determinato da $\varphi v_1, \dots, \varphi v_n$, allora $\text{Vol}_n(\varphi \Pi) = \det \varphi \text{Vol}_n(\Pi)$.

In particolare le trasformazioni ortogonali conservano i volumi (non orientati), mentre le conformità li moltiplicano per la potenza n -esima del rapporto di conformità.

1.24. TEOREMA (CALCOLO DI m -VOLUMI DI m -PARALLELEPIPEDI E m -EDRI). Siano v_1, \dots, v_m m vettori di $V_n(\mathbb{R})$, con $m \leq n$. Il volume m -dimensionale dell' m -parallelepipedo $\Pi(v_1, \dots, v_m)$ generato da quei vettori è dato da

$$\text{Vol}_m(\Pi(v_1, \dots, v_m)) = \sqrt{\det(W^t W)} = \sqrt{\det(v_i \cdot v_j)_{i,j}} = \|W\|$$

mentre quello dell' m -edro $\Delta(v_1, \dots, v_m)$ generato è $\frac{1}{m!}$ volte quello di $\Pi(v_1, \dots, v_m)$, e dunque:

$$\text{Vol}_m(\Delta(v_1, \dots, v_m)) = \frac{1}{m!} \sqrt{\det(W^t W)} = \frac{1}{m!} \sqrt{\det(v_i \cdot v_j)_{i,j}} = \frac{1}{m!} \|W\|$$

ove $W \in M_{n,m}$ è la matrice le cui colonne sono gli m vettori dati.

DIMOSTRAZIONE. Sia $T \in M_{n,n-m}$ una matrice le cui colonne formino una base ortonormale dello spazio ortogonale a $\langle v_1, \dots, v_m \rangle$. Allora il volume cercato è

$$|\det(W|T)| = \sqrt{\det((W|T)^t(W|T))} = \sqrt{\det\left(\begin{pmatrix} W^t \\ T^t \end{pmatrix}(W|T)\right)} = \sqrt{\det\begin{pmatrix} W^tW & 0 \\ 0 & \mathbb{I}_{n-m} \end{pmatrix}} = \sqrt{\det(W^tW)}.$$

Per quanto riguarda gli m -edri, si tratta di mostrare che un m -parallelepipedo si decompone in $m!$ m -edri tutti di “ugual volume”. Questo si può “vedere” per induzione nel modo seguente: è ben noto per $n = 2$ (un parallelogramma si decompone in due triangoli sovrapponibili) e anche per $n = 3$ (un parallelepipedo si decompone in sei tetraedri di ugual volume, avendo a due a due basi uguali e uguali altezze); preso poi un m -parallelepipedo, e scelta una sua $m-1$ -faccia come “base”, questa può essere decomposta per ipotesi induttiva in $(m-1)!$ $m-1$ -edri di ugual volume, in modo da ottenere $(m-1)!$ m -solidi con “facce parallele” e basi gli $m-1$ -edri. Ciascuno di questi solidi contiene esattamente m m -edri, ciascuno dei quali ha una base $m-1$ -edrale di ugual volume con un’altro e stessa altezza. Provare a rendere rigoroso questo discorso, discutendo il caso dell’ n -cubo unitario. \square

1.24.1. Si osservi che dalla formula $\text{Vol}_m(\Pi) = \sqrt{\det(v_i \cdot v_j)_{i,j}}$ segue che se i vettori sono a due a due ortogonali allora il volume del parallelepipedo m -dimensionale è semplicemente il prodotto delle norme dei vettori che lo generano.

1.24.2. AREA DI TRIANGOLI. Dati due vettori indipendenti $v_1, v_2 \in V_n(\mathbb{R})$ abbiamo che l’area del triangolo $\Delta(v_1, v_2)$ da essi definito è

$$\text{Vol}_2\Delta(v_1, v_2) = \frac{1}{2} \|(v_1 \ v_2)\| = \frac{1}{2} \sqrt{\det(v_i \cdot v_j)} = \frac{1}{2} \sqrt{\|v_1\|^2 \|v_2\|^2 - (v_1 \cdot v_2)^2} = \frac{1}{2} \|v_1\| \|v_2\| |\sin \vartheta(v_1, v_2)|$$

e dall’ultima formula si riconosce l’area in senso elementare.

1.24.3. VOLUME DI TETRAEDRI. Dati tre vettori indipendenti $v_1, v_2, v_3 \in V_n(\mathbb{R})$ abbiamo che il volume del tetraedro $\Delta(v_1, v_2, v_3)$ da essi definito è

$$\text{Vol}_3\Delta(v_1, v_2, v_3) = \frac{1}{6} \|(v_1 \ v_2 \ v_3)\| = \frac{1}{6} \sqrt{\det(v_i \cdot v_j)} = \frac{1}{6} \|v_1\| \|v_2\| \|v_3\| \sqrt{\det(\cos \vartheta(v_i, v_j))}$$

1.24.4. $(n-1)$ -VOLUME DI $(n-1)$ -EDRI. Dati $n-1$ vettori indipendenti $v_1, \dots, v_{n-1} \in V_n(\mathbb{R})$ abbiamo che il volume dell’ $n-1$ -edro $\Delta(v_1, \dots, v_{n-1})$ da essi definito è

$$\text{Vol}_{n-1}\Delta(v_1, \dots, v_{n-1}) = \frac{1}{(n-1)!} \|(v_1 \cdots v_{n-1})\| = \frac{1}{(n-1)!} \sqrt{\det(v_i \cdot v_j)}$$

1.24.5. n -VOLUME DI n -EDRI. Dati n vettori indipendenti $v_1, \dots, v_n \in V_n(\mathbb{R})$ abbiamo che il volume dell’ n -edro $\Delta(v_1, \dots, v_n)$ da essi definito è

$$\text{Vol}_n\Delta(v_1, \dots, v_n) = \frac{1}{n!} |v_1 \cdots v_n|.$$

1.24.6. INTERPRETAZIONE GEOMETRICA DEL CROSS PRODUCT. Nel caso di spazi euclidei $V_n(\mathbb{R})$, da un punto di vista geometrico, il cross product di $n-1$ vettori linearmente indipendenti si caratterizza come: il vettore di direzione ortogonale ai vettori dati, di verso tale che l’orientazione di $\text{cross}(v_1, \dots, v_{n-1}), v_1, \dots, v_{n-1}$ concordi con quella della base scelta per esprimere le coordinate (si osservi che il determinante della matrice che ha come colonne i vettori nell’ordine scritto è esattamente il quadrato della norma di $\text{cross}(v_1, \dots, v_{n-1})$), di lunghezza pari al volume $(n-1)$ -dimensionale del “poliparallelepipedo” formato dai vettori v_1, \dots, v_{n-1} (per Lagrange).

1.24.7. VOLUME E VOLUME LATERALE PER CUBI ED EDRI UNITARI. Si osservi che il volume dell’ n -cubo unitario di $V_n(\mathbb{R})$ è sempre 1, mentre il volume laterale (somma degli $(n-1)$ -volumi delle sue facce laterali) cresce al variare di n , e vale esattamente $2n$. Quindi il rapporto tra volume e volume laterale per l’ n -cubo unitario è $1/2n$ e diminuisce con n .

Sappiamo che l’ n -edro costruito sui vettori della base canonica ha n -volume $1/n!$ e un facile calcolo permette di stabilire che il suo $(n-1)$ -volume laterale è $\frac{n+\sqrt{n}}{(n-1)!}$. Quindi il rapporto tra volume e volume laterale per l’ n -edro unitario è $1/n(n+\sqrt{n})$ e diminuisce con n più velocemente di quello dell’ n -cubo.

2. Spazi Euclidei.

2.1. DEFINIZIONE (SPAZIO EUCLIDEO). *Uno spazio euclideo reale è uno spazio affine \mathbb{E} il cui spazio delle traslazioni sia uno spazio vettoriale euclideo reale. Lo spazio euclideo reale standard di dimensione n è $\mathbb{E}^n(\mathbb{R})$ il cui spazio delle traslazioni $V_n(\mathbb{R})$ è dotato del prodotto scalare; si indica con $\mathbb{E}^n(\mathbb{R})$.*

2.2. RIFERIMENTI ORTOGONALI E ORTONORMALI. Un riferimento affine in uno spazio euclideo \mathbb{E} si dice ortogonale (risp. ortonormale) se la base associata di $V_n(\mathbb{R})$ è ortogonale (risp. ortonormale).

2.3. INTERPRETAZIONE EUCLIDEA DELLE EQUAZIONI CARTESIANE. I coefficienti delle variabili formano dei vettori che sono ortogonali al sottospazio direttore della varietà. Se L è il sottospazio $P_0 + \langle v_1, \dots, v_m \rangle$ ed ha equazioni cartesiane date dal sistema $AX - b = 0$ con $A \in M_{r,n}(\mathbb{R})$, $b \in \mathbb{R}^r$ ed $r = n - m$, allora risulta che le righe $A^{(1)}, \dots, A^{(r)}$ intese come (coordinate di) elementi di $V_n(\mathbb{R})$ sono indipendenti e ortogonali al sottospazio $\langle v_1, \dots, v_m \rangle$. Si ha $V_n(\mathbb{R}) = \langle v_1, \dots, v_m \rangle \boxplus \langle A^{(1)}, \dots, A^{(r)} \rangle$ (significa che i due sottospazi sono in somma diretta e che sono ortogonali tra loro).

2.4. DEFINIZIONE-TEOREMA (Distanza tra punti). *Definiamo la funzione distanza*

$$d : \mathbb{E}^n(\mathbb{R}) \times \mathbb{E}^n(\mathbb{R}) \longrightarrow \mathbb{R}$$

tramite: $d(P, Q) := \|Q - P\|$. *Proprietà della funzione distanza:*

- (D1) $d(P, Q) = 0$ se e solo se $P = Q$;
- (D2) simmetria: $d(P, Q) = d(Q, P)$;
- (D3) disuguaglianza triangolare: $d(P, Q) \leq d(P, R) + d(R, Q)$.

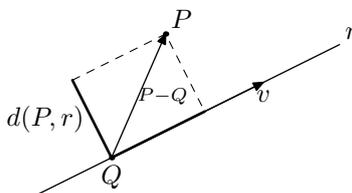
DIMOSTRAZIONE. Discende dalle proprietà analoghe viste per il prodotto scalare e la norma di vettori. \square

2.5. DEFINIZIONE-TEOREMA (Distanza tra punti e sottospazi). *La distanza tra un punto P e il sottospazio L è definita come $d(P, L) := \inf_{Q \in L} d(P, Q)$. Si annulla se e solo se $P \in L$. Se $P \notin L$ allora esiste unico $P' \in L$ tale che $d(P, L) = d(P, P')$, e si chiama il punto di minima distanza. Si trova imponendo al vettore $P - P'$ di essere ortogonale allo spazio direttore di L .*

DIMOSTRAZIONE. Mostriamo la caratterizzazione del punto di minima distanza: per ogni $Q \in L$ si ha $P - Q = v + v'$ con v appartenente allo spazio direttore di L e v' ortogonale a tale spazio; inoltre tale v' è indipendente da P , come si vede facilmente. Di conseguenza $d(P, Q) = \|v\|^2 + \|v'\|^2$, e tale termine è minimo quando $v = 0$, dunque quando $P - Q$ è ortogonale allo spazio direttore di L . \square

2.5.1. DISTANZA TRA PUNTI E RETTE. Dati un punto P e una retta $r = Q + \langle v \rangle$, abbiamo

$$d(P, r) = \sqrt{\|P - Q\|^2 - \frac{((P - Q) \cdot v)^2}{v \cdot v}} = \|P - Q\| |\sin \vartheta(P - Q, v)|$$



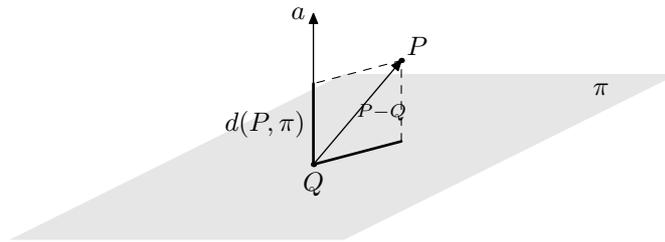
2.5.2. DISTANZA TRA PUNTI E IPERPIANI. Dati un punto P di coordinate $(x_1, \dots, x_n)^t$ e un iperpiano π di equazione $a_1 X_1 + \dots + a_n X_n + a_0 = 0$, abbiamo

$$d(P, \pi) = \frac{|a_1 x_1 + \dots + a_n x_n + a_0|}{\sqrt{a_1^2 + \dots + a_n^2}}.$$

Infatti, ponendo $a = (a_1, \dots, a_n)^t$ abbiamo che a è un vettore ortogonale all'iperpiano, e quindi basta calcolare la proiezione lungo a di un vettore $P - Q$ con $Q \in \pi$ qualsiasi:

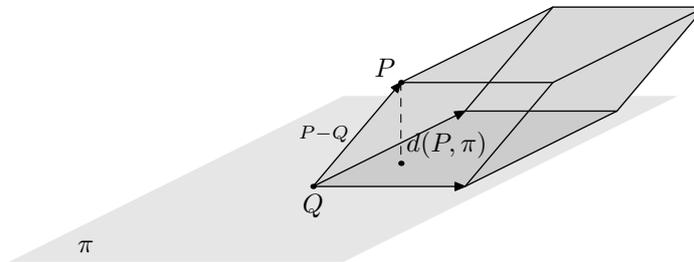
$$d(P, \pi) = \frac{|a \cdot (P - Q)|}{\|a\|} = \frac{|\sum_i a_i x_i - \sum_i a_i y_i|}{\|a\|}$$

ove le y_i sono le coordinate di Q , per cui $-\sum_i a_i y_i = a_0$.



Se l'iperpiano π è dato tramite un punto Q e generatori v_1, \dots, v_n dello spazio direttore, possiamo calcolare la distanza come l'altezza dell' n -parallelepipedo formato da $P-Q, v_1, \dots, v_{n-1}$ con base l' $(n-1)$ -parallelepipedo formato da v_1, \dots, v_{n-1} , dunque:

$$d(P, \pi) = \frac{|\det(P-Q \ v_1 \cdots v_{n-1})|}{\|\text{cross}(v_1, \dots, v_{n-1})\|} = \frac{|\det(P-Q \ v_1 \cdots v_{n-1})|}{\sqrt{\det(v_i \cdot v_j)}}.$$



2.6. DEFINIZIONE-TEOREMA (Distanza tra sottospazi). siano L ed L' sue sottospazi di dimensioni m ed m' ; la loro distanza è definita da

$$d(L, L') := \inf_{Q \in L, Q' \in L'} d(Q, Q').$$

Si annulla se e solo se $L \cap L' \neq \emptyset$.

Se $L \cap L' = \emptyset$, allora si possono trovare le coppie di punti di minima distanza $P \in L$ e $P' \in L'$, cioè tali che $d(L, L') = d(P, P')$, imponendo che $P-P'$ sia ortogonale ad entrambi i sottospazi direttori.

I punti di minima distanza sono unici se e solo se le varietà L ed L' sono sghembe.

DIMOSTRAZIONE. Esercizio, tenendo conto che se $Q \in L$ e $Q' \in L'$, allora $d(Q, Q') = d(P+v, P'+v') = \|(P-P') + v - v'\|$ e se $P-P'$ è ortogonale agli spazi direttori si ha $\|(P-P') + v - v'\|^2 = \|P-P'\|^2 + \|v - v'\|^2 \dots$ \square

2.6.1. In generale: $d(P + W, P' + W') = d(P, P' + W' + W)$. Questa formula permette di ricondurre il calcolo di distanze tra sottospazi affini ad un calcolo di distanze tra punti e sottospazi.

2.6.2. DISTANZA TRA SPAZI COMPLEMENTARI. Per calcolare la distanza tra un sottospazio affine $L = P + \langle v_1, \dots, v_{r-1} \rangle$ di dimensione $r-1$ e un sottospazio affine $M = Q + \langle v_r, \dots, v_{n-1} \rangle$ di codimensione r , possiamo calcolare la distanza di P dal sottospazio affine $Q + \langle v_1, \dots, v_{n-1} \rangle$, che è un iperpiano se e solo se v_1, \dots, v_{n-1} sono linearmente indipendenti. Si ha in tal caso

$$d(L, M) = \frac{|\det(P-Q \ v_1 \cdots v_{n-1})|}{\sqrt{\det(v_i \cdot v_j)}}.$$

2.7. TEOREMA (VOLUMI DI m -EDRI). dati $m+1$ punti indipendenti P_0, \dots, P_m , detti $v_i = P_i - P_0$, risulta che l' $(m+1)$ -edro definito da quei punti ha misura m -dimensionale data da

$$\text{Vol}_m(\Delta(P_0, \dots, P_m)) = \sqrt{\det(v_i \cdot v_j)} = \frac{1}{m!} \|(v_1 \ \dots \ v_m)\|$$

ove definiamo che la "norma" di una matrice $m \times n$ con $m \leq n$ come la radice quadrata della somma dei quadrati dei minori di ordine m della matrice stessa (si tratta di $\binom{n}{m}$ termini).

Per un insieme di indici $1 \leq i_1 < \dots < i_m \leq n$, abbreviato I , indichiamo con $P(I)$ la m -upla delle coordinate di P dei posti in I , e con $P(\widehat{I})$ la $(n-m)$ -upla delle coordinate di P dei posti non in I . Allora l' m -volume in questione si scrive come

$$\text{Vol}_m(\Delta(P_0, \dots, P_m)) = \frac{1}{m!} \sqrt{\sum_I \begin{vmatrix} 1 & \dots & 1 \\ P_0(I) & \dots & P_m(I) \end{vmatrix}^2}$$

ove la somma è sulle m -ple intere tali che $1 \leq i_1 < \dots < i_m \leq n$.

DIMOSTRAZIONE. Basta ricordare quanto fatto per gli Spazi Vettoriali Euclidei, a cui ci si riconduce immediatamente. \square

2.7.1. TEOREMA (AREA DI TRIANGOLI). Dati tre punti non allineati P_0, P_1 e P_2 , detti $P_1 - P_0 = (l_1, \dots, l_n)^t$ e $P_2 - P_0 = (m_1, \dots, m_n)^t$, l'area del triangolo da essi definito è

$$A(P_0, P_1, P_2) = \frac{1}{2} \sqrt{\det((P_i - P_0) \cdot (P_j - P_0))} = \frac{1}{2} \sqrt{\sum_{i < j} \begin{vmatrix} l_i & m_i \\ l_j & m_j \end{vmatrix}^2} = \frac{1}{2} \sqrt{\sum_{i < j} \begin{vmatrix} 1 & 1 & 1 \\ P_{0,i} & P_{1,i} & P_{2,i} \\ P_{0,j} & P_{1,j} & P_{2,j} \end{vmatrix}^2}.$$

2.7.2. In particolare per $m = n-1$ risulta:

$$\text{Vol}_{n-1}(\Delta(P_0, \dots, P_{n-1})) = \frac{1}{(n-1)!} \sqrt{\sum_{i=1}^n \begin{vmatrix} 1 & \dots & 1 \\ P_0(\widehat{i}) & \dots & P_{n-1}(\widehat{i}) \end{vmatrix}^2}$$

2.7.3. E per $m = n$ risulta: $\text{Vol}_n(\Delta(P_0, \dots, P_n)) = \frac{1}{n!} |\det \begin{pmatrix} 1 & \dots & 1 \\ P_0 & \dots & P_n \end{pmatrix}|$.

3. Trasformazioni Euclidee.

3.1. DEFINIZIONE (CONGRUENZA). Una applicazione $F \in \text{Aff}(\mathbb{E})$ si dice una congruenza (o rigidità, o isometria) se l'applicazione φ associata è una trasformazione ortogonale (rispetta la struttura euclidea, i.e. il prodotto scalare). Indichiamo con $\text{Rig}(\mathbb{E})$ questo sottogruppo di $\text{Aff}(\mathbb{E})$.

3.1.1. CONGRUENZE E AFFINITÀ. Si osservi che una applicazione insiemistica dello spazio euclideo in sè che rispetti le distanze tra i punti, è necessariamente una biiezione.

D'altra parte una applicazione insiemistica dello spazio euclideo in sè tale da rispettare il prodotto scalare tra i due vettori per ogni terna di punti è necessariamente una affinità, e dunque una congruenza come definita sopra.

3.1.2. TRASLAZIONI. È immediato che le traslazioni dello spazio affine sono rigidità: dunque $\text{Rig}(\mathbb{E}) \supseteq \text{Trasl}(\mathbb{E})$.

3.1.3. RIGIDITÀ CENTRALI. Le rigidità centrali di centro un punto $R \in \mathbb{E}$ sono quelle rigidità che fissano R ; definiamo dunque $\text{Rig}_R(\mathbb{E}) := \text{Rig}(\mathbb{E}) \cap \text{Centr}_R(\mathbb{E})$.

3.1.4. FORME MATRICIALI. Si verifica subito che una affinità è una rigidità se e solo se la matrice associata in un riferimento ortonormale di \mathbb{E} è del tipo $A = \begin{pmatrix} 1 & 0 \\ v & A' \end{pmatrix}$ ove A' è una matrice ortogonale.

3.2. TEOREMA (DECOMPOSIZIONE DI RIGIDITÀ). Ogni elemento di $\text{Rig}(\mathbb{E})$ si può scrivere come composizione di una traslazione e di una rigidità di centro R preassegnato, e anche in ordine inverso.

DIMOSTRAZIONE. Analoga al caso delle affinità. \square

♠ 3.3. TEOREMA (CLASSIFICAZIONE DELLE RIGIDITÀ). Le rigidità di \mathbb{E} si dividono in:

(D) dirette (conservano l'orientamento dello spazio):

(T) traslazioni;

(m -R) m -rotazioni: composizioni di m rotazioni su piani tra loro ortogonali, ove $m \leq [n/2]$ (parte intera di $n/2$);

- (T m-R) *glisso-m-rotazioni*: composizioni di m rotazioni su piani tra loro ortogonali, ove $m \leq [n/2] - 1$ se n è pari, $m \leq [n/2]$ se n è dispari, con una traslazione parallela allo spazio ortogonale ai piani di rotazione;
- (I) *inverse* (rovesciano l'orientamento dello spazio):
- (R) *riflessioni di direzione una retta*;
- (m-R R) *m-roto-riflessioni*: composizioni di una m -rotazione e di una riflessione di direzione ortogonale ai piani di rotazione, ove $m \leq [n/2] - 1$ se n è pari, $m \leq [n/2]$ se n è dispari
- (T-R) *glisso-m-roto-riflessioni*: composizioni di una m -rotazione e di una riflessione di direzione ortogonale ai piani di rotazione, ove $m \leq [n/2] - 1$, con una traslazione di direzione ortogonale sia ai piani di rotazione, sia alla direzione di riflessione.

DIMOSTRAZIONE. Si applica il teorema di decomposizione delle rigidità, il teorema di decomposizione in blocchi per applicazioni lineari (isometrie reali, notando che i blocchi possono avere autovalori ± 1 , oppure essere di ordine due ma in $\text{SO}_2(\mathbb{R})$: la rigidità sarà diretta o inversa a seconda che la molteplicità di -1 sia pari o dispari), e si semplifica la traslazione tenendo conto dei blocchi (i blocchi di rotazioni non identiche e l'eventuale riflessione permettono di "cancellare" la corrispondente traslazione). \square

3.4. DEFINIZIONE-TEOREMA (SIMILITUDINI). Sia f un'affinità di $\mathbb{E}_{\mathbb{R}}^n$ in sè; le seguenti proprietà sono equivalenti:

- (a) f conserva gli angoli retti, cioè per ogni $P, Q \in E$ si ha $(P-Q) \cdot (P'-Q') = 0$ se e solo se $(f(P)-f(Q)) \cdot (f(P')-f(Q')) = 0$;
- (b) esiste un numero reale $\alpha > 0$, tale che per ogni $P, Q \in E$ si abbia $d(P, Q) = \alpha d(f(P), f(Q))$;
- (c) esiste un numero reale $\alpha > 0$, tale che per ogni $P, Q, P', Q' \in E$ si abbia $(P-Q) \cdot (P'-Q') = \alpha^2 (f(P)-f(Q)) \cdot (f(P')-f(Q'))$;
- (d) f conserva gli angoli.

Le affinità di questo tipo si dicono similitudini (o omotetie); il numero α si dice il rapporto di similitudine

DIMOSTRAZIONE. Analoga al caso delle conformità. \square

3.4.1. Osservazioni simili a quelle per le rigidità.

3.4.2. FORMA MATRICIALE. Sia $A = \begin{pmatrix} 1 & 0 \\ v & A' \end{pmatrix}$ la matrice di un'affinità f di \mathbb{E} in sè in un riferimento ortonormale. Allora f è una similitudine se e solo se A' è una matrice conforme, i.e. $A'^t A' = \alpha^2 I_n$, per qualche numero reale $\alpha > 0$. Se $\det(A) > 0$ la similitudine si dice diretta, nel caso contrario si dice inversa.

3.4.3. PROBLEMA. Si mostri che l'insieme delle similitudini di \mathbb{E} in sè è un sottogruppo del gruppo delle affinità, e che tale sottogruppo contiene il gruppo delle isometrie. Si mostri poi che il sottoinsieme delle similitudini dirette è un sottogruppo del gruppo delle similitudini.

3.4.4. DILATAZIONI. Una dilatazione di centro R è un elemento di $\text{Centr}_R(\mathbb{E})$ tale che la matrice della applicazione lineare associata sia $\alpha \mathbb{I}$ (α è il fattore di dilatazione); si tratta di una similitudine.

3.4.5. TEOREMA (DECOMPOSIZIONE DI SIMILITUDINI). Ogni similitudine si scrive come composizione di una rigidità seguita da una dilatazione di centro R preassegnato, o anche in ordine inverso

DIMOSTRAZIONE. Analoga al caso delle affinità. \square

3.4.6. SIMILITUDINE DI FIGURE. Due figure F_1, F_2 (cioè sottoinsiemi di E) si dicono simili se esiste una similitudine f tale che $f(F_1) = F_2$. Si mostri che due triangoli di \mathbb{E} sono simili se esiste una corrispondenza tra i vertici (o tra i lati) dell'uno e quelli dell'altro, tale che a vertici corrispondenti corrispondano angoli uguali, oppure tale che il rapporto tra le lunghezze dei lati corrispondenti sia costante.

4. Piano euclideo.

4.1. INTERPRETAZIONE EUCLIDEA DELLE EQUAZIONI CARTESIANE DELLE RETTE: la retta r di equazione $aX+bY+c=0$ ha direzione ortogonale al vettore $\begin{pmatrix} a \\ b \end{pmatrix}$, dunque ha vettore direttore $\begin{pmatrix} b \\ -a \end{pmatrix}$.

L'angolo $\vartheta(r, r')$ tra due rette r ed r' è l'angolo formato dai vettori normali alle due rette, e quindi

$$\cos \vartheta(r, r') = \frac{|aa' + bb'|}{\sqrt{a^2 + b^2} \sqrt{a'^2 + b'^2}}.$$

4.2. DISTANZA PUNTO-RETTA:

$$d(P_0, r) = \frac{|ax_0 + by_0 + c|}{\sqrt{a^2 + b^2}}.$$

Se $r = P_1 + \langle v_1 \rangle$ e $u_1 = \text{cross}(v_1)$ (i.e. un vettore normale alla retta) allora

$$d(P_0, r) = \frac{|(P_1 - P_0) \cdot u_1|}{\|u_1\|}$$

(interpretazione geometrica?).

4.3. ASSE DI UN SEGMENTO: si tratta della retta dei punti equidistanti dai due punti dati P_0 e P_1 ; si scrive $(\frac{1}{2}P_0 + \frac{1}{2}P_1) + \langle P_1 - P_0 \rangle^\perp$, oppure tramite l'equazione:

$$(x_1 - x_0) \left(X - \frac{x_0 + x_1}{2} \right) + (y_1 - y_0) \left(Y - \frac{y_0 + y_1}{2} \right) = 0.$$

4.4. BISETTRICI DI DUE RETTE INCIDENTI: se $r_0 = P_0 + \langle v_0 \rangle$ e $r_1 = P_1 + \langle v_1 \rangle$ e $\|v_0\| = \|v_1\|$, allora le bisettrici sono date da $P + \langle v_0 \pm v_1 \rangle$ ove $P = r_0 \cap r_1$.

Se abbiamo equazioni cartesiane $a_0X + b_0Y + c_0 = 0$ e $a_1X + b_1Y + c_1 = 0$ con $a_0^2 + b_0^2 = a_1^2 + b_1^2$ allora le bisettrici hanno equazioni $(a_0X + b_0Y + c_0) \pm (a_1X + b_1Y + c_1) = 0$.

4.5. AREA DI TRIANGOLI:

$$A(P_0, P_1, P_2) = \frac{1}{2} \left| \det \begin{pmatrix} 1 & 1 & 1 \\ P_0 & P_1 & P_2 \end{pmatrix} \right| = \frac{1}{2} \left| \begin{vmatrix} 1 & 1 & 1 \\ x_0 & x_1 & x_2 \\ y_0 & y_1 & y_2 \end{vmatrix} \right|.$$

4.6. DISTANZA TRA RETTE PARALLELE: è la distanza tra una retta e un punto qualsiasi dell'altra retta.

4.7. CONGRUENZE PIANE. La scelta di un riferimento ortonormale sul piano $\mathbb{A}^2(\mathbb{R})$ determina un isomorfismo del gruppo $\text{Rig}(\mathbb{A}^2(\mathbb{R}))$ delle rigidità del piano con il sottogruppo

$$\left\{ \begin{pmatrix} 1 & 0 & 0 \\ a & A \end{pmatrix} \mid a, b \in \mathbb{R}; A \in O_2(\mathbb{R}) \right\}$$

di $\text{GL}_3(C)$. Ricordiamo che le rigidità si distinguono in dirette o inverse a seconda che $\det(A)$ sia 1 o -1. Le rigidità piane si classificano allora nel modo seguente:

4.7.1. ROTAZIONI. Sono le rigidità dirette che hanno un punto unito.

4.7.2. TRASLAZIONI. Sono le rigidità dirette prive di punti uniti.

4.7.3. RIFLESSIONI. Sono le rigidità inverse che hanno punti uniti (una retta, in effetti, di punti uniti).

4.7.4. GLISSORIFLESSIONI. Sono le rigidità inverse prive di punti uniti: si possono sempre scrivere come composizione di una riflessione e di una traslazione parallela all'asse di riflessione.

4.7.5. Questa classificazione si ottiene facilmente studiando le forme matriciali, oppure specializzando il teorema generale.

4.7.6. Che tipo di rigidità piana è la composizione di una rotazione e di una riflessione?

5. Spazio euclideo.

5.1. INTERPRETAZIONE EUCLIDEA DELLE EQUAZIONI DEI PIANI E DELLE RETTE: il piano π di equazione cartesiana $aX + bY + cZ + d = 0$ è ortogonale al vettore $\begin{pmatrix} a \\ b \\ c \end{pmatrix}$; dunque il sottospazio direttore del piano è dato da $\left(\begin{pmatrix} a \\ b \\ c \end{pmatrix} \right)^\perp$.

La retta $r = \pi \cap \pi'$ determinata dalle equazioni cartesiane di due piani non paralleli ha direzione ortogonale ai vettori $\begin{pmatrix} a \\ b \\ c \end{pmatrix}$ e $\begin{pmatrix} a' \\ b' \\ c' \end{pmatrix}$, dunque un suo vettore direttore è dato da $\begin{pmatrix} a \\ b \\ c \end{pmatrix} \times \begin{pmatrix} a' \\ b' \\ c' \end{pmatrix}$.

L'angolo $\vartheta(\pi, \pi')$ tra due piani π e π' , corrisponde all'angolo tra i vettori normali, e dunque

$$\vartheta(\pi, \pi') = \frac{|aa' + bb' + cc'|}{\sqrt{a^2 + b^2 + c^2} \sqrt{a'^2 + b'^2 + c'^2}}.$$

L'angolo tra due rette incidenti si misura come l'angolo tra i vettori direttori.

L'angolo tra un piano π e una retta $r = \pi' \cap \pi''$ si scrive come

$$\sin \vartheta(\pi, r) = \frac{|(a \ b \ c)v|}{\sqrt{a^2 + b^2 + c^2} \|v\|}$$

se v è un vettore direttore della retta, per esempio $v = \begin{pmatrix} a' \\ b' \\ c' \end{pmatrix} \times \begin{pmatrix} a'' \\ b'' \\ c'' \end{pmatrix}$.

5.2. DISTANZA PUNTO-PIANO:

$$d(P_0, \pi) = \frac{|ax_0 + by_0 + cz_0 + d|}{\sqrt{a^2 + b^2 + c^2}}.$$

Se $\pi = P_1 + \langle v_1, v_1' \rangle$ allora

$$d(P_0, \pi) = \frac{|(P_1 - P_0) \cdot (v_1 \times v_1')|}{\|v_1 \times v_1'\|}$$

(interpretazione geometrica: il numeratore è il volume di un parallelepipedo di cui il denominatore è la base). Il disegno è già stato visto: dove?

5.3. DISTANZA TRA PIANI PARALLELI: si tratta della distanza tra un punto qualsiasi di un piano e l'altro piano.

5.4. DISTANZA RETTA-PIANO: è nulla se non sono paralleli, e se lo sono è la distanza dal piano di un punto qualsiasi della retta.

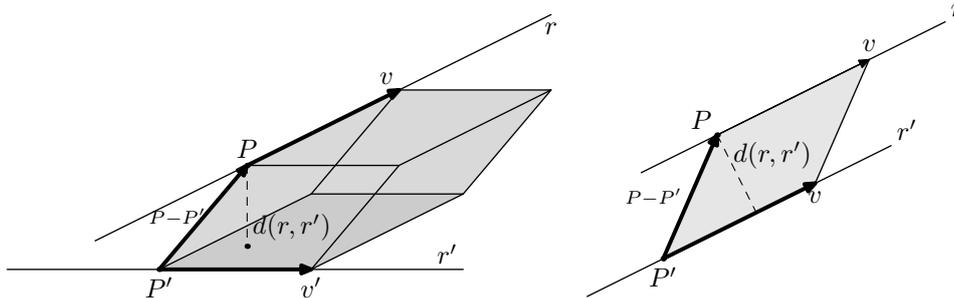
5.5. DISTANZA RETTA-RETTA: siano $r = P + \langle v \rangle$ e $r' = P' + \langle v' \rangle$; allora se r ed r' non sono parallele:

$$d(r, r') = \frac{|(P - P') \cdot (v \times v')|}{\|v \times v'\|}$$

(interpretazione geometrica: il numeratore è il volume di un parallelepipedo di cui il denominatore è l'area di base); mentre se sono parallele:

$$d(r, r') = \frac{\|(P - P') \times v\|}{\|v\|}$$

(interpretazione geometrica: il numeratore è area di un parallelogramma di cui il denominatore è la misura della base).



5.6. DISTANZA PUNTO-RETTA: sia $r = P + \langle v \rangle$, allora

$$d(P_0, r) = \frac{\|(P - P_0) \times v\|}{\|v\|}$$

(interpretazione geometrica?).

5.7. ASSE DI UN SEGMENTO: si tratta del piano dei punti equidistanti dai due punti dati P_0 e P_1 ; si scrive $(\frac{1}{2}P_0 + \frac{1}{2}P_1) + \langle P_1 - P_0 \rangle^\perp$, oppure tramite l'equazione:

$$(x_1 - x_0) \left(X - \frac{x_0 + x_1}{2} \right) + (y_1 - y_0) \left(Y - \frac{y_0 + y_1}{2} \right) + (z_1 - z_0) \left(Z - \frac{z_0 + z_1}{2} \right) = 0.$$

5.8. BISSETTRICI DI DUE PIANI INCIDENTI: se abbiamo equazioni cartesiane $a_0X + b_0Y + c_0Z + d_0 = 0$ e $a_1X + b_1Y + c_1Z + d_1 = 0$ con $a_0^2 + b_0^2 + c_0^2 = a_1^2 + b_1^2 + c_1^2$ allora i piani bisettrici hanno equazioni $(a_0X + b_0Y + c_0Z + d_0) \pm (a_1X + b_1Y + c_1Z + d_1) = 0$.

5.9. AREA DI TRIANGOLI: $A(P_0, P_1, P_2) = \frac{1}{2} \|(P_1 - P_0) \times (P_2 - P_0)\|$, e si esplicita come

$$\frac{1}{2} \sqrt{\det((P_i - P_0) \cdot (P_j - P_0))} = \frac{1}{2} \sqrt{\left| \begin{array}{ccc} 1 & 1 & 1 \\ x_0 & x_1 & x_2 \\ y_0 & y_1 & y_2 \end{array} \right|^2 + \left| \begin{array}{ccc} 1 & 1 & 1 \\ x_0 & x_1 & x_2 \\ z_0 & z_1 & z_2 \end{array} \right|^2 + \left| \begin{array}{ccc} 1 & 1 & 1 \\ y_0 & y_1 & y_2 \\ z_0 & z_1 & z_2 \end{array} \right|^2}$$

ove le $(x_i, y_i, z_i)^t$ sono le coordinate di P_i in un riferimento ortonormale.

5.10. VOLUME DI TETRAEDRI:

$$V(P_0, P_1, P_2, P_3) = \frac{1}{6} \left| \det \begin{pmatrix} 1 & 1 & 1 & 1 \\ P_0 & P_1 & P_2 & P_3 \end{pmatrix} \right| = \frac{1}{6} \left| \begin{array}{cccc} 1 & 1 & 1 & 1 \\ x_0 & x_1 & x_2 & x_3 \\ y_0 & y_1 & y_2 & y_3 \\ z_0 & z_1 & z_2 & z_3 \end{array} \right|$$

ove le $(x_i, y_i, z_i)^t$ sono le coordinate di P_i in un riferimento ortonormale.

5.11. CONGRUENZE DELLO SPAZIO. La scelta di un riferimento ortonormale sullo spazio $\mathbb{E}^3(\mathbb{R})$ determina un isomorfismo del gruppo $\text{Rig}(\mathbb{A}^3(\mathbb{R}))$ delle rigidità dello spazio con il sottogruppo

$$\left\{ \begin{pmatrix} 1 & 0 & 0 & 0 \\ a & A & & \\ b & & & \\ c & & & \end{pmatrix} \mid a, b, c \in \mathbb{R}; A \in \text{GL}_3(\mathbb{R}) \right\}$$

di $\text{GL}_4(\mathbb{R})$. Tali rigidità si classificano nel modo seguente:

5.11.1. ROTAZIONI (DI ASSE UNA RETTA). Sono le rigidità dirette con (una retta di) punti uniti.

5.11.2. TRASLAZIONI. Sono rigidità dirette senza punti uniti.

5.11.3. ROTO-TRASLAZIONI O GLISSOROTAZIONI. Sono rigidità dirette senza punti uniti, composizioni di una rotazione di asse una retta e di una traslazione parallela all'asse.

5.11.4. RIFLESSIONI. Sono le rigidità inverse con (un piano di) punti uniti.

5.11.5. ROTO-RIFLESSIONI. Sono le rigidità inverse con un punto unito: composizione di una riflessione e di una rotazione di asse ortogonale al piano di riflessione.

5.11.6. GLISSORIFLESSIONI. Sono le rigidità inverse prive di punti uniti: composizione di una riflessione e di una traslazione di direzione parallela al piano di riflessione.

5.11.7. Anche questa classificazione si ottiene facilmente studiando le forme matriciali, oppure specializzando il teorema generale.

5.11.8. Che tipo di rigidità spaziale è la composizione di una rotazione e di una riflessione d'asse parallelo al piano di rotazione?

6. Spazio euclideo di dimensione quattro.

La stesura di questo paragrafo è un esercizio per il lettore.

7. Spazi Euclidei Complessi o Spazi Hermitiani.

7.1. Si può pensare di estendere al caso di spazi vettoriali complessi tutte le strutture (prodotto scalare, norme, angoli, prodotto vettore,...) che abbiamo definito nel primo paragrafo. Un modo ovvio, e utile in certi contesti, ma che porta a spazi molto diversi dagli "usuali" è di definire il prodotto scalare nello stesso modo che per spazi reali: se $v, w \in V_n(\mathbb{C})$ allora $v \cdot w := v^t w = \sum_{j=1}^n z_j z'_j$ se $v = (z_j)^t$ e $w = (z'_j)^t$. Tuttavia questo comporta alcune conseguenze che allontanano dall'intuizione geometrica:

7.1.1. si trovano vettori non nulli "ortogonali a sé stessi": per esempio il vettore $v = \begin{pmatrix} 1 \\ i \end{pmatrix} \in V_2(\mathbb{C})$ ha la proprietà che $v \cdot v = 1^2 + i^2 = 0$;

7.1.2. si trovano vettori il cui prodotto con sé stessi non è un numero reale, e quindi diventa impossibile parlare di positività e difficile parlare di norme: per esempio il vettore $v = \begin{pmatrix} 1 \\ 1+i \end{pmatrix} \in V_2(\mathbb{C})$ ha la proprietà che $v \cdot v = 1^2 + (1+i)^2 = 1 + 2i$.

Quindi questa è una estensione a $V_n(\mathbb{C})$ del prodotto scalare di $V_n(\mathbb{R})$ che fuori dallo "scheletro reale" (in cui le parti immaginarie sono tutte nulle) si comporta in modo bizzarro. Tuttavia un'altra estensione si rivela essere molto più vicina all'intuizione, e risulta estremamente utile.

7.2. DEFINIZIONE-TEOREMA (PRODOTTO HERMITIANO). Sia $V_n(\mathbb{C})$ lo spazio vettoriale standard su \mathbb{C} di dimensione n . Definiamo il prodotto hermitiano di due vettori $v = (z_j)^t$ e $w = (z'_j)^t$ come $v \cdot w := v^t \bar{w} = \sum_j z_j \bar{z}'_j$, ove si sono usate le coordinate nella base canonica.

Il prodotto hermitiano dà una funzione $V_n(\mathbb{C}) \times V_n(\mathbb{C}) \rightarrow \mathbb{C}$ che gode delle seguenti proprietà:

- (PH1) hermitianità o emisimmetria: $v \cdot w = \overline{w \cdot v}$ (per ogni $v, w \in V_n(\mathbb{C})$);
 (PH2) linearità sinistra: $(\alpha_1 v_1 + \alpha_2 v_2) \cdot w = \alpha_1 (v_1 \cdot w) + \alpha_2 (v_2 \cdot w)$ e emilinearità destra: $v \cdot (\alpha_1 w_1 + \alpha_2 w_2) = \alpha_1 (v \cdot w_1) + \alpha_2 (v \cdot w_2)$ (per ogni $v, v_1, v_2, w, w_1, w_2 \in V_n(\mathbb{C})$, ed ogni $\alpha_1, \alpha_2 \in \mathbb{C}$);
 (PH3) positività: $v \cdot v \geq 0$ (per ogni $v \in V_n(\mathbb{C})$); $v \cdot v = 0$ se e solo se $v = 0$.

Lo spazio vettoriale $V_n(\mathbb{C})$ dotato del prodotto hermitiano si dice lo spazio euclideo (complesso) standard di dimensione n o spazio Hermitiano standard di dimensione n .

Si possono allora ripetere molti risultati e definizioni della geometria usuale:

7.3. DEFINIZIONE (NORMA). La norma di un vettore $v \in V_n(\mathbb{C})$ è definita come

$$\|v\| := \sqrt{v \cdot v}$$

(si usa la positività). Un vettore di norma 1 si dice un versore.

7.4. TEOREMA (DISUGUAGLIANZA DI CAUCHY-SCHWARZ). Per ogni $v, w \in V_n(\mathbb{C})$ vale che

$$|v \cdot w|^2 \leq (v \cdot v)(w \cdot w)$$

(si noti che $v \cdot w \in \mathbb{C}$, e usiamo la norma in senso complesso) e dunque

$$|v \cdot w| \leq \|v\| \|w\|.$$

Inoltre vale l'uguaglianza se e solo se v e w sono linearmente dipendenti.

DIMOSTRAZIONE. Conviene imporre la condizione $u \cdot u \geq 0$ ove $u = xv - yw$ e $x = w \cdot w$, $y = v \cdot w$. \square

7.5. TEOREMA (PROPRIETÀ DELLA NORMA).

- (N1) $\|v\| = 0$ se e solo se $v = 0$;
 (N2) $\|\alpha v\| = |\alpha| \|v\|$;
 (N3) $\|v + w\| \leq \|v\| + \|w\|$ (disuguaglianza triangolare);
 (N4) $\|v \pm w\|^2 = \|v\|^2 \pm 2\Re(v \cdot w) + \|w\|^2$ (versione complessa del teorema di Carnot);
 (N5) $\|v + w\|^2 + \|v - w\|^2 = 2(\|v\|^2 + \|w\|^2)$.

7.6. DEFINIZIONE (ORTOGONALITÀ). Due vettori $v, w \in V_n(\mathbb{C})$ si dicono ortogonali e si scrive $v \perp w$ se vale $v \cdot w = 0$ (il loro prodotto hermitiano è zero).

7.7. TEOREMA (PITAGORA). Abbiamo che $\Re(v \cdot w) = 0$ ($v \cdot w$ è puramente immaginario) se e solo se $\|v + w\|^2 = \|v\|^2 + \|w\|^2$. In generale, vedi (N4) del teorema precedente.

7.8. DEFINIZIONE (PROIEZIONE ORTOGONALE). Proiezione ortogonale di un vettore v nella direzione di w :

$$p_w(v) = \frac{v \cdot w}{\|w\|^2} w = \frac{v \cdot w}{w \cdot w} w.$$

Risulta che $p_w(v) \perp (v - p_w(v))$.

7.9. BASI ORTOGONALI E ORTONORMALI. Una base di $V_n(\mathbb{C})$ si dice ortogonale se essa è formata di vettori a due a due ortogonali; si dice ortonormale se inoltre i suoi vettori hanno tutti norma 1. Se (v_1, \dots, v_n) è una base ortonormale di $V_n(\mathbb{C})$, allora le coordinate di un vettore $v \in V_n(\mathbb{C})$ in quella base sono date da $(v \cdot v_1, \dots, v \cdot v_n)^t$.

Usando la nozione di proiezione ortogonale è sempre possibile, come nel caso euclideo reale, trovare una base ortonormale a partire da un insieme qualsiasi di generatori, tramite il procedimento di Gram-Schmidt.

7.10. DEFINIZIONE-TEOREMA (ORTOGONALI DI SOTTOSPACI). Per S sottinsieme di $V_n(\mathbb{C})$ definiamo l'ortogonale $S^\perp = \{v \in V_n(\mathbb{C}) | v \perp s \ (\forall s \in S)\}$, che risulta un sottospazio vettoriale.

Valgono esattamente le stesse proprietà (O i) per $i = 0, 1, 2, 3, 4$ che per l'analogia nozione reale:

(O0) $\{0\}^\perp = V_n(\mathbb{C}), V_n(\mathbb{C})^\perp = 0,$

(O1) Se $S \subseteq T$ allora $T^\perp \subseteq S^\perp;$

(O2) $\langle S \rangle = (S^\perp)^\perp;$ dunque per W sottospazio: $(W^\perp)^\perp = W.$ Inoltre $((S^\perp)^\perp)^\perp = S^\perp.$

(O3) Se W e W' sono sottospazi vettoriali di $V_n(\mathbb{C})$: $(W + W')^\perp = W^\perp \cap W'^\perp$

(O4) Se W e W' sono sottospazi vettoriali di $V_n(\mathbb{C})$: $(W \cap W')^\perp = W^\perp + W'^\perp.$

7.11. DEFINIZIONE-TEOREMA (TRASFORMAZIONI HERMITIANE O ISOMETRIE COMPLESSE).

Sia φ un automorfismo di $V_n(\mathbb{C})$ in sè; le due proprietà seguenti sono equivalenti:

(1) φ rispetta la struttura hermitiana, i.e. $\varphi(v) \cdot \varphi(w) = v \cdot w$ per ogni $v, w \in V_n(\mathbb{C});$

(2) φ rispetta la norma dei vettori, i.e. $\|\varphi(v)\| = \|v\|$ per ogni $v \in V_n(\mathbb{C}).$

Tali automorfismi si dicono trasformazioni hermitiane o isometrie complesse di $V_n(\mathbb{C}).$

Per vedere che (2) implica (1) conviene applicare (2) ai vettori $v + w$ (e si ottiene $\Re(\varphi(v) \cdot \varphi(w)) = \Re(v \cdot w)$) e $iv + iw$ (e si ottiene $\Im(\varphi(v) \cdot \varphi(w)) = \Im(v \cdot w)$)

7.11.1. DA CONTROLLARE. Una applicazione insiemistica di $V_n(\mathbb{C})$ in sè che soddisfi alla proprietà (1) è necessariamente un morfismo lineare; infatti si tratta di verificare che $\varphi(v + \alpha w) - \varphi(v) - \alpha\varphi(w) = 0$, ovvero che il suo prodotto hermitiano con sé stesso è nullo.

D'altra parte un morfismo lineare che rispetti la proprietà (2) è necessariamente biiettivo, e dunque un automorfismo. Infatti da $\varphi v = 0$ segue $\|v\| = \|\varphi v\| = 0$, e dunque $v = 0$.

Quindi il teorema poteva essere enunciato così: una applicazione insiemistica di $V_n(\mathbb{C})$ in sè rispetta il prodotto hermitiano se e solo se è una applicazione lineare che rispetta la norma; e in tal caso si tratta di una applicazione biettiva, dunque di un automorfismo.

7.12. TEOREMA (GRUPPO UNITARIO). Sia φ una trasformazione hermitiana. Ogni matrice A associata a φ usando una base di vettori ortonormali (tali che $v_i \cdot v_j = \delta_{i,j}$) risulta una matrice unitaria, i.e. tale che $A^t \bar{A} = \mathbb{I}$, ovvero $A^{-1} = \bar{A}^t$. Le matrici unitarie formano un sottogruppo (non normale, se $n > 1$) di $GL(n, \mathbb{C})$ che si indica con $U(n, \mathbb{C})$ o $U_n(\mathbb{C})$ e si dice il Gruppo Unitario. Se $A \in U_n(\mathbb{C})$, allora $|\det A| = 1$ ($\det A$ è numero complesso di modulo 1).

7.12.1. GRUPPO UNITARIO SPECIALE. Il sottinsieme di $U_n(\mathbb{C})$ formato dalle matrici di determinante 1 si indica con $SU(n, \mathbb{C})$ o $SU_n(\mathbb{C})$ e si dice il gruppo unitario speciale. Si tratta di un sottogruppo normale di $U_n(\mathbb{C})$, e il quoziente $U_n(\mathbb{C})/SU_n(\mathbb{C})$ è isomorfo a \mathbb{S}^1 (gruppo moltiplicativo dei complessi di modulo 1).

7.12.2. Si osservi che l'intersezione di $U_n(\mathbb{C})$ e $SU_n(\mathbb{C})$ con $GL_n(\mathbb{R})$ danno rispettivamente $O_n(\mathbb{R})$ e $SO_n(\mathbb{R})$

7.12.3. FORMULA DI PARSEVAL. Se v_1, \dots, v_n è una base ortonormale di $V_n(\mathbb{C})$, allora le coordinate di $v \in V_n(\mathbb{C})$ in questa base ($v = \sum_i x_i v_i$) sono date da $x_i = v \cdot v_i = \bar{v}_i \cdot \bar{v}$.

Se poi $v, w \in V_n(\mathbb{C})$ allora il prodotto hermitiano si calcola con la formula di Parseval: $v \cdot w = \sum_i (v \cdot v_i)(\bar{w} \cdot \bar{v}_i) = \sum_i (v \cdot v_i)(v_i \cdot w).$

7.13. TEOREMA (TEOREMA SPETTRALE COMPLESSO (VERSIONE MATRICIALE)). Una matrice $A \in M_n(\mathbb{C})$ si dice hermitiana se $A^t = \bar{A}$ (la trasposta coincide con la coniugata; se si tratta di matrici reali significa che è simmetrica). Ogni matrice hermitiana è unitariamente diagonalizzabile, cioè esiste una matrice $P \in U_n(\mathbb{C})$ tale che $P^{-1}AP = \bar{P}^t AP$ sia diagonale (reale).

7.13.1. Tralasciamo la dimostrazione, che è simile a quella svolta nel caso reale. Facciamo invece notare che il viceversa dell'enunciato non è assolutamente vero: esistono matrici che sono unitariamente diagonalizzabili, ma non sono hermitiane. Per esempio una qualsiasi matrice diagonale complessa ma non reale. Un altro esempio sono le matrici antisimmetriche reali: non sono hermitiane, ma lo diventano moltiplicate per i ; quindi sono unitariamente diagonalizzabili (autovalori puramente immaginari).

7.13.2. La stessa tecnica di dimostrazione permette di arrivare a questo risultato: una matrice complessa A è unitariamente diagonalizzabile se e solo se A e \bar{A}^t commutano per prodotto (i.e. $A\bar{A}^t = \bar{A}^t A$, e queste matrici si dicono normali).

Infatti, prima di tutto si osserva che A e \bar{A}^t hanno lo stesso nucleo (poiché $Av = 0$ sse $\overline{(Av)}^t(Av) = 0$ sse $\overline{(\bar{A}^t v)}^t(\bar{A}^t v) = 0$ sse $\bar{A}^t v = 0$); quindi l'autospazio di A relativo all'autovalore λ coincide con l'autospazio di \bar{A}^t relativo all'autovalore $\bar{\lambda}$: $Av = \lambda v$ sse $\bar{A}^t v = \bar{\lambda}v$.

A questo punto, se v e w sono autovettori di autovalori λ e μ distinti dalle solite uguaglianze

$$\bar{\lambda}\bar{v}^t w = \bar{\lambda}v^t w = \bar{A}v^t w = \bar{v}^t \bar{A}^t w = \bar{v}^t \bar{\mu}w = \bar{\mu}\bar{v}^t w$$

si ottiene che $(\lambda - \mu)\bar{v}^t w = 0$, da cui l'ortogonalità (hermitiana) di autospazi distinti. Dunque dal solito ragionamento (stabilità di ortogonali di sottospazi stabili) si arriva alla diagonalizzabilità.

7.13.3. Si vede allora che vi sono vari casi interessanti:

- (1) una matrice è hermitiana se e solo se è normale (o unitariamente diagonalizzabile) con spettro reale;
- (2) una matrice è antihermitiana ($A^t = -\bar{A}$) se e solo se è normale (o unitariamente diagonalizzabile) con spettro puramente immaginario;
- (3) una matrice è unitaria se e solo se è normale (o unitariamente diagonalizzabile) con spettro unitario;
- (4) una matrice reale è ortogonale se e solo se è normale (o unitariamente diagonalizzabile) con spettro unitario.

7.14. DESCRIZIONE ESPLICITA DI $U_2(\mathbb{C})$ E $SU_2(\mathbb{C})$. Le matrici in $U_2(\mathbb{C})$ sono tutte e sole le matrici complesse della forma

$$\begin{pmatrix} \alpha & \beta \\ -\varrho\bar{\beta} & \varrho\bar{\alpha} \end{pmatrix} \quad \text{con} \quad |\alpha|^2 + |\beta|^2 = 1 \quad \text{e} \quad |\varrho| = 1,$$

mentre le matrici in $SU_2(\mathbb{C})$ sono tutte e sole le matrici complesse della forma

$$\begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix} \quad \text{con} \quad |\alpha|^2 + |\beta|^2 = 1;$$

entrambi i risultati si vedono facilmente esplicitando la condizione $A^t \bar{A} = \mathbb{I}$, e che $\det A = 1$ nel caso speciale.

♠♠ **7.14.1.** RELAZIONI TRA $SU_2(\mathbb{C})$ E $SO_3(\mathbb{R})$. Per $SU_2(\mathbb{C})$ possiamo ottenere una descrizione più suggestiva usando le componenti reali: se $\alpha = x_0 + ix_1$ e $\beta = x_2 + ix_3$ otteniamo

$$\begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix} = x_0 \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + x_1 \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} + x_2 \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} + x_3 \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} = x_0 \mathbb{I}_2 + x_1 I + x_2 J + x_3 K.$$

Si osserva subito che lo spazio vettoriale reale di dimensione 4 generato da \mathbb{I}_2, I, J, K in $GL_2(\mathbb{C})$ ha (considerando il prodotto tra matrici) struttura di corpo isomorfo a quello dei quaternioni; infatti $I^2 = J^2 = K^2 = -\mathbb{I}_2$, $IJ = K = -JI$, $JK = I = -KJ$, $KI = J = -IK$; il quadrato della norma dei quaternioni corrisponde al determinante delle matrici, quindi i quaternioni unitari corrispondono alle matrici unitarie speciali. Di conseguenza possiamo dire che: $SU_2(\mathbb{C})$ sta a \mathbb{H}^1 (sfera tridimensionale in \mathbb{R}^4) come $SO_2(\mathbb{R})$ sta a S^1 (sfera unidimensionale in \mathbb{R}^2).

Da quanto abbiamo allora visto nella descrizione di $SO_3(\mathbb{R})$, possiamo concludere che esiste un omomorfismo canonico di gruppi $SU_2(\mathbb{C}) \rightarrow SO_3(\mathbb{R})$, che manda la matrice sopra scritta nella matrice corrispondente al quaternioni unitario (x_0, x_1, x_2, x_3) . Questo morfismo è suriettivo, e ogni trasformazione euclidea tridimensionale viene determinata da due trasformazioni unitarie speciali (una e l'opposta). Quindi possiamo concludere che dare un elemento di $SU_2(\mathbb{C})$ consiste nel dare un elemento di $SO_3(\mathbb{R})$ con un segno ± 1 ; per questo $SU_2(\mathbb{C})$ viene spesso chiamato il gruppo degli spin.

Descrizione diretta della rotazione associata ad un elemento di $SU_2(\mathbb{C})$: senza passare attraverso il calcolo fatto con i quaternioni, possiamo procedere nel modo seguente. Ogni elemento A di $SU_2(\mathbb{C})$ determina una isometria φ_A dello spazio vettoriale euclideo reale $\langle I, J, K \rangle_{\mathbb{R}}$, di cui I, J, K formano una base ortonormale (la norma essendo data dal determinante delle matrici), tramite la formula $\varphi_A(X) = AX\bar{A}^t$. Questo determina un omomorfismo di gruppi $SU_2(\mathbb{C}) \rightarrow \text{Aut}(\langle I, J, K \rangle_{\mathbb{R}}) = SO_3(\mathbb{R})$; si tratta di un morfismo suriettivo con nucleo $\{\pm \mathbb{I}_2\}$.

7.15. PRODOTTO VETTORE. Nello spazio Hermitiano ha ancora senso definire il prodotto vettore come abbiamo fatto per lo spazio vettoriale Euclideo Reale, e possiede ugualmente le proprietà (C_i)

per $i = 1, 2, 4, 5$. Tuttavia la proprietà fondamentale (C3) diventa ora: il prodotto vettore è ortogonale ai coniugati di ciascuno dei suoi fattori, ovvero $\overline{v_i} \cdot \text{cross}(v_1, \dots, v_{n-1}) = 0$. Per il teorema di Lagrange?

7.16. EQUAZIONI DI SOTTOSPAZI. Si osservi che l'interpretazione hermitiana (o euclidea complessa) delle equazioni di sottospazi diventa ora la seguente: i coefficienti di ogni equazione formano un vettore il cui coniugato è ortogonale al sottospazio stesso. In particolare, in $V_3(\mathbb{C})$, il sottospazio generato da due vettori indipendenti v e w ha come coefficienti dell'equazione le componenti del prodotto vettore $v \times w$ (proprietà affine o vettoriale), ma come vettore ortogonale il coniugato $\overline{v \times w}$ (proprietà metrica, o hermitiana, o euclidea complessa).

7.17. RELAZIONI CON IL CASO REALE. L'applicazione biiettiva

$$r : V_n(\mathbb{C}) \longrightarrow V_{2n}(\mathbb{R})$$

che manda un vettore complesso $v = (z_i)^t = (x_i + iy_i)^t$ nel vettore reale $r(v) = (x_1, \dots, x_n, y_1, \dots, y_n)^t$ possiede la proprietà che $\|r(v)\| = \|v\|$ per ogni $v \in V_n(\mathbb{C})$ (norme euclidea nel primo membro, ed hermitiana nel secondo), e più in generale

$$r(v) \cdot r(w) = \Re(v \cdot w)$$

(prodotto scalare euclideo nel primo membro, ed hermitiano nel secondo) per $v, w \in V_n(\mathbb{C})$. In effetti possiamo esplicitare: $v \cdot v' = \sum_{j=1}^n (x_j x'_j + y_j y'_j) + i \sum_{j=1}^n (x_j y'_j - y_j x'_j)$ mentre $r(v) \cdot r(v') = \sum_{j=1}^n (x_j x'_j + y_j y'_j)$.

7.18. SPAZI HERMITIANI. Uno spazio affine su $V_n(\mathbb{C})$, quest'ultimo dotato della struttura di spazio Hermitiano, permette una trattazione simile a quella fatta per gli Spazi Euclidei reali; lasciamo il compito al lettore, dicendo solo che questi spazi si dicono Euclidei Complessi o Spazi Hermitiani. L'applicazione biiettiva naturale $r : \mathbb{A}^n(\mathbb{C}) \longrightarrow \mathbb{A}^{2n}(\mathbb{R})$ risulta allora una isometria (cioè $d(P, P') = d(r(P), r(P'))$ per ogni $P, P' \in \mathbb{A}^n(\mathbb{C})$).

8. Esercizi.

8.1. Esercizi su Spazi Vettoriali Euclidei.

8.1.1. Sia $V = V_n(\mathbb{R})$ lo spazio vettoriale standard di dimensione n su \mathbb{R} , dotato del prodotto scalare. Indichiamo con u, v, w elementi di $V_n(\mathbb{R})$. Dire se le seguenti affermazioni sono vere o false, fornendo dimostrazioni o controesempi:

- (a) se u è non nullo e $u \cdot v = u \cdot w$ per allora $v = w$;
- (b) se $v \cdot w = 0$ per ogni $w \in V$ allora $v = 0$;
- (b') se $v \cdot w = 0$ per ogni vettore w di una base di V allora $v = 0$;
- (c) se $u \cdot v = u \cdot w$ per ogni $u \in V$ allora $v = w$;
- (c') se $u \cdot v = u \cdot w$ per ogni vettore u di una base di V allora $v = w$.

8.1.2. Sia $V = V_n(\mathbb{R})$ lo spazio vettoriale standard di dimensione n su \mathbb{R} , dotato del prodotto scalare. Indichiamo con u, v, w elementi di $V_n(\mathbb{R})$. Dire se le seguenti affermazioni sono vere o false, fornendo dimostrazioni o controesempi:

- (a) $\|v + w\| = \|v - w\|$ se e solo se $v \cdot w = 0$;
- (b) $\|v + tw\| \geq \|v\|$ per ogni $t \in \mathbb{R}$ se e solo se $v \cdot w = 0$;
- (c) $\|v + w\|^2 + \|v - w\|^2 = 2(\|v\|^2 + \|w\|^2)$ (interpretazione geometrica?);
- (d) $\|v + w\|^2 - \|v - w\|^2 = 4v \cdot w$

8.1.3. Siano u_1 e u_2 due vettori linearmente indipendenti dello spazio vettoriale standard di dimensione n su \mathbb{R} , dotato del prodotto scalare. Sia $v = \alpha_1 v_1 + \alpha_2 v_2$. Poniamo v_1 la proiezione ortogonale di v lungo u_1 e v_2 la proiezione ortogonale di v lungo u_2 . Che relazioni vi sono tra α_1 , α_2 , v_1 e v_2 ?

8.1.4. Siano u_1 e u_2 due vettori linearmente indipendenti dello spazio vettoriale standard di dimensione n su \mathbb{R} , dotato del prodotto scalare. Sia $v = \alpha_1 v_1 + \alpha_2 v_2$. Trovare le relazioni tra le aree dei triangolo definiti dalle seguenti coppie di vettori: u_1 e u_2 , u_1 e v , v e u_2 .

Generalizzare considerando tre vettori e i volumi dei tetraedri.

8.1.5. Siano v_1 e v_2 due vettori linearmente indipendenti dello spazio vettoriale standard di dimensione n su \mathbb{R} , dotato del prodotto scalare. Siano u_2 la proiezione ortogonale di v_2 lungo v_1 e u_1 la proiezione ortogonale di v_1 lungo v_2 . Che relazioni vi sono tra le aree A, A_1, A_2, A' dei quattro tetraedri identificati rispettivamente dalle coppie di vettori v_1 e v_2, v_1 e u_1, v_2 e u_2, u_1 e u_2 ?

8.1.6. Siano v e w due vettori linearmente indipendenti e sia $u = v - w$. Mostrare che i tre parallelogrammi definiti dalle coppie di vettori v e w, v e u, u e w sono uguali.

8.1.7. Siano v e w due vettori linearmente indipendenti e sia u la proiezione ortogonale di w su v . Trovate la relazione tra l'area del triangolo definito dai vettori v e w e l'area del triangolo definito dai vettori u e w .

8.1.8. Siano v_1 e v_2 due vettori linearmente indipendenti dello spazio vettoriale standard di dimensione 2 su \mathbb{R} , dotato del prodotto scalare. Sia u un vettore non nullo, e siano u_1 la proiezione ortogonale di u lungo v_1 e u_2 la proiezione ortogonale di u lungo v_2 . Mostrare che $u = u_1 + u_2$ se e solo se v_1 è ortogonale a v_2 .

È vero lo stesso risultato in uno spazio vettoriale euclideo di dimensione 3? Se no, come si può modificare l'enunciato affinché diventi vero?

E per uno spazio di dimensione n ?

8.1.9. Siano v_1 e v_2 due vettori linearmente indipendenti dello spazio vettoriale standard di dimensione n su \mathbb{R} , dotato del prodotto scalare. Mostrare che $\vartheta(v_1, v_1 + v_2) = \vartheta(v_2, v_1 + v_2)$ se e solo se $\|v_1\| = \|v_2\|$ (indichiamo con $\vartheta(v, w)$ l'angolo tra i vettori v e w).

8.1.10. Siano v e w due vettori linearmente indipendenti (indichiamo con $\vartheta(v, w)$ l'angolo tra i vettori v e w).

- (a) mostrare che $\lim_{t \rightarrow \infty} \vartheta(v, v + tw) = \vartheta(v, w)$;
 (b) mostrare che $\sum_{i=1}^{\infty} \vartheta(v + iw, v + (i+1)w) = \vartheta(v, w)$.

8.1.11. Nello spazio euclideo \mathbb{R}^3 si considerino i vettori $v = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$ e $w = \begin{pmatrix} 2 \\ 2 \\ 1 \end{pmatrix}$.

- (a) Si decomponga il vettore v come somma $v_1 + v_2$ ove v_1 sia ortogonale a w , e v_2 parallelo a w .
 (b) Si determinino le superfici dei due parallelogrammi aventi come lati i vettori v, v_1 (primo parallelogramma) e v, v_2 (secondo parallelogramma)
 (c) Le due superfici del punto precedente risultano uguali: dire se si tratta di un risultato generale (indipendente dai vettori v e w scelti), ed eventualmente giustificarlo e darne una interpretazione in termini di geometria (piana) elementare.

8.1.12. Nello spazio euclideo \mathbb{R}^3 si considerino i vettori $v_1 = \begin{pmatrix} 2 \\ 0 \\ -1 \end{pmatrix}$ e $v_2 = \begin{pmatrix} 0 \\ -2 \\ 1 \end{pmatrix}$.

- (a) determinare il sottospazio ortogonale a $\langle v_1, v_2 \rangle$;
 (b) decomporre il vettore $w = \begin{pmatrix} 1 \\ -1 \\ -9 \end{pmatrix}$ come somma $w = w_1 + w_2 + w_3$ ove w_1 sia parallelo a v_1, w_2 sia parallelo a v_2 e w_3 sia ortogonale sia a v_1 che a v_2 .
 (c) mostrare che i volumi dei tre tetraedri formati rispettivamente da

$$w, w_1, w_2 \quad , \quad w, w_1, w_3 \quad \text{e} \quad w, w_2, w_3$$

sono uguali tra loro (senza calcolarli).

8.1.13. Nello spazio euclideo \mathbb{R}^3 si considerino i vettori $v = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$ e $w = \begin{pmatrix} 0 \\ 1 \\ \sqrt{3} \end{pmatrix}$.

- (a) calcolare l'angolo formato da v e w ;
 (b) determinare, se esistono, tutti i vettori che formano due angoli uguali di ampiezza 30° con v e w ;
 (c) determinare, se esistono, tutti i vettori che formano due angoli uguali di ampiezza 60° con v e w ;
 (d) determinare, se esistono, tutti i vettori che formano due angoli uguali di ampiezza 90° con v e w ;
 (e) dire se i tre sottinsiemi di \mathbb{R}^3 prima trovati sono o no sottospazi vettoriali.

8.1.14. Determinare tutte le matrici reali ortogonali di ordini 2, 3 e 4 discutendone autovalori (reali e complessi) e diagonalizzabilità.

8.1.15. Costruire le matrici delle simmetrie ortogonali e delle proiezioni ortogonali di asse o schermo i seguenti sottospazi di \mathbb{R}^3 ed \mathbb{R}^4 :

- (1) $U = \left\langle \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \right\rangle$, $U = \left\langle \begin{pmatrix} 1 \\ -1 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} \right\rangle$,
 (2) $U = \left\langle \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} \right\rangle$, $U = \left\langle \begin{pmatrix} 1 \\ -1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \right\rangle$, $U = \left\langle \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \right\rangle$.

Cos'hanno in comune queste matrici?

8.1.16. Una matrice quadrata reale A è simmetrica se e solo se è ortogonalmente diagonalizzabile (cioè è diagonalizzabile con un cambiamento di base ortogonale, ovvero esiste P con $P^t P = \mathbb{I}$ tale che $P^t A P$ sia diagonale). *Sugg.*: per vedere che ha tutti gli autovalori, si considerino gli autovalori complessi (sia $Av = \alpha v$, dunque $A\bar{v} = \bar{\alpha}\bar{v}$) e si dimostri che sono reali calcolando $\bar{v}^t Av$; poi si mostri che autovalori distinti ($\lambda \neq \mu$ con $Av = \lambda v$ e $Aw = \mu w$) hanno autospazi ortogonali calcolando $(\lambda - \mu)v^t w$; infine si dimostri che le basi degli autospazi danno luogo ad una base di $V_n(\mathbb{R})$, per assurdo completandola altrimenti ad una base ortogonale...

8.1.17. Dire per quali valori di β la matrice $\begin{pmatrix} 1 & 0 & 0 \\ 0 & \beta & \beta \\ 0 & \beta & -\beta \end{pmatrix}$ è ortogonalmente diagonalizzabile. Per quali valori è ortogonale? È sempre vero che una matrice ortogonale è ortogonalmente diagonalizzabile?

8.1.18. Mostrare che le matrici in $M_n(\mathbb{R})$ che sono contemporaneamente ortogonali ed ortogonalmente diagonalizzabili sono tutte e sole le matrici di simmetrie ortogonali (nel senso che asse e direzione della simmetria sono ortogonali tra loro). Per ogni n , dare esempi di matrici ortogonali ma non ortogonalmente diagonalizzabili, e di matrici ortogonalmente diagonalizzabili, ma non ortogonali.

8.1.19. Dire se la matrice $\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix}$ è ortogonalmente diagonalizzabile; studiare autovalori ed autospazi.

8.1.20. Dare un esempio di matrice non simmetrica i cui autospazi siano ortogonali tra loro (attenzione: non può essere una matrice diagonalizzabile: perché?).

8.1.21. Costruire se possibile una matrice simmetrica e una non simmetrica aventi come autospazi (eventualmente generalizzati) i seguenti sottospazi di \mathbb{R}^3 o \mathbb{R}^4 :

- (1) $U = \left\langle \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} \right\rangle$ e $V = \left\langle \begin{pmatrix} 1 \\ 0 \\ -1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \right\rangle$
 (2) $U = \left\langle \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} \right\rangle$ e $V = \left\langle \begin{pmatrix} 1 \\ 0 \\ 2 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \right\rangle$
 (3) $U = \left\langle \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} \right\rangle$ e $V = \left\langle \begin{pmatrix} 1 \\ 0 \\ -1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} \right\rangle$
 (4) $U = \left\langle \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} \right\rangle$ e $V = \left\langle \begin{pmatrix} 1 \\ 0 \\ 2 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} \right\rangle$

8.2. Esercizi su Spazi Euclidei e Rigidità.

8.2.1. Nel piano euclideo $\mathbb{E}^2(\mathbb{R})$ si consideri un triangolo \mathcal{T} .

- (i) Si mostri che le rette che contengono le tre altezze di \mathcal{T} appartengono ad un fascio;
 (ii) Si mostri che gli assi dei lati di \mathcal{T} appartengono ad un fascio (l'asse di un segmento è la retta ortogonale al segmento passante per il suo punto di mezzo);
 (iii) Si mostri che le bisettrici degli angoli interni di \mathcal{T} appartengono ad un fascio;
 (iv) Si mostri che le bisettrici degli angoli esterni di \mathcal{T} intersecano i lati opposti in tre punti allineati.

8.2.2. Nel piano euclideo $\mathbb{E}^2(\mathbb{R})$ si considerino le tre rette r, s, t di equazioni rispettive

$$X + Y - 4 = 0, \quad X + 5Y - 26 = 0, \quad 15X - 27Y - 424 = 0.$$

- (i) Si scrivano le equazioni delle rette n_r, n_s, n_t passanti per l'origine e normali a r, s, t , rispettivamente;
 (ii) Si verifichi che i tre punti $r \cap n_r, s \cap n_s, t \cap n_t$ sono allineati.

8.2.3. Si considerino le rette $r, s \in \mathbb{E}^2(\mathbb{R})$ di equazioni $X + Y - 4 = 0$ e $3X + 2Y = 0$.

- (i) Trovare le bisettrici dei quattro angoli formati da r, s ;
 (ii) Individuare, tra le due, la bisettrice b dell'angolo più piccolo;

- (iii) Per ogni punto $P \in b$, si indichino con P_r e P_s le sue proiezioni ortogonali su r ed s rispettivamente. Si calcoli l'applicazione di r in s che manda P_r in P_s .

8.2.4. Nello spazio euclideo $\mathbb{E}^3(\mathbb{R})$ si considerino la retta r ed il piano α di equazioni rispettive $\frac{X-1}{2} = \frac{Y+1}{3} = \frac{Z-1}{4}$, $X+Y+Z-1=0$. Si trovino delle equazioni cartesiane della proiezione ortogonale di r su α .

8.2.5. Nello spazio euclideo $\mathbb{E}^3(\mathbb{R})$ si considerino le rette r ed s di equazioni rispettive $X-1=Y$, $X+Y=Z$; $X=Z$, $X-Y=2$.

- (i) Trovare la retta n normale ad r ed s ed incidente sia r che s ;
 (ii) Trovare la distanza tra r ed s ;
 (iii) Sia P_z il punto di s la cui terza coordinata è z . Calcolare la distanza di P_z da r , in funzione di z .

8.2.6. Si trovino delle equazioni cartesiane delle rette dello spazio euclideo $\mathbb{E}^3(\mathbb{R})$, che passano per il punto $P = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$, distano $1/\sqrt{2}$ dall'origine, e sono parallele al piano di equazione $X-Y+7=0$.

8.2.7. Determinare le rette contenute nel piano di equazione $37X-12Y+41Z-49=0$, che distano 2 ed 1 rispettivamente dalle rette r ed s di equazioni $X=0$, $Y=2$; $X=3Y=1$.

8.2.8. Nello spazio euclideo $\mathbb{E}^3(\mathbb{R})$ si considerino quattro punti non complanari, a tre a tre non allineati P_1, P_2, P_3, P_4 . Sia $P_i - P_1 = \begin{pmatrix} a_i \\ b_i \\ c_i \end{pmatrix}$, per $i = 2, 3, 4$.

- (i) Si calcoli l'area del triangolo (P_1, P_2, P_3) in funzione di $a_1, b_1, c_1, a_2, b_2, c_2$.
 (ii) Si calcoli il volume del tetraedro (P_1, P_2, P_3, P_4) in funzione delle coordinate dei vettori $P_i - P_1$;
 (iii) Si supponga che sia $P_1 = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$; si trovino le equazioni dei piani luogo dei punti P , tali che $\text{Vol}(P_1, P_2, P_3, P_4) = \text{Vol}(P_1, P_2, P_3, P)$.

8.2.9. Nello spazio euclideo $\mathbb{E}^3(\mathbb{R})$, si considerino le rette $r : \begin{cases} x = 1 + t \\ y = 2 + t \\ z = -1 + 2t \end{cases}$, $s : \begin{cases} x = 2 + 2t \\ y = 3 + t \\ z = 1 + t \end{cases}$.

- (a) Si mostri che r, s sono incidenti e si trovi un'equazione del piano che le contiene.
 (b) Si trovino delle equazioni cartesiane delle rette passanti per $r \cap s$, parallele al piano di equazione $x+y+z=0$, e formanti angoli uguali con r ed s .

8.2.10. Nello spazio euclideo $\mathbb{E}^3(\mathbb{R})$ si considerino le rette di equazioni $r : \begin{cases} x - y = 0 \\ z = 2 \end{cases}$ $s : \begin{cases} x - y + z = 5 \\ 2x - y = 4 \end{cases}$.

- (i) Trovare la retta n normale ad r ed s ed incidente sia r che s ;
 (ii) Trovare la distanza tra r ed s ;
 (iii) Sia P_t il punto di r la cui prima coordinata è t . Calcolare la distanza di P_t da s , in funzione di t ;
 (iv) Si scrivano le equazioni delle proiezioni ortogonali di r, s ed n sul piano passante per l'origine, parallelo ad r e s .

8.2.11. Nello spazio euclideo standard $\mathbb{E}^3(\mathbb{R})$ si considerino i seguenti punti: $P = \begin{pmatrix} -1 \\ -1 \\ 0 \end{pmatrix}$, $Q = \begin{pmatrix} 1 \\ 1 \\ 2 \end{pmatrix}$, $R = \begin{pmatrix} 2 \\ 1 \\ 1 \end{pmatrix}$.

- (a) Si scrivano le equazioni del luogo dei punti S di $\mathbb{E}^3(\mathbb{R})$ tali che il volume del tetraedro (non orientato) (P, Q, R, S) sia $1/\sqrt{6}$.
 (b) Tra i punti S di cui in (a) si trovino quelli la cui proiezione ortogonale sul piano per P, Q, R è il baricentro del triangolo (P, Q, R) .

8.2.12. Nello spazio euclideo $\mathbb{E}^3(\mathbb{R})$ è data la famiglia di rette r_t di equazioni $\begin{cases} X - Y + 2Z = t \\ 2X - 2tY - (1+t)Z = 2 - 4t, \end{cases}$ al variare di t in \mathbb{R} .

- (i) Si mostri che le rette r_t sono a due a due sghembe;
 (ii) Si mostri che esiste una retta n incidente e normale a tutte le rette della famiglia;
 (iii) Si trovi la distanza tra r_0 ed r_1 .

8.2.13. Nello spazio euclideo $\mathbb{E}^3(\mathbb{R})$ si consideri la retta r di equazioni $\begin{cases} x - y + z = 1 \\ 2x + y + z = -1. \end{cases}$

- (a) Si scrivano le equazioni parametriche della retta s passante per l'origine, parallela al piano di equazione $x - y + z = 1$, ed ortogonale ad r .

- (b) Si trovi la distanza tra r ed s .
 (c) Si trovino un punto P su r ed un punto Q su s , tali che la distanza tra P e Q sia uguale alla distanza tra r ed s . Si mostri poi che P e Q sono unici.

8.2.14. Nello spazio euclideo standard $\mathbb{E}^3(\mathbb{R})$ si considerino la retta r di equazioni $\begin{cases} x - y + 2z = 0 \\ 2x - 2y - z = 0 \end{cases}$,

il piano π di equazione $x + 2y + z = 1$ ed il punto P di coordinate $\begin{pmatrix} 2 \\ 1 \\ 1 \end{pmatrix}$.

- (a) Determinare le rette per P , parallele a π e complanari con r ;
 (b) Determinare i piani per P , paralleli a r ed aventi distanza 1 da essa;
 (c) Determinare le rette per P , parallele a π , la cui distanza da r coincide con la distanza di P da r .

8.2.15. Nello spazio euclideo standard $\mathbb{E}^2(\mathbb{R})$ si considerino le rette r, s, t con le seguenti equazioni:

$$r : \begin{cases} x + 3y + z = 0 \\ x + y - z = 2 \end{cases}, \quad s : \begin{cases} y + 2z = -1 \\ z = 0 \end{cases}, \quad t : \begin{cases} 3x - y - z = 1 \\ x + y - z = -1 \end{cases}.$$

- (i) Si mostri che s incide sia r che t ;
 (ii) si ponga $T = t \cap s$ e si mostri che T è il punto di t che ha distanza minima da r ;
 (iii) siano R' il punto di r che ha distanza minima da t e $R = r \cap s$; determinare l'area del triangolo di vertici R, R', T .

8.2.16. Nello spazio euclideo standard $\mathbb{E}^3(\mathbb{R})$, ove è stato fissato il riferimento canonico, si considerino le rette r ed s di equazioni $\begin{cases} X + Y - Z = 0 \\ 2X - Y + Z = 0 \end{cases}$ e $\begin{cases} 3X - 2Y - 2Z = 0 \\ X - Y - 3Z = 2 \end{cases}$.

- (i) Si verifichi che r ed s sono sghembe.
 (ii) Si trovi la distanza d di r da s .
 (iii) Si trovi un punto P , tale che le sue distanze da r ed s siano $d/2$.

8.2.17. Nello spazio euclideo $\mathbb{E}^3(\mathbb{R})$ con riferimento canonico, si considerino le rette r, s di equazioni cartesiane $r : \begin{cases} x - y + z = 1 \\ x - 2z = 1 \end{cases}$, $s : \begin{cases} x - y = -1 \\ x - z = 1 \end{cases}$.

- (a) Si trovino delle equazioni cartesiane di tutte le rette complanari con r ed s ed incidenti l'asse z ;
 (b) Si indichi con r_k la retta della famiglia di cui al punto (a) che passa per il punto di coordinate $(0, 0, k)$; si chiede se esistono dei k per i quali r_k sia ortogonale ad uno degli assi coordinati.

8.2.18. Nello spazio euclideo \mathbb{R}^4 , si considerino i piani $\sigma_1 : \begin{cases} x_1 - x_3 = 2 \\ x_2 + 2x_4 = -1 \end{cases}$, $\sigma_2 : \begin{cases} x_1 + 2x_4 = 0 \\ x_2 + x_3 = 1 \end{cases}$

e la retta $r : \begin{cases} x_1 + x_2 + x_3 = 1 \\ x_2 - x_3 = -1 \\ x_1 + 2x_2 - 2x_4 = 0 \end{cases}$.

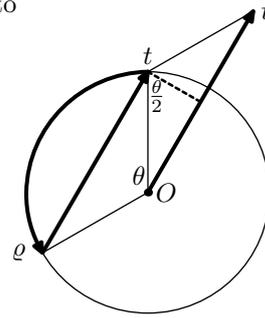
- (a) Si mostri che σ_1 e σ_2 hanno in comune un unico punto P e si determinino le coordinate di tale punto.
 (b) Si mostri che la retta r interseca entrambi i piani e si determinino le coordinate dei punti $Q_1 = r \cap \sigma_1$ e $Q_2 = r \cap \sigma_2$.
 (c) Si determinino il baricentro G e l'area del triangolo PQ_1Q_2 .
 (d) Si scrivano le equazioni cartesiane del piano π , passante per G e perpendicolare al piano contenente il triangolo PQ_1Q_2 .

8.2.19. Nello spazio euclideo tridimensionale si consideri la retta r per $P = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}$, e direzione $v = \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}$.

- (a) si scriva l'equazione cartesiana del cilindro \mathcal{C} formato dai punti che distano 1 da r .
 (b) Si determinino i punti di intersezione di \mathcal{C} con i tre assi coordinati.
 (c) Si calcoli il volume del tetraedro definito dai punti trovati in (b).

8.2.20.

- (1) Si mostri che ogni isometria $\varphi : \mathbb{E}_{\mathbb{R}}^2 \rightarrow \mathbb{E}_{\mathbb{R}}^2$ che conserva l'orientamento è una traslazione o una rotazione (attorno ad un punto).
- (2) Si mostri che ogni rotazione ϱ di $\mathbb{E}_{\mathbb{R}}^2$ è decomponibile nel prodotto $\varrho = t \circ \varrho_0 = \varrho_0 \circ t'$, ove ϱ_0 è una rotazione attorno all'origine, e t e t' sono traslazioni.
- (3) Si determini il centro di ϱ in funzione di t e ϱ_0 .
- (4) Determinare il centro di ϱ con una costruzione grafica e verificare che i risultati coincidono con quelli trovati precedentemente.



8.2.21. Determinare centro e angolo della rotazione di $\mathbb{E}_{\mathbb{R}}^2$ avente matrice $\begin{pmatrix} 1 & 0 & 0 \\ 1 & 1/2 & -\sqrt{3}/2 \\ 2 & \sqrt{3}/2 & 1/2 \end{pmatrix}$.

8.2.22. Trovare la matrice della rotazione di $\mathbb{E}_{\mathbb{R}}^2$ di centro $(1, 1)$ e angolo $-\pi/4$.

8.2.23.

- (1) Sia $\varphi : \mathbb{E}_{\mathbb{R}}^3 \rightarrow \mathbb{E}_{\mathbb{R}}^3$ una rotazione (attorno ad un asse r); trovare delle condizioni necessarie e sufficienti affinché $t \circ \varphi$ sia ancora una rotazione (ove t è una traslazione).
- (2) Mostrare che ogni isometria di $\mathbb{E}_{\mathbb{R}}^3$ in sè che conserva l'orientamento è del tipo $t \circ \varrho$ ove ϱ è una rotazione e t è una traslazione parallela all'asse di ϱ . È vero che t e ϱ commutano tra loro?
- (3) descrivere con un disegno la traiettoria del punto $(1, 0, 0)$ sotto l'azione di $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \cos \vartheta & -\sin \vartheta & 0 \\ 0 & \sin \vartheta & \cos \vartheta & 0 \\ \vartheta & 0 & 0 & 1 \end{pmatrix}$ al variare di $\vartheta \in \mathbb{R}$.

8.2.24. Studiare la isometria di matrice $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 0 & -1 & 0 \\ -1 & 0 & 0 & 1 \\ -1 & -1 & 0 & 0 \end{pmatrix}$.

8.2.25. Sia φ la isometria di $\mathbb{E}_{\mathbb{R}}^3$ data dalla composizione della rotazione di angolo $\pi/2$ e asse la retta per $P(1, -1, 0)$ e direzione $(1, 1, 0)$ con la traslazione di vettore $(1, 1, 1)$.

- (1) vero che φ è una rotazione?
- (2) si calcoli la matrice di φ nel riferimento dato.
- (3) scrivere φ come composizione di una rotazione (in particolare determinare l'asse) seguita da una traslazione parallela all'asse.

8.2.26. La simmetria di $\mathbb{E}_{\mathbb{R}}^3$ di asse una retta r e direzione ortogonale è una isometria che conserva l'orientamento? È vero che si tratta di una rotazione?

Normalmente si dice che "lo specchio scambia la (mano) sinistra con la destra". Che senso ha?

Le composizioni di due riflessioni speculari (simmetrie rispetto ad un piano nella direzione ortogonale al piano) conservano l'orientamento di $\mathbb{E}_{\mathbb{R}}^3$. Di che isometrie si tratta?

8.2.27. Due rette r, s di $\mathbb{E}_{\mathbb{R}}^3$ si specchiano sul piano $\pi : x + y + z = 1$. La prima retta ha equazioni $x - 3y = 3$ e $2y - z = 2$, mentre la riflessione della seconda è $\sigma(s) : (1, -1, 1) + \langle (0, 1, -1) \rangle$.

- (1) r ed s si incontrano?
- (2) $\sigma(r)$ ed s si intersecano?
eventualmente trovare i punti di intersezione.

8.2.28. Una isometria φ di $\mathbb{E}^3(\mathbb{R})$ si rappresenta tramite la matrice $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1/2 & 0 & -\sqrt{3}/2 \\ 1 & 0 & 1 & 0 \\ 1 & \sqrt{3}/2 & 0 & 1/2 \end{pmatrix}$ nel riferimento canonico.

- (i) dire se è una isometria diretta;
- (ii) dire se è una rotazione (di asse una retta);
- (iii) scrivere φ come composizione di una rotazione ϱ seguita da una traslazione τ di direzione parallela all'asse di rotazione ($\varphi = \tau \circ \varrho$); in particolare si determini una espressione cartesiana per l'asse della rotazione ϱ .
- (iv) è vero che τ e ϱ commutano tra di loro? È vero che φ si può scrivere anche come composizione $\varrho \circ \tau'$ ove τ' è una traslazione di direzione parallela all'asse di ϱ ?

8.2.29. Come il precedente esercizio, usando la matrice $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 2 & 0 & 0 & -1 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \end{pmatrix}$

8.2.30. Una isometria φ di $\mathbb{E}^3(\mathbb{R})$ si rappresenta tramite la matrice $\begin{pmatrix} 1 & 0 & 0 \\ 2 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$ nel riferimento canonico.

- (i) dire se è una isometria diretta;
- (ii) dire se è una rotazione (di asse una retta);
- (iii) scrivere φ come composizione di una rotazione ϱ seguita da una traslazione τ di direzione parallela all'asse di rotazione ($\varphi = \tau \circ \varrho$); in particolare si determini una espressione cartesiana per l'asse della rotazione ϱ .
- (iv) è vero che τ e ϱ commutano tra di loro? È vero che φ si può scrivere anche come composizione $\varrho \circ \tau'$ ove τ' è una traslazione di direzione parallela all'asse di ϱ ?

