



SAPIENZA
UNIVERSITÀ DI ROMA

UNIVERSITÀ "SAPIENZA" DI ROMA
FACOLTÀ DI INFORMATICA

Algebra

Appunti integrati con il libro "Geometria analitica con elementi di Algebra lineare", M. Abate, C. De Fabritiis

Author
Simone Bianco

15 febbraio 2023

Indice

0	Introduzione	1
1	Strutture algebriche principali	2
1.1	Richiami di insiemistica	2
1.2	Operazioni binarie, Assiomi e Proprietà	4
1.3	Semigrupperi, Monoidi e Gruppi	6
1.4	Anelli e Campi	7
1.5	Sottogruppi ed Ideali	9
2	Numeri Complessi	12
2.1	Il campo dei numeri complessi	13
2.2	Forma polare dei numeri complessi	15
2.3	Teorema fondamentale dell'algebra	17
3	Relazioni e Induzione	19
3.1	Classi di equivalenza	21
3.2	Relazione di Divisore	24
3.3	Relazione di Congruenza	25
3.4	Teorema della divisione con resto euclidea	26
3.5	Relazione di Coniugio	27
3.6	Induzione matematica	28
4	Elementi di Teoria degli Anelli	31
4.1	Insieme quoziente	31
4.1.1	Classi laterali sinistre	31
4.1.2	Teorema di Lagrange	33
4.2	L'anello commutativo \mathbb{Z}_n	34
4.3	Invertibili e Divisori dello zero	36
4.4	Elementi irriducibili e primi	39
4.5	Massimo comun divisore	42
4.5.1	Algoritmo di Euclide	45
4.5.2	Approfondimento sull'Identità di Bezout	49
4.5.3	Criteri di divisibilità	50
4.6	Minimo comune multiplo	51
4.6.1	Teorema fondamentale dell'aritmetica	52
4.7	Teorema cinese dei resti	54
4.8	Piccolo teorema di Fermat	60
4.9	Ordine di un elemento di un gruppo	63

5	Gruppo Simmetrico	70
5.1	Ordine di una permutazione	73
5.2	Segno delle permutazioni	76
6	Morfismi	83
6.1	Isomorfismi, Endomorfismi ed Automorfismi	84
6.2	Nucleo ed Immagine di un morfismo	87
6.3	Teorema fondamentale di isomorfismo	88
6.4	Sottogruppi normali	90
6.5	Gruppi diedrali	97
6.6	Gruppo di Klein e Teorema di Cauchy	101
7	Polinomi	105
7.1	Divisione con resto di polinomi	107
7.1.1	Regola di Ruffini	109
7.2	Proprietà dell'anello polinomiale	111
7.3	Polinomi in \mathbb{Z}_p	118
8	Spazi vettoriali	121
8.1	Span e Base di uno spazio	123
8.2	Trasformazioni lineari	128
8.2.1	Teorema del Rango e Formula di Grassman	131
8.3	Spazi affini, Sottospazi affini e Giacitura	135
8.4	Prodotto scalare	136
9	Matrici	138
9.1	Prodotto tra matrici	140
9.2	Rango di una matrice	141
9.2.1	Riduzione a scala di una matrice	143
9.3	Teorema di Rouché-Capelli	146
9.3.1	Equazioni parametriche	149
9.4	Matrice di una trasformazione lineare	151
9.5	Determinante di una matrice	154
9.5.1	Formula di Leibniz e Regola di Sarrus	155
9.5.2	Determinante tramite riduzione a scala	157
9.5.3	Sviluppo di Laplace	159
9.5.4	Regola di Cramer	161
9.6	Inversa di una matrice	162
9.7	Teorema degli orlati	167
9.8	Matrici simili	173
9.8.1	Invarianti per similitudine	174
9.8.2	Diagonalizzazione di una matrice	179
9.9	Matrici ortogonali	184

Capitolo 0

Introduzione

Il seguente corso mira all'apprendimento dei principali elementi di Algebra Elementare, Algebra Lineare e Teoria dei Gruppi, incentrandosi principalmente su:

- **Insiemi**, partizioni, applicazioni, **relazioni** d'equivalenza e d'ordine, permutazioni. I numeri naturali e il **principio di induzione**. Il teorema binomiale.
- **Strutture algebriche**: Gruppi, anelli e campi, reticoli, sottostrutture, omomorfismi. Anelli di polinomi. L'algoritmo di Euclide. Classi resto modulo un intero. Congruenze ed equazioni in \mathbb{Z}/n . Il teorema di Eulero-Fermat.
- **Sistemi di equazioni lineari**: algoritmo di Gauss, determinante di una matrice quadrata. Matrice inversa. Rango di una matrice: Il teorema di Cramer ed il teorema di Rouché-Capelli. Risoluzione di sistemi lineari omogenei.
- **Spazi vettoriali**: dipendenza e indipendenza lineare, basi. Matrici. Applicazioni lineari e loro rappresentazione: cambiamenti di base, diagonalizzazione di un operatore lineare. Polinomio caratteristico e relativa invarianza.
- **Elementi di teoria dei gruppi**: Gruppi ciclici, periodo di un elemento di un gruppo. Classificazione dei gruppi ciclici. Classi laterali modulo un sottogruppo. Il teorema di Lagrange e le sue conseguenze, sottogruppi normali. Il teorema fondamentale di omomorfismo tra gruppi.

Prima di approcciarsi al seguente corso, è consigliato avere una conoscenza sufficiente dei concetti espressi nel corso di *Metodi Matematici per l'Informatica*.

Capitolo 1

Strutture algebriche principali

1.1 Richiami di insiemistica

Definiamo **insieme** una collezione di elementi su cui vengono svolte delle **operazioni algebriche**.

$$S : \{1, 2, 3, 4, \dots\}$$

In questo corso tratteremo molto le proprietà e le operazioni applicabili sulle varie **strutture algebriche** rappresentate tramite insiemi, pertanto effettuiamo un breve ripasso di **teoria degli insiemi**:

- Dati due insiemi A, B , definiamo l'**insieme unione** $A \cup B$ come l'insieme dove

$$A \cup B : \{x \in A \vee x \in B\}$$

- Definiamo invece come **insieme intersezione** $A \cap B$ l'insieme dove

$$A \cap B : \{x \in A \wedge x \in B\}$$

- Considerato un insieme B , affermiamo che l'insieme B è **sottoinsieme** dell'insieme A (denotato come $B \subseteq A$) se si verifica che

$$B \subseteq A \iff x \in B \implies x \in A$$

- Considerato un insieme X e un insieme A tale che $A \subseteq X$, denotiamo l'**insieme complementare** di A su X come

$$X - A = \{x \in X \mid x \notin A\}$$

- La **legge di De Morgan** afferma che

$$X - (A \cup B) = (X - A) \cap (X - B)$$

$$X - (A \cap B) = (X - A) \cup (X - B)$$

- Dato un insieme di partenza detto **dominio** ed un insieme di arrivo detto **codominio**, definiamo come **funzione** la relazione che associa ogni elemento del dominio ad un elemento del codominio

$$f : X \rightarrow Y : x \mapsto y$$

- Definiamo come **immagine della funzione** l'insieme di tutti gli elementi del codominio raggiungibili da un elemento del dominio

$$Im(f) = \{y \in Y \mid f(x) = y, \exists x \in X\}$$

- Una funzione viene detta **iniettiva** se ogni elemento del dominio è associato ad un elemento diverso del codominio

$$\text{Iniettività} : \forall x_1, x_2 \in X \mid x_1 \neq x_2 \implies f(x_1) \neq f(x_2)$$

- Una funzione viene detta **suriettiva** se ogni elemento del codominio è raggiungibile da almeno un elemento del dominio

$$\text{Suriettività} : \forall y \in Y, \exists x \in X \mid f(x) = y$$

In alternativa, potremmo affermare che una funzione è suriettiva se la sua immagine coincide con il suo codominio

$$\text{Suriettività} : Im(f) = Y$$

- Una funzione viene detta **biettiva** (o biunivoca) se è sia iniettiva sia suriettiva. Se esiste una funzione biettiva tra due insiemi X ed Y , allora tali insiemi possiedono la **stessa cardinalità**

$$\exists f : X \rightarrow Y \mid f \text{ è biettiva} \implies |X| = |Y|$$

- Definiamo come **prodotto cartesiano** di due insiemi X e Y l'insieme contenente tutte le coppie (x, y) dove $x \in X$ e $y \in Y$

$$X \times Y : \{(x, y) \mid x \in X, y \in Y\}$$

- Date due funzioni f, g , la loro **funzione composta** è una funzione che associa un elemento del dominio di f ad un elemento del codominio di g

$$f : X \rightarrow Y : x \mapsto f(x)$$

$$g : Y \rightarrow Z : x \mapsto g(x)$$

$$g \circ f : X \rightarrow Z : x \mapsto g(f(x)) : x \mapsto (g \circ f)(x)$$

1.2 Operazioni binarie, Assiomi e Proprietà

Definition 1. Operazione binaria

Dato un insieme S , definiamo **operazione binaria** una funzione che manda ogni coppia di elementi appartenenti ad S in S stesso.

Tale proprietà viene anche detta **assioma di chiusura**.

$$m : S \times S \rightarrow S : (x, y) \mapsto m(x, y)$$

Attenzione: per comodità di scrittura, d'ora in poi indicheremo l'applicazione di un'operazione binaria generica $m(x, y)$ come xy .

Tuttavia, tale scrittura non corrisponde all'operazione prodotto (a meno che non sia specificato), bensì corrisponde ad un semplice "segnaposto" per una qualsiasi operazione binaria.

Esempio:

- Sull'insieme \mathbb{R} l'**operazione additiva**, indicata come

$$+ : \mathbb{R} \times \mathbb{R} \rightarrow \mathbb{R} : (x, y) \mapsto x + y$$

e l'**operazione moltiplicativa**, indicata come

$$\cdot : \mathbb{R} \times \mathbb{R} \rightarrow \mathbb{R} : (x, y) \mapsto xy$$

sono entrambe operazioni binarie

- Sull'insieme $X = \{f : A \rightarrow A : a \mapsto a\}$ la **composizione tra funzioni** corrisponde ad un'operazione binaria:

$$\circ : X \times X \rightarrow X : (g, f) \mapsto g \circ f$$

Definition 2. Assioma di Associatività

Data un'operazione binaria $m : S \times S \rightarrow S$, tale operazione rispetta l'**assioma di associatività** se l'ordine di applicazione di tale operazione binaria non influenza il risultato:

$$x(yz) = (xy)z = xyz, \forall x, y, z \in S$$

Esempi:

- Operazione additiva: $(x + y) + z = x + (y + z) = x + y + z, \forall x, y, z \in S$
- Operazione prodotto: $(xy)z = x(yz) = xyz, \forall x, y, z \in S$

Definition 3. Assioma di esistenza dell'Elemento neutro

Data un'operazione binaria $m : S \times S \rightarrow S$, tale operazione rispetta l'**assioma di esistenza dell'elemento neutro** se esiste un unico elemento $e \in S$, detto neutro, tale che:

$$xe = ex = x, \forall x \in S$$

Dimostrazione unicità:

- Supponiamo che

$$\exists e_1, e_2 \in S \mid e_1x = xe_1 = x \wedge e_2x = xe_2 = x, \forall x \in S$$

- Di conseguenza, si ha che

$$e_1 = e_1e_2 = e_2e_1 = e_2 \iff e_1 = e_2$$

□

Esempi:

- Operazione additiva: $x + 0 = x, \forall x \in S$
- Operazione prodotto: $x \cdot 1 = x, \forall x \in S$

Definition 4. Assioma di esistenza dell'Elemento inverso

Data un'operazione binaria $m : S \times S \rightarrow S$, tale operazione rispetta l'**assioma di esistenza dell'elemento inverso** se esiste un unico elemento $x^{-1} \in S$, detto inverso, tale che:

$$xx^{-1} = x^{-1}x = e, \forall x \in S$$

Attenzione: con la scrittura x^{-1} indichiamo l'elemento inverso di x rispetto all'operazione binaria definita, non il "classico" inverso del prodotto (ossia $\frac{1}{x}$)

Dimostrazione unicità:

- Supponiamo che

$$\exists x_1^{-1}, x_2^{-1} \in S \mid xx_1^{-1} = x_1^{-1}x = e \wedge xx_2^{-1} = x_2^{-1}x = e, \forall x \in S$$

- Di conseguenza, si ha che

$$x_1^{-1}x = e = x_2^{-1}x \iff x_1^{-1}x = x_2^{-1}x \iff x_1^{-1} = x_2^{-1}$$

□

Esempi:

- Operazione additiva: $x + (-x) = 0, \forall x \in S$
- Operazione prodotto: $x \cdot \frac{1}{x} = 1, \forall x \in S$

Definition 5. Assioma di Commutatività

Data un'operazione binaria $m : S \times S \rightarrow S$, tale operazione rispetta l'**assioma di commutatività** se l'ordine degli elementi su cui viene applicata tale operazione non influenza il risultato:

$$xy = yx \forall x, y \in S$$

Esempi:

- Operazione additiva: $x + y = y + x, \forall x \in S$
- Operazione prodotto: $xy = yx, \forall x \in S$

1.3 Semigrupperi, Monoidi e Gruppi

Una volta definiti i quattro assiomi principali delle operazioni binarie, possiamo definire le seguenti quattro **strutture algebriche**:

Definition 6. Strutture algebriche semplici

Data la coppia (S, m) dove S è un **insieme** e m l'**operazione binaria** applicata su di esso, diciamo che tale **struttura algebrica** è un:

- Un **semigruppero** se vale l'assioma di associatività
- Un **monoide** se valgono gli assiomi di d'associatività e di elemento neutro
- Un **gruppo** se valgono gli assiomi di associatività, elemento neutro e elemento inverso
- Un **gruppo abeliano** (o commutativo) se valgono gli assiomi di associatività, elemento neutro, elemento inverso e commutatività

Esempi:

- $(\mathbb{N} - \{0\}, +)$ è un **semigruppero**
- $(\mathbb{N}, +)$ è un **monoide** commutativo
- (\mathbb{Q}, \div) è un **gruppo**
- (\mathbb{Z}, \cdot) è un **monoide** commutativo
- Dati due insiemi X, Y , denotiamo con Y^X l'insieme composto da tutte le funzioni da X in Y

$$Y^X : \{f : X \rightarrow Y\}$$

Allora, la coppia (X^X, \circ) è un monoide, poiché si ha:

– **Associatività:**

$$f, g, h \in X^X \implies h \circ (g \circ f) = (h \circ g) \circ f$$

– **Elemento neutro:**

$$\exists \text{id} \in X^X \mid \forall f \in X^X, f \circ \text{id} = \text{id} \circ f = f$$

dove id è la funzione identità, ossia $\text{id}(x) = x, \forall x \in X$.

1.4 Anelli e Campi

Definition 7. Anello

Date le due operazioni binarie di somma e prodotto, definite come:

$$+ : A \times A \rightarrow A : (x, y) \mapsto xy$$

$$\cdot : A \times A \rightarrow A : (x, y) \mapsto x + y$$

Definiamo una struttura algebrica $(A, +, \cdot)$ come **anello** se:

- $(A, +)$ è un **gruppo abeliano**
- (A, \cdot) è un **monoide**
- Vale la **relazione distributiva**, definita come:

$$a(b + c) = ab + ac, \forall a, b, c \in A$$

$$(b + c)a = ba + ca, \forall a, b, c \in A$$

Inoltre, definiamo tale struttura come **anello commutativo** se nella coppia (A, \cdot) vale anche l'assioma **commutativo**:

$$ab = ba, \forall a, b \in A$$

Observation 1

Sia $(A, +, \cdot)$ un anello. Dato l'elemento neutro della somma $0 \in A$, si ha che:

$$a \cdot 0 = 0, \forall a \in A$$

Dimostrazione:

- Dato un elemento $a \in A$ si ha che:

$$a = a \cdot 1 = a \cdot (0 + 1) = a \cdot 0 + a \cdot 1 = a \cdot 0 + a \iff$$

$$\iff a = a \cdot 0 + a \iff a + (-a) = a \cdot 0 + a + (-a) \iff 0 = a \cdot 0$$

□

Observation 2

Sia $(A, +, \cdot)$ un anello. Dati due elementi $x, y \in A$, si ha che:

$$(xy)^{-1} = y^{-1}x^{-1}, \forall a \in A$$

Dimostrazione:

- Dati due elementi $x, y \in A$ si ha che:

$$\begin{aligned} (xy)^{-1}(xy) = 1 &\iff (xy)^{-1}xy = 1 \iff (xy)^{-1}xyy^{-1} = y^{-1} \iff \\ &\iff (xy)^{-1}x = y^{-1} \iff (xy)^{-1}xx^{-1} = y^{-1}x^{-1} \iff (xy)^{-1} = 1y^{-1}x^{-1} \end{aligned}$$

□

Corollary 1

Sia $(A, +, \cdot)$ un anello commutativo. Dati due elementi $x, y \in A$, si ha che:

$$(xy)^{-1} = y^{-1}x^{-1} = x^{-1}y^{-1}, \forall a \in A$$

Definition 8. Campo

Definiamo una struttura algebrica $(K, +, \cdot)$ come **campo** se:

- $(K, +, \cdot)$ è un **anello commutativo**
- $(K - \{0\}, \cdot)$ ammette l'assioma di **elemento inverso**, ossia se:

$$\forall a \in K - \{0\}, \exists a^{-1} \in K \mid a \cdot a^{-1} = 1$$

In un campo, sostanzialmente, si ha che anche $(K - \{0\}, \cdot)$ è un gruppo abeliano

Esempi:

- $(\mathbb{Z}, +, \cdot)$ è un **anello commutativo**
- $(\mathbb{Q}, +, \cdot)$ è un **campo**
- $(\mathbb{R}, +, \cdot)$ è un **campo**

1.5 Sottogruppi ed Ideali

Definition 9. Sottogruppo

Sia G un gruppo. Definiamo H come **sottogruppo** di G , indicato come $H \leq G$, se:

- $e \in H$, dove e è l'elemento neutro di G
- $x, y \in H \implies xy \in H$
- $x \in H \implies x^{-1} \in H$

Attenzione: ricordiamo che con \cdot intendiamo una qualsiasi operazione binaria

Esempi:

- $(\mathbb{Z}, +) \leq (\mathbb{Q}, +) \leq (\mathbb{R}, +) \leq (\mathbb{C}, +)$
- $(\mathbb{Z} - \{0\}, \cdot) \not\leq (\mathbb{Q} - \{0\}, \cdot) \leq (\mathbb{R} - \{0\}, \cdot)$

Definition 10. Ideale

Sia A un anello commutativo. Definiamo I come **ideale** di A , se si verifica che:

- $(I, +) \leq (A, +)$
- $x \in I, a \in A \implies ax = xa \in I$ ossia se $AI = IA \subseteq I$

dove $AI : \{ax \mid x \in I, a \in A\}$ e $IA : \{xa \mid x \in I, a \in A\}$

Esempio:

- Sia $I(a_1, \dots, a_n) : \{a_1b_1 + \dots + a_nb_n \mid b_1, \dots, b_n \in A\}$ dove A è anello commutativo e siano $a_1, \dots, a_n \in A$. Verifichiamo che $I(a_1, \dots, a_n) \leq A$ sia un ideale di A :

– Verifichiamo che l'elemento neutro della somma sia in $I(a_1, \dots, a_n)$:

$$0 = a_1 \cdot 0 + \dots + a_n \cdot 0 \in I(a_1, \dots, a_n)$$

– Verifichiamo che $I(a_1, \dots, a_n)$ sia chiuso rispetto alla somma:

$$\begin{aligned} x, y \in I(a_1, \dots, a_n) &\iff x = a_1b_1 + \dots + a_nb_n, y = a_1c_1 + \dots + a_nc_n \iff \\ &\iff x + y = a_1(b_1 + c_1) + \dots + a_n(b_n + c_n) \implies x + y \in I(a_1, \dots, a_n) \end{aligned}$$

– Verifichiamo che $I(a_1, \dots, a_n)$ sia chiuso rispetto agli inversi della somma:

$$\begin{aligned} x \in I(a_1, \dots, a_n) &\iff x = a_1b_1 + \dots + a_nb_n \iff \\ &\iff -x = -a_1b_1 - \dots - a_nb_n = a_1(-b_1) - \dots - a_n(-b_n) \implies -x \in I(a_1, \dots, a_n) \end{aligned}$$

– Verifichiamo che $I(a_1, \dots, a_n)$ sia chiuso rispetto al prodotto:

$$\begin{aligned} x \in I(a_1, \dots, a_n) &\iff x = a_1b_1 + \dots + a_nb_n \implies c \in A \mid cx = c(a_1b_1 + \dots + a_nb_n) \\ &\implies cx = c(a_1b_1 + \dots + a_nb_n) = a_1(b_1c) + \dots + a_n(b_nc) \implies cx \in I(a_1, \dots, a_n) \end{aligned}$$

Definition 11. Ideale principale

Sia A un anello commutativo. Dato $I(a) = \{ax \mid x \in A\} \subseteq A$ come **ideale principale** generato da a di A

Proposition 1. Somma tra ideali

Dato un anello commutativo A e due suoi ideali $I, J \leq A$, la loro somma corrisponde a:

$$I + J : \{i + j \mid i \in I, j \in J\}$$

inoltre, $I + J \leq A$ è un ideale

Dimostrazione:

- $I + J \leq A$ poiché:

$$- 0 \in I, 0 \in J \implies 0 = 0 + 0 \in I + J$$

$$- x, y \in I + J \iff x + y = (i_1 + j_1) + (i_2 + j_2) = (i_1 + i_2) + (j_1 + j_2) \implies x + y \in I + J$$

$$- x = i + j \in I + J \iff -x = -(i + j) = (-i) + (-j), -i \in I, -j \in J \implies -x \in I + J$$

- $a \in A, x \in I + J \implies ax \in I + J$, poiché:

$$a \in A \mid ai \in I, aj \in J \implies ai + aj = a(i + j) \in I + J$$

□

Proposition 2. Intersezioni tra ideali

Dato un anello commutativo A e due suoi ideali $I, J \leq A$, la loro intersezione corrisponde a:

$$I \cap J : \{h \mid h \in I \wedge h \in J\}$$

inoltre, $I \cap J \leq A$ è un ideale

Dimostrazione:

- $I \cap J \leq A$ poiché:

$$- 0 \in I \wedge 0 \in J \implies 0 \in I \cap J$$

$$- x, y \in I \cap J \implies x, y \in I \wedge x, y \in J \implies x + y \in I \wedge x + y \in J \implies x + y \in I \cap J$$

$$- x \in I \wedge x \in J \implies -x \in I \wedge -x \in J \implies -x \in I \cap J$$

- $a \in A, x \in I \cap J \implies ax \in I \cap J$, poiché:

$$a \in A, x \in I \cap J \implies ax \in I \wedge ax \in J \implies ax \in I \cap J$$

□

Proposition 3. Prodotto tra ideali

Dato un anello commutativo A e due suoi ideali $I, J \leq A$, la loro prodotto corrisponde a:

$$I \cdot J : \{i_1 j_1 + i_2 j_2 + \dots + i_n j_n \mid i_k \in I, j_h \in J\}$$

inoltre, $I \cdot J \leq A$ è un ideale

Dimostrazione:

- $I \cdot J \leq A$, poiché:

$$- 0 \in I \wedge 0 \in J \implies 0 = 0 + 0 \in I \cdot J$$

$$- x = i_1 j_1 + i_2 j_2 + \dots + i_n j_n \in I \cdot J, y = i'_1 j'_1 + i'_2 j'_2 + \dots + i'_n j'_n \in I \cdot J \implies \\ x + y = i_1 j_1 + i'_1 j'_1 + \dots + i_n j_n + i'_n j'_n \in I \cdot J$$

$$- x \in I \cdot J \implies -x = x = (-i_1)j_1 + (-i_2)j_2 + \dots + (-i_n)j_n \mid -i_k \in I, j_h \in J \implies -x \in I \cdot J$$

- $a \in A, x \in I \cdot J \implies ax \in I \cdot J$, poiché:

$$a \in A, x \in I \cdot J \implies ax = (ai_1)j_1 + (ai_2)j_2 + \dots + (ai_n)j_n \implies ax \in I \cdot J$$

□

Capitolo 2

Numeri Complessi

Introduciamo il simbolo i con cui indichiamo l'**unità immaginaria**, avente la seguente proprietà: $i^2 = -1$. Definiamo l'insieme dei **numeri complessi** come

$$\mathbb{C} : \{a + ib \mid a, b \in \mathbb{R}\}$$

ossia l'insieme delle espressioni $z = a + ib$ composte dalla somma di una **parte reale**, indicata con $Re(z) = a$, ed una **parte immaginaria**, indicata con $Im(z) = b$.

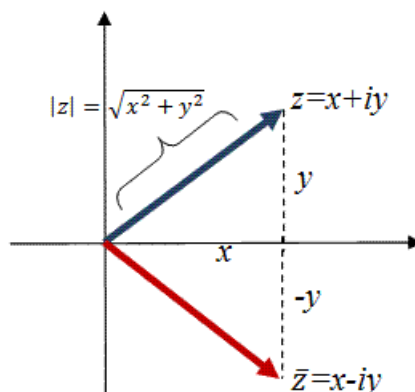
Ovviamente, da tale definizione di insieme dei numeri complessi ne segue che $\mathbb{R} \subseteq \mathbb{C}$, poiché $\forall a \in \mathbb{R} \implies \exists z \in \mathbb{C} \mid z = a + i \cdot 0 = a$. Inoltre, definiamo un **numero immaginario puro** come un numero nella forma $z \in \mathbb{C} \mid z = 0 + i \cdot b = ib$.

Definition 12. Coniugato di un numero complesso

Definiamo come **coniugato di** z (indicato come $\bar{z} \in \mathbb{C}$) il numero complesso avente come parte immaginaria il valore inverso della parte immaginaria di z :

$$\forall z \in \mathbb{C}, \exists \bar{z} \in \mathbb{C} \mid Im(\bar{z}) = -Im(z) \implies z = a + ib, \bar{z} = a - ib$$

Poiché un numero complesso è determinato da una **coppia di valori** $a, b \in \mathbb{R} \mid z \in \mathbb{C}, z = a + ib$, possiamo rappresentare tale numero graficamente attraverso il **piano di Gauss**, avente come ascisse la **parte reale** dei numeri complessi e come ordinate la **parte immaginaria**.



Per tale motivo, dato un elemento $z \in \mathbb{C}$, definiamo come suo **valore assoluto** il numero reale corrispondente alla distanza di z stesso dall'origine, facilmente ricavabile attraverso il **teorema di Pitagora**:

$$|z| = \sqrt{a^2 + b^2}$$

Observation 3

Dati $z, w \in \mathbb{C} \mid z = a + ib, w = c + id$, la **somma dei loro coniugati** equivale al **coniugato della loro somma**

$$\bar{z} + \bar{w} = a - ib + c - id = (a + c) - i(b + d) = \overline{z + w}$$

Dati $z, w \in \mathbb{C} \mid z = a + ib, w = c + id$, il **prodotto dei loro coniugati** equivale al **coniugato del loro prodotto**

$$\bar{z} \cdot \bar{w} = (a - ib)(c - id) = (ac - bd) - i(ad + bc) = \overline{zw}$$

Dato $z \in \mathbb{C}$, il **prodotto** tra esso e il suo **coniugato** corrisponde al **quadrato del valore assoluto** di z

$$z \cdot \bar{z} = (a + ib)(a - ib) = a^2 - (ib)^2 = a^2 + b^2 = |z|^2$$

2.1 Il campo dei numeri complessi

Proposition 4

Dato insieme dei numeri complessi \mathbb{C} , si ha che $(\mathbb{C}, +, \cdot)$ è un **campo**

Dimostrazione:

- Le operazioni binarie di somma e prodotto sono ben definite:

$$z, w \in \mathbb{C} \implies z + w = (a + ib) + (c + id) = (a + c) + i(b + d) \implies z + w \in \mathbb{C}$$

$$z, w \in \mathbb{C} \implies zw = (a + ib)(c + id) = (ac - bd) + i(ad + bc) \implies zw \in \mathbb{C}$$

- Per costruzione di \cdot e $+$, vale la **relazione distributiva**:

$$\forall z, w, q \in \mathbb{C} \mid z(w + q) = zw + zq$$

- È un gruppo abeliano nella somma:

– **Associatività della somma**

$$\begin{aligned} z := a + bi, w := c + di, q := e + fi \in \mathbb{C} &\implies (z + w) + q = (a + bi + c + di) + e + fi \\ &= a + bi + c + di + e + fi = a + bi + (c + di + e + fi) = z + (w + q) \end{aligned}$$

– **Elemento neutro della somma**

$$\forall z \in \mathbb{C}, \exists! 0 \in \mathbb{C} \mid z + 0 = a + bi + 0 = a + bi = z$$

– **Elemento inverso della somma**

$$\forall z \in \mathbb{C}, \exists! -z \in \mathbb{C} \mid z + (-z) = a + bi + (-a - bi) = 0$$

– **Commutatività della somma**

$$\forall z, w \in \mathbb{C} \mid z + w = a + bi + c + di = c + di + a + bi = w + z$$

- È un gruppo abeliano nel prodotto (escludendo 0):

– **Associatività del prodotto**

$$\begin{aligned} \forall z := a+bi, w := c+di, q := e+fi \in \mathbb{C} &\implies (zw)q = [(a+bi) \cdot (c+di)] \cdot (e+fi) = \\ &= (a+bi) \cdot (c+di) \cdot (e+fi) = (a+bi) \cdot [(c+di) \cdot (e+fi)] = z(wq) \end{aligned}$$

– **Elemento neutro del prodotto**

$$\forall z \in \mathbb{C}, \exists! 1 \in \mathbb{C} \mid z \cdot 1 = (a+bi) \cdot 1 = a+bi = z$$

- **Elemento inverso del prodotto:** l'inverso $z^{-1} = \frac{1}{a+ib}$ non risulta apparire nella forma $c+id \mid c, d \in \mathbb{R}$. Riscriviamo quindi z^{-1} come:

$$z = a + ib \implies z^{-1} = \frac{1}{z} = \frac{\bar{z}}{z \cdot \bar{z}} = \frac{\bar{z}}{|z|^2} = \frac{a - ib}{a^2 + b^2} = \frac{a}{a^2 + b^2} + i \cdot \frac{-b}{a^2 + b^2}$$

Ponendo $c := \frac{a}{a^2+b^2} \in \mathbb{R}$ e $d := \frac{-b}{a^2+b^2} \in \mathbb{R}$, otteniamo che $z^{-1} = c + id \in \mathbb{C}$. Quindi l'assioma è verificato per:

$$\forall z \in \mathbb{C} - \{0\}, \exists! z^{-1} := \frac{\bar{z}}{z \cdot \bar{z}} \mid z \cdot z^{-1} = 1$$

– **Commutatività del prodotto**

$$\forall z, w \in \mathbb{C} \mid z \cdot w = (a+bi)(c+di) = (c+di)(a+bi) = w \cdot z$$

□

2.2 Forma polare dei numeri complessi

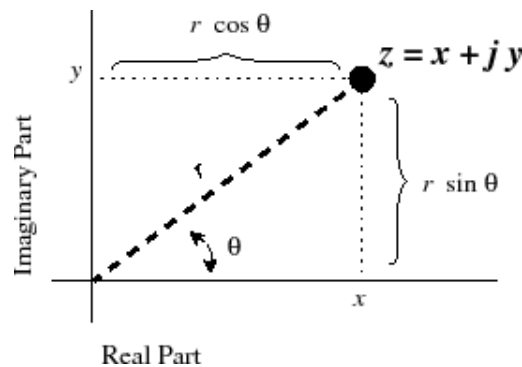
Inoltre, abbiamo visto come un numero complesso possa essere espresso come un punto sul piano gaussiano tramite una **coppia di valori**, descrivendo la distanza di tale punto dall'origine del piano $(0, 0)$ come $|z|$.

Possiamo quindi descrivere una **circonferenza di raggio** $r = |z|$ rappresentante tutti i numeri complessi aventi la stessa distanza dall'origine, dove θ corrisponde all'**arco in radianti** descritto dal **vettore** costruito attraverso le due coordinate gaussiane rappresentate da z .

Dunque, se $r = |z|$, abbiamo che:

$$r = |z| \implies \begin{cases} a = r \cdot \cos(\theta) \\ b = r \cdot \sin(\theta) \end{cases} \implies \begin{cases} \cos(\theta) = \frac{a}{r} = \frac{a}{|z|} \\ \sin(\theta) = \frac{b}{r} = \frac{b}{|z|} \end{cases}$$

Graficamente, ciò corrisponde a dire che:



Tuttavia, ricordando le proprietà delle funzioni seno e coseno, notiamo come il sistema imposto ammetta **infinite soluzioni**, poiché se θ è una soluzione allora anche $\theta + 2k\pi, k \in \mathbb{Z}$ è soluzione del sistema.

Per tale motivo, ogni soluzione valida viene detta **argomento di z** e, in particolare, esiste **un solo argomento principale** tale che $0 \leq \theta \leq 2\pi$. Definiamo quindi come $\arg(z)$ l'insieme contenente tutti gli argomenti di z , mentre definiamo come $Arg(z)$ l'argomento principale di z .

Definition 13. Forma polare dei numeri complessi

Dato un numero complesso $z := a + ib \in \mathbb{C}$, definiamo come **forma polare** di tale numero come:

$$z = r(\cos(\theta) + i \cdot \sin(\theta))$$

dove $r = |z|$ e $\theta = Arg(z)$.

Utilizziamo anche la **notazione contratta**:

$$e^{i\theta} := \cos(\theta) + i \cdot \sin(\theta)$$

dunque:

$$z = re^{i\theta}$$

Giustificazione per la notazione contratta:

- Matematicamente, tramite le proprietà degli esponenti abbiamo che

$$e^{i\theta_1} \cdot e^{i\theta_2} = e^{i(\theta_1+\theta_2)}$$

- Svolgiamo ora tale calcolo tramite la notazione esplicita

$$(\cos(\theta_1) + i \cdot \sin(\theta_1)) \cdot (\cos(\theta_2) + i \cdot \sin(\theta_2)) =$$

$$[\cos(\theta_1) \cdot \cos(\theta_2) - \sin(\theta_1) \cdot \sin(\theta_2)] + i \cdot [\cos(\theta_1) \cdot \sin(\theta_2) + \sin(\theta_1) \cdot \cos(\theta_2)] =$$

- Tramite le proprietà trigonometriche, in particolare $\cos(a+b) = \cos(a)\cos(b) - \sin(a)\sin(b)$ e $\sin(a+b) = \cos(a)\sin(b) + \sin(a)\cos(b)$, riscriviamo tale espressione come:

$$\cos(\theta_1 + \theta_2) + i \cdot \sin(\theta_1 + \theta_2)$$

- Riscrivendo il risultato nella forma contratta, otteniamo che i due calcoli matematici risultano essere equivalenti tra di loro:

$$\cos(\theta_1 + \theta_2) + i \cdot \sin(\theta_1 + \theta_2) = e^{i(\theta_1+\theta_2)}$$

L'uso di tale notazione ci permette di svolgere in modo rapido operazioni tra numeri complessi, in particolare tramite la **formula di De Moivre**:

Definition 14. Formula di De Moivre

Dato $z \in \mathbb{C}$, si ha che:

$$z = re^{i\theta} \implies z^n = (re^{i\theta})^n = r^n e^{in\theta}$$

Esempi:

1. Dato $z = -i$, calcolare z^4 .

- Calcoliamo l'argomento principale di z :

$$|z| = \sqrt{0^2 + (-1)^2} = 1$$

$$\begin{cases} \cos(\theta) = \frac{0}{1} = 0 \\ \sin(\theta) = \frac{-1}{1} = -1 \end{cases} \implies \text{Arg}(z) = \frac{3}{2}\pi \implies \arg(z) = \text{Arg}(z) + 2k\pi, k \in \mathbb{Z}$$

- Quindi, riscriviamo z come

$$z = re^{\text{Arg}(z) \cdot i} = e^{\frac{3}{2}\pi \cdot i}$$

- A questo punto, z^4 corrisponderà a:

$$z^4 = e^{4 \cdot \frac{3}{2}\pi \cdot i} = e^{6\pi \cdot i} = e^{0 \cdot i} = 1$$

2. Dato $z = 1 - i$, calcolare z^{10} .

- Calcoliamo l'argomento principale di z :

$$|z| = \sqrt{1^2 + (-1)^2} = \sqrt{2}$$

$$\begin{cases} \cos(\theta) = \frac{1}{\sqrt{2}} \\ \sin(\theta) = \frac{-1}{\sqrt{2}} \end{cases} \implies \text{Arg}(z) = \frac{7}{4}\pi \implies \arg(z) = \text{Arg}(z) + 2k\pi, k \in \mathbb{Z}$$

- Quindi, riscriviamo z come

$$z = re^{\text{Arg}(z) \cdot i} = \sqrt{2}e^{\frac{7}{4}\pi \cdot i}$$

- A questo punto, z^{10} corrisponderà a:

$$z^{10} = (\sqrt{2})^{10} e^{10 \cdot \frac{7}{4}\pi \cdot i} = 2^5 e^{\frac{35}{2}\pi \cdot i} = 2^5 e^{(16\pi + \frac{3}{2}\pi) \cdot i} = 2^5 e^{\frac{3}{2}\pi i}$$

- Siccome abbiamo visto che $e^{\frac{3}{2}\pi i} = -i$, allora riscriviamo z^{10} come:

$$z^{10} = 2^5 e^{\frac{3}{2}\pi i} = -2^5 i$$

2.3 Teorema fondamentale dell'algebra

Considerati due numeri z e n dove $z \in \mathbb{C}$ e $n \in \mathbb{N}, n \geq 2$, ci chiediamo quante siano le **soluzioni complesse dell'equazione** $x^n = z$. Nel caso in cui $z = 0$, l'unica soluzione risulta essere $x = 0$. Nel caso in cui $z \neq 0$, invece, esistono n **distinte soluzioni**.

Utilizzando la formula di De Moivre, possiamo riscrivere tale espressione come:

$$x^n = z \iff x = \sqrt[n]{z} \iff x = z^{\frac{1}{n}} \iff$$

$$\iff x = r^{\frac{1}{n}} e^{\frac{1}{n}\theta i}$$

Abbiamo quindi trovato **una soluzione valida** per l'equazione. Tuttavia, ricordando che un numero complesso z possiede **infiniti argomenti**, riscriviamo x come:

$$x = r^{\frac{1}{n}} e^{i(\frac{\theta}{n} + \frac{2k\pi}{n})}$$

A questo punto, al variare di $k = 0, 1, \dots, n-1$ otteniamo le n **soluzioni all'equazione**. Difatti, quando $k = n$, riotteniamo la prima soluzione dell'equazione, mentre quando $k = n+1$ otteniamo la seconda, e così via.

Esempio:

- Dato $z = i$, vogliamo sapere le soluzioni dell'equazione $x^3 = z$.

$$x^3 = i \iff x^3 = e^{\frac{1}{2}\pi i} \iff x = e^{i(\frac{1}{2 \cdot 3}\pi + \frac{2k\pi}{3})}$$

– Se $k = 0$

$$x_1 = e^{i(\frac{1}{2 \cdot 3}\pi)} = e^{\frac{1}{6}\pi i}$$

– Se $k = 1$

$$x_2 = e^{i(\frac{1}{2 \cdot 3}\pi + \frac{2\pi}{3})} = e^{\frac{5}{6}\pi i}$$

– Se $k = 2$

$$x_3 = e^{i(\frac{1}{2 \cdot 3}\pi + \frac{4\pi}{3})} = e^{\frac{9}{6}\pi i} = e^{\frac{3}{2}\pi i}$$

– Se $k = 3$

$$x_4 = e^{i(\frac{1}{2 \cdot 3}\pi + \frac{6\pi}{3})} = e^{i(\frac{1}{6}\pi + 2\pi)} = e^{\frac{1}{6}\pi i} \implies x_4 = x_1$$

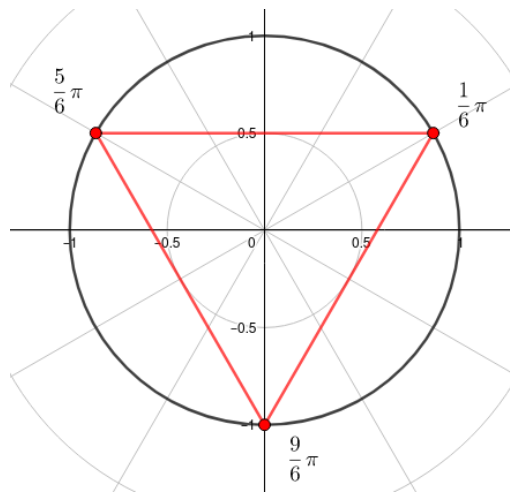
– Se $k = 4$

$$x_5 = e^{i(\frac{1}{2 \cdot 3}\pi + \frac{8\pi}{3})} = e^{i(\frac{1}{6}\pi + \frac{2\pi}{3} + 2\pi)} = e^{\frac{5}{6}\pi i} \implies x_5 = x_2$$

– ...

Notiamo quindi che nonostante esistano **infiniti argomenti di z** , le soluzioni risultano essere cicliche tra di loro, risultando in solo **3 soluzioni valide per l'equazione**.

Inoltre, graficando sul piano di Gauss le tre radici soluzioni dell'equazione, notiamo come ognuna di esse corrisponda al vertice di un triangolo equilatero inscritto in una circonferenza di raggio 1:



Observation 4

Le n radici n -esime di un numero complesso corrispondono ai vertici di un poligono regolare di n lati inscritto in una circonferenza di raggio $|z|^{\frac{1}{n}}$.

Theorem 5. Teorema fondamentale dell'algebra

Dato un polinomio $p(x) := a_0 + a_1x + \dots + a_nx^n = 0$ dove $a_i \in \mathbb{C}, n \geq 1, a_n \neq 0$, **esistono sempre n radici complesse** di $p(x)$:

$$\exists x_1, \dots, x_n \in \mathbb{C} \mid p(x_i) = 0$$

Capitolo 3

Relazioni e Induzione

Definition 15. Relazione

Dato un insieme X , definiamo come **relazione** R su X un **sottoinsieme del prodotto cartesiano** $X \times X$:

$$R \subseteq X \times X \iff R \subseteq \{(x, y) \mid x, y \in X\}$$

Data una coppia (x, y) , se essa appartiene alla relazione R allora affermiamo ciò con la notazione $x \sim y$ (oppure con $R(x, y)$), altrimenti affermiamo che essa non appartiene alla relazione con la notazione $x \not\sim y$ (oppure con $\neg R(x, y)$).

$$x \sim y \iff (x, y) \in R \qquad x \not\sim y \iff (x, y) \notin R$$

Definition 16. Relazione di equivalenza

Una relazione \sim viene detta **relazione di equivalenza** se su di essa valgono le seguenti proprietà:

- **Riflessività:**

$$x \sim x, \forall x \in X$$

- **Simmetria:**

$$x \sim y \implies y \sim x, \forall x, y \in X$$

- **Transitività:**

$$x \sim y \wedge y \sim z \implies x \sim z, \forall x, y, z \in X$$

Esempi:

- La relazione di eguaglianza $a \sim b \iff a = b$ è una relazione di equivalenza
- Dato l'insieme X corrispondente ad un insieme di automobili, la relazione $a \sim b \iff a$ ha lo stesso colore di b è una relazione di equivalenza

Definition 17. Relazione d'ordine totale e parziale

Una relazione \prec viene detta **relazione d'ordine totale** se su di essa valgono le seguenti proprietà:

- **Riflessività:**

$$x \prec x, \forall x \in X$$

- **Anti-simmetria:**

$$x \prec y, y \prec x \implies x = y, \forall x, y \in X$$

- **Transitività:**

$$x \prec y, y \prec z \implies x \prec z, \forall x, y, z \in X$$

- **Totalità:**

$$x \prec y \vee y \prec x, \forall x, y \in X$$

Se \prec è una relazione che soddisfa la riflessività, l'anti-simmetria, la transitività ma non la totalità, allora tale relazione viene detta **relazione d'ordine parziale**

Esempi:

- La relazione di minor-eguaglianza $a \sim b \iff a \leq b$ è una relazione d'ordine
- Dato un insieme X , definiamo come $\mathcal{P}(X)$ l'insieme contenente tutte le parti di X (ossia i suoi sottoinsiemi)

$$\mathcal{P}(X) = \{X' \mid X' \subseteq X\}$$

La relazione \subseteq su $\mathcal{P}(X)$ risulta essere una relazione d'ordine parziale, poiché:

- Ogni sottoinsieme A è sottoinsieme di se stesso (riflessività):

$$A \subseteq A, \forall A \in \mathcal{P}(X)$$

- Se un sottoinsieme A è sottoinsieme di B e B è sottoinsieme di A , allora ciò è possibile solo se A e B sono lo stesso sottoinsieme (anti-simmetria):

$$A \subseteq B \wedge B \subseteq A \implies A = B$$

- Se un sottoinsieme A è sottoinsieme di B e B è sottoinsieme di C , allora anche A è sottoinsieme di C (transitività):

$$A \subseteq B \wedge B \subseteq C \implies A \subseteq C$$

- Non tutti i sottoinsiemi sono confrontabili tra loro (ordine non totale). Ad esempio, se $X = \{a, b, c\}$ si ha che:

$$\{a\}, \{b, c\} \in \mathcal{P}(X) \implies \{a\} \not\subseteq \{b, c\} \wedge \{b, c\} \not\subseteq \{a\}$$

3.1 Classi di equivalenza

Definition 18. Classe di equivalenza

Sia \sim relazione d'equivalenza definita su un insieme X . Dato un elemento $x \in X$, denotiamo come $[x]$ la sua **classe di equivalenza su \sim** , ossia l'insieme di tutti gli elementi in relazione con x :

$$[x] = \{y \in X \mid x \sim y\}$$

Observation 5

Sia \sim relazione d'equivalenza definita su un insieme X . Dato un elemento $x \in X$, per riflessività della relazione \sim si ha che:

$$x \sim x \iff x \in [x]$$

dunque un elemento è sempre nella sua classe di equivalenza

Definition 19. Insieme quoziente

Sia \sim relazione d'equivalenza definita su un insieme X . Definiamo come **insieme quoziente di X su \sim** l'insieme di tutte le classi di equivalenza indotte dalla relazione:

$$X/\sim: \{[x] \mid x \in X\}$$

Definition 20. Partizione di un insieme

Dato un insieme X , definiamo come **partizione di X** l'insieme $\{X_1, \dots, X_n\}$ delle sue **parti**, ossia i suoi sottoinsiemi disgiunti tra loro la cui unione corrisponde ad X :

$$X = \bigsqcup_{1 \leq i \leq n} X_i$$

dove \bigsqcup corrisponde al simbolo di **unione disgiunta**, equivalente a:

$$X = \bigcup_{1 \leq i \leq n} X_i \text{ dove } X_i \cap X_j = \emptyset, \forall i \neq j$$

Observation 6

Data una relazione d'equivalenza \sim definita su un insieme X , si verifica che:

$$x \sim y \iff [x] = [y] \qquad x \not\sim y \iff [x] \cap [y] = \emptyset$$

Dunque, **tutte le classi di equivalenza** indotte da \sim sono **disgiunte tra loro**.

Dimostrazione:

- $x \sim y \implies [x] = [y]$
 - Se $x \sim y$, allora si ha che:

$$z \in [x] \iff z \sim x \implies z \sim x, x \sim y \implies z \sim y \iff z \in [y] \implies [x] \subseteq [y]$$
 - Viceversa, siccome $x \sim y \iff y \sim x$, si ha che:

$$w \in [y] \iff w \sim y \implies w \sim y, y \sim x \implies w \sim x \iff w \in [x] \implies [y] \subseteq [x]$$
- $[x] = [y] \implies x \sim y$
 - Se $[x] = [y]$, allora si ha che:

$$z \in [x] = [y] \iff z \sim x, z \sim y \iff x \sim z, z \sim y \implies x \sim y$$
- $x \not\sim y \implies [x] \cap [y] = \emptyset$
 - Supponiamo per assurdo che $x \not\sim y$ e che $[x] \cap [y] \neq \emptyset$. Dunque, si ha che:

$$\begin{aligned} [x] \cap [y] \neq \emptyset &\iff \exists z \in [x] \cap [y] \iff z \in [x] \wedge z \in [y] \iff \\ &\iff z \sim x, z \sim y \iff x \sim z, z \sim y \implies x \sim y \end{aligned}$$
 contraddicendo l'ipotesi iniziale, dunque $x \not\sim y \implies [x] \cap [y] = \emptyset$
- $[x] \cap [y] = \emptyset \implies x \not\sim y$
 - Supponiamo per assurdo che $[x] \cap [y] = \emptyset$ e che $x \sim y$. Dunque, si ha che:

$$x \sim y \iff x \in [x] = [y] \implies [x] \cap [y] = [x] = [y] \neq \emptyset$$
 contraddicendo l'ipotesi iniziale, dunque $[x] \cap [y] = \emptyset \implies x \not\sim y$

□

Corollary 2

Data una relazione d'equivalenza \sim definita su un insieme X , l'insieme quoziente X/\sim è una **partizione** di X :

$$X = \bigsqcup_{[x] \in X/\sim} [x]$$

Dimostrazione:

- Poiché tutte le classi di equivalenza appartenenti a X/\sim sono disgiunte tra loro, si ha che:

$$\bigcup_{[x] \in X/\sim} [x] = \bigsqcup_{[x] \in X/\sim} [x]$$

- Dato $x \in X$, si ha che:

$$x \in X \iff x \sim x \iff x \in [x] \implies x \in \bigsqcup_{[x] \in X/\sim} [x]$$

- Viceversa, si ha che:

$$z \in \bigsqcup_{[x] \in X/\sim} [x] \implies \exists [x] \in A/X \mid z \in [x] \iff z \sim x \implies z \in X$$

□

Proposition 6

Dato un insieme X , una partizione $P := \{X_1, \dots, X_n\}$ di X **induce una relazione di equivalenza** sull'insieme X

Dimostrazione:

- Definiamo la relazione $x \sim y \iff x, y \in X_i$, dove $X_i \in P$, indicante che due elementi sono in relazione se e solo se appartengono alla stessa parte della partizione.
- Verifichiamo che si tratti di una relazione di equivalenza:

– Riflessività:

$$\forall x \in X, \exists X_i \in P \mid x \in X_i \implies x \sim x$$

– Simmetria:

$$x \sim y \iff x, y \in X_i, \exists X_i \in P \implies y \sim x$$

– Transitività:

$$x \sim y, y \sim z \iff x, y \in X_i \wedge y, z \in X_j, \exists X_i, X_j \in P \implies y \in X_i \cap X_j$$

Poiché tutte le parti sono per definizione disgiunte tra loro, abbiamo che $y \in X_i \cap X_j \iff X_i = X_j$, dunque si ha che:

$$x \sim y, y \sim z \implies x, y \in X_i \wedge y, z \in X_j \iff x, y, z \in X_i = X_j \implies x \sim z$$

□

Proposition 7. Proiezione canonica al quoziente

Una relazione di equivalenza \sim su un insieme X induce una funzione suriettiva detta **proiezione canonica al quoziente** la quale mappa ogni elemento $x \in X$ alla propria classe di equivalenza su \sim :

$$\pi : X \rightarrow X/\sim : x \mapsto [x]$$

Dimostrazione:

- Poiché per riflessività si ha che $x \sim x \iff x \in [x]$, la funzione di proiezione π risulta essere evidentemente suriettiva:

$$x \in [x] \implies \forall [x] \in X/\sim, \exists x \in X \mid \pi(x) = [x]$$

□

3.2 Relazione di Divisore

Definition 21. Relazione di divisore

Dati due numeri naturali $m, n \in \mathbb{Z}$, definiamo la relazione " m è divisore di n ", indicato come $m \mid n$, se esiste un elemento $q \in \mathbb{Z} \mid n = mq$:

$$m \mid n \iff \exists q \in \mathbb{Z} \mid n = mq$$

Attenzione: $m \mid n$ non è il simbolo matematico "tale che"

Observation 7

Dati $m, n \in \mathbb{Z}$, la relazione di divisore $m \mid n$ è una relazione **riflessiva** e **transitiva**

Dimostrazione:

- Soddisfa la **riflessività**:

$$\forall n \in \mathbb{Z}, n = n \cdot 1 \iff n \mid n \cdot 1 \iff n \mid n$$

- Soddisfa la **transitività**:

$$m \mid n, n \mid d \iff \exists p, q \in \mathbb{Z} \mid n = mp, d = nq \implies d = (mp)q = m(pq) \implies m \mid d$$

- Non soddisfa l'**anti-simmetria**:

$$m \mid n, n \mid m \iff \exists p, q \in \mathbb{Z} \mid n = mp, m = nq \implies n = mp = (np)q = n(pq)$$

A questo punto, si verificano due casi:

- Se $n = 0$ allora

$$n = 0 \implies m = nq = 0 \cdot q = 0 \implies m = 0 \implies n = m = 0$$

- Se $n \neq 0$ allora

$$n \neq 0 \implies n = n(pq) \implies qp = 1 \implies p = q = \pm 1 \implies$$

$$\implies \begin{cases} n = m & \text{se } p = q = 1 \\ n = -m & \text{se } p = q = -1 \end{cases}$$

Dunque, non in tutti i casi la relazione è anti-simmetrica.

□

Corollary 3

Dati $m, n \in \mathbb{N}$, la relazione di divisore $m \mid n$ è una **relazione d'ordine**

Dimostrazione:

- Ovviamente, poiché $m, n \in \mathbb{N} \subseteq \mathbb{Z}$, se segue che la relazione di divisore sia riflessiva e transitiva
- Procedendo analogamente alla dimostrazione precedente, il caso in cui $p = q = -1$ verrebbe scartato poiché $-1 \notin \mathbb{N}$, rendendo quindi $m = n$ l'unica possibilità

$$m \mid n, n \mid m, m, n \in \mathbb{N} \implies m = n$$

□

3.3 Relazione di Congruenza

Definition 22. Relazione di congruenza

Dato $a, b \in \mathbb{Z}$ e dato $n \geq 2 \in \mathbb{N}$, definiamo la relazione " a è congruente a b in modulo n ", denotata come con $a \equiv b(\text{mod } n)$, se e solo se $n \mid b - a$

$$a \equiv b(\text{mod } n) \iff n \mid (b - a)$$

Esempi:

- $7 \equiv 22(\text{mod } 5) \implies n \mid b - a \implies 5 \mid (22 - 7) \implies 5 \mid 15$
- $7 \equiv 2(\text{mod } 5) \implies n \mid b - a \implies 5 \mid (2 - 7) \implies 5 \mid -5$

Observation 8

La relazione di congruenza $a \equiv b(\text{mod } n)$ è una **relazione di equivalenza**.

Dimostrazione:

- **Riflessiva:**

$$a = a \iff a = n \cdot 0 + a \iff a - a = n \cdot 0 \iff n \mid a - a \iff a \equiv a(\text{mod } n)$$

- **Simmetrica:**

$$\begin{aligned} a \equiv b(\text{mod } n) &\iff n \mid b - a \iff \exists p \in \mathbb{Z} \mid b - a = np \iff \\ &\iff a - b = n(-p) \iff n \mid a - b \iff b \equiv a(\text{mod } n) \end{aligned}$$

- **Transitiva:**

$$\begin{aligned} a \equiv b(\text{mod } n), b \equiv c(\text{mod } n) &\iff \exists p, q \in \mathbb{Z} \mid b - a = np, c - b = nq \implies \\ \implies c - a = (c - b) + (b - a) &= nq + np = n(q + p) \iff n \mid c - a \iff a \equiv c(\text{mod } n) \end{aligned}$$

3.4 Teorema della divisione con resto euclidea

Theorem 8. Teorema della divisione con resto euclidea

Dati due interi $m, n \in \mathbb{Z}$ dove $n > 0$, si ha che:

$$\exists! q, r \in \mathbb{Z}, 0 \leq r < n \mid m = nq + r$$

dove q viene definito come **quoziente** e r come **resto** della divisione

Dimostrazione dell'esistenza:

- Dato $[m] : \{a \in \mathbb{Z} \mid a \equiv m \pmod{n}\}$, si ha che:
 $a \in [m] \iff a \equiv m \pmod{n} \iff n \mid m-a \iff \exists p \in \mathbb{Z} \mid m-a = np \iff a = m-np$
- Consideriamo quindi $[m]_{\geq 0} : \{a \in [m] \mid a \in \mathbb{N}\}$. Poiché $[m]_{\geq 0} \subseteq \mathbb{N}$, per il **principio del buon ordinamento** si ha che:
 $\exists r \in [m]_{\geq 0} \mid r \text{ è il minimo di } [m]_{\geq 0} \implies \exists q \in \mathbb{Z} \mid m = nq + r \implies r = m - nq$
- Supponiamo per assurdo che $r \geq n$, da cui ne segue che $r - n \geq 0 \implies r - n \in \mathbb{N}$. Quindi, abbiamo che:
 $r - n = (m - nq) - n \iff r - n = m - n(q+1) \iff r - n \in [m]_{\geq 0}$
- Poiché $r - n \leq r$, se $r \geq n$ si contraddirebbe l'ipotesi per cui r sia il minimo di $m_{\geq 0}$, dunque l'unica possibilità è che $r < n$
- Dunque, concludiamo che
 $\exists q, r \in \mathbb{Z}, 0 \leq r < n \mid r = m - nq \implies m = nq + r$

□

Dimostrazione dell'unicità:

- Supponiamo che q ed r non siano unici. Allora, ne segue che:
 $\exists q_1, q_2, r_1, r_2 \in \mathbb{Z}, 0 \leq r_1, r_2 < n \mid nq_1 + r_1 = m = nq_2 + r_2 \implies$
 $\implies nq_1 + r_1 = nq_2 + r_2 \implies r_2 - r_1 = n(q_1 - q_2) \iff n \mid r_2 - r_1$
- Siccome $0 \leq r_1, r_2 < n \implies -n < r_2 - r_1 < n$ e siccome $n \mid r_2 - r_1$, allora $r_2 - r_1$ deve necessariamente essere un multiplo di n compreso tra $-n$ ed n stesso.
- Poiché l'unico numero rispettante tali caratteristiche è 0, ne segue che:

$$\begin{cases} -n < r_2 - r_1 < n \\ n \mid r_2 - r_1 \end{cases} \iff \exists b \in \mathbb{Z} \mid r_2 - r_1 = nb \iff r_2 - r_1 = 0 \iff r_2 = r_1$$
- A questo punto, si ha che:
 $nq_1 + r_1 = nq_2 + r_2 \iff nq_1 + r_1 = nq_2 + r_1 \iff nq_1 = nq_2 \iff q_1 = q_2$

□

3.5 Relazione di Coniugio

Definition 23. Relazione di coniugio

Dato un gruppo G e dati $g, h \in G$, definiamo la relazione " g è coniugato di h " se si verifica che:

$$g \sim h \iff \exists a \in G \mid h = aga^{-1}$$

Observation 9

Se G è un gruppo abeliano, allora si ha che:

$$g \sim h \iff h = aga^{-1} = aa^{-1}g = g$$

Observation 10

La relazione di coniugio è una **relazione di equivalenza**.

Dimostrazione:

- **Riflessività:**

$$g = 1 \cdot g \cdot 1^{-1} \implies g \sim g$$

- **Simmetria:**

$$g \sim h \implies h = aga^{-1} \implies a^{-1}ha = a^{-1}aga^{-1}a \implies a^{-1}ha = g$$

ponendo $b := a^{-1}$, si ha che:

$$bhb^{-a} = g \implies h \sim g$$

- **Transitività:**

$$g \sim h \wedge h \sim k \implies h = aga^{-1}, k = bhb^{-1} \implies k = b(aga^{-1})b^{-1} = (ba)g(a^{-1}b^{-1})$$

ponendo $c := ba$, si ha che:

$$k = cgc^{-1} \implies g \sim k$$

□

3.6 Induzione matematica

Vogliamo dimostrare una successione di n proposizioni, etichettate come $p_1), p_2), \dots, p_n)$. Supponiamo di aver dimostrato la proposizione $p_1)$, che denominiamo come **caso base**. Se le prime $p_1), \dots, p_n)$ sono vere, allora anche la proposizione $p_{n+1})$ è vera (**passo induttivo**).

Per esprimere tale concetto matematicamente, possiamo dire che:

Theorem 9. Principio di induzione

Data una successione di proposizioni $p_1), \dots, p_n)$, si ha che:

$$\begin{aligned} p_1) &\implies p_2) \\ p_1), p_2) &\implies p_3) \\ &\dots \\ p_1), \dots, p_n) &\implies p_{n+1}) \end{aligned}$$

Esempi:

- Vogliamo verificare che la proposizione seguente proposizione sia vera $\forall n \geq 1$:

$$1 + 2 + 3 + \dots + (n - 1) + n = \frac{n(n + 1)}{2}$$

- Verifichiamo quindi il **caso base** $p_1)$, ossia $n = 1$

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

che risulta essere vero

- A questo punto, assumiamo per **ipotesi induttiva** che $p_n)$ sia vera.
- Impostiamo quindi il **passo induttivo**, ossia $p_{n+1})$:

$$1 + 2 + 3 + \dots + n + (n + 1) = \frac{(n + 1)(n + 1 + 1)}{2}$$

- Notiamo come il **passo induttivo contenga al suo interno l'ipotesi induttiva stessa**, che abbiamo affermato essere vera:

$$\begin{aligned} \underbrace{1 + 2 + 3 + \dots + n}_{\text{Ipotesi induttiva}} + (n + 1) &= \frac{(n + 1)(n + 1 + 1)}{2} \iff \\ \frac{n(n + 1)}{2} + (n + 1) &= \frac{(n + 1)(n + 2)}{2} \iff \frac{n(n + 1) + 2(n + 1)}{2} = \frac{(n + 1)(n + 2)}{2} \\ &\iff \frac{(n + 1)(n + 2)}{2} = \frac{(n + 1)(n + 2)}{2} \end{aligned}$$

Dunque, anche il passo induttivo risulta essere vero, concludendo che **la proposizione** p_n) **sia valida** $\forall n \geq 1$

2. • La funzione di Fibonacci è definita come:

$$\begin{cases} F_0 = 0 & \text{se } n = 0 \\ F_1 = 1 & \text{se } n = 1 \\ F_n = F_{n-1} + F_{n+2} & \text{se } n \geq 2 \end{cases}$$

- Le costanti φ e ψ , corrispondenti alle soluzioni dell'equazione $x^2 = x + 1$, sono definite come:

$$\varphi = \frac{1 + \sqrt{5}}{2} \quad \psi = \frac{1 - \sqrt{5}}{2}$$

- Vogliamo verificare per induzione che la seguente proposizione sia vera $\forall n$:

$$F_n = \frac{\varphi^n - \psi^n}{\varphi - \psi}$$

- Verifichiamo quindi p_0) e p_1 :

$$F_0 = \frac{\varphi^0 - \psi^0}{\varphi - \psi} = \frac{1 - 1}{\varphi - \psi} = 0$$

$$F_1 = \frac{\varphi^1 - \psi^1}{\varphi - \psi} = \frac{\varphi - \psi}{\varphi - \psi} = 1$$

- Assumiamo quindi per ipotesi induttiva che p_{n-1}) sia vera e verifichiamo il passo induttivo p_n , utilizzando però la definizione originale di F_n :

$$F_n = F_{n-1} + F_{n+2} = \frac{\varphi^{n-1} - \psi^{n-1}}{\varphi - \psi} + \frac{\varphi^{n-2} - \psi^{n-2}}{\varphi - \psi} = \frac{\varphi^{n-2}(\varphi + 1) - \psi^{n-2}(\psi + 1)}{\varphi - \psi}$$

- Siccome per definizione stessa $\varphi^2 = \varphi + 1$ e $\psi^2 = \psi + 1$, allora abbiamo che:

$$F_n = F_{n-1} + F_{n+2} = \frac{\varphi^{n-2}\varphi^2 - \psi^{n-2}\psi^2}{\varphi - \psi} = \frac{\varphi^n - \psi^n}{\varphi - \psi}$$

verificando quindi la validità del passo induttivo

3. • Vogliamo dimostrare per induzione l'identità binomiale di Newton, definita come:

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

dove il coefficiente binomiale è definito come:

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

- Verifichiamo quindi il caso base:

$$1 = (a + b)^0 = \sum_{k=0}^0 \binom{0}{k} a^k b^{0-k} = \binom{0}{0} a^0 b^{0-0} = 1$$

- A questo punto effettuiamo il passo induttivo:

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

- Trasliamo di -1 l'indice della prima sommatoria e portiamo fuori il suo ultimo termine:

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

- Nella seconda sommatoria, invece, portiamo fuori il primo termine, in modo che gli indici di entrambe le sommatorie coincidano:

$$\begin{aligned} &= a^{n+1} + \sum_{k=1}^n \binom{n}{k-1} a^k b^{n+1-k} + \sum_{k=1}^n \binom{n}{k} a^k b^{n-k+1} + \binom{n}{0} a^0 b^{n-0+1} = \\ &= a^{n+1} + \sum_{k=1}^n \binom{n}{k-1} a^k b^{n+1-k} + \sum_{k=1}^n \binom{n}{k} a^k b^{n-k+1} + b^{n+1} = \end{aligned}$$

- A questo punto uniamo nuovamente le due sommatorie:

$$= a^{n+1} + b^{n+1} + \sum_{k=1}^n \left[\binom{n}{k-1} + \binom{n}{k} \right] a^k b^{n-k+1} =$$

- Per le proprietà dei coefficienti binomiali (facilmente verificabili) si ha che $\binom{n+1}{k} = \binom{n}{k-1} + \binom{n}{k}$, dunque riscriviamo la sommatoria come:

$$= a^{n+1} + b^{n+1} + \sum_{k=1}^n \binom{n+1}{k} a^k b^{n-k+1} =$$

- A questo punto, poiché $\binom{n}{0} = \binom{n}{n+1} = 1$, riscriviamo i due termini esterni alla sommatoria in modo da poterli reinserire in essa, ottenendo il risultato cercato:

$$= \binom{n+1}{n+1} a^{n+1} + \binom{n+1}{0} b^{n+1} + \sum_{k=1}^n \binom{n+1}{k} a^k b^{n-k+1} = \sum_{k=0}^{n+1} \binom{n+1}{k} a^k b^{n+1-k}$$

Capitolo 4

Elementi di Teoria degli Anelli

4.1 Insieme quoziente

4.1.1 Classi laterali sinistre

Proposition 10

Sia G un gruppo e sia $H \subseteq G$ sottogruppo. Definiamo la seguente **relazione d'equivalenza**:

$$x \sim y \iff x^{-1}y \in H$$

Dimostrazione:

- **Riflessività:**

$$x \sim x \implies x^{-1}x = 1 \in H$$

- **Simmetria:**

$$x \sim y \implies h := x^{-1}y \in H \implies h^{-1} := y^{-1}x \in H \implies y \sim x$$

- **Transitività:**

$$\begin{aligned} x \sim y, y \sim z &\implies h := x^{-1}y, k := y^{-1}z \in H \implies \\ &\implies hk = x^{-1}yy^{-1}z = x^{-1}z \implies x^{-1}z \in H \end{aligned}$$

□

Definition 24. Classi laterali sinistre

Sia G un gruppo e sia $H \leq G$. Definiamo come **classi laterali sinistre di H di G** le classi d'equivalenza generate dalla relazione d'equivalenza $x \sim y \iff x^{-1}y \in H$:

$$x \in G, [x] = \{y \in G \mid x \sim y\}$$

Denotiamo come G/H (letto " G modulo H ") l'**insieme quoziente di tutte le classi laterali sinistre di H in G** .

Esempio:

- Dato $I(n) : \{nk \mid k \in \mathbb{Z}\}$ si ha che $I(3) \leq \mathbb{Z}$, generando una partizione di \mathbb{Z} in tre classi laterali sinistre:

$$\mathbb{Z}/I(3) : \{[0], [1], [2]\}$$

- In particolare, notiamo che:

- $0 \in [0]$, poiché $0 \sim 0 \iff -0 + 0 = 0 = 3 \cdot 0 \in I(3)$
- $1 \in [1]$, poiché $1 \sim 1 \iff -1 + 1 = 0 = 3 \cdot 0 \in I(3)$
- $2 \in [2]$, poiché $2 \sim 2 \iff -2 + 2 = 0 = 3 \cdot 0 \in I(3)$
- $3 \in [3]$, poiché $3 \sim 3 \iff -3 + 3 = 0 = 3 \cdot 0 \in I(3)$
- $4 \in [1]$, poiché $4 \sim 1 \iff -4 + 1 = -3 = 3 \cdot (-1) \in I(3)$
- $5 \in [2]$, poiché $5 \sim 2 \iff -5 + 2 = -3 = 3 \cdot (-1) \in I(3)$
- $6 \in [3]$, poiché $6 \sim 3 \iff -6 + 3 = -3 = 3 \cdot (-1) \in I(3)$
- $7 \in [1]$, poiché $7 \sim 1 \iff -7 + 1 = -6 = 3 \cdot (-2) \in I(3)$
- $8 \in [2]$, poiché $8 \sim 2 \iff -8 + 2 = -6 = 3 \cdot (-2) \in I(3)$
- $9 \in [3]$, poiché $9 \sim 3 \iff -9 + 3 = -6 = 3 \cdot (-2) \in I(3)$
- ...

- Più in generale, si verifica che:

$$\mathbb{Z}/I(n) : \{[0], \dots, [n-1]\}$$

Definition 25. Insieme quoziente \mathbb{Z}_n

Dato $(I(n), +) \leq (\mathbb{Z}, +)$ dove $I(n) : \{nk \mid k \in \mathbb{Z}\}$, l'insieme quoziente $\mathbb{Z}/I(n)$ **coincide** con l'insieme quoziente \mathbb{Z}/ \equiv .

Tale particolare insieme quoziente viene detto **insieme quoziente \mathbb{Z}_n**

$$\mathbb{Z}_n := \{[0], \dots, [n-1]\} = \mathbb{Z}/I(n) = \mathbb{Z}/ \equiv$$

Dimostrazione:

- Come dimostrato precedentemente, si ha che $(I(n), +) \leq (\mathbb{Z}, +)$.
- Considerando la relazione $a \sim b \iff (-a) + b \in I(n)$ (poiché a^{-1} nell'operazione somma corrisponde a $-a$), otteniamo che:

$$a \sim b \iff -a + b = b - a \in I(n) \iff -a + b = nk, \exists k \in \mathbb{Z} \iff$$

$$\iff n \mid b - a \iff a \equiv b \pmod{n}$$

dunque si ha che $\mathbb{Z}_n := \mathbb{Z}/I(n) = \mathbb{Z}/ \equiv$

□

Observation 11

Dato un gruppo G e $H \leq G$, per ogni $[x] \in G/H$ si ha che:

$$[x] = xH := \{xh \mid h \in H\}$$

Dimostrazione:

- Dimostriamo che $[x] = xH$:

$$\begin{aligned} y \in [x] &\iff x \sim y \iff h := x^{-1}y \in H \iff h = x^{-1}y \iff \\ &\iff xh = xx^{-1}y \iff xh = y \in xH \end{aligned}$$

□

4.1.2 Teorema di Lagrange**Observation 12**

Dato un gruppo G e $H \leq G$, per ogni $[x] = xH \in G/H$ si ha che:

$$|[x]| = |xH| = |H|$$

Dimostrazione:

- Dato $x \in G$ consideriamo la funzione $\varphi : H \rightarrow xH : h \mapsto xh$
- La funzione risulta essere iniettiva poiché:

$$h, k \in H \mid \varphi(h) \neq \varphi(k) \iff xh \neq xk \iff h \neq k$$

- La funzione risulta essere suriettiva poiché per costruzione di xH si ha che:

$$\forall xh \in xH, \exists h \in H \mid \varphi(h) = xh$$

- Poiché esiste una funzione biettiva $\varphi : H \rightarrow xH$, ne segue che $|H| = |xH|$

□

Theorem 11. Teorema di Lagrange

Sia G un **gruppo finito** e sia $H \leq G$. In tal caso, si ha che:

$$|G| = |H| \cdot |G/H|$$

Inoltre, definiamo $[G : H] := |G/H|$ come l'**indice di H in G**

Dimostrazione:

- Poiché G/H è una partizione di G e poiché $\forall [x] \in G/H, |[x]| = |H|$:

$$G = \bigsqcup_{[x] \in G/H} [x] \implies |G| = |H| \cdot |G/H|$$

□

4.2 L'anello commutativo \mathbb{Z}_n

Proposition 12. Gruppo quoziente G/H

Se $(G, +)$ è un **gruppo abeliano** e $H \leq G$, allora $(G/H, +)$ è un **gruppo abeliano**.

Dimostrazione:

- Dimostriamo prima che l'operazione somma intesa come $[x] + [y] = [x + y]$ sia ben definita, ossia che $[x] = [x'], [y] = [y'] \implies [x + y] = [x' + y']$:

$$[x] = [x'], [y] = [y'] \iff x \sim x', y \sim y' \iff x' - x, y' - y \in H$$

Poiché $h_1 := x' - x, h_2 := y' - y \in H$, per chiusura nella somma di H si ha che:

$$\begin{aligned} h_1 + h_2 \in H &\implies (x' - x) + (y' - y) = x' - x + y' - y = x' + y' - (x + y) \in H \iff \\ &x' + y' \sim x + y \iff [x + y] = [x' + y'] \end{aligned}$$

- Successivamente, verifichiamo gli assiomi di gruppo abeliano:

– **Associatività:**

$$([x] + [y]) + [z] = [x + y] + [z] = [x + y + z] = [x] + [y + z] = [x] + ([y] + [z])$$

– **Elemento neutro:**

$$[x] + [0] = [x + 0] = [x]$$

– **Elemento inverso:**

$$[x] + [-x] = [x + (-x)] = [0]$$

– **Commutatività:**

$$[x] + [y] = [x + y] = [y + x] = [y] + [x]$$

□

Corollary 4. Gruppo quoziente \mathbb{Z}_n

Poiché \mathbb{Z} è un anello commutativo, $(\mathbb{Z}_n, +)$ è un **gruppo abeliano**

Esempi:

Operando nel gruppo \mathbb{Z}_{11} si avrà che:

- $[9] + [8] = [17] = [6]$, poiché $17 \equiv 6 \pmod{11}$
- $[4] + [3] = [7]$
- $[5] - [6] = [-1] = [10]$, poiché $-1 \equiv 10 \pmod{11}$

Proposition 13. Anello quoziente G/H

Se $(A, +, \cdot)$ è un **anello commutativo** e $I \leq A$ **ideale**, allora $(A/I, +, \cdot)$ è un **anello commutativo**.

Dimostrazione:

- Poiché $I \leq A$, per dimostrazione precedente si ha che $(A/I, +)$ è gruppo abeliano
- Dimostriamo prima che l'operazione prodotto intesa come $[x][y] = [xy]$ sia ben definita, ossia che $[x] = [x'], [y] = [y'] \implies [xy] = [x'y']$:

$$[x] = [x'], [y] = [y'] \iff x \sim x', y \sim y' \iff x' - x, y' - y \in I$$

Poiché $i_1 := x' - x, i_2 := y' - y \in I$, per chiusura nel prodotto di I si ha che:

$$\begin{aligned} i_1, i_2 \in I &\implies i_1 y', x i_2 \in I \implies i_1 y' + x i_2 \in I \implies \\ i_1 y' + x i_2 &= (x' - x)y' + x(y' - y) = x'y' - xy' + xy' - xy = x'y' - xy \in I \iff \\ &\iff x'y' \sim xy \iff [x'y'] = [xy] \end{aligned}$$

- Successivamente, verifichiamo i rimanenti assiomi di anello commutativo
 - **Associatività nel prodotto:**

$$([x][y])[z] = [xy][z] = [xyz] = [x][yz] = [x]([y][z])$$

- **Elemento neutro nel prodotto:**

$$[x][1] = [x \cdot 1] = [x]$$

- **Commutatività nel prodotto:**

$$[x][y] = [xy] = [yx] = [y][x]$$

- **Distributività:**

$$[x]([y] + [z]) = [x][y + z] = [x(y + z)] = [xy + xz] = [xy] + [xz] = [x][y] + [x][z]$$

□

Corollary 5. Anello quoziente \mathbb{Z}_n

Poiché \mathbb{Z} è un anello commutativo, $(\mathbb{Z}_n, +, \cdot)$ è un **anello commutativo**

Esempi:

Operando nell'anello \mathbb{Z}_4 avremo che:

- $[2][3] = [6] = [2]$, poiché $6 \equiv 2 \pmod{4}$
- $[2][3]^{-1} = [2][3] = [4]$, poiché $[3]$ è l'inverso di $[3]$ in \mathbb{Z}_4 in quanto $[3][3] = [9] = [1]$

4.3 Invertibili e Divisori dello zero

Definition 26. Invertibile e Divisore dello zero

Dato un anello commutativo A e un elemento $a \in A$, definiamo a come **elemento invertibile** se e solo se

$$\exists a^{-1} \in A \mid aa^{-1}a^{-1}a = 1$$

Definiamo invece a come **divisore dello zero** se e solo se:

$$a \mid 0 \iff \exists c \neq 0 \in A \mid 0 = ac$$

Definition 27. Gruppo degli invertibili

Dato un anello commutativo $(A, +, \cdot)$, definiamo l'**insieme degli invertibili di A** come:

$$A^* := \{a \in A \mid \exists a^{-1} \in A\}$$

Inoltre, (A^*, \cdot) è un **gruppo**

Dimostrazione:

- **Chiusura:**

$$x, y \in A^* \implies (xy)^{-1} = y^{-1}x^{-1} \implies xy \in A^*$$

- **Associatività:**

$$x, y, z \in A^* \implies x(yz) = xyz = (xy)z$$

- **Elemento neutro:**

$$1 = 1^{-1} \in A \mid 1 \cdot 1^{-1} = 1 \cdot 1 = 1 \implies 1 \in A^* \mid a \cdot 1 = a, \forall a \in A^*$$

- **Elemento inverso:**

$$x \in A^* \implies x = (x^{-1})^{-1} \implies x^{-1} \in A^*$$

□

Observation 13

Dato un anello commutativo A e un elemento $a \in A$, se a è un **divisore dello zero** allora esso **non è invertibile**:

$$a \mid 0 \implies a \notin A^*$$

Dunque, per la contro-nominale di tale implicazione, se a è **invertibile** allora esso **non è un divisore dello zero**:

$$a \in A^* \implies a \nmid 0$$

Dimostrazione per assurdo:

- Supponiamo che per assurdo che $a \mid 0$ e che $a \in A^*$. Allora, si ha che:

$$a \mid 0 \iff \exists b \neq 0 \in A \mid 0 = ab \implies a^{-1} \cdot 0 = a^{-1}ab \implies 0 = b$$

contraddicendo quindi l'ipotesi iniziale $b \neq 0$, dunque l'unica possibilità è che $a \notin A^*$

□

Definition 28. Dominio di integrità

Sia A un anello commutativo. Definiamo A come **dominio di integrità** se $0 \in A$ è l'unico divisore dello zero:

$$\nexists a \neq 0 \in A \text{ t.c. } a \mid 0 \iff a \nmid 0, \forall a \neq 0 \in A$$

Observation 14

Un anello commutativo A è un dominio di integrità se e solo se vale la **legge di annullamento del prodotto**:

$$\forall x, y \in A \mid xy = 0 \implies x = 0 \vee y = 0$$

Dimostrazione:

- Supponiamo per assurdo che A sia un dominio di integrità e che $\exists x, y \neq 0 \in A \mid xy = 0$, implicando che non valga la legge di annullamento del prodotto. Dunque, si ha che:

$$xy = 0 \implies x^{-1}xy = x^{-1}0 \implies y = 0$$

contraddicendo l'ipotesi per cui $y \neq 0$, dunque l'unica possibilità è che valga la legge di annullamento del prodotto

- Supponiamo ora per assurdo che valga la legge di annullamento del prodotto e che A non sia un dominio di integrità. Dunque, si ha che:

$$\exists a \neq 0 \in A \text{ t.c. } a \mid 0 \implies ab = 0, \exists b \neq 0$$

Poiché vale la legge di annullamento del prodotto, si ha che

$$ab = 0 \implies a = 0 \vee b = 0$$

Tuttavia, poiché $b \neq 0$, l'unica possibilità è che $a = 0$, contraddicendo l'ipotesi per cui $a \neq 0$. Di conseguenza, A è un dominio di integrità

□

Corollary 6

L'anello commutativo \mathbb{Z} è un **dominio di integrità** poiché in esso vale la **legge di annullamento del prodotto**

Observation 15

Se K è un **campo**, allora esso è un **dominio di integrità** poiché $K^* = K - \{0\}$

Dimostrazione:

- Se K è un campo, allora

$$\forall a \neq 0 \in K, \exists a^{-1} \in K \mid aa^{-1} = 1 \iff K^* = K - \{0\}$$

- Inoltre, siccome tutti gli elementi di K escluso zero sono invertibili, si ha che:

$$\forall a \neq 0 \in K, a \in K^* \implies a \nmid 0, \forall a \neq 0 \in K$$

□

Proposition 14

Dato un **dominio di integrità** A e dati $a, b \in A$, si ha che:

$$I(a) = I(b) \iff a = bc, \exists c \in A^*$$

Dimostrazione:

- $a = bc, \exists c \in A^* \implies I(a) = I(b)$

$$a = bc, \exists c \in A^* \implies ac^{-1} = b \implies \begin{cases} a = bc \implies a \in I(b) \implies I(a) \subseteq I(b) \\ b = ac^{-1} \implies b \in I(a) \implies I(b) \subseteq I(a) \end{cases}$$

- $I(a) = I(b) \implies a = bc, \exists c \in A^*$

$$I(a) = I(b) \implies \begin{cases} a \in I(a) = I(b) \implies a = bc, \exists c \in A \\ b \in I(b) = I(a) \implies b = ad, \exists d \in A \end{cases}$$

Dunque si verifica che:

$$\begin{aligned} a = bc = adc &\implies a = adc \implies a(1 - dc) = 0 \implies \\ \implies \begin{cases} a = 0 \implies b = ad = 0 \implies a = bc = 0 \\ 1 - dc = 0 \implies dc = 1 \implies c = d^{-1} \implies c \in A^* \end{cases} \end{aligned}$$

□

Corollary 7

Dato il dominio di integrità \mathbb{Z} e dati $a, b \in \mathbb{Z}$, si verifica che:

$$I(a) = I(b) \iff a = \pm b$$

Dimostrazione:

- Poiché \mathbb{Z} è un dominio di integrità, dati $a, b \in \mathbb{Z}$ si ha che:

$$I(a) = I(b) \iff a = bc, \exists c \in \mathbb{Z}^*$$

- Tuttavia, siccome $\mathbb{Z}^* = \{1, -1\}$, si ha che:

$$I(a) = I(b) \iff a = bc, c = 1 \vee c = -1 \iff a = \pm b$$

□

4.4 Elementi irriducibili e primi

Definition 29. Elementi irriducibili e primi

Dato un anello commutativo A e un elemento $a \in A$, definiamo a come **elemento irriducibile** se e solo se:

$$a \neq 0, a \notin A^*, a = bc \implies b \in A^* \vee c \in A^*$$

Definiamo invece a come **elemento primo** se e solo se:

$$a \neq 0, a \notin A^*, a \mid bc \implies a \mid b \vee a \mid c$$

Attenzione: la definizione di elemento primo non coincide con la "normale" definizione di numero primo

Definition 30. Insieme dei numeri interi primi

Definiamo come **insieme dei numeri interi primi** l'insieme:

$$\mathbb{P} : \{p \in \mathbb{N}_{>1} \mid \nexists y \in \mathbb{N} - \{1, p\} \text{ t.c. } y \mid a\}$$

Attenzione: gli elementi appartenenti a tale insieme coincidono con la "normale" definizione di **numero primo**

Observation 16

Dati un elemento $p \in \mathbb{P}$, si verifica che

$$p \in \mathbb{P} \implies p \text{ elemento primo}$$

Dimostrazione:

- Poiché $\mathbb{P} \subseteq \mathbb{N} \subseteq \mathbb{Z}$, allora $p \in \mathbb{P} \implies p \in \mathbb{Z}$
- Supponiamo che $p \mid ab$, dove $ab \in \mathbb{Z}$, dunque necessariamente p apparterrà alla fattorizzazione di ab , implicando che $p \mid a \vee p \mid b$

□

Observation 17

Dato un dominio di integrità A ed un elemento $a \in A$, si verifica che

$$a \text{ elemento primo} \implies a \text{ elemento irriducibile}$$

Dimostrazione:

- Se $a \in A$ è primo, allora per definizione si ha che $a \neq 0, a \notin A^*$.
- Se $a = bc$, allora si ha che $a \mid a \implies a \mid bc \implies a \mid b \vee a \mid c$
- A questo punto, si ha che:

$$a \mid b \implies b = ad, \exists d \in A \implies a = bc = adc \implies a = adc \implies a(1 - cd) = 0$$

- Siccome $a \neq 0$, allora:

$$a(1 - cd) = 0, a \neq 0 \implies 1 - cd = 0 \implies cd = 1 \implies c = d^{-1} \implies c \in A^*$$

- Analogamente, dimostriamo che $a \mid c \implies b \in A^*$
- Dunque, concludiamo che se a è primo allora esso è anche irriducibile:

$$a \text{ primo} \mid a = bc \implies a \mid b \vee a \mid c \implies b \in A^* \vee c \in A^*$$

□

Proposition 15

Dato il dominio di integrità \mathbb{Z} e un elemento $p \in \mathbb{Z} \mid p \geq 2$, le seguenti condizioni sono equivalenti:

- $p \in \mathbb{P}$
- p è un elemento primo
- p è un elemento irriducibile

Dimostrazione:

- Per dimostrazione precedente, sappiamo che

$$p \in \mathbb{P} \implies p \text{ elemento primo} \implies p \text{ elemento irriducibile}$$

- Supponiamo che $p \geq 2 \in \mathbb{Z}$ sia irriducibile e che esistano $a, b \in \mathbb{N}$, tali che:

$$p = ab \in \mathbb{N} \subseteq \mathbb{Z} \implies a \in \mathbb{Z}^* \vee b \in \mathbb{Z}^*$$

- Poiché $\mathbb{Z}^* = \{-1, 1\}$ e poiché $a, b \in \mathbb{N}$, allora ne segue che:

$$a \in \mathbb{Z}^* \vee b \in \mathbb{Z}^* \implies a = 1 \vee b = 1$$

- Se $a \in \mathbb{Z}^*, b \in \mathbb{Z}^*$, allora

$$a \in \mathbb{Z}^*, b \in \mathbb{Z}^* \implies a = 1, b = 1 \implies p = 1$$

contraddicendo l'ipotesi per cui $p \geq 2$, dunque si tratta di un caso impossibile

- Se $a \in \mathbb{Z}^*, b \notin \mathbb{Z}^*$, allora

$$a \in \mathbb{Z}^* \implies a = 1 \implies p = b \implies b \mid p \vee 1 \mid p, b = p$$

- Se $a \notin \mathbb{Z}^*, b \in \mathbb{Z}^*$, allora

$$b \in \mathbb{Z}^* \implies b = 1 \implies p = a \implies a \mid p \vee 1 \mid p, a = p$$

- Dunque, in entrambi i casi possibili si ottiene che

$$p \text{ elemento irriducibile} \implies p \in \mathbb{P}$$

□

Proposition 16. Dominio di integrità \mathbb{Z}_p

Dato l'anello commutativo \mathbb{Z}_n , si ha che

$$\mathbb{Z}_n \text{ dominio di integrità} \iff n \in \mathbb{P}$$

Nel caso in cui $n \in \mathbb{P}$, per comodità utilizziamo la **notazione** \mathbb{Z}_p .

Dimostrazione:

- Supponiamo per assurdo che \mathbb{Z}_n sia dominio di integrità e che $n \notin \mathbb{P}$, implicando che:

$$\begin{aligned} n \notin \mathbb{P} &\implies ab = n, \exists a, b \notin \mathbb{Z}^*, 0 < a, b < n \implies \\ &\implies [ab] = [n] = [0] \in \mathbb{Z}_n \implies [a][b] = [0] \implies [a] = [0] \vee [b] = [0] \end{aligned}$$

Tuttavia, per ipotesi si ha che $a, b > 0 \implies [a] \neq 0, [b] \neq 0$, creando una contraddizione, dunque l'unica possibilità è che $n \in \mathbb{P}$

- Supponiamo per assurdo che $n \in \mathbb{P}$ e che \mathbb{Z}_n non sia dominio di integrità, implicando che:

$$\begin{aligned} \exists [a] \neq [0] \in \mathbb{Z}_n \text{ t.c. } [a] \mid [0] &\implies [0] = [a][b], \exists [b] \neq [0] \in \mathbb{Z}_n \implies \\ &\implies [0] = [ab] \iff ab \equiv 0 \pmod{n} \iff n \mid ab - 0 \end{aligned}$$

Poiché $n \in \mathbb{P}$, si ha che:

$$\begin{aligned} n \mid ab &\implies n \mid a \vee n \mid b \implies a \equiv 0 \pmod{n} \vee b \equiv 0 \pmod{n} \implies \\ &\implies [a] = [n] = [0] \vee [b] = [n] = [0] \end{aligned}$$

Tuttavia, per ipotesi si ha che $a, b \neq 0 \implies [a], [b] \neq [0]$, creando una contraddizione, dunque l'unica possibilità è che \mathbb{Z}_n sia dominio di integrità

□

4.5 Massimo comun divisore

Definition 31. Dominio ad ideali principali

Dato un dominio di integrità A , definiamo A come **dominio ad ideali principali** se e solo se considerato un qualsiasi $I \leq A$ ideale si ha che:

$$\exists d \in I \mid I = I(d)$$

In altre parole, ogni ideale coincide esattamente con un ideale principale

Proposition 17

Il dominio di integrità \mathbb{Z} è un **dominio ad ideali principali**

Dimostrazione:

- Supponiamo che esista $I \leq \mathbb{Z}$ ideale tale che $I = \{0\}$. In tal caso, si ha che $I = I(0)$
- Supponiamo quindi che $I \neq \{0\}$, implicando che per definizione stessa di ideale si abbia che:

$$\forall n \in I \implies -n \in I$$

Dunque, possiamo considerare direttamente il sottoinsieme $I_{>0}$, poiché per i numeri negativi basterebbe considerare il loro opposto.

- Siccome $I_{>0} \subseteq \mathbb{N}$, per il principio del buon ordinamento si ha che

$$\exists d \in I_{>0} \mid d \text{ è il minimo di } I_{>0}$$

- Dimostriamo quindi che $I = I(d)$:

- Dato $x \in I(d)$, si ha che:

$$x \in I(d) \implies \exists y \in \mathbb{Z} \mid x = dy$$

- Siccome $d \in I_{>0} \subseteq I$, allora $x = dy \in I$
- Dato $x \in I$, per il teorema della divisione con resto euclidea si ha che:

$$\exists! q, r \in \mathbb{Z}, 0 \leq r, d \mid x = dq + r \implies r = x - dq \in I$$

- Assumiamo per assurdo che $r \neq 0$, implicando che $r > 0$ e dunque che $r \in I_{>0}$. Tuttavia, poiché $r < d$, allora ne seguirebbe che d non sia il minimo di $I_{>0}$.
- Dunque, l'unica possibilità è che $r = 0$, implicando che:

$$x = dq + r = dq + 0 = dq \implies x = dq \implies x \in I(d)$$

□

Definition 32. Massimo comun divisore (MCD)

Dato il dominio ad ideali principali \mathbb{Z} e degli elementi $a_1, \dots, a_n \in \mathbb{Z}$, si ha che:

$$\exists! d \in \mathbb{N} \mid I(a_1, \dots, a_n) = I(d)$$

dove $d := MCD(a_1, \dots, a_n)$, ossia è il **massimo comun divisore** di a_1, \dots, a_n

In altre parole, si ha che:

$$\exists x_1, \dots, x_n \in \mathbb{Z} \mid a_1x_1 + \dots + a_nx_n = d$$

che definiamo come **identità di Bezout**.

Dimostrazione:

- Per ogni divisore comune di a_1, \dots, a_n , ossia $\forall k \in \mathbb{Z}$ tali che $k \mid a_i, \forall i \in [1, n]$, si ha che:

$$k \mid a_i, \forall i \in [1, n] \implies a_i = kb_i, \exists b_i \in \mathbb{Z}$$

- Dunque, si verifica facilmente che:

$$\begin{aligned} d \in I(d) = I(a_1, \dots, a_n) &\implies \exists x_1, \dots, x_n \mid \underbrace{d = a_1x_1 + \dots + a_nx_n}_{\text{Identità di Bezout}} \implies \\ &\implies d = (kb_1)x_1 + \dots + (kb_n)x_n = k(b_1x_1 + \dots + b_nx_n) \implies k \mid d \end{aligned}$$

- Dunque, poiché ogni divisore in comune di a_1, \dots, a_n divide anche d , si ha che d è il massimo comun divisore di a_1, \dots, a_n

•

□

Proposition 18

Dato l'anello commutativo \mathbb{Z}_n e dato $0 < a < n$ si ha che:

$$[a] \in \mathbb{Z}_n^* \iff MCD(a, n) = 1$$

Dimostrazione:

- Se $[a] \in \mathbb{Z}_n^*$ si ha che:

$$\exists 0 < b < n \mid [a][b] = 1 \iff ab \equiv 1 \pmod{n} \iff \exists k \in \mathbb{Z} \mid 1 = ab + nk$$

Posto $d := MCD(a, n) > 0$, si ha che:

$$1 = ab + nk \in I(a, n) = I(d) \implies 1 \in I(d) \implies \exists p \in \mathbb{Z} \mid 1 = dp \implies d = p = \pm 1$$

Poiché $d > 0$, l'unico caso possibile è $d = 1$

- Viceversa, supponendo che $MCD(a, n) = 1$ si ha che:

$$\begin{aligned} I(d) = I(a, n) &\implies d \in I(a, n) \implies \exists b, k \in \mathbb{Z} \mid d = ab + nk \implies \\ &\implies [1] = [ab + nk] \in \mathbb{Z}_n \implies [a][b] + [n][k] = [a][b] + [0][k] = [a][b] \\ &\implies [b] = [a]^{-1} \implies [a] \in \mathbb{Z}_n^* \end{aligned}$$

□

Corollary 8. Campo \mathbb{Z}_p

Dato $p \in \mathbb{P}$, il dominio di integrità \mathbb{Z}_p è un **campo**

Dimostrazione:

- Poiché $\nexists y \in \mathbb{Z} - \{1, p\}$ tale che $y \mid p$, allora:

$$MCD(a, p) = 1, \forall 0 < a < p \iff [a] \in \mathbb{Z}_p^*, \forall 0 < a < p \implies \mathbb{Z}_p^* = \mathbb{Z}_p - \{0\}$$

□

Theorem 19

Dato l'anello commutativo \mathbb{Z}_n e data la seguente equazione:

$$ax \equiv b \pmod{n}$$

Posto $d := MCD(a, n)$ si verifica che:

- Se $d \nmid b$, allora $\nexists x \in \mathbb{Z}_n \mid ax = b \pmod{n}$ (**non esistono soluzioni**)
- Se $d \mid b$, allora posti $p := \frac{a}{d}, q := \frac{b}{d}, m := \frac{n}{d}$, l'equazione è **equivalente** a:

$$ax \equiv b \pmod{n} \iff px \equiv q \pmod{m}$$

Dimostrazione:

- Prima di tutto, affermiamo che se l'equazione ammette una soluzione $x \in \mathbb{Z}$, allora

$$ax \equiv b \pmod{n} \iff ax = b + nk, \exists k \in \mathbb{Z} \iff ax - nk = b$$

- Poiché $d := MCD(a, n)$, si ha che

$$d \mid a, d \mid n \implies d \mid ax, d \mid nk \implies d \mid ax - nk = b$$

- Viceversa, ciò dimostra che se $d \nmid b$, allora tale equazione non potrebbe ammettere soluzioni.
- Supponiamo quindi che $d \mid b$ e poniamo $p := \frac{a}{d}, q := \frac{b}{d}, m := \frac{n}{d}$ (implicando quindi che $a = pd, b = qd, n = md$). Dunque si verifica che:

$$\begin{aligned} ax \equiv b \pmod{n} &\iff pdx \equiv qd \pmod{md} \iff \\ &\iff dp x = dq + dm k, \exists k \in \mathbb{Z} \iff px = q + mk \iff px \equiv q \pmod{m} \end{aligned}$$

□

4.5.1 Algoritmo di Euclide

Lemma 20

Dati tre elementi $a, b, c \in \mathbb{Z}$, si ha che:

$$a \mid b, a \mid c \implies a \mid z, \forall z \in I(b, c)$$

Dimostrazione:

- Se $a \mid b$ e che $a \mid c$, si ha che:

$$\begin{aligned} z \in I(b, c) &\iff z = bx + cy, \exists x, y \in \mathbb{Z} \implies z = (ak)x + (ah)c, \exists k, h \in \mathbb{Z} \implies \\ &\implies z = a(kx) + a(hc) = a(kx + hc) \implies a \mid z \end{aligned}$$

□

Method 1. Algoritmo di Euclide

Siano $a, b \in \mathbb{Z}$ e sia $d := MCD(a, b)$. Il seguente **algoritmo di Euclide** permette di calcolare d :

1. Assumiamo $0 < a \leq b$ poniamo $r_0 := b$ e $r_1 := a$
2. Poniamo $r_{i+1} := r_{i-1} \pmod{r_i}$ ad ogni iterazione, da cui ne segue che $r_{i-1} = r_i q_i + r_{i+1}$, ripetendo tale operazione fino a quando $r_{i+1} = 0$
3. All'n-esima iterazione, ossia quando $r_{n+1} = 0$, si ha che $MCD(a, b) = r_n$

Dimostrazione correttezza algoritmo:

- Poiché $I(a, b) = I(-a, b) = I(a, -b) = I(-a, -b)$, supponiamo che $0 < a, b$.
- Inoltre, poiché $I(a, b) = I(b, a)$, $MCD(0, b) = 0$ e $MCD(a, 0) = 0$, supponiamo che $0 < a \leq b$.
- Siccome $r_0 := b, r_1 := a \in I(a, b)$, si ha che:

$$r_2 \equiv r_0 \pmod{r_1} \iff r_0 = r_1 q_1 + r_2 \iff r_2 = r_0 + r_1 q_1 \in I(a, b) = I(d)$$

- Supponiamo per ipotesi induttiva che $r_i \in I(a, b) = I(d), \forall i \in [0, n]$.

Dimostriamo quindi il passo induttivo:

$$r_{i+1} \equiv r_{i-1} \pmod{r_i} \iff r_{i-1} = r_i q_1 + r_{i+1} \iff r_{i+1} = r_{i-1} + r_i q_i \in I(a, b) = I(d)$$

- Di conseguenza, si ha che

$$r_i \in I(a, b) = I(d), \forall i \in [0, n] \iff r_i = dp, \exists p \in \mathbb{Z} \iff d \mid r_i$$

In particolare, quindi, si ha che $d \mid r_n$

- Poiché l'algoritmo termina quando $r_{n+1} = 0$, ne segue che:

$$r_{n+1} \equiv r_{n-1} \pmod{r_n} \iff 0 \equiv r_{n-1} \pmod{r_n} \iff r_{n-1} = r_n q_n \iff r_n \mid r_{n-1}$$

- Siccome $r_n \mid r_n$ e $r_n \mid r_{n-1}$, per il lemma precedente si ha che:

$$r_n \equiv r_{n-2} \pmod{r_{n-1}} \iff r_{n-2} = r_{n-1} q_{n-1} + r_n \in I(r_{n-1}, r_n) \implies r_n \mid r_{n-2}$$

- A questo punto, procedendo analogamente si ha che

$$r_n \mid r_n, r_n \mid r_{n-1} \implies r_n \mid r_{n-2}$$

$$r_n \mid r_{n-1}, r_n \mid r_{n-2} \implies r_n \mid r_{n-3}$$

...

$$r_n \mid r_2, r_n \mid r_1 \implies r_n \mid r_0$$

- Dunque, poiché $d := MCD(a, b)$ si ha che:

$$r_n \mid a, r_n \mid b \implies r_n \mid d$$

- Infine, siccome $d, r_n \in \mathbb{N}$ (sezione 3.2) si ha che:

$$d \mid r_n, r_n \mid d \implies d = r_n$$

□

Esempi:

- Vogliamo calcolare $MCD(448, 216)$. Poniamo quindi inizialmente $r_0 = 448$ e $r_1 = 216$. Applicando l'algoritmo abbiamo quindi che:

$$r_0 = r_1 \cdot q_1 + r_2$$

$$448 = 216 \cdot 2 + 16$$

$$216 = 16 \cdot 13 + 8$$

$$16 = 8 \cdot 2 + 0$$

Dunque, otteniamo che $MCD(448, 216) = 8$

- Vogliamo calcolare l'**identità di Bezout** per $b = 216$ e $a = 448$ ossia i due valori x e y tali che:

$$x, y \in \mathbb{Z} \mid MCD(488, 216) = 216x + 448y$$

Tramite l'**algoritmo di Euclide** utilizzato nell'esercizio precedente, sappiamo che $MCD(488, 216) = 8$. Poniamo quindi:

$$216x + 448y = 8$$

A questo punto, ripercorrendo al contrario i calcoli dell'algoritmo di Euclide, otteniamo che:

$$216x + 448y = 8$$

$$216x + 448y = 216 - 16 \cdot 13$$

$$216x + 448y = 216 - (448 - 216 \cdot 2) \cdot 13$$

$$216x + 448y = 216(1 + 13 \cdot 2) - 448 \cdot 13$$

$$216x + 448y = 216(27) + 448(-13)$$

Otteniamo quindi che $x = 27$ e $y = -13$

- Vogliamo calcolare l'identità di Bezout e MCD per $a = 1470$, $b = 8316$ e $c = 12600$:

$$MCD(a, b, c) = MCD(a, MCD(b, c)) = MCD(MCD(a, b), c)$$

$$- d := MCD(b, c) = MCD(8316, 12600)$$

$$12600 := 8316 \cdot 1 + 4284$$

$$8316 := 4284 \cdot 1 + 4032$$

$$4284 := 4032 \cdot 1 + 252$$

$$4032 := 252 \cdot 16 + 0$$

dunque $d = 252$

- L'identità di Bezout per $MCD(8316, 12600) = 252 = 8316x + 12600y$ corrisponde a:

$$8316x + 12600y = 252$$

$$8316x + 12600y = 4284 - 4032$$

$$8316x + 12600y = (12600 - 8316) - (8316 - 4284)$$

$$8316x + 12600y = (12600 - 8316) - (8316 - (12600 - 8316))$$

$$8316x + 12600y = 12600 - 8316 - 8316 + 12600 - 8316$$

$$8316x + 12600y = 12600(2) + 8316(-3)$$

dunque $x = -3, y = 2$

- $p := MCD(a, d) = MCD(1470, 252)$

$$1470 = 252 \cdot 5 + 210$$

$$252 = 210 \cdot 1 + 42$$

$$210 = 42 \cdot 5 + 0$$

dunque $p = 42$

- L'identità di Bezout per $MCD(1470, 252) = 42 = 1470x + 252y$ corrisponde a:

$$1470z + 252w = 42$$

$$1470z + 252w = 252 - 210$$

$$1470z + 252w = 252 - (1470 - 252 \cdot 5)$$

$$1470z + 252w = 1470(-1) + 252(6)$$

dunque $x = -1, y = 6$

- L'identità di Bezout per $MCD(1470, 8316, 12600) = 42 = 1470x + 8316y + 12600z$ corrisponde a:

$$1470x + 8316y + 12600z = 42$$

$$1470x + 8316y + 12600z = 1470(-1) + (12600(2) + 8316(-3))(6)$$

$$1470x + 8316y + 12600z = 1470(-1) + 12600(12) + 8316 \cdot (-18)$$

dunque $x = -1, y = 12, z = -18$

4.5.2 Approfondimento sull'Identità di Bezout

Grazie all'algoritmo di Euclide, possiamo trovare due **soluzioni particolari** all'equazione dell'**identità di Bezout**, ossia $ax + by = MCD(a, b)$, per poi trovare tutte le soluzioni in grado di risolvere l'equazione:

Proposition 21

Data l'equazione $ax + by = d$, dove $d := MCD(a, b)$, e date x_0 e y_0 due soluzioni particolari dell'equazione, la soluzione ammette **infinite soluzioni** nella seguente forma:

$$x = x_0 + \frac{m}{a}k, \forall k \in \mathbb{Z} \quad y = y_0 - \frac{m}{b}k, \forall k \in \mathbb{Z}$$

dove $m := mcm(a, b)$, ossia il minimo comune multiplo tra a e b

Dimostrazione:

- Innanzitutto, verifichiamo che le soluzioni possibili siano effettivamente valide:

$$a(x_0 + \frac{m}{a}k) + b(y_0 - \frac{m}{b}k) = d$$

$$ax_0 + mk + by_0 - mk = d$$

$$ax_0 + by_0 = d$$

- A questo punto, verifichiamo che tali soluzioni appaiano solo nella forma indicata:

$$\begin{aligned} \begin{cases} ax_0 + by_0 = d \\ ax_1 + by_1 = d \end{cases} &\implies (ax_1 + by_1) - (ax_0 + by_0) = d - d \implies \\ a(x_1 - x_0) + b(y_1 - y_0) &= 0 \implies a(x_1 - x_0) = -b(y_1 - y_0) \implies \\ &\implies a(x_1 - x_0) = b(y_0 - y_1) \end{aligned}$$

- Posto $N := a(x_1 - x_0) = b(y_0 - y_1)$, si ha che $a \mid N$ e $b \mid N$, implicando che N sia un multiplo di $m := mcm(a, b)$. Dunque si ha che $\exists k \in \mathbb{Z} \mid N = mk$:

$$\begin{cases} a(x_1 - x_0) = N = mk \\ b(y_0 - y_1) = N = mk \end{cases} \implies \begin{cases} x_1 - x_0 = \frac{m}{a}k \\ y_0 - y_1 = \frac{m}{b}k \end{cases} \implies \begin{cases} x_1 = x_0 + \frac{m}{a}k \\ y_1 = y_0 - \frac{m}{b}k \end{cases}$$

□

4.5.3 Criteri di divisibilità

Sia $a \in \mathbb{Z}$ con la sua **rappresentazione decimale**:

$$a = a_k \cdot 10^k + \dots + a_0 \cdot 10^0 = \sum_{i=0}^k a_i \cdot 10^i \text{ dove } a_i \in \{0, \dots, 9\}$$

Osserviamo che:

- $10 \equiv 1 \pmod{3} \implies 10x \equiv x \pmod{3}$
- $10 \equiv 1 \pmod{9} \implies 10x \equiv x \pmod{9}$
- $10 \equiv -1 \pmod{11} \implies 10x \equiv -x \pmod{11}$

Quindi:

- In \mathbb{Z}_3 si ha che

$$a = \sum_{i=0}^k a_i \cdot 10^i \equiv \left[\sum_{i=0}^k a_i \cdot (1)^i \right] \pmod{3}$$

- In \mathbb{Z}_9 si ha che

$$a = \sum_{i=0}^k a_i \cdot 10^i \equiv \left[\sum_{i=0}^k a_i \cdot (1)^i \right] \pmod{9}$$

- In \mathbb{Z}_{11} si ha che

$$a = \sum_{i=0}^k a_i \cdot 10^i \equiv \left[\sum_{i=0}^k a_i \cdot (-1)^i \right] \pmod{11}$$

Observation 18

Dati $x, y, k \in \mathbb{Z}_n$, si ha che:

$$x \equiv y \pmod{n}, k \mid n \implies x \equiv y \pmod{k}$$

Dimostrazione:

$$x \equiv y \pmod{n} \iff y - x = nq = (kp)q = k(pq) \in I(k) \implies x \equiv y \pmod{k}$$

□

Esempi:

- Vogliamo sapere se $3 \mid 129383716$. Siccome siamo in \mathbb{Z}_3 abbiamo che:

$$129383716 \equiv [6 + 1 + 7 + 3 + 8 + 3 + 9 + 2 + 1] \pmod{3} \implies 129383716 \equiv 40 \pmod{3}$$

Tuttavia, siccome $3 \nmid 40$, ne segue che $3 \nmid 129383716$

- Vogliamo sapere se $3 \mid 129383716$. Siccome siamo in \mathbb{Z}_{11} abbiamo che:

$$129383716 \equiv [6 - 1 + 7 - 3 + 8 - 3 + 9 - 2 + 1](\text{mod } 11) \implies 129383716 \equiv 22(\text{mod } 11)$$

Dunque, siccome $11 \mid 22$, ne segue che $11 \mid 129383716$

4.6 Minimo comune multiplo

Definition 33. Minimo comune multiplo (mcm)

Dato il dominio ad ideali principali \mathbb{Z} e degli elementi $a_1, \dots, a_n \in \mathbb{Z}$, si ha che:

$$\exists! m \in \mathbb{N} \mid I(m) = I(a_1) \cap I(a_2) \cap \dots \cap I(a_n)$$

dove $m := \text{mcm}(a_1, \dots, a_n)$, ossia il **minimo comune multiplo** di a_1, \dots, a_n

Dimostrazione:

- Poiché $m \in I(m)$ si ha che:

$$m \in I(m) = I(a_1) \cap I(a_2) \cap \dots \cap I(a_n) \iff m = a_i k_i, \exists k_i \in \mathbb{Z}, \forall i \in [0, n] \implies a_i \mid m$$

dunque m è un multiplo in comune di a_1, \dots, a_n

- Per ogni multiplo comune di a_1, \dots, a_n , ossia $\forall k \in \mathbb{Z}$ tali che $a_i \mid k, \forall i \in [1, n]$, si ha che:

$$\begin{aligned} a_i \mid k, \forall i \in [1, n] &\implies k = a_i b_i, \exists b_i \in \mathbb{Z} \implies \\ \implies k \in I(a_i), \forall i \in [1, n] &\implies k \in I(a_1) \cap \dots \cap I(a_n) = I(m) \implies \\ \implies k \in I(m) &\implies k = mh, \exists h \in \mathbb{Z} \implies m \mid k \end{aligned}$$

- Dunque, poiché ogni multiplo in comune di a_1, \dots, a_n è multiplo anche di d , si ha che m è il minimo comune multiplo di a_1, \dots, a_n

□

Observation 19

Dato il dominio ad ideali principali \mathbb{Z} e dati $I_1, \dots, I_n \leq A$ ideali, $\exists! a_1, \dots, a_n \in \mathbb{Z}$ tali che :

- $I_1 + \dots + I_n = I(a_1, \dots, a_n) = I(d)$, dove $d := \text{MCD}(a_1, \dots, a_n)$
- $I_1 \cdot \dots \cdot I_n = I(a_1) \cdot \dots \cdot I(a_n) = I(a_1 \cdot \dots \cdot a_n)$
- $I_1 \cap \dots \cap I_n = I(a_1) \cap \dots \cap I(a_n) = I(m)$, dove $m := \text{mcm}(a_1, \dots, a_n)$

Dimostrazione:

- Poiché \mathbb{Z} è un dominio ad ideali principali si ha che

$$I_i = I(a_i), \exists! a_i \in \mathbb{Z}, \forall i \in [1, n]$$

- Di conseguenza, si ha che:

$$\begin{aligned} I_1 + \dots + I_n &= I(a_1) + \dots + I(a_n) = \{b_1 + \dots + b_n \mid b_i \in I(a_i), \forall i \in [1, n]\} = \\ &= \{b_1 + \dots + b_n \mid b_i = a_i x_i, \exists x_i \in \mathbb{Z}, \forall i \in [1, n]\} = \{a_1 x_1 + \dots + a_n x_n \mid x_i \in \mathbb{Z}, \forall i \in [1, n]\} = \\ &= I(a_1, \dots, a_n) = I(d) \end{aligned}$$

dove $d : MCD(a_1, \dots, a_n)$

- Preso $x \in I_1 \cdot \dots \cdot I_n$, si ha che:

$$\begin{aligned} x \in I_1 \cdot \dots \cdot I_n &= I(a_1) \cdot \dots \cdot I(a_n) \implies \\ \implies \exists b_{j_{a_i}} \in I(a_i), \forall i, j \in [1, n] \mid x &= a_1 b_{1_{a_1}} \cdot \dots \cdot a_n b_{1_{a_n}} + \dots + a_1 b_{n_{a_1}} \cdot \dots \cdot a_n b_{n_{a_n}} \implies \\ \implies x &= a_1 \cdot \dots \cdot a_n (b_{1_{a_1}} \cdot \dots \cdot b_{1_{a_n}} + \dots + b_{n_{a_1}} \cdot \dots \cdot b_{n_{a_n}}) \implies x \in I(a_1 \cdot \dots \cdot a_n) \end{aligned}$$

- Viceversa, si ha che

$$\begin{aligned} x \in I(a_1 \cdot \dots \cdot a_n) &\implies x = a_1 \cdot \dots \cdot a_n k, \exists k \in \mathbb{Z} \implies \\ \implies x &= a_1 \cdot \dots \cdot a_{n-1} (a_n k) \mid a_n k \in I(a_n), a_i \in I(a_i), \forall i \in [1, n-1] \implies \\ \implies x &\in I(a_1) \cdot \dots \cdot I(a_n) = I_1 \cdot \dots \cdot I_n \end{aligned}$$

Dunque, si ha che $I_1 \cdot \dots \cdot I_n = I(a_1 \cdot \dots \cdot a_n)$

- Infine, per dimostrazione precedente si ha che:

$$I_1 \cap \dots \cap I_n = I(a_1) \cap \dots \cap I(a_n) = I(m)$$

dove $m := mcm(a_1, \dots, a_n)$

□

4.6.1 Teorema fondamentale dell'aritmetica

Theorem 22. Teorema fondamentale dell'aritmetica

Dato il dominio ad ideali principali \mathbb{Z} e dati $a, b \in \mathbb{N}$, si ha che:

$$mcm(a, b) \cdot MCD(a, b) = ab$$

Attenzione: dati $a_1, \dots, a_n \in \mathbb{N} \mid n > 2 \in \mathbb{N}$, si ha che:

$$mcm(a_1, \dots, a_n) \cdot MCD(a_1, \dots, a_n) \neq a_1 \cdot \dots \cdot a_n$$

dunque tale teorema vale se e solo se $n = 2$

Dimostrazione:

- Se $a = 0 \vee b = 0$, allora:

$$mcm(a, b) = 0 \implies mcm(a, b) \cdot MCD(a, b) = 0 \cdot MCD(a, b) = 0 = ab$$

- Siano quindi $a, b > 0$. Considerando $n \in \mathbb{N} - \{0\}$, tale numero può essere scritto come una **fattorizzazione in numeri interi primi**, ossia:

$$\exists! n_2, n_3, n_5, \dots, n_p, \dots \text{ dove } p \in \mathbb{P}, n_p \in \mathbb{N} \mid n = 2^{n_2} \cdot 3^{n_3} \cdot \dots \cdot p^{n_p} \cdot \dots = \prod_{p \in \mathbb{P}} p^{n_p}$$

$$\text{dove } p \nmid n \implies n_p = 0$$

- Riscriviamo quindi a e b come:

$$a = \prod_{p \in \mathbb{P}} p^{a_p} \quad b = \prod_{p \in \mathbb{P}} p^{b_p}$$

- Poniamo inoltre $d := MCD(a, b)$ e $m := mcm(a, b)$, che per loro definizione corrispondono a:

$$d = \prod_{p \in \mathbb{P}} p^{\min(a_p, b_p)} \quad m = \prod_{p \in \mathbb{P}} p^{\max(a_p, b_p)}$$

- A questo punto, osserviamo che:

$$\min(a_p, b_p) = a_p \iff \max(a_p, b_p) = b_p$$

- Quindi, il prodotto tra d e m corrisponde a:

$$dm = \prod_{p \in \mathbb{P}} p^{\min(a_p, b_p)} \cdot \prod_{p \in \mathbb{P}} p^{\max(a_p, b_p)} = \prod_{p \in \mathbb{P}} p^{a_p + b_p} = \prod_{p \in \mathbb{P}} p^{a_p} \cdot \prod_{p \in \mathbb{P}} p^{b_p} = ab$$

□

Corollary 9. Calcolo del mcm

Dato il dominio ad ideali principali \mathbb{Z} e dati $a, b \in \mathbb{N}$, per il teorema fondamentale dell'aritmetica si ha che:

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

4.7 Teorema cinese dei resti

Lemma 23. Numeri coprimi ed mcm

Dato il dominio ad ideali principali \mathbb{Z} e dati $a_1, \dots, a_n \geq 2 \in \mathbb{N}$, si ha che:

$$MCD(a_i, a_j) = 1, \forall i \neq j \in \mathbb{N} \implies mcm(a_1, \dots, a_n) = a_1 \cdot \dots \cdot a_n$$

Inoltre, due elementi $a, b \in \mathbb{N} \mid MCD(a, b) = 1$, definiamo tali elementi come **coprimi**

Dimostrazione:

- Se a_1, \dots, a_n sono coprimi tra loro, si ha che

$$MCD(a_i, a_j) = 1, \forall i \neq j \in \mathbb{N} \implies \forall p \in \mathbb{P}, p \mid a_i \implies p \nmid a_j, \forall i \neq j \in \mathbb{N}$$

- Consideriamo anche la loro fattorizzazione in primi:

$$a_1 = \prod_{p \in \mathbb{P}} p^{a_{1,p}}, \quad a_2 = \prod_{p \in \mathbb{P}} p^{a_{2,p}}, \quad \dots, \quad a_n = \prod_{p \in \mathbb{P}} p^{a_{n,p}}$$

- Dati i due punti precedenti, si ha che:

$$a_{i,p} > 0 \implies a_{j,p} = 0, \forall j \neq i \implies \forall p \in \mathbb{P}, a_{1,p} + \dots + a_{n,p} = \max(a_{1,p}, \dots, a_{n,p})$$

- Ponendo $m := mcm(a_1, \dots, a_n)$ abbiamo che:

$$m = \prod_{p \in \mathbb{P}} p^{\max(a_{1,p}, \dots, a_{n,p})} = \prod_{p \in \mathbb{P}} p^{a_{1,p} + \dots + a_{n,p}} = \prod_{p \in \mathbb{P}} p^{a_{1,p}} \cdot \dots \cdot \prod_{p \in \mathbb{P}} p^{a_{n,p}} = a_1 \cdot \dots \cdot a_n$$

□

Lemma 24

Consideriamo la notazione $x(\bmod q)$, indicante la classe $[x] \in \mathbb{Z}_q$, dove $q \in \mathbb{N}$.

Dati $a_1, \dots, a_n \geq 2$ e posto $m := mcm(a_1, \dots, a_n)$, la seguente funzione è **ben definita** ed **iniettiva**

$$\varphi : \mathbb{Z}_m \rightarrow \mathbb{Z}_{a_1} \times \dots \times \mathbb{Z}_{a_n} : x(\bmod m) \mapsto (x(\bmod a_1), \dots, x(\bmod a_n))$$

Dimostrazione:

$$x \equiv x'(\bmod m) \iff x' - x \in I(m) = I(a_1) \cap \dots \cap I(a_n) \iff$$

$$\iff x' - x \in I(a_i), \forall i \in [1, n] \iff \begin{cases} x' - x \in I(a_1) \\ x' - x \in I(a_2) \\ \vdots \\ x' - x \in I(a_n) \end{cases} \iff \begin{cases} x \equiv x'(\bmod a_1) \\ x \equiv x'(\bmod a_2) \\ \vdots \\ x \equiv x'(\bmod a_n) \end{cases}$$

□

Theorem 25. Teorema cinese dei resti

Dati $a_1, \dots, a_n \geq 2 \in \mathbb{N}$ **coprime tra loro**, dunque tali che $MCD(a_i, a_j) = 1, \forall i \neq j$ e dati $0 \leq b_i < a_i \in \mathbb{N}, \forall i \in [1, n]$, il seguente sistema di congruenze (se compatibile) ammette un'**unica soluzione**

$$\begin{cases} x \equiv b_1 \pmod{a_1} \\ x \equiv b_2 \pmod{a_2} \\ \vdots \\ x \equiv b_n \pmod{a_n} \end{cases} \iff \exists! x \pmod{m}$$

dove $m := mcm(a_1, \dots, a_n) = a_1 \cdot \dots \cdot a_n$ e dove $x \pmod{m}$ indica la classe $[x] \in \mathbb{Z}_m$

Dimostrazione:

- Per il lemma precedente, la seguente funzione è ben definita ed iniettiva

$$\varphi : \mathbb{Z}_n \rightarrow \mathbb{Z}_{a_1} \times \dots \times \mathbb{Z}_{a_n} : x \pmod{m} \mapsto (x \pmod{a_1}, \dots, x \pmod{a_n})$$

- Inoltre, posto $m := mcm(a_1, \dots, a_n)$, per il lemma precedente si ha che:

$$MCD(a_i, a_j) = 1, \forall i \neq j \implies m = a_1 \cdot \dots \cdot a_n$$

- A questo punto, notiamo che:

$$|\mathbb{Z}_{a_1} \times \dots \times \mathbb{Z}_{a_n}| = |\mathbb{Z}_{a_1}| \cdot \dots \cdot |\mathbb{Z}_{a_n}| = a_1 \cdot \dots \cdot a_n = m = |\mathbb{Z}_m|$$

- Di conseguenza, poiché $|\mathbb{Z}_{a_1} \times \dots \times \mathbb{Z}_{a_n}| = |\mathbb{Z}_m|$ e poiché φ è iniettiva, ne segue che φ possa essere iniettiva se e solo se è suriettiva.
- Concludiamo quindi che $\exists! x \pmod{m}$ tale che

$$\varphi(x \pmod{m}) = (b_1 \pmod{a_1}, \dots, b_n \pmod{a_n})$$

implicando che $x \pmod{m}$ sia l'unica soluzione del sistema.

□

Esempi:

- Consideriamo il seguente sistema:

$$\begin{cases} x \equiv 2 \pmod{3} \\ x \equiv 3 \pmod{5} \\ x \equiv 2 \pmod{7} \end{cases}$$

- Poiché $x \equiv 2 \pmod{3} \iff x = 2 + 3a, \exists a \in \mathbb{Z}$, sostituendo $x = 2 + 3a$ dentro $x \equiv 3 \pmod{5}$ otteniamo che:

$$2 + 3a \equiv 3 \pmod{5}$$

- Impostiamo la seguente equazione, dove le seguenti classi di congruenza appartengono tutte a \mathbb{Z}_5 :

$$\begin{aligned} [2 + 3a] = [3] &\iff [2] + [3][a] = [3] \iff \\ \iff [3][a] = [3] - [2] &\iff [a] = [1][3]^{-1} \iff \\ \iff [a] = [1][2] &\iff [a] = [2] \end{aligned}$$

- Quindi si ha che $[a] = [2] \in \mathbb{Z}_5 \iff a \equiv 2(\text{mod } 5) \iff a = 2 + 5b, \exists b \in \mathbb{Z}$
- Sostituendo $x = 2 + 3(2 + 5b) = 8 + 15b$ dentro $x \equiv 2(\text{mod } 7)$, otteniamo che:

$$8 + 15b \equiv 2(\text{mod } 5)$$

- Ripetiamo quindi i passaggi analoghi a prima, stavolta lavorando in \mathbb{Z}_7 :

$$\begin{aligned} [8 + 15b] = [2] &\iff [8] + [15][b] = [2] \iff \\ \iff [15][b] = [2] - [8] &\iff [1][b] = [2] - [1] \iff [b] = [1] \end{aligned}$$

- Quindi si ha che $[b] = [1] \in \mathbb{Z}_7 \iff b \equiv 1(\text{mod } 7) \iff b = 1 + 7c, \exists c \in \mathbb{Z}$
- Infine, otteniamo che

$$x = 8 + 15(1 + 7c) = 23 + 105c, \exists c \in \mathbb{Z} \iff x \equiv 23(\text{mod } 105)$$

- Notiamo come $mcm(3, 5, 7) = 105$. Difatti, $x \equiv 23(\text{mod } 105)$ è l'unica soluzione del sistema:

$$\begin{cases} 23 \equiv 2(\text{mod } 3) \\ 23 \equiv 3(\text{mod } 5) \\ 23 \equiv 2(\text{mod } 7) \end{cases}$$

2. • Consideriamo il seguente sistema:

$$\begin{cases} x \equiv 6(\text{mod } 15) \\ x \equiv 9(\text{mod } 20) \end{cases}$$

- Poiché 15 e 20 non sono fattori primi, scomponiamo le due congruenze utilizzando il **teorema cinese dei resti**, in particolare la funzione φ :

$$x \equiv 6(\text{mod } 15) \iff \begin{cases} x \equiv 0(\text{mod } 3) \\ x \equiv 1(\text{mod } 5) \end{cases}$$

$$x \equiv 9(\text{mod } 20) \iff \begin{cases} x \equiv 1(\text{mod } 4) \\ x \equiv 4(\text{mod } 5) \end{cases}$$

- Il sistema iniziale, quindi, è equivalente a:

$$\begin{cases} x \equiv 6(\text{mod } 15) \\ x \equiv 9(\text{mod } 20) \end{cases} \iff \begin{cases} x \equiv 0(\text{mod } 3) \\ x \equiv 1(\text{mod } 5) \\ x \equiv 1(\text{mod } 4) \\ x \equiv 4(\text{mod } 5) \end{cases}$$

- Notiamo come il sistema sia **incompatibile**, poiché

$$x \equiv 1(\text{mod } 5) \iff x \not\equiv 4(\text{mod } 5)$$

dunque il sistema **non ammette alcuna soluzione**

3. • Consideriamo il seguente sistema:

$$\begin{cases} x \equiv 6(\text{mod } 15) \\ x \equiv 11(\text{mod } 20) \\ x \equiv 15(\text{mod } 21) \end{cases}$$

- Scomponendo in fattori primi si ha che:

$$x \equiv 6(\text{mod } 15) \iff \begin{cases} x \equiv 0(\text{mod } 3) \\ x \equiv 1(\text{mod } 5) \end{cases}$$

$$x \equiv 11(\text{mod } 20) \iff \begin{cases} x \equiv 3(\text{mod } 4) \\ x \equiv 1(\text{mod } 5) \end{cases}$$

$$x \equiv 15(\text{mod } 21) \iff \begin{cases} x \equiv 0(\text{mod } 3) \\ x \equiv 1(\text{mod } 7) \end{cases}$$

- Il sistema iniziale, quindi, è equivalente a:

$$\begin{cases} x \equiv 6(\text{mod } 15) \\ x \equiv 11(\text{mod } 20) \\ x \equiv 15(\text{mod } 21) \end{cases} \implies \begin{cases} x \equiv 0(\text{mod } 3) \\ x \equiv 1(\text{mod } 5) \\ x \equiv 3(\text{mod } 4) \\ x \equiv 1(\text{mod } 7) \end{cases}$$

- Poiché $x \equiv 0(\text{mod } 3) \iff x = 0 + 3a, \exists a \in \mathbb{Z}$, sostituendo nella seconda congruenza otteniamo che $3a \equiv 1(\text{mod } 5)$. Lavorando in \mathbb{Z}_5 quindi si ha che:

$$[3a] = [1] \iff [3][a] = [1] \iff$$

$$\iff [a] = [1][3]^{-1} \iff [a] = [2]$$

- Dunque $[a] = [2] \in \mathbb{Z}_5 \iff a \equiv 2(\text{mod } 5) \iff a = 2 + 5b, \exists b \in \mathbb{Z}$.

- Sostituendo nella terza congruenza otteniamo $x = 3(2 + 5b) = 6 + 15b \iff 6 + 15b \equiv 3 \pmod{4}$. Lavorando in \mathbb{Z}_4 si ha che:

$$\begin{aligned} [6 + 15b] &= [3] \iff [6] + [15][b] = [3] \iff \\ \iff [2] + [3][b] &= [3] \iff [3][b] = [3] - [2] \iff \\ \iff [b] &= [1][3]^{-1} \iff [b] = [3] \end{aligned}$$

- Dunque $[b] = [3] \in \mathbb{Z}_4 \iff b \equiv 3 \pmod{4} \iff b = 3 + 4c, \exists c \in \mathbb{Z}$
- Sostituendo nella quarta congruenza otteniamo $x = 6 + 15(3 + 4c) = 51 + 60c \iff 51 + 60c \equiv 1 \pmod{7}$. Lavorando in \mathbb{Z}_7 quindi si ha che:

$$\begin{aligned} [51 + 60c] &= [1] \iff [2] + [4][c] = [1] \iff [2] + [4][c] = [1] \iff \\ \iff [4][c] &= [1] - [2] \iff [4][c] = [-1] \iff [c] = [6][4]^{-1} \iff \\ \iff [c] &= [6][2] \iff [c] = [12] \iff [c] = [5] \end{aligned}$$

- Dunque $[c] = [2] \iff c \equiv 5 \pmod{7} \implies c = 5 + 7d, \exists d \in \mathbb{Z}$.
- Infine, otteniamo che

$$x = 51 + 60(5 + 7d) = 351 + 420d \implies x \equiv 351 \pmod{420}$$

che risulta essere l'unica soluzione del sistema. Difatti verifichiamo che:

$$\begin{cases} 351 \equiv 6 \pmod{15} \\ 351 \equiv 11 \pmod{20} \\ 351 \equiv 15 \pmod{21} \end{cases} \implies \begin{cases} 351 \equiv 0 \pmod{3} \\ 351 \equiv 1 \pmod{5} \\ 351 \equiv 3 \pmod{4} \\ 351 \equiv 1 \pmod{7} \end{cases}$$

- Vogliamo calcolare le ultime due cifre di 37^{37} . Poniamo quindi $x := 37^{37}$ e calcoliamo la classe di equivalenza $x \pmod{100}$.
 - Scomponiamo quindi $100 = 4 \cdot 25$ in modo da poter applicare il teorema cinese dei resti:
 - Calcoliamo la classe di equivalenza di x in \mathbb{Z}_4

$$[x] = [37^{37}] = [37]^{37} = [1]^{37} = [1]$$

- Calcoliamo la classe di equivalenza di x in \mathbb{Z}_{25}

$$\begin{aligned} [x] &= [37^{37}] = [37]^{37} = [12]^{37} = [12][12]^{36} = [12][(12)^2]^{18} = [12][144]^{18} = \\ &= [12][19]^{18} = [12][-6]^{18} = [12][(-6)^2]^9 = [12][36]^9 = [12][11]^9 = \\ &= [12][11][(11)^2]^4 = [12][11][121]^4 = [12][11][-4]^4 = [12][11][6] = [792] = [17] \end{aligned}$$

- Impostiamo quindi il seguente sistema e procediamo applicando il teorema cinese:

$$\begin{cases} x \equiv 1(\text{mod } 4) \\ x \equiv 17(\text{mod } 25) \end{cases}$$

- Abbiamo quindi che $x = 1 + 4k \implies 1 + 4k \equiv 17(\text{mod } 25)$:

$$\begin{aligned} [1] + [4][k] &= [17] \iff [4][k] = [16] \iff [k] = [16][4]^{-1} \iff \\ &\iff [k] = [16][19] \iff [k] = [304] \iff [k] = [4] \end{aligned}$$

- Dunque $k \equiv 4(\text{mod } 25) \implies k = 4 + 25j \implies x = 1 + 4(4 + 25j) = 17 + 100j$
- Quindi concludiamo che $x \equiv 17(\text{mod } 100)$ e quindi che le ultime cifre di 37^{37} corrispondono a 17

5. • Vogliamo calcolare l'inverso di 193 in \mathbb{Z}_{240} . Per definizione, ciò equivale a calcolare $193x \equiv 1(\text{mod } 240)$
- Scomponiamo $240 = 24 \cdot 10$ e osserviamo che se $x \equiv y(\text{mod } n)$ e $d \mid n$ allora si ha che

$$x \equiv y(\text{mod } n) \iff y - x \in I(n) \iff y - x = nk = dhk, \exists h, k \in \mathbb{Z} \implies x \equiv y(\text{mod } d)$$

- Quindi, siccome $16 \mid 240, 3 \mid 240$ e $5 \mid 240$, impostiamo il seguente sistema

$$\begin{cases} 193x \equiv 1(\text{mod } 3) \\ 193x \equiv 1(\text{mod } 5) \\ 193x \equiv 1(\text{mod } 16) \end{cases}$$

- Riduciamo le classi di equivalenza del sistema:

- Riduciamo $193x \equiv 1(\text{mod } 3)$ in:

$$[193][x] = [1] \implies [1][x] = [1] \implies [x] = [1]$$

- Riduciamo $193x \equiv 1(\text{mod } 5)$ in:

$$[193][x] = [1] \implies [3][x] = [1] \implies [x] = [3]^{-1} \implies [x] = [2]$$

- Riduciamo $193x \equiv 1(\text{mod } 16)$ in:

$$[193][x] = [1] \implies [1][x] = [1] \implies [x] = [1]$$

- Riconduciamo quindi il sistema iniziale ad una versione semplificata sulla quale possiamo applicare il teorema cinese:

$$\begin{cases} 193x \equiv 1(\text{mod } 3) \\ 193x \equiv 1(\text{mod } 5) \\ 193x \equiv 1(\text{mod } 16) \end{cases} \implies \begin{cases} x \equiv 1(\text{mod } 3) \\ x \equiv 2(\text{mod } 5) \\ x \equiv 1(\text{mod } 16) \end{cases}$$

- Quindi si ha che $x = 1 + 16k \implies 1 + 16k \equiv 1 \pmod{3}$:

$$[1] + [16][k] = [1] \iff [k] = [0][16]^{-1} \iff [k] = [0]$$

- Dunque $k = 0 + 3j \implies x = 1 + 16(0 + 3j) = 1 + 48j \implies 1 + 48j \equiv 2 \pmod{5}$:

$$[1] + [48][j] = [2] \iff [j] = [1][3]^{-1} \iff [j] = [2]$$

- Infine $j = 2 + 5h \implies x = 1 + 48(2 + 5h) = 97 + 240h \implies x \equiv 97 \pmod{240}$
- Dunque $[197]^{-1} = [97] \in \mathbb{Z}_{240}$. Difatti, in \mathbb{Z}_{240} si ha che $[193][97] = [1]$

4.8 Piccolo teorema di Fermat

Lemma 26

Dato $p \in \mathbb{P}$ e dato $0 < k < p$ si ha che:

$$p \mid \binom{p}{k}$$

Dimostrazione:

- Poiché $p \in \mathbb{P}$, allora esso non potrà essere semplificato dal denominatore, dunque si ha che:

$$\binom{p}{k} = \frac{p!}{k! \cdot (p-k)!} = p \cdot \frac{(p-1)!}{k! \cdot (p-k)!} = ph \iff p \mid \binom{p}{k}$$

dove $h := \frac{(p-1)!}{k! \cdot (p-k)!} \in \mathbb{Z}$ per definizione di coefficiente binomiale

□

Esempio:

$$\binom{7}{3} = \frac{7!}{3! \cdot 4!} = \frac{7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2}{3 \cdot 2 \cdot 4 \cdot 3 \cdot 2} = 7 \cdot 5 \implies 7 \mid \binom{7}{3}$$

Corollary 10

Dato $p \in \mathbb{P}$, dato dato $0 < k < p$ e dato $[a] \in \mathbb{Z}_p$, si ha che:

$$\binom{p}{k} \cdot [a] = [0]$$

Dimostrazione:

- Per il lemma precedente si ha che

$$p \mid \binom{p}{k} \iff \binom{p}{k} = ph, \exists h \in \mathbb{Z}$$

- Di conseguenza, si ha che:

$$\binom{p}{k} \cdot [a] = ph \cdot [a] = [p][h][a] = [0][h][a] = [0], \exists h \in \mathbb{Z}$$

□

Lemma 27

Dato $p \in \mathbb{P}$ e dati $[a], [b] \in \mathbb{Z}_p$ si ha che:

$$([a] + [b])^p = [a]^p + [b]^p$$

Dimostrazione:

- Dato il **binomio di Newton** (dimostrato nella sezione 3.6), sappiamo che:

$$([a] + [b])^p = \sum_{k=0}^p \binom{p}{k} [a]^k [b]^{p-k}$$

- Se $k = 0 \vee k = p$, si ha che:

$$\binom{p}{0} = \binom{p}{p} = 1$$

- Se invece $0 < k < p$, per il corollario precedente sappiamo dato $[x] \in \mathbb{Z}_p$ si ha che:

$$p \mid \binom{p}{k} \implies \binom{p}{k} \cdot [x] = 0$$

- Di conseguenza, ogni termine della sommatoria, escluso il primo e l'ultimo, può essere ricondotto alla classe $[0]$:

$$\begin{aligned} ([a] + [b])^p &= \sum_{k=0}^p \binom{p}{k} [a]^k [b]^{p-k} = \binom{p}{0} [b]^p + \binom{p}{p} [a]^p + \sum_{k=1}^{p-1} \binom{p}{k} [a]^k [b]^{p-k} = \\ &= [b]^p + [a]^p + \sum_{k=1}^{p-1} [0] = [b]^p + [a]^p \end{aligned}$$

□

Corollary 11

Dato $p \in \mathbb{P}$ e dati $[a_1], \dots, [a_n] \in \mathbb{Z}_p \mid n \in \mathbb{N}$ si ha che:

$$([a_1] + \dots + [a_n])^p = [a_1]^p + \dots + [a_n]^p$$

Dimostrazione:

- Caso base ($n=1$):

$$[a_1]^p = [a_1]^p$$

- Caso base (n=2):

$$([a_1] + [a_2])^p = [a_1]^p + [a_2]^p$$

- Ipotesi induttiva:

$$([a_1] + \dots + [a_n])^p = [a_1]^p + \dots + [a_n]^p \mid n \in \mathbb{N}$$

- Passo induttivo:

$$\begin{aligned} ([a_1] + \dots + [a_n] + [a_{n+1}])^p &= (([a_1] + \dots + [a_n]) + [a_{n+1}])^p = \\ &= ([a_1] + \dots + [a_n])^p + [a_{n+1}]^p = [a_1]^p + \dots + [a_n]^p + [a_{n+1}]^p \end{aligned}$$

□

Theorem 28. Piccolo teorema di Fermat

Dato il campo \mathbb{Z}_p dove $p \in \mathbb{P}$, dato $[a] \in \mathbb{Z}_p$ si ha che:

$$a^p \equiv a \pmod{p}$$

Dimostrazione:

- Caso base (a=0):

$$[0]^p = [0]$$

- Ipotesi induttiva:

$$[a]^p = [a]$$

- Passo induttivo:

$$[a + 1]^p = ([a] + [1])^p = [a]^p + [1]^p = [a]^p + [1] = [a] + [1] = [a + 1]$$

□

Corollary 12

Dato il campo \mathbb{Z}_p dove $p \in \mathbb{P}$, dato $[a] \in \mathbb{Z}_p$ si ha che:

$$a^{p+k} \equiv a^{k+1} \pmod{p}$$

In particolare, se $k = -2$, si ha che:

$$a^{p-2} \equiv a^{-1} \pmod{p}$$

dunque è sempre possibile calcolare comodamente $a^{-1} \in \mathbb{Z}_p$

Dimostrazione:

- Per il piccolo teorema di Fermat, si ha che:

$$\begin{aligned} [a]^p = [a] &\iff [a]^k [a]^p = [a][a]^k \iff [a]^{p+k} = [a][a]^{k+1-1} \iff \\ &\iff [a]^{p+k} = [a][a]^{-1}[a]^{k+1} \iff [a]^{p+k} = [1][a]^{k+1} \iff [a]^{p+k} = [a]^{k+1} \end{aligned}$$

□

Esempio:

- Vogliamo trovare $[4]^{-1} \in \mathbb{Z}_{13}$. Per il corollario appena mostrato, si ha che:

$$\begin{aligned} 4^{-1} &\equiv 4^{13-2} \pmod{13} \iff [4]^{-1} = [4]^{11} = [4][4]^{10} = [4][4^2]^5 = [4][16]^5 = \\ &= [4][3]^5 = [4][3]^2[3]^3 = [4][9][27] = [4][9][1] = [36] = [10] \end{aligned}$$

4.9 Ordine di un elemento di un gruppo

Definition 34. Sottogruppo ciclico ed Ideale d'ordine

Sia G un gruppo. Dato $g \in G$, definiamo il **sottogruppo ciclico** $H(g) \leq G$ e l'**ideale d'ordine** $I(g) \leq \mathbb{Z}$ come:

$$\begin{aligned} H(g) &: \{g^n \mid n \in \mathbb{Z}\} \\ I(g) &: \{n \in \mathbb{Z} \mid g^n = e\} \end{aligned}$$

Dimostrazioni:

- $H \leq G$

$$\begin{aligned} - g^0 = e &\implies e \in H(g) \\ - g^n, g^m \in H(g) &\implies g^n \cdot g^m = g^{n+m} \implies g^{n+m} \in H(g) \\ - g^n \in H(g) &\implies (g^n)^{-1} = g^{-n} \implies g^{-n} \in H(g) \end{aligned}$$

- $I(g) \leq \mathbb{Z}$ ideale

$$\begin{aligned} - g^0 = e &\implies 0 \in I(g) \\ - n, m \in I(g) &\implies g^n = g^m = e \implies g^{n+m} = g^n \cdot g^m = e \implies n+m \in I(g) \\ - n \in I(g) &\implies g^{-n} = (g^n)^{-1} = e^{-1} = e \implies -n \in I(g) \\ - n \in I(g), k \in \mathbb{Z} &\implies g^{nk} = (g^n)^k = e^k = e \implies kn \in I(g) \end{aligned}$$

□

Definition 35. Ordine di un elemento

Sia G un gruppo. Dato $g \in G$, definiamo l'**ordine di** g come:

$$o(g) := |H(g)|$$

Proposition 29

Sia G un gruppo. Dato $g \in G$, si ha che $\exists! d \in \mathbb{N} \mid I(g) = I(d)$ tale che

- $d = 0 \implies o(g) = +\infty$
- $d > 0 \implies o(g) = d$

Dunque, $o(g)$ corrisponde al **più piccolo esponente** d tale che $g^d = e$

Dimostrazione:

- Poiché $I(g) \leq \mathbb{Z}$ ideale e poiché \mathbb{Z} è un dominio ad ideali principali, si ha che $\exists! d \in \mathbb{N} \mid I(g) = I(d)$.
- Di conseguenza, si ha che:

$$\begin{aligned} n, m \in I(g) &\iff g^n = g^m \iff g^{-n} \cdot g^n = g^m \cdot g^{-n} \iff e = g^{m-n} \iff \\ &\iff m - n \in I(g) = I(d) \iff m - n = dh, \exists h \in \mathbb{Z} \iff d \mid m - n \end{aligned}$$

- Consideriamo la funzione $f : \mathbb{Z} \rightarrow H(g) : n \mapsto g^n$, la quale risulta essere suriettiva per definizione stessa di $H(g)$
- Nel caso in cui $d = 0$, si ha che:

$$\begin{aligned} g^n = g^m &\iff d \mid m - n \iff 0 \mid m - n \iff \\ &\iff m - n = 0k, \exists k \in \mathbb{Z} \iff m - n = 0 \iff m = n \end{aligned}$$

di conseguenza, si ha che $f(n) = f(m) \iff m = n, \forall m, n \in \mathbb{Z}$, implicando che f sia anche iniettiva. Dunque, siccome f sarebbe una funzione biettiva, ne segue che

$$o(g) := |H(g)| = |\mathbb{Z}| = +\infty$$

- Nel caso in cui $d > 0$, invece, si ha che $d \in I(d) = I(g) \iff g^d = e$

$$\begin{aligned} \forall n \in \mathbb{Z}, \exists! q, r \in \mathbb{Z}, 0 \leq r < d \mid n = dq + r &\implies \\ \implies g^n = g^{dq+r} = g^{dq} g^r = (g^d)^q g^r = e^q g^r = g^r \end{aligned}$$

- Poiché $\forall n \in \mathbb{Z}, \exists 0 \leq r < d \mid g^n = g^r$ ne segue che possano esistere al massimo d potenze di g , implicando che $|H(g)| \leq d$
- Consideriamo ora invece la seguente restrizione di f , ossia $g : \{0, \dots, d-1\} \rightarrow H(g) : n \mapsto g^n$
- Considerando ancora il caso in cui $d > 0$ e presi $0 \leq m, n < d$, da cui traiamo che $-d < m - n < d$, si ha che:

$$\begin{aligned} g^n = g^m &\iff g^n g^{-m} = g^m g^{-n} \iff g^{m-n} = e \iff \\ &\iff m - n \in I(g) = I(d) \iff m - n = dp, \exists p \in \mathbb{Z} \end{aligned}$$

- Tuttavia, poiché $-d < m - n < d$, l'unica possibilità è $m - n = 0$, implicando che $m = n$. Di conseguenza, si ha che $g(n) = g(m) \iff n = m, \forall 0 \leq m, n < d$, implicando che g sia iniettiva, implicando a sua volta che:

$$o(g) := |H(g)| \leq |\{0, \dots, d-1\}| = d$$

- Infine, quindi, otteniamo che $d \geq |H(g)| \leq d \implies |H(g)| = d$, implicando quindi che g possa essere iniettiva se e solo se è suriettiva, da cui concludiamo che $g(x) = g^x \in H(g), \forall 0 \leq x < d$:

$$H(g) = \{g^0, \dots, g^{d-1}\}$$

□

Observation 20

Sia G un gruppo con cardinalità finita. Dato $g \in G$ si ha che

$$o(g) := |H(g)| \leq |G| < +\infty \implies o(g) \mid |G| \implies g^{|G|} = e$$

Attenzione: se $o(g) = +\infty$ allora $o(g) \nmid |G|$

Dimostrazione:

- Dato $o(g) = d := |H(g)| \leq |G| < +\infty$, per il teorema di Lagrange si ha che:

$$o(g) \mid |G| \implies |G| = dk, \exists k \in \mathbb{Z} \implies g^{|G|} = g^{dk} = (g^d)^k = e^k = e$$

□

Corollary 13. Piccolo teorema di Fermat (seconda dimostrazione)

Dato il campo \mathbb{Z}_p dove $p \in \mathbb{P}$, dato $[a] \in \mathbb{Z}_p$ si ha che:

$$a^p \equiv a \pmod{p}$$

Dimostrazione:

- Se $[a] = [0]$, allora abbiamo che $[a]^p = [0]$
- Poiché \mathbb{Z}_p è un campo, si ha che $\mathbb{Z}_p^* = \mathbb{Z}_p - \{0\}$, implicando che $|\mathbb{Z}_p^*| = p - 1$.
- Di conseguenza, dato $[a] \neq [0] \in \mathbb{Z}_p^*$ si ha che:

$$[a]^{|\mathbb{Z}_p^*|} = [1] \implies [a]^{p-1} = [1] \implies [a]^p [a]^{-1} = [1] \implies [a]^p = [a]$$

□

Proposition 30. Gruppo ciclico

Sia G un gruppo con cardinalità finita. Dato $g \in G$ si ha che

$$o(g) := |H(g)| = |G| \iff H(g) = G$$

In tal caso definiamo G come **gruppo ciclico**

Dimostrazione:

- Poiché $H(g) \leq G \implies H(g) \subseteq G$, per definizione stessa di insieme improprio si ha

$$|H(g)| = |G| \iff H(g) = G$$

□

Corollary 14

Sia G un gruppo. Dato $g \in G$, si ha che:

$$g \in G^* \implies g^{o(g)-1} = g^{-1}$$

Dimostrazione:

- Siccome $g \in G^* \iff \exists g^{-1} \in G$, allora:

$$g^{o(g)} = 1 \iff g^{o(g)} g^{-1} = g^{-1} \iff g^{o(g)-1} = g^{-1}$$

□

Lemma 31

Sia G un gruppo. Dato $g \in G$, si ha che:

$$g \in g^{-1} \implies o(g) = o(g^{-1})$$

Dimostrazione:

- Siccome $g \in G^* \iff \exists g^{-1} \in G$, allora:

$$(g^{-1})^n \in H(g^{-1}) \implies (g^{-1})^n = g^{-n} \in H(g)$$

- Analogamente, si ha che:

$$g^n \in H(g) \implies g^n = (g^{-1})^{-n} \in H(g^{-1})$$

- Di conseguenza, si verifica che $H(g) = H(g^{-1}) \implies o(g) = o(g^{-1})$

□

Lemma 32

Sia G un gruppo finito e $k \in \mathbb{Z}$, per ogni $g \in G$ si verifica che:

$$o(g^k) \mid o(g)$$

Dimostrazione:

- Dimostriamo che $H(g^k) \leq H(g)$
 - $(g^k)^n \in H(g^k) \implies (g^k)^n = g^{kn} \in H(g) \implies H(g^k) \subseteq H(g)$
 - $(g^k)^0 = g^0 = e \in H(g^k)$

$$\begin{aligned}
 - (g^k)^n, (g^k)^m \in H(g) &\implies (g^k)^n (g^k)^m = g^{kn} g^{km} = g^{kn+km} = g^{k(n+m)} = \\
 &(g^k)^{n+m} \in H(g) \\
 - (g^k)^n \in H(g^k) &\implies ((g^k)^n)^{-1} = (g^k)^{-n} \in H(g^k)
 \end{aligned}$$

- Di conseguenza, per il teorema di Lagrange si ha che

$$|H(g^k)| \mid |H(g)| \iff o(g^k) \mid o(g)$$

□

Lemma 33

Sia G un gruppo finito. Dati $g, h \in G \mid gh = hg$, si ha che:

$$\frac{m}{d} \mid o(gh) \quad \text{e} \quad o(gh) \mid m$$

dove $m := mcm(o(g), o(h))$ e $d := MCD(o(g), o(h))$.

In particolare, se $d = 1$, allora $o(gh) = o(g)o(h)$.

Dimostrazione:

- Per definizione stessa di $m := mcm(o(g), o(h))$, si ha che

$$o(g) \mid m, o(h) \mid m \iff o(g) \cdot p = m = o(h) \cdot q, \exists p, q \in \mathbb{Z}$$

- Siccome per ipotesi $gh = hg$, si ha che:

$$\begin{aligned}
 (gh)^m &= \underbrace{gh \cdot \dots \cdot gh}_{m \text{ volte}} = g^m h^m = g^{o(g) \cdot p} h^{o(h) \cdot q} = (g^{o(g)})^p (h^{o(h)})^q = e^p e^q = e \implies \\
 &\implies m \in I(gh) = I(o(gh)) \implies o(gh) \mid m
 \end{aligned}$$

- Inoltre, abbiamo che

$$e = (gh)^{o(gh)} = \underbrace{gh \cdot \dots \cdot gh}_{o(gh) \text{ volte}} = g^{o(gh)} h^{o(gh)} \implies e = g^{o(gh)} h^{o(gh)} \iff g^{o(gh)} = h^{-o(gh)}$$

- Per il lemma precedente, abbiamo che

$$o(g^{o(gh)}) \mid o(g), o(h^{-o(gh)}) \mid o(h)$$

e dato che $g^{o(gh)} = h^{-o(gh)}$, otteniamo che

$$o(g^{o(gh)}) \mid o(g), o(h^{-o(gh)}) \mid o(h) \iff o(g^{o(gh)}) \mid o(g), o(g^{o(gh)}) \mid o(h) \implies o(g^{o(gh)}) \mid d$$

dove $d = MCD(o(g), o(h))$

- A questo punto, notiamo che:

$$\frac{m}{d} \cdot \frac{d}{o(g^{o(gh)})} = \frac{m}{o(g^{o(gh)})} \implies \frac{m}{d} \mid \frac{m}{o(g^{o(gh)})}$$

- Inoltre, ponendo $k := g^{o(gh)}$ abbiamo che

$$g^{o(g^{o(gh)})o(gh)} = g^{k \cdot o(gh)} = (g^{o(gh)})^k = k^{o(k)} = e \implies o(g) \mid o(g^{o(gh)})o(gh)$$

e analogamente che:

$$\begin{aligned} h^{-o(g^{o(gh)})o(gh)} &= (h^{-o(gh)})^{o(g^{o(gh)})} = (g^{o(gh)})^{o(g^{o(gh)})} = k^{o(k)} = e \implies \\ \implies o(h) \mid -o(g^{o(gh)})o(gh) &\implies o(h) \mid o(g^{o(gh)})o(gh) \end{aligned}$$

di conseguenza si ha che $m \mid o(g^{o(gh)})o(gh)$

- Quindi, $\exists j \in \mathbb{Z}$ tale che:

$$o(g^{o(gh)})o(gh) = mj \implies o(gh) = \frac{m}{o(g^{o(gh)})} \cdot j \implies \frac{m}{o(g^{o(gh)})} \mid o(gh)$$

- Infine, per transitività si ha che:

$$\frac{m}{d} \mid \frac{m}{o(g^{o(gh)})}, \frac{m}{o(g^{o(gh)})} \mid o(gh) \implies \frac{m}{d} \mid o(gh)$$

- Per l'ultima affermazione notiamo che se $d = 1$, allora:

$$\frac{m}{d} \mid o(gh) \implies m \mid o(gh)$$

di conseguenza, poiché $m, d \in \mathbb{N}$, per anti-simmetria (sezione 3.2) si ha che:

$$m \mid o(gh), o(gh) \mid m \iff m = o(gh)$$

- Dunque, per il teorema fondamentale dell'algebra, se $d = 1$ si ha che:

$$o(g)(h) = m = o(g)o(h)$$

□

Proposition 34

Siano $n_1, \dots, n_k \neq 0 \in \mathbb{N} \mid MCD(a_i, a_j) \iff i \neq j$ e sia $N := mcm(n_1, \dots, n_k) = n_1 \cdot \dots \cdot n_k$.

Dato $[a] \in \mathbb{Z}_{\gg}^*$, dove $m := mcm(o_1, \dots, o_k)$ e dove $o_h := o([a])$ nel gruppo $\mathbb{Z}_{\times \sim}^*$, $\forall 0 < h < k$, posto $o := o([a])$ nel gruppo \mathbb{Z}_{\gg}^* si ha che:

$$o = m := mcm(o_1, \dots, o_k)$$

Dimostrazione:

- Per il teorema cinese dei resti, abbiamo che:

$$\begin{aligned} a^o \equiv 1 \pmod{N} &\iff \begin{cases} a^o \equiv 1 \pmod{n_1} \\ \vdots \\ a^o \equiv 1 \pmod{n_k} \end{cases} \iff \\ &\iff \begin{cases} o_1 \mid o \\ \vdots \\ o_k \mid o \end{cases} \iff m := mcm(o_1, \dots, o_k) \mid o \end{aligned}$$

- Inoltre, poiché $m := mcm(o_1, \dots, o_k)$, abbiamo che:

$$\begin{cases} o_1 \mid m \\ \vdots \\ o_k \mid m \end{cases} \iff \begin{cases} a^m \equiv 1 \pmod{n_1} \\ \vdots \\ a^m \equiv 1 \pmod{n_k} \end{cases} \iff a^m \equiv 1 \pmod{N} \implies o \mid m$$

- Poiché $o, m \in \mathbb{N}$, per anti-simmetria (sezione 3.2) si ha che:

$$o \mid m, m \mid o \iff o = m$$

□

Esempio:

- Vogliamo trovare tutti gli inversi di \mathbb{Z}_{21} e il loro ordine, determinando se \mathbb{Z}_{21} sia un gruppo ciclico
- Dato $g \in \mathbb{Z}_{21}$, sappiamo che $g \in \mathbb{Z}_{21}^* \iff MCD(a, 21) = 1$ (sezione 4.5). Dunque abbiamo che:

$$\mathbb{Z}_{21}^* : \{[1], [2], [4], [5], [8], [10], [11], [13], [16], [17], [19], [20]\} \implies |\mathbb{Z}_{21}^*| = 12$$

- Dato $g \in \mathbb{Z}_{21}^*$, per Lagrange abbiamo che $o(g)$ può essere solo un divisore di $|\mathbb{Z}_{21}^*|$, riducendo i tentativi necessari a trovare l'ordine di ogni elemento da 21 a 6:

$$o(g) \mid |\mathbb{Z}_{21}^*| \implies o(g) \mid 12 \implies o(g) \in \{1, 2, 3, 4, 6, 12\}$$

- Calcoliamo quindi gli ordini dei vari invertibili in \mathbb{Z}_{21} trovati:

$$\begin{aligned} - [1]^1 &= 1 \implies \begin{cases} o([1]) = 1 \\ [1]^{-1} = [1]^0 = [1] \end{cases} \\ - [2]^6 &= [64] = [1] \implies \begin{cases} o([2]) = 6 \\ [2]^{-1} = [2]^5 = [11] \end{cases} \implies \begin{cases} o([11]) = 6 \\ [11]^{-1} = [2] \end{cases} \\ - [4]^3 &= [2]^6 = [64] = [1] \implies \begin{cases} o([4]) = 3 \\ [4]^{-1} = [4]^2 = [16] \end{cases} \implies \begin{cases} o([16]) = 3 \\ [16]^{-1} = [4] \end{cases} \\ - [5]^6 &= [5^2]^3 = [4]^3 = [1] \implies \begin{cases} o([5]) = 6 \\ [5]^{-1} = [5]^5 = [17] \end{cases} \implies \begin{cases} o([17]) = 6 \\ [17]^{-1} = [5] \end{cases} \\ - [8]^2 &= [2]^6 = [1] \implies \begin{cases} o([8]) = 2 \\ [8]^{-1} = [8] \end{cases} \\ - [10]^6 &= [10^3]^2 = [13]^2 = [1] \implies \begin{cases} o([10]) = 6 \\ [10]^{-1} = [10]^5 = [19] \end{cases} \implies \begin{cases} o([19]) = 6 \\ [19]^{-1} = [10] \end{cases} \\ - [13]^2 &= [1] \implies \begin{cases} o([13]) = 2 \\ [13]^{-1} = [13]^1 = [13] \end{cases} \\ - [20]^2 &= [1] \implies \begin{cases} o([20]) = 2 \\ [20]^{-1} = [20]^1 = [20] \end{cases} \end{aligned}$$

- Poiché $\nexists g \in \mathbb{Z}_{21}^* \mid o(g) = |\mathbb{Z}_{21}^*|$, concludiamo che \mathbb{Z}_{21}^* non è un gruppo ciclico

Capitolo 5

Gruppo Simmetrico

Observation 21

Una funzione $f : X \rightarrow Y : x \mapsto f(x)$ è invertibile se e solo se f è biettiva.

$$f \text{ invertibile} \iff f \text{ biettiva}$$

dove l'essere invertibile equivale a dire che $\exists f^{-1} : Y \rightarrow X : f(x) \mapsto x$

Dimostrazione:

- Sia $f : X \rightarrow Y : x \mapsto f(x)$
- Se $\exists f^{-1} : Y \rightarrow X : f(x) \mapsto x$, ossia f è invertibile, allora

$$f(x) = f(y) \implies f^{-1}(f(x)) = f^{-1}(f(y)) \implies x = y$$

dunque f è iniettiva

- Analogamente, si ha che

$$\forall y \in Y, \exists x \in X \mid y = f(x) = f(f^{-1}(y))$$

dunque f è anche suriettiva, implicando che essa sia biettiva

- Inoltre, poiché $f = (f^{-1})^{-1}$, anche f^{-1} è invertibile e di conseguenza biettiva
- Se invece f è biettiva, allora

$$\forall x \in X, \exists! y \in Y \mid f(x) = y \implies f(f^{-1}(y)) = y$$

di conseguenza, f è invertibile

□

Definition 36. Gruppo simmetrico

Dato un insieme X , denotiamo come \mathcal{S}_X l'insieme:

$$\mathcal{S}_X : \{f : X \rightarrow X \mid f \text{ è biettiva}\}$$

Inoltre, si ha che (\mathcal{S}_X, \circ) è un gruppo.

Dimostrazione:

- Per natura stessa della composizione tra funzione si ha che

$$f, g, h \in \mathcal{S}_X \implies h \circ (g \circ f) = h \circ g \circ f = (h \circ g) \circ f$$

- La funzione identità $\text{id} : X \rightarrow X : x \mapsto x$ è biettiva, dunque

$$\exists \text{id} \in \mathcal{S}_X \mid \forall f \in \mathcal{S}_X, f \circ \text{id} = \text{id} \circ f = f$$

- Poiché una funzione è biettiva se e solo se è invertibile, ne segue che

$$\forall f \in \mathcal{S}_X, \exists f^{-1} \in \mathcal{S}_X \mid f \circ f^{-1} = f^{-1} \circ f = \text{id}$$

□

Observation 22

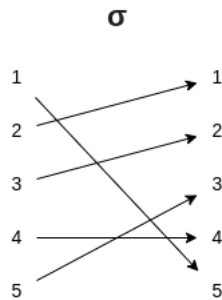
Dato il gruppo simmetrico \mathcal{S}_X , ogni $f \in \mathcal{S}_X$ corrisponde ad una **permutazione** del dominio X , poiché $f : X \rightarrow X$ è biettiva. Dunque, è possibile definire impropriamente \mathcal{S}_X come il "**gruppo delle permutazioni di X** ".

In particolare, se $|X| = n$ dove $n \in \mathbb{N}$, ogni $f \in \mathcal{S}_X$ corrisponderà ad una permutazione di n elementi. In tal caso, denotiamo come \mathcal{S}_n il **gruppo simmetrico di ordine n** , la cui cardinalità corrisponde a $|\mathcal{S}_n| = n!$

Esempio:

- Data la permutazione $\sigma \in \mathcal{S}_5$, possiamo utilizzare due **notazioni** per poterne descrivere il comportamento:

Tramite grafo



Tramite matrice

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 1 & 2 \end{pmatrix}$$

Observation 23

Per comodità di scrittura, definiamo l'operazione binaria **prodotto tra permutazioni** come:

$$\cdot : \mathcal{S}_n \times \mathcal{S}_n \rightarrow \mathcal{S}_n : (\sigma, \tau) \mapsto \tau \circ \sigma$$

In altre parole, si ha che $\sigma\tau := \sigma \circ \tau = \sigma(\tau(x)), \forall x$.

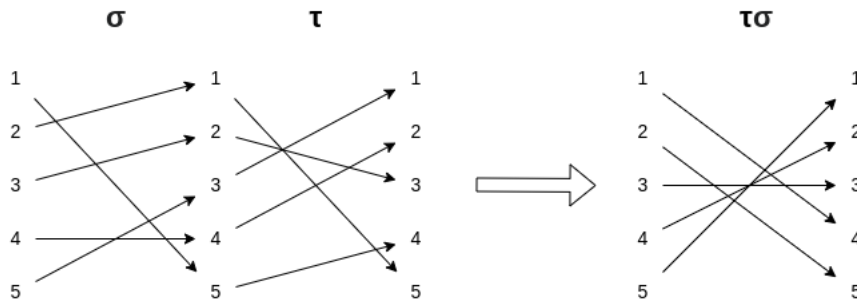
Ovviamente, (\mathcal{S}_n, \cdot) risulta essere un **gruppo** (non abeliano poiché per natura stessa della composizione si ha che $\sigma\tau \neq \tau\sigma$)

Esempio:

- Siano $\sigma, \tau \in \mathcal{S}_5$ tali che:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 2 & 4 & 3 \end{pmatrix} \quad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 1 & 2 & 4 \end{pmatrix}$$

- Per calcolare il prodotto tra le due permutazioni (dunque la loro composizione), utilizziamo due metodi:
 - Tramite **grafo**, considerando la composizione delle frecce rappresentanti le due permutazioni



- Tramite **matrici**, dove ci basta "allineare" gli elementi in input della seconda permutazione con gli elementi in output della seconda. Il risultato del prodotto sarà costituito dagli **elementi in input della prima** e gli **elementi in output della seconda**.

$$\begin{array}{l} \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 2 & 4 & 3 \end{pmatrix} \\ \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 1 & 2 & 4 \end{pmatrix} \end{array} \Rightarrow \begin{array}{l} \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 2 & 4 & 3 \end{pmatrix} \\ \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 2 & 4 & 3 \end{pmatrix} \end{array} \Rightarrow \tau\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 3 & 2 & 1 \end{pmatrix}$$

5.1 Ordine di una permutazione

Definition 37. Ciclo di una permutazione

Sia $\sigma \in \mathcal{S}_n$. Definiamo come **ciclo di σ** una sequenza di interi $1 \leq i_1, \dots, i_n \leq n$ tutti distinti tra loro tali che:

$$\sigma(i_1) = i_2, \sigma(i_2) = i_3, \dots, \sigma(i_n) = i_1$$

Definiamo come **lunghezza del ciclo** il numero di elementi appartenenti al ciclo.

Esempio:

- Consideriamo la seguente permutazione in $\sigma \in \mathcal{S}_9$:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 5 & 7 & 6 & 9 & 2 & 3 & 1 & 4 & 8 \end{pmatrix}$$

- Notiamo la presenza di tre cicli all'interno di tale permutazione:
 - $1 \rightarrow 5 \rightarrow 2 \rightarrow 7 \rightarrow 1$ che abbreviamo come (1587)
 - $3 \rightarrow 6 \rightarrow 3$ che abbreviamo come (36)
 - $4 \rightarrow 9 \rightarrow 8 \rightarrow 4$ che abbreviamo come (498)

Definition 38. Decomposizione in cicli

Data $\sigma \in \mathcal{S}_n$ composta da k cicli, definiamo la sua **decomposizione in cicli** come:

$$\sigma = \gamma_1 \gamma_2 \dots \gamma_k$$

dove γ_i è un ciclo di σ

Esempio:

- Considerando ancora l'esempio precedente, possiamo riscrivere σ tramite la sua decomposizione in cicli:

$$\sigma \in \mathcal{S}_9 \mid \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 5 & 7 & 6 & 9 & 2 & 3 & 1 & 4 & 8 \end{pmatrix} \implies \sigma = (1587)(36)(498)$$

- Ovviamente, tramite una decomposizione in cicli è possibile ricostruire la permutazione associata:

$$\tau \in \mathcal{S}_8 \mid \tau = (235)(1874)(6) \implies \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 3 & 5 & 1 & 2 & 6 & 4 & 7 \end{pmatrix}$$

Definition 39

Sia $\sigma \in \mathcal{S}_n$. Dati $1 \leq i \leq n$, definiamo:

$$I(\sigma, i) : \{n \in \mathbb{Z} \mid \sigma^n(i) = i\}$$

$$I(\sigma) : \{n \in \mathbb{Z} \mid \sigma^n = \text{id}\}$$

dove:

- id è la permutazione identica, dunque $\text{id} = (1)(2) \dots (n-1)(n)$
- $(I(\sigma(i)), +) \leq (\mathbb{Z}, +)$ ideale
- $(I(\sigma), +) \leq (\mathbb{Z}, +)$ ideale

Dimostrazione:

- $I(\sigma, i) \leq \mathbb{Z}$ ideale:
 - $\sigma^0(i) = \text{id}(i) = i \implies 0 \in I(\sigma, i)$
 - $m, n \in I(\sigma, i) \implies \sigma^n(i) = i = \sigma^m(i) \implies \sigma^{n+m}(i) = \sigma^n(\sigma^m(i)) = \sigma^n(i) = i \implies m+n \in I(\sigma, i)$
 - $n \in I(\sigma, i) \implies \sigma^{-n}(i) = (\sigma^n)^{-1}(i) = i \implies -n \in I(\sigma, i)$
 - $n \in I(\sigma, i) \implies \sigma^{nk}(i) = (\sigma^n)^k(i) = i, \forall k \in \mathbb{Z} \implies nk \in I(\sigma, i), \forall k \in \mathbb{Z}$
 - Per gli ultimi due punti è necessario osservare che poiché $\sigma^n(i) = i$, allora $(\sigma^n)^k(i) = i, \forall k \in \mathbb{Z}$, poiché i viene sempre mandato in se stesso
- Viene omessa la dimostrazione di $I(\sigma) \leq \mathbb{Z}$ ideale poiché analoga a quella di $I(\sigma, i) \leq \mathbb{Z}$ ideale

□

Lemma 35

Sia $\sigma \in \mathcal{S}_n$ e sia $\gamma_1 \dots \gamma_k$ la sua decomposizione in cicli. Dato il dominio ad ideali principali \mathbb{Z} e dato $i \in \gamma_j \mid j \in [1, k]$ si ha che:

$$I(\sigma, i) = I(d_j)$$

dove d_j è la lunghezza di γ_j

Dimostrazione:

- Poiché \mathbb{Z} è un dominio ad ideali principali e poiché $I(\sigma, i) \leq \mathbb{Z}$ ideale, si ha che:

$$\exists! h \in \mathbb{N} \mid I(\sigma, i) = I(h)$$

dove $h := \min(I(\sigma, i)_{>0})$

- Sia $i \in (i_1 i_2 \dots i_{d_j})$, dunque appartenente ad un ciclo di lunghezza d_j . Per comodità, supponiamo che $i = i_1$, poiché scorrere l'ordine degli elementi del ciclo non ne cambia le proprietà (ad esempio: $(2783) = (7832) = (8327) = \dots$)

- Se $0 < h < d_j$, si ha che:

$$0 < h < d_j \implies \sigma^h(i) = \sigma(\sigma^{h-1}(i)) = \sigma(i_h) = i_{h+1} \implies h \notin I(\sigma, i)$$

- Nel caso in cui invece $h = d_j$, si verifica che:

$$h = d_j \implies \sigma^h(i) = \sigma^{d_j}(i) = \sigma(\sigma^{d_j-1}(i)) = \sigma(i_{d_j}) = i_1 = i \implies h \in I(\sigma, i)$$

- Di conseguenza, affinché $I(\sigma, i) = I(h)$, ne segue necessariamente che $h = d_j$

□

Proposition 36. Ordine di una permutazione

Sia $\sigma \in \mathcal{S}_n$ e sia $\gamma_1 \dots \gamma_k$ la sua decomposizione in cicli. Dato il dominio ad ideali principali \mathbb{Z} , si ha che:

$$I(\sigma) = I(m) \implies o(\sigma) = m$$

dove $m := \text{mcm}(d_1, \dots, d_k)$ e dove d_1, \dots, d_k sono rispettivamente le lunghezze di $\gamma_1 \dots \gamma_k$.

Dunque, $o(\sigma)$ corrisponde al **minimo comune multiplo delle lunghezze dei cicli di σ**

Dimostrazione:

- Per definizione stessa di $I(\sigma)$ e $I(\sigma, i)$, si ha che:

$$n \in I(\sigma) \iff \sigma^n = \text{id} \iff \sigma^n(i) = i, \forall i \in [1, n] \iff$$

$$\iff n \in I(\sigma, i), \forall i \in [1, n] \iff n \in I(\sigma, 1) \cap \dots \cap I(\sigma, n)$$

implicando quindi che $I(\sigma) = I(\sigma, 1) \cap \dots \cap I(\sigma, n)$

- Poiché \mathbb{Z} è un dominio ad ideali principali e poiché $I(\sigma) \leq \mathbb{Z}$ ideale, per il lemma precedente si ha che:

$$I(\sigma) = I(\sigma, 1) \cap \dots \cap I(\sigma, n) = I(d_1) \cap \dots \cap I(d_k) = I(m)$$

dove $m := \text{mcm}(d_1, \dots, d_k)$

□

Esempi:

- Data $\sigma \in S_7$ tale che:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 6 & 5 & 7 & 2 & 1 & 4 \end{pmatrix} = (13526)(47)$$

L'ordine di tale permutazione risulta essere:

$$o(\sigma) = \text{mcm}(5, 2) = 10$$

- Data $\sigma \in S_{15}$ tale che:

$$\sigma = (1\ 2\ 10\ 8\ 3)(11\ 7)(4\ 12\ 14\ 6)(13)(5\ 15\ 9)$$

L'ordine di tale permutazione risulta essere:

$$o(\sigma) = mcm(5, 2, 4, 1, 3) = 60$$

5.2 Segno delle permutazioni

Definition 40. Segno di una permutazione

Sia $\sigma \in \mathcal{S}_n$. Definiamo il **segno** di σ come:

$$sgn(\sigma) = (-1)^{|Inv(\sigma)|} = \begin{cases} +1 & \text{se } |Inv(\sigma)| \text{ è pari} \\ -1 & \text{se } |Inv(\sigma)| \text{ è dispari} \end{cases}$$

Dove $Inv(\sigma)$ è l'**insieme delle sue inversioni**:

$$Inv(\sigma) : \{(i, j) \mid 1 \leq i < j \leq n, \sigma(i) > \sigma(j)\}$$

Definiamo σ come **pari** se $sgn(\sigma) = +1$, mentre come **dispari** $sgn(\sigma) = -1$

Esempio:

- Sia $\sigma \in \mathcal{S}_5$ tale che

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 3 & 1 & 4 \end{pmatrix}$$

- L'insieme delle sue inversioni sarà:

$$Inv(\sigma) : \{(1, 4), (2, 3), (2, 4), (2, 5), (3, 4)\}$$

da cui otteniamo che $sgn(\sigma) = -1$

Definition 41. Trasposizione e Trasposizione adiacente

Definiamo $\tau_{i,j} \in \mathcal{S}_n$, dove $1 \leq i < j \leq n$, come **trasposizione** se:

$$\tau_{i,j}(k) = \begin{cases} j & \text{se } k = i \\ i & \text{se } k = j \\ k & \text{se } k \neq i, k \neq j \end{cases}$$

In particolare, definiamo come $\tau_{i,j} \in \mathcal{S}_n$ come **trasposizione adiacente** se $j = i + 1$, dunque avente l'effetto di scambiare due elementi adiacenti tra loro.

Lemma 37

Data $\sigma \in \mathcal{S}_n$, si ha che:

$$\exists 1 \leq i_1, \dots, i_k \leq n \mid \sigma = \tau_{i_1, i_1+1} \cdot \dots \cdot \tau_{i_k, i_k+1}$$

In altre parole, σ può essere espressa come il **prodotto di k trasposizioni adiacenti**

Dimostrazione tramite esempio:

- Prima di tutto, osserviamo che dati $\sigma, \tau_{i,j} \in \mathcal{S}_n$ tali che:

$$\sigma = \begin{pmatrix} 1 & \dots & i & \dots & j & \dots & n \\ \sigma(1) & \dots & \sigma(i) & \dots & \sigma(j) & \dots & \sigma(n) \end{pmatrix}$$

$$\tau_{i,j} = \begin{pmatrix} 1 & \dots & i & \dots & j & \dots & n \\ 1 & \dots & j & \dots & i & \dots & n \end{pmatrix}$$

si ha che:

$$\sigma \tau_{i,j} = \begin{pmatrix} 1 & \dots & i & \dots & j & \dots & n \\ \sigma(1) & \dots & \sigma(j) & \dots & \sigma(i) & \dots & \sigma(n) \end{pmatrix}$$

- Dunque, data $\sigma \in S_3$ tale che:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}$$

abbiamo che:

$$\sigma \cdot \tau_{3,4} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix} \implies \sigma \cdot \tau_{3,4} \cdot \tau_{2,3} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \implies$$

$$\implies \sigma \cdot \tau_{3,4} \cdot \tau_{2,3} \cdot \tau_{1,2} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix} \implies \sigma \cdot \tau_{3,4} \cdot \tau_{2,3} \cdot \tau_{1,2} \cdot \tau_{3,4} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} = \text{id}$$

- Di conseguenza, si ha che:

$$\begin{aligned} \sigma(\tau_{3,4}\tau_{2,3}\tau_{1,2}\tau_{3,4}) &= \text{id} \iff \\ \iff \sigma(\tau_{3,4}\tau_{2,3}\tau_{1,2}\tau_{3,4})(\tau_{3,4}\tau_{2,3}\tau_{1,2}\tau_{3,4})^{-1} &= \text{id}(\tau_{3,4}\tau_{2,3}\tau_{1,2}\tau_{3,4})^{-1} \iff \\ \iff \sigma = (\tau_{3,4}\tau_{2,3}\tau_{1,2}\tau_{3,4})^{-1} &\iff \sigma = \tau_{3,4}\tau_{1,2}\tau_{2,3}\tau_{3,4} \end{aligned}$$

□

Proposition 38

Data $\sigma \in \mathcal{S}_n \mid \sigma = \tau_1 \cdot \dots \cdot \tau_k$, dove $\tau_i := \tau_{i,i+1} \in \mathcal{S}_n$, si ha che:

$$\text{sgn}(\sigma) = (-1)^k$$

dove k è il numero di trasposizioni adiacenti che compongono σ

Dimostrazione:

- Sia $\tau_i = \tau_{i,i+1}$. Allora si ha che:

$$\sigma\tau_i = \begin{pmatrix} 1 & \dots & i & i+1 & \dots & n \\ \sigma(1) & \dots & \sigma(i+1) & \sigma(i) & \dots & \sigma(n) \end{pmatrix}$$

- Lo scambio effettuato genera una di due situazioni possibili: viene **creata una nuova inversione** oppure viene **risolta un'inversione pre-esistente**:

$$\text{Inv}(\sigma\tau_i) = \begin{cases} \text{Inv}(\sigma) \cup \{(i, i+1)\} & \text{se } (i, i+1) \notin \text{Inv}(\sigma) \\ \text{Inv}(\sigma) - \{(i, i+1)\} & \text{se } (i, i+1) \in \text{Inv}(\sigma) \end{cases}$$

- Di conseguenza, si ha che

$$\begin{aligned} |\text{Inv}(\sigma\tau_i)| = |\text{Inv}(\sigma)| \pm 1 &\implies \text{sgn}(\sigma\tau_i) = \begin{cases} -1 & \text{se } \text{sgn}(\sigma) = +1 \\ +1 & \text{se } \text{sgn}(\sigma) = -1 \end{cases} \implies \\ &\implies \text{sgn}(\sigma\tau) = -\text{sgn}(\sigma) \end{aligned}$$

- Di conseguenza, se $\sigma = \tau_1 \cdot \dots \cdot \tau_k$, si ha che:

$$\sigma(\tau_i \cdot \dots \cdot \tau_k)^{-1} = (\tau_i \cdot \dots \cdot \tau_k)(\tau_i \cdot \dots \cdot \tau_k)^{-1} = \text{id}$$

- Poiché per definizione stessa di **id** si ha che $|\text{Inv}(\text{id})| = 0 \implies \text{sgn}(\text{id}) = 1$, ne segue che:

$$\begin{aligned} 1 = \text{sgn}(\text{id}) &= \text{sgn}(\sigma(\tau_i \cdot \tau_2 \cdot \tau_3 \cdot \dots \cdot \tau_k)^{-1}) = \text{sgn}(\sigma \cdot \tau_k \cdot \dots \cdot \tau_3 \cdot \tau_2 \cdot \tau_1) = \\ &= -\text{sgn}(\sigma \cdot \tau_k \cdot \dots \cdot \tau_3 \cdot \tau_2) = \text{sgn}(\sigma \cdot \tau_k \cdot \dots \cdot \tau_3) = \dots = (-1)^k \cdot \text{sgn}(\sigma) \end{aligned}$$

- Quindi, otteniamo che:

$$1 = (-1)^k \cdot \text{sgn}(\sigma) \implies \text{sgn}(\sigma) = (-1)^k$$

□

Corollary 15

Date $\sigma, \sigma' \in \mathcal{S}_n$, si verifica che:

$$\text{sgn}(\sigma\sigma') = \text{sgn}(\sigma) \cdot \text{sgn}(\sigma')$$

□

Dimostrazione:

- Data $\sigma = \tau_1 \cdot \dots \cdot \tau_k$ e $\sigma' = \tau'_1 \cdot \dots \cdot \tau'_k$, si ha che:

$$\operatorname{sgn}(\sigma\sigma') = \operatorname{sgn}(\tau_1 \cdot \dots \cdot \tau_k \cdot \tau'_1 \cdot \dots \cdot \tau'_k) = (-1)^{k+j} = (-1)^k(-1)^j = \operatorname{sgn}(\sigma) \cdot \operatorname{sgn}(\sigma')$$

Corollary 16

Data $\sigma \in \mathcal{S}_n$, si verifica che:

$$\operatorname{sgn}(\sigma^{-1}) = \operatorname{sgn}(\sigma)$$

Dimostrazione:

$$\begin{aligned} 1 &= \operatorname{sgn}(\operatorname{id}) = \operatorname{sgn}(\sigma\sigma^{-1}) = \operatorname{sgn}(\sigma) \cdot \operatorname{sgn}(\sigma^{-1}) \implies \\ \implies 1 &= \operatorname{sgn}(\sigma) \cdot \operatorname{sgn}(\sigma^{-1}) \iff \operatorname{sgn}(\sigma) = \pm 1 = \operatorname{sgn}(\sigma^{-1}) \end{aligned}$$

□

Definition 42

Dato il gruppo \mathcal{S}_n , definiamo $\mathcal{A}_n \leq \mathcal{S}_n$ come il **sottogruppo alterno di ordine n** :

$$\mathcal{A}_n := \{\sigma \in \mathcal{S}_n \mid \operatorname{sgn}(\sigma) = +1\}$$

Dimostrazione:

- $\operatorname{sgn}(\operatorname{id}) = 1 \implies \operatorname{id} \in \mathcal{A}_n$
- $\sigma, \tau \in \mathcal{A}_n \implies \operatorname{sgn}(\sigma\tau) = \operatorname{sgn}(\sigma)\operatorname{sgn}(\tau) = 1 \cdot 1 = 1 \implies \sigma\tau \in \mathcal{A}_n$
- $\sigma \in \mathcal{A}_n \implies \operatorname{sgn}(\sigma^{-1}) = \operatorname{sgn}(\sigma) = 1 \implies \sigma^{-1} \in \mathcal{A}_n$

□

Observation 24

Dato \mathcal{S}_n e $\mathcal{A}_n \leq \mathcal{S}_n$, si ha che:

- $|\mathcal{A}_n| = \frac{n!}{2}$
- $[\mathcal{S}_n : \mathcal{A}_n] = 2$

Dimostrazione:

- Date $\sigma, \sigma' \in \mathcal{S}_n$, si ha che:

$$\begin{aligned} \sigma \sim \sigma' &\iff \sigma^{-1}\sigma' \in \mathcal{A}_n \iff \operatorname{sgn}(\sigma^{-1}\sigma') = 1 \iff \\ &\iff \operatorname{sgn}(\sigma^{-1})\operatorname{sgn}(\sigma') = 1 \iff \operatorname{sgn}(\sigma) = \operatorname{sgn}(\sigma') \end{aligned}$$

- Di conseguenza, poiché $\text{sgn}(\sigma) = \pm 1, \forall \sigma \in \mathcal{S}_n$ e poiché $\text{sgn}(\text{id}) = +1$, esistono solo due classi laterali sinistre:

– La classe $[+1] : \{\sigma \in \mathcal{S}_n \mid \sigma \sim \text{id}\}$

– La classe $[-1] : \{\sigma \in \mathcal{S}_n \mid \sigma \not\sim \text{id}\}$

dunque si ha che $[\mathcal{S}_n : \mathcal{A}_n] = 2$

- Infine, per il teorema di Lagrange, concludiamo che:

$$|A_n| = \frac{|\mathcal{S}_n|}{[\mathcal{S}_n : \mathcal{A}_n]} = \frac{n!}{2}$$

□

Proposition 39

Sia \sim la **relazione di coniugio** (sezione 3.5) e siano $\sigma, \sigma' \in \mathcal{S}_n$, tali che:

- $\gamma_1 \dots \gamma_k$ è la decomposizione in cicli di σ e d_1, \dots, d_k sono le lunghezze rispettive dei cicli
- $\gamma'_1 \dots \gamma'_k$ è la decomposizione in cicli di σ' e d'_1, \dots, d'_k sono le lunghezze rispettive dei cicli

In tal caso, si ha che:

$$\sigma \sim \sigma' \iff \begin{cases} k = h \\ d_1 = d'_1 \\ \dots \\ d_k = d'_h \end{cases}$$

Dimostrazione:

- Supponiamo che $\sigma \sim \sigma'$, dunque $\exists \alpha \in \mathcal{S}_n \mid \sigma' = \alpha \sigma \alpha^{-1}$
- Sia $\gamma_j = (i_1 \dots i_d) \mid j \in [1, k]$ un ciclo di σ . Allora, $\forall i_q \in \gamma_j \mid q \in [1, d]$ si ha che:

$$\sigma'(i_q) = \alpha \sigma \alpha^{-1}(i_q) \iff \sigma' \alpha(i_q) = \alpha \sigma \alpha^{-1} \alpha(i_q) \iff \sigma' \alpha(i_q) = \alpha \sigma(i_q) \implies$$

$$\implies \sigma' \alpha(i_q) = \alpha \sigma(i_q) = \begin{cases} \alpha(i_{q+1}) & \text{se } q < d \\ \alpha(i_1) & \text{se } q = d \end{cases}$$

- Di conseguenza, σ' possiede un ciclo nella forma $(\alpha(i_1), \dots, \alpha(i_d))$. Applicando lo stesso ragionamento con gli altri σ , possiamo creare una corrispondenza biunivoca tra i cicli di σ e i cicli di σ' , da cui otteniamo che $h = k$ e che $d_p = d'_p, \forall p \in [1, k]$
- Viceversa, supponiamo che σ e σ' abbiano lo stesso numero di cicli e le stesse lunghezze per ogni ciclo, dunque tali che:

$$\sigma = (i_1 \dots i_{d_1}) \dots (j_1 \dots j_{d_k}) \quad \sigma' = (a_1 \dots a_{d_1}) \dots (b_1 \dots b_{d_k})$$

- Presa $\alpha \in \mathcal{S}_n$ tale che:

$$\alpha(i_1) = a_1, \dots, \alpha(i_{d_1}) = a_{d_1}, \alpha(j_1) = b_1, \dots, \alpha(j_{d_k}) = b_{d_k}$$

dunque tale che:

$$\begin{array}{ccccccc} \sigma = & (i_1 & \dots & i_{d_1}) & \dots & (j_1 & \dots & j_{d_k}) \\ & \downarrow & & \downarrow & & \downarrow & & \downarrow \\ \sigma' = & (a_1 & \dots & a_{d_1}) & \dots & (b_1 & \dots & j_{b_k}) \end{array}$$

- Dato $t \in [1, n]$ e dato $j \in [1, k]$, quindi, si ha che:

$$\begin{aligned} \alpha\sigma\alpha^{-1}(a_t) = \alpha\sigma(i_t) &= \begin{cases} \alpha(i_{k+1}) & \text{se } t < d_j \\ \alpha(i_1) & \text{se } t = d_j \end{cases} = \begin{cases} a_{k+1} & \text{se } k < d_j \\ a_1 & \text{se } k = d_j \end{cases} \implies \\ \alpha\sigma\alpha^{-1}(a_t) &= \sigma'(a_t) \implies \sigma \sim \sigma' \end{aligned}$$

□

Esempi:

1. Date le seguenti permutazioni $\sigma, \sigma' \in S_6$, trovare $\alpha \in S_6$ tale che $\sigma' = \alpha\sigma\alpha^{-1}$:

$$\begin{aligned} \sigma &= (13)(254)(876) \\ \sigma' &= (25)(184)(376) \end{aligned} \implies \alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 1 & 5 & 4 & 8 & 6 & 7 & 3 \end{pmatrix}$$

2. Date le seguenti permutazioni $\sigma, \sigma' \in S_7$, trovare $\alpha \in S_7$ tale che $\sigma' = \alpha\sigma\alpha^{-1}$:

$$\begin{aligned} \sigma &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 6 & 1 & 4 & 2 & 7 & 5 \end{pmatrix} = (4)(13)(2675) \\ \sigma' &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 4 & 1 & 6 & 5 & 7 \end{pmatrix} = (7)(56)(1234) \end{aligned} \implies \alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 1 & 6 & 7 & 4 & 2 & 3 \end{pmatrix}$$

Observation 25

Sia \sim la relazione di coniugio. Date $\sigma, \sigma' \in \mathcal{S}_n$, si ha che:

$$\sigma \sim \sigma' \implies \text{sgn}(\sigma) = \text{sgn}(\sigma')$$

Dimostrazione:

- Se $\sigma \sim \sigma'$, allora

$$\exists \alpha \in \mathcal{S}_n \mid \sigma' = \alpha\sigma\alpha^{-1} \implies \text{sgn}(\sigma') = \text{sgn}(\alpha\sigma\alpha^{-1}) = \text{sgn}(\alpha)\text{sgn}(\sigma)\text{sgn}(\alpha^{-1})$$

- Dunque, poiché $\text{sgn}(\alpha) = \text{sgn}(\alpha^{-1}) = \pm 1 \implies \text{sgn}(\alpha)\text{sgn}(\alpha^{-1}) = 1$, se segue che:

$$\begin{aligned} \text{sgn}(\sigma') &= \text{sgn}(\alpha)\text{sgn}(\sigma)\text{sgn}(\alpha^{-1}) \implies \\ \implies \text{sgn}(\sigma') &= \begin{cases} 1 \cdot \text{sgn}(\sigma) \cdot 1 = \text{sgn}(\sigma) & \text{se } \text{sgn}(\alpha) = 1 \\ (-1) \cdot \text{sgn}(\sigma) \cdot (-1) = \text{sgn}(\sigma) & \text{se } \text{sgn}(\alpha) = -1 \end{cases} \implies \\ &\implies \text{sgn}(\sigma') = \text{sgn}(\sigma) \end{aligned}$$

□

Proposition 40

Data $\sigma \in \mathcal{S}_n$ e data la sua scomposizione in cicli $\sigma = \gamma_1 \dots \gamma_k$, si ha che:

$$\text{sgn}(\sigma) = (-1)^{n-k}$$

dove k è il numero di cicli

Dimostrazione:

- Sia $\sigma \in \mathcal{S}_n$ tale che

$$\sigma = (i_1 \dots i_{d_1})(i_{d_1+1} \dots i_{d_2}) \dots (j_1 \dots j_{d_k})$$

- Consideriamo una permutazione $\sigma' \in \mathcal{S}_n$ definita come:

$$\begin{aligned} \sigma' &= (1, \dots, d_1)(d_1 + 1, \dots, d_1 + d_2) \dots (n - d_k + 1, n - d_k + 2, \dots, n - 1, n) = \\ &= \begin{pmatrix} 1 & 2 & \dots & d_1 & d_1 + 1 & \dots & d_1 + d_2 & \dots & n - d_k + 1 & \dots & n \\ 2 & 3 & \dots & 1 & d_1 + 2 & \dots & d_1 + 1 & \dots & n - d_k + 2 & \dots & n - d_k + 1 \end{pmatrix} \end{aligned}$$

- Poiché σ e σ' hanno la stessa quantità di cicli ognuno avente la stessa lunghezza del ciclo corrispondente, ne segue che $\sigma \sim \sigma'$. Di conseguenza, si ha che

$$\sigma \sim \sigma' \implies \text{sgn}(\sigma) = \text{sgn}(\sigma')$$

dunque, ci basterà trovare il segno di σ' per ottenere il segno di σ

- A questo punto, le seguenti $d_1 - 1$ trasposizioni otteniamo che:

$$\begin{aligned} &\sigma \cdot \tau_{d_1-1, d_1} \cdot \tau_{d_1-2, d_1-1} \cdot \dots \cdot \tau_{2,3} \cdot \tau_{1,2} = \\ &= (1)(2) \dots (d_1 - 1)(d_1)(d_1 + 1, \dots, d_1 + d_2) \dots (n - d_k + 1, n - d_k + 2, \dots, n - 1, n) = \\ &= \begin{pmatrix} 1 & 2 & \dots & d_1 & d_1 + 1 & \dots & d_1 + d_2 & \dots & n - (d_k + 1) & \dots & n \\ 1 & 2 & \dots & d_1 & d_1 + 2 & \dots & d_1 + 1 & \dots & n - (d_k + 1) + 1 & \dots & n - (d_k + 1) \end{pmatrix} \end{aligned}$$

- Ripetendo tale procedimento per ogni ciclo di σ' , otteniamo la permutazione identica.
- Di conseguenza, il numero di trasposizioni componenti σ' corrisponde a:

$$\sum_{j=1}^k d_j - 1 = \sum_{j=1}^k d_j - \sum_{j=1}^k 1 = n - k$$

poiché la somma di tutte le lunghezze dei cicli corrisponde ad n .

- Dunque, poiché σ' è composta da $n - k$ trasposizioni adiacenti, concludiamo che:

$$\text{sgn}(\sigma) = \text{sgn}(\sigma') = (-1)^{n-k}$$

□

Capitolo 6

Morfismi

Definition 43. Morfismo

Date due strutture algebriche (G, \cdot) e (H, \odot) dello stesso tipo (dunque entrambe monoidi, gruppi, anelli, ...), definiamo come **morfismo** una funzione $f : G \rightarrow H$ tale che:

$$f(g \cdot h) = f(g) \odot f(h), \forall g, h \in G$$

Attenzione: se le strutture algebriche presentano più operazioni binarie, è necessario che la condizione di morfismo sia valida per ognuna di esse

Esempi:

- Dati i due gruppi (G, \cdot) e (H, \cdot) , la funzione $f : G \rightarrow H$ è un morfismo tra gruppi se e solo se:

$$f(gh) = f(g)f(h), \forall g, h \in G$$

- Dati i due gruppi (G, \cdot) e $(H, +)$, la funzione $f : G \rightarrow H$ è un morfismo tra gruppi se e solo se:

$$f(gh) = f(g) + f(h), \forall g, h \in G$$

- Dati i due anelli $(A, +, \cdot)$ e $(B, +, \cdot)$, la funzione $f : A \rightarrow B$ è un morfismo tra anelli se e solo se:

$$f(a + b) = f(a) + f(b), \forall a, b \in A$$

$$f(ab) = f(a)f(b), \forall a, b \in A$$

Observation 26

Dati due gruppi G ed H e un morfismo $f : G \rightarrow H$, si ha che:

1. $f(1_G) = 1_H$
2. $f(g^{-1}) = f(g)^{-1}, \forall g \in G$

dove 1_G ed 1_H sono rispettivamente l'elemento neutro di G ed H

Dimostrazione:

1. Dato $g \in G$, per le proprietà del morfismo f ne segue che:

$$\begin{aligned} f(g) &= f(1_G \cdot g) = f(1_G)f(g) \implies f(g)f(g)^{-1} = f(1_G)f(g)f(g)^{-1} \implies \\ &\implies 1_H = f(1_G) \cdot 1_H \implies f(1_G) = 1_H \end{aligned}$$

2. Dato $g \in G$, per le proprietà del morfismo f ne segue che:

$$\begin{aligned} f(1_G) &= 1_H \implies f(g \cdot g^{-1}) = 1_H \implies f(g)f(g^{-1}) = 1_H \implies \\ &\implies f(g^{-1}) = 1_H \cdot f(g)^{-1} \implies f(g^{-1}) = f(g)^{-1} \end{aligned}$$

□

6.1 Isomorfismi, Endomorfismi ed Automorfismi

Definition 44. Isomorfismo, Endomorfismo ed Automorfismo

Date due strutture algebriche G, H ed una funzione $f : G \rightarrow H$, definiamo f come:

- **Isomorfismo** se è un **morfismo** ed è **biettiva**
- **Endomorfismo** se è un morfismo e $G = H$, ossia è un **morfismo sullo stesso gruppo**
- **Automorfismo** se è un **isomorfismo** e un **endomorfismo**

Observation 27

Se $f : G \rightarrow H$ è un isomorfismo, esiste sempre l'isomorfismo inverso $f^{-1} : H \rightarrow G$

Dimostrazione:

- Se $f : G \rightarrow H$ è un isomorfismo, dunque è biettiva, allora $\exists f^{-1} : H \rightarrow G$ poiché una funzione è biettiva se e solo se è invertibile. Inoltre, poiché $(f^{-1})^{-1} = f$, anche f^{-1} è invertibile e dunque biettiva
- Dati $g, h \in H$, mostriamo che f^{-1} sia anche un morfismo:

$$\begin{aligned} gh &= f(f^{-1}(g))f(f^{-1}(h)) \implies gh = f((f^{-1}(g)(f^{-1}(h))) \implies \\ &\implies f^{-1}(gh) = f^{-1}(f((f^{-1}(g)(f^{-1}(h)))) \implies f^{-1}(gh) = f^{-1}(g)f^{-1}(h) \end{aligned}$$

□

Observation 28

Se $f : G \rightarrow H$ e $g : H \rightarrow K$ sono due isomorfismi, la loro composta $g \circ f : G \rightarrow K$ è un isomorfismo

Dimostrazione:

- Poiché la composizione di due funzioni biettive è anch'essa biettiva, si ha che

$$h := g \circ f : G \rightarrow K \text{ biettiva}$$

- Dati $x, y \in G$, mostriamo che h sia anche un morfismo:

$$h(xy) = g(f(xy)) = g(f(x)f(y)) = g(f(x))g(f(y)) = h(x)h(y)$$

□

Definition 45. Relazione di isomorfismo

Date due strutture algebriche G ed H , definiamo la **relazione di equivalenza** " G è **isomorfo** ad H ", indicato come $G \cong H$, se e solo se esiste un isomorfismo $f : G \rightarrow H$.

$$G \cong H \iff \exists f : G \rightarrow H \text{ isomorfismo}$$

Dimostrazione:

- Per ogni gruppo G esiste l'automorfismo $\text{id} : G \rightarrow G : g \rightarrow g$

$$\text{id}(gh) = gh = \text{id}(g)\text{id}(h), \forall g, h \in G \implies G \cong G$$

- Se $G \cong H$ allora:

$$G \cong H \implies \exists f : G \rightarrow H \text{ isomorfismo} \iff$$

$$\iff \exists f^{-1} : H \rightarrow G \text{ isomorfismo inverso} \implies H \cong G$$

- Se $G \cong H, H \cong K$ allora:

$$G \cong H, H \cong K \implies \exists f : G \rightarrow H \text{ isomorfismo}, \exists g : H \rightarrow K \text{ isomorfismo} \implies$$

$$\implies g \circ f : G \rightarrow K \text{ isomorfismo} \implies G \cong K$$

□

Esempi:

1. • Dato $n \in \mathbb{Z}$, definiamo come **radice n-esima dell'unità**, ossia il numero 1, un elemento $z \in \mathbb{C}$ tale che $z^n = 1$.
 • Come già visto nella sezione 2.3, l'equazione $z^n = 1$ dove $z \in \mathbb{C}$ ammette n radici. Di conseguenza, esistono n radici n-esime (z_0, \dots, z_{n-1}) tali che $z_k^n = 1$, dove $z_k := e^{i \cdot \frac{2\pi k}{n}}$.
 • Inoltre, poiché tutte le z_k differiscono solo di k all'esponente, denotiamo $\zeta := e^{i \cdot \frac{2\pi}{n}}$, ottenendo quindi che $\zeta^k = z_k$ (tale operazione risulta essere più comoda poiché ci permette di utilizzare le proprietà delle potenze)

- Definiamo quindi il seguente insieme:

$$H^n = \{z \in \mathbb{C} \mid z^n = 1\} = \{\zeta^0, \dots, \zeta^{n-1}\}$$

e dimostriamo che $(H^n, \cdot) \leq (\mathbb{C}^*, \cdot)$:

- $1 = \zeta^0 \implies 1 \in H^n$
- $z, w \in H^n \iff z^n = w^n = 1 \implies 1 = z^n w^n = (zw)^n \implies zw \in H^n$
- $z \in H^n \iff z^n = 1 \implies (z^{-1})^n = (z^n)^{-1} = 1^{-1} = 1 \implies z^{-1} \in H^n$

- Definiamo inoltre la seguente funzione

$$f : (\mathbb{Z}_n, +) \rightarrow (H^n, \cdot) : [k] \mapsto \zeta^k$$

la quale risulta essere biettiva poiché $|\mathbb{Z}_n| = |H^n|$.

- Posto $[k] := [i] + [j]$ dove $[i], [j] \in \mathbb{Z}_n$, si ha che:

$$[k] = [i] + [j] \iff i + j = k + nh, \exists h \in \mathbb{Z} \iff i + j - nh = k$$

- Verifichiamo quindi che f sia anche un morfismo:

$$f([i] + [j]) = f([k]) = \zeta^k = \zeta^{i+j-nh} = \zeta^i \zeta^j \zeta^{-nh} = \zeta^i \zeta^j (\zeta^n)^{-h} = \zeta^i \zeta^j = f([i])f([j])$$

- Dunque, si ha che $\mathbb{Z}_n \cong H^n$

- Sia G un gruppo e sia $g \in G$. La funzione $f : (\mathbb{Z}, +) \rightarrow (G, \cdot) : n \mapsto g^n$ è un morfismo:

$$f(n + m) = g^{n+m} = g^n g^m = f(n)f(m)$$

- Supponiamo per assurdo che f non sia iniettiva e che $o(g) = +\infty$, implicando che:

$$\begin{aligned} \exists n \neq m \mid f(n) = f(m) &\implies g^n = g^m \implies \\ \implies 1_G = g^0 = g^{n-n} = g^{m-n} &\implies \exists m-n \neq 0 \mid g^{m-n} = 1_G \implies m-n \neq 0 \in I(g) \end{aligned}$$

- Tuttavia, come dimostrato nella sezione 4.9, abbiamo che $o(g) = +\infty \iff I(g) = I(0)$ e poiché $m - n \neq 0 \implies m - n \notin I(g) = I(0)$, siamo giunti ad una contraddizione. Dunque, l'unica possibilità è che $o(g) < +\infty$
- Dunque, concludiamo che f non iniettiva $\implies o(g) = +\infty$ e di conseguenza che $o(g) < +\infty \implies f$ iniettiva

- Dato il gruppo (G, \cdot) e $g \in G$, la funzione $f_g : G \rightarrow G : h \mapsto ghg^{-1}$ è un endomorfismo:

$$f_g(h)f_g(h') = (ghg^{-1})(gh'g^{-1}) = ghgh'g^{-1} = f_g(hh')$$

Observation 29

La proiezione canonica al quoziente $\pi : (\mathbb{Z}, +, \cdot) \rightarrow (\mathbb{Z}_n, +, \cdot) : x \rightarrow [x]$ è un **morfismo suriettivo** di anelli

Dimostrazione:

- Sappiamo già che π sia suriettiva. Verifichiamo quindi che sia un morfismo di anelli:

$$\pi(x + y) = [x + y] = [x] + [y] = \pi(x) + \pi(y)$$

$$\pi(xy) = [xy] = [x][y] = \pi(x)\pi(y)$$

□

6.2 Nucleo ed Immagine di un morfismo

Proposition 41. Nucleo ed Immagine di un morfismo

Dato un morfismo $f : G \rightarrow H$, viene sempre generato $\text{Ker}(f) \leq G$, detto **nucleo di f** , e $\text{Im}(f) \leq H$, detto **immagine di f** , dove:

$$\text{Ker}(f) : \{g \in G \mid f(g) = 1_H\}$$

$$\text{Im}(f) : \{y \in H \mid f(x) = y, \exists x \in G\}$$

Dimostrazione:

- $\text{Ker}(f) \leq G$:
 - $f(1_G) = 1_H \implies 1_G \in \text{Ker}(f)$
 - $x, y \in \text{Ker}(f) \implies f(x) = f(y) = 1_H \implies f(xy) = f(x)f(y) = 1_H \cdot 1_H = 1_H \implies xy \in \text{Ker}(f)$
 - $x \in \text{Ker}(f) \implies f(x) = 1_H \implies 1_H = 1_H^{-1} = f(x)^{-1} = f(x^{-1}) \implies x^{-1} \in \text{Ker}(f)$
- $\text{Im}(f) \leq H$:
 - $f(1_G) = 1_H \implies 1_H \in \text{Im}(f)$
 - $x, y \in \text{Im}(f) \implies x = f(g), y = f(h) \implies xy = f(g)f(h) = f(gh) \implies xy \in \text{Im}(f)$
 - $x \in \text{Im}(f) \implies x = f(g) \implies x^{-1} = f(g)^{-1} = f(g^{-1}) \implies x^{-1} \in \text{Im}(f)$

□

Observation 30

Un morfismo è **iniettivo** se e solo se il nucleo è **semplice**, ossia $\text{Ker}(f) = \{1_G\}$

Dimostrazione:

- Poiché $\text{Ker}(f) \leq G \implies 1_G \in \text{Ker}(f)$, supponiamo per assurdo che f iniettiva e che $\exists x \neq 1_G \in \text{Ker}(f)$:

$$g \neq 1_G \in \text{Ker}(f) \implies f(g) = 1_H = f(1_G)$$

contraddicendo l'ipotesi per cui f sia iniettiva, dunque l'unica possibilità è che

$$\nexists g \neq 1_G \in \text{Ker}(f) \implies \text{Ker}(f) = \{1_G\}$$

- Supponiamo invece che $\text{Ker}(f) = \{1_G\}$. In tal caso, si ha che:

$$\begin{aligned} \forall g, g' \in G, f(g) = f(g') &\iff f(g^{-1})f(g) = f^{-1}(g)f(g') \iff \\ &\iff 1_H = f^{-1}(g)f(g') \iff 1_H = f(g^{-1}g) \end{aligned}$$

Tuttavia, poiché $\text{Ker}(f) = \{1_G\}$, si ha che $f(x) = 1_H, \forall x \in G \iff x = 1_G$, allora

$$1_H = f(g^{-1}g) \iff 1_G = g^{-1}g' \iff g = g'$$

dunque, f risulta essere iniettiva

□

Observation 31

Se $f : A \rightarrow B$ è un morfismo di anelli, allora:

$$\text{Ker}(f) : \{a \in A \mid f(a) = 0_B\}$$

$$\text{Im}(f) : \{b \in B \mid f(a) = b, \exists a \in A\}$$

6.3 Teorema fondamentale di isomorfismo

Definition 46. Sottoanello

Sia A un anello. Definiamo $(B, +, \cdot) \subseteq (A, +, \cdot)$ come **sottoanello** se:

- $(B, +) \leq (A, +)$
- $x, y \in B \implies xy \in B$

Observation 32

Se $f : A \rightarrow B$ è un morfismo di anelli, allora

- $Ker(f)$ è un **ideale** di A
- $Im(f)$ è **sottoanello** di B

Dimostrazione:

- Abbiamo già dimostrato che $Ker(f) \leq A$ e $Im(f) \leq B$.
- $x \in Ker(f), y \in A \implies f(xy) = f(x)f(y) = 0_B \cdot f(y) = 0_B \implies xy \in Ker(f)$
- $x, y \in Im(f) \iff x = f(a), y = f(b), \exists a, b \in A \implies xy = f(a)f(b) = f(ab) \implies xy \in Im(f)$

□

Theorem 42. Teorema fondamentale di isomorfismo

Se $f : A \rightarrow B$ è un morfismo tra anelli, allora

$$A/Ker(f) \cong Im(f)$$

Dimostrazione:

- Mostriamo che esiste $\varphi : A/Ker(f) \rightarrow Im(f) : [a] \mapsto f(a)$ e che è **ben definita**, ossia che $[a], [b] \in A/Ker(f) \mid [a] = [b] \implies f(a) = f(b)$:

$$\begin{aligned} [a] = [b] &\iff a \equiv b \pmod{Ker(f)} \iff b - a \in Ker(f) \iff \\ &\iff 0_B = f(b - a) = f(b) - f(a) \iff f(a) = f(b) \end{aligned}$$

- Mostriamo che φ è un **morfismo** sia un morfismo di anelli:

$$\begin{aligned} \varphi([a]) + \varphi([b]) &= f(a) + f(b) = f(a + b) = \varphi([a + b]) \\ \varphi([a])\varphi([b]) &= f(a)f(b) = f(ab) = \varphi([ab]) \end{aligned}$$

- Mostriamo che φ è **iniettiva** poiché il suo nucleo è semplice:

$$\begin{aligned} [x] \in Ker(\varphi) &\iff \varphi([x]) = 0_B \iff f(x) = 0_B \iff \\ &\implies x \in Ker(f) \iff x \in [0_A] \iff [x] = [0_A] \implies Ker(\varphi) = \{[0_A]\} \end{aligned}$$

- Mostriamo che φ è **suriettiva** poiché il suo codominio, ossia $Im(f)$, coincide con la sua immagine, ossia $Im(\varphi)$:

$$\begin{aligned} f(a) \in Im(\varphi) &\iff \exists [a] \in A/Ker(f) \mid \varphi([a]) = f(a) \iff \\ &\iff \exists a \in A \mid \varphi([a]) = f(a) \iff \varphi([a]) \in Im(f) \end{aligned}$$

- Concludiamo quindi che $\varphi : A/Ker(f) \rightarrow Im(f)$ è un **isomorfismo** e dunque che

$$A/Ker(f) \cong Im(f)$$

□

6.4 Sottogruppi normali

Definition 47. Classi laterali sinistre e destre

Dati G gruppo e $H \leq G$, definiamo le seguenti due relazioni di equivalenza:

$$x \sim_{sx} y \iff x^{-1}y \in H \qquad x \sim_{dx} y \iff xy^{-1} \in H$$

Definiamo come **classi laterali sinistre** le classi di equivalenza generate da \sim_{sx} e come **classi laterali destre** le classi di equivalenza generate da \sim_{dx} .

$$[x]_{sx} : \{y \in G \mid x \sim_S y\} \qquad [x]_{dx} : \{y \in G \mid x \sim_D y\}$$

(*dimostrazione equivalenza analoga alla sezione 4.1.1*)

Definition 48. Insieme quoziente sinistro e destro

Dati G gruppo e $H \leq G$, denotiamo come G/H_{sx} l'**insieme quoziente** generato da \sim_{sx} e come G/H_{dx} l'**insieme quoziente** generato da \sim_{dx} .

Nel caso in cui non sia specificato il pedice, ossia G/H , verrà sottointeso che si tratti di uno qualsiasi dei due insiemi quozienti, poiché irrilevante

Observation 33

Dati G gruppo, $H \leq G$ e le due relazioni \sim_{sx} e \sim_{dx} , si ha che:

$$[x]_{sx} = xH = \{xh \mid h \in H\} \qquad [x]_{dx} = Hx = \{hx \mid h \in H\}$$

Inoltre, si ha che:

$$|xH| = |H| = |Hx|$$

(*dimostrazioni analoghe alla sezione 4.1.1*)

Observation 34

Dati G gruppo finito e $H \leq G$, si ha che:

$$[G : H] := |G/H_{sx}| = |G/H_{dx}|$$

Dimostrazione:

- Poiché sia G/H_{sx} sia G/H_{dx} sono partizioni di G le cui classi laterali possiedono tutte la stessa cardinalità di H , si ha che:

$$|G/H_{sx}| = \frac{|G|}{|H|} = |G/H_{dx}|$$

□

Observation 35

La **classe neutra**, ossia generata dall'elemento neutro di G , è sia una classe laterale **sinistra** sia una classe laterale **destra**:

$$[1_G]_{sx} = 1_G \cdot H = H = H \cdot 1_G = [1_G]_{dx}$$

Definition 49. Sottogruppo normale

Sia G un gruppo. Definiamo H come **sottogruppo normale** di G , indicato come $H \trianglelefteq G$, se:

- $H \leq G$
- $\forall x \in G$ si ha che $xH = Hx$, ossia la classe laterale sinistra di ogni elemento coincide con la classe laterale destra dell'elemento stesso

Attenzione: tale condizione non implica che valga la commutatività tra elementi di G ed elementi di H (ossia che valga $gh = hg, \forall g \in G, \forall h \in H$)

Proposition 43

Sia G un gruppo. Le seguenti condizioni sono **equivalenti**:

1. $H \trianglelefteq G$
2. $\forall g \in G, h \in H$ si ha che $ghg^{-1} \in H$
3. $\forall g \in G, h \in H, \exists k \in H \mid gh = kg$

Dimostrazione:

- 1) \implies 3)

$$g \in G, h \in G \implies gh \in gH = Hg = \{kg \mid k \in H\} \implies \exists k \in H \mid gh = kg$$

- 3) \implies 2)

$$g \in G, h \in H, \exists k \in H \mid gh = kg \implies ghg^{-1} = kgg^{-1} \implies ghg^{-1} = k \in H$$

- 2) \implies 1)

– Dato $g \in G$, si ha che:

$$\begin{aligned} gh \in gH &\implies g \in G, h \in H \implies x := ghg^{-1} \in H \implies \\ &\implies xg = ghg^{-1}g \in Hg \implies xg = gh \implies gh \in Hg \implies gH \subseteq Hg \end{aligned}$$

– Analogamente, si ha che:

$$\begin{aligned} kg \in Hg &\implies g \in G, h \in H \implies \exists g^{-1} \in G \implies y := g^{-1}k(g^{-1})^{-1} = g^{-1}kg \in H \\ &\implies gy = gg^{-1}kg \in gH \implies gy = kg \in gH \implies kg \in gH \implies Hg \subseteq gH \end{aligned}$$

- Dunque, poiché $\forall g \in G$ si ha che $gh = Hg$, ne segue che $H \trianglelefteq G$

□

Observation 36

Se G un **gruppo abeliano** e $H \leq G$, allora $H \trianglelefteq G$

Dimostrazione:

- Poiché G è abeliano e poiché $k \in H \implies k \in G$, ne segue che:

$$\forall g \in G, h \in H, \exists h \in H \mid gh = hg$$

dunque $H \trianglelefteq G$

□

Proposition 44

Se (G, \cdot) è un gruppo e $H \trianglelefteq G$, allora $(G/H, \cdot)$ è un **gruppo**

Dimostrazione:

- Dimostriamo che il prodotto $[x][y] = [xy]$ sia ben definito, ossia che $[x] = [x'], [y] = [y'] \implies [xy] = [x'y']$
 - Poiché $H \trianglelefteq G$ e poiché $[x] = [x'], [y] = [y']$, si ha che:

$$xH = Hx = [x] = [x'] = x'H = Hx'$$

$$yH = Hy = [y] = [y'] = y'H = Hy'$$

- Di conseguenza, otteniamo che:

$$\begin{aligned} x'y'h \in x'y'H = [x'y'] &\implies \exists k, j \in H \mid x'y'h = x(ky') = \\ &= (xk)y' = (jx)y = jxy \implies x'y'h \in Hxy = [xy] \end{aligned}$$

e che:

$$\begin{aligned} xyb \in xyH = [xy] &\implies \exists d, q \in H \mid xyb = x(dy') = (xd)y' = \\ &= (qx')y' = qx'y' \implies xyb \in Hx'y' = [x'y'] \end{aligned}$$

dunque il prodotto è ben definito

- Dimostriamo quindi che $(G/H, \cdot)$ sia un gruppo
 - $([x][y])[z] = [xy][z] = [xyz] = [x][yz] = [x]([y][z])$
 - $\forall [x] \in G/H, \exists [1_G] \in G/H \mid [x][1_G] = [x \cdot 1_G] = [x]$
 - $\forall [x] \in G/H, \exists [x]^{-1} \in G/H \mid [x][x]^{-1} = [x][x^{-1}] = [xx^{-1}] = [1_G]$

□

Corollary 17

Se (G, \cdot) è un gruppo abeliano e $H \trianglelefteq G$, allora $(G/H, \cdot)$ è un **gruppo abeliano**

Dimostrazione:

- Sappiamo già che $(G/H, \cdot)$ è un gruppo, dunque verifichiamo che valga la commutatività:

$$[x], [y] \in G/H \implies [x][y] = [xy] = [yx] = [y][x]$$

□

Observation 37

Dato G gruppo e $H \leq G$, si ha che:

$$[G : H] = 2 \implies H \trianglelefteq G$$

Dimostrazione:

- Supponiamo che $[G : H] = 2$, implicando che esistano solo due classi laterali sinistre e due classi laterali destre. Poiché la classe neutra $[1_G]_{sx} = H = [1_G]_{dx}$ è condivisa da entrambi gli insiemi quozienti, ne segue che:

$$G/H_{sx} = \{[1_G], [x]\}$$

$$G/H_{dx} = \{[1_G], [y]\}$$

- Poiché G/H è una partizione di G , ne segue che:

$$z \in [x] \iff z \notin [1_G]_{sx} = [1_G]_{dx} \iff z \in [y]$$

implicando quindi che $[x] = [y]$ e di conseguenza che $H \trianglelefteq G$

- In particolare, si ha che:

$$G/H_{sx} = \{H, G - H\}$$

$$G/H_{dx} = \{H, G - H\}$$

□

Corollary 18

Dato \mathcal{S}_n , si ha che $\mathcal{A}_n \trianglelefteq \mathcal{S}_n$

Dimostrazione:

- Poiché $\mathcal{A}_n \leq \mathcal{S}_n$ e poiché $[\mathcal{S}_n : \mathcal{A}_n] = 2$ (sezione 5.2), ne segue che $\mathcal{A}_n \trianglelefteq \mathcal{S}_n$

□

Observation 38

Se $f : G \rightarrow H$ è un morfismo di gruppi, allora $\text{Ker}(f) \trianglelefteq G$ e $\text{Im}(f) \leq H$

Dimostrazione:

- Sappiamo già che $\text{Ker}(f) \leq G$ e $\text{Im}(f) \leq H$
- Verifichiamo quindi che $\text{Ker}(f) \trianglelefteq G$

$$\begin{aligned} g \in G, h \in \text{Ker}(f) &\implies f(ghg^{-1}) = f(g)f(h)f(g)^{-1} = f(g) \cdot 1_H \cdot f(g)^{-1} = \\ &= f(g)f(g)^{-1} = 1_H \implies ghg^{-1} \in \text{Ker}(f) \implies \text{Ker}(f) \trianglelefteq G \end{aligned}$$

□

Corollary 19. Teorema fondamentale di isomorfismo

Se $f : G \rightarrow H$ è un morfismo tra gruppi, allora:

$$G/\text{Ker}(f) \cong \text{Im}(f)$$

Dimostrazione:

- Poiché $\text{Ker}(f) \trianglelefteq G$, sappiamo che $(G/\text{Ker}(f), \cdot)$ sia un gruppo con l'operazione di prodotto ben definita. A questo punto, la dimostrazione risulta essere analoga a quella vista nel caso degli anelli (sezione 6.3)

□

Proposition 45

Sia gruppo G e sia $g \in G$. Posto $d := o(g)$, si ha che:

$$H(g) \cong \begin{cases} \mathbb{Z} & \text{se } d = 0 \\ \mathbb{Z}_d & \text{se } d > 0 \end{cases}$$

Dimostrazione:

- Riprendiamo il seguente morfismo di gruppi $f : \mathbb{Z} \rightarrow G : n \rightarrow g^n$, già visto negli esempi precedenti

$$f(n+m) = g^{n+m} = g^n g^m = f(n)f(m)$$

- Di conseguenza, per il teorema fondamentale di isomorfismo si ha che:

$$\mathbb{Z}/\text{Ker}(f) \cong \text{Im}(f)$$

- Tuttavia, notiamo che:

$$\text{Im}(f) = \{f(n) \mid n \in \mathbb{Z}\} = \{g^n \mid n \in \mathbb{Z}\} = H(g)$$

$$\text{Ker}(f) = \{n \in \mathbb{Z} \mid g^n = 1_G\} = I(g)$$

- Dunque, si ha che:

$$\mathbb{Z}/I(g) = \mathbb{Z}/Ker(f) \cong Im(f) = H(g)$$

- Poiché in \mathbb{Z} si ha che: $\exists! d \geq 0 \mid I(g) = I(d)$ tale che:

$$- d = 0 \implies o(g) := |H(g)| = +\infty$$

$$- d > 0 \implies o(g) := |H(g)| = d$$

ne segue che:

$$\mathbb{Z}_d := \mathbb{Z}/I(d) = \mathbb{Z}/I(g) = \mathbb{Z}/Ker(f) \cong Im(f) = H(g)$$

- In particolare, se $d = 0$, per ogni $[x] \in \mathbb{Z}_0$, si ha che:

$$[y] = [x] \iff x \sim y \iff y - x \in I(0) \iff$$

$$\iff x - y = 0k, \exists k \in \mathbb{Z} \iff x - y = 0 \iff x = y$$

- Di conseguenza, ne segue che proiezione canonica al quoziente $\pi : \mathbb{Z} \rightarrow \mathbb{Z}_0 : x \mapsto [x]$, la quale sappiamo già essere un morfismo suriettivo, sia anche iniettiva, risultando quindi in un isomorfismo

$$\forall x, y \in \mathbb{Z} \mid x \neq y \implies [x] \neq [y] \implies \pi(x) \neq \pi(y)$$

da cui concludiamo che:

$$H(g) \cong \mathbb{Z}_0, \mathbb{Z}_0 \cong \mathbb{Z} \implies H(g) \cong \mathbb{Z}$$

- In definitiva, concludiamo che:

$$H(g) = Im(f) \cong \mathbb{Z}/Ker(f) = \mathbb{Z}/I(g) = \mathbb{Z}/I(d) = \begin{cases} \mathbb{Z}_0 \cong \mathbb{Z} & \text{se } d = 0 \\ \mathbb{Z}_d & \text{se } d > 0 \end{cases}$$

□

Corollary 20

Dato G un gruppo finito dove $|G| = n$, con $n \in \mathbb{N}$, si ha che:

$$\exists g \in G \mid o(g) = n \implies G \cong \mathbb{Z}_n$$

Dimostrazione:

- Supponiamo che $\exists g \in G \mid o(g) = n$. In tal caso, per la proposizione precedente, si ha che:

$$o(g) = n \implies H(g) \cong \mathbb{Z}_n$$

- Siccome $H(g) \leq G \implies H(g) \subseteq G$ e $|H(g)| = |G|$, allora ne segue che $G = H(g)$, implicando quindi che:

$$G = H(g) \cong \mathbb{Z}_n$$

□

Corollary 21

Se G è un gruppo finito e $|G| = p$ dove $p \in \mathbb{P}$, allora

$$G \cong \mathbb{Z}_p$$

Dimostrazione:

- Poiché $|G| = p$ ne segue che $\exists g \in G \mid g \neq 1_G$.
- Dato $H(g) \leq G$, per il teorema di Lagrange, si ha che

$$|H(g)| \mid |G| = p \implies |H(g)| = \begin{cases} 1 \\ p \end{cases}$$

- Poiché $g \neq 1_G \implies |H(g)| > 1$, ne segue che l'unica possibilità sia $o(p) := |H(g)| = p$.
- Di conseguenza, per il corollario precedente, ne segue che:

$$o(g) = p \implies G = H(g) \cong \mathbb{Z}_p$$

□

Observation 39

Sia G un gruppo. Se $H \trianglelefteq G$ allora la proiezione canonica al quoziente $\pi : (G, \cdot) \rightarrow (G/H, \cdot) : x \rightarrow [x]$ è un morfismo suriettivo e $\text{Ker}(\pi) = H$

Dimostrazione:

- Sappiamo già che $\pi : (G, \cdot) \rightarrow (G/H, \cdot) : x \rightarrow [x]$ sia un morfismo suriettivo
- Verifichiamo quindi che $\text{Ker}(\pi) = H$:

$$g \in \text{Ker}(\pi) \iff \pi(g) = [1_G] \iff [g] = [1_G] = H \iff g \in [g] = H$$

□

Esempio:

- La funzione $\text{sgn} : \mathcal{S}_n \rightarrow \{+1, -1\}$ è un morfismo

$$\text{sgn}(\sigma\sigma') = \text{sgn}(\sigma)\text{sgn}(\sigma')$$

- Dunque, per il teorema fondamentale di isomorfismo, si ha che:

$$\mathcal{S}_n / \text{Ker}(\text{sgn}) \cong \text{Im}(\text{sgn})$$

- Inoltre, si ha che:

$$\begin{aligned} \text{Ker}(\text{sgn}) &= \{\sigma \in \mathcal{S}_n \mid \text{sgn}(\sigma) = +1\} = \mathcal{A}_n \trianglelefteq \mathcal{S}_n \implies \\ \implies [\mathcal{S}_n : \text{Ker}(\text{sgn})] &= [\mathcal{S}_n : \mathcal{A}_n] = 2 \implies |\text{Im}(\text{sgn})| = 2 \implies \text{Im}(\text{sgn}) = \{+1, -1\} \end{aligned}$$

6.5 Gruppi diedrali

Definition 50. Gruppo diedrale

Definiamo come **gruppo diedrale** \mathcal{D}_n il gruppo delle **simmetrie di un poligono regolare di n lati**, dove con simmetrie intendiamo tutte le azioni che mantengono la figura simmetrica, ossia:

- Rotazioni di un angolo giro (ossia $\frac{2\pi}{n}$) in senso antiorario (o orario, vista come l'inverso di una rotazione antioraria)

$$\rho: \text{rotazione antioraria di } \frac{2\pi}{n}$$

- Riflessioni a specchio rispetto agli assi di simmetria del poligono (ogni poligono regolare possiede n assi di simmetria)

$$\sigma_i: \text{riflessione rispetto all'asse di simmetria } r_i$$

Attenzione: il prodotto è dato dalla composizione (dunque viene trattato come nel caso delle permutazioni), ossia $\rho\sigma(i) = \rho(\sigma(i))$

Observation 40

Dato \mathcal{D}_n , effettuare n volte una rotazione riporta il poligono allo stato iniziale (poiché $n \cdot \frac{2\pi}{n} = 2\pi$), dunque

$$\rho^n = \rho^0 = 1 \implies \rho^{n+k} = \rho^n \rho^k = \rho^0 \rho^k = \rho^k$$

Analogamente, poiché un poligono regolare di n lati possiede solo n assi di simmetria, si ha che:

$$\sigma_n = \sigma_0 \implies \sigma_{n+k} = \sigma_k$$

Observation 41

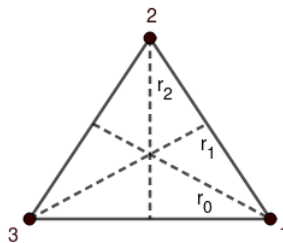
Per definizione stessa, ogni riflessione a specchio è uguale alla sua inversa.

Dunque, riflettere due volte rispetto allo stesso asse corrisponde alla simmetria neutra, ossia $\rho^0 = 1$

$$\sigma_i = \sigma_i^{-1} \implies \sigma_i^2 = 1$$

Esempi:

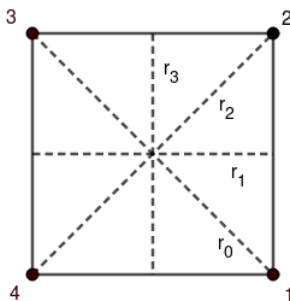
- Consideriamo il gruppo \mathcal{D}_3 , corrispondente alle simmetrie di un triangolo equilatero.



In tal caso, abbiamo che:

$$\mathcal{D}_3 : \{1, \rho, \rho^2, \sigma_0, \sigma_1, \sigma_2\}$$

- Consideriamo il gruppo \mathcal{D}_4 , corrispondente alle simmetrie di un quadrato.

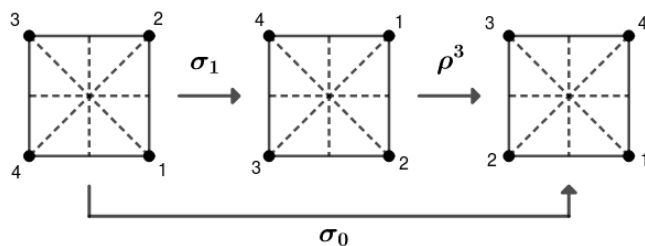


In tal caso, abbiamo che:

$$\mathcal{D}_4 : \{1, \rho, \rho^2, \rho^3, \sigma_0, \sigma_1, \sigma_2, \sigma_3\}$$

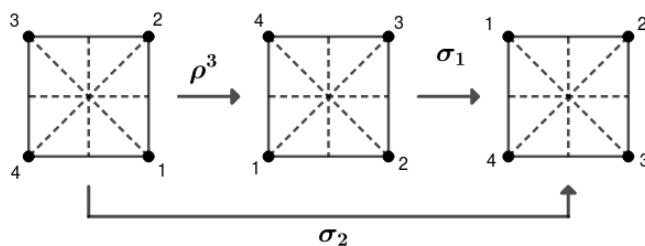
Notiamo inoltre come in \mathcal{D}_4 si ha:

$$\rho^3 \sigma_1 = \sigma_0$$



E che:

$$\sigma_1 \rho^3 = \sigma_2$$



Dunque, concludiamo che il prodotto non sia commutativo:

$$\rho^3 \sigma_1 \neq \sigma_1 \rho^3$$

Observation 42

Dato il gruppo \mathcal{D}_n , si ha che:

- $\rho^i \rho^j = \rho^{i+j(\bmod n)}$
- $\sigma_i \sigma_j = \rho^{i-j(\bmod n)}$
- $\rho^i \sigma_j = \sigma_{i+j(\bmod n)}$
- $\sigma_i \rho^j = \sigma_{i-j(\bmod n)}$

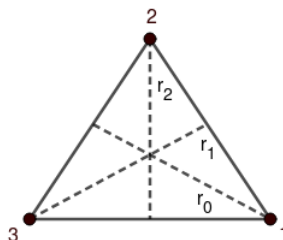
Proposition 46

Numerando i vertici del poligono, ogni simmetria **corrisponde** ad una permutazione dei vertici, dunque si verifica che \mathcal{D}_n è **iniettivamente incluso** in \mathcal{S}_n .

In generale, se $\alpha \in \mathcal{D}_n$, ovvero una simmetria del poligono regolare di n lati, manda il vertice i nel vertice j , allora la corrispondente permutazione $\sigma_\alpha \in \mathcal{S}_n$ manderà anch'essa i in j

Esempio:

- Consideriamo il gruppo \mathcal{D}_3 , numerando i vertici del triangolo corrispondente



In tal caso abbiamo che:

$$\begin{aligned} 1 &= \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} & \rho &= \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} & \rho^2 &= \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \\ \sigma_0 &= \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} & \sigma_1 &= \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} & \sigma_2 &= \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \end{aligned}$$

Corollary 22

Dato il gruppo \mathcal{D}_n e dato $H_n \subseteq \mathcal{S}_n$ dove:

$$H : \{\sigma_\alpha \in \mathcal{S}_n \mid \sigma_\alpha = \alpha, \exists \alpha \in \mathcal{D}_n\}$$

si ha che:

$$\mathcal{D}_n \cong H \leq \mathcal{S}_n$$

Dimostrazione:

- Posto $H_n : \{\sigma_\alpha \in \mathcal{S}_n \mid \sigma_\alpha = \alpha, \exists \alpha \in \mathcal{D}_n\}$, ogni simmetria in \mathcal{D}_n corrisponde ad una permutazione in $H \leq \mathcal{S}_n$, dunque si ha che:

$$\begin{cases} \alpha = \sigma_\alpha : i \mapsto j \\ \beta = \sigma_\beta : j \mapsto k \end{cases} \implies \beta\alpha = \sigma_\beta\sigma_\alpha : i \mapsto k$$

- Inoltre, si ha che:

$$\beta\alpha \in \mathcal{D}_n \implies \exists \sigma_{\beta\alpha} \in H_n \mid \sigma_{\beta\alpha} = \beta\alpha = \sigma_\beta\sigma_\alpha$$

- Definiamo quindi la funzione $f : (\mathcal{D}_n, \cdot) \rightarrow (H_n, \cdot) : \alpha \mapsto \sigma_\alpha$, la quale risulta essere un morfismo poiché:

$$f(\beta\alpha) = \sigma_{\beta\alpha} = \sigma_\beta\sigma_\alpha = f(\beta)f(\alpha)$$

- In particolare, f risulta essere suriettiva poiché

$$\forall \sigma_\alpha \in H_n, \exists \alpha \in \mathcal{D}_n \mid f(\alpha) = \sigma_\alpha$$

- Infine, poiché $|\mathcal{D}_n| = |H, n|$, ne segue che f possa essere suriettiva se e solo se è anche iniettiva, dunque f è un isomorfismo

□

6.6 Gruppo di Klein e Teorema di Cauchy

Definition 51. Gruppo di Klein

Definiamo come **gruppo di Klein** (o gruppo quadrimo) il più piccolo gruppo non ciclico:

$$\mathcal{K}_4 : \{1, a, b, c\}$$

dove si verifica che:

- $a^2 = b^2 = c^2 = 1 \implies o(a) = o(b) = o(c) = 2$
- $ab = ba = c$
- $bc = cb = a$
- $ac = ca = b$

Esempio:

- Consideriamo il gruppo $\mathcal{D}_2 : \{1, \rho, \sigma_0, \sigma_1\}$. Notiamo come:

$$- \rho^2 = \sigma_0^2 = \sigma_1^2 = 1$$

$$- \rho\sigma_0 = \sigma_0\rho = \sigma_1$$

$$- \rho\sigma_1 = \sigma_1\rho = \sigma_0$$

$$- \sigma_1\sigma_0 = \sigma_0\sigma_1 = \rho$$

Dunque, concludiamo facilmente che $\mathcal{D}_2 \cong \mathcal{K}_4$

Proposition 47

Se G è un gruppo finito dove $|G| = 4$, si verifica che:

$$G \cong \mathbb{Z}_4 \text{ oppure } G \cong \mathcal{K}_4$$

Dimostrazione:

- Sia $a \neq 1 \in G$. Per Lagrange, sappiamo che $o(a) \mid |G| = 4 \iff o(a) \in \{1, 2, 4\}$
- Come visto nella sezione 6.4, sappiamo che G è ciclico se:

$$\exists a \in G \mid o(a) = 4 \implies G \cong \mathbb{Z}_4$$

- Ipotizziamo ora che non sia ciclico, dunque che $\exists a \in G \mid o(a) = 2$, implicando quindi che $G = \{1, a, b, c\}$, dove $o(a) = o(b) = o(c) = 2$. Verifichiamo che in tal caso $ab = c$:

- Supponiamo per assurdo che $ab = 1$

$$ab = 1 \implies b = a^{-1} = a$$

il che è impossibile

- Supponiamo per assurdo che $ab = a$

$$ab = a \implies a^{-1}ab = a^{-1}a \implies b = 1$$

il che è impossibile

- Supponiamo per assurdo che $ab = b$

$$ab = b \implies abb^{-1} = bb^{-1} \implies a = 1$$

il che è impossibile

- Siccome $ab \neq 1$, $ab \neq a$ e $ab \neq b$, allora l'unica possibilità affinché valga la chiusura del gruppo è $ab = c$
- Analogamente, dimostriamo che $ac = b$ e $bc = a$, concludendo quindi che:

$$G \cong \mathcal{K}_4$$

□

Theorem 48. Teorema di Cauchy

Sia G un gruppo finito. Dato un numero primo $p \in \mathbb{P}$, si verifica che:

$$p \mid |G| \implies \exists g \in G \mid o(g) = p$$

In particolare, se $|G| = q \in \mathbb{P}$, allora G è ciclico poiché

$$\exists g \in G \mid o(g) = q \implies |G| = o(g) \implies G = H(g)$$

Proposition 49

Se G è un gruppo finito dove $|G| = 6$, si verifica che:

$$G \cong \mathbb{Z}_6 \text{ oppure } G \cong \mathcal{S}_3$$

Dimostrazione:

- Come già visto, se $\exists g \in G \mid o(g) = 6$, allora $G \cong \mathbb{Z}_6$
- Ipotizziamo quindi che G non sia ciclico, dunque che $\nexists g \in G \mid o(g) = 6$. Per il teorema di Cauchy sappiamo che

$$- \exists \alpha \in G \mid o(\alpha) = 3 \implies o(\alpha^k) \mid o(\alpha) = 3, k \neq 0 \implies o(\alpha^3) = 3$$

$$- \exists \beta \in G \mid o(\beta) = 2 \implies \beta^{-1} = \beta$$

- Notiamo che:

$$\alpha^i \beta = \alpha^j \beta \iff \alpha^i = \alpha^j \iff 1 = \alpha^j \alpha^{-i} = \alpha^{j-i} \iff 0 = j - i \iff j = i$$

e che

$$\alpha^i = \alpha^j \beta \iff \alpha^{i-j} = \beta$$

- Tuttavia, l'ultima affermazione risulta essere assurda poiché:

$$o(\beta) = 2 \quad o(p^{i-j}) = \begin{cases} o(1) = 1 & \text{se } i = j \\ o(p^k) = 3 & \text{se } i \neq j \end{cases}$$

di conseguenza si ha che $\beta \neq \alpha^{i-j}$.

- Mostriamo inoltre che $\beta\alpha = \alpha^2\beta$:

- Supponiamo per assurdo che $\beta\alpha = 1$

$$\beta\alpha = 1 \implies \alpha = \beta^{-1} \implies \alpha = \beta$$

il che è impossibile

- Supponiamo per assurdo che $\beta\alpha = \alpha$

$$\beta\alpha = \alpha \implies \beta = 1$$

il che è impossibile

- Supponiamo per assurdo che $\beta\alpha = \alpha^2$

$$\beta\alpha = \alpha^2 \implies \beta = \alpha$$

il che è impossibile

- Supponiamo per assurdo che $\beta\alpha = \beta$

$$\beta\alpha = \beta \implies \alpha = 1$$

il che è impossibile

- Supponiamo per assurdo che $\beta\alpha = \alpha\beta$, implicando che $o(\beta\alpha) = o(\alpha\beta)$:

$$* (\alpha\beta)^1 = \alpha\beta$$

$$* (\alpha\beta)^2 = (\beta\alpha)(\beta\alpha) = \beta\beta\alpha\alpha = \beta^2\alpha^2 = \alpha^2$$

$$* (\alpha\beta)^3 = (\alpha\beta)(\alpha\beta)^2 = (\alpha\beta)\alpha^2 = \alpha^3\beta = \beta$$

$$* (\alpha\beta)^4 = (\alpha\beta)(\alpha\beta)^3 = (\alpha\beta)\beta = \alpha\beta^2 = \alpha$$

$$* (\alpha\beta)^5 = (\alpha\beta)(\alpha\beta)^4 = (\alpha\beta)\alpha = \alpha^2\beta$$

$$* (\alpha\beta)^6 = (\alpha\beta)(\alpha\beta)^5 = (\alpha\beta)\alpha^2\beta = \beta^2\alpha^3 = 1$$

dunque $o(\alpha\beta) = 6 \implies o(\alpha\beta) = |G| \implies G = H(\beta\alpha)$, ossia che il gruppo sia ciclico, contro l'ipotesi che invece esso non lo sia.

- Quindi l'unica possibilità è che $\beta\alpha = \alpha^2\beta$

- Concludiamo quindi che:

$$G = \{1, \alpha, \alpha^2, \beta, \alpha\beta, \alpha^2\beta\}$$

- A questo punto, possiamo stendere una **tavola di Cayley**, ossia una tavola moltiplicativa:

	1	α	α^2	β	$\alpha\beta$	$\alpha^2\beta$
1	1	α	α^2	β	$\alpha\beta$	$\alpha^2\beta$
α	α	α^2	1	$\alpha\beta$	$\alpha^2\beta$	β
α^2	α^2	1	α	$\alpha^2\beta$	β	$\alpha\beta$
β	β	$\alpha^2\beta$	$\alpha\beta$	1	α^2	α
$\alpha\beta$	$\alpha\beta$	β	$\alpha^2\beta$	α	1	α^2
$\alpha^2\beta$	$\alpha^2\beta$	$\alpha\beta$	β	α^2	α	1

- Ricordando le proprietà dei prodotti dei gruppi diedrali (sezione 6.5), si ottiene una mappatura univoca $\alpha^i \mapsto \rho^i$ e analogamente $\alpha^i\beta \mapsto \sigma_i$. Ciò implica quindi che:

$$G \cong \mathcal{D}_3$$

- Inoltre, abbiamo visto che $\mathcal{D}_3 \cong H_3 \leq \mathcal{S}_3$ dove

$$H_3 : \{\sigma_\alpha \in \mathcal{S}_3 \mid \sigma_\alpha = \alpha, \alpha \in \mathcal{D}_3\}$$

e dove $|\mathcal{D}_3| = 2 \cdot 3 = 6$ e $|\mathcal{S}_3| = 3! = 6$.

- Affinché l'isomorfismo esista si ha necessariamente che $|H| = |\mathcal{D}_3| = 6$, implicando quindi che

$$H_3 \leq \mathbb{S}_3, |H_3| = |\mathcal{S}_3| \implies G \cong \mathcal{D}_3 \cong H = \mathcal{S}_3$$

□

Capitolo 7

Polinomi

Definition 52. Anello polinomiale

Dato un anello commutativo A , definiamo l'**insieme dei polinomi** aventi come coefficienti elementi in A come:

$$A[x] : \{a_0 + a_1x + \dots + a_nx^n \mid a_0, \dots, a_n \in A, a_n \neq 0\}$$

Inoltre, $A[x]$ risulta essere un **anello commutativo**

Dimostrazione:

- Dati due polinomi $p(x), q(x) \in A[x]$, dunque definiti come

$$p(x) = \sum_{i=0}^n a_i x^i \quad q(x) = \sum_{i=0}^m b_i x^i$$

abbiamo che:

- Nell'anello la somma è definita come:

$$p(x), q(x) \in A[x] \implies p(x) + q(x) = \sum_{i=0}^{\max(n,m)} (a_i + b_i) x^i$$

- Nell'anello il prodotto è definita come:

$$p(x), q(x) \in A[x] \implies p(x) \cdot q(x) = \sum_{i=0}^n \left(\sum_{j=0}^m a_i b_j x^{i+j} \right)$$

- Gli assiomi di associatività e commutatività possono essere facilmente verificati tramite la definizione stessa della somma
- L'elemento neutro nella somma è il polinomio neutro $e(x) = 0$, mentre nel prodotto è il polinomio costante $d(x) = 1$
- L'elemento inverso nella somma è:

$$\forall p(x) \in A[x], \exists -p(x) \in A[x] \mid p(x) + (-p(x)) = 0$$

- Per via della definizione data di polinomio, non esiste un inverso moltiplicativo.

Si pensi ad esempio a $p(x) = x + 3$. Tale polinomio non ammette inverso moltiplicativo poiché $\frac{1}{x+3} \notin A[x]$.

Di conseguenza, $A[x]$ non può essere un campo.

□

Observation 43

Se K è un campo, allora $K[x]$ è un anello commutativo, poiché non ammette comunque l'esistenza dell'inverso nel prodotto

Definition 53. Grado di un polinomio

Dato $p(x) \in A[x]$ indichiamo il **grado del polinomio** come $\deg(p(x))$, dove:

- $p(x) = 0 \iff \deg(p(x)) = -\infty$ (polinomio nullo)
- $p(x) = a_0 + a_1x + \dots + a_nx^n \neq 0, a_n \neq 0 \implies \deg(p(x)) = n$

Definition 54. Coefficienti direttori

Dato $p(x) = a_0 + a_1x + \dots + a_nx^n \neq 0 \in A[x]$, definiamo a_n come **coefficiente direttore** del polinomio

Proposition 50

Ogni elemento $a \in A$ può essere visto come un **polinomio costante**, ossia di grado 0:

$$\forall a \in A, \exists a(x) \in A[x] \mid a(x) = a \iff \deg(a(x)) = 0$$

Dunque, si ha che $A \leq A[x]$ sottoanello

Observation 44

Siano $p(x), q(x) \in A[x]$. Si verifica che:

$$\deg(p(x)q(x)) = \deg(p(x)) + \deg(q(x))$$

Dimostrazione:

- Poiché il prodotto è definito come

$$p(x) \cdot q(x) = \sum_{i=0}^n \left(\sum_{j=0}^m a_i b_j x^{i+j} \right) = a_0 b_0 + a_0 b_1 x^1 + \dots + a_n b_m x^{n+m}$$

$$\text{allora } \deg(p(x)q(x)) = \deg(p(x)) + \deg(q(x)) = n + m$$

□

Proposition 51

Dato l'anello commutativo $K[x]$, si ha che:

$$K[x]^* = K^* = K - \{0\}$$

dunque gli unici elementi invertibili di $K[x]$ sono i **polinomi costanti**

Dimostrazione:

- Supponiamo per assurdo che $\exists a(x) \neq 0 \in K[x] \mid \deg(a(x)) \geq 1$ e che $\exists a(x)^{-1} \neq 0 \in K[x] \mid \deg(a(x)^{-1}) \geq 0$, da cui otteniamo che:

$$\deg(1) = \deg(a(x)a(x)^{-1}) = \deg(a(x)) + \deg(a(x)^{-1}) \geq 1$$

giungendo quindi ad una contraddizione, poiché $1 \in K \implies \deg(1) = 0$. Dunque, l'unica possibilità è:

$$\deg(a(x)) \geq 1 \implies a(x) \neq 0 \notin K[x]^*$$

da cui ricaviamo che

$$a(x) \neq 0 \in K[x]^* \implies \deg(a(x)) = 0$$

- Supponiamo invece che $\deg(a(x)) = 0$, implicando che

$$\exists a_0 \neq 0 \in K \mid a(x) = a_0 \implies \exists a_0^{-1} \in K \mid a_0 a_0^{-1} = 1 \implies$$

da cui concludiamo che:

$$\deg(a(x)) = 0 \implies a(x) \neq 0 \in K[x]^*$$

□

7.1 Divisione con resto di polinomi

Theorem 52. Divisione con resto di polinomi

Dati $a(x), b(x) \in K[x]$ con $b(x) \neq 0$ allora

$$\exists! q(x), r(x) \in K[x] \mid a(x) = b(x)q(x) + r(x)$$

dove $\deg(r(x)) < \deg(b(x))$

Dimostrazione unicità (esistenza omessa)

- Supponiamo che

$$b(x)q_1(x) + r_1(x) = a(x) = b(x)q_2(x) + r_2(x)$$

dove $\deg(r_1(x)), \deg(r_2(x)) < \deg(b(x))$, da cui otteniamo che:

$$\deg(r_1(x)), \deg(r_2(x)) < \deg(b(x)) \implies \deg(r_1(x) - r_2(x)) < \deg(b(x))$$

- Dunque si ha che:

$$\begin{aligned} b(x)q_1(x) + r_1(x) &= b(x)q_2(x) + r_2(x) \implies b(x)[q_1(x) - q_2(x)] = r_2(x) - r_1(x) \implies \\ \implies \deg(r_2(x) - r_1(x)) &= \deg(b(x)) + \deg(q_1(x) - q_2(x)) \end{aligned}$$

- Se $\deg(q_1(x) - q_2(x)) \geq 0$ avremmo $\deg(r_2(x) - r_1(x)) \geq \deg(b(x))$, contraddicendo l'ipotesi
- Di conseguenza, l'unica possibilità è:

$$q_1(x) - q_2(x) = 0 = r_1(x) - r_2(x)$$

e dunque che $q_1(x) = q_2(x)$ e $r_1(x) = r_2(x)$

□

Esempio:

- Calcolo della divisione con resto di $a(x) = 2x^4 + 3x^3 - 2x^2 + x - 4$ e $b(x) = x^2 - x + 1$

$$\begin{array}{r|rrrrr} +2x^4 & +3x^3 & -2x^2 & +x & -4 & \\ -2x^4 & +2x^3 & -2x^2 & & & \\ \hline & +5x^3 & -4x^2 & +x & -4 & \\ & -5x^3 & +5x^2 & -5x & & \\ \hline & & x^2 & -4x & -4 & \\ & & -x^2 & +x & -1 & \\ \hline & & & +3x & -5 & \end{array}$$

Quindi concludiamo che:

$$2x^4 + 3x^3 - 2x^2 + x - 4 = (x^2 - x + 1)(2x^2 + 5x + 1) + 3x - 5$$

7.1.1 Regola di Ruffini

Method 2. Regola di Ruffini

Dati $a(x), b(x) \in K[x]$ dove $b(x) = x - c, \exists c \in K$, è facile calcolare il quoziente $q(x) \in K[x]$ e il resto $r(x) = r_0 \in K$ della divisione di $a(x)$ per $b(x)$:

1. Sia $a(x) = a_0 + \dots + a_n x^n$ con $a_n \neq 0$
2. Poiché $\deg(a(x)) = \deg(b(x)) + \deg(q(x)) = 1 + \deg(q(x)) \implies \deg(q(x)) = \deg(a(x)) - 1$, allora

$$q(x) = q_0 + \dots + q_{n-1} x^{n-1}$$

dove q_0, \dots, q_{n-1} sono dati da:

- $q_{n-1} = a_n$
- $q_{n-1-k} = cq_{n-k} + a_{n-k}$
- $r_0 = cq_0 + a_0$

3. In formato grafico, riassumiamo tale concetto con:

$$\begin{array}{c|cccc|c} & a_n & a_{n-1} & \dots & a_1 & a_0 \\ c & & cq_{n-1} & \dots & cq_1 & cq_0 \\ \hline & q_{n-1} & q_{n-2} & \dots & q_0 & r_0 \end{array}$$

Esempio:

- Calcolare la divisione tra $a(x) = x^4 - 3x^3 + 2x - 5$ e $b(x) = x + 2$

$$\begin{array}{c|cccc|c} & 1 & -3 & 0 & 2 & -5 \\ -2 & & -2 & 10 & -20 & 36 \\ \hline & 1 & -5 & 10 & -18 & 31 \end{array}$$

Dunque si ha che:

$$x^4 - 3x^3 + 2x - 5 = (x + 2)(x^3 - 5x^2 + 10x - 18) + 31$$

Proposition 53. Teorema del fattore

Dato $p(x) \in K[x]$ e dato $c \in K$

$$p(c) = 0 \iff x - c \mid p(x)$$

in tal caso, c viene detta **radice (o zero) del polinomio**

Dimostrazione:

- $x - c \mid p(x) \implies p(c) = 0$

$$x - c \mid p(x) \implies p(x) = (x - c)q(x) \implies p(c) = (c - c)q(c) = 0$$

- $p(c) = 0 \implies x - c \mid p(x)$
 - Siano $q(x)$ e $r(x)$ il quoziente e il resto della divisione di $p(x)$ per $(x - c)$

$$p(x) = (x - c)q(x) + r(x)$$

- Per ipotesi, si ha che:

$$0 = p(c) = (c - c)q(c) + r(x) \implies r(x) = 0$$

dunque, la divisione non ha resto, implicando che:

$$(x - c) \mid p(x)$$

□

Corollary 23

Dato $p(x) \in K[x] \mid \deg(a(x)) = n$, allora $a(x)$ ha al massimo n radici

Inoltre, se $p(x) \in \mathbb{C}[x]$, allora, per il teorema fondamentale dell'algebra, esistono esattamente n radici

Dimostrazione:

- Sia $\deg(p(x)) = n$ e siano per assurdo c_1, \dots, c_m dove $m > n$ e $c_i \neq c_j \iff i \neq j$ tali che

$$p(c_i) = 0, \forall 1 \leq i \leq m$$

- Poiché un polinomio può essere scritto come il prodotto di tutte le sue radici, si verifica che:

$$\begin{cases} x - c_1 \mid p(x) \\ \vdots \\ x - c_m \mid p(x) \end{cases} \implies \underbrace{(x - c_1) \cdot \dots \cdot (x - c_m)}_{q(x)} \mid p(x)$$

- Poiché $\deg(q(x)) = m$, tale divisione risulta essere impossibile, poiché un polinomio non può dividere un polinomio di grado minore

7.2 Proprietà dell'anello polinomiale

Proposition 54

L'anello commutativo $K[x]$ è un **dominio di integrità** poiché vale la **legge di annullamento del prodotto**

Corollary 24

Dato il dominio di integrità $K[x]$ e dati $p(x), q(x) \in K[x]$, si ha che:

$$I(p(x)) = I(q(x)) \iff p(x) = c \cdot q(x), \exists c \in K[x]^*$$

(*dimostrazione nella sezione 4.3*)

Theorem 55

L'anello commutativo $K[x]$ è un **dominio ad ideali principali**, dunque

$$\exists! p(x) \in I \mid I = I(p(x))$$

Dimostrazione esistenza:

- $I \subseteq I(p(x))$
 - Sia $p(x) \neq 0 \in I$ del più piccolo grado possibile.
 - Dato $a(x) \in I \mid a(x) = p(x)q(x) + r(x)$ si ha che $\deg(r(x)) < \deg(p(x))$, da cui ricaviamo che:

$$a(x) = p(x)q(x) + r(x) \in I \implies r(x) = a(x) - p(x)q(x) \in I$$

- Tuttavia, poiché $p(x)$ è il polinomio non nullo all'interno dell'ideale del più piccolo grado possibile e poiché $\deg(r(x)) < \deg(p(x))$, ne segue necessariamente che $r(x) = 0$.
- Dunque, si ha che:

$$a(x) = p(x)q(x) + r(x) \in I \implies a(x) = p(x)q(x) \implies a(x) \in I(p(x))$$

- $I(p(x)) \subseteq I$
 - Dato $p(x) \neq 0 \in I$ del più piccolo grado possibile, si ha che:

$$a(x) \in I(p(x)) \implies a(x) = p(x)b(x), \exists b(x) \in K[x] \implies a(x) \in I$$

poiché $p(x) \in I$

Dimostrazione unicità:

- Se $I = \{0\}$, allora $I = I(0)$
- Sia invece $p(x) \neq 0 \in I$ del più piccolo grado possibile tale che $I = I(p(x))$, implicando che

$$\forall q(x) \in I \mid \deg(q(x)) < \deg(p(x)) \implies q(x) = 0$$

dunque non può esistere un polinomio in I con grado minore di $p(x)$

□

Definition 55. Massimo comun divisore di polinomi

Dato il dominio ad ideali principali $K[x]$ e degli elementi $a_1(x), \dots, a_n(x) \in K[x]$, si ha che:

$$\exists! p(x) \in K[x] \mid I(a_1(x), \dots, a_n(x)) = I(p(x))$$

dove $d(x) := \text{MCD}(a_1(x), \dots, a_n(x))$

In particolare, individuiamo l'analogo dell'**identità di Bezout**:

$$\exists p_1(x), \dots, p_n(x) \in K[x] \mid a_1(x)p_1(x) + \dots + a_n(x)p_n(x) = d(x)$$

Definition 56. Minimo comune multiplo di polinomi

Dato il dominio ad ideali principali \mathbb{Z} e degli elementi $a_1(x), \dots, a_n(x) \in K[x]$, si ha che:

$$\exists! p(x) \in K[x] \mid I(a_1(x)) \cap \dots \cap I(a_n(x)) = I(p(x))$$

dove $m(x) := \text{mcm}(a_1(x), \dots, a_n(x))$

Observation 45

Poiché $K[x]$ è un dominio dominio di integrità, sappiamo che

$$I(p(x)) = I(q(x)) \iff p(x) = c \cdot q(x), \exists c \in K[x]^*$$

Dunque, dati $a_1(x), \dots, a_n(x) \in K[x]$, si ha che $d(x) := \text{MCD}(a_1(x), \dots, a_n(x))$ e $m(x) := \text{mcm}(a_1(x), \dots, a_n(x))$ possano essere ben definiti solo a meno di una costante moltiplicativa non nulla.

Affinché valga l'unicità, quindi, basta imporre che i polinomi $d(x)$ e $m(x)$ abbiano **coefficiente direttore** $a_n = 1$

Definition 57. Polinomio monico

Dato $a(x) = a_0 + \dots + a_n x^n \in K[x]$, definiamo $a(x)$ come **polinomio monico** se e solo se $a_n = 1$

Method 3

Dati $a(x), b(x) \in K[x]$, possiamo calcolare $d(x) := \text{MCD}(a(x), b(x))$ tramite l' **algoritmo di Euclide** e $m(x) := \text{mcm}(a(x), b(x))$ tramite il **teorema fondamentale dell'aritmetica**:

$$m(x) = \frac{a(x)b(x)}{d(x)}$$

Observation 46

Dati $a_1(x), \dots, a_n(x) \in K[x]$ data $c \in K$, si ha che:

$$a_1(c) = \dots = a_n(c) = 0 \iff d(c) = 0$$

dove $d(x) := \text{MCD}(a_1(x), \dots, a_n(x)) \in K[x]$.

In altre parole, le uniche radici in comune tra due polinomi sono le radici del loro MCD

Dimostrazione:

- Sia $c \in K$ tale che:

$$a_i(c) = 0, \forall i \in [1, n] \iff (x - c) \mid a_i(x), \forall i \in [1, n]$$

- Poiché $d(x) := \text{MCD}(a_1(x), \dots, a_n(x))$, per definizione stessa si ha che:

$$(x - c) \mid a_i(x), \forall i \in [1, n] \implies (x - c) \mid d(x) \iff d(c) = 0$$

- Viceversa, sempre per definizione stessa di $d(x)$ si ha che:

$$d(c) = 0 \implies (x - c) \mid d(x), d(x) \mid a_i(x), \forall i \in [1, n] \implies (x - c) \mid a_i(x), \forall i \in [1, n]$$

□

Proposition 56

Dato $p(x) \in K[x]$, si ha che:

$$p(x) \text{ elemento irriducibile} \iff p(x) \text{ elemento primo}$$

Dimostrazione:

- Sappiamo già che in un dominio di integrità si ha:

$$p(x) \text{ primo} \implies p(x) \text{ irriducibile}$$

(*dimostrazione nella sezione 4.4*)

- Dati $a(x), b(x) \in K[x]$, supponiamo che $p(x) \mid a(x)b(x)$:

$$p(x) \mid a(x)b(x) \mid a(x)b(x) = p(x)k(x), \exists k(x) \in K[x]$$

- Se $p(x) \nmid a(x)$, si ha che $d(x) := MCD(p(x), a(x)) = 1$. Dunque, tramite l'identità di Bezout otteniamo che:

$$\begin{aligned} & \exists f(x), g(x) \in K[x] \mid d(x) = p(x)f(x) + a(x)g(x) \implies \\ & \implies 1 = p(x)f(x) + a(x)g(x) \implies b(x) = p(x)b(x)f(x) + a(x)b(x)g(x) \implies \\ & \implies b(x) = p(x)b(x)f(x) + [a(x)b(x)]g(x) \implies b(x) = p(x)b(x)f(x) + p(x)k(x)g(x) \implies \\ & \implies b(x) = p(x)[q(x)f(x) + g(x)b(x)] \implies p(x) \mid b(x) \end{aligned}$$

- Analogamente, se $p(x) \nmid b(x)$ si ha che $d(x) := MCD(p(x), b(x)) = 1$. Dunque, seguendo gli stessi passaggi otteniamo che $p(x) \mid a(x)$
- Concludiamo quindi che se $p(x)$ è irriducibile, allora:

$$p(x) \mid a(x)b(x) \implies p(x) \mid a(x) \vee p(x) \mid b(x)$$

□

Proposition 57

Dato $p(x) \in \mathbb{C}[x]$, si ha che:

$$p(x) \in \mathbb{C}[x] \text{ irriducibile} \iff \deg(p(x)) = 1$$

Dimostrazione:

- Dato $p(x) \neq 0 \in \mathbb{C}[x]$, se $\deg(p(x)) > 1$, per il teorema fondamentale dell'algebra si ha che:

$$\begin{aligned} & \exists z \in \mathbb{C} \mid p(z) = 0 \iff x - z \mid p(x) \iff \\ & \iff p(x) = (x - z)q(x), \exists q(x) \in \mathbb{C}[x] \implies \\ & \implies \deg(q(x)) = \deg(p(x)) - 1 > 0 \implies q(x) \notin \mathbb{C}^* = \mathbb{C}[x]^* \end{aligned}$$

dunque $p(x)$ non può essere irriducibile poiché $\deg((x - z)) = 1 \implies (x - z) \notin \mathbb{C}[x]^*$ e $q(x) \notin \mathbb{C}[x]^*$

- Se invece $\deg(p(x)) = 1$ allora

$$p(x) = a(x)b(x) \iff \begin{cases} \deg(a(x)) = 0, \deg(b(x)) = 1 \implies a(x) \in \mathbb{C}[x]^* \\ \deg(a(x)) = 1, \deg(b(x)) = 0 \implies b(x) \in \mathbb{C}[x]^* \end{cases}$$

dunque $p(x)$ è irriducibile

□

Proposition 58

Dato $p(x) \in \mathbb{R}[x]$, si ha che:

$$p(x) \in \mathbb{R}[x] \text{ irriducibile} \iff \deg(p(x)) = 1 \text{ oppure } \deg(p(x)) = 2, \Delta < 0$$

dove $\deg(p(x)) = 2 \implies ax^2 + bx + c, \Delta := b^2 - 4ac$

Dimostrazione:

- Se $\deg(p(x)) = 1$, la dimostrazione è analoga al caso in cui $p(x) \in \mathbb{C}[x]$
- Supponiamo quindi per assurdo che $\deg(p(x)) = 2, \Delta < 0$ e che $p(x)$ non sia irriducibile, implicando che:

$$\exists a(x)b(x) \in \mathbb{R}[x] - \mathbb{R}[x]^* \mid p(x) = a(x)b(x) \wedge \deg(p(x)) = 2$$

$$\implies \deg(a(x)) = \deg(b(x)) = 1 \implies$$

$$\implies \left\{ \begin{array}{l} \exists c, d \in \mathbb{R} \mid a(x) = cx + d \implies a(-c^{-1}d) = 0 \iff (x + c^{-1}d) \mid a(x) \\ \exists f, g \in \mathbb{R} \mid b(x) = fx + g \implies b(-f^{-1}g) = 0 \iff (x + f^{-1}g) \mid b(x) \end{array} \right. \implies$$

$$\implies \left\{ \begin{array}{l} (x + c^{-1}d) \mid a(x), a(x) \mid p(x) \implies (x + c^{-1}d) \mid p(x) \iff p(-c^{-1}d) = 0 \\ (x + f^{-1}g) \mid b(x), b(x) \mid p(x) \implies (x + f^{-1}g) \mid p(x) \iff p(-f^{-1}g) = 0 \end{array} \right.$$

dunque $x_1 := -c^{-1}d \in \mathbb{R}$ e $x_2 := -f^{-1}g \in \mathbb{R}$ sarebbero le radici di $p(x)$, contraddicendo l'ipotesi per cui $\Delta < 0 \implies x_1, x_2 \in \mathbb{C} - \mathbb{R}$.

Dunque, l'unica possibilità è:

$$\deg(p(x)) = 2, \Delta < 0 \implies p(x) \in \mathbb{R} \text{ irriducibile}$$

- Sia quindi $p(x) = a_0 + \dots + a_n x^n \in \mathbb{R}[x]$ irriducibile con $\deg(p(x)) > 1$. Per il teorema fondamentale dell'algebra, $\exists z \in \mathbb{C} \mid p(z) = 0$. Se tale z fosse anche reale (ossia $z \in \mathbb{R}$), allora si avrebbe che

$$(x - z) \mid p(x) \implies p(x) = (x - z)q(x) \mid \exists q(x) \in \mathbb{R}[x]$$

- Poiché $a_1, \dots, a_n \in \mathbb{R}$, si ha che:

$$\forall j \in [1, n], \exists c_j \in \mathbb{R} \mid a_j := c_j + i \cdot 0 = c - j \cdot 0 =: \overline{a_j} \implies a_j = \overline{a_j}, \forall j \in [1, n]$$

- Inoltre, per le proprietà dei coniugati (sezione 2), si ha che:

$$p(\bar{z}) = a_0 + \dots + a_n \bar{z}^n = a_0 + \dots + \overline{a_n} \bar{z}^n = \overline{a_0 + \dots + a_n z^n} = \overline{a_0 + \dots + a_n z^n} = \overline{p(z)}$$

- Siccome per ipotesi $p(z) = 0$, ne segue che $\overline{p(z)} = \bar{0} = 0$. Di conseguenza, si ha che anche \bar{z} è una radice di $p(x)$, da cui deriva che:

$$x - z \mid p(x) \wedge x - \bar{z} \mid p(x) \implies (x - z)(x - \bar{z}) \mid p(x) \implies x^2 - (z + \bar{z})x + z \cdot \bar{z} \mid p(x)$$

- Siccome $z + \bar{z} = (c + id)(c - id) = 2c \in \mathbb{R}$ e $z \cdot \bar{z} = (c + id)(c - id) = c^2 + d^2 \in \mathbb{R}$, allora ne segue che $x^2 - (z + \bar{z})x + z \cdot \bar{z} = x^2 - 2cx + c^2 + d^2 \in \mathbb{R}$

- Poiché $p(x)$ è irriducibile, in definitiva abbiamo che:

$$p(x) = k(x^2 - 2cx + c^2 + d^2), \exists k \in \mathbb{R}^*$$

- Possiamo concludere, quindi, che $p(x)$ dove $\deg(p(x)) > 1$ è irriducibile se e solo se:

$$\Delta := (-2kc)^2 - 4k^2(c^2 + d^2) = 4k^2c^2 - 4k^2(c^2 + d^2) = -4kd^2 < 0$$

Theorem 59. Fattorizzazione in polinomi irriducibili e monici

Dato $p(x) \neq 0 \in K[x]$, si ha che:

$$\exists! q_1(x), \dots, q_k(x) \in K[x], \exists c \in K^* \mid p(x) = c \cdot q_1(x) \cdot \dots \cdot q_k(x)$$

dove $q_1(x), \dots, q_k(x)$ sono **polinomi irriducibili e monici**

Dimostrazione esistenza:

- Se $\deg(p(x)) = 1$, allora $p(x)$ è irriducibile (e di conseguenza anche primo).

Difatti, se esistesse una fattorizzazione di $p(x)$ (dunque non fosse irriducibile) avremmo che:

$$\deg(p(x)) = \deg(q_1(x)) + \dots + \deg(q_k(x))$$

dove $\deg(q_i(x)) > 0$ (poiché altrimenti sarebbe una costante), implicando quindi che $\deg(p(x)) > 1$ contro l'ipotesi

- Sia quindi $\deg(p(x)) > 1$, implicando che $p(x)$ non sia irriducibile, dunque $p(x) = a(x)b(x)$
- Supponiamo per ipotesi induttiva che $a(x)$ e $b(x)$ siano fattorizzati in polinomi irriducibili e monici

$$a(x) = c \cdot q_1(x) \cdot \dots \cdot q_k(x)$$

$$b(x) = c' \cdot q'_1(x) \cdot \dots \cdot q'_j(x)$$

si ha quindi che:

$$p(x) = c \cdot c' \cdot q_1(x) \cdot q'_1(x) \cdot \dots \cdot q_k(x) \cdot q'_j(x)$$

Dimostrazione unicità:

- Se $\deg(p(x)) = 0$ allora $p(x) = c$
- Se $\deg(p(x)) > 0$, supponiamo due fattorizzazioni possibili per $p(x)$

$$c \cdot q_1(x) \cdot \dots \cdot q_k(x) = p(x) = c' \cdot q'_1(x) \cdot \dots \cdot q'_j(x)$$

- Notiamo che se $p(x) = a_0 + a_1x + \dots + a_nx^n$, allora $c = a_n = c'$. Supponendo che $q_1(x), \dots, q_k(x), q'_1(x), \dots, q'_j(x) \in K[x]$ siano monici, allora anche il loro prodotto è monico

$$p(x) = a_0 + \dots + a_nx^n = c) = c \cdot q_1(x) \cdot \dots \cdot q_k(x) = c' \cdot q'_1(x) \cdot \dots \cdot q'_j(x) \implies$$

$$\implies q_1(x) \mid p(x) = c' \cdot q'_1(x) \cdot \dots \cdot q'_j(x) \implies$$

$$q_1(x) \mid q'_1(x) \vee \dots \vee q_1(x) \mid q'_j(x)$$

- Supponiamo che $q_1(x) \mid q'_1(x) \implies q'_1(x) = k \cdot q_1(x), \exists k \in K^*$, implicando che:

$$c \cdot q_1(x) \cdot \dots \cdot q_k(x) = p(x) = c' \cdot q'_1(x) \cdot \dots \cdot q'_j(x) \implies$$

$$\implies c \cdot q_1(x) \cdot \dots \cdot q_k(x) = p(x) = c' \cdot k \cdot q_1(x) \cdot \dots \cdot q'_j(x) \implies$$

$$\implies c \cdot q_2(x) \cdot \dots \cdot q_k(x) = \frac{p(x)}{q_1(x)} = c' \cdot k \cdot q'_2(x) \cdot \dots \cdot q'_j(x)$$

- Poiché $\deg(\frac{p(x)}{q(x)}) < \deg(p(x))$ possiamo concludere che $k = k$ e, a meno di riordinare i fattori, possiamo assumere che $q_2(x) = q'_2(x), \dots, q_k(x) = q'_k(x)$

Theorem 60

Sia $p(x) \in \mathbb{Z}[x]$ dove $p(x) = a_0 + \dots + a_n x^n$ con $a_0, a_n \neq 0$. Se $\frac{a}{b} \in \mathbb{Q}$ è radice di $p(x)$ e $MCD(a, b) = 1$, allora

$$p\left(\frac{a}{b}\right) = 0 \implies a \mid a_0 \wedge b \mid a_n$$

Dimostrazione:

- Sia $p(x) = a_0 + \dots + a_n x^n \in \mathbb{Z}[x]$. Supponendo che $\frac{a}{b} \in \mathbb{Q} \mid MCD(a, b) = 1$ sia radice di $p(x)$, allora

$$\begin{aligned} 0 &= p\left(\frac{a}{b}\right) = a_0 + a_1 \cdot \left(\frac{a}{b}\right) + \dots + a_n \cdot \left(\frac{a}{b}\right)^n \implies \\ \implies b^n \cdot 0 &= b^n \left(a_0 + a_1 \cdot \left(\frac{a}{b}\right) + \dots + a_n \cdot \left(\frac{a}{b}\right)^n \right) \implies \\ \implies 0 &= a_0 b^n + \dots + a_{n-1} \cdot a^{n-1} \cdot b + a_n a^n \implies \\ \implies a_n a^n &= -a_0 b^n - \dots - a_{n-1} \cdot a^{n-1} \cdot b \implies \\ \implies a_n a^n \cdot \frac{1}{b} &= -a_0 b^{n-1} - \dots - a_{n-1} \cdot a^{n-1} \implies b \mid a_n a^n \end{aligned}$$

- Poiché $MCD(a, b) = 1 \implies MCD(a^n, b) = 1$, allora

$$b \mid a_n a^n \implies b \mid a_n$$

- Seguendo gli stessi passaggi, arriviamo a dimostrare che $MCD(a, b) = 1 \implies MCD(a, b^n) = 1$ implica che

$$a \mid a_0 b^n \implies a \mid a_0$$

Esempi:

- Dato $p(x) = x^3 - 19x - 30$, se $\frac{a}{b} \in \mathbb{Q}$ fosse soluzione, allora

$$p\left(\frac{a}{b}\right) \implies a \mid a_0 = 30 \wedge b \mid a_n = 1$$

quindi le uniche soluzioni possibili di $p(x)$ possono essere:

$$x = \pm 1, \pm 2, \pm 3, \pm 5, \pm 6, \pm 10, \pm 15, \pm 30$$

- Dato $p(x) = 6x^3 - 11x^2 + 6x - 1$, se $\frac{a}{b} \in \mathbb{Q}$ fosse soluzione, allora

$$p\left(\frac{a}{b}\right) \implies a \mid a_0 = -1 \wedge b \mid a_n = 6$$

quindi le uniche soluzioni possibili di $p(x)$ possono essere:

$$x = \pm 1, \pm \frac{1}{2}, \pm \frac{1}{3}, \pm \frac{1}{6}$$

7.3 Polinomi in \mathbb{Z}_p

Poiché anche \mathbb{Z}_p è un campo, è possibile trattare anche polinomi a coefficienti in \mathbb{Z}_p .

Ad esempio, ricordando che in \mathbb{Z}_p si ha $([a] + [b])^p = [a]^p + [b]^p$, allora

$$\begin{aligned} (1+x)^p &\equiv 1^p + x^p \equiv 1 + x^p \pmod{n} \implies \\ \implies (1+x)^{pn} &\equiv (1+x^p)^n \pmod{n} \implies \sum_{i=0}^{np} \binom{np}{i} x^i \equiv \sum_{i=0}^n \binom{n}{j} x^{p(n-j)} \pmod{n} \end{aligned}$$

Corollary 25

Dato $p \in \mathbb{P}$ si ha che:

$$\begin{aligned} \binom{np}{i} &\equiv 0 \pmod{p} \iff p \nmid i \\ \binom{np}{pj} &\equiv \binom{n}{j} \pmod{p} \end{aligned}$$

Lemma 61

Dato $p \in \mathbb{P}$, si ha che:

$$\prod_{0 < a < p} (x - a) \equiv x^{p-1} - 1 \pmod{p}$$

Dimostrazione:

- Per il piccolo teorema di Fermat, dato $0 < a < p$ dove $p \in \mathbb{P}$ si ha che:

$$a^{p-1} \equiv 1 \pmod{p} \implies a^{p-1} - 1 \equiv 0 \pmod{p}$$

dunque $[a] \in \mathbb{Z}_p$ è una radice di $q(x) = x^{p-1} - [1] \in \mathbb{Z}_p[x]$

- Siccome $[a]$ è soluzione, allora per il teorema dei fattori si ha che:

$$\begin{aligned} x - [a] \mid x^{p-1} - [1], \forall 0 < a < p &\implies \prod_{0 < a < p} (x - [a]) \mid x^{p-1} - [1] \implies \\ \implies x^{p-1} - [1] &= k \cdot \prod_{0 < a < p} (x - [a]), \exists k \in \mathbb{Z} \end{aligned}$$

- Poiché il coefficiente direttore di $q(x)$ è 1, allora necessariamente si ha che $k = 1$, concludendo che:

$$\prod_{0 < a < p} (x - a) \equiv x^{p-1} - 1 \pmod{p}$$

Observation 47

Dato $p \in \mathbb{P}$, si ha che:

$$\prod_{0 < a < p} (x - a) = \sum_{k=1}^p (-1)^{p-k-1} \begin{bmatrix} p \\ k \end{bmatrix} x^{k-1}$$

dove $\begin{bmatrix} p \\ k \end{bmatrix}$ è un **numero di Stirling di prima specie senza segno**, ossia il numero di permutazioni in \mathcal{S}_p aventi k cicli

Esempio:

- Dato

$$S_3 : \{(1)(2)(3), (12)(3), (13)(2), (23)(1), (123), (132)\}$$

si ha che:

$$\begin{bmatrix} 3 \\ 1 \end{bmatrix} = 2, \begin{bmatrix} 3 \\ 2 \end{bmatrix} = 3, \begin{bmatrix} 3 \\ 3 \end{bmatrix} = 1$$

Lemma 62

Se $d \mid p - 1$, l'equazione $x^d \equiv 1 \pmod{p}$ ammette d soluzioni distinte in \mathbb{Z}_p

Dimostrazione:

- Supponiamo che $d \mid p - 1 \implies p - 1 = dk, \exists k \in \mathbb{Z}$
- Per dimostrazione precedente, sappiamo che

$$\prod_{0 < a < p} (x - a) \equiv x^{p-1} - 1 = x^{nd} - [1] = (x^d - [1])^n = (x^d - [1]) \underbrace{(x^d - [1])^{n-1}}_{q(x)} \pmod{p}$$

- Sempre per dimostrazione precedente, si ha che:

$$x - [a] \mid x^d - [1] \iff [a]^d = [1], \forall 0 < a < p$$

oppure che

$$x - [a] \mid q(x)$$

- Per motivi di grado, riapplicando tale procedimento su $q(x)$ e sui suoi fattori, otteniamo esattamente d radici di $x^d - [1]$

Lemma 63

Se $d \mid p - 1$, allora $\exists [a] \in \mathbb{Z}_p^* \mid o([a]) = d$

Dimostrazione:

- Se $d = 1$, allora $\exists 1 \in \mathbb{Z}_p^* \mid o([1]) = 1$

- Se $d = q^k$ dove $q \in \mathbb{P}$, allora per il lemma precedente si ha che $x^{q^k} - [1] = [0]$ ha q^k soluzioni.
- Siccome $x^{q^k-1} - [1] = [0]$ ha $q^k - 1$ soluzioni, allora $\exists [a] \in \mathbb{Z}_p^*$ che è soluzione della prima ma non della seconda, implicando che:

$$o([a]) \mid q^k \wedge o([a]) \nmid q^{k-1} \implies o([a]) = q^k$$

- Supponiamo per induzione di aver verificato tale condizione per tutti gli n divisori più piccoli di d .

Sia quindi $d = nq^k$ dove $q \in \mathbb{P} \mid MCD(n, q^k) = 1$. Per induzione, si ha che:

$$\exists [b], [c] \in \mathbb{Z}_p \mid o([b]) = n, o([c]) = q^k$$

- Come visto nella sezione 4.9, allora

$$MCD(o([b]), o([c])) = 1 \implies \exists a \in \mathbb{Z}_p \mid [a] = [bc] \implies o([a]) = nq^k = d$$

Corollary 26

Dato il gruppo (\mathbb{Z}_p, \cdot) dove $p \in \mathbb{P}$, tale gruppo è sempre ciclico, poiché:

$$p-1 \mid p-1 \implies \exists [a] \in \mathbb{Z}_p^* \mid o([a]) = p-1 = |\mathbb{Z}_p^*| \iff \mathbb{Z}_p^* = H([a])$$

Capitolo 8

Spazi vettoriali

Definition 58. Spazio vettoriale

Dato un campo K , i cui elementi vengono detti **scalari**, definiamo uno **spazio vettoriale** V , i cui elementi vengono detti **vettori**, sul campo K .

$(V, +)$ è un gruppo abeliano munito di un'operazione aggiuntiva detta **prodotto con scalare**

$$\cdot : K \times V \rightarrow V : (\lambda, v) \mapsto w$$

la quale rispetta le seguenti proprietà:

- $\forall s, t \in K, v \in V \implies s(t \cdot v) = stv = (s \cdot t)v$ (Associatività scalare)
- $1 \in K, v \in V \implies 1 \cdot v = v$ (Elemento neutro)
- $\forall s, t \in K, v \in V \implies (s + t)v = sv + tv$ (Distributività vettoriale)
- $\forall s \in K, v, w \in V \implies s(v + w) = sv + sw$ (Distributività scalare)

Esempio fondamentale:

- Lo spazio vettoriale $V = K^n = \underbrace{K \times K \times \dots \times K}_{n \text{ volte}}$ corrisponde a:

$$V = K^n = \{(x_1, \dots, x_n) \mid x_1, \dots, x_n \in K\}$$

- Presi dunque due vettori $v, w \in V = K^n$, si ha che

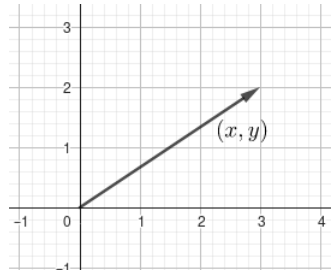
$$\begin{cases} v := (t_1, \dots, t_n) \in V = K^n \\ w := (s_1, \dots, s_n) \in V = K^n \end{cases} \implies v + w := (t_1 + s_1, \dots, t_n + s_n) \in V = K^n$$

- Preso invece uno scalare $\lambda \in K$, si ha che:

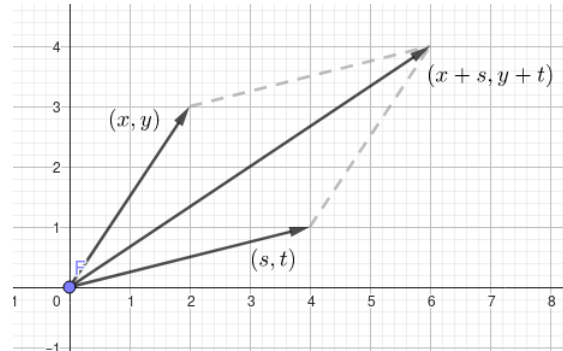
$$\lambda \cdot v = (\lambda t_1, \dots, \lambda t_n) \in V = K^n$$

Volendo dare un'interpretazione geometrica al tutto, prendiamo come esempio lo spazio vettoriale \mathbb{R}^2 .

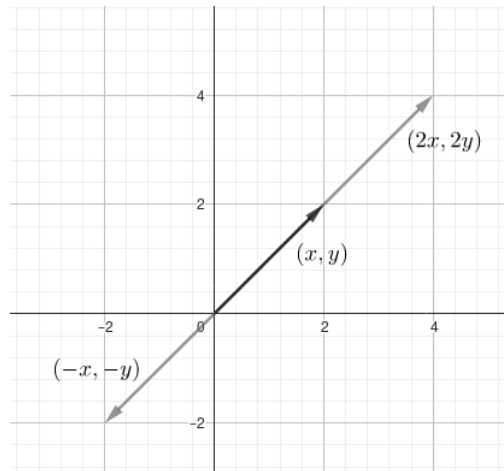
Dato $v := (x, y) \in \mathbb{R}^2$, possiamo rappresentare tale vettore come:



Dato anche $w := (s, t) \in \mathbb{R}^2$, la somma vettoriale $v + w$ corrisponde al *metodo del parallelogramma*:



Dato $\lambda \in \mathbb{R}$, si ha che il vettore $\lambda \cdot v$ ha la stessa direzione del vettore v , ma con lunghezza aumentata o diminuita e verso uguale o invertito



Observation 48

Dato $0_v \in V$, ossia l'elemento neutro di V (detto vettore nullo), e $0 \in K$, ossia l'elemento neutro di K , si ha che:

- $\forall \lambda \in K \implies \lambda \cdot 0_v = 0_v$
- $\forall w \in V \implies 0 \cdot w = 0_v$

8.1 Span e Base di uno spazio

Definition 59. Sottospazio vettoriale

Dato lo spazio vettoriale V definito su K , definiamo $W \subseteq V$ come sottospazio vettoriale di V in K se:

- $(W, +) \subseteq (V, +)$ è un sottogruppo
- $w \in W, \lambda \in K \implies \lambda w \in W$

Esempi:

- $\mathbb{Z}^n \subseteq \mathbb{R}^n$ non è sottospazio vettoriale poiché non verifica la seconda condizione
- $\mathbb{R}_{>0}^n \subseteq \mathbb{R}^n$ non è sottospazio vettoriale poiché non verifica nessuna delle due condizioni

Definition 60. Span

Dato uno spazio vettoriale V su K e dei vettori $v_1, \dots, v_n \in V$, definiamo **Span** (o sottospazio generato da v_1, \dots, v_n) l'insieme di tutte le **combinazioni lineari** di tali vettori:

$$\text{Span}(v_1, \dots, v_n) : \{\lambda_1 v_1 + \dots + \lambda_n v_n \mid \lambda_1, \dots, \lambda_n \in K\}$$

Verifica condizioni per il sottospazio:

- $0_V = 0 \cdot v_1 + \dots + 0 \cdot v_n \in \text{Span}(v_1, \dots, v_n)$
- $v, w \in \text{Span}(v_1, \dots, v_n) \implies v + w = \lambda_1 v_1 + \dots + \lambda_n v_n + \mu_1 v_1 + \dots + \mu_n v_n = (\lambda_1 + \mu_1)v_1 + \dots + (\lambda_n + \mu_n)v_n \in \text{Span}(v_1, \dots, v_n)$
- $v \in \text{Span}(v_1, \dots, v_n) \implies -v = (-\lambda_1)v_1 + \dots + (-\lambda_n)v_n \in \text{Span}(v_1, \dots, v_n)$
- $v \in \text{Span}(v_1, \dots, v_n), c \in K \implies cv = (c\lambda_1)v_1 + \dots + (c\lambda_n)v_n \in \text{Span}(v_1, \dots, v_n)$

Definition 61. Insieme di generatori

Dato uno spazio vettoriale V su K e dei vettori $v_1, \dots, v_n \in V$, definiamo tali vettori come **insieme di generatori di V** se $V = \text{Span}(v_1, \dots, v_n)$

Definition 62. Indipendenza lineare

Dato uno spazio vettoriale V su K e dei vettori $v_1, \dots, v_n \neq 0_V \in V$, definiamo tali vettori come **linearmente indipendenti** se

$$\lambda_1 v_1 + \dots + \lambda_n v_n = 0_V \iff \lambda_1 = \dots = \lambda_n = 0$$

In caso contrario, vengono detti linearmente dipendenti

Definition 63. Base

Dato uno spazio vettoriale V su K e dei vettori $v_1, \dots, v_n \neq 0_V \in V$, definiamo tali vettori come una **base** se sono un insieme di generatori e linearmente indipendenti

Esempio:

- Dato lo spazio vettoriale $V = K^n$, consideriamo i seguenti vettori $e_1, \dots, e_n \in V$:
 - $e_1 = (1, 0, 0, \dots, 0, 0)$
 - $e_2 = (0, 1, 0, \dots, 0, 0)$
 - $e_3 = (0, 0, 1, \dots, 0, 0)$
 - \vdots
 - $e_n = (0, 0, 0, \dots, 0, 1)$
- Tali vettori vengono detto **base canonica di V** , difatti:
 - e_1, \dots, e_n sono generatori di V

$$v = (t_1, t_2, \dots, t_n) \in V \iff v = (t_1, 0, \dots, 0) + (0, t_2, \dots, 0) + \dots + (0, 0, \dots, t_n) \iff$$

$$\iff v = t_1 e_1 + t_2 e_2 + \dots + t_n e_n \in \text{Span}(e_1, e_2, \dots, e_n)$$
 - e_1, \dots, e_n sono linearmente indipendenti:

$$\lambda_1 e_1 + \dots + \lambda_n e_n = (0, \dots, 0) \iff (\lambda_1, 0, \dots, 0) + \dots + (0, 0, \dots, \lambda_n) = (0, \dots, 0) \iff$$

$$(\lambda_1, \lambda_2, \dots, \lambda_n) = (0, \dots, 0) \iff \lambda_1 = \dots = \lambda_n = 0$$

Observation 49

Dato uno spazio vettoriale V su K , i vettori $v_1, \dots, v_n \neq 0_V \in V$ sono linearmente indipendenti se e solo se v_1, \dots, v_{n-1} sono linearmente indipendenti e $v_n \notin \text{Span}(v_1, \dots, v_{n-1})$

Dimostrazione (solo in un verso):

- Supponiamo che $v_1, \dots, v_n \neq 0_V \in V$ siano linearmente indipendenti, dunque che

$$\lambda_1 v_1 + \dots + \lambda_n v_n = 0_V \iff \lambda_1 = \dots = \lambda_n = 0$$
- Se si avesse $\lambda_n \neq 0$, allora

$$\lambda_1 v_1 + \dots + \lambda_n v_n = 0_V \iff \lambda_1 = \dots = \lambda_n = 0 \implies \lambda_n v_n = -\lambda_1 v_1 - \dots - \lambda_{n-1} v_{n-1} \implies$$

$$\implies v_n = -\lambda_n^{-1} \lambda_1 v_1 - \dots - \lambda_n^{-1} \lambda_{n-1} v_{n-1} \implies v_n \in \text{Span}(v_1, \dots, v_{n-1})$$
- Di conseguenza, si ha che $\lambda_n = 0 \implies v_n \notin \text{Span}(v_1, \dots, v_{n-1})$ e che:

$$\lambda_n = 0 \implies \lambda_1 v_1 + \dots + \lambda_{n-1} v_{n-1} + \lambda_n v_n = 0_V \implies$$

$$\implies \lambda_1 v_1 + \dots + \lambda_{n-1} v_{n-1} = 0_V \iff \lambda_1 = \dots = \lambda_{n-1} = 0 = \lambda_n$$

Proposition 64

Se i vettori $v_1, \dots, v_k \in \text{Span}(w_1, \dots, w_n) \subseteq V$ sono linearmente indipendenti, allora $k \leq n$

Dimostrazione:

- Supponiamo $v_1 \neq 0_V \in \text{Span}(w_1, \dots, w_n)$, dunque

$$v = \lambda_1 w_1 + \dots + \lambda_n w_n \neq 0_V \iff \exists i \in [1, n] \mid \lambda_i \neq 0$$

- A meno di riordinare i termini, supponiamo $\lambda_1 \neq 0$

$$\begin{aligned} v &= \lambda_1 w_1 + \dots + \lambda_n w_n \implies \lambda_1 w_1 = v - \lambda_2 w_2 - \dots - \lambda_n w_n \implies \\ \implies w_1 &= \lambda_1^{-1} v + (-\lambda_1^{-1} \lambda_2) w_2 - \dots + (-\lambda_1^{-1} \lambda_n) w_n \implies w_1 \in \text{Span}(v_1, w_2, \dots, w_n) \end{aligned}$$

- Poiché $w_1 = \mu_1 v_1 + \mu_2 w_2 + \dots + \mu_n w_n \in \text{Span}(v_1, w_2, \dots, w_n)$, allora

$$\begin{aligned} u \in \text{Span}(w_1, \dots, w_n) &\implies u = \lambda_1 w_1 + \lambda_2 w_2 + \dots + \lambda_n w_n = \\ &= \lambda_1 (\mu_1 v_1 + \mu_2 w_2 + \dots + \mu_n w_n) + \lambda_2 w_2 + \dots + \lambda_n w_n = \\ &= (\lambda_1 \mu_1) v_1 + (\lambda_1 \lambda_2 \mu_2) w_2 + \dots + (\lambda_1 \lambda_n \mu_n) w_n \implies u \in \text{Span}(v_1, w_2, \dots, w_n) \end{aligned}$$

- Dunque si ha che $\text{Span}(w_1, \dots, w_n) \subseteq \text{Span}(v_1, w_2, \dots, w_n)$. Analogamente, possiamo dimostrare che $\text{Span}(v_1, w_2, \dots, w_n) \subseteq \text{Span}(w_1, \dots, w_n)$, concludendo quindi che $\text{Span}(v_1, w_2, \dots, w_n) = \text{Span}(w_1, \dots, w_n)$
- Supponiamo quindi induttivamente che

$$\text{Span}(v_1, \dots, v_i, w_{i+1}, \dots, w_n) = \text{Span}(w_1, \dots, w_n)$$

- Dato $v_{i+1} = \mu_1 v_1 + \dots + \mu_i v_i + \lambda_{i+1} w_{i+1} + \dots + \lambda_n w_n \in \text{Span}(v_1, \dots, v_i, w_{i+1}, \dots, w_n)$, se si avesse $(\lambda_{i+1}, \dots, \lambda_n) = (0, \dots, 0)$, allora avremmo

$$v_{i+1} = \mu_1 v_1 + \dots + \mu_i v_i \implies 0_V = (-1)v_{i+1} + \mu_1 v_1 + \dots + \mu_i v_i$$

contraddicendo l'ipotesi che v_1, \dots, v_k siano linearmente indipendenti, dunque l'unica possibilità è

$$v_{i+1} = \mu_1 v_1 + \dots + \mu_i v_i + \lambda_{i+1} w_{i+1} + \dots + \lambda_n w_n \neq 0_V \iff \exists j \in [i+1, n] \mid \lambda_j \neq 0$$

- A meno di riordinare i termini, supponiamo $\lambda_{i+1} \neq 0$

$$\begin{aligned} v_{i+1} &= \mu_1 v_1 + \dots + \mu_i v_i + \lambda_{i+1} w_{i+1} + \dots + \lambda_n w_n \implies \\ \implies \lambda_{i+1} w_{i+1} &= v_{i+1} - \mu_1 v_1 - \dots - \mu_i v_i - \lambda_{i+2} w_{i+2} - \dots - \lambda_n w_n \implies \\ w_{i+1} &= \lambda_{i+1}^{-1} v_{i+1} + (-\lambda_{i+1}^{-1} \mu_1) v_1 + \dots + (-\lambda_{i+1}^{-1} \mu_i) v_i + (-\lambda_{i+1}^{-1} \lambda_{i+2}) w_{i+2} + \dots + (-\lambda_{i+1}^{-1} \lambda_n) w_n \\ \implies w_{i+1} &\in \text{Span}(v_1, \dots, v_i, v_{i+1}, w_{i+2}, \dots, w_n) \end{aligned}$$

- Dunque si ha che

$$\text{Span}(v_1, \dots, v_i, w_{i+1}, w_{i+2}, \dots, w_n) \subseteq \text{Span}(v_1, \dots, v_i, v_{i+1}, w_{i+2}, \dots, w_n)$$

.

Analogamente, possiamo dimostrare che

$$\text{Span}(v_1, \dots, v_i, v_{i+1}, w_{i+2}, \dots, w_n) \subseteq \text{Span}(v_1, \dots, v_i, w_{i+1}, w_{i+2}, \dots, w_n)$$

concludendo quindi che

$$\text{Span}(v_1, \dots, v_i, v_{i+1}, w_{i+2}, \dots, w_n) = \text{Span}(v_1, \dots, v_i, w_{i+1}, w_{i+2}, \dots, w_n)$$

e quindi, per induzione, che $\text{Span}(v_1, \dots, v_n) = \text{Span}(w_1, \dots, w_n)$

- Se per assurdo si avesse che $k > n$, allora

$$v_{n+1} \in \text{Span}(w_1, \dots, w_n) = \text{Span}(v_1, \dots, v_n)$$

contraddicendo l'ipotesi che v_1, \dots, v_k siano indipendenti.

Corollary 27

Siano $v_1, \dots, v_n \in V$ e $w_1, \dots, w_m \in V$ due basi di V . In tal caso, si ha che $n = m$, ossia hanno la stessa **cardinalità**

Dimostrazione:

- Siccome sono entrambi basi, si ha che

$$\text{Span}(v_1, \dots, v_n) = V = \text{Span}(w_1, \dots, w_m)$$

- Di conseguenza, poiché i vettori $v_1, \dots, v_n \in V = \text{Span}(w_1, \dots, w_m)$ sono linearmente indipendenti, allora $n \leq m$
- Analogamente, poiché i vettori $w_1, \dots, w_m \in V = \text{Span}(v_1, \dots, v_n)$ sono linearmente indipendenti, allora $m \leq n$
- Dunque, l'unica possibilità è che $n = m$

Definition 64. Dimensione di uno spazio vettoriale

Dato uno spazio vettoriale V su K , definiamo come **dimensione di V** ($\dim(V)$) la cardinalità di una sua base

Esempio:

- Data la base canonica di K^n , ossia e_1, \dots, e_n , si ha che:

$$\dim(K^n) = n$$

Observation 50

I vettori $v_1, \dots, v_n \in V$ sono una base di V se e solo se

$$\forall v \in V, \exists! \lambda_1, \dots, \lambda_n \mid v = \lambda_1 v_1 + \dots + \lambda_n v_n$$

Inoltre, chiamiamo tali unici scalari come **coordinate di v in tale base**

Dimostrazione:

- Se $v_1, \dots, v_n \in V$ sono una base di V , in quanto generatori di V si ha che ogni vettore $v \in V$ può essere espresso come una combinazione lineare di v_1, \dots, v_n .
- Supponiamo ora che esistano due combinazioni lineari tali che

$$\mu_1 v_1 + \dots + \mu_n v_n = v = \lambda_1 v_1 + \dots + \lambda_n v_n$$

- In tal caso si ha che

$$\begin{aligned} \mu_1 v_1 + \dots + \mu_n v_n = \lambda_1 v_1 + \dots + \lambda_n v_n &\implies \mu_1 v_1 + \dots + \mu_n v_n - \lambda_1 v_1 - \dots - \lambda_n v_n = 0_V \implies \\ &\implies (\lambda_1 - \mu_1) v_1 + \dots + (\lambda_n - \mu_n) v_n = 0_V \end{aligned}$$

- Poiché v_1, \dots, v_n sono linearmente indipendenti, si ha che:

$$(\lambda_1 - \mu_1) v_1 + \dots + (\lambda_n - \mu_n) v_n = 0_V \iff (\lambda_1 - \mu_1) = \dots = (\lambda_n - \mu_n) = 0$$

implicando quindi che

$$\lambda_1 = \mu_1, \dots, \lambda_n = \mu_n$$

Observation 51

Diciamo che V ha dimensione infinita se non esiste un insieme finito di generatori

Esempi:

- Lo spazio vettoriale V definito su $K[x]$ non può avere base finita: dati $p_1(x), \dots, p_n(x) \in V$ e $\lambda_1, \dots, \lambda_n \in K$ si ha che:

$$\deg(\lambda_1 p_1(x) + \dots + \lambda_n p_n(x)) \leq \max(\deg(p_1(x)), \dots, \deg(p_n(x)))$$

Infatti, in tale esempio la base è data dai monomi $1, x, x^2, \dots$

- Lo spazio vettoriale V definito su $K^S : \{f : S \rightarrow K\}$ ha dimensione finita se e solo se S ha cardinalità finita

8.2 Trasformazioni lineari

Definition 65. Trasformazione lineare

Dati due spazi vettoriali V e W definiti sullo stesso campo K , la funzione $f : V \rightarrow W$ viene detta **trasformazione lineare** (o morfismo tra spazi vettoriali) se:

- $\forall v, v' \in V, f(v + v') = f(v) + f(v')$
- $\forall \lambda \in K, v \in V, f(\lambda v) = \lambda f(v)$

Theorem 65

Dato uno spazio vettoriale V si ha che:

$$\dim(V) = n \implies V \cong K^n$$

Dimostrazione:

- Siano v_1, \dots, v_n una base di V (dunque $\dim(V) = n$). Definiamo la funzione

$$f : K^n \rightarrow V : (t_1, \dots, t_n) \mapsto (t_1 v_1 + \dots + t_n v_n)$$

- Poiché $\forall v \in V, \exists! \lambda_1, \dots, \lambda_n \mid v = \lambda_1 v_1 + \dots + \lambda_n v_n$, la funzione f è automaticamente biettiva:

$$\left. \begin{array}{l} v_1, \dots, v_n \text{ generatori di } V \implies f \text{ suriettiva} \\ v_1, \dots, v_n \text{ lin. indipendenti} \implies f \text{ iniettiva} \end{array} \right\} \implies f \text{ biettiva}$$

- Dati quindi $x = (x_1, \dots, x_n), y = (y_1, \dots, y_n) \in K^n$, si ha che:

$$f(x+y) = (x_1+y_1)v_1 + \dots + (x_n+y_n)v_n = x_1 v_1 + \dots + x_n v_n + y_1 v_1 + \dots + y_n v_n = f(x) + f(y)$$

- Dato invece $\lambda \in K$, si ha che:

$$f(\lambda v) = \lambda x_1 v_1 + \dots + \lambda x_n v_n = \lambda(x_1 v_1 + \dots + x_n v_n) = \lambda f(x)$$

- Dunque, concludiamo che f sia un isomorfismo, implicando che anche f^{-1} lo sia.

$$V \cong K^n$$

Theorem 66

Dati due spazi vettoriali V e W definiti sullo stesso K , si ha che:

$$V \cong W \iff \dim(V) = \dim(W)$$

Dimostrazione:

- $\dim(V) = \dim(W) \implies V \cong W$
 - Sappiamo già che $\dim(V) = \dim(W) = n \implies V \cong K^n \cong W$
- $V \cong W \implies \dim(V) = \dim(W)$
 - Supponiamo che $V \cong W$, dove f è l'isomorfismo, e sia v_1, \dots, v_n una base di V .
 - Siccome f è suriettiva si ha che $\forall w \in W, \exists v \in V \mid w = f(v)$, dunque si ha che
$$w = f(v) = f(\lambda_1 v_1 + \dots + \lambda_n v_n) = \lambda_1 f(v_1) + \dots + \lambda_n f(v_n) \in \text{Span}(f(v_1), \dots, f(v_n))$$

Dunque $f(v_1), \dots, f(v_n)$ sono generatori di W

- Siccome f è un morfismo, si ha che

$$f(0_V) = 0_W = \lambda_1 f(v_1) + \dots + \lambda_n f(v_n) = f(\lambda_1 v_1 + \dots + \lambda_n v_n)$$

- Siccome f è suriettiva, allora

$$f(0_V) = f(\lambda_1 v_1 + \dots + \lambda_n v_n) \iff 0_V = \lambda_1 v_1 + \dots + \lambda_n v_n$$

- Siccome v_1, \dots, v_n sono linearmente indipendenti, allora

$$0_V = \lambda_1 v_1 + \dots + \lambda_n v_n \iff \lambda_1 = \dots = \lambda_n = 0$$

implicando quindi che anche $f(v_1), \dots, f(v_n)$ siano linearmente indipendenti

$$0_W = \lambda_1 f(v_1) + \dots + \lambda_n f(v_n) \iff \lambda_1 = \dots = \lambda_n = 0$$

- I vettori $f(v_1), \dots, f(v_n)$ sono quindi una base di W , la cui dimensione corrisponde a quella di V

Definition 66. Spazio quoziente

Dato uno spazio vettoriale V e un sottospazio $W \subseteq V$, lo **spazio quoziente** V/W è uno spazio vettoriale con la somma $[v] + [v'] = [v + v']$ e il prodotto con scalare $\lambda[x] = [\lambda x]$

Dimostrazione:

- La dimostrazione della ben definizione della somma è analoga a quella del normale gruppo quoziente
- Dimostriamo quindi che il prodotto con scalare sia ben definito

$$[v] = [v'] \implies v' - v \in W \implies \lambda(v' - v) = \lambda v' - \lambda v \in W \implies [\lambda v] = [\lambda v']$$

Theorem 67. Dimensione spazio quoziente

Dato uno spazio vettoriale V e un sottospazio $W \subseteq V$, si verifica che

$$\dim(V/W) = \dim(V) - \dim(W)$$

Dimostrazione:

- Sia w_1, \dots, w_k una base di W . Se $\dim(V) > k$ allora $\text{Span}(w_1, \dots, w_k) \subsetneq V$.
- Di conseguenza, esiste $v_{k+1} \in V \mid v_{k+1} \notin \text{Span}(w_1, \dots, w_k)$, implicando che w_1, \dots, w_k, v_{k+1} siano linearmente indipendenti
- A questo punto, se $\dim(V) > k+1$, allora esiste $v_{k+2} \in V \mid v_{k+2} \notin \text{Span}(w_1, \dots, w_k, v_{k+1})$, implicando che $w_1, \dots, w_k, v_{k+1}, v_{k+2}$ siano linearmente indipendenti
- Ripetendo tale procedimento $n - k = \dim(V) - \dim(W)$ volte arriviamo a costruire una base di V della forma $w_1, \dots, w_k, v_{k+1}, \dots, v_n$
- Dato $v \in \text{Span}(w_1, \dots, w_k, v_{k+1}, \dots, v_n)$, si ha che:

$$\begin{aligned} v &= \lambda_1 w_1 + \dots + \lambda_k w_k + \lambda_{k+1} v_{k+1} + \dots + \lambda_n v_n \implies \\ \implies [v] &= \lambda_1 [w_1] + \dots + \lambda_k [w_k] + \lambda_{k+1} [v_{k+1}] + \dots + \lambda_n [v_n] \end{aligned}$$

- Notiamo come

$$\begin{aligned} w_1, \dots, w_k \in W &\implies 0_V - w_1, \dots, 0_V - w_k \in W \implies \\ \implies w_1 \sim 0_V, \dots, w_k \sim 0_V &\implies [0_V] = [w_1] = \dots = [w_k] \end{aligned}$$

- Di conseguenza, si ha che $[v_{k+1}], \dots, [v_n]$ sono generatori di V/K

$$\begin{aligned} [v] &= \lambda_1 [w_1] + \dots + \lambda_k [w_k] + \lambda_{k+1} [v_{k+1}] + \dots + \lambda_n [v_n] \implies \\ \implies [v] &= \lambda_1 [0_V] + \dots + \lambda_k [0_V] + \lambda_{k+1} [v_{k+1}] + \dots + \lambda_n [v_n] = \lambda_{k+1} [v_{k+1}] + \dots + \lambda_n [v_n] \end{aligned}$$

- Supponiamo quindi $[0_V] \in V/W$ possa essere scritto come una combinazione lineare di V/W :

$$\begin{aligned} [0_V] &= \lambda_{k+1} [v_{k+1}] + \dots + \lambda_n [v_n] \implies \\ \implies [0_V] &= [\lambda_{k+1} v_{k+1} + \dots + \lambda_n v_n] \implies \end{aligned}$$

- Poiché $\lambda_{k+1} v_{k+1} + \dots + \lambda_n v_n \in W$, si ha che

$$\begin{aligned} \lambda_{k+1} v_{k+1} + \dots + \lambda_n v_n &= \lambda_1 w_1 + \dots + \lambda_k w_k \implies \\ \lambda_{k+1} v_{k+1} + \dots + \lambda_n v_n - \lambda_1 w_1 - \dots - \lambda_k w_k &= 0_V \end{aligned}$$

- Poiché $w_1, \dots, w_k, v_{k+1}, \dots, v_n$ sono linearmente indipendenti, allora

$$\lambda_{k+1} v_{k+1} + \dots + \lambda_n v_n - \lambda_1 w_1 - \dots - \lambda_k w_k = 0_V \iff \lambda_1 = \dots = \lambda_k = \lambda_{k+1} = \dots = \lambda_n = 0$$

implicando quindi che anche $\lambda_{k+1} v_{k+1} + \dots + \lambda_n v_n$ siano linearmente indipendenti, rendendoli una base di V/W , la cui dimensione è $n - k = \dim(V) - \dim(W)$

8.2.1 Teorema del Rango e Formula di Grassman

Proposition 68

Dati due spazi vettoriali V e W e una trasformazione lineare $f : V \rightarrow W$, il nucleo $Ker(f) \subseteq V$ e l'immagine $Im(f) \subseteq W$ di f sono definiti come

$$Ker(f) : \{v \in V \mid f(v) = 0_W\}$$

$$Im(f) : \{w \in W \mid w = f(v), \exists v \in V\}$$

I quali sono entrambi sottospazi vettoriali, rispettivamente di V e W

Dimostrazione:

- Sappiamo già che essi sono sottogruppi per la somma
- Verifichiamo quindi che siano chiusi nel prodotto con scalare

$$v \in Ker(f), \lambda \in K \implies f(\lambda v) = \lambda f(v) = \lambda 0_W = 0_W \implies \lambda v \in Ker(f)$$

$$w = f(v) \in Im(f), \lambda \in K \implies \lambda w = \lambda f(v) = f(\lambda v) \implies \lambda w \in Im(f)$$

Observation 52. Teorema fondamentale di isomorfismo

Data una trasformazione lineare $f : V \rightarrow W$, si ha che

$$V/Ker(f) \cong Im(f)$$

Implicando anche che $\dim(V/Ker(f)) = \dim(Im(f))$

Theorem 69. Teorema del Rango

Data una trasformazione lineare $f : V \rightarrow W$, definiamo come **rango di f** la dimensione della sua immagine:

$$rk(f) := \dim(Im(f)) = \dim(V/Ker(f)) = \dim(V) - \dim(Ker(f))$$

Proposition 70

Sia $\dim(W) = n$. Si verifica che:

1. Dati $w_1, \dots, w_k \in W$ linearmente indipendenti, dove $k < n$, allora $\exists w_{k+1}, \dots, w_n \mid w_1, \dots, w_n$ è base (estensione ad una base)
2. Dati $w_1, \dots, w_m \in W$ generatori, dove $m \geq n$, allora $\exists 1 \leq i_1, \dots, i_n \leq m \mid w_{i_1}, \dots, w_{i_n}$ sono una base di W (riduzione ad una base)
3. Dati $w_1, \dots, w_n \in W$, siccome $\dim(W) = n$, allora w_1, \dots, w_n sono linearmente indipendenti se e solo se sono anche generatori

Dimostrazioni:

1.
 - Poiché $k < n$, allora $\exists w_{k+1} \in W \mid w_{k+1} \notin \text{Span}(w_1, \dots, w_k)$, implicando che w_1, \dots, w_{k+1} siano linearmente indipendenti.
 - Analogamente, possiamo ripetere tale procedimento $n - k$ volte, estendendo tale insieme linearmente indipendente fino a che $\text{Span}(w_1, \dots, w_n) = W$, ossia fino a che diventino anche generatori e quindi una base
 - Notiamo come non potremmo ripetere tale procedimento $n - k + 1$ volte, poiché $w_{n+1} \in W = \text{Span}(w_1, \dots, w_n) \implies w_1, \dots, w_n, w_{n+1}$ non linearmente indipendenti

2.
 - Poiché w_1, \dots, w_m sono generatori, possiamo assumere che $\exists w_{i_1} \neq 0$ tra di essi, il quale è (ovviamente) linearmente indipendente con se stesso
 - Siccome $\text{Span}(w_{i_1}) \subsetneq W = \text{Span}(w_1, \dots, w_m)$, allora $\exists w_{i_2} \mid w_{i_2} \notin \text{Span}(w_{i_1})$, implicando che w_{i_1}, w_{i_2} siano linearmente indipendenti
 - Ripetendo tale procedimento n volte fino a che $\text{Span}(w_{i_1}, \dots, w_{i_n}) = W = \text{Span}(w_1, \dots, w_m)$, ossia fino a che diventino anche generatori e quindi una base
 - Notiamo come non potremmo ripetere tale procedimento $n + 1$ volte, poiché $w_{i_{n+1}} \in W = \text{Span}(w_{i_1}, \dots, w_{i_n}) \implies w_{i_1}, \dots, w_{i_n}, w_{i_{n+1}}$ non linearmente indipendenti

3.
 - w_1, \dots, w_n linearmente indipendenti \implies generatori
 - Supponiamo per assurdo che w_1, \dots, w_n siano linearmente indipendenti ma non generatori, dunque che $\text{Span}(w_1, \dots, w_n) \subsetneq W$
 - Di conseguenza, si ha che $\exists w_{n+1} \in W \mid w_{n+1} \notin \text{Span}(w_1, \dots, w_n)$, implicando che w_1, \dots, w_{n+1} siano linearmente indipendenti
 - Tuttavia, come visto nella prima osservazione, sappiamo che se $\dim(W) = n$, allora w_1, \dots, w_{n+1} non possono essere linearmente indipendenti
 - w_1, \dots, w_n generatori \implies linearmente indipendenti
 - Supponiamo per assurdo che w_1, \dots, w_n siano generatori ma non linearmente indipendenti, dunque che

$$\lambda_1 w_1 + \dots + \lambda_n w_n = 0_W, \exists j \in [1, n] \mid \lambda_j \neq 0 \implies$$

$$\begin{aligned} \implies w_j &= -\lambda_j^{-1} \lambda_1 w_1 - \dots - \lambda_j^{-1} \lambda_n w_n \implies w \in \text{Span}(w_1, \dots, \hat{w}_j, \dots, w_n) \implies \\ &\implies \text{Span}(w_1, \dots, w_n) = W \subseteq \text{Span}(w_1, \dots, \hat{w}_j, \dots, w_n) \end{aligned}$$

dove \hat{w} indica che tale elemento è escluso

- Inoltre, per definizione stessa, sappiamo che

$$\text{Span}(w_1, \dots, \hat{w}_j, \dots, w_n) \subseteq \text{Span}(w_1, \dots, w_n) = W$$

dunque concludiamo che

$$\text{Span}(w_1, \dots, \hat{w}_j, \dots, w_n) = W = \text{Span}(w_1, \dots, w_n)$$

- Tuttavia, $\dim(W) = n$ è impossibile che W possa avere una base di dimensione $n - 1$

Theorem 71. Formula di Grassmann

Sia W uno spazio vettoriale su K e siano $U, V \subseteq W$ due sottospazi. Esistono due sottospazi di W , ossia:

$$U + V : \{u + v \mid u \in U, v \in V\}$$

$$U \cap V : \{w \mid w \in U \wedge w \in V\}$$

da cui si ha che:

$$\dim(U + V) = \dim(U) + \dim(V) - \dim(U \cap V)$$

Dimostrazione:

- Posti $k := \dim(U \cap V)$, $m := \dim(U)$, $n := \dim(V)$, siano:

- w_1, \dots, w_k una base di $U \cap V$
- $B_1 := w_1, \dots, w_k, u_{k+1}, \dots, u_m$ una base di U
- $B_2 := w_1, \dots, w_k, v_{k+1}, \dots, v_n$ una base di V

- Consideriamo quindi il seguente insieme di vettori:

$$B_1 \cup B_2 = w_1, \dots, w_k, u_{k+1}, \dots, u_m, v_{k+1}, \dots, v_n$$

- Consideriamo ora $u \in \text{Span}(B_1) = U$ e $v \in \text{Span}(B_2)$, dunque

$$u = \sum_{i=1}^k \lambda_i w_i + \sum_{j=k+1}^m \lambda_j u_j \quad v = \sum_{i=1}^k \lambda_i w_i + \sum_{j=k+1}^n \lambda_j v_j$$

- Dunque $\forall u \in U, v \in V$ si ha che :

$$\begin{aligned} u + v &= \sum_{i=1}^k \lambda_i w_i + \sum_{j=k+1}^m \lambda_j u_j + \sum_{i=1}^k \mu_i w_i + \sum_{j=k+1}^n \mu_j v_j \implies \\ \implies u + v &= \sum_{i=1}^k (\lambda_i + \mu_i) w_i + \sum_{j=k+1}^m \lambda_j u_j + \sum_{j=k+1}^n \mu_j v_j \implies \implies u + v \in \text{Span}(B_1 \cup B_2) \end{aligned}$$

- Dunque, si ha che $B_1 \cup B_2$ sono generatori di $U + V$

- Consideriamo quindi $0_W \in U + V$ scritto come combinazione lineare di tale base

$$\sum_{i=1}^k \beta_i w_i + \sum_{j=k+1}^m \gamma_j u_j + \sum_{h=k+1}^n \eta_h v_h = 0_W$$

- A questo punto, poniamo:

$$a := \sum_{i=1}^k \beta_i w_i \quad b := \sum_{j=k+1}^m \gamma_j u_j \quad c := \sum_{h=k+1}^n \eta_h v_h$$

dunque si ha che:

$$a + b + c = 0_W \implies b = -a - c = -(a + c)$$

- Siccome $b \in \text{Span}(u_{k+1}, \dots, u_m) \subsetneq U \implies b \in U$ e $-(a + c) \in \text{Span}(B_2) = V$, allora (poiché $b = -(a + c)$) ne segue che $b \in U \cap V$
- Di conseguenza, possiamo riscrivere b anche come una combinazione lineare della base di $U \cap V$, ossia w_1, \dots, w_k :

$$\sum_{j=k+1}^m \gamma_j u_j = b = \sum_{t=0}^k \alpha_t w_t \implies \sum_{j=k+1}^m \gamma_j u_j - \sum_{t=0}^k \alpha_t w_t = 0_W$$

- Poiché u_{k+1}, \dots, u_m e w_1, \dots, w_k sono entrambi insiemi linearmente indipendenti, allora ne segue che

$$\sum_{j=k+1}^m \gamma_j u_j - \sum_{t=0}^k \alpha_t w_t = 0_W \iff \gamma_{k+1} = \dots = \gamma_m = \alpha_1 = \dots = \alpha_k = 0$$

e dunque che $w_1, \dots, w_k, u_{k+1}, \dots, u_m$ siano anch'essi linearmente indipendenti, implicando quindi che

$$a + b + c = 0_W \iff a + c = 0_W$$

poiché $\gamma_{k+1} = \dots = \gamma_m = 0$

- Analogamente, ponendo $c = -(a+b)$, arriviamo a dimostrare che $w_1, \dots, w_k, v_{k+1}, \dots, v_n$ siano anch'essi linearmente indipendenti, implicando quindi che

$$a + c = 0_W \iff a = 0_W$$

poiché $\eta_{k+1} = \dots = \eta_n = 0$

- Infine, sappiamo già che w_1, \dots, w_k sono linearmente indipendenti, poiché sono una base di $U \cap V$, implicando quindi che $\beta_1 = \dots = \beta_k = 0$, e di conseguenza che

$$a + b + c = 0_W \iff \beta_1 = \dots = \beta_k = \gamma_{k+1} = \dots = \gamma_m = \eta_{k+1} = \dots = \eta_n = 0$$

e dunque che i generatori di $U + V$ siano anche linearmente indipendenti e quindi che siano una base

- Infine, concludiamo affermando che la base di $U + V$ abbia dimensione pari a:

$$\dim(U + V) = k + (m - k) + (n - k) = m + n - k = \dim(U) + \dim(V) - \dim(U \cap V)$$

8.3 Spazi affini, Sottospazi affini e Giacitura

Definition 67. Spazio affine

Dato uno spazio vettoriale V , definiamo come **spazio affine** A la struttura algebrica dotata della funzione:

$$f : A \times V \rightarrow A : (P, v) \rightarrow a + v$$

tale che:

- $\forall P \in A$ fissato, la funzione associa il punto $P + v$ al vettore $v \in V$, creando una biezione $g : V \rightarrow A$
- $\forall P \in A, \forall v, w \in V$ si ha che:

$$(P + v) + w = P + (v + w)$$

Definition 68. Sottospazio affine

Dato uno spazio vettoriale V , un suo sottospazio vettoriale W e un vettore $v \in V$, definiamo come **sottospazio affine** il sottospazio di V generato da:

$$S = v + W : \{v + w \mid w \in W\}$$

In altre parole, si tratta del sottospazio W traslato dal vettore v . Ogni sottospazio affine può essere visto come una **classe laterale di un sottospazio** (poiché l'operazione primaria degli spazi vettoriali è $+$)

Definition 69. Giacitura

Dato uno spazio vettoriale V ed un suo sottospazio affine $S \subset V$, definiamo come **giacitura di S** , indicata con $Giac(S)$, il sottospazio vettoriale associato a S , ossia il sottospazio vettoriale tale che:

$$S = v + Giac(S)$$

dove $v \in V$.

In altre parole, la giacitura è il sottospazio generante le sue stesse classi laterali su V .

Inoltre, si ha che $\dim(S) = \dim(Giac(S))$

8.4 Prodotto scalare

Definition 70. Prodotto scalare

Il **prodotto scalare** tra due vettori corrisponde all'operazione binaria

$$\cdot : K^n \times K^n \rightarrow K : (v, v') \mapsto \eta$$

In particolare, dati due vettori $v = (\lambda_1, \dots, \lambda_n), v' = (\mu_1, \dots, \mu_n) \in K^n$, il prodotto scalare tra di essi è definito come:

$$v \cdot v' = \sum_{i=1}^n \lambda_i \mu_i$$

Observation 53

Il prodotto scalare gode delle seguenti proprietà:

- $u, v \in K^n \implies u \cdot v = v \cdot u$
- $u, v, w \in K^n \implies u(v + w) = uv + uw$
- $u, v \in K^n, \lambda \in K \implies u(\lambda v) = \lambda uv$

Definition 71. Norma di un vettore

Dato $v \in \mathbb{R}^n$, definiamo la **norma (o lunghezza)** di tale vettore come

$$\|v\| := \sqrt{v \cdot v} = \sqrt{x_1 \cdot x_1 + \dots + x_n \cdot x_n} = \sqrt{x_1^2 + \dots + x_n^2}$$

Observation 54

Dati $u, v \in \mathbb{R}^n$ e l'angolo $0 < \theta < \pi$ interno tra u e v , si ha che

$$\cos \theta = \frac{uv}{\|u\| \|v\|}$$

e in particolare che:

- $\theta < \frac{\pi}{2} \iff uv > 0$
- $\theta = \frac{\pi}{2} \iff uv = 0$
- $\theta > \frac{\pi}{2} \iff uv < 0$

Dimostrazione:

- Tramite il [Teorema del Coseno](#) (normalmente utilizzato per calcolare la lunghezza di un lato di un triangolo qualsiasi sapendo la lunghezza degli altri due lati), nel caso dei vettori si ha che:

$$\|v - u\|^2 = \|u\|^2 + \|v\|^2 - 2 \|u\| \|v\| \cos \theta \implies$$

$$\implies \|v - u\|^2 - \|u\|^2 - \|v\|^2 = -2 \|u\| \|v\| \cos \theta \implies$$

$$\implies \sum_{i=1}^n (y_i - x_i)^2 - \sum_{j=1}^n x_j^2 - \sum_{k=1}^n y_k^2 = -2 \|u\| \|v\| \cos \theta \implies$$

$$\implies \sum_{i=1}^n (y_i^2 - 2y_i x_i + x_i^2) - \sum_{j=1}^n x_j^2 - \sum_{k=1}^n y_k^2 = -2 \|u\| \|v\| \cos \theta \implies$$

$$\implies \sum_{i=1}^n y_i^2 - 2 \sum_{h=1}^n y_h x_h + \sum_{t=1}^n x_t^2 - \sum_{j=1}^n x_j^2 - \sum_{k=1}^n y_k^2 = -2 \|u\| \|v\| \cos \theta \implies$$

$$\implies \sum_{h=1}^n y_h x_h = \|u\| \|v\| \cos \theta \implies \sum_{h=1}^n y_h x_h = \|u\| \|v\| \cos \theta \implies$$

$$\implies uv = \|u\| \|v\| \cos \theta \implies \frac{uv}{\|u\| \|v\|} = \cos \theta$$

Capitolo 9

Matrici

Definition 72. Matrici

Dati $m, n \neq 0 \in \mathbb{N}$, una **matrice** $m \times n$ a coefficienti in un campo K è una griglia con m righe e n colonne, le cui entrate sono elementi in K

$$A \in \text{Mat}_{m \times n}(K) \implies A = \begin{pmatrix} a_{1,1} & \cdots & a_{1,n} \\ \vdots & \ddots & \vdots \\ a_{m,1} & \cdots & a_{m,n} \end{pmatrix}$$

Esempio:

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix} \in \text{Mat}_{2 \times 3}(\mathbb{R})$$

Definition 73. Vettori colonna e Vettori riga

Definiamo una matrice $1 \times n$ come **vettore riga**

$$\begin{pmatrix} a_1 & \cdots & a_n \end{pmatrix} \in \text{Mat}_{1 \times n}(K)$$

e analogamente definiamo una matrice $m \times 1$ come **vettore colonna**

$$\begin{pmatrix} a_1 \\ \vdots \\ a_m \end{pmatrix} \in \text{Mat}_{m \times 1}(K)$$

Observation 55

Una matrice $m \times n$ può essere definita come un **vettore di m vettori riga aventi n elementi** (che vengono indicati con un pedice)

$$A_1, \dots, A_n \in K^m \implies A = \begin{pmatrix} A_1 & \cdots & A_n \end{pmatrix}$$

o come un **vettore di n vettori colonna aventi m elementi** (che vengono indicati con un apice)

$$A^1, \dots, A^m \in K^n \implies A = \begin{pmatrix} A^1 \\ \vdots \\ A^m \end{pmatrix}$$

Observation 56

Una matrice $m \times n$ è uno spazio vettoriale di dimensione $m \cdot n$

$$\dim(Mat_{m \times n}(K)) = m \cdot n$$

Esempi:

- Siano $A, B \in Mat_{m \times n}(K)$ e sia $\lambda \in K$. Si verifica che:

$$A + B = \begin{pmatrix} a_{1,1} + b_{1,1} & \cdots & a_{1,n} + b_{1,n} \\ \vdots & \ddots & \vdots \\ a_{m,1} + b_{m,1} & \cdots & a_{m,n} + b_{m,n} \end{pmatrix}$$

$$\lambda A = \begin{pmatrix} \lambda a_{1,1} & \cdots & \lambda a_{1,n} \\ \vdots & \ddots & \vdots \\ \lambda a_{m,1} & \cdots & \lambda a_{m,n} \end{pmatrix}$$

- La base canonica di una matrice 2×2 è la cui base canonica è

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

9.1 Prodotto tra matrici

Definition 74. Prodotto tra matrici

Siano $A \in \text{Mat}_{h \times m}(K)$, $B \in \text{Mat}_{m \times n}(K)$. Siano quindi $A_1, \dots, A_h \in K^m$ i vettori riga di A e siano $B^1, \dots, B^n \in K^m$ i vettori colonna di B .

Il **prodotto tra matrici** è l'operazione binaria

$$\cdot : \text{Mat}_{h \times m}(K) \times \text{Mat}_{m \times n}(K) \rightarrow \text{Mat}_{h \times n}(K) : (A, B) \mapsto AB$$

Il prodotto AB è una matrice appartenente a $\text{Mat}_{h \times n}(K)$ (dunque avente la stessa quantità di righe di A e la stessa quantità di colonne di B) ed è definito come:

$$AB = \begin{pmatrix} A_1 B^1 & \cdots & A_1 B^n \\ \vdots & \ddots & \vdots \\ A_h B^1 & \cdots & A_h B^n \end{pmatrix}$$

Attenzione: affinché il prodotto ben definito è necessario che la quantità di colonne di A sia uguale alla quantità di righe di B

Esempi:

- $\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \begin{pmatrix} 5 & 6 \\ 7 & 8 \end{pmatrix} = \begin{pmatrix} 1 \cdot 5 + 2 \cdot 7 & 1 \cdot 6 + 2 \cdot 8 \\ 3 \cdot 5 + 4 \cdot 7 & 3 \cdot 6 + 4 \cdot 8 \end{pmatrix} = \begin{pmatrix} 19 & 22 \\ 43 & 50 \end{pmatrix}$
- $\begin{pmatrix} 5 & 6 \\ 7 & 8 \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} = \begin{pmatrix} 5 \cdot 1 + 6 \cdot 3 & 5 \cdot 2 + 6 \cdot 4 \\ 7 \cdot 1 + 8 \cdot 3 & 7 \cdot 2 + 8 \cdot 4 \end{pmatrix} = \begin{pmatrix} 23 & 34 \\ 32 & 46 \end{pmatrix}$
- $\begin{pmatrix} 1 & 2 \\ 4 & 5 \end{pmatrix} \begin{pmatrix} 3 & 6 & 7 \\ -2 & 0 & 8 \end{pmatrix} = \begin{pmatrix} 1 \cdot 3 + 2 \cdot (-2) & 1 \cdot 6 + 2 \cdot 0 & 1 \cdot 7 + 2 \cdot 8 \\ 4 \cdot 3 + 5 \cdot (-2) & 4 \cdot 6 + 5 \cdot 0 & 4 \cdot 7 + 5 \cdot 8 \end{pmatrix} =$
 $= \begin{pmatrix} -1 & 6 & 23 \\ 2 & 24 & 68 \end{pmatrix}$
- $\begin{pmatrix} 3 & 6 & 7 \\ -2 & 0 & 8 \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 4 & 5 \end{pmatrix} = \nexists$ poiché la quantità di colonne nella prima non corrisponde a quella delle righe della seconda

Observation 57

Date tre matrici A, B, C ed uno scalare λ , se i prodotti sono ben definiti si ha che:

- $(AB)C = ABC = A(BC)$
- $A(B + C) = AB + AC$
- $(A + B)C = AC + BC$
- $\lambda(AB) = (\lambda A)B = A(\lambda B)$

Corollary 28

Uno spazio vettoriale $Mat_{n \times n}(K)$ (anche detto spazio delle matrici quadrate di ordine n) è un **anello non commutativo**, dove l'elemento neutro è:

$$I_n = \begin{pmatrix} 1 & 0 & \cdots & \cdots & 0 \\ 0 & 1 & 0 & \ddots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \ddots & 0 & 1 & 0 \\ 0 & \cdots & \cdots & 0 & 1 \end{pmatrix}$$

9.2 Rango di una matrice

Definition 75. Sottospazio ortogonale

Sia $V \subseteq K^n$ un sottospazio. Definiamo il **sottospazio ortogonale** $V^\perp \subseteq K^n$ come

$$V^\perp = \{w \in K^n \mid wv = 0, \forall v \in V\}$$

dove

$$\dim(V^\perp) = \dim(K^n) - \dim(V) = n - \dim(V)$$

Definition 76. Rango di una matrice

Data una matrice $A \in Mat_{m \times n}(K)$, definiamo la trasformazione lineare del **prodotto sinistro dei vettori colonna**

$$L_A : K^n \rightarrow K^m : x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \rightarrow Ax$$

Definiamo il **rango della matrice** A come:

$$rk(A) := rk(L_A) = \dim(\text{Span}(A^1, \dots, A^n)) = \dim(\text{Span}(A_m, \dots, A_m))$$

Dimostrazione:

- Analizziamo meglio il comportamento di tale funzione:

$$L_A(x) = Ax = \begin{pmatrix} a_{1,1} & \cdots & a_{1,n} \\ \vdots & \ddots & \vdots \\ a_{m,1} & \cdots & a_{m,n} \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} a_{1,1}x_1 + \cdots + a_{1,n}x_n \\ \vdots \\ a_{m,1}x_1 + \cdots + a_{m,n}x_n \end{pmatrix}$$

da cui traiamo che

$$\begin{aligned} \text{Ker}(L_A) &= \{x \in K^n \mid L_A(x) = Ax = 0_{K^m}\} = \\ &= \left\{ x \in K^n \mid \begin{pmatrix} xA_1 \\ \vdots \\ xA_m \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} \right\} = \text{Span}(A_1, \dots, A_m)^\perp \end{aligned}$$

ossia che $\text{Ker}(L_A)$ contiene tutte i vettori $x = (x_1, \dots, x_n) \in K^n$ che sono soluzione del seguente sistema:

$$\begin{cases} a_{1,1}x_1 + \dots + a_{1,n}x_n = 0 \\ \vdots \\ a_{m,1}x_1 + \dots + a_{m,n}x_n = 0 \end{cases}$$

- Tuttavia, possiamo anche riscrivere tale prodotto come una combinazione lineare dei vettori colonna di A (ossia A^1, \dots, A^n)

$$\begin{aligned} Ax &= \begin{pmatrix} a_{1,1}x_1 + \dots + a_{1,n}x_n \\ \vdots \\ a_{m,1}x_1 + \dots + a_{m,n}x_n \end{pmatrix} = x_1 \begin{pmatrix} a_{1,1} \\ \vdots \\ a_{m,1} \end{pmatrix} + \dots + x_n \begin{pmatrix} a_{1,n} \\ \vdots \\ a_{m,n} \end{pmatrix} = \\ &= x_1 A^1 + \dots + x_n A^n \implies Ax \in \text{Span}(A^1, \dots, A^n) \end{aligned}$$

e quindi abbiamo che $\text{Im}(L_A) = \text{Span}(A^1, \dots, A^n)$

- Il rango della matrice corrisponderà a:

$$\begin{aligned} rk(A) &:= rk(L_A) = \dim(\text{Span}(A^1, \dots, A^n)) = \dim(\text{Im}(L_A)) = \\ &= \dim(K^n) - \dim(\text{Ker}(L_A)) = n - \dim(\text{Ker}(L_A)) = \\ &= n - \dim(\text{Span}(A_1, \dots, A_n)^\perp) = \dim(\text{Span}(A_1, \dots, A_m)) \end{aligned}$$

Definition 77. Operazioni elementari su matrici

Possiamo effettuare tre tipi di **operazioni elementari** sulle righe o sulle colonne di $A \in \text{Mat}_{m \times n}(K)$:

1. Scambiare due righe (o colonne) tra di loro
2. Moltiplicare una riga (o colonna) per $\lambda \in K^*$
3. Sommare ad una riga (o colonna) un multiplo di un'altra riga (o colonna)

Nessuna di tali operazioni altera $\text{Ker}(L_A)$, mentre $\text{Im}(L_A)$ viene potenzialmente modificata, tuttavia mantenendo la stessa dimensione e di conseguenza lo stesso **rango della matrice**, poiché $\dim(\text{Im}(L_A)) = \dim(K^n) - \dim(\text{Ker}(L_A))$ e la dimensione di $\text{Ker}(L_A)$ e di K^n rimangono invariate.

Corollary 29

Diciamo che due matrici $A, B \in Mat_{m \times n}(K)$ sono uguali se è possibile l'una partendo dall'altra utilizzando solo operazioni elementari

Proposition 72

Se A e B sono equivalenti solo per righe, allora $Ker(L_A) = Ker(L_B)$ e $Im(L_A) \neq Im(L_B)$.

Se A e B sono equivalenti solo per colonne, allora $Im(L_A) = Im(L_B)$ e $Ker(L_A) \neq Ker(L_B)$.

In entrambi i casi si verifica che $rk(A) = rk(B)$

Observation 58

Data $A \in Mat_{m \times n}(K)$, si ha che:

$$0 \leq rk(A) \leq \min(m, n)$$

9.2.1 Riduzione a scala di una matrice**Definition 78. Matrice a scala**

Definiamo come **pivot** di una riga di una matrice il primo elemento non nullo a partire da sinistra di tale riga.

Una matrice $A \in Mat_{m \times n}(K)$ viene detta **matrice a scala** se $\forall i \in [1, m]$ si verifica che il pivot della riga A_i è più a sinistra pivot della riga A_{i+1}

Esempi:

- Le seguenti matrici sono a scala, i cui pivot sono cerchiati:

$$\begin{pmatrix} \textcircled{1} & 0 & 2 & 0 & -1 \\ 0 & \textcircled{1} & 0 & 3 & 4 \\ 0 & 0 & 0 & \textcircled{1} & 2 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} \quad \begin{pmatrix} 0 & \textcircled{1} & 2 & 3 & 4 \\ 0 & 0 & 0 & \textcircled{5} & 6 \\ 0 & 0 & 0 & 0 & \textcircled{7} \end{pmatrix}$$

- Le seguenti matrici non sono a scala:

$$\begin{pmatrix} 1 & 3 & 0 \\ 0 & 3 & 3 \\ 0 & 9 & 2 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 6 \\ 0 & 0 & 3 \\ 8 & 0 & 0 \end{pmatrix}$$

Method 4. Algoritmo di Gauss-Jordan

Ogni matrice $A \in \text{Mat}_{n \times m}(K)$ può essere ridotta ad una **matrice a scala** $S \in \text{Mat}_{n \times m}(K)$ tramite il seguente algoritmo:

1. Sia A^j , dove $j \in [1, n]$ la prima colonna a partire da sinistra non nulla, ossia $\exists i[1, n] \mid c := a_{i,j} \neq 0$
2. Se $c \notin A_1$, allora la i -esima riga contenente c viene scambiata con A_1
3. Per $k = 2, \dots, m$, sottraiamo λA_1 alla riga A_k , dove λ è uno scalare scelto apposta in modo da annullare l' i -esimo elemento della
4. Se la matrice risultante non è ancora ridotta a scala, allora viene ripetuto ricorsivamente l'algoritmo su A_2 , ignorando le prime i colonne, e così via

Theorem 73

Data una matrice $A \in \text{Mat}_{m \times n}(K)$ e la sua versione ridotta a scala S , se S^{j_1}, \dots, S^{j_h} sono le colonne contenenti i pivot della scal, allora A^{j_1}, \dots, A^{j_h} sono una base di $\text{Span}(A^1, \dots, A^n)$, implicando che $h = rk(S) = rk(A)$

Esempio:

- Consideriamo il seguente sistema:

$$\begin{cases} x + 2y + 3z = 0 \\ 4x + 5y + 6z = 0 \\ 7x + 8y + 9z = 0 \end{cases}$$

- Tale sistema corrisponde fedelmente alla seguente matrice, dove A_1, \dots, A_m sono le righe:

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

- Sottraiamo $-4A_1$ ad A_2 e $-7A_1$ ad A_3 :

$$\begin{pmatrix} 1 & 2 & 3 \\ 0 & -3 & -6 \\ 0 & -6 & -12 \end{pmatrix}$$

- Sommiamo $-2A_2$ ad A_3 :

$$\begin{pmatrix} 1 & 2 & 3 \\ 0 & -3 & -6 \\ 0 & 0 & 0 \end{pmatrix}$$

- La matrice ottenuta risulta essere a scala:

$$\begin{pmatrix} 1 & 2 & 3 \\ 0 & -3 & -6 \\ 0 & 0 & 0 \end{pmatrix}$$

dove abbiamo che $rk(A) = 2$, mentre S^1 e S^2 sono una base di $Span(A^1, A^2, A^3)$

- Possiamo ridurre ancora tale matrice, moltiplicando prima A_2 per $-\frac{1}{3}$ per poi sommare $-2A_2$ a A_1 , mantenendo la forma a scala

$$\begin{pmatrix} 1 & 2 & 3 \\ 0 & 1 & 2 \\ 0 & 0 & 0 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 0 & -1 \\ 0 & 1 & 2 \\ 0 & 0 & 0 \end{pmatrix}$$

- Otteniamo quindi che il sistema di partenza è equivalente al seguente:

$$\begin{cases} x - z = 0 \\ y + 2z = 0 \end{cases}$$

- Risolvendo tale sistema in funzione di una variabile ausiliaria t , otteniamo che:

$$\begin{cases} x - z = 0 \\ y + 2z = 0 \end{cases} \implies \begin{cases} x = z \\ y = -2z \end{cases} \implies \begin{cases} x = t \\ y = -2t \\ z = t \end{cases} \implies v = \begin{pmatrix} 1 \\ -2 \\ 1 \end{pmatrix}$$

dunque il vettore v è base di $Ker(L_A)$

9.3 Teorema di Rouché-Capelli

Definition 79. Matrice completa

Dato un sistema di equazioni lineari (dette **equazioni cartesiane**) nella forma

$$\begin{cases} a_{1,1}x_1 + \dots + a_{1,n}x_n = b_1 \\ \vdots \\ a_{m,1}x_1 + \dots + a_{m,n}x_n = b_m \end{cases}$$

individuiamo una **matrice di coefficienti** ed un **vettore delle incognite**:

$$A = \begin{pmatrix} a_{1,1} & \cdots & a_{1,n} \\ \vdots & \ddots & \vdots \\ a_{m,1} & \cdots & a_{m,n} \end{pmatrix} \quad b = \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix}$$

le quali corrispondono fedelmente alla seguente **matrice completa**:

$$A_b = \left(\begin{array}{ccc|c} a_{1,1} & \cdots & a_{1,n} & b_1 \\ \vdots & \ddots & \vdots & \vdots \\ a_{m,1} & \cdots & a_{m,n} & b_m \end{array} \right)$$

Theorem 74. Teorema di Rouché-Capelli

Data una matrice di coefficienti $A \in \text{Mat}_{m \times n}(K)$ e un vettore di coefficienti $b \in K^m$, il sistema $Ax = B$ **ammette soluzioni** se e solo se $\text{rk}(A) = \text{rk}(A_b)$, dove A_b è la matrice completa associata al sistema.

L'**insieme delle soluzioni** (se esistenti) è un **sottospazio affine** di K^n di dimensione $n - \text{rk}(A)$.

Se $n - \text{rk}(A) = 0$, allora esiste un'unica soluzione e il sistema viene detto **determinato**, altrimenti ne esistono infinite ed esso viene detto **indeterminato**.

Dimostrazione:

- Dato il sistema $Ax = b$, si verifica che:

$$\begin{aligned} \exists x \in K^n \mid Ax = b &\iff \exists x_1, \dots, x_n \in K \mid x_1 A^1 + \dots + x_n A^n = b \iff \\ &\iff b \in \text{Span}(A^1, \dots, A^n) \iff \text{Span}(A^1, \dots, A^n) = \text{Span}(A^1, \dots, A^n, b) \iff \\ &\iff \text{rk}(A) = \text{rk}(A_b) \end{aligned}$$

- Inoltre, da ciò deduciamo che $W \subseteq V$ e che $W = V \iff \dim(W) = \dim(V)$
- Verifichiamo ora la seconda parte del teorema: sia V l'insieme di soluzioni del sistema (ipotizzando che ne esista almeno una)

$$V = \{x \in K^n \mid Ax = b\}$$

- Consideriamo quindi il sottospazio $W \subseteq K^n$:

$$W = \{x \in K^n \mid Ax = 0\} = \text{Ker}(L_A)$$

- Considerato $x_0 \in V$, si ha che

$$x \in V \iff Ax = b = Ax_0 \iff A(x - x_0) = 0 \iff x - x_0 \in W \iff x \in x_0 + W$$

dove $x_0 + W$ è una classe laterale sinistra di W , dunque un suo sottospazio affine

Esempi:

1. Consideriamo il seguente sistema lineare:

$$\begin{cases} w + 2x + z = 1 \\ 2w + 4x + y = 3 \\ w + 2x + y - z = 2 \end{cases}$$

- La matrice completa corrispondente sarà:

$$A_b = \left(\begin{array}{cccc|c} 1 & 2 & 0 & 1 & 1 \\ 2 & 4 & 1 & 0 & 3 \\ 1 & 2 & 1 & -1 & 2 \end{array} \right)$$

- Sommiamo $-A_1$ a A_3 e $-2A_1$ a A_2 :

$$A_b = \left(\begin{array}{cccc|c} 1 & 2 & 0 & 1 & 1 \\ 0 & 0 & 1 & -2 & 1 \\ 0 & 0 & 1 & -2 & 1 \end{array} \right)$$

- Sommiamo $-A_2$ a A_3 , ottenendo una matrice a scala, dove $rk(A) = rk(A_b) = 2$

$$\left(\begin{array}{cccc|c} 1 & 2 & 0 & 1 & 1 \\ 0 & 0 & 1 & -2 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{array} \right)$$

- Il sistema di partenza quindi ammette infinite soluzioni ed è equivalente a:

$$\begin{aligned} & \begin{cases} w + 2x + z = 1 \\ y - 2z = 1 \end{cases} \implies \\ & \implies \begin{pmatrix} w \\ x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 1 - 2x - z \\ x \\ 1 + 2z \\ z \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix} + x \begin{pmatrix} -2 \\ 1 \\ 0 \\ 0 \end{pmatrix} + z \begin{pmatrix} -1 \\ 0 \\ 2 \\ 1 \end{pmatrix} \end{aligned}$$

2. Consideriamo il seguente sistema

$$\begin{cases} x + y + z = 1 \\ -x + y + 5z = 0 \\ 2y + 6z = 0 \end{cases}$$

- La matrice completa corrispondente sarà:

$$A_b = \left(\begin{array}{ccc|c} 1 & 1 & 1 & 1 \\ -1 & 1 & 5 & 0 \\ 0 & 2 & 6 & 0 \end{array} \right)$$

- Sommiamo A_1 a A_2 :

$$A_b = \left(\begin{array}{ccc|c} 1 & 1 & 1 & 1 \\ 0 & 2 & 6 & 1 \\ 0 & 2 & 6 & 0 \end{array} \right)$$

- Sommiamo $-A_2$ a A_3 , ottenendo una matrice a scala, dove $rk(A) \neq rk(A_b)$:

$$A_b = \left(\begin{array}{ccc|c} 1 & 1 & 1 & 1 \\ 0 & 2 & 6 & 1 \\ 0 & 0 & 0 & -1 \end{array} \right)$$

- Dunque, il sistema non ammette soluzioni

3. Consideriamo il seguente sistema:

$$\begin{cases} x + ky = 4 - k \\ kx + 4y = 4 \end{cases}$$

- La matrice completa corrispondente sarà:

$$A_b = \left(\begin{array}{cc|c} 1 & k & 4 - k \\ k & 4 & 4 \end{array} \right)$$

- Sommiamo $-kA_1$ a A_2 :

$$A_b = \left(\begin{array}{cc|c} 1 & k & 4 - k \\ 0 & 4 - k^2 & 4 - 2k + k^2 \end{array} \right) = \left(\begin{array}{cc|c} 1 & k & 4 - k \\ 0 & 4 - k^2 & (2 - k)^2 \end{array} \right)$$

- A questo punto, a seconda del valore di k si verificano tre casi:
 - Se $k \neq \pm 2$, allora $4 - k^2 \neq 0$, dunque si ha che $rk(A) = rk(A_b) = 2$, implicando che il sistema ammetta un'unica soluzione, poiché il sottospazio affine generato avrebbe dimensione pari a 0.
 - Se $k = -2$, si ha che $rk(A) \neq rk(A_b)$, dunque il sistema non ammette soluzioni

- Se $k = 2$, si ha che $rk(A) = rk(A_b)$, allora la matrice equivale a

$$A_b = \left(\begin{array}{cc|c} 1 & 2 & 2 \\ 0 & 0 & 0 \end{array} \right) \implies \{x + 2y = 2\} \implies \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 2 \\ 0 \end{pmatrix} + t \begin{pmatrix} -2 \\ 2 \end{pmatrix}$$

dunque $rk(A) = rk(A_b) = 1$, implicando l'esistenza di infinite soluzioni

9.3.1 Equazioni parametriche

Definition 80. Equazioni parametriche

Sia V uno spazio vettoriale e W un suo sottospazio affine, dove $\dim(W) = d$, dunque $\exists x_0 \in V \mid W = x_0 + \text{Giac}(W)$.

Data g_1, \dots, g_d una base di $\text{Giac}(W)$, si verifica che:

$$\forall x \in W \implies \exists! t_1, \dots, t_d \in K \mid x = x_0 + t_1 g_1 + \dots + t_d g_d$$

definiamo l'insieme di tali equazioni come **equazioni parametriche** di W

Dimostrazione:

- Dato $x_0 \in V$ e data g_1, \dots, g_d una base di $\text{Giac}(W)$, si verifica che:

$$\begin{aligned} \forall x \in W &\implies x - x_0 \in \text{Giac}(W) \implies \\ &\implies \exists! t_1, \dots, t_d \in K \mid x - x_0 = t_1 g_1 + \dots + t_d g_d \\ &\implies x = x_0 + t_1 g_1 + \dots + t_d g_d \end{aligned}$$

Proposition 75

Dato uno spazio vettoriale V , un sistema $Ax = b$ e il sottospazio affine W delle soluzioni di quest'ultimo (se esistenti), espresso come l'insieme delle sue equazioni parametriche

$$W = \{x_0 + t_1 v_1 + \dots + t_d v_d \mid t_1, \dots, t_d \in K\}$$

dove $x_0 \in V$ e v_1, \dots, v_d sono base di $\text{Giac}(W)$, si verifica che:

$$x \in W \iff rk(v_1, \dots, v_d, x - x_0) = \dim(W)$$

Dimostrazione:

- Sia

$$W = \{x_0 + t_1 v_1 + \dots + t_d v_d \mid t_1, \dots, t_d \in K\}$$

dove $x_0 \in V$ e v_1, \dots, v_d sono base di $\text{Giac}(W)$, implicando quindi che:

$$\dim(W) = \dim(\text{Giac}(W)) = d$$

- In tal caso, si ha che:

$$\begin{aligned} x \in W &\iff x - x_0 \in \text{Giac}(W) = \text{Span}(v_1, \dots, v_d) \iff \\ &\iff \text{Span}(v_1, \dots, v_d) = \text{Span}(v_1, \dots, v_d, x - x_0) \iff \\ &\iff \text{rk}(v_1, \dots, v_d, x - x_0) = d = \dim(W) \end{aligned}$$

Esempio:

- Consideriamo il seguente insieme di equazioni parametriche corrispondenti ad un sottospazio affine in \mathbb{R}^3

$$V = \left\{ \begin{pmatrix} 1 \\ 0 \\ -1 \end{pmatrix} + t_1 \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} + t_2 \begin{pmatrix} 4 \\ 5 \\ 6 \end{pmatrix} \mid t_1, t_2 \in \mathbb{R} \right\}$$

- Siccome $\dim(V) = 2$, si verifica che

$$\begin{pmatrix} x \\ y \\ z \end{pmatrix} \in V \iff \text{rk} \begin{pmatrix} 1 & 4 & x-1 \\ 2 & 5 & y \\ 3 & 6 & z+1 \end{pmatrix} = 2$$

- Effettuando la riduzione a scala di tale matrice, si ha che:

$$\begin{aligned} \begin{pmatrix} 1 & 4 & x-1 \\ 2 & 5 & y \\ 3 & 6 & z+1 \end{pmatrix} &\xrightarrow{R_2=-2R_1} \begin{pmatrix} 1 & 4 & x-1 \\ 0 & -3 & y-2x+2 \\ 3 & 6 & z+1 \end{pmatrix} \\ &\xrightarrow{R_3=-3R_1} \begin{pmatrix} 1 & 4 & x-1 \\ 0 & -3 & y-2x+2 \\ 0 & -6 & z-3x+4 \end{pmatrix} \xrightarrow{R_3=-2R_2} \begin{pmatrix} 1 & 4 & x-1 \\ 0 & -3 & y-2x+2 \\ 0 & 0 & z+x-2y \end{pmatrix} \end{aligned}$$

- Affinché la riduzione in scala abbia solo 2 pivot, è necessario che l'ultima riga della matrice contenga tutti zeri, implicando quindi che:

$$\text{rk}(A) = 2 \iff z + x - 2y = 0$$

- L'insieme di equazioni parametriche dato, quindi, equivale al seguente sistema di equazioni cartesiane:

$$\{ x - 2y + z = 0$$

corrispondente ad una retta in \mathbb{R}^3

9.4 Matrice di una trasformazione lineare

Theorem 76. Matrice di una trasformazione lineare

Sia $f : V \rightarrow W$ una trasformazione lineare.

Date $\mathcal{B} = v_1, \dots, v_n$ una base di V e $\mathcal{C} = w_1, \dots, w_m$ una base di W e i conseguenti due isomorfismi (sezione 8.2):

$$\varphi_{\mathcal{B}} : K^n \rightarrow V : (t_1, \dots, t_n) \mapsto (t_1 v_1 + \dots + t_n v_n)$$

$$\varphi_{\mathcal{C}} : K^m \rightarrow W : (h_1, \dots, h_m) \mapsto (h_1 w_1 + \dots + h_m w_m)$$

si verifica che:

$$\exists! A \in \text{Mat}_{m \times n}(K) \mid f = \varphi_{\mathcal{C}} \circ L_A \circ \varphi_{\mathcal{B}}^{-1}$$

$$\begin{array}{ccc} V & \xrightarrow{f} & W \\ \varphi_{\mathcal{B}}^{-1} \downarrow & & \uparrow \varphi_{\mathcal{C}} \\ K^n & \xrightarrow{L_A} & K^m \end{array}$$

Definiamo tale matrice A come **la matrice di f nelle basi \mathcal{B} e \mathcal{C}**

Dimostrazione:

- Consideriamo la base canonica di K^n , ossia e_1, \dots, e_n . Si verifica che:

$$\varphi_{\mathcal{B}} : K^n \rightarrow V : e_i \mapsto v_i \implies \varphi_{\mathcal{B}}^{-1} : V \rightarrow K^n : v_i \mapsto e_i$$

e dunque che $\varphi_{\mathcal{B}}^{-1}(v_i) = e_i$

- Notiamo come, in generale, si ha che:

$$L_A(e_i) = A e_i = A \begin{pmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{pmatrix} = \begin{pmatrix} a_{1,i} \\ \vdots \\ a_{m,i} \end{pmatrix} = A^i$$

dove i è la rispettiva posizione contenente 1 dei vari vettori e_i appartenenti alla base canonica

- Infine, notiamo che:

$$\varphi_{\mathcal{C}}(A^i) = a_{1,i} w_1 + \dots + a_{m,i} w_m = w_i$$

e che, per sua costruzione stessa, si ha $f(v_i) = w_i$

- Dunque, concludiamo che:

$$\varphi_C \circ L_A \circ \varphi_{\mathcal{B}^{-1}}(v_i) = \varphi_C \circ L_A(e_i) = \varphi_C(A^i) = w_i \implies$$

$$f = \varphi_C \circ L_A \circ \varphi_{\mathcal{B}^{-1}}$$

Esempi:

- Sia $V = \mathbb{R}[x]_{\leq 4}$, ossia lo spazio vettoriale inerente ai polinomi di grado minore o uguale a 4 con coefficienti in \mathbb{R} .
 - La base di V corrisponde a: $\mathcal{B} : 1, x, x^2, x^3, x^4$, dunque si ha che $\dim(V) = 5$
 - Sia inoltre $W = \mathbb{R}[x]_{\leq 3}$, la cui base è $\mathcal{C} : 1, x, x^2, x^3$, dunque $\dim(W) = 4$
 - Sia $f' : V \rightarrow W : p(x) \mapsto p'(x)$ la trasformazione lineare corrispondente alla derivata di un polinomio
 - La matrice di f' nelle basi \mathcal{B} e \mathcal{C} corrisponde a:

$$\begin{cases} f'(x^4) = 4x^3 \\ f'(x^3) = 3x^2 \\ f'(x^2) = 2x \\ f'(x) = 1 \\ f'(1) = 0 \end{cases} \implies \begin{pmatrix} 4 & 0 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

- Dati ancora $V = \mathbb{R}[x]_{\leq 4}$ e $W = \mathbb{R}[x]_{\leq 3}$, consideriamo invece la trasformazione lineare $\Delta : V \rightarrow W : p(x) \mapsto p(x+1) - p(x)$, corrispondente all'operatore differenza (anche detta "derivata discreta")
 - La matrice di Δ nelle basi \mathcal{B} e \mathcal{C} corrisponde a:

$$\begin{cases} \Delta(x^4) = (x+1)^4 - x^4 = 4x^3 + 6x^2 + 4x + 1 \\ \Delta(x^3) = (x+1)^3 - x^3 = 3x^2 + 3x + 1 \\ \Delta(x^2) = (x+1)^2 - x^2 = 2x + 1 \\ \Delta(x) = (x+1) - x^0 = 1 \\ \Delta(1) = (x+1)^0 - x^0 = 0 \end{cases} \implies \begin{pmatrix} 4 & 0 & 0 & 0 & 0 \\ 6 & 3 & 0 & 0 & 0 \\ 4 & 3 & 2 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 \end{pmatrix}$$

- Siano $V = W = \mathbb{R}^2$ e sia:

$$f : \mathbb{R}^2 \rightarrow \mathbb{R}^2 : \begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} 1 & 3 \\ 2 & 4 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x + 3y \\ 2x + 4y \end{pmatrix}$$

- Siano

$$\mathcal{B} = \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ -1 \end{pmatrix} \quad \mathcal{C} = \begin{pmatrix} 1 \\ 3 \end{pmatrix}, \begin{pmatrix} -2 \\ 1 \end{pmatrix}$$

rispettivamente la base di $V = \mathbb{R}^2$ e di $W = \mathbb{R}^2$

- Consideriamo quindi la matrice A di f nelle basi \mathcal{B} e \mathcal{C}

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

- Poiché

$$f \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \cdot 1 + 3 \cdot 1 \\ 2 \cdot 1 + 4 \cdot 1 \end{pmatrix} = \begin{pmatrix} 4 \\ 6 \end{pmatrix}$$

e poiché la prima colonna di A è determinata dalle coordinate di $f \begin{pmatrix} 1 \\ 1 \end{pmatrix}$ nella base \mathcal{C} , ne segue che sia necessario risolvere il seguente sistema affinché si possa ottenere il valore di a e c :

$$a \begin{pmatrix} 1 \\ 1 \end{pmatrix} + c \begin{pmatrix} -2 \\ 1 \end{pmatrix} = \begin{pmatrix} 4 \\ 6 \end{pmatrix} \implies \begin{cases} a - 2c = 4 \\ 3a + 4c = 6 \end{cases} \implies \left(\begin{array}{cc|c} 1 & -2 & 4 \\ 3 & 4 & 6 \end{array} \right)$$

- Tramite la riduzione a scala, troviamo che:

$$\begin{aligned} \left(\begin{array}{cc|c} 1 & -2 & 4 \\ 3 & 4 & 6 \end{array} \right) &\xrightarrow{R_2+=-3R_1} \left(\begin{array}{cc|c} 1 & -2 & 4 \\ 0 & 10 & -6 \end{array} \right) \xrightarrow{R_2*=\frac{1}{10}} \left(\begin{array}{cc|c} 1 & -2 & 4 \\ 0 & 1 & -\frac{3}{5} \end{array} \right) \\ &\xrightarrow{R_1+=-2R_2} \left(\begin{array}{cc|c} 1 & 0 & \frac{14}{5} \\ 0 & 1 & -\frac{3}{5} \end{array} \right) \implies \begin{cases} a = \frac{14}{5} \\ c = -\frac{3}{5} \end{cases} \end{aligned}$$

- Analogamente, otteniamo il valore di b e d risolvendo il seguente sistema:

$$\begin{aligned} b \begin{pmatrix} 1 \\ 1 \end{pmatrix} + d \begin{pmatrix} -2 \\ 1 \end{pmatrix} &= f \begin{pmatrix} 1 \\ -1 \end{pmatrix} \implies b \begin{pmatrix} 1 \\ 1 \end{pmatrix} + d \begin{pmatrix} -2 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 + 3(-1) \\ 2 + 4(-1) \end{pmatrix} \implies \\ \implies b \begin{pmatrix} 1 \\ 1 \end{pmatrix} + d \begin{pmatrix} -2 \\ 1 \end{pmatrix} &= \begin{pmatrix} -2 \\ -2 \end{pmatrix} \implies \begin{cases} b - 2d = -2 \\ 3b + 4d = -2 \end{cases} \implies \left(\begin{array}{cc|c} 1 & -2 & -2 \\ 3 & 4 & -2 \end{array} \right) \end{aligned}$$

- Riducendo a scala, otteniamo che:

$$\begin{aligned} \left(\begin{array}{cc|c} 1 & -2 & -2 \\ 3 & 4 & -2 \end{array} \right) &\xrightarrow{R_2+=-3R_1} \left(\begin{array}{cc|c} 1 & -2 & -2 \\ 0 & 10 & 4 \end{array} \right) \xrightarrow{R_2*=\frac{1}{10}} \left(\begin{array}{cc|c} 1 & -2 & -2 \\ 0 & 1 & \frac{2}{5} \end{array} \right) \\ &\xrightarrow{R_1+=-2R_2} \left(\begin{array}{cc|c} 1 & 0 & -\frac{6}{5} \\ 0 & 1 & \frac{2}{5} \end{array} \right) \implies \begin{cases} b = -\frac{6}{5} \\ d = \frac{2}{5} \end{cases} \end{aligned}$$

- Quindi, concludiamo la matrice di f nelle basi \mathcal{B} e \mathcal{C} sia:

$$A = \begin{pmatrix} \frac{14}{5} & -\frac{6}{5} \\ -\frac{3}{5} & \frac{2}{5} \end{pmatrix}$$

9.5 Determinante di una matrice

Definition 81. Trasformazione multilineare

Una trasformazione lineare del tipo

$$f : V_1 \times \dots \times V_k \rightarrow W : (v_1, \dots, v_k) \rightarrow f(v_1, \dots, v_k)$$

viene detta **multilineare** se $\forall i \in [1, k]$ dati $\lambda, \mu \in K$ si verifica che:

$$f(v_1, \dots, \lambda v'_i + \mu v''_i, \dots, v_n) = \lambda f(v_1, \dots, v'_i, \dots, v_n) + \mu f(v_1, \dots, v''_i, \dots, v_n)$$

Corollary 30

Ricordando che

$$\underbrace{K^n \times \dots \times K^n}_{n \text{ volte}} = Mat_{n \times n}(K) = A^1, \dots, A^n = A_1, \dots, A_n$$

è facilmente intuibile una naturale correlazione tra una trasformazione multilineare ed una matrice

Definition 82. Determinante di una matrice

Definiamo come **determinante** di una matrice l'unica trasformazione lineare $det : Mat_{n \times n}(K) \rightarrow K$ che verifica le seguenti tre proprietà:

1. det è multilineare su righe e colonne della matrice
2. A_1, \dots, A_n e A^1, \dots, A^n sono una base di $A \in Mat_{n \times n}(K)$ se e solo se $det(A) \neq 0$
3. $det(I_n) = 1$, dove I_n è la matrice identità di ordine n

Observation 59

Per la proprietà 2), se una matrice $A \in Mat_{n \times n}(K)$ contiene due righe (o colonne) uguali, allora A_1, \dots, A_n (o A^1, \dots, A^n) non sono linearmente indipendenti e di conseguenza neanche una base di A , implicando quindi che $det(A) = 0$

Proposition 77. Determinante alternante su righe e colonne

Data una matrice $A = (A_1, \dots, A_i, \dots, A_j, \dots, A_n) \in Mat_{n \times n}(K)$, si verifica che:

$$det(A_1, \dots, A_i, \dots, A_j, \dots, A_n) = -det(A_1, \dots, A_j, \dots, A_i, \dots, A_n)$$

dunque, scambiando due righe (o colonne) della matrice il determinante cambia segno

Dimostrazione:

- Supponiamo che $1 \neq -1$ nel campo K (escludendo quindi campi come Z_2)
- Data una matrice $A = (A_1, \dots, A_i + A_j, \dots, A_i + A_j, \dots, A_n)$, per la proprietà 2) del determinante si ha che:

$$\det(A_1, \dots, A_i + A_j, \dots, A_i + A_j, \dots, A_n) = 0$$

- Per multilinearità del determinante, si ha che:

$$\begin{aligned} 0 &= \det(A_1, \dots, A_i + A_j, \dots, A_i + A_j, \dots, A_n) \implies \\ \implies 0 &= \det(A_1, \dots, A_i, \dots, A_i + A_j, \dots, A_n) + \det(A_1, \dots, A_j, \dots, A_i + A_j, \dots, A_n) \implies \\ \implies 0 &= \det(A_1, \dots, A_i, \dots, A_i, \dots, A_n) + \det(A_1, \dots, A_i, \dots, A_j, \dots, A_n) + \\ &\quad + \det(A_1, \dots, A_j, \dots, A_i, \dots, A_n) + \det(A_1, \dots, A_j, \dots, A_j, \dots, A_n) \implies \\ \implies 0 &= 0 + \det(A_1, \dots, A_i, \dots, A_j, \dots, A_n) + \det(A_1, \dots, A_j, \dots, A_i, \dots, A_n) + 0 \implies \\ \implies \det(A_1, \dots, A_i, \dots, A_j, \dots, A_n) &= -\det(A_1, \dots, A_j, \dots, A_i, \dots, A_n) \end{aligned}$$

Theorem 78. Formula di Binet

Date due matrici $A, B \in Mat_{n \times n}$, si ha che:

$$\det(AB) = \det(A) \cdot \det(B)$$

(*dimostrazione omessa*)

9.5.1 Formula di Leibniz e Regola di Sarrus

Definition 83. Formula di Leibniz

Tramite le sue proprietà 1), 3) e la sua alternanza su righe e colonne, il determinante di una matrice $A \in Mat_{n \times n}(K)$ può essere definito come:

$$\det(A) := \sum_{\sigma \in S_n} \text{sgn}(\sigma) \cdot a_{1,\sigma(1)} \cdot \dots \cdot a_{n,\sigma(n)}$$

Corollary 31

Se $A \in Mat_{2 \times 2}(K)$, allora

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \implies \det(A) = ad - bc$$

Dimostrazione:

- Sia

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} := \begin{pmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{pmatrix}$$

- Dato $S_2 = \{(1)(2), (12)\}$, si verifica che:

$$\det(A) = \sum_{\sigma \in S_2} \operatorname{sgn}(\sigma) \cdot a_{1,\sigma(1)} \cdot a_{2,\sigma(2)} = a_{1,1}a_{2,2} - a_{1,2}a_{2,1} = ad - bc$$

Corollary 32

Se $A \in \operatorname{Mat}_{3 \times 3}(K)$, allora

$$A = \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix} \implies \det(A) = aei + bfg + cdh - afh - bdi - ceg$$

Dimostrazione:

- Sia

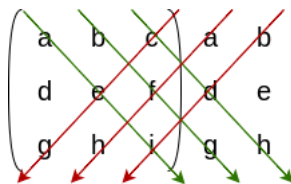
$$A = \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix} := \begin{pmatrix} a_{1,1} & a_{1,2} & a_{1,3} \\ a_{2,1} & a_{2,2} & a_{2,3} \\ a_{3,1} & a_{3,2} & a_{3,3} \end{pmatrix}$$

- Dato $S_3 = \{(1)(2)(3), (12)(3), (13)(2), (23)(1), (123), (321)\}$, si verifica che:

$$\begin{aligned} \det(A) &= \sum_{\sigma \in S_3} \operatorname{sgn}(\sigma) \cdot a_{1,\sigma(1)} \cdot a_{2,\sigma(2)} \cdot a_{3,\sigma(3)} = \\ &= a_{1,1}a_{2,2}a_{3,3} - a_{1,2}a_{2,1}a_{3,3} - a_{1,1}a_{2,3}a_{3,2} - a_{1,3}a_{2,2}a_{3,1} + a_{1,2}a_{2,3}a_{3,1} + a_{1,3}a_{2,1}a_{3,2} = \\ &= aei - bdi - ceg - afh + bfg + cdh \end{aligned}$$

Method 5. Regola di Sarrus

La **Regola di Sarrus** permette ricordare facilmente il calcolo del determinante di una matrice quadrata di ordine 3, ricopiando a destra della matrice le sue prime due colonne, per poi **sommare le tre diagonal** e **sottrarre le tre anti-diagonal**:



$$A \in \operatorname{Mat}_{3 \times 3}(K) \implies \det(A) = aei + bfg + cdh - afh - bdi - ceg$$

Esempio:

- Data la matrice

$$A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$$

si ha che:

$$\det(A) = 1 \cdot 4 - 2 \cdot 3 = -2$$

- Data la matrice

$$B = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 0 \end{pmatrix}$$

si ha che:

$$\det(B) = 1 \cdot 5 \cdot 0 + 2 \cdot 6 \cdot 7 + 3 \cdot 4 \cdot 8 - 2 \cdot 4 \cdot 0 - 3 \cdot 5 \cdot 7 - 1 \cdot 6 \cdot 8 = 27$$

Observation 60

Data una matrice $A \in \text{Mat}_{n \times n}(K)$, se esiste almeno una riga A_i o colonna A^j contenente tutti zeri, allora $\det(A) = 0$

9.5.2 Determinante tramite riduzione a scala**Definition 84. Matrice triangolare**

Sia $A \in \text{Mat}_{n \times n}(K)$. Tale matrice viene detta **triangolare superiore** se $\forall i > j$ si ha che $a_{i,j} = 0$, ossia se sotto la diagonale principale vi sono tutti zeri

$$A = \begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & \cdots & a_{1,n} \\ 0 & a_{2,2} & a_{2,3} & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & 0 & a_{n-1,n-1} & a_{n-1,n} \\ 0 & \cdots & \cdots & 0 & a_{n,n} \end{pmatrix}$$

o **triangolare inferiore** se $\forall i < j$ si ha che $a_{i,j} = 0$, ossia se sopra la diagonale principale vi sono tutti zeri

$$A = \begin{pmatrix} a_{1,1} & 0 & \cdots & \cdots & 0 \\ a_{1,2} & a_{2,2} & 0 & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & a_{n-1,n-2} & a_{n-1,n-1} & 0 \\ a_{n,1} & \cdots & \cdots & a_{n,n-1} & a_{n,n} \end{pmatrix}$$

Observation 61

Se $T \in Mat_{n \times n}(K)$ è una matrice triangolare, allora il suo determinante corrisponde al **prodotto della sua diagonale**

$$\det(T) = a_{1,1} \cdot a_{2,2} \cdot \dots \cdot a_{n,n}$$

Nel caso in cui vi sia uno zero sulla diagonale di T , ne segue naturalmente che $\det(T) = 0$

Observation 62

Una matrice ridotta a scala è sempre triangolare.

Method 6. Calcolo del determinante tramite riduzione a scala

Data una matrice $A \in Mat_{n \times n}(K)$, è possibile ricavare il suo determinante tramite la sua riduzione a scala, poiché:

1. Scambiare due righe (o colonne) **inverte il segno del determinante**
2. Moltiplicare una riga (o colonna) per uno scalare $\lambda \in K^*$ **moltiplica anche il determinante** per tale scalare
3. Sommare ad una riga (o colonna) un multiplo di un'altra riga (o colonna) **non altera il determinante**

Dunque, data la riduzione a scala S di A , è possibile calcolare $\det(A)$ tramite il calcolo di $\det(S)$, per poi invertire gli effetti subiti dal determinante in base alle operazioni svolte durante la riduzione.

Dimostrazione degli effetti della riduzione:

- Sia $A = (A_1, \dots, A_i, \dots, A_j, \dots, A_n) \in Mat_{n \times n}(K)$
- Abbiamo già dimostrato come scambiare due righe o colonne implichi che il determinante cambi segno, dunque

$$\det(A_1, \dots, A_i, \dots, A_j, \dots, A_n) = -\det(A_1, \dots, A_j, \dots, A_i, \dots, A_n)$$

- Data $A' = (A_1, \dots, \lambda A_i, \dots, A_j, \dots, A_n) \in Mat_{n \times n}(K)$, per multilinearità del determinante si ha che:

$$\det(A') \det(A_1, \dots, \lambda A_i, \dots, A_j, \dots, A_n) = \lambda \cdot \det(A_1, \dots, A_i, \dots, A_j, \dots, A_n) = \lambda \cdot \det(A)$$

- Data $A'' = (A_1, \dots, A_i + \mu A_j, \dots, A_j, \dots, A_n) \in Mat_{n \times n}(K)$, per multilinearità del determinante si ha che:

$$\begin{aligned} \det(A'') &= \det(A_1, \dots, A_i + \mu A_j, \dots, A_j, \dots, A_n) = \\ &= \det(A_1, \dots, A_i, \dots, A_j, \dots, A_n) + \mu \cdot \det(A_1, \dots, A_j, \dots, A_j, \dots, A_n) = \\ &= \det(A_1, \dots, A_i, \dots, A_j, \dots, A_n) + \mu \cdot 0 = \det(A_1, \dots, A_i, \dots, A_j, \dots, A_n) = \det(A) \end{aligned}$$

Esempio:

- Riprendiamo la matrice dell'esempio precedente, il cui determinante sappiamo già essere 27:

$$B = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 0 \end{pmatrix}$$

- Effettuiamo la riduzione a scala di tale matrice:

$$\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 0 \end{pmatrix} \xrightarrow{R_2 += -4R_1} \begin{pmatrix} 1 & 2 & 3 \\ 0 & -3 & -6 \\ 7 & 8 & 0 \end{pmatrix} \xrightarrow{R_3 += -7R_1} \begin{pmatrix} 1 & 2 & 3 \\ 0 & -3 & -6 \\ 0 & -6 & -21 \end{pmatrix}$$

$$\xrightarrow{R_2 * = \frac{1}{3}} \begin{pmatrix} 1 & 2 & 3 \\ 0 & 1 & 2 \\ 0 & -6 & -21 \end{pmatrix} \xrightarrow{R_3 += -6R_2} \begin{pmatrix} 1 & 2 & 3 \\ 0 & 1 & 2 \\ 0 & 0 & -9 \end{pmatrix} \implies \det(S) = -9$$

- Tra i vari passaggi effettuati durante la riduzione a scala, l'unico ad influenzare il determinante è la terza. Dunque, si ha che:

$$\det(S) = -\frac{1}{3} \cdot \det(A) \implies -9 = -\frac{1}{3} \cdot \det(A) \implies \det(A) = 27$$

9.5.3 Sviluppo di Laplace**Definition 85. Sottomatrice**

Data una matrice $A \in \text{Mat}_{m \times n}(K)$, definiamo come **sottomatrice di A** una matrice ottenuta cancellando un determinato numero di righe e/o colonne dalla matrice originale

Definition 86. Minore di una matrice

Data una matrice $A \in \text{Mat}_{n \times n}(K)$, definiamo come **minori di A** tutte le sottomatrici quadrate ottenute da A .

Denotiamo come $M_{i,j}$ il minore ottenuto cancellando la riga i e la colonna j dalla matrice A .

Theorem 79. Sviluppo di Laplace

Data una matrice $A \in Mat_{n \times n}(K)$, lo **sviluppo di Laplace sulla i -esima riga di A** è definito come:

$$\det(A) = \sum_{k=1}^n (-1)^{i+k} \cdot a_{i,k} \cdot \det(M_{i,k}) = \sum_{k=1}^n a_{i,k} \cdot \text{cof}_{i,k}(A)$$

dove $\text{cof}_{i,k}(A) = (-1)^{i+k} \cdot \det(M_{i,k})$ viene detto il **cofattore (o complemento algebrico)** dell'entrata $a_{i,k}$.

Analogamente, lo sviluppo di Laplace sulla j -esima colonna di A è definito come:

$$\det(A) = \sum_{h=1}^n (-1)^{h+j} \cdot a_{h,j} \cdot \det(M_{h,j}) = \sum_{h=1}^n a_{h,j} \cdot \text{cof}_{h,j}(A)$$

Lo sviluppo di Laplace è conveniente nel caso in cui si debba calcolare il determinante di una matrice di ordine 4+ o avente una riga o colonna contenente molti zeri.

(*dimostrazione omessa*)

Esempi:

1. • Riprendiamo la matrice già vista in vari esempi precedenti, il cui determinante sappiamo già essere 27:

$$B = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 0 \end{pmatrix}$$

- Effettuiamo lo sviluppo di Laplace su A_3 :

$$\begin{aligned} \det(B) &= (-1)^{3+1} \cdot 7 \cdot \det \begin{pmatrix} 2 & 3 \\ 5 & 6 \end{pmatrix} + (-1)^{3+2} \cdot 8 \cdot \det \begin{pmatrix} 1 & 3 \\ 4 & 6 \end{pmatrix} + (-1)^{3+3} \cdot 0 \cdot \det \begin{pmatrix} 1 & 2 \\ 4 & 5 \end{pmatrix} = \\ &= 7(2 \cdot 6 - 3 \cdot 5) - 8(1 \cdot 6 - 3 \cdot 4) + 0 = -21 + 48 = 27 \end{aligned}$$

2. • Calcoliamo il determinante della seguente matrice quadrata di ordine 4:

$$A = \begin{pmatrix} 1 & 4 & 0 & -1 \\ 2 & 3 & 5 & 4 \\ 7 & 8 & 0 & -2 \\ 0 & 1 & 0 & 6 \end{pmatrix}$$

- Effettuiamo lo sviluppo di Laplace su A^3 :

$$\det(A) = 0 + (-1)^{2+3} \cdot 5 \cdot \det \begin{pmatrix} 1 & 4 & -1 \\ 7 & 8 & -2 \\ 0 & 1 & 6 \end{pmatrix} + 0 - 0 = -5 \cdot \det \begin{pmatrix} 1 & 4 & -1 \\ 7 & 8 & -2 \\ 0 & 1 & 6 \end{pmatrix}$$

- Il calcolo di $\det(A)$ viene quindi ridotto al calcolo di $\det(M_{2,3})$, il quale può essere facilmente calcolato tramite la regola di Sarrus o tramite un nuovo sviluppo di Laplace
- Utilizzando la regola di Sarrus, abbiamo che:

$$\det(A) = -5 \cdot \det \begin{pmatrix} 1 & 4 & -1 \\ 7 & 8 & -2 \\ 0 & 1 & 6 \end{pmatrix} = -5(48 + 0 + (-7) - 168 - 0 - (-2)) = 625$$

- Utilizzando lo sviluppo di Laplace su $(M_{2,3})^1$, invece, abbiamo che:

$$\begin{aligned} \det(A) = -5 \cdot \det \begin{pmatrix} 1 & 4 & -1 \\ 7 & 8 & -2 \\ 0 & 1 & 6 \end{pmatrix} &= -5 \left[(-1)^{1+1} \cdot 1 \cdot \det \begin{pmatrix} 8 & -2 \\ 1 & 6 \end{pmatrix} + \right. \\ &\quad \left. + (-1)^{2+1} \cdot 7 \cdot \det \begin{pmatrix} 4 & -1 \\ 1 & 6 \end{pmatrix} \right] = -5[50 - 175] = 625 \end{aligned}$$

9.5.4 Regola di Cramer

Theorem 80. Regola di Cramer

Dato un sistema lineare $Ax = b$:

$$\begin{cases} a_{1,1}x_1 + \dots + a_{1,n}x_n = b_1 \\ \vdots \\ a_{m,1}x_1 + \dots + a_{m,n}x_n = b_m \end{cases}$$

dove A è una matrice di coefficienti tale che $\det(A) \neq 0$, allora il sistema ammette la seguente unica soluzione:

$$\begin{cases} x_1 = \frac{\det(b, A^2, \dots, A^{n-1}, A^n)}{\det(A)} \\ x_2 = \frac{\det(A^1, b, \dots, A^{n-1}, A^n)}{\det(A)} \\ \vdots \\ x_n = \frac{\det(A^1, A^2, \dots, b, A^n)}{\det(A)} \\ x_n = \frac{\det(A^1, A^2, \dots, A^{n-1}, b)}{\det(A)} \end{cases}$$

Esempio:

- Consideriamo il sistema

$$\begin{cases} x + 2y + 3z = 1 \\ 4x + 5y + 6z = 0 \\ 7x + 8y = 0 \end{cases}$$

la cui matrice dei coefficienti corrisponde è

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 0 \end{pmatrix}$$

dove $\det(A) = 27$

- Per la regola di Cramer, si ha che:

$$\begin{cases} x = \frac{1}{27} \cdot \det \begin{pmatrix} 1 & 2 & 3 \\ 0 & 5 & 6 \\ 0 & 8 & 0 \end{pmatrix} \\ y = \frac{1}{27} \cdot \det \begin{pmatrix} 1 & 1 & 3 \\ 4 & 0 & 6 \\ 7 & 0 & 0 \end{pmatrix} \\ z = \frac{1}{27} \cdot \det \begin{pmatrix} 1 & 2 & 1 \\ 4 & 5 & 0 \\ 7 & 8 & 0 \end{pmatrix} \end{cases} \implies \begin{cases} x = \frac{1}{27} \cdot (-48) = -\frac{16}{9} \\ y = \frac{1}{27} \cdot (42) = \frac{14}{9} \\ z = \frac{1}{27} \cdot (-3) = -\frac{1}{9} \end{cases}$$

9.6 Inversa di una matrice

Theorem 81. Inversione di una matrice

Una matrice $A \in \text{Mat}_{n \times n}(K)$ è invertibile solo se $\exists! A^{-1} \in \text{Mat}_{n \times n}(K) \mid A \cdot A^{-1} = A^{-1} \cdot A = I_n$.

Le seguenti condizioni sono equivalenti tra loro:

1. A è invertibile
2. $\text{rk}(A) = n$
3. A_1, \dots, A_n sono una base di K^n
4. A^1, \dots, A^n sono una base di K^n
5. $\det(A) \neq 0$

Dimostrazione:

- 1) \iff 2)
 - Supponiamo che $\exists! B \in \text{Mat}_{n \times n}(K) \mid A \cdot B = B \cdot A = I_n$
 - Sia $B = (B^1, \dots, B^n)$. Allora, ne segue che $AB = (A \cdot B^1, \dots, A \cdot B^n)$

– Dunque, si ha che:

$$\begin{aligned} AB = I_n &\iff AB^1 = e_1, AB^2 = e_2, \dots, AB^n = e_n \iff \\ &\iff L_A(B^1) = e_1, L_A(B^2) = e_2, \dots, L_A(B^n) = e_n \iff e_1, e_2, \dots, e_n \in \text{Im}(L_A) \iff \\ &\iff \text{Im}(L_A) = \text{Span}(e_1, \dots, e_n) = K^n \iff \text{rk}(A) = n \end{aligned}$$

• 2) \iff 3), 4)

– Supponendo che $\text{rk}(A) = n$, allora

$$\begin{aligned} \text{rk}(A) = n &\iff \dim(\text{Span}(A^1, \dots, A^n)) = \dim(\text{Span}(A_1, \dots, A_n)) \iff \\ &\iff \text{Span}(A^1, \dots, A^n) = K^n \iff \begin{cases} A^1, \dots, A^n \text{ sono base di } K^n \\ A_1, \dots, A_n \text{ sono base di } K^n \end{cases} \end{aligned}$$

• 3), 4) \iff 5)

– Per definizione stessa di determinante, si ha che A^1, \dots, A^n e A_1, \dots, A_n sono base di K^n se e solo se $\det(A) \neq 0$

Method 7. Inversione tramite algoritmo di Gauss-Jordan

Se $A \in \text{Mat}_{n \times n}(K)$ è invertibile e $(A \mid I_n)$ e $(I_n \mid B)$ sono equivalenti per righe, allora $B = A^{-1}$

Esempi:

1. • Sia

$$A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$$

dove $\det(A) = -2$, dunque A è invertibile

• Procedendo con l'algoritmo di Gauss-Jordan, si ha che:

$$\begin{aligned} (A \mid I_n) &= \left(\begin{array}{cc|cc} 1 & 2 & 1 & 0 \\ 3 & 4 & 0 & 1 \end{array} \right) \xrightarrow{R_2 += -3R_1} \left(\begin{array}{cc|cc} 1 & 2 & 1 & 0 \\ 0 & -2 & -3 & 1 \end{array} \right) \\ &\xrightarrow{R_1 += R_2} \left(\begin{array}{cc|cc} 1 & 0 & -2 & 1 \\ 0 & -2 & -3 & 1 \end{array} \right) \xrightarrow{R_2 * = -\frac{1}{2}} \left(\begin{array}{cc|cc} 1 & 0 & -2 & 1 \\ 0 & 1 & \frac{3}{2} & -\frac{1}{2} \end{array} \right) = (I_n \mid B) \\ &\implies A^{-1} = \begin{pmatrix} -2 & 1 \\ \frac{3}{2} & -\frac{1}{2} \end{pmatrix} \end{aligned}$$

dove $\det(A^{-1}) = -\frac{1}{2}$

2. • Sia

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 0 \end{pmatrix}$$

dove $\det(A) = 27$, dunque A è invertibile

- Procedendo con l'algoritmo di Gauss-Jordan, si ha che:

$$\begin{aligned}
(A \mid I_N) &= \left(\begin{array}{ccc|ccc} 1 & 2 & 3 & 1 & 0 & 0 \\ 4 & 5 & 6 & 0 & 1 & 0 \\ 7 & 8 & 0 & 0 & 0 & 1 \end{array} \right) \xrightarrow{R_2+=-4R_1} \left(\begin{array}{ccc|ccc} 1 & 2 & 3 & 1 & 0 & 0 \\ 0 & -3 & -6 & -4 & 1 & 0 \\ 7 & 8 & 0 & 0 & 0 & 1 \end{array} \right) \\
&\xrightarrow{R_3+=-7R_1} \left(\begin{array}{ccc|ccc} 1 & 2 & 3 & 1 & 0 & 0 \\ 0 & -3 & -6 & -4 & 1 & 0 \\ 0 & -6 & -21 & -7 & 0 & 1 \end{array} \right) \xrightarrow{R_3+=-2R_2} \left(\begin{array}{ccc|ccc} 1 & 2 & 3 & 1 & 0 & 0 \\ 0 & -3 & -6 & -4 & 1 & 0 \\ 0 & 0 & -9 & 1 & -2 & 1 \end{array} \right) \\
&\xrightarrow{R_2*=-\frac{1}{3}} \left(\begin{array}{ccc|ccc} 1 & 2 & 3 & 1 & 0 & 0 \\ 0 & 1 & 2 & \frac{4}{3} & -\frac{1}{3} & 0 \\ 0 & 0 & -9 & 1 & -2 & 1 \end{array} \right) \xrightarrow{R_3*=-\frac{1}{9}} \left(\begin{array}{ccc|ccc} 1 & 2 & 3 & 1 & 0 & 0 \\ 0 & 1 & 2 & \frac{4}{3} & -\frac{1}{3} & 0 \\ 0 & 0 & 1 & -\frac{1}{9} & \frac{2}{9} & -\frac{1}{9} \end{array} \right) \\
&\xrightarrow{R_1+=-2R_2} \left(\begin{array}{ccc|ccc} 1 & 0 & -1 & -\frac{5}{3} & \frac{2}{3} & 0 \\ 0 & 1 & 2 & \frac{4}{3} & -\frac{1}{3} & 0 \\ 0 & 0 & 1 & -\frac{1}{9} & \frac{2}{9} & -\frac{1}{9} \end{array} \right) \xrightarrow{R_1+=R_3} \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & -\frac{16}{9} & \frac{8}{9} & -\frac{1}{9} \\ 0 & 1 & 2 & \frac{4}{3} & -\frac{1}{3} & 0 \\ 0 & 0 & 1 & -\frac{1}{9} & \frac{2}{9} & -\frac{1}{9} \end{array} \right) \\
&\xrightarrow{R_2+=-2R_3} \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & -\frac{16}{9} & \frac{8}{9} & -\frac{1}{9} \\ 0 & 1 & 0 & \frac{14}{9} & -\frac{7}{9} & \frac{2}{9} \\ 0 & 0 & 1 & -\frac{1}{9} & \frac{2}{9} & -\frac{1}{9} \end{array} \right) \Rightarrow A^{-1} = \left(\begin{array}{ccc} -\frac{16}{9} & \frac{8}{9} & -\frac{1}{9} \\ \frac{14}{9} & -\frac{7}{9} & \frac{2}{9} \\ -\frac{1}{9} & \frac{2}{9} & -\frac{1}{9} \end{array} \right) \Rightarrow \\
&\Rightarrow A^{-1} = \frac{1}{9} \begin{pmatrix} -16 & 8 & -1 \\ 14 & -7 & 2 \\ -1 & 2 & -1 \end{pmatrix}
\end{aligned}$$

dove $\det(A^{-1}) = \frac{1}{27}$

Corollary 33

Data una matrice $A \in \text{Mat}_{n \times n}(K)$, si ha che:

$$\det(A^{-1}) = \det(A)^{-1}$$

Dimostrazione:

- Per la formula di Binet, si ha che:

$$1 = \det(I_n) = \det(A \cdot A^{-1}) = \det(A)\det(A^{-1}) \Rightarrow \det(A)^{-1} = \det(A^{-1})$$

Definition 87. Matrice trasposta

Data una matrice $A \in \text{Mat}_{m \times n}(K)$, definiamo come **matrice trasposta** la matrice $A^T \in \text{Mat}_{n \times m}(K)$ avente come i -esima riga la i -esima colonna della matrice A e come j -esima colonna la j -esima colonna di A

$$A = \begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ a_{2,1} & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \vdots \\ a_{m,1} & \cdots & \cdots & a_{m,n} \end{pmatrix} \Rightarrow A^T = \begin{pmatrix} a_{1,1} & a_{2,1} & \cdots & a_{m,1} \\ a_{1,2} & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \vdots \\ a_{1,n} & \cdots & \cdots & a_{m,n} \end{pmatrix}$$

Esempio:

- Data la seguente matrice A , la sua trasposta corrisponde a:

$$A = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 \\ 9 & 10 & 11 & 12 \end{pmatrix} \Rightarrow A^T = \begin{pmatrix} 1 & 5 & 9 \\ 2 & 6 & 10 \\ 3 & 7 & 11 \\ 4 & 8 & 12 \end{pmatrix}$$

Observation 63

Date due matrici $A, B \in \text{Mat}_{n \times n}(K)$, si verifica che:

- $\det(A) = \det(A^T)$
- $(AB)^T = B^T A^T$

(dimostrazione omessa)

Definition 88. Matrice dei cofattori

Data una matrice $A \in \text{Mat}_{n \times n}(K)$, definiamo come **matrice dei cofattori** la matrice $A^* \in \text{Mat}_{n \times n}(K)$ avente come entrate i cofattori di ogni entrata della matrice A

$$A = \begin{pmatrix} a_{1,1} & \cdots & a_{1,n} \\ \vdots & \ddots & \vdots \\ a_{n,1} & \cdots & a_{n,n} \end{pmatrix} \Rightarrow A^* = \begin{pmatrix} \text{cof}(A)_{1,1} & \cdots & \text{cof}(A)_{1,n} \\ \vdots & \ddots & \vdots \\ \text{cof}(A)_{n,1} & \cdots & \text{cof}(A)_{n,n} \end{pmatrix}$$

dove ricordiamo che

$$\text{cof}(A)_{i,j} = (-1)^{i+j} \cdot \det(M_{i,j})$$

Definition 89. Matrice aggiunta

Data una matrice $A \in Mat_{n \times n}(K)$, definiamo come **matrice aggiunta** la trasposta della matrice dei cofattori di A :

$$adj(A) = (A^*)^T$$

Theorem 82. Inversa di una matrice tramite aggiunta

Data una matrice $A \in Mat_{n \times n}(K)$ dove $\det(A) \neq 0$, si verifica che:

$$A^{-1} = \frac{1}{\det(A)} \cdot adj(A)$$

Dimostrazione:

- Come conseguenza dello sviluppo di Laplace, si verifica che:

$$A \cdot adj(A) = adj(A) \cdot A = \det(A) \cdot I_n$$

- Dunque, concludiamo facilmente che:

$$\det(A)^{-1} \cdot A \cdot adj(A) = I_n \implies \det(A)^{-1} \cdot adj(A) = A^{-1}$$

Esempio:

- Prendiamo ancora una volta la nostra solita matrice esempio, il cui determinante sappiamo essere $\det(A) = 27$:

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 0 \end{pmatrix}$$

- La sua matrice dei cofattori corrisponde a:

$$A^* = \begin{pmatrix} cof_{1,1}(A) & cof_{1,2}(A) & cof_{1,3}(A) \\ cof_{2,1}(A) & cof_{2,2}(A) & cof_{2,3}(A) \\ cof_{3,1}(A) & cof_{3,2}(A) & cof_{3,3}(A) \end{pmatrix} = \begin{pmatrix} -48 & 42 & -3 \\ 24 & -21 & 6 \\ -3 & 6 & -3 \end{pmatrix}$$

mentre la conseguente matrice aggiunta corrisponde a:

$$adj(A) = \begin{pmatrix} -48 & 24 & -3 \\ 42 & -21 & 6 \\ -3 & 6 & -3 \end{pmatrix}$$

- Dunque, la matrice inversa di A corrisponde a:

$$A^{-1} = \frac{1}{27} \begin{pmatrix} -48 & 24 & -3 \\ 42 & -21 & 6 \\ -3 & 6 & -3 \end{pmatrix} = \frac{1}{9} \begin{pmatrix} -16 & 8 & -1 \\ 14 & -7 & 2 \\ -1 & 2 & -1 \end{pmatrix}$$

Observation 64

Data una matrice $A \in Mat_{2 \times 2}(K)$, si verifica che:

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \implies A^{-1} = \frac{1}{ad - bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

Dimostrazione:

- Sia

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

- La sua matrice aggiunta corrisponde a:

$$A^* = \begin{pmatrix} d & -c \\ -b & a \end{pmatrix} \implies adj(A) = (A^*)^T = A = \begin{pmatrix} d & -b \\ -c & d \end{pmatrix}$$

- Di conseguenza, la sua inversa sarà:

$$A^{-1} = \frac{1}{\det(A)} \cdot adj(A) = \frac{1}{ad - bc} \begin{pmatrix} d & -b \\ -c & d \end{pmatrix}$$

9.7 Teorema degli orlati

Definition 90. Orlato di un minore

Data una matrice $A \in Mat_{m \times n}(K)$ e dati un suo minore M di ordine r e un minore M' di ordine $r + 1$, diciamo che M' è un **orlato** di M se quest'ultimo è anche un minore di M'

Esempio:

- Consideriamo la matrice

$$A = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 \\ 9 & 10 & 11 & 12 \end{pmatrix}$$

e il suo minore M di ordine 2 ottenuto eliminando le colonne 2 e 4 e la riga 3

$$M = \begin{pmatrix} 1 & 3 \\ 5 & 7 \end{pmatrix}$$

- Gli orlati di M corrispondono a:

$$M'_1 = \begin{pmatrix} 1 & 3 & 4 \\ 5 & 7 & 8 \\ 9 & 11 & 12 \end{pmatrix} \quad M'_2 = \begin{pmatrix} 1 & 2 & 3 \\ 5 & 6 & 7 \\ 9 & 10 & 11 \end{pmatrix}$$

Observation 65

Data $A \in \text{Mat}_{m \times r}(K)$ e un suo minore M di ordine r , allora M ha $(m-r)(n-r)$ orlati in A

Theorem 83. Teorema degli orlati (o di Kronecker)

Data $A \in \text{Mat}_{m \times r}(K)$, le seguenti condizioni sono equivalenti:

1. $rk(A) = r$
2. Esiste un minore M di ordine r con $\det(M) \neq 0$, dove per ogni minore B di ordine maggiore di r si ha che $\det(B) = 0$
3. Esiste un minore M di ordine r con $\det(M) \neq 0$, dove per ogni orlato M' di M si ha $\det(M') = 0$

Esempi:

1. • Vogliamo discutere il comportamento di tale sistema al variare dei parametri $a, b \in \mathbb{R}$:

$$\begin{cases} ax + y + z = 1 \\ x + ay + z = 0 \\ x + y + az = b \end{cases} \implies A_b = \left(\begin{array}{ccc|c} a & 1 & 1 & 1 \\ 1 & a & 1 & 0 \\ 1 & 1 & a & b \end{array} \right) \implies$$

$$\implies \begin{cases} rk(A_b) = rk(A) & \text{se } \dim(A^1, \dots, A^n, b) = \dim(A^1, \dots, A^n) \\ rk(A_b) = rk(A) + 1 & \text{se } \dim(A^1, \dots, A^n, b) \neq \dim(A^1, \dots, A^n) \end{cases}$$

- Tramite la regola di Sarrus, otteniamo che il determinante corrisponde a:

$$\det(A) = a^3 + 1 + 1 - a - a - a = a^3 - 3a + 2 = (a+2)(a-1)^2$$

- Se $a \neq 1$ o $a \neq -2$ allora $\det(A) \neq 0$, implicando che $rk(A) = 3$.

Inoltre, siccome $rk(A_b) \leq \min(3, 4) = 3$ e siccome $rk(A_b) = rk(A)$ oppure $rk(A_b) = rk(A) + 1$, allora ne segue necessariamente che $rk(A) = rk(A_b) = 3$.

Per il teorema di Rouché-Capelli, lo spazio affine generato dalle soluzioni ha dimensione pari a 0, dunque il sistema è **determinato** ed esiste un'unica soluzione dipendente dai parametri assunti da a e b .

- Se $a = 1$, allora $\det(A) = 0$, poiché radice del polinomio precedentemente trovato.

Tuttavia, dalla riduzione a scala otteniamo che::

$$A_b = \left(\begin{array}{ccc|c} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & b \end{array} \right) \xrightarrow{R_2+=-R_1} \left(\begin{array}{ccc|c} 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & -1 \\ 1 & 1 & 1 & b \end{array} \right)$$

$$\begin{aligned} &\xrightarrow{R_3+=-R_1} \left(\begin{array}{ccc|c} 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & b-1 \end{array} \right) \xrightarrow{R_3+=-R_2} \left(\begin{array}{ccc|c} 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & b \end{array} \right) \\ &\xrightarrow{R_3+=b \cdot R_2} \left(\begin{array}{ccc|c} 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 \end{array} \right) \end{aligned}$$

implicando che $rk(A) = 1$ e $rk(A_b) = 2$, dunque il sistema **non ammette soluzioni**.

- Se $a = -2$, allora $\det(A) = 0$, poiché radice del polinomio precedentemente trovato.

Per il teorema degli orlati, si ha che l'unico orlato del minore $M_{3,3}$, dove $\det(M_{3,3}) = 3$ è la matrice A stessa, che sappiamo avere determinante nullo, dunque $rk(A) = 2$

$$A = \begin{pmatrix} -2 & 1 & 1 \\ 1 & -2 & 1 \\ 1 & 1 & -2 \end{pmatrix} \implies rk(A) = 2$$

Nel caso della matrice A_b , invece, consideriamo il seguente minore:

$$A_b = \left(\begin{array}{ccc|c} -2 & 1 & 1 & 1 \\ 1 & -2 & 1 & 0 \\ 1 & 1 & -2 & b \end{array} \right)$$

Gli unici due orlati di tale minore sono:

$$\left\{ \begin{array}{l} M'_1 = \begin{pmatrix} -2 & 1 & 1 \\ 1 & -2 & 1 \\ 1 & 1 & -2 \end{pmatrix} = A \implies \det(M'_1) = \det(A) = 0 \\ M'_2 = \begin{pmatrix} -2 & 1 & 1 \\ 1 & -2 & 0 \\ 1 & 1 & b \end{pmatrix} \implies \det(M'_2) = 4b + 0 + 1 + 2 - b = 3b + 3 \end{array} \right.$$

Dunque, si ha che:

$$rk(A) = \begin{cases} 2 & \text{se } a = -2, b = -1 \implies rk(A) = rk(A_b) \implies \exists \text{ inf. soluzioni} \\ 3 & \text{se } a = -2, b \neq -1 \implies rk(A) \neq rk(A_b) \implies \nexists \text{ soluzioni} \end{cases}$$

- In particolare, se $a = -2$ e $b = -1$, possiamo trovare le infinite soluzioni del sistema in funzione di x :

$$\begin{cases} -2x + y + z = 1 \\ x - 2y + z = 0 \\ x + y - 2z = -1 \end{cases} \implies \begin{cases} -2y + z = -x \\ y - 2z = 1 - x \end{cases}$$

applichiamo la regola di Cramer per trovare il valore di y in funzione di x , per poi sostituire il valore ottenuto nella seconda equazione, trovando il valore di z in funzione di x :

$$\begin{cases} y = \frac{1}{3} \cdot \det \begin{pmatrix} -x & 1 \\ -1-x & -2 \end{pmatrix} = \frac{1}{3}(3x+1) = x + \frac{1}{3} \\ y - 2z = 1 - x \end{cases} \implies \begin{cases} y = x + \frac{1}{3} \\ z = \frac{2}{3} + x \end{cases}$$

Le soluzioni del sistema indeterminato, quindi, appaiono nella forma:

$$\begin{pmatrix} y \\ z \end{pmatrix} = \begin{pmatrix} \frac{1}{3} \\ \frac{2}{3} \end{pmatrix} + x \begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

dunque generanti una retta (difatti, la dimensione dello spazio affine generato è $n - rk(A) = 3 - 2 = 1$)

2. • Consideriamo il seguente insieme di equazioni parametriche corrispondenti ad un sottospazio affine in \mathbb{R}^3 , già analizzato precedentemente:

$$V = \left\{ \begin{pmatrix} 1 \\ 0 \\ -1 \end{pmatrix} + t_1 \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} + t_2 \begin{pmatrix} 4 \\ 5 \\ 6 \end{pmatrix} \mid t_1, t_2 \in \mathbb{R} \right\}$$

- Siccome $\dim(V) = 2$, si verifica che

$$\begin{pmatrix} x \\ y \\ z \end{pmatrix} \in V \iff rk(A) = rk \begin{pmatrix} 1 & 4 & x-1 \\ 2 & 5 & y \\ 3 & 6 & z+1 \end{pmatrix} = 2$$

- Considerando il minore $M_{3,3}$, si ha che:

$$M_{3,3} = \begin{pmatrix} 1 & 4 \\ 2 & 5 \end{pmatrix} \implies \det(M_{3,3}) = 5 - 8 = -3 \neq 0$$

- Siccome la matrice iniziale stessa è l'unico orlato di $M_{3,3}$, per il teorema degli orlati si verifica che:

$$rk(A) = \begin{cases} 2 & \text{se } \det(A) = 0 \\ 3 & \text{se } \det(A) \neq 0 \end{cases}$$

- Dunque, si ha che:

$$\begin{pmatrix} x \\ y \\ z \end{pmatrix} \in V \iff rk(A) = 2 \iff \det(A) = 0$$

- Utilizzando lo sviluppo di Laplace sulla terza colonna, si ha che:

$$\begin{aligned} \det(A) = 0 &\iff (x-1) \cdot \det \begin{pmatrix} 2 & 5 \\ 3 & 6 \end{pmatrix} - y \cdot \det \begin{pmatrix} 1 & 4 \\ 3 & 6 \end{pmatrix} + (z-1) \cdot \det \begin{pmatrix} 1 & 4 \\ 2 & 5 \end{pmatrix} = 0 \iff \\ &\iff -3(x-1) + 6y - 3(z+1) \iff -3x + 6y - 3z = 0 \iff x - 2y + z = 0 \end{aligned}$$

- L'insieme di equazioni parametriche dato, quindi, equivale al seguente sistema di equazioni cartesiane:

$$\{ x - 2y + z = 0$$

corrispondente ad una retta in \mathbb{R}^3

3. • Dati la seguente retta r e il seguente piano π

$$r = \begin{cases} x = -2 + 3a \\ y = 1 - 2a \\ z = 5a \end{cases} \quad \pi = \begin{cases} x = 4 - 2b + 5c \\ y = 3b - c \\ z = 1 + b - 2c \end{cases}$$

possiamo trovare l'intersezione $r \cap \pi$ in \mathbb{R}^3 nei seguenti tre modi:

- (a) Troviamo i valori di a, b e c unendo i due sistemi:

$$\begin{cases} -2 + 3a = 4 - 2b + 5c \\ 1 - 2a = 3b - c \\ 5a = 1 + b - 2c \end{cases} = \begin{cases} 3a + 2b - 5c = 6 \\ 2a + 3b - c = 1 \\ 5a - b + 2c = 1 \end{cases} \implies A = \left(\begin{array}{ccc|c} 3 & 2 & -5 & 6 \\ 2 & 3 & -1 & 1 \\ 5 & -1 & 2 & 1 \end{array} \right)$$

Siccome $\det(A) = 82$ (*calcolo omissso*), possiamo applicare la regola di Cramer per trovare il valore di a , per poi sostituirlo nel sistema e trovare il valore di b e c :

$$\begin{aligned} &\begin{cases} a = \frac{1}{82} \cdot \det \begin{pmatrix} 6 & 2 & -5 \\ 1 & 3 & -1 \\ 1 & -1 & 2 \end{pmatrix} = \frac{1}{82} \cdot 44 = \frac{22}{41} \\ c = 2a + 3b - 1 \\ b = 5a + 2c - 1 \end{cases} \implies \\ &\begin{cases} a = \frac{22}{41} \\ c = \frac{44}{41} + 3b - 1 = 3b + \frac{3}{41} \\ b = \frac{110}{41} + 2c - 1 = 2c + \frac{69}{41} \end{cases} \implies \begin{cases} a = \frac{22}{41} \\ c = 3 \left(2c + \frac{69}{41} \right) + \frac{3}{41} = 6c + \frac{210}{41} \\ b = 2c + \frac{69}{41} \end{cases} \implies \\ &\implies \begin{cases} a = \frac{22}{41} \\ c = -\frac{42}{41} \\ b = 2 \left(-\frac{42}{41} \right) + \frac{69}{41} = -\frac{15}{41} \end{cases} \implies \begin{cases} x = -2 + 3a \\ y = 1 - 2a \\ z = 5a \end{cases} = \begin{cases} x = -\frac{16}{41} \\ y = -\frac{3}{41} \\ z = \frac{110}{41} \end{cases} \end{aligned}$$

(b) Troviamo il sistema di equazioni cartesiane descrittive π :

$$\begin{aligned}\pi = \begin{cases} x = 4 - 2b + 5c \\ y = 3b - c \\ z = 1 + b - 2c \end{cases} &\iff \begin{pmatrix} x-4 \\ y \\ z-1 \end{pmatrix} = b \begin{pmatrix} -2 \\ 3 \\ 1 \end{pmatrix} + c \begin{pmatrix} 5 \\ -1 \\ -2 \end{pmatrix} \iff \\ &\iff rk \begin{pmatrix} -2 & 5 & x-4 \\ 3 & -1 & y \\ 1 & -2 & z-1 \end{pmatrix} = 2\end{aligned}$$

Siccome $\det(M_{3,3}) = -13 \neq 0$, per il teorema degli orlati, si ha che:

$$\begin{aligned}\iff rk \begin{pmatrix} -2 & 5 & x-4 \\ 3 & -1 & y \\ 1 & -2 & z-1 \end{pmatrix} = 2 &\iff \det \begin{pmatrix} -2 & 5 & x-4 \\ 3 & -1 & y \\ 1 & -2 & z-1 \end{pmatrix} = 0 \iff \\ (x-4)(-5) - y(-1) + (z-1)(-13) &= 0 \iff 5x - y + 13z = 33\end{aligned}$$

Siccome $x \in r \cap \pi \iff x \in r \wedge x \in \pi$, sostituendo i valori assunti da x, y e z nell'equazione cartesiana di π otteniamo che:

$$-5x + y - 13z = 33 \iff 5(-2 + 3a) - (1 - 2a) + 13(5a) = 33 \iff a = \frac{22}{41}$$

Una volta trovato il valore di a , procediamo analogamente al metodo precedente, sostituendo a nell'equazione parametrica di π e ricavando b e c per sostituzione.

(c) Troviamo il sistema di equazioni cartesiane descrittive π e il sistema di equazioni cartesiane descrittive r .

Sappiamo già che:

$$\begin{pmatrix} x \\ y \\ z \end{pmatrix} \in \pi \iff 5x - y + 13z = 33$$

dunque ricaviamo le equazioni cartesiane di r :

$$\begin{aligned}r = \begin{cases} x = -2 + 3a \\ y = 1 - 2a \\ z = 5a \end{cases} &\iff \begin{pmatrix} x+2 \\ y-1 \\ z \end{pmatrix} = a \begin{pmatrix} 3 \\ -2 \\ 5 \end{pmatrix} \iff \\ &\iff rk \begin{pmatrix} 3 & x+2 \\ -2 & y-1 \\ 5 & z \end{pmatrix} = 1\end{aligned}$$

Considerando il minore di ordine 1 corrispondente all'entrata $a_{1,1} = 3$, dove quindi $\det(a_{1,1}) = 3$, per il teorema degli orlati si ha che:

$$rk \begin{pmatrix} 3 & x+2 \\ -2 & y-1 \\ 5 & z \end{pmatrix} = 1 \iff \begin{cases} \det \begin{pmatrix} 3 & x+2 \\ -2 & y-1 \end{pmatrix} = 0 \\ \det \begin{pmatrix} 3 & x+2 \\ 5 & z \end{pmatrix} = 0 \end{cases} \iff \begin{cases} 2x + 3y + 1 = 0 \\ -5x + 3z - 10 = 0 \end{cases}$$

Possiamo quindi costruire un nuovo sistema di equazioni cartesiane corrispondente a $r \cap \pi$ utilizzando le due equazioni cartesiane descrittive r e l'equazione cartesiana descrivente π :

$$\begin{pmatrix} x \\ y \\ z \end{pmatrix} \in r \cap \pi \iff \begin{cases} 5x - y + 13z = 33 \\ 2x + 3y + 1 = 0 \\ -5x + 3z - 10 = 0 \end{cases}$$

Poiché il determinante della matrice dei coefficienti associata a tale sistema è diverso da 0, è possibile ricavare i valori di x, y e z tramite la regola di Cramer, ottenendo una soluzione analoga agli altri due metodi

9.8 Matrici simili

Definition 91. Gruppo generale e speciale lineare

Definiamo come **gruppo generale lineare** il gruppo (GL, \cdot) , dove

$$GL(n, K) = \{A \in Mat_{n \times n}(K) \mid \det(A) \neq 0\}$$

Definiamo come **gruppo speciale lineare** il sottogruppo $(SL, \cdot) \subset (GL, \cdot)$, dove

$$SL(n, K) = \{A \in Mat_{n \times n}(K) \mid \det(A) = 1\}$$

Definition 92. Matrici simili

Date due matrici $A, B \in Mat_{n \times n}(K)$, tali matrici vengono dette **simili** se si verifica che:

$$\exists C \in GL(n, K) \mid A = C^{-1}BC$$

Definition 93. Matrice di transizione (o di cambiamento di base)

Sia $f : V \rightarrow V$ un endomorfismo e siano $\mathcal{B} = v_1, \dots, v_n$ e $\mathcal{C} = w_1, \dots, w_n$ due basi di V .

Data B la matrice di f in base \mathcal{B} e C la matrice di f in base \mathcal{C} , definiamo come **matrice di transizione (o di cambiamento di base)** la matrice $A = (A^1, \dots, A^n)$ tale che:

$$\forall j \in [1, n], A^j = \begin{pmatrix} a_{1,j} \\ \vdots \\ a_{n,j} \end{pmatrix} \mid w_j = a_{1,j}v_1 + \dots + a_{n,j}v_n$$

In tal caso, si verifica che $A \in GL(n, K)$ e $C = A^{-1}BA$:

(*dimostrazione omessa*)

9.8.1 Invarianti per similitudine**Proposition 84**

Se $A, B \in Mat_{n \times n}(K)$ sono matrici simili, allora

$$\det(A) = \det(B)$$

Dimostrazione:

- Sia $C \in GL(n, K) \mid B = C^{-1}AC$. Siccome $\det(C^{-1}) = \det(C)^{-1}$, si verifica che:

$$\det(B) = \det(C^{-1}AC) = \det(C^{-1})\det(A)\det(C) = \det(C)^{-1}\det(A)\det(C) = \det(A)$$

Definition 94. Traccia di una matrice

Data una matrice $A \in Mat_{n \times n}(K)$, definiamo come **traccia** di A la somma delle entrate sulla diagonale principale:

$$tr(A) = \sum_{k=1}^n a_{k,k}$$

Observation 66

Date $A \in Mat_{m \times n}(K)$ e $B \in Mat_{n \times m}(K)$, si verifica che:

$$tr(AB) = tr(BA)$$

Dimostrazione:

- Il risultato segue dalla definizione stessa di prodotto tra matrici:

$$\operatorname{tr}(AB) = \sum_{k=1}^n (ab)_{k,k} = \sum_{k=1}^n \sum_{j=1}^m a_{k,j} b_{j,k} = \sum_{j=1}^m \sum_{k=1}^n b_{j,k} a_{k,j} = \sum_{k=1}^n (ba)_{k,k} = \operatorname{tr}(BA)$$

Proposition 85

Se $A, B \in \operatorname{Mat}_{n \times n}(K)$ sono matrici simili, allora

$$\operatorname{tr}(A) = \operatorname{tr}(B)$$

Dimostrazione:

- Se $\exists C \in GL(n, K) \mid B = C^{-1}AC$, allora

$$\operatorname{tr}(B) = \operatorname{tr}(C^{-1}AC) = \operatorname{tr}(C^{-1}CA) = \operatorname{tr}(A)$$

Definition 95. Polinomio caratteristico

Data una matrice $A \in \operatorname{Mat}_{n \times n}(K)$, definiamo come **polinomio caratteristico** di A come:

$$p_A(x) := \det(xI_n - A)$$

Esempio:

- Data la matrice

$$A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$$

il suo polinomio caratteristico corrisponde a:

$$p_A(x) = \det \left(\begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix} - \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \right) = \det \begin{pmatrix} x-1 & -2 \\ -3 & x-4 \end{pmatrix} = x^2 - 5x - 2$$

- Data la matrice

$$A = \begin{pmatrix} 1 & 0 & -1 \\ 2 & 3 & 0 \\ 1 & 0 & 1 \end{pmatrix}$$

il suo polinomio caratteristico corrisponde a:

$$p_A(x) = \det \begin{pmatrix} x-1 & 0 & +1 \\ -2 & x+3 & 0 \\ -1 & 0 & x-1 \end{pmatrix} = (x-3)(x^2 - 2x + 2)$$

Proposition 86

Se $A, B \in Mat_{n \times n}(K)$ sono matrici simili, allora

$$p_A(x) = p_B(x)$$

Dimostrazione:

- Se $\exists C \in GL(n, K) \mid B = C^{-1}AC$, allora

$$\begin{aligned} p_B(x) &= \det(xI_n - B) = \det(xI_n - C^{-1}AC) = \det(xC^{-1}C - C^{-1}AC) = \\ &= \det(C^{-1}xI_nC - C^{-1}AC) = \det(C^{-1}(xI_n - A)C) = \det(C^{-1})\det(xI_n - A)\det(C) = \\ &= \det(C)^{-1}\det(xI_n - A)\det(C) = \det(xI_n - A) = p_A(x) \end{aligned}$$

Observation 67

Data una matrice $A \in Mat_{n \times n}(K)$, si verifica che:

$$p_A(x) = x^n - \text{tr}(A)x^{n-1} + \dots + (-1)^n \det(A)$$

Definition 96. Autovalori ed Autovettori

Data $A \in Mat_{n \times n}$ e uno scalare $\lambda \in K$, le seguenti condizioni sono equivalenti:

1. $p_A(\lambda) = 0$
2. $\exists v \neq 0_{K^n} \in K^n \mid Av = \lambda v$

Definiamo quindi come **autovalori** della matrice le radici del polinomio caratteristico di A . Se $\lambda \in K$ è un autovalore di A , allora definiamo **autovettore** relativo a λ una qualunque soluzione $v \neq 0_{K^n}$ del sistema:

$$(\lambda I_n - A)v = 0 \quad \text{oppure} \quad (A - \lambda I_n)v = 0$$

Dimostrazione:

- Notiamo come

$$\exists v \in K^n \mid Av = \lambda v \iff \begin{cases} 0 = \lambda v - Av \iff 0 = (\lambda I_n - A)v \\ Av - \lambda v = 0 \iff (A - \lambda I_n)v = 0 \end{cases}$$

- Poiché $(\lambda I_n - A) \cdot 0_{K^n} = 0_{K^n}$, esiste sempre una soluzione banale del sistema.
- Supponiamo quindi che esista $\exists v \neq 0_{K^n} \in K^n \mid Av = \lambda v$:

$$\begin{aligned} \exists v \neq 0_{K^n} \in K^n \mid (\lambda I_n - A)v = 0 &\iff \text{Ker}(L_{(\lambda I_n - A)}) \neq \{0_{K^n}\} \iff \\ &\iff \dim(\text{Ker}(L_{(\lambda I_n - A)})) > 0 \iff \text{rk}(\lambda I_n - A) = n - \dim(\text{Ker}(L_{(\lambda I_n - A)})) < n \iff \\ &\iff \det(\lambda I_n - A) = 0 \iff p_A(\lambda) = 0 \end{aligned}$$

Definition 97. Spettro e Autospazio relativo

Data una matrice $A \in \text{Mat}_{n \times n}(K)$, definiamo come **spettro** di A l'insieme dei suoi autovalori

$$Sp(A) = \{\lambda \in K \mid p_A(\lambda) = 0\}$$

e come **autospazio relativo a λ** il sottospazio di A generato dagli autovettori relativi a λ :

$$E_\lambda(A) = \{v \in K^n \mid Av = \lambda v\}$$

Proposition 87

Se $A, B \in \text{Mat}_{n \times n}(K)$ sono matrici simili, allora

$$Sp(A) = Sp(B)$$

Inoltre, dato $\lambda \in Sp(A) = Sp(B)$ si ha che:

$$E_\lambda(A) = E_\lambda(B) \iff A = B$$

Dimostrazione:

- Se $\exists C \in GL(n, K) \mid B = C^{-1}AC$, allora $p_A(x) = p_B(x)$, dunque si ha che:

$$\mu \in Sp(A) \iff p_A(\mu) = p_B(\mu) = 0 \iff \mu \in Sp(B)$$

- Dato $\lambda \in Sp(A) = Sp(B)$, supponiamo che $E_\lambda(A) = E_\lambda(B)$. Ne segue quindi che:

$$E_\lambda(A) = E_\lambda(B) \iff \exists v \in K^n \mid Av = \lambda v = Bv \iff Av = Bv \iff A = B$$

Esempio:

- Consideriamo la seguente matrice

$$A = \begin{pmatrix} 1 & 1 & 3 \\ 1 & 0 & -5 \\ -2 & -1 & 2 \end{pmatrix}$$

- Il suo polinomio caratteristico corrisponde a:

$$p_A(x) = \det \begin{pmatrix} x-1 & -1 & -3 \\ -1 & x & 5 \\ 2 & 1 & x-2 \end{pmatrix} = x(x-1)(x-2)$$

dunque otteniamo che $Sp(A) = \{0, 1, 2\}$

- Gli autovettori dell'autospazio $E_0(A)$ corrispondono a:

$$v = \begin{pmatrix} x \\ y \\ z \end{pmatrix} \in E_0(A) \iff (0 \cdot I_n - A)v = 0 \iff \begin{cases} -x - y - 3z = 0 \\ -x + 5z = 0 \\ 2x + y - 2z = 0 \end{cases} \iff$$

$$\iff \begin{cases} x = 5t \\ y = -8t \\ z = t \end{cases} \iff \begin{pmatrix} x \\ y \\ z \end{pmatrix} = t \begin{pmatrix} 5 \\ -8 \\ 1 \end{pmatrix}, t \neq 0$$

- Gli autovettori dell'autospazio $E_1(A)$ corrispondono a:

$$v = \begin{pmatrix} x \\ y \\ z \end{pmatrix} \in E_1(A) \iff (1 \cdot I_n - A)v = 0 \iff \begin{cases} -y - 3z = 0 \\ -x + y + 5z = 0 \\ 2x + y - z = 0 \end{cases} \iff$$

$$\iff \begin{cases} x = 2t \\ y = -3t \\ z = t \end{cases} \iff \begin{pmatrix} x \\ y \\ z \end{pmatrix} = t \begin{pmatrix} 2 \\ -3 \\ 1 \end{pmatrix}, t \neq 0$$

- Gli autovettori dell'autospazio $E_2(A)$ corrispondono a:

$$v = \begin{pmatrix} x \\ y \\ z \end{pmatrix} \in E_0(A) \iff (2 \cdot I_n - A)v = 0 \iff \begin{cases} x - y - 3z = 0 \\ -x + 2y + 5z = 0 \\ 2x + y = 0 \end{cases} \iff$$

$$\iff \begin{cases} x = t \\ y = -2t \\ z = t \end{cases} \iff \begin{pmatrix} x \\ y \\ z \end{pmatrix} = t \begin{pmatrix} 1 \\ -2 \\ 1 \end{pmatrix}, t \neq 0$$

Definition 98. Molteplicità algebrica e geometrica

Data una matrice $A \in Mat_{n \times n}(K)$, per ogni autovalore $\lambda \in Sp(A)$ definiamo la sua:

- **Molteplicità algebrica** $\mu(\lambda)$, ossia la sua molteplicità come radice del polinomio caratteristico $p_A(x)$, corrispondente al più grande intero tale che:

$$\mu(\lambda) \in \mathbb{N}, (x - \lambda)^{\mu(\lambda)} \mid p_A(x)$$

- **Molteplicità geometrica** $\nu(\lambda)$, ossia la dimensione del suo autospazio relativo, corrispondente a:

$$\nu(\lambda) = \dim(E_\lambda(A)) = n - rk(\lambda I_n - A)$$

Per ogni $\lambda \in Sp(A)$, si verifica che:

$$1 \leq \nu(\lambda) \leq \mu(\lambda)$$

Proposition 88

Se $A, B \in Mat_{n \times n}(K)$ sono matrici simili, allora $\forall \lambda \in Sp(A) = Sp(B)$ si ha che:

$$\mu_A(\lambda) = \mu_B(\lambda) \quad \nu_A(\lambda) = \nu_B(\lambda)$$

9.8.2 Diagonalizzazione di una matrice**Definition 99. Matrice diagonale**

Sia $A \in Mat_{n \times n}(K)$. Tale matrice viene detta **diagonale** se $\forall i \neq j$ si ha che $a_{i,j} = 0$, ossia se sopra e sotto la diagonale principale vi sono tutti zeri

$$A = \begin{pmatrix} a_{1,1} & 0 & \cdots & \cdots & 0 \\ 0 & a_{2,2} & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & a_{n-1,n-1} & 0 \\ 0 & \cdots & \cdots & 0 & a_{n,n} \end{pmatrix}$$

In altre parole, una matrice viene detta diagonale se è sia triangolare superiore sia triangolare inferiore.

Definition 100. Matrici triangolarizzabili e diagonalizzabili

Una matrice $A \in Mat_{n \times n}(K)$ viene detta **triangolarizzabile** se simile ad una matrice triangolare $T \in Mat_{n \times n}(K)$, mentre viene detta **diagonalizzabile** se simile ad una matrice diagonale $D \in Mat_{n \times n}(K)$

Proposition 89

Data una matrice $A \in Mat_{n \times n}(K)$, le seguenti affermazioni sono equivalenti:

1. A è triangolarizzabile
2. La somma di tutte le sue molteplicità algebriche è n :

$$\sum_{\lambda \in Sp(A)} \mu(\lambda) = n = \dim(K^n)$$

3. Il suo polinomio caratteristico è completamente fattorizzabile:

$$p_A(x) = \prod_{\lambda \in Sp(A)} (x - \lambda)^{\mu(\lambda)}$$

Corollary 34

Per il teorema fondamentale dell'algebra, ne segue che ogni matrice $A \in Mat_{n \times n}(\mathbb{C})$ è triangolarizzabile.

Analogamente, ne segue che $A \in Mat_{n \times n}(\mathbb{R})$ è triangolarizzabile se e solo se

$$\lambda \in Sp(A) \implies \lambda \in \mathbb{R} \implies Sp(A) \subseteq \mathbb{R}$$

Esempio:

- Data la matrice

$$A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \in Mat_{2 \times 2}(\mathbb{R})$$

il suo polinomio caratteristico corrisponde a:

$$p_A(x) = \det \begin{pmatrix} x & 1 \\ -1 & x \end{pmatrix} = x^2 + 1$$

- Siccome $p_A(x) \in \mathbb{R}[x]$, $\deg(p_A(x)) = 2$ e $\Delta_{p_A(x)} < 0$, tale polinomio non è fattorizzabile, dunque A non è triangolarizzabile
- Se invece consideriamo la matrice $A' \in Mat_{2 \times 2}(\mathbb{C})$ avente entrate coincidenti a quelle di A , otteniamo che:

$$p_{A'}(x) = (x - i)(x + i) \in \mathbb{C}[x] \implies Sp(A') = \{\pm i\} \subseteq \mathbb{C}$$

dunque A' è triangolarizzabile

Proposition 90

Data una matrice $A \in Mat_{n \times n}(K)$, le seguenti affermazioni sono equivalenti:

1. A è diagonalizzabile
2. La somma di tutte le sue molteplicità geometriche è n :

$$\sum_{\lambda \in Sp(A)} \nu(\lambda) = n = \dim(K^n)$$

3. Esiste una base B^1, \dots, B^n di K^n tale che:

$$\lambda_1, \dots, \lambda_n \in Sp(A) \implies B^1 \in E_{\lambda_1}(A), \dots, B^n \in E_{\lambda_n}(A)$$

4. Il suo spettro contiene n autovalori diversi tra loro:

$$Sp(A) = \{\lambda_1, \dots, \lambda_n\}, \forall i \neq j \mid \lambda_i \neq \lambda_j$$

Observation 68

Data una matrice $A \in Mat_{n \times n}(K)$ e dati $v_1 \in E_{\lambda_1}(A), \dots, v_k \in E_{\lambda_k}(A)$, se $\forall i \neq j \mid \lambda_i \neq \lambda_j$, allora v_1, \dots, v_k sono linearmente indipendenti

Proposition 91. Matrice diagonalizzante

Data una matrice $A \in Mat_{n \times n}(K)$, se esiste una base B^1, \dots, B^n di K^n tale che:

- B^1 è base di $E_{\lambda_1}(A)$
- \vdots
- B^n è base di $E_{\lambda_n}(A)$

dove $\lambda_k \in Sp(A)$ e dove $\forall i \neq j \mid \lambda_i \neq \lambda_j$, allora:

$$\exists B = (B^1, \dots, B^n) \in GL(n, K) \mid D = B^{-1}AB$$

dove $D \in Mat_{n \times n}(K)$ è una matrice diagonale e dove B viene detta **matrice diagonalizzante**.

Esempio:

1. • Consideriamo la seguente matrice

$$A = \begin{pmatrix} 5 & -8 & 3 \\ 4 & -8 & 4 \\ 5 & -12 & 7 \end{pmatrix} \in Mat_{3 \times 3}(\mathbb{R})$$

- Il suo polinomio caratteristico corrisponde a:

$$\begin{aligned} p_A(x) &= \det \begin{pmatrix} x-5 & 8 & -3 \\ -4 & x+8 & -4 \\ -5 & 12 & x-7 \end{pmatrix} = \\ &= (x-5) \det \begin{pmatrix} x+8 & -4 \\ 12 & x-7 \end{pmatrix} + 4 \det \begin{pmatrix} 8 & -3 \\ 12 & x-7 \end{pmatrix} - 5 \det \begin{pmatrix} 8 & -3 \\ x+8 & -4 \end{pmatrix} = \\ &= (x-5)(x^2 + x - 8) + 4(8x - 20) - 5(3x - 8) = x^3 - 4x^2 + 4x = x(x-2)^2 \end{aligned}$$

dunque sappiamo che A è triangolarizzabile e che il suo spettro è $Sp(A) = \{0, 2\}$.

- Siccome affinché A sia anche diagonalizzabile è necessario che $\nu(0) + \nu(2) = 3 = \dim(\mathbb{R}^3)$, notiamo come:

$$1 \leq \nu(0) \leq \mu(0) \iff 1 \leq \nu(0) \leq 1 \iff \nu(0) = 1$$

di conseguenza, si ha che:

$$\nu(0) + \nu(2) = 3 \iff 1 + \nu(2) = 3 \iff \nu(2) = 2$$

- Consideriamo quindi il sistema $(2 \cdot I_n - A)v = 0$:

$$\begin{cases} -3x + 8y - 3z = 0 \\ -4x + 10y - 4z = 0 \\ -5x + 12y - 5z = 0 \end{cases} \implies (2 \cdot I_n - A) = \begin{pmatrix} -3 & 8 & -3 \\ -4 & 10 & -4 \\ -5 & 12 & -5 \end{pmatrix}$$

Si ha che:

$$\nu(2) = 2 = \dim(E_2(A)) = 3 - rk(2 \cdot I_n - A) = \iff rk(2 \cdot I_n - A) = 1$$

- Tuttavia, considerando il minore $M_{3,3}$, per il teorema degli orlati si verifica che:

$$\det \begin{pmatrix} -3 & 8 \\ -4 & 10 \end{pmatrix} = -30 + 32 = 2 \neq 0 \implies rk(2 \cdot I_n - A) \geq 2$$

Dunque si ha che $rk(2 \cdot I_n - A) \neq 1$, implicando quindi che A non sia diagonalizzabile.

- Difatti, si ha che:

$$1 \leq \nu(2) = 3 - rk(2 \cdot I_n - A) \leq 3 - 2 = 1 \iff \nu(2) = 1$$

e dunque che:

$$\nu(0) + \nu(2) = 1 + 1 = 2 \neq 3 = \dim(\mathbb{R}^3)$$

2. • Consideriamo la seguente matrice

$$A = \begin{pmatrix} 1 & k \\ 2 & k-1 \end{pmatrix} \in Mat_{2 \times 2}(\mathbb{R})$$

- Il suo polinomio caratteristico corrisponde a:

$$\begin{aligned} p_A(x) &= \det \begin{pmatrix} x-1 & -k \\ -2 & x-k-1 \end{pmatrix} = (x-1)(x-k-1) - 2k \\ &= x^2 - kx - k - 1 = (x+1)(x-k-1) \end{aligned}$$

dunque si ha che $Sp(A) = \{-1, k+1\}$

- Siccome $p_A(x)$ è completamente fattorizzabile indipendentemente dal valore assunto da k , allora A è sempre triangolarizzabile.
- Se $k = -2$, si ha che:

$$A = \begin{pmatrix} 1 & -2 \\ 2 & -3 \end{pmatrix} \implies p_A(x) = (x+1)^2 \implies Sp(A) = \{-1\}$$

Dunque A è diagonalizzabile se e solo se $\nu(-1) = 2$.

Tuttavia, considerando il sistema $(-1 \cdot I_n - A)v = 0$, notiamo che :

$$\begin{aligned} \begin{cases} -2x + 2y = 0 \\ -2x + 2y = 0 \end{cases} &\iff \{ x = ty = t \} \iff \\ \iff \begin{pmatrix} x \\ y \end{pmatrix} &= t \begin{pmatrix} 1 \\ 1 \end{pmatrix} \implies \nu(-1) = \dim(E_{-1}(A)) = 1 \end{aligned}$$

Dunque A non è diagonalizzabile se $k = -2$

- Se invece $k \neq -2$, si ha che:

$$p_A(x) = (x+1)(x-k-1) \implies Sp(A) = \{-1, k+1\}$$

Dunque A è diagonalizzabile, poiché vi sono 2 autovalori distinti.

- Difatti, notiamo come considerando il sistema $(-1 \cdot I_n - A)v = 0$ si ha che :

$$\begin{aligned} \begin{cases} -2x + ky = 0 \\ -2x + ky = 0 \end{cases} &\iff \{ x = ty = -\frac{k}{2}t \} \iff \\ \iff \begin{pmatrix} x \\ y \end{pmatrix} &= t \begin{pmatrix} 1 \\ -\frac{k}{2} \end{pmatrix} \implies \nu(-1) = \dim(E_{-1}(A)) = 1 \end{aligned}$$

mentre per il sistema $((k+1) \cdot I_n - A)v = 0$ si ha che :

$$\begin{aligned} \begin{cases} kx - ky = 0 \\ -2x + 2y = 0 \end{cases} &\iff \{ x = ty = t \} \iff \\ \iff \begin{pmatrix} x \\ y \end{pmatrix} &= t \begin{pmatrix} 1 \\ 1 \end{pmatrix} \implies \nu(k+1) = \dim(E_{k+1}(A)) = 1 \end{aligned}$$

dunque si ha che $\nu(-1) + \nu(k+1) = 2 = \dim(\mathbb{R}^2)$

- Inoltre, otteniamo che i due vettori trovati sono base della matrice diagonalizzante B :

$$B = \begin{pmatrix} 1 & 1 \\ -\frac{k}{2} & 1 \end{pmatrix} \implies D = B^{-1}AB \implies D = \begin{pmatrix} -1 & 0 \\ 0 & k+1 \end{pmatrix}$$

9.9 Matrici ortogonali

Definition 101. Base ortogonale

Siano v_1, \dots, v_n una base di \mathbb{R}^n , tale base viene detta **ortogonale** se i vettori sono a due a due perpendicolari, dunque se

$$\forall i \neq j, v_i \cdot v_j = 0$$

Definition 102. Base ortonormale

Siano v_1, \dots, v_n una base di \mathbb{R}^n , tale base è detta **ortonormale** se sono ortogonali e sono **versori**, ossia aventi norma pari ad 1, dunque se:

$$v_i \cdot v_j = \delta_{ij} = \begin{cases} \|v_i\| = 1 & \text{se } i = j \\ 0 & \text{se } i \neq j \end{cases}$$

dove δ_{ij} viene detto **delta di Kroneker**.

Observation 69

Le basi ortonormali possono essere ottenute da dalla base canonica e_1, \dots, e_n attraverso rotazioni e riflessioni

Observation 70

Data una base ortonormale $\mathcal{B} = v_1, \dots, v_n$ di \mathbb{R}^n e dato un vettore $w \in \mathbb{R}^n$, le coordinate di w nella base \mathcal{B} corrispondono a:

$$w = (w \cdot v_1) \cdot v_1 + \dots + (w \cdot v_n) \cdot v_n$$

Proposition 92

Data una matrice $A \in Mat_{n \times n}(\mathbb{R})$, le seguenti affermazioni sono equivalenti:

1. Le colonne A^1, \dots, A^n sono base ortogonale di \mathbb{R}^n
2. Le righe A_1, \dots, A_n sono base ortogonale di \mathbb{R}^n
3. $A^T \cdot A = I_n \iff A \in GL(n, \mathbb{R}) \mid A^{-1} = A^T$
4. $L_A : \mathbb{R}^n \rightarrow \mathbb{R}^n$ è isometria, ossia non cambia la distanza tra i punti del piano

Definition 103. Matrice ortogonale

Data una matrice $A \in Mat_{n \times m}(\mathbb{R})$, tale matrice viene detta **ortogonale** se A^1, \dots, A^n o A_1, \dots, A_n sono base ortonormale di \mathbb{R}^n

Corollary 35. Gruppo ortogonale

Definiamo come **gruppo ortogonale**, indicato come $O(n)$, il sottogruppo di $GL(n, \mathbb{R})$ contenente tutte le matrici ortogonali di ordine n :

$$O(n) = \{A \in GL(n, \mathbb{R}) \mid A^{-1} = A^T\}$$

Method 8. Algoritmo di Gram-Schmidt

Data una base v_1, \dots, v_n di \mathbb{R}^n , è possibile ottenere una base ortonormale di \mathbb{R}^n tramite il seguente algoritmo:

1. Preso $w_1 \in \mathbb{R}^n \mid ||w_1|| = 1$ e stessa direzione di v_1 , si ha che:

$$w_1 = \frac{v_1}{||v_1||} = \frac{v_1}{v_1 \cdot v_1} = \frac{1}{v_1} \iff w_1 \cdot v_1 = 1$$

dunque w_1, v_2, \dots, v_n sono base di \mathbb{R}^n

2. Poniamo $u_2 := v_2 - (v_2 \cdot w_1)w_1$, geometricamente equivalente alla proiezione di v_2 sulla retta perpendicolare a quella di w_1 . In tal modo, si ha che:

$$u_2 = v_2 - (v_2 \cdot w_1)w_1 \implies u_2 \cdot v_1 = v_2 \cdot v_1 - (v_2 \cdot w_1)w_1 \cdot v_1 = 0$$

dunque u_2 e v_1 sono perpendicolari

3. Ripetendo il punto 1) e 2), all'i-esima iterazione si ha che $w_1, \dots, w_{i-1}, v_i, \dots, v_n$ sono base di \mathbb{R}^n . Poniamo quindi

$$u_i := v_i - \sum_{j < i} (v_i \cdot w_j)w_j \implies u_i \cdot w_j = 0, \forall j < i$$

da cui ne segue che:

- $||w_1|| = \dots = ||w_i|| = 1$
- e $w_j \cdot w_h = 0, \forall 1 \leq j, h \leq i$
- $Span(w_1, \dots, w_i) = Span(v_1, \dots, v_i)$

4. Dopo n iterazioni otteniamo una base ortogonale w_1, \dots, w_n di \mathbb{R}^n

Definition 104. Matrice simmetrica

Data una matrice $A \in Mat_{n \times n}(K)$, tale matrice viene detta **simmetrica** se

$$A = A^T$$

Theorem 93. Teorema spettrale

Data una matrice simmetrica $S \in Mat_{n \times n}(\mathbb{R})$, le seguenti affermazioni sono equivalenti:

1. $Sp(S) \subset \mathbb{R}$
2. S è diagonalizzabile
3. Esiste una base ortonormale $\mathcal{B} = B^1, \dots, B^n$ di \mathbb{R}^n tale che B^i, \forall è autovettore di S
4. $\exists B \in O(n) \mid D = B^{-1}AB = B^TAB$ dove $D \in Mat_{n \times n}(\mathbb{R})$ è una matrice diagonale